Poster ID: 07

Vu Quang Minh, 2nd Year Master Student
Computer Communications Lab., The University of Aizu

Poster Session at Graduate School Information Fair

Relay-assisted Satellite Free-Space Optical Quantum Key Distribution Systems

General Background

Classical cryptography

Symmetrical cryptography

Asymmetrical cryptography

Based on mathematical complexities (computational security)

Future advances in computer hardware and algorithms

Especially in quantum computing

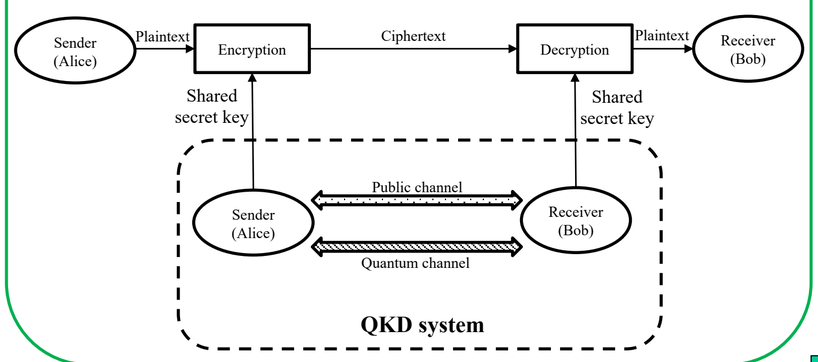
Existing information security can be compromised

Towards unconditional security

A solution against quantum attacks

Quantum key distribution (QKD)

QKD provides an unconditionally secure way to distribute secret keys based on the laws of physics.



Satellite Free-space Optical QKD (FSO/QKD)

The use of optical fibers in QKD system is popular. However, these systems just can be used for **fixed users**.

Thanks to high data-rate, cost effectiveness, liciense-free operation, and quick deployment/redeployment, FSO is a promising solution to deploy QKD systems for **mobie users or stations that are at remote areas.**

Credit: C. Bickel/Science

The world's first quantum satellite, Micius, using FSO was launched successfully in 2016

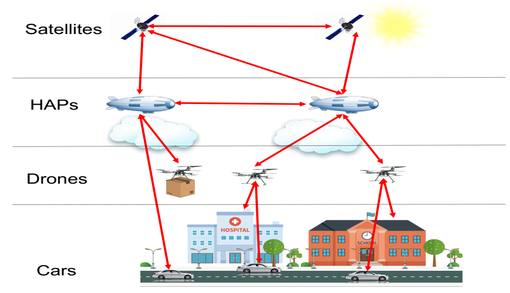
Towards global-scale QKD networks

Relay-assisted Satellite FSO/QKD

The effects of atmospheric condtions including absorbtion, scattering, atmospheric turbulence can degrade the performance of satellite-based QKD → The operation distances are limited.

→ Deploying relay nodes is a potential solution to extend the operation range.

High altitude platforms (HAPs) are the promising candidate to deploy as relay nodes between satellites and mobile users.

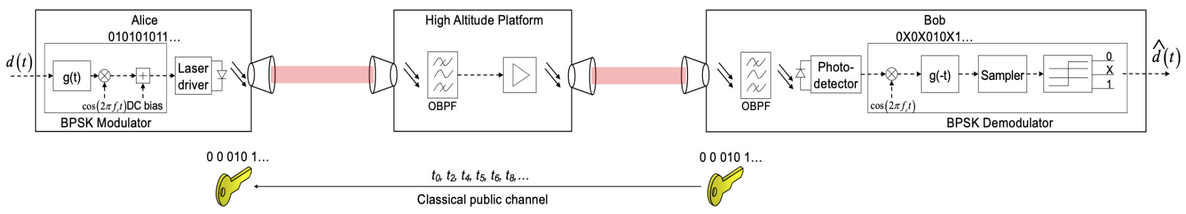


HAPs can be airships, balloons, unmanned or manned aircrafts located in the stratosphere at an altitude of 20 km.

HAPs have the both advantages of both satellite and terrestrial communications consisting of large coverage area, less interference caused by obstacles, resonable cost, fast deployment, and easy maintanence.

System Model

A HAP-based relay-assisted FSO/QKD system using sub-carrier intensity modulation/binary phase-shift keying (SIM/BPSK) with dual-threshold/direct detection (DT/DD) scheme is propose to achieve QKD function with simple setup and low cost.



The operation of the proposed system:

Step 1: The sender (Alice) generates SIM/BPSK modulated signals with a small modulation depth accordingly for bits "0" and "1".

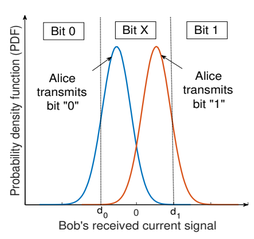
Step 2: The receiver (Bob) uses an DT/DD receiver to detect the transmitted bit "0" and "1" using two threshold d_0 and d_1. The detection rule is

$$\text{Decision} = \begin{cases} 0 & \text{if} \quad i \le d_0, \\ 1 & \text{if} \quad i \ge d_1, \\ X & \text{otherwise}, \end{cases}$$

"X" represents the case that Bob is unable to recover the transmitted bit.

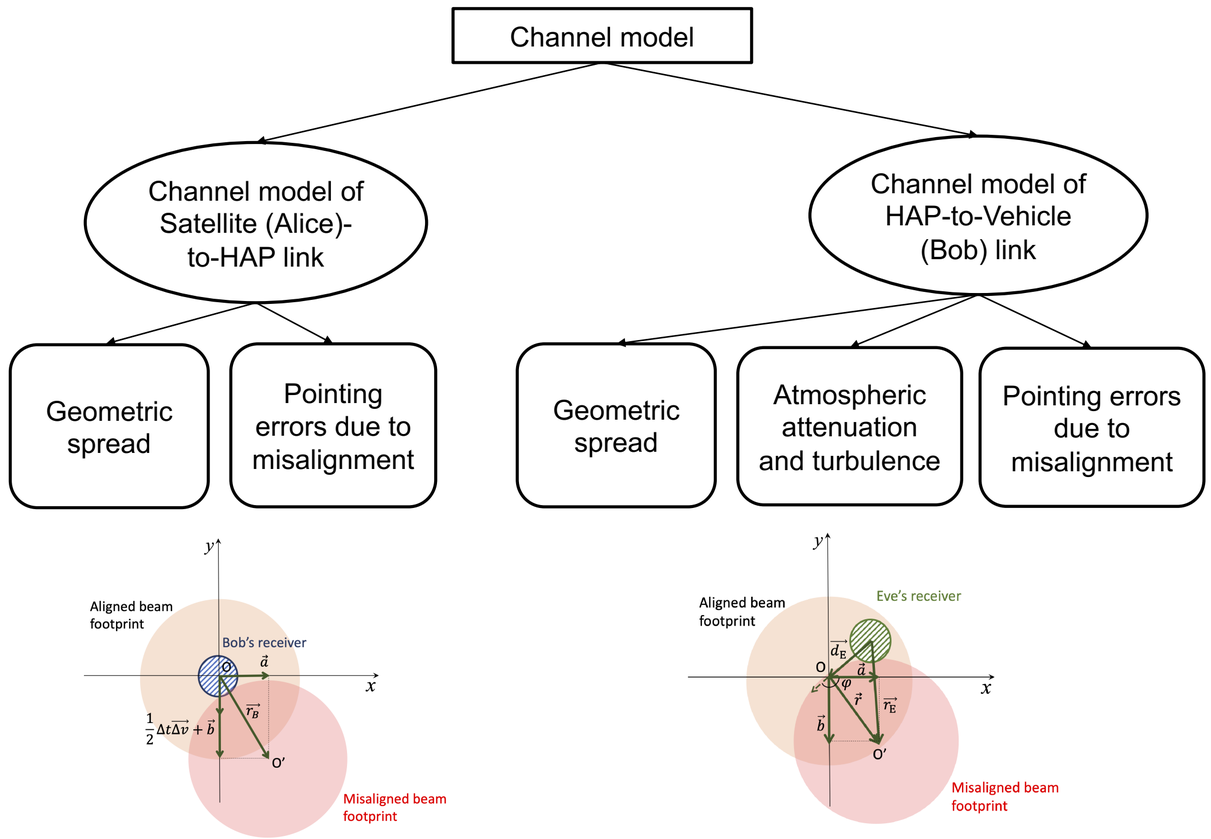
Step 3: Bob informs Alice of the time instants at which he can decode either bit "0" or bit "1" by using public channel. Then, Alice and Bob share an identical bit sequence *(sifted key.)*

Step 4: Alice and Bob perform *information reconciliation* and *privacy amplification* over public channel to correct errors and generate secret keys.



The PDF of Bob's received signal with the DT detection

Channel Model



Misalignment between HAP and Bob

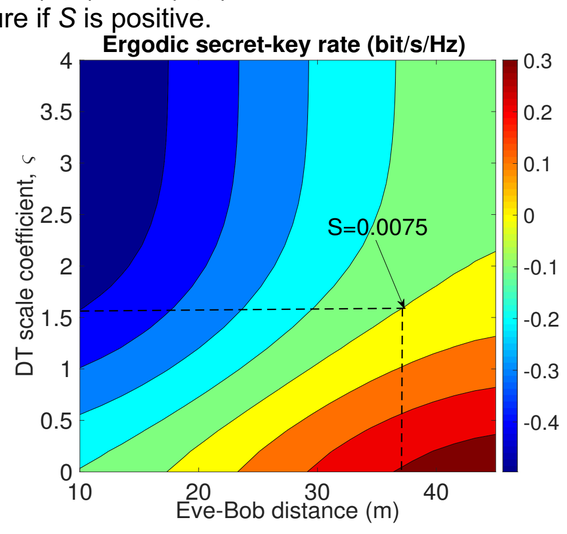
Misalignment between HAP and Eve (Eveasdropper)

Numerical Results

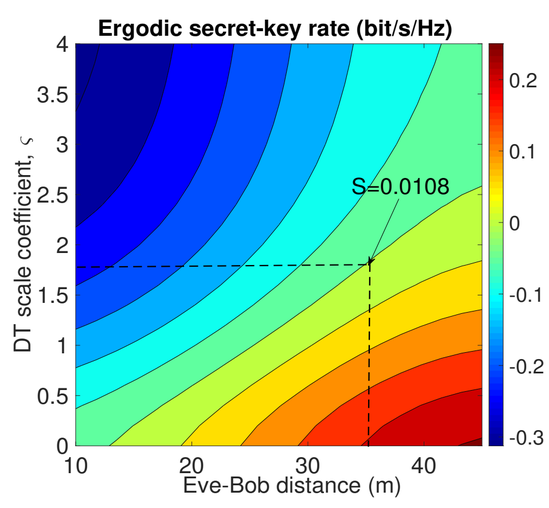
The ergodic secret-key rate, which is defined as the maximum transmission rate between Alice and Bob at which Eve (Eveasdropper) is not able to decode any information from her received signal, is investigated. It is calculated by

$$S = I(A;B) - I(A;E)$$

where $I(A;B)$ and $I(A;E)$ are the mutual information between Alice-Bob and Alice-Eve, respectively. The system is considered as secure if S is positive.



Ergodic secret-key rate versus DT scale coefficient (to adjust threshold d_0 and d_1) (Log-normal turbulence model)



Ergodic secret-key rate versus DT scale coefficient (to adjust threshold d_0 and d_1) (Gamma-Gamma turbulence model)

Two figures show the ergodic secret-key rate versus DT scale coefficient and Bob-Eve distance for weak and strong turbulence conditions. With the smallest possible values of DT scale coefficient to guarantee sufficient Bob's sifted-key rate, it is seen that the minimum Eve-Bob distances are 38 m and 36.25 m for weak and strong turbulence conditions, respectively. A minimum distance of 38 m should be maintained to ensure the system is secure over a wide range of turbulence regimes.

Conclusion

- The HAP-based relay-assisted FSO/QKD system using SIM/BPSK with DT/DD scheme was proposed.
- The effects of transceiver misalignment and atmospheric turbulence conditions were considered for thorough channel modeling.
- Numerical results were analyzed to determine the minimum Eve-Bob distances for secure communication between Alice and Bob.

Reference

P. V. Trinh *et al.*, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, Jan. 2018.