Research report

Analyzing the quantum based satellite communications

OTKA PD 112529

2015-2017

László Bacsárdi, Ph.D.

General overview

In the research named Analyzing the quantum based satellite communications, we focused on the open questions of the quantum based satellite communication. Our main points were the following: Modeling the optical channels which could be used in the quantum based satellite communications and creating a complex network which enables the global key distribution via satellites,

Introducing the research

The quantum communication is based on the laws of quantum mechanics, and utilizes different quantum-based algorithms and protocols. Comparing with classical algorithms, which are used in classical computation, the advantages of quantum algorithms are the quickness, the factorization and encryption. The base unit of the quantum computing is the quantum bit (qubit), which can be represented by different polarization states of a photon. The state of a classical bit can be represented by only one of the 0 and 1 values, but the qubit can be an in arbitrary superposition of 0 and 1.

The first quantum cryptographic protocol was published by Bennet and Brassard in 1984 followed by several others like B94 or S09. The BB84 key distribution protocol was the first which worked on quantum physic principle. It creates random bit sequences which is known only by the two communications parties and it also cover the security of the communication. This property of the BB84 protocol is based on the so-called No Cloning Theorem (NCT). The result of the exchange process is a classical string of bits, which can be further applied in nowadays used symmetrical coding protocols.

There are two groups of the currently used QKD solutions. The first generation protocols use singe-photon sources, while coherent laser is used and the wave properties of light is exploited in the second generation protocols. This first approach is named as Discrete Variable QKD (DV-QKD), the second one is named as Continuous Variable QKD (CV-QKD). Although commercial applications of QKD technology are already available, currently direct fiber based QKD links cannot reach distances beyond a few hundred kilometers due to the optical losses on the fiber. With the help of quantum repeaters, long-distance QKD networks may be feasible, but such devices are not ready for operational integration. Instead of wired-links, satellite links can be used as free-space quantum channels to provide a global free-space QKD network. This is why Chine has launched the world's first quantum communication satellite in 2016.

The design process of quantum communication system has recognizable steps: coding classical information into quantum bits or start right with a quantum bit, applying different transformation, sending the information (classical or quantum) through a channel (classical or quantum), applying different transformation, performing a measurement if classical information is needed. From mathematical point of view, the channel itself is an abstract transformation, which performs an identity transformation in an ideal case, or causes errors and decoherence in real world. But for engineers, the properties of the quantum channels are very important.

The research was supported by the Hungarian Scientific Research Fund – OTKA PD-112529.

In a satellite-based quantum key distribution network, we use quantum bit to transfer data from the sender to the receiver. In the communication channel, there is a point where we have to do a measurement to determine the classical value of a qubit. Compared the quantum communication channel to the classic communication channel, in case of an eavesdropping attack, the measurement performed by an attacker changes the quantum state and by this, the opportunity is given to detect the attacker. This is one of the biggest advantage of the quantum communication channel.

For satellite-based quantum communication, we distinguished three types of communication links: satellite–satellite, satellite–ground, ground–satellite. A complex, satellite-based network could enable a global quantum key exchange service. Due to the nature of quantum-based protocols, the noise of the channels need to be estimated since the errors introduced by an eavesdropper could be masked by the natural noise of the channel. This research has been started in January of 2015. In August of 2016, the world's first quantum communications satellite has been launched by China. The Chinese Micius is using entanglement, so secret keys will be shared between the ground stations using entangled-pairs. Using the measured data of the Chinese experiment, we were able to validate our channel model.

Key results of the research

Loss model of quantum-based satellite communication

We need to model a satellite-based quantum key distribution network. Due to the nature of quantum-based protocols, the noise of the channels need to be estimated since the errors introduced by an eavesdropper could be masked by the natural noise of the channel. With our model based on the behavior of single-photon sources, we are able to analyze the effects of losses originated from beam spreading and pointing error on the first generation QKD protocols. Several parameters need to be taken into account while calculating the Quantum Bit Error rate (QBER) of a complex communication network. In our model, we took into consideration the following atmospheric influences: wind speed, season, climate, weather as well as the following factors: wavelength, mean photon number by laser impulses, probability of polarization measuring error, quantum efficiency of detector, zenith angle, aperture diameter, targeting angular error, number of detectors, mirror diameter, height above sea level of the satellite.

Quantum Satellite Communication Simulator

Based on our channel model, we have developed a Java Swing simulation platform named Quantum Satellite Communication Simulator to analyze different scenarios and different types of QKD networks. In the latest version of our simulation software, we extended the structure of the atmospheric properties by the subarctic climate in both summer and winter seasons. We refined also the formulas what we used to determine the beam widening. We split the calculation into geometric and diffraction models. The *Calculating by constant parameters* scenario is a simple channel simulation. Here is possible to execute calculation for all of the three channel types, i.e., ground–satellite, satellite–satellite and satellite–ground channel. In the *Calculating by varying parameters* scenario, it is possible to analyze the four QKD protocols by numerical analysis way. In the *Sensitivity analysis* scenario, it is possible to analyze physical variables and the protocols by simulation way. The application can execute calculations for the following physical formulas and protocols: beam widening in vacuum, dynamic loss, total scattering and strength of turbulence. In the *Time driven communication* scenario, it is possible to simulate the working of the protocols from the network aspect. This scenario is probably the most comprehensive in the application. It handles locations of ground stations and satellites, which are previously loaded into the program. Every necessary component is rendered by OpenGL. The application creates a graph by vertices and edges and uses the Dijkstra algorithm to find the shortest paths and as result it issues some statistical values of the network. Calculations for determining the

channel lengths and number of satellites by the possible lowest QBER value can be executed in the *Optimization* scenario.

Model and measured data

The Chinese QuESS (Quantum Experiment at Space Scale) experiment realized the first satellite-Earth quantum channel. The satellite produced entangled photon pars and transmitted them to two ground stations at Lijiang and Delingha (both in China) via two downlinks (and later to Graz, Austria and Xinglong, China). We compared theoretical predictions for channel loss with measured values. This is necessary because theoretical predictions of quantum communication are based on mathematical models describing classical light beams. This approach requires the assumption that properties of the atmosphere are either completely or at the very least largely independent of light intensity and that individual photons behave in a way that is consistent with an infinitesimal part of a classical light beam.

Using the value of beam spreading measured in the QuESS experiment, we could validate our method of calculating the channel loss. We found that the geometrical optic approximation yields results in the same order of magnitude as the reported value of beam divergence. The exact result depends on the model of optical turbulence strength being used. In our calculations, we examined the HV 5/7, HV Night and Greenwood models of optical turbulence and found that the reported value of beam divergence falls within the range of the values calculated using these approximations.

Entanglement-based QKD network

We proposed to use three satellites for sharing secret keys in the following way. Satellite *G* generates the entangled pairs and sends one photon of each pair to the two ground stations (*Alice* and *Bob*). The range is extended with mirror satellites M_a and M_b which only mirrors the photons from the space to the ground. If we place the links between the generator and the mirrors above the atmosphere, a significant amount of distortion can be avoided.
What happens if an entangled photon is generated onboard satellite G? Let us consider that we generate an entangled pair $|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. The two half of the entangled pair is transmitted to the ground stations using the mirror satellites. Alice performs a projective measurement in the $|0\rangle$ and $|1\rangle$ basis, which will collapse Bob's half into the same state as Alice's results. Bob only has to perform the same projective measurement, i.e., with the $|0\rangle$ and $|1\rangle$ basis. But Alice and Bob can consider any orthogonal basis states as $|0\rangle$ and $|1\rangle$. How will they know what basis states has the other one chosen? How can they be sure that they use the same basis states which were used to generate the entangled photons onboard the satellite? While the moving satellite G generates and reflects the entangled pairs of photons, the basis states of the received quantum bits has to be rotated in reference to what the basis states were on the satellite G. We showed how the measurement basis can be corrected in such network and analyzed its efficiency as well.

Quantum error correction on satellite links

We created a communication network which consists of a satellite, a ground station and other communication points connected to the ground station via fiber. We tested different quantum error correcting codes in such a network including bit-flip code, Shor code, Steane code, 5 qubit code) and a special 4 qubit code for amplitude damping channels, using common channel models like depolarizing or amplitude damping channel.

Simulation of complex satellite-based QKD network

We tested the feasibility of different quantum satellite constellation by simulating secure information transfer via satellites. To ensure security, we applied symmetric cryptography protocols (AES/Rijndael block cipher) for which the symmetric keys were provided by quantum-based key distribution protocols (namely BB84, B92). We used one-hop and multi-hop secure communication links.

Publications

The results of the research have been published in 2 journal articles, 7 full conference papers (in English), 1 Hungarian conference paper (in Hungarian), 5 abstracts (in English) and 1 abstract (in Hungarian). Two Hungarian journal articles have been published in "Természet Világa" (August 2015 and January 2016). Detailed list is available in Section "List of publications".

As part of the work of a researcher, we have focused on outreach activities as well. Different lectures were held about quantum based computing and a Hungarian Facebook page was started (named "Adventures in the world of quantum bit").

Recognitions

I was proud to receive five recognitions based on my OTKA-sponsored research during the 3 years of the research.

- I was interviewed for the OTKA Magazine "Researcher of the Month" for the November 2015 issue.
- In December 2015, I received the "Exceptional Young Researcher Award" from the Regional Centre of the Hungarian Academy of Sciences, Veszprém, as a recognition of my research on satellite-based quantum communications.
- In Jun 2016, I became member of the executive office of the UN established Space Generation Advisory Council.
- In 2016, I became substitute management committee member of the COST Action CA15220 Quantum Technologies in Space. In 2017, I became the communication manager of the Action.
- In 2017, I received one of the highest international award available for young researcher in the space sector (and I became the first Hungarian who received it): the IAF Young Space Leadership Award from the International Astronautical Federation (IAF).

List of publications

Journal articles

- T. Bisztray, L. Bacsárdi, „The Evolution of Free-Space Quantum Key Distribution", INFOCOMMUNICATIONS JOURNAL, 2018:(1) [accepted for publications]
- L. Bacsardi, R. Birkeland, A. Hornig, M. Shar, B. Morrison, Y Tsodikovich, „Present and the Future of Space Internet: The Space Generation Perspective", NEW SPACE 5:(4) pp. 257-267. (2017)

International conference papers

- A. Kiss, L. Bacsárdi, „Analyzing the Effects of Atmospheric Factors in Earth-space and Space-Earth Quantum Communication Channels", Proc. of H-SPACE 2018, pp.1-5.
- M. Galambos, L. Bacsárdi, „Comparing Calculated and Measured Losses in QuESS's Quantum Channel", Proc. of H-SPACE 2018, pp.1-4.

- A. Kiss, L. Bacsárdi, „Entangled-based quantum information transfer on Earth-satellite channel”, Proc of 68th International Astronautical Congress, Adelaide, Australia, pp. 1-5.
- A. Korsós, L. Bacsárdi, Zs. Kis, „An analysis of entanglened-based solutions on Earth-satellite channel”, Selected papers of the 3rd International Conference on Research, Technology and Education of Space (H-SPACE2017), pp.1-5.
- A. Kiss, L. Bacsárdi, „Analyzing the Quantum Efficiency in Satellite-based Quantum Key Distribution Network”, Selected papers of the 3rd International Conference on Research, Technology and Education of Space (H-SPACE2017), pp.1-5.
- I. Vercseg, L. Bacsardi, „Simulation of information transfer on quantum-based satellite network”, Proc. of 67th International Astronautical Congress, Guadalajara, Mexico, pp. 1-5. (2016)
- A. Kiss, L. Bacsardi, „Quantum-based solutions in Low Earth Orbit Satellite Networks”, Proc of. H-SPACE 2016, pp 37-38.

Hungarian conference papers

- Kiss A., Bacsárdi L., „Műholdas kvantum kulcsszétosztó hálózat hatékonyságának vizsgálata”, Magyar Űrkutatási Fórum 2017 válogatott közleménye, pp. 1-4.

International conference abstracts

- A. Iván, L. Bacsardi, „Simulation of different quantum error correction codes in free-space channels”, Proc of. H-SPACE 2018, abstract only
- L. Bacsárdi, A. Korsós, Zs. Kis, „Analyzing entanglement-based quantum key distribution on satellite-ground channel”, Quantum Technology in Space, First Conference and Working Group Meeting, 2017, Malta, abstract only
- A. Kiss, L. Bacsardi, „Simulating Secure Key Distribution over Quantum Satellite Channel”, Nanoposter 2016, abstract only
- L. Bacsárdi, „Quantum-based Satellite Communication: an Overview”, SpaceUp2016, Geneva, Switzerland, abstract only
- A. Kiss, L. Bacsardi, „Analyzing First Generation Quantum Key Distribution Protocols in Low Earth Orbit Satellite Networks”, Nanoposter 2015, abstract only

Hungarian conference abtracts

- Kiss A., Bacsárdi L., Első generációs kvantum kulcsszétosztás vizsgálata lézer alapú műholdas kommunikációban, Proc. of Magyar Űrkutatási Fórum 2015: Az előadások összefoglalói, abstract only

Journal articles (in Hungarian)

- Bacsárdi L., „Az igazi kvantum csendje. Kvantumeszközök a hatékony kommunikáció szolgálatában”, TERMÉSZET VILÁGA 147:(1) pp. 11-14. (2016)
- Bacsárdi L., „Biztonságos kommunikáció kvantumalapú hálózatokban”, TERMÉSZET VILÁGA 146:(1. különszám) pp. 44-48. (2015)

I’m thankful for the OTKA/NKFIH for their support

László Bacsárdi