Performance Enhancement and Security Analysis of Satellite FSO/QKD Systems using HAP-based Relaying and ARQ

Project Proposal of 563 Class

I Information

1) Name: Nam Nguyen (nguynam4@oregonstate.edu)
2) Research Interests:
   - Free-space optical communication systems: modulation techniques, channel models, and system performance analysis
   - Free-space quantum key distribution networks: design, analysis, and optimization of link-layer retransmissions and relaying techniques

   My current studies are on free-space quantum key distribution networks and appeared in some papers:
   - **Nam D. Nguyen**, Hang T. T. Phan, Hien T. T. Pham, Vuong V. Mai, and Ngoc T. Dang, "Reliability Improvement of Satellite-based Quantum Key Distribution Systems using Retransmission Scheme," *Photonic Network Communications*, Vol. 42, No.1, pp. 27-39, Aug. 2021.
   - **Nam D. Nguyen**, Hien T. T. Pham, Vuong V. Mai, and Ngoc T. Dang, "Comprehensive Performance Analysis of Satellite-to-Ground FSO/QKD Systems using Key Retransmission," *Optical Engineering*, Vol. 59, No. 12, pp. 126102-1-25, Dec. 2020.
3) Graduate Student at School of Electrical and Computer Engineering of Oregon State University

II Title of the project

"Performance Enhancement and Security Analysis of Satellite FSO/QKD Systems using HAP-based Relaying and ARQ"

III Project description

A. Problem Statement

The desire to connect everything over the Internet requires secure communication to prevent unauthorized access, stealing and changing information. Quantum key distribution (QKD), a well-known protocol based on the rule of quantum physics to share the secret key via two lawful parties (namely Alice and Bob) with an eavesdropper (namely Eve), is a promising method that meets the requirements [1]. A global-scale QKD network can be implemented utilizing satellite-to-ground free-space optical (FSO) links and several proof-of-principle experiments have been performed recently. However, the performance of satellite QKD systems is degraded by atmospheric channels including scattering, absorption, and atmospheric turbulence [2], [3]. Due to these factors, even if no eavesdropper existed, the quantum key error rate (QKER) may be very high under strong turbulence.

B. Motivation

To reduce QKER, the reconciliation process based on the forward error correction (FEC) has been proposed in [4] and further developed in [5]. Nevertheless, highly computational algorithms are needed for optimizing FEC redundancy and, more importantly, FEC-only techniques are not robust enough to guarantee reliability due to relatively long-distance transmissions from satellite to ground stations.

The purposes of this research are to design satellite FSO/QKD systems that can effectively distribute the secret keys between two parties living far away and investigate the feasibility and reliability of

the proposed system. If a designed satellite FSO/QKD system can offer considerable performance improvement over the conventional ones, it could largely contribute to the possibility of a global QKD network for secure communication.

C. Solution Approach

The main objective of this project is to explore additional techniques to improve the performances of satellite FSO/QKD systems. I am first going to strengthen the physical layer by considering a relaying technique based on a high-altitude platform (HAP). Here, a relaying node is located at a HAP that recovers the quantum keys transmitted from a satellite and forwards those keys to a ground station. Thanks to the HAP-based relaying technique, the signal is regenerated and thus the QKER will be reduced.

Also, I am going to propose to improve the link layer by considering a key-retransmission technique, namely automatic repeat request (ARQ). Unlike the FEC technique, in which key errors are corrected based on the redundancy added to quantum keys to reduce QKER in the reconciliation process, the link-layer ARQ technique retransmits unsuccessfully keys to assure QKD reliability. Therefore, the ARQ technique does not require high computational algorithms for error control.

For the security analysis, the ergodic secret-key rate and final key-creation rate will be obtained in closed-form expressions.

D. Evaluation Method

The methods of research in this research plan are using the mathematical model, theoretical analysis, and Monte-Carlo simulation (using Matlab) of the proposed free-space quantum key distribution system.

E. High-Level Execution Plan

- Phase 1:
  - Fundamental of QKD and relaying FSO communication systems
  - Studying the operation and architecture of high-altitude platform (HAP)-based relaying systems
  - Studying the performance of satellite FSO/QKD systems with the influences of the atmospheric channel
  - Studying the link-layer automatic repeat request (ARQ) techniques
- Phase 2:
  - Proposing the satellite FSO/QKD systems using HAP-based relaying and ARQ
  - Proposing the architecture of the proposed system including the transmitter, the HAP-based relay node, and the receiver
  - Proposing the channel model with atmospheric turbulence
- Phase 3:
  - Investigating the performance and security analysis of the proposed system in terms of key loss rate, delay outage rate, ergodic secret-key rate, and final key-creation rate
  - Comparing with conventional QKD systems
  - Completing project final report and presenting

References

[1] H. P. Yuen, "Security of quantum key distribution," *IEEE Access,* vol. 4, pp. 724–749, 2016.

[2] G. Vallone et. al., "Experimental satellite quantum communications," *Phys. Rev. Lett.* 115(4), 040502, 2015.

[3] S.-K. Liao et. al., "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.* 120(3), 030501, 2018.

[4] W.T. Buttler et. al., "Fast efficient error reconciliation for quantum cryptography," *Phys. Rev. A,* vol. 67, No. 5, p. 052303, 2003.

[5] X. Ai et. al., "A reconciliation strategy for real-time satellite-based QKD," *IEEE Wireless Commun. Lett.,* vol. 24, no. 5, pp. 1062–1066, May 2020.