Quantum cryptography for satellite communication

M Mariola[1], A Mirza[1] and F Petruccione[1,2]

[1]University of KwaZulu-Natal, Westville Campus, Durban, South Africa
[2]National Institute for Theoretical Physics, South Africa

E-mail: mmspazio@libero.it

Abstract. This project shows the possibility to use a Quantum key distribution system (QKD) for aerospace applications. The project includes the possibility to use the radio signal of a public channel to synchronize the Quantum bit (qbit) from Alice (transmitter) to Bob (receiver). We also use the radio signal for tracking.

1. Introduction

The research project consists of an aerospace system protecting the communication through QKD cryptography .The key is transmitted and received as polarized photons. There are many kinds of transmission protocols, but it is important to send and receive the photons with the same synchronization from the transmitter and receiver systems. At present this kind of communication is possible in optics fibre and in free space where the transmitter and receiver are fixed. The fixed systems don't undergo the Doppler effect and it is possible to synchronize the signals through GPS signals and it is not complicated to track the receiver and transmitter as it is a mobile system. Generally we call Alice the Receiver System and Bob the transmitter system.

If Eva (Hacker) is in the middle between Alice and Bob the system should not send the QKD. The possible links are : Satellite to Earth Station, Satellite to Balloon, Balloon to Earth Station, Satellite to Satellite. The first link is difficult for Eva to intercept Alice and Bob. In effect for Eva it is possible to intercept Bob only if she is geographically near to him. Eva couldn't use an Aircraft because Bob or Alice could see Eva optically or with Radar and Eva couldn't use another satellite because the orbital speed would be different. The second and third links are more secure against an attack by Eva because she must follow the link line of Alice and Bob. For the forth link , if Alice and Bob have a particular Orbit Eva could intercept them by another satellite.

The other problems are the tracking for the Laser of Alice and the sensor of Bob and the Synchronism of the Quantum bit of the key. The issue of protecting the key is analyzed in a condition where the satellite is ready in the workshop. When the satellite is ready Alice sends Bob the Key (We are sure that Eva is not in the workshop). Once Alice is at the site of the spacecraft ,the password is sent in order to be recognized. As soon as Alice receives the password, she sends Bob the answer. If any problem arises Alice request from Bob (or vice versa) that he shift some bits of the Old key and repeat the process (Eva doesn't know the key).If Alice and Bob are certain that Eva doesn't intercept the QKD , they send another key and start the communication from the public channel. In the follow picture there is a flow-chart of the safe protocol:

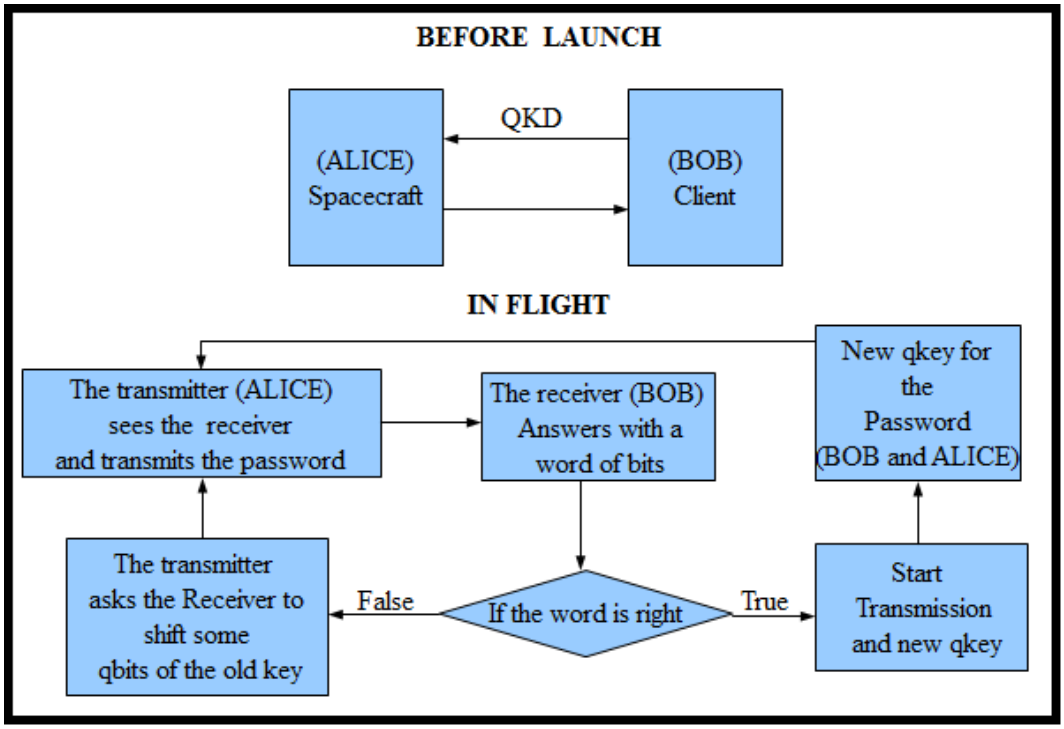

Figure 1. This figure represents the algorithm to recognize Alice to Bob and vice versa during the flight.

The password is transmitted on public channel because Eva doesn't know the key. If we have **n** quantum bits we have a minimum of 2^nattempts.

2. Synchronization

Generally Bob sends the Qbit with a kind of random polarization. Alice doesn't know which polarization Bob is using, but it is necessary that she knows the time. For this reason timing is necessary for the process of synchronization between Alice and Bob. In the stationary frame system it is possible to use the GPS signal, but if we want to use this signal it is necessary to know the position of any satellite and there is no autonomous system. The idea is to synchronize Alice and Bob with a signal from Alice. The channel of the signal of synchronization can be optics or Radio. The optic channel exhibits the problem of noise and if an external body is in the middle of the channel , the system loses synchronism. With the second system we don't have the problem of an external body and can use the public channel to synchronize, send information and track. To design the synchronization we must build a computational model to see the difference in propagation time between laser and radio signal. The frequency of the Radio channel is 1.2 GHz. The variation Δf of the frequency for Doppler effect is shown in equation 1:

$$\Delta f = \frac{1}{\lambda} v_s \cos \chi \tag{1}$$

Where v_s is a tangent orbit velocity , χ is the angle between velocity vector and the direction of the Earth station , λ the wave length. The order of variation of the frequency is 30 kHz. The variation of the frequency is independent from the shape. If the transmitter and receiver choose the clock like a ratio of the frequency of the radio carrier signal, we can take the clock from the radio signal that Bob receives. The system uses the BPSK modulation to send information and synchronization. The receiver recovers the currier and takes the clock from it. When Alice receives the password from Bob,

they begin to transmit. It is necessary to add the delay time due to different propagation time between Laser and radio signal. The distance between Alice and Bob in terms of the Radio signal is longer if compared to the Laser path because there is a refraction problem in the atmosphere and the final trajectory is a curve. For the same reason the tracking's angle of the Laser and Arial can be different from each other. We can have this kind of problem in the highest layers of troposphere and ionosphere. In the following paragraph we'll study the refractive index in the atmosphere. In case of difference in time of propagation between Laser and Radio Signal we can play on the time of persistence of Laser (red line). In this mode when we have a clock impulse the system takes the value of Quantum Bit This is shown in Figure 3:

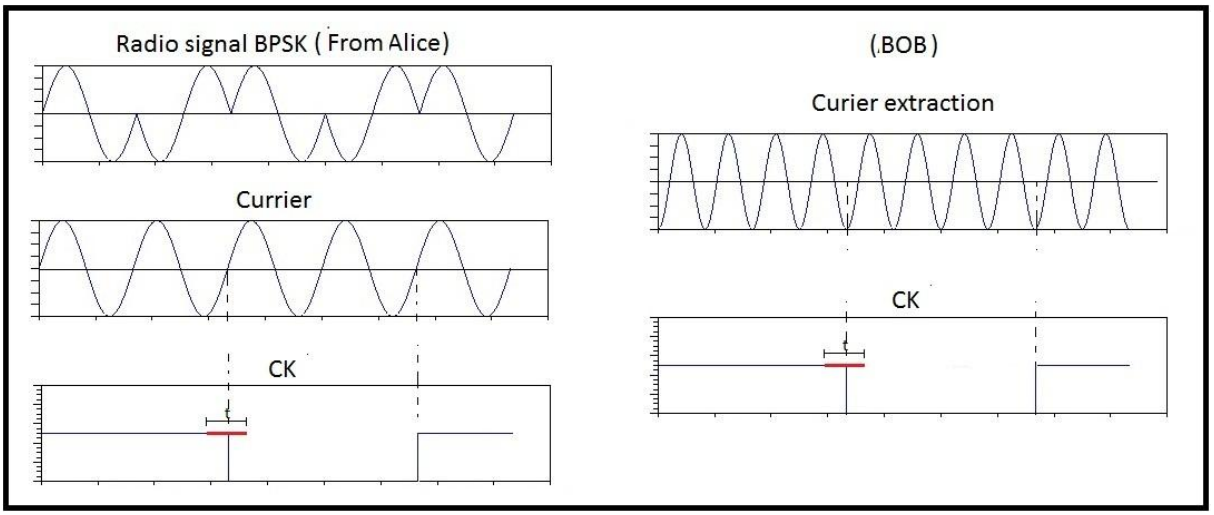

Figure 2. Clock reconstruction

2.1 Refractive index

The trajectory of signals are dependent of the atmospheric conditions. The State parameter of atmospheric gas like pressure , temperature and humidity changes in function of the altitude and consequently also changes the refractive index. The trajectory will be a curve and the angle of tracking will be different from the real position of the satellite. We'll make an estimation of the refractive index from the average annual atmospheric conditions. The refractive index formula is:

$$n = 1 + N * 10^6 \tag{2}$$

Where:

$$N = \frac{77}{T}\left(P + 4810\frac{e}{T}\right) \tag{3}$$

P and T as pressure and temperature are functions of the altitude. The behaviour of these state parameters is calculate by the Rec. ITU-R 835-3 and for the vapour pressure we have:

$$e = \frac{\rho T}{216.7} \tag{4}$$

We have the following shape in the function of Latitude and Season:

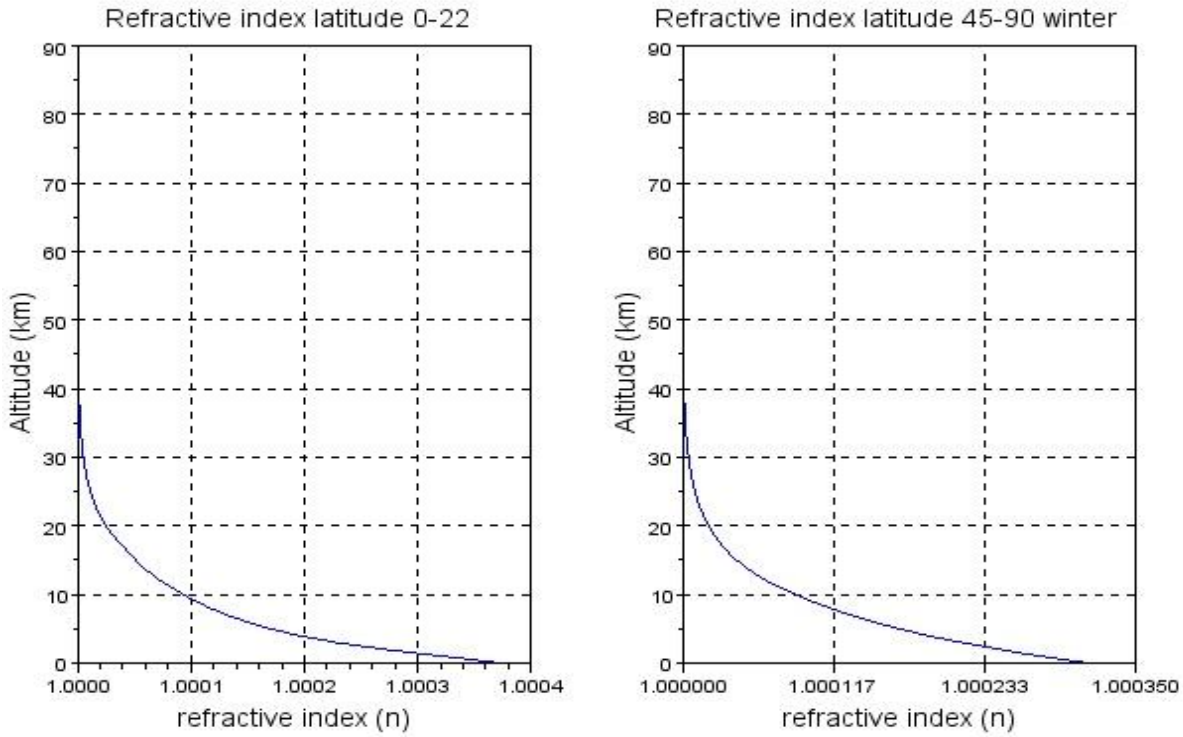

Figure 3. Refractive index for the first 50 km of altitude

Equation 2 can be used only for altitude between 0 km to 50 km. Over 50 km of altitude , the Solar activity ionizes the gas leading to presence of free charge. The formulas of the refractive index in the ionosphere are shown in equations 5 and 6:

$$n_{os}^2 = 1 - \frac{f_c^2/f^2}{1+(f_b/f)\cos\theta} \tag{5}$$

$$n_{xd}^2 = 1 - \frac{f_c^2/f^2}{1-(f_b/f)\cos\theta} \tag{6}$$

where n_{os}^2 and n_{xd}^2 are the refractive index for the characteristic waves propagation respectively to the angle of terrestrial magnetic field θ. Calling with f_b gyrofrequency ,f_c Critical frequency and f the frequency of satellite. The refractive index depends on solar activity and for that we have periodical changes every eleven years and also changes the refractive index of day and night. We can make an estimation about the electronics charge by the ionograms from different institutes of research. In the first approximation we use the data from latitude of Rome and obtain the diagrams in Figure 5.

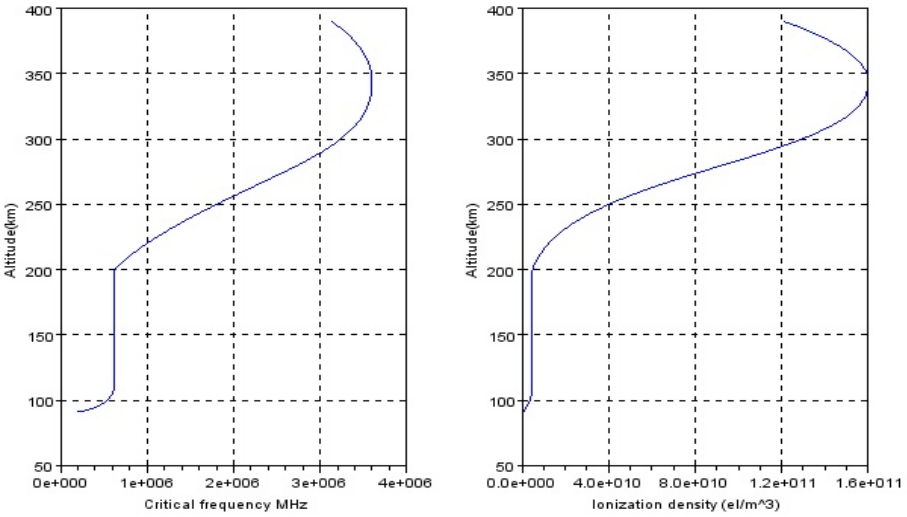

Figure 4. Critical frequency and Ionization density for Latitude of Rome

The gyrofrequency can be determined through the Figure 6 for 90 km of altitude:

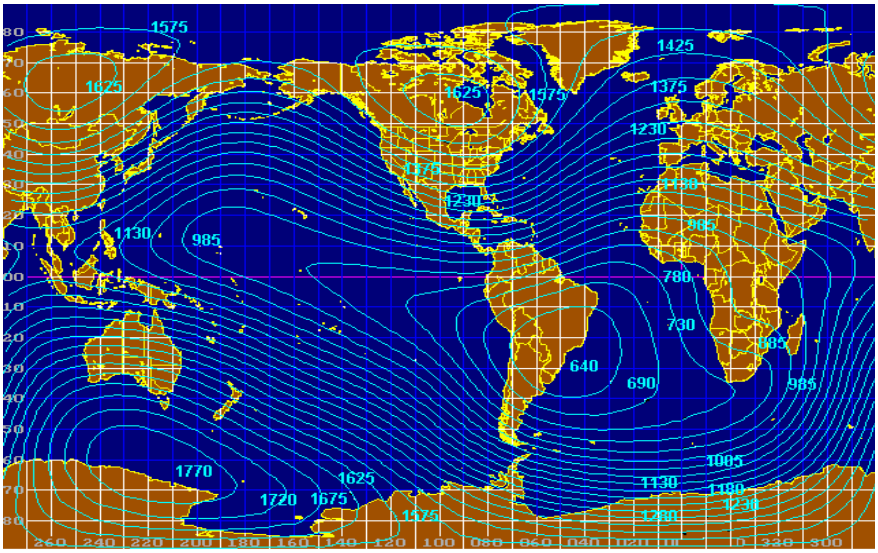

Figure 5. Map of the Gyrofrequency for 90 km of altitude

With these frequencies and for low orbit we can estimate that the radio signal and Laser have the same path because in the lowest layer of atmosphere the refractive index depends on the thermodynamic conditions and in the low ionosphere the value of the refractive index is not so high ($n_{os} \cong 1$ and $n_{xd} \cong 1$). If the radio signal has some delay time respectively to the Laser we can compensate with long laser input or use a higher radiofrequency. For the highest layers of atmosphere the gas molecules can have a distance comparable with the wave length of a laser. In this case the path between Laser and the radio signal is different. In the highest layers of ionosphere we can have a problem with the electronics density.

3. Tracking

Using the public channel and a minimum of two Arials it is possible to make a project that is a tracking system for a Satellite or Balloon with Earth station and vice versa. The conceptual scheme is shown in the following picture:

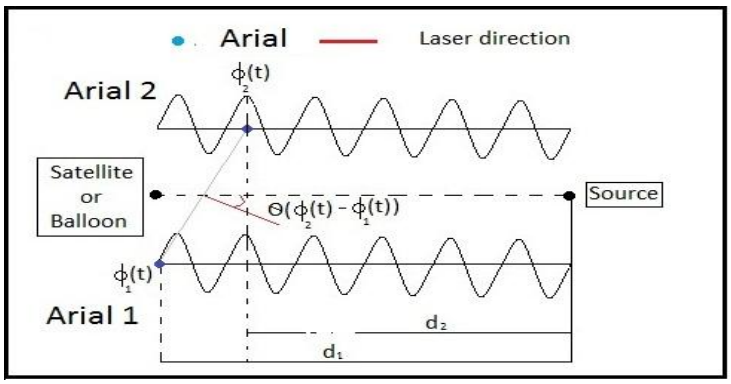

Figure 6. Principle diagram of the tracking system

Arial 1 receives the signal with phase Φ_1 and Arial 2 with phase Φ_2. From the difference of the two phases we know the angular position of the Satellite or Balloon with respect to earth station or vice versa. For that we must use two different frequencies for Alice and Bob in transmission and reception.

4. Conclusion

From the study of refractive index it is evident that the radio signal and Laser signal have paths that are very near. For this reason it is a possible to synchronize the Quantum Bit with Clock from the radio signal and it is possible to use the same signal for tracking and data transmission. The performance can be improved if we use a low orbit because the radio and laser signals are inclined to approach one another . This is also an advantage for the power budget.

5. Acknowledgements

This work is based on research supported by the South African Research Chair Initiative of the Department of science and Technology and National Research Foundation.

References

[1] Bernardini A " Lezioni del corso di sistemi di comunicazione satellitari" ,January 2008,Edizioni Ingegneria 2000,pp.192-199

[2] M.H. De Canck " Ionosphere Properties and Behaviors – Part 1" p.5, June 2006

[3] http://ionos.ingv.it/Roma/

[4] Rec. ITU-R P.835-3

[5] Rec. ITU-R P.453-8

[6] Bennett C and Brassard G 1984 Quantum cryptography:Public Key Distribution and Coin Tossing Proc of *IEEE International Conference on Computer Systems and Signal Processing 175-179*

[7] Ursin R *et al.*3 June 2007 Entanglement-based quantum communication over 144 km 481-486

[8] Richard J Hughes,William T.Buttler 1999 Pratical quantum cryptography for secure free-space communications, Los Alamos,University of California

[9] Bennet C1992 Quantum Cryptography using two nonorthogonal states *Lett. 683121-3124*