American Journal of Applied Sciences 8 (1): 71-76, 2011
ISSN 1546-9239


# Integration of Quantum Cryptography through Satellite Networks Transmission

[1]Skander Aris, [1]Abderraouf Messai, [1]Malek Benslama,
[2]Merabtine Nadjim and [2]Mosleh M-Elharti
[1]Electromagnetism and Telecommunication Laboratory, Department of Electronics,
Faculty of Engineering, Constantine University, 25000 Algeria
[2]Electrical Engineering Departments, Faculty of Engineering,
Taif University, Saudi Arabia

**Abstract: Problem statement**: The security of the telecommunications satellite has become a crucial issue. The telecommunications can be set using the classical cryptography. But this so-called classical cryptography provides cryptographic security. This means that security is based on the difficulty of some mathematics problems. On the other hand, quantum cryptography provides security without conditions based on the law of quantum physics. This method, called the theoretic information security is evidenced using the theory of information. **Approach:** In this study, we study whether quantum cryptography can be applied in the frame of the satellite telecommunications network. To do this in our project, we present theories regarding the following issues: Telecommunications Station and Satellite Communication Networks, Quantum Key Distribution, Open Space and Satellites, Analyses in different Scenarios between the Satellite and Earth station. **Results:** Quantum communications offers many advantages for secure data transmission, in our implementation study, we presented different scenarios of quantum key exchange between satellites and ground stations for possible approach to subsystem with quantum communication in space, capable of generating and detecting entangled photons as well as faint laser pulses. **Conclusion:** The use of satellites to distribute quantum photon provides a unique solution for long-distance. Moreover, quantum cryptography is a satisfactory solution to improve the safety problem. So, the quantum transmissions are the future of telecommunications.

**Key words:** Quantum cryptography, satellite transmission, quantum key distribution, laser transmission, satellite networks, telecommunications network, telecommunications station, classical cryptography, quantum physics

## INTRODUCTION

The satellite offers a guarantee of high quality transmission, regardless of the distance between the points of your network. Satellite communications are extremely safe. The satellite carries a near-perfect digital transmission across your network and satellite technology is so reliable it provides, to an unusual degree, the availability of services to all unsaved areas. They allow a very wide geographical serves especially for mobile users. They offer an advantage for multicast applications (Bacsardi, 2005). Progress in physics technology plays a very important role in the development of Quantum Cryptography. Normally, a quantum system contains at least one transmitter (photon source) and receiver (detector) and a quantum channel. The optic link is one of two solutions for the quantum channel, the other is free space. Up to now, most researchers use optical links to guide the photons from Alice to Bob. Although optic systems are very advanced, such a system cannot operate above the range of 150 km due to the combination of the loss induced by the fibre optics and detector noise. Moreover, the optic connection may not be available due to other reasons such as geographical difficulties. That is why we will see a proposal on the integration of quantum cryptography in satellite networks in the following study.

**Principles of quantum cryptography:** The idea of applying Quantum physics facts in cryptography was first proposed by Wiesner in 1970s but his study appeared a decade later. Quantum cryptography really started in 1984 by Bennett and Brassard when they

**Corresponding Author:** Skander Aris, Department of Electronics Electromagnetism and Telecommunication Laboratory, Faculty of Engineering, Constantine University, 25000 Algeria

introduced their famous Quantum Key Distribution protocols (Krishnan and Thangavel, 2010). One of the main principles used in Quantum Cryptography is the uncertainty principle denoted by HUP (Heisenberg Uncertainty Principle (HUP) (Bolonkin, 2009). HUP is explained in terms of momentum and position. For a moving article such as an electron we can characterize its motion by telling where it is (position) and what its velocity is (momentum).

In macroscopic levels we can measure these two quantities to infinite precision, but in Quantum Mechanics world we will not be able to measure them precisely. There is an uncertainty associated with measuring each of them. The reason is that in order to measure the system we inevitably disturb the system. Uncertainties are related to each other, for example if we try to measure the exact momentum, the uncertainty with position must be infinite.

Based on the above principles quantum physics establishes the following rules that are applicable in Quantum Communications:

- Measurement perturbs the system
- The position and momentum of a photon cannot be simultaneously measured with high accuracy
- The polarization of the photon cannot simultaneously be measured in both rectilinear and diagonal direction
- One cannot copy an unknown quantum state. Note that all the above rules used to sound negative in the past, but recently changed to be looked at positively when their applications for Quantum Cryptography were suggest

**Analysis and scenarios:** In June 2004, two groups have managed to exchange keys with a distance of one km in free space and ongoing experiments show that distances of 10 and 23 km can easily be reached (Lijun et *al*., 2004). All experiments were designed to reduce the size, mass and energy of the main equipment to enable portability in the short term and the fully automated remote operation in the long term. In the future, we may consider the modern equipment that will enable the exchange of photons over 1000 km (Fernandez *et al*., 2007). That is why one can imagine scenarios of quantum key distribution, how can we do? This is the question that we will try to recapture.

**Scenario of quantum key exchange:** In this step, we analyze scenarios of key exchange between a station on earth and a low earth orbit satellite (~ 800 km). There are three options to analyse:

- Station sends the key to the satellite
- Satellite transmits the key to the station
- Station sends the key to another station

For all three models, we need a classical channel that is capable of exchanging digital data at high speed to allow interactive alignment, the synchronous time, the shared key and error correction to be made in time real (Markus et *al*., 2003). The Ethernet bandwidth (10 MHz) is necessary for real-time operations. For the optical channel, we suggest telescopes as following:

- A large telescope at the station on the ground with a diameter of 30-100 cm which is able to track the satellite
- A small telescope on the satellite with a diameter of 10 or 30 centimetres. With the optical system 10 cm, we can construct 3 kg optical system but the 30 cm optics it will be difficult to construct for less than five kilograms. Thus, it is necessary to consider the size of the telescope to improve the cost and the maximum distance (Carter and Beach, 2007)

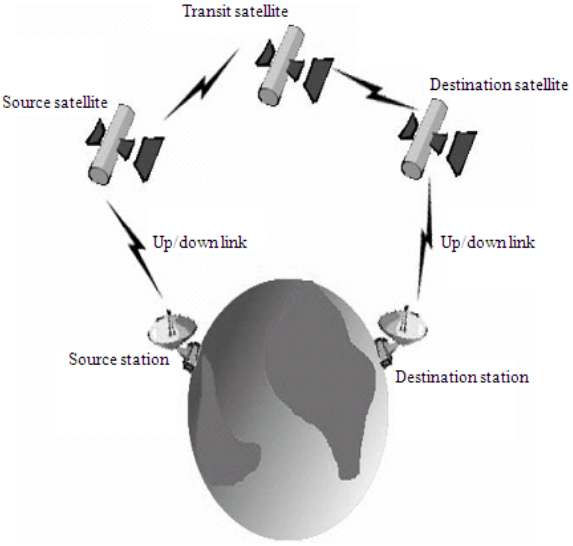


Fig. 1: Satellite Networks constellation

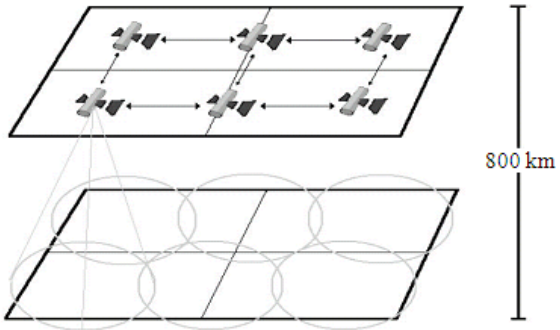


Fig. 2: The coverage of satellite networks

**Network satellite:** Using three scenarios of secure key exchange in the free space, it is not difficult to exchange the key between two points. The problem suggested here is the cover of a huge space. So we need a network of satellite coverage, shown in Fig. 1 and 2. To install this network, there are several questions to be answered:

- How many satellites does this networks need?
- How satellites and stations on earth do they communicate?

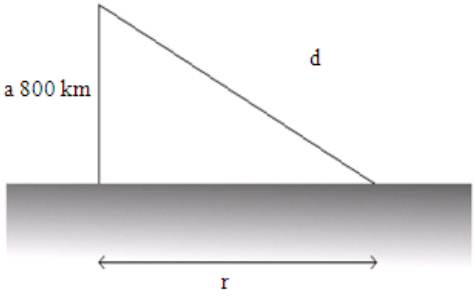


Fig. 3: Satellite altitude from the satellite station on earth

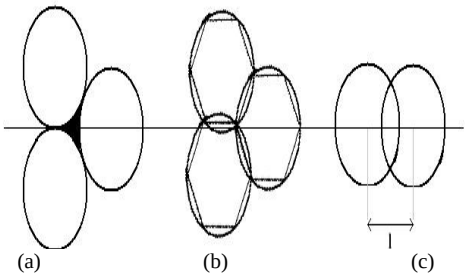


Fig. 4: Distance between two satellite networks

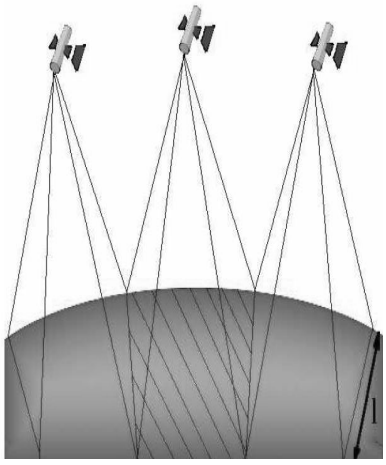


Fig. 5: Three satellite constellation networks

In this study we propose some models to create a satellite network. There are two possibilities:

- Transmitter ground: the key is transmitted from the station on the earth to the satellite,
- Relay satellite (Handover) : the key is transmitted from the satellite system to the satellite
- Receiver ground: the key is transmitted from the satellite station on earth. Normally, a satellite with the altitude (a = 800 km) and its maximum distance (d) we can calculate the covered area on the land of diameter 2r, shown in Fig. 3:

$$r = \sqrt{d^2 - a^2} \quad (1)$$

In reality, when we form a network of satellites to cover a huge area, you cannot install a satellite distance 2r because there is a small unknown region (black space), shown in Fig. 3. Each satellite covers only a surface hexagon inscribed in a circle, Fig. 4.

Therefore, the distance between two satellites, shown in Fig. 5:

$$l = r\sqrt{3} \quad (2)$$

Theoretically, the radius of the earth is about 6378 km and the satellite altitude is 800 km. Therefore, the radius of the satellite orbit is about 7178 km and it needs (n) satellites to cover a surface with (l) km:

$$\eta = \frac{2\pi 7178}{l} \approx \frac{45100}{l} \quad (3)$$

## MATERIALS AND METHODS

Photons are clearly the best way to transmit information, since they move at the speed of light and do not strongly interact with their environment. This near-perfect characteristic for quantum communication makes photons problematic for quantum computation. In fact, early approaches to using photons for quantum computation suffered from a requirement of exponential number of optical elements and resources as one scaled the system. A second problem was that creating conditional logic for two-qubit gates appeared very difficult since two photons do not interact strongly even in highly nonlinear materials. In fact, most nonlinear phenomena involving light fields result only at high intensity. Recently, new approaches for doing quantum computation with photons have appeared that depend on using measurement in a “dual-rail” approach to create entanglement. This approach removes many of the constraints of early approaches, but provides an alternative approach to creating quantum logic. Experimental efforts using this approach are just beginning. The approach will still have to solve the

technically challenging problems caused by high-speed motion of their qubits, a benefit in communication and a possible benefit in computational speed and by the lack of high efficient, single photon detectors that are essential to the success of this approach.

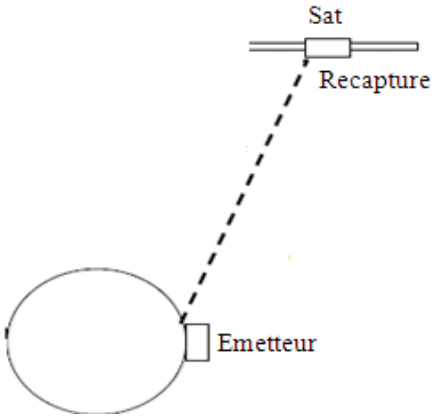


Fig. 6: Simple scenario satellite-earth station

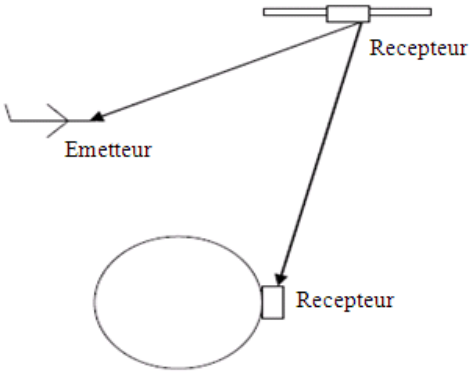


Fig. 7: Scenario aircraft satellite substation

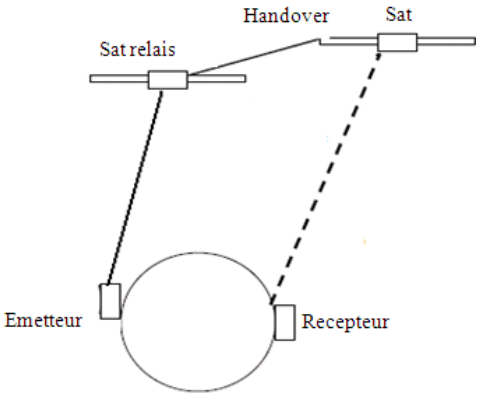


Fig. 8: Scenario proposed for the integration of quantum transmission

The single photon emitter is placed at the station. The laser link to the top receiver on the satellite using the BB84 protocol can be used to run the shared secret key negotiation (Sellami *et al*., 2009) Fig. 6.

To get things really going in this proposal we can integrate in the system-Plane Satellite Station, the transmitter pairs of entangled photons is placed on the satellite. It is the most interesting use of technology pairs of entangled photons (Markus et *al*., 2003). In the simplest scenario, the shared key secret of a plane can be determined by directing each of entangled photons to the satellite Fig. 7.

**Integration for a satellite network using quantum encryption:** Our first contribution is to provide a significant improvement on the satellite transmission, to ensure their compatibility with quantum telecommunication. Secondly, make a proposal that quantum cryptography could become an efficient technique with broad application. These specific points are thus the main purpose of our study. We try to highlight the quantum cryptography with satellite networks (handover). The BB84 protocol allows both partners to communicate a secret cryptographic key. For this we proposed the use of the BB 84 protocol subject to a quantum key distribution with single photon transmitter placed on the broadcast station (transmitter). This case seems more complex because it is impossible to directly negotiate a shared key between the transmitter and receiver using quantum technology. It must be like the following, Fig. 8.

## RESULTS

Quantum Network is a large scale resource of modern telecommunications and requires a utility program that coordinates the operations of all Quantum Key Distribution nodes, such as switching, polarization recovery, timing alignment and protocol initialization, as well as provides services to upper layer security applications such as routing availability and synchronization (Lijun et *al*., 2004). However, while the realization of such schemes is routine work in the laboratory, nontrivial problems emerge in long-distance applications. At present, the only suitable system for long-distance quantum communication is photons. To fully exploit the advantages of free-space, it will be necessary to use space and satellite technology. By transmitting and/or receiving either photon to and/or from a satellite, quantum bit can be distributed over truly large distances and thus would allow quantum communication applications on a global scale. Such a scenario looks unrealistic at first sight, but in this study

we will show that the demonstration of quantum communication protocols using satellites is already feasible today. To do so, we will describe different approach space scenarios based on quantum transmission. We then analyze prerequisites to distribute via satellites, describe experimental scenarios for first proof-of-principle experiments and finally give the scenarios involving an Earth-based transmitter terminal allow to quantum key either between ground and satellite, or between two ground stations, or between two satellites and thus to communicate between such terminals employing quantum communication protocols.

## DISCUSION

The secure distribution of the secret random bit sequences known as “key” material is an essential precursor to their use for the encryption and decryption of confidential communications. Quantum cryptography is an emerging technology for secure key distribution with single-photon transmissions: Heisenberg’s uncertainty principle ensures that an adversary can neither successfully tap the key transmissions, nor evade detection (eavesdropping raises the key error rate above a threshold value).

Quantum communications offers many advantages for secure data transmission, e.g. confidentiality, integrity, eavesdropper's detestability. Information is encoded in quantum bits (qubits), intrinsic physical properties, such as polarization of a photon. Quantum physics allows encoding information using the correlation between two or more particles (photons, atoms). Quantum Key Distribution is one of the innovative methods of information processing that emerged from the properties of “superposition of states” and “entanglement». In this study; we present an approach subsystem for quantum communication in space, a photonic transceiver capable of generating and detecting entangled photons as well as faint laser pulses, which the first method of quantum information science that will find its way into our everyday life.

## CONCLUSION

In this dissertation study, we presented scenarios of quantum key exchange between satellites and ground stations. There are three scenarios:

- Station sends the key to the satellite
- Satellite transmits the key to the station
- Station sends the key to another station using the satellite as a mirror

Each scenario has its strengths and also weaknesses. In reality, we cannot use a single scenario because we need a satellite network to exchange the key with the station. Thus, the use of three scenarios depends on the condition of each network node. But we can reduce the budget by looking for a satellite network diagram where the second scenario satellite transmits the key to the station “is the most used. With the second scenario, we place great telescopes at the station on land and on small satellites. Therefore, the maintenance budget of satellites is low. Indeed, this method provides a way to share the key too long-distance with the lowest budget, the most rigorous accuracy and QBER acceptable. Through these scenarios, we can calculate the needs of a satellite network. In addition, we proposed a protocol for secure communication with both authentication methods:

- Authentication symmetric quantum
- Authentication asymmetric
- This approach to the problems of our subject is theoretical, through journals, scientific books. In fact, nowadays the theory of QKD is not yet applicable. But there are experiments in laboratories. For this, their facilities are very rare and their prices too high.

In any case, security is crucial in satellite telecommunications. Moreover, quantum cryptography is a satisfactory solution to improve the safety problem. So, the quantum transmissions are the future of telecommunications.

## ACKNOWLEDGEMENT

I would like to thank Dr. Messai Abderraouf for providing support and material related to educational research and for his valuable feedback as tutor. Also, I am grateful to Prof. Malek Benslama for his support in Electromagnetism and Telecommunication Laboratory which he is heading and for his supervising.

## REFERENCES

Bacsardi, L., 2005. Using quantum computing algorithms in future satellite communication. Acta Astronautica, 57: 224-229. DOI: 10.1016/j.actaastro.2005.03.023

Bolonkin, A.A., 2009. Femtotechnology: Nuclear Matter with Fantastic Properties. Am. J. Eng. Applied Sci., 2: 501-514. DOI: 10.3844/ajeassp.2009.501.514

Carter, P. and M.A. Beach, 2007. Evaluation of handover mechanisms in shadowed low earth orbit land mobile satellite systems. Int. J. Satellite Communi., 13: 177-190. DOI: 10.1002/sat.4600130305

Fernandez, V., R.J. Collins, K.J. Gordon, P.D. Paul and G.S. Buller, 2007. Passive optical network approach to gigahertz-clocked multiuser quantum key distribution. J. Quantum Elect. 43: 130-138. DOI: 10.1109/JQE.2006.887175

Krishnan, A. and T.S. Thangavel, 2010. Integrated quantum and classical key scheme for two servers password authentication. J. Comput. Sci., 6: 1396-1405. DOI: 10.3844/jcssp.2010.1396.1405

Lijun, M., M. Alan and T. Xiao, 2009. High speed quantum key distribution over optical fiber network system, J. Res. Natl. Inst. Stand. Technol. 114: 149-177.

Markus, A., J. Thomas, P. Martin, L. Walter and Z. Anton, 2003. Long-distance quantum communication with entangled photons using satellites. IEEE J. Selected Top. Quantum Electronics, 9: 1541-1551.

Sellami, A., S. Shuhairi and M.R.B. Wahiddin, 2009. Quantum key distribution using decoy state protocol. Am. J. Eng. Applied Sci., 2: 694-698. DOI: 10.3844/ajeassp.2009.694.698