Opportunistic quantum network coding based on quantum teleportation

Tao Shang, Gang Du, Jian-wei Liu
School of Electronic and Information Engineering, Beihang University, Beijing 100083, China

With the development of quantum information, network coding has been gradually applied to quantum network. Quantum network coding (QNC) has gradually become a major research area by virtue of its capability to improve the security and efficiency of quantum communication. Several achievements have been made in theoretical research in recent years. As a paradigm of wireless network coding protocol, “COPE” (complete opportunity encoding) allows nodes to combine more than two packets together through opportunistic listening. However, these existing schemes cannot provide opportunistic characteristic for quantum network like COPE. Recently, the achievement of air-to-ground quantum key distribution represents a key milestone towards quantum communication in free space. Thus it is worth concerning whether quantum network coding with opportunistic characteristic is also feasible or not. Inspired by the characteristic of mixed channels of quantum teleportation, we present an opportunistic quantum network coding scheme to solve above problem by utilizing quantum channel for secure transmission of quantum states and classical channel for both opportunistic listening to neighbor states and opportunistic coding by means of broadcasting measurement outcome.

Our objective is to strengthen the cooperation by virtue of opportunistic characteristics and maximize the gain from network coding. From the viewpoint of motivation, an opportunistic quantum network coding scheme is considered to provide opportunistic characteristic for quantum network so as to improve network performance. Since the demand of channel listening has great conflicts with the fact that quantum channel cannot be overheard without disturbance, it is a key issue to provide a feasible approach to channel listening and distinguish between legal listening and illegal eavesdropping in quantum communication.

The main idea of our scheme is described as follows: quantum teleportation uses EPR pairs as quantum channel by sharing EPR pairs between communication parties, while it uses classical channel to transmit the measurement outcome. Assume there exists an eavesdropper during the transmission process. If it listens to quantum channel, quantum channel verification can help find the eavesdropper. If it listens to classical channel, the leakage of measurement outcome does not destroy the security of transmitted quantum states even though the eavesdropper cannot be found. Thus if channel listening was desired for normal acquisition information, only does it happen to classical channel. As a more meaningful approach, the transmission over classical channel can provide an immediate notification for neighboring nodes that a quantum information has just been transmitted from one communication party to another communication party, which is very important for opportunistic network coding to grasp opportunity to obtain neighbor's states at the right time. Meanwhile, multiple measurement outcomes can be transmitted simultaneously by broadcast, which will reduce the times of transmissions.

A typical network model for opportunistic quantum network coding is constructed as shown in Figure 1. In this scenario, L is a relay node which will try to overhear its neighbors and encode own packets, A and B are L’s neighbors and can communicate with each other. E is an eavesdropper who may launch classical attacks or quantum attacks. Every two legal nodes share prior entangled EPR pairs, which are the foundation of quantum teleportation and quantum channel verification.

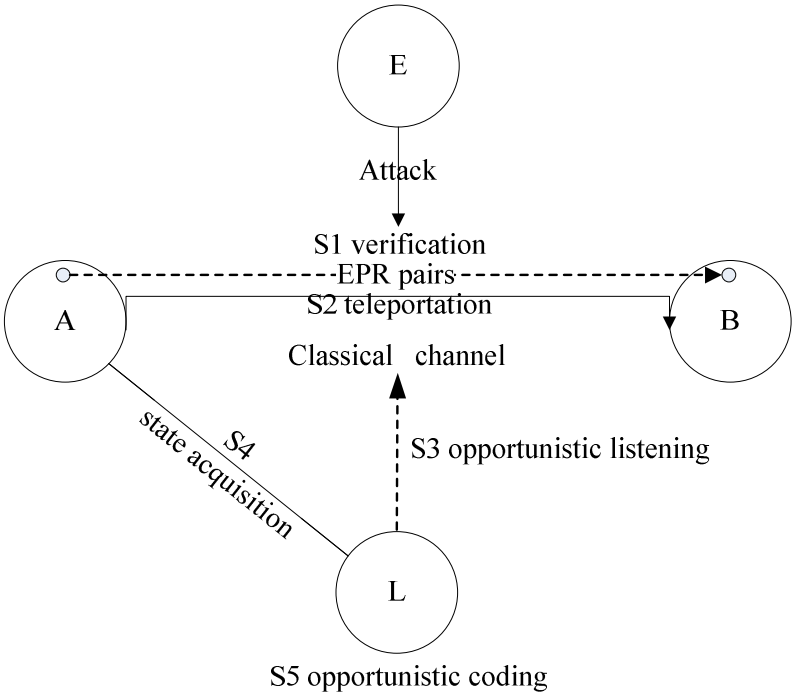

Fig. 1. Network model (Si denotes the step of the proposed scheme)

As we know, it is most difficult for opportunistic quantum network coding to realize opportunistic operation such as opportunistic listening and opportunistic coding in the three core parts of COPE due to the unconditional security of quantum communication. Thus we will focus on how to acquire coding opportunity from neighborhood and use the broadcasting characteristic of classical channels to reduce the times of transmissions. Concretely, the main contributions of our work are: (1) A quantum network coding scheme with opportunistic characteristic is first proposed by taking full advantage of channel characteristic of quantum teleportation. Based on the principle that the measurement outcome of quantum teleportation is transmitted over a classical channel, the scheme has two main opportunistic characteristics. One is opportunistic listening. A listener can tell when the quantum information transmission is occurring in the neighborhood so as to further obtain neighbor's state. The other is opportunistic coding. A relay node can transmit multiple measurement outcomes simultaneously by broadcast. Such opportunistic characteristics can improve network throughput. (2) The problem of how to distinguish between legal listener and illegal eavesdropper is well solved. Quantum channel verification method for EPR pair is used to detect eavesdroppers, while auxiliary classical channels for quantum teleportation are delicately used to provide the opportunity of channel listening for the transmitted quantum states.

According to the above approach, our scheme has opportunistic characteristic by listening to classical channel and broadcasting measurement outcomes via classical channel, which generally cannot be achieved in conventional quantum network. Meanwhile, it can resist classical passive attack and quantum active attack. Furthermore, we will explore the usage of mixed channels of quantum teleportation. Classical channel can not only be used to broadcast measurement outcomes, but also be used to broadcast encoded packet directly on the premise of secure transmission. Moreover, some new quantum operations on qubit can be designed for the part of opportunistic coding, which will realize the improvement of transmission performance in quantum networks.