BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023
http://excel.fit.vutbr.cz

Quantum key distribution

Martin Litwora*

Abstract
The goal of this work is to explore the possibilities of secure key distribution over the quantum channel and its application in laser transfers. It is also necessary to find proper cryptographic methods that are efficient in terms of energy consumption and provide enough security. Quantum key distribution (QKD) is a distribution of random keys over a quantum channel. The channel's security is guaranteed by quantum mechanics rather than based on the complexity of mathematical problems as in the case of asymmetric cryptography. Measurement of a quantum state disturbs the system. If the attacker tries to listen and measure the values of qubits on the channel he introduces an anomaly that can be detected. This paper also describes one of the QKD protocols used in a real environment with the possibility of using satellites for laser communication over long distances. The attenuation effect of the atmosphere is described in the last section of this paper.

*xlitwo00@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Motivation

Once efficient quantum computers become a reality the security of asymmetric cryptography will drastically reduce as shown in the Figure 1 on the poster. There are in general 3 solutions to this problem:

1. Use of post-quantum algorithms. At this moment there is an ongoing programme and competition by NIST to select and standardize the best post-quantum algorithm. They are based on the shortest vector problem (lattice-based cryptography) [1].
2. The symmetric cryptography will not suffer as much. When the key size doubles the level of security remains the same as before the appearance of quantum computers.
3. One-time pad algorithm combined with the QKD system. The Vernam Cipher is proven to be unbreakable under the condition of having a truly random key, that is never used twice and that is the same length as the message.

The third option is the long-term solution to this problem. By using the quantum key distribution we can achieve a level of security that is defined by quantum physics. IoT devices have limited battery and computational power. It is necessary to find a proper cryptographic method that is secure and saves the valuable resources of a device.

2. Challenegs of QKD

The correct implementation of quantum channels is crucial. There are limitations that need to be solved in order to be used in a real environment. First is the low rate at which the keys are generated. Usually, the key rate is something around 3 kbit/s, see Figure 2. However, this depends on the power of the device. Companies developing QKD systems usually have multiple products that vary in price and efficiency.

The second issue is the complexity of the generator of single photons. The basic quantum distribution protocol uses the polarization of a single photon to represent a qubit value. Since the generators of single photons are difficult to construct, other protocols needed to be developed. This includes the COW protocol, described in section 3.

The third issue is the short distance on which we can create the quantum channel. The maximum distance is usually 100 km at most due to losses on optical fibres. This can be an issue for communication over long distances. Quantum repeaters are also in the distant future. The solution to this can be using satellites and laser transfer in free space. Laser data transfers are much faster and can carry more data. However, they are limited by weather conditions, more on that in section 4.

3. COW protcol

The Coherent One Way implements the key distribution over the quantum channel. The protocol uses weak coherent pulses. Each pulse contains a small number of photons. This is given by the mean photon number, usually $\mu = 0.5$. The protocol uses time-bin encoding. This means that the bits are represented by a pair of consecutive pulses where the pulse arrival time is important. If the first pulse is full (pulse contains photons) and the second one is empty (vacuum state) then this represents the binary 1. Empty and a full pulse represent binary 0. The protocol is shown in the Figure 5.

Protocol also implements decoy states that are used to detect the presence of an attacker listening on the channel. Part of the system is a Mach-Zehnder interferometer (Figure 4) that is used to check the coherence of the incoming pulses. The receiver usually checks about 10 % of all pulses. They are sent to the monitoring branch (D_M in Figure 5). The coherence can be checked between the two consecutive full pulses (grey colour in the figure). The first pulse is delayed by the φ. If the coherence is broken, it may indicate the presence of an attacker. However, we still need to calculate with imperfections of the channel and the detectors.

After the raw key has been transferred, comes a phase called key distillation. The sender Alice tells Bob which pulses were decoys and Bob calculates the QBER (Quantum bit error). If the value is too high (usually above 11 %) communicating parties abandon the key as it may be compromised. Otherwise, some bits are removed and distilled in order to amplify the security of the final key. The final key is then stored and can be used by an authorized application that asks for it [2].

4. Laser transfers using satellites

Satellites used for laser data transfers usually fly in Low Earth Orbit (200 – 2000 km above the ground). A satellite can serve either as a transmitter of the signal – downlink, described in Figure 3) or a receiver – uplink. It is also possible to combine multiple satellites together. In order for this to work the ground station needs to be in the line of sight with a satellite. The laser beam has to accurately target the satellite. Coordination is crucial here. The data transfer over the air is limited by the current conditions in the atmosphere. Clouds, fog, rain, turbulences in the atmosphere and high background solar noise can scatter or absorb the laser beam.

Clouds are the biggest problem for laser transfers [3]. There exists a project and research to develop lasers that are capable of creating a hole in the cloud through which the data could be sent [4].

5. Laser transfers simmulation

The goal is to measure the attenuation of a quantum channel that is created over the optical fibre. Then simulate the attenuation of the laser quantum channel that passes through clouds.

I connected to the fibre quantum channel a small box that simulates the presence of an attacker. It deflects a portion of pulses and creates artificial delay. The reaction to this is a slower key rate depending on the portion of the deflected signal. The key rate can drastically slow down similar to how the key rate would drop if the channel had to pass the different types of clouds. The measured data can then be used to simulate the attenuation of a laser beam travelling through the clouds.

Clouds can be classified into three types depending on their height. The higher clouds are usually thinner and have a lower density than the ones at a lower height. Which means they do not scatter the beam as much. In the Figure 6 we can see the cloud coverage for 1st June 2022 in Brno. Three types of clouds are shown there, data were collected from the weather forecast. The next graph (Figure 7) shows the throughput during three days in summer in Brno. The speed is higher when clouds are not present during the day. In the evening and when the cloud coverage increases the speed goes down. The weather and clouds, in particular, depend also on the part of the year. Winter is more cloudy than summer.

6. Conclusions

Quantum key distribution is a complex process that lacks any standardization at this moment. The promising field of development and research is using lasers and satellites for quantum channels over free space. However, these transfers can be negatively affected by weather conditions, especially clouds. The simulation shows that the key rate (throughput in general) can differ during the day. It highly depends on current cloud conditions, where clouds in low and middle height can scatter the beam the most.

References

[1] Gorjan Alagic, David Cooper, Quynh Dang, Thinh Dang, John M. Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl A. Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Daniel Apon. Status report on the third round of the nist post-quantum cryptography standardization process, 07 2022. DOI: https://doi.org/10.6028/NIST.IR.8413.

[2] Nicolas Gisin, Gregoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, and Valerio Scarani. Towards practical and fast quantum cryptography, 2004. DOI: 10.48550/ARXIV.QUANT-PH/0411022.

[3] Nikolaos K. Lyras, Charilaos I. Kourogiorgas, and Athanasios D. Panagopoulos. Cloud attenuation statistics prediction from ka-band to optical frequencies: Integrated liquid water content field synthesizer. *IEEE Transactions on Antennas and Propagation*, 65(1):319–328, 2017. DOI:10.1109/TAP.2016.2630602.

[4] Bursting the clouds for better communication. online, 10 2018. Université de Genève. Published by ScienceDaily.