UDC 621.391

O.S. Albul, PhD
(National Aerospace University, Ukraine)

Ways to ensure secure communications using satellite systems

The purpose of this research is to analyze the application of quantum cryptography for high-speed data transmission in telecommunication satellite systems.

At present, the rapid development of telecommunications requires the development of new methods that ensure the protection of data during transmission in satellite systems.

The relevance and importance of data protection in satellite communication channels is due to global requirements to improve the security and reliability of such systems.

General security principles are devided to the following categories:

– physical security;

– information security;

– transmission security.

Physical security is concerned with protecting the actual equipment that makes up a system.

Specific user requirements will have to be considered and will have to follow the security requirements of the system to be protected [1]:

- high key rate (both: bits/s and average bits/year);
- geographic coverage (Europe, overseas regions, worldwide);
- security requirements (eg. trusted nodes; certification complexity for space/ground segment);
- ground terminal number, size and complexity (must be installed close to user locations);
- suitability for services;
- overall system cost (space segment, ground segment, operations).

Quantum cryptography provides new ways to securely transfer information. In modern communication networks, the widespread use of optical fiber and passive optical elements allows the use of quantum cryptography in today's standard optical network infrastructure.

Quantum Key Distribution (QKD) is a secure communication technique that uses quantum properties of photons, the elementary particles of light, to encrypt secret keys that can be shared by two parties to protect their communications. The technique, deemed unhackable since any attempt to eavesdrop on the communication changes the state of the photons and destroys the keys [2].

In Space Optical Communication compared to Radio Communication has the following advantages:

- bandwidth - the radio frequency spectrum is becoming scarce, while the optical spectrum is not regulated and bandwidth (= data that can be transmitted) is available in abundance;

- security - Optical Communication is safer against jamming, interference and eavesdropping.

But there are disadvantages:

- availability - cloud coverage;
- new technology with little heritage.

Different atmospheric conditions like snow, fog and rain scatter and absorb the transmitted signal in Optical Communication, which leads to attenuation of information signal before receiving at receiver end. As a result of attenuation caused by atmospheric conditions the range and the capacity of wireless channel are degraded. Thereby restricting the potential of the Optical communication link by limiting the regions and times [3].

Comparison of attenuation of light in fibres and in free space has been considered in [4]:

a) optical fibers:

- Exponential loss, 0.3 dB/km;
- no amplification for quantum;
- example: 80 dB for 270 km.

b) free space:

- Quadratic loss, depends on telescope size
- example: 80 dB for 400000 km for moon-earth distance, 10 cm transmitter, 1 m receiver, 1550 nm.

The QKDSat satellites will enable the exchange and distribution of secure encryption keys across a vast number of locations and billions of devices anywhere in the world through their space-to-ground optical quantum communication. This improves resilience against future hacking threats, as quantum keys are generated from high-quality random sources and distributed across the cloud network.

A study is being made of a method for protecting satellite telecommunication networks using quantum cryptography technology. An international research project in the field of quantum physics QUESS (Quantum Experiments at Space Scale) is considered as an example. The mission of the project is an experimental study of the concepts of data transmission over long distances using quantum technologies. For this purpose, the Mozi experimental satellite for quantum communications was launched into orbit [5]. This successfully demonstrated integration with existing ground-based networks, generating unconditionally secure quantum cryptographic keys over intercontinental distances between Asia and Europe, and the demonstration of quantum entanglement distribution and quantum teleportation at space scales.

It is assumed that QUESS will allow ground stations that are thousands of kilometers away to establish secure quantum communication channels. At the moment, the Mozi satellite has limited communication capabilities: it needs a line of sight and, due to the physical features of quantum mechanics, can only work if it is outside the zone of sunlight [6].

LEO satellite systems, which use intersatellite laser lines, differ from existing solutions by combining the speed of optical fiber with the "ubiquity" of satellites. LEO satellites are capable of providing truly global coverage, ubiquitous availability and rapid deployment.

A conclusion is made about the prospects for the use of quantum cryptographic systems in satellite communication systems and, in particular, as applied to high-speed data transmission satellite systems. The high speed and large bandwidth offered by Optic communication technology makes QKD perspective as a means to meet future demand for broadband internet access services. It has come up as a better alternative to Radio communication technology for reliable and feasible deployment of communication networks.

References

1. R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” npj Quantum Inf. 3, 30 (2017).
2. "Secure communication via quantum cryptography," ESA Applications, 2021,URL: https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Secure_communication_via_quantum_cryptography
3. M. Ijaz, Z. Ghassemlooy, J. Perez, V. Brazda and O. Fiser, Enhancing the Atmospheric Visibility and Fog Attenuation using a Controlled FSO Channel, IEEE Photonics Technology Letters, vol. 25(13), pp. 1262–1265, (2013).
4. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” Adv. Opt. Photon. 12, 1012 (2020).
5. Sheng-Kai, L. et al. Satellite-to-ground quantum key distribution. - Nature (2017).
6. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. - Nat. Commun. 8, 15043 (2017)