Review of Computer Engineering Research
2016 Vol.3, No.1, pp.7-12
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/journal.76/2016.3.1/76.1.7.12

GENERALIZED QUANTUM KEY DISTRIBUTION FOR WDM ROUTER APPLICATIONS

N. Djeffal[1] --- M. Benslama[2] --- I. Messaoudene[3]†
[1,2]*Laboratoire d'Electromagnétisme et de Télécommunication, Université Frères Mentouri Constantine. Constantine Algérie*
[3]*Laboratoire d'Electronique et des Télécommunications Avancées, Université de Bordj Bou Arréridj Bordj Bou Arréridj Algérie*

ABSTRACT

In this paper, we study the ability of quantum networks to support both random and non-random data traffic single-photon quantum communications signals on a shared infrastructure. The effect of wave length on distance coverage with the quantum bit error rate (QBER) of a quantum key distribution (QKD) system is increasing. The results of random phase showed minimal distance coverage over non-random phase. For fluctuating amplitude of random show a change in system performance improved sending capabilities. Hence, it is found that rare fluctuations should not degrade system performance significantly, but the data sending mode has a significant effect on channel integrity.

Keywords: Quantum bit error rate, Quantum key distribution, Wavelength division multiplexing.

Received: 23 November 2015/ **Revised:** 23 December 2015/ **Accepted:** 6 January 2016/ **Published:** 13 January 2016

Contribution/ Originality

This study presents an original structure of generalized quantum key distribution suitable for wavelength division multiplexing (WDM) application.

1. INTRODUCTION

The Quantum algorithmic for adapting networks in WDM (Wavelength Division Multiplexing) routers for voice, data, and multimedia applications have brought a new playing field in supporting predictable and secured communication networks. Nowadays, Multimedia communication for reliable data exchange requires the communication to meet stringent standard where information can be easily transmitted and received feedback with ease and comfort [1-3]. High demand of network has forced a rapid increase in communication bandwidth, but unfortunately it is done with expenses on communication traffic and forfeit traffic security [4-7]. In order to solve the problem, quantum cryptography is the alternative to solve this problem and

† Corresponding author

Quantum key distribution (QKD)uses quantum mechanics to guarantee secured communication data [4-7].

In general, a communication model consists of a system involves a source that input data to a channeling medium and a receiver where modulation and demodulation occur [2, 3]. The source carries and the initial information which uses symbols from a finite set data (alphabet, digit or its equivalent) and the mode of transmission can be done either in one shot or sends them to regular intervals [4-7]. In this case, each of the transmitted symbolsdata is not depended on the previous ones [8-10]. Discrete channels transmit symbols froma specific set (input alphabet), and they generate in their output another set of symbols (output alphabet) [1]. As the input alphabet and the output alphabet can be different, it is necessary to use an encoding that maximizes the efficiency of the transmission [1, 4-7]. Basically, the encoding consists in assigning a specific word to each one of the symbols in the input (built with elements of the output alphabet) [8-10]. This must be done by finding a mean length of the code to be minimized, but also a unique decoding in the receiver. Also, usually the channel is not ideal, the received information differs from the sent information, and this difference translates into a probability of error in the behavior of the receiver; whose mission is just to recover the original information, with the maximum possible fidelity [1, 11].

In Quantum communication approach, the above mentioned concepts still utilized, but with some intense changes and modifications. Initially, a quantum data is mostrelated to the symbol generated by the input source. Meaning the data through the channel is a dimensional Hilbert space (qubits). It is usually also needed that the source encoding assign to each symbol-state a representation in qubits [11]. In a second place, any process related to the transmission of information that alters its state, is characterized by a super-operator [12-14]. But in this case, the usual thing is to include the noisy behavior of the channel, because of the interaction between the system and the environment (more or less active), in the inputdata. In the error-free channels, a pure state is associated with each symbol [8-10] meanwhile in the noisy channels a mixed state is used. They are closed quantum systems, composed of subsystems associated with the information (open system) and to the noisy environment [11].

2. METHOD

A Wavelength Division Multiplexing (WDM) switch network consists of switching nodes with communication that links interconnecting the nodes. Each Channel link carries a certain number of wavelengths and each wavelength is further divided into a number of time slots to control the package transfer. The node architecture for sub-wavelength demands a multicast data transfer mode supporting three links with congestion and free links. The package of wavelengths link and three time slots for all the channels and node for the determination of sessions utilizing the time slot of bandwidth. Quantum communication network consists of input source, communication channel and output just like classical mode and the security of data depends on all of the three stages of communication, the current research demonstrates that the mode of data transmission depends on the channel integrity and its capacity [11]. From classical information theory, we have bits which can be either 0 or 1. In quantum information theory the equivalent is quantum bits or qubits [11]. These are two dimensional quantum mechanical states. We can encode the bits as qubits using orthogonal states, with the notation 0 and 1 [11]. The advantage of the qubits is that they can be in a superposition and through the channel while sending the data; the combiner will combines the two data of orthogonal polarization in directing them to the correct channel [8-10]. However, the combiner and splitter can only differ the polarizations by a finite value, introducing cross-talk [12-14]. This means that a small part of pulse addressed might still inject, and vice versa. In a balanced interferometer, this would affect interference, since then a small part would be modulated which should not have been, and vice versa. In this setup where the interference is unbalanced, the difference in optical path lengths makes the pulses leave sender and arrive to the receiver with a time delay [8-10]. This directs the crosstalk to arrive at different times in channel coupler to identify the required data signal. The network wave converted or wavelength converter is a device that allows the conversion of a signal from one wavelength to another wavelength. In optical networks without wavelength converters, each message can only be switched from a certain wavelength at an input port to the same wavelength on an output port [8, 12, 13]. Although wavelength convertersimprove the network blocking performance, it is well known thatall-optical wavelength converters are prohibitively expensive [8-10].

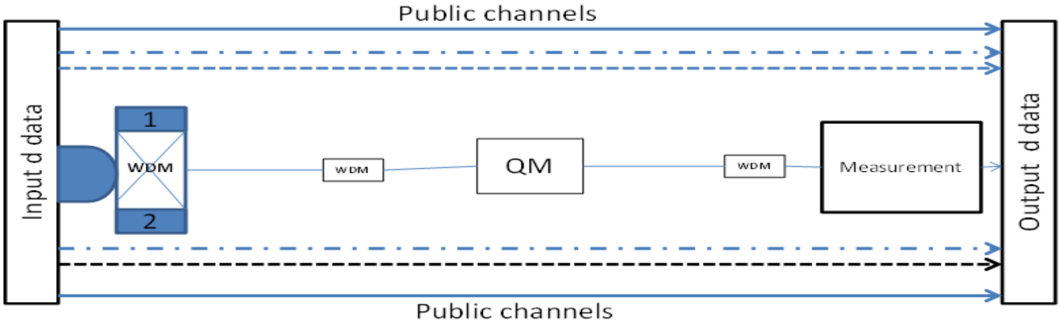

Fig-1. Schematic of network supporting QKD and WDM channels.

A system and a method for quantum key distribution over a multi-user wavelength division multiplexing (WDM) network are shown in Fig.1.

The fig.2. shows the quantum bit error rate (QBER) response as a function of propagation distance in Km, the channels are varied between -10 and -30 dBm. The transmitter can select a receiver among the receivers to be communicated therewith, and transmits quantum signals to the selected receiver over the WDM network. The quantum signals are on a wavelength equal to a receiving-wavelength of the receiver. Therefore the WDM network allows quantum signals to be communicated between the transmitter and the receivers by wavelength routing. A communications network has a plurality of nodes interconnected by an optical transmission medium. The transmission medium is capable of a carrying a plurality of wavelengths organized into bands. A filter at each node for drops a band associated therewith, and passively forwards other bands through the transmission medium [11].

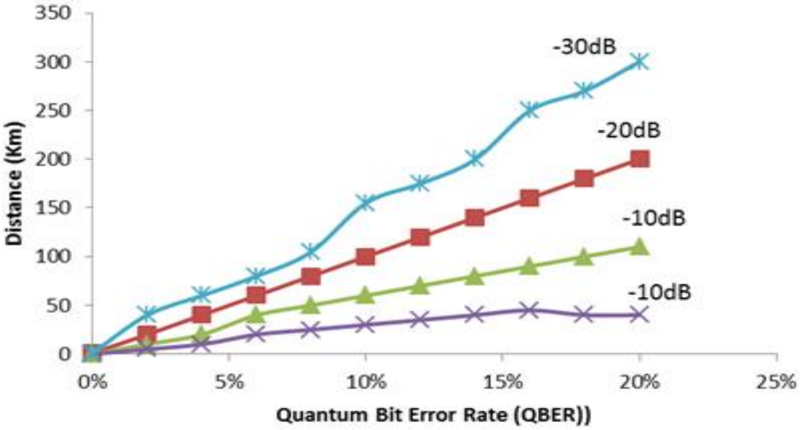

Fig-2. The QBER response as a function of propagation distance

A device is provided at each node for adding a band to the transmission medium. Communication can be established directly between a pair of nodes in the network sharing a common band without the active intervention of any intervening node. This allows the network to be protocol independent. Also, the low losses incurred by the passive filters permit relatively long path lengths without optical amplification.

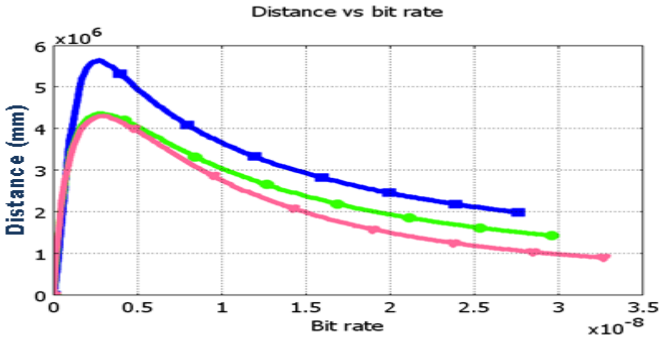

Fig-3. The bit rate as a function of distance

The fig.3. shows thekey generation rate that quantum bit rate as a function of distance in line with transmission parameters and prior to channel transmission reduction the maximum transmission distance was about 6Km and that is expected the rate is with stable amplitude, while minimum is obtained for random or fluctuating data exchange. The difference between random and uniform random phase is quite obvious hence although both are plotted, only uniform data phase is visible and attained high distance. As mentioned earlier that the maximum transmission distance is reached at a rate around 6Km, with lower bitrate around 2.5x10^{-7}. This has agreed with the general principle of congested and decongested phenomena of if the channel is fully occupied with random data, the channel officially will definitely low and of course, is also through that the data are fully restricted to travel far [12-14]. To find the maximum transmission key generation rate, the distance bit rate for each distance was calculated for all model was found and it can be seen that stable amplitude gives the best key generation rate [11]. For varying amplitude, non-random fluctuations appear to be best. It actually gives about the same maximum transmission distance, only with a lower rate around 2.5x10^{-7}. The reason for this may be that at most one of the values is the optimal value. Hence, many pulses will be of non-optimal amplitudes, which have the lowest rate. The random fluctuation gives a lower rate for all distances, and a shorter maximum distance. When having random fluctuations, one model has no prior knowledge of the amplitude. Thus, having announced fluctuations giving another model, this prior knowledge should give one model an advantage, and lower key generation rate. However, we must remember that in these two situations, the channels sharethe same knowledge about the amplitude as third dose. Hence, we can interpret from this plot that it is better that all of them given the amplitude than none.

3. CONCLUSION

Generally, the present study provides a communication system for quantum key distribution, the effects on source data phase where random phase and uniform transmission mode where studied for stable amplitude. The results of random phase showed minimal distance coverage over non-random phase. For fluctuating amplitude of random shows change in system performance improved sending capabilities. Hence, it is concluded that rare fluctuations should not degrade system performance significantly, but the data sending mode has a significant effect on channel integrity.

Funding: This study received no specific financial support.

Competing Interests: The authors declare that they have no competing interests.

Contributors/Acknowledgement: All authors contributed equally to the conception and design of the study.

REFERENCES

[1] V. Alipasha, W. Gregor, and Z. Anton, "Experimental two-photon, three-dimensional entanglement for quantum communication," *Physical Review Letters*, vol. 89, pp. 240401-240404, 2002.

[2] Y. Chen and W. Tang, "Reconfigurable asymmetric optical burst switching for concurrent DWDM multimode switching: Architecture and research directions topics in optical communications," *Communications Magazine, IEEE*, vol. 48, pp. 57 –65, 2010.

[3] G. V. Chowdhary and C. S. R. Murthy, "Dynamic multicast transfer engineering in WDM groomed mesh networks," Proc. BROADNETS'04, 2004.

[4] A. Khalil, C. Assi, A. Hadjiantonis, G. Ellinas, and M. A. Ali, "On multicast traf_c grooming in WDM networks," *Proc. IEEE ISCC'04,Canadian Conf. Electrical and Comp. Eng. 2004 (IEEE Cat.No.04CH37513)*, vol. 2, pp. 785–788, 2004.

[5] T. Kiyoshi, C. Marcos, K. Go, L. Hoi-Kwong, and A. Koji, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev.*, vol. A90, pp. 052314-052323, 2014.

[6] M. A. Nielsen and I. L. Chuang, *Quantum information and quantum communication.* Cambridge, U.K: Cambridge University Press, 2000.

[7] M. Oystein, L. Lars, and S. Johannes, "Security of quantum key distribution with arbitrary individual imperfections," *Phys. Rev.*, vol. 3, pp. 032337-032343, 2009.

[8] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics*, vol. 1, pp. 165– 171, 2007.

[9] D. M. Ignacio, V. Reinaldo, B. Alejandra, and D. J. Ramón, "Genetic algorithm for joint routing and dimensioning of dynamic WDM networks," *Journal of Optical Communication Network*, vol. 1, pp. 608-621, 2009.

[10] M. A. Juan and L. Norbert, "Quantum communication with coherent states and linear optics," *Phys. Rev. A.*, vol. 90, pp. 042335-042335, 2014.

[11] N. Gisin and R. Thew, "Quantum communication technology," *Electronics Letters*, vol. 46, pp. 965-967, 2010.

[12] N. l. Singha and B. Mukherjee, "Protecting multicast sessions in WD moptical mesh networks," *IEEE J. Lightwave Tech.*, vol. 21, pp. 884-892, 2003.

[13] M. Vadim, "Quantum cryptography and quantum cryptanalysis," PhD Thesis, Norwegian University of Science and Technology, 2007.

[14] K. Zhu, H. Zang, and B. Mukherjee, "A comprehensive study on nextgenerationoptical grooming switches," *IEEE J. Select. Areas Commun.*, vol. 21, pp. 1173-1186, 2003.

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.