Cluster States-based Quantum Networks

Ivan B. Djordjevic
University of Arizona, Department of Electrical and Computer Eng., 1230 E. Speedway Blvd., Tucson, AZ 85721, USA
E-mail: ivan@email.arizona.edu

Abstract– We propose to implement multipartite quantum communication network (QCN) by employing the cluster-state-based concept. The proposed QCN can be used to: (i) perform distributed quantum computing, (ii) teleport quantum states between any two nodes in QCN, and (iii) enable next generation of cyber security systems.

Quantum communication (QuCom) employs the quantum information theory concepts to realize the distribution of keys with verifiable security, commonly referred to as quantum key distribution (QKD) [1],[2]. Despite the appealing features of QuCom, there are some fundamental and technical challenges that need to be addressed prior to its widespread applications. For instance, the rate and distance of QuCom are fundamentally limited by the channel loss, which is specified by the rate-loss tradeoff.

Modern classical communication networks consist of multiple nodes connected by various types of channels, including free-space optical (FSO) links, optical fibers, ground-satellite links, wireless links, and coaxial cables. Such a heterogeneous architecture would be equally important for quantum communication networks (QCNs) as quantum nodes may access a QCN by different kinds of channels. Unfortunately, quantum communications have been individually validated in free-space, optical fibers, and between a satellite and a ground station, but a combined heterogeneous QCN entailing multiple types of heterogeneous channels remains elusive. Unlike in the point-to-point communication case, the fundamental quantum communication rate limits are not known even for the simplest broadcast and multiple-access channel settings. This motivates us to propose a global, cluster states based QCN. Several QKD testbeds have been reported so far including DARPA QKD network [3], Tokyo QKD network [4], and secure communication based on quantum cryptography (SECOQC) network [5]. The QKD can also be used to establish QKD-based campus-to-campus virtual private network [6]. However, all these networks employ the dark fiber infrastructure.

We propose to implement the multipartite QCN by employing the cluster state-based concept. The proposed quantum network can be used to: (i) perform distributed quantum computing, (ii) teleport quantum states between any two nodes in the network, and (iii) enable next generation of cyber security systems. The cluster states can be described using the stabilizer formalism and as such they can easily be certified by simple syndrome measurements. In this formalism, the cluster states can be interpreted as codewords of corresponding quantum error correction code, and corresponding errors can be corrected by simple syndrome decoding, among others. By performing simple Y and Z measurements on properly selected nodes we can straightforwardly establish the EPR pair between any two nodes in the network. Moreover, multiple EPR pairs can be established simultaneously. We propose further a cluster state-based quantum network of satellites that enables global coverage. The proposed satellite QCN will be composed of quantum subnetworks comprised of LEO satellites. Some of these LEO satellite-based quantum subnetworks will be connected to a subnetwork of MEO/GEO satellites. The LEO satellites will also be used to interconnect terrestrial cluster state-based quantum networks. Such a global QCN will enable the security on a global scale. This quantum global network can also be used to distribute the entangled states for quantum sensing applications and to enable distributed quantum computing on a global scale. To reconfigure the proposed QCN, the SDN concepts should be employed.

The cluster states belong to the class of the graph states [7], which also include Bell states, GHZ states, W-states, and various entangled states used in quantum error correction. When the cluster C is defined as a connected subset on a d-dimensional lattice, it obeys the set of eigenvalue equations $S_a|\phi\rangle_C = |\phi\rangle_C$, $S_a = X_a \underset{b\in N(a)}{\otimes} Z_b$, where S_a are *stabilizer operators* with $N(a)$ denoting the neighborhood of $a\in C$. To create a 2-D cluster state, we should use the approach proposed by Gilbert *at al.* [8], which employs linear states, generated by spontaneous parametric down conversion (SPDC), local unitaries, and type I fusion to create the desired 2-D cluster state. Once 2-D cluster state of nodes is created, by using properly selected Y and Z measurements we can establish the EPR pair between arbitrary two nodes in the quantum network. As an illustration, in Fig. 1 the 2-D cluster state with 9 nodes is shown. We are interested establishing EPR pairs between nodes 3 and 7 as well as nodes 1 and 9. To do so, we first perform Y measurements as follows: Y_8, Y_5, and Y_6 to get the intermediate stage. We then perform Z-measurement on 2 and Y measurement on 4 to get the two desired EPR pairs. Given that the 2-D cluster state is universal it is possible to use the same network architecture for both QCN and distributed quantum computing. We also imagine the scenario in which each node is equipped with multiple qubits, wherein several layers of 2-D cluster states are active at the time, which will allow us to simultaneously perform QCN and distributing quantum computing. Moreover, when several 2-D cluster states are run in parallel on the same set of network nodes, we will be able to reconfigure the QCN on the fly. This can be done with the help of the SDN concept. The SDN has been introduced to separate the control plane and data plane, manage network services through abstraction of higher-level functionality, and implement new applications and algorithms efficiently. It has already been studied to enable the coexistence of classical and quantum communication channels. Our SDN-based QCN architecture contains three layers, namely, application layer, control layer, and QCN layer. Users send their requests from application layer with the help of northbound interface to the SDN controller. The SDN controller allocates the QCN resources with the help of its global map through the southbound interface. The QCN layer can be composed of DWDM FSO/single-mode fiber (SMF)/few-mode fiber (FMF) links and QCN nodes. Any two nodes in QCN can communicate through either a dedicated SMF/FSO/FMF link or a wavelength channel. The SDN control can also help to determine sequence of measurements to be performed in order to establish the desired EPR pairs. To deal with time-varying channel conditions over heterogeneous links, we need to adapt channel configuration based on both application requirement and link condition.

The discrete variable (DV) QKD can be used to build QKD networks. Unfortunately, the DV-QKD is affected by the deadtime of single-photon detectors (SPDs), which limits the baud rate and consequently the secret-key rate (SKR). Moreover, even if Eve cannot get the key because DV-QKD is used, she can prevent parties from creating secure keys, which is similar to the Denial of Service (DoS) attack. Further, since SKRs for DV-QKD are low, the *quantum key pool*, storing the secure keys, will often be empty, hampering the operation of QKD networks. To solve for this problem we propose to use hybrid QKD-post-quantum cryptography (PQC) protocols, in which entanglement assisted QKD is used for raw key transmission (by employing established EPR pairs) and PQC in information reconciliation to reduce the leakage during the error reconciliation. PQC is typically referred to various cryptographic algorithms that are thought to be secure against any quantum computer-based attack. Unfortunately, the PQC is also based on unproven assumptions and some of the QPC algorithms might be broken in future by developing more sophisticated quantum algorithms. When quantum algorithm is used to break-up the PQC protocol the number of security bits $\log_2(L)$ (where L is number of operations) is much shorter than that for classical algorithms, and it is not sufficient to enable perfect security algorithms, such as one-time pad. However, when an (N,K) LDPC code of high rate is used in information reconciliation the number of parity bits $N–K << n$ (the codeword length used in PQC subsystem), which is sufficient to eliminate the leakage during the error correction stage. This is the reason why we propose here to use the PQC algorithms only in information reconciliation phase to limit the leakage due to transmission of parity bits over an authenticated classical channel (in conventional QKD). By using this approach, as illustrated in Fig. 2, the transmission distance between two nodes in QCN can be extended to even 1127 km, for typical system parameters. (The simulation details will be provided at the conference.)

Now, by connecting the *base stations* to the nodes in proposed QCNs we can provide the unconditional security to the future wireless networks. By organizing the base stations in a quantum optical mesh network and by employing the proposed hybrid QKD-PQC concept we can offer unconditional security to a large number of users. The IoT architecture will comprise widely distributed nodes connected via different types of channels to enable new functionalities in communication, sensing, and computing. Communication security in such a giant network is of paramount importance. Our proposed QCNs will underpin the unconditional physical-layer security of the IoT given that it will allow arbitrary two nodes to securely transmit data at high rate via an optical link. Critically, the security of such a network will not rest upon the trusted-node assumption, and a compromised node will not affect the security of other nodes. As such, the proposed cluster states based QCNs will lead to a substantially stronger security level for IoT.

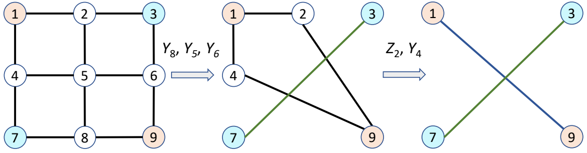

Fig. 1 Establishing EPR pairs between nodes 1 and 9 as well as between nodes 3 and 7 in a cluster state-based QCN.

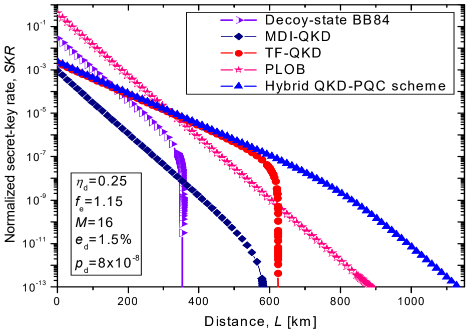

Fig. 2 Proposed hybrid QKD-PQC scheme against measurement device independent (MDI)-QKD and twin field (TF)-QKD in terms of SKR vs. distance, assuming that ultra-low loss fiber is used. PLOB: Pirandola-Laurenza-Ottaviani-Banchi bound.

References

[1] S.-K. Liao, *et al.*, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, pp. 43–47, 2017.

[2] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution.* Springer Nature Switzerland, 2019.

[3] C. Elliott, *et al.*, “Current status of the DARPA quantum network (Invited Paper),” in Proc. *SPIE 5815, Quantum Information and Computation III*, (25 May 2005).

[4] M. Sasaki, *et al.*, “Field test of quantum key distribution in the Tokyo QKD Network,” *Opt. Express*, vol. 19, p. 10387, 2011.

[5] R. Alléaume, *et al.*, “Using quantum key distribution for cryptographic purposes,” *J. Theoretical Computer Science*, vol. 560, no. P1, pp. 62-81, Dec. 2014.

[6] A. Mink, *et al.*, “Quantum Key Distribution (QKD) and commodity security protocols: introduction and integration,” *Intern. J. Netw. Sec. & Its Applications*, vol. 1, pp. 101-112, 2009.

[7] H. J. Briegel, “Cluster States,” *Compendium of Quantum Physics* (D. Greenberger, *et al.* (eds)), pp. 96-105. Springer, 2009.

[8] G. Gilbert, *et al.*, “Efficient construction of photonic quantum-computational clusters,” *Phys. Rev. A*, vol. 73, p. 064303, 2006.