CC-01-03

Research on quantum-secured networking: QKD for networks and networks for QKD

Chankyun Lee

KISTI

Abstract

Quantum-secured networking forms a layered architecture comprising quantum, key management, and service layers. Quantum layer distributes quantum keys by means of quantum key distribution (QKD) protocol. Key management layer relays quantum keys to establish an end-to-end key. Service layer utilizes the key to provide end-to-end quantum-secured service.

The nature of quantum mechanics provides us with new opportunities to improve networking system. As a research on the quantum layer in the quantum-secured networking, the first part of this talk will cover a research on eavesdropping detection in classical fiber networks, by means of BB84 QKD protocol. An eavesdropper in the BB84 QKD protocol cannot avoid affecting quantum bit error rate, which provides us an opportunity to detect the eavesdropper statistically with sufficiently high accuracy.

For practical quantum-secured service, efficient utilization of a quantum key resource is required, which is a limited and costly resource in the current quantum technology. In the second part of this talk, I will deliver a research on quantum key resource aware key relay algorithms for key management layer in the quantum-secured networking. The key relay algorithm can control the balance between max-min fairness and efficiency in the key relay.