Proceedings Paper:
Razavi, M and Salehi, JA (2000) Fiber-optic CDMA networks incorporating multiple optical amplifiers. In: IEEE Global Telecommunications Conference, Vol. 2. GLOBECOM '00, 27 Nov - 01 Dec 2000, San Francisco, CA, USA. IEEE, pp. 1247-1253. ISBN: 0-7803-6451-1.

https://doi.org/10.1109/GLOCOM.2000.891336

Feasibility of Wireless Quantum Key Distribution in Indoor Environments

Osama Elmabrok and Mohsen Razavi
School of Electronic and Electrical Engineering
University of Leeds, Leeds, LS2 9JT, UK
Email: elome@leeds.ac.uk and m.razavi@leeds.ac.uk

***Abstract*—We propose and study the feasibility of wireless quantum key distribution (QKD) in indoor environments. Such systems are essential in providing wireless access to the developing quantum communications networks. We find a practical regime of operation, where, in the presence of background noise and loss, secret keys can be exchanged. Our findings identify the trade-off between the acceptable amount of background noise and the receiver field of view, where the latter determines the accessibility of the QKD system. In particular, we show that, with a proper setting, we can provide mobility for the QKD users without imposing stringent conditions on beam steering.**

I. Introduction

Quantum key distribution (QKD) provides a promising means for achieving security in the quantum era [1], when our conventional techniques for data security, based on computational complexity, may fail. QKD provides a method for securely distributing random keys between two users based on the laws of physics. It has been demonstrated over both optical-fiber [2] and free-space channels [3]. Today, various QKD systems are commercially available, e.g. ID Quantique. In order to support a wider group of end users, QKD networks are also being developed across the world. The focus of most of these efforts is mainly on the core network [4], or the wired access to such a backbone [5]. This works looks at another unexplored dimension for QKD technology, and that is the much needed wireless access to quantum networks. Wireless QKD links will provide easy and convenient access to the network nodes and can be implemented in office spaces or corporates, such as banks, who are the main users of secure communications. For instance, customers in a bank office can exchange secret keys with the bank wirelessly without the need for waiting for a teller or a cash machine, or being afraid of skimming frauds. Such systems can eventually be implemented for home users when QKD technologies reach that market. This is in line with the ever increasing use of portable personal devices and the high demand for data security in indoor environments. Here we find the feasibility regime for QKD in a single-room single-user scenario. Multiple users can also be supported by using relevant multiple-access techniques [6]. Our results confirm that there exists a practical regime of operation where secret keys can be exchanged using wireless QKD links.

II. System Description

Here we look at a particular scenario in which we have an empty window-less room, which has been illuminated by an artificial source of light; see Fig. 1. For the sake of our numerical results, we assume a $4\times4\times3$ m^3 room. The lighting source is assumed to be a Lambertian one with a semi-angle at half power of 70°. The key contribution of the light source is via its power spectral density (PSD), denoted by S, at the operating wavelength of the QKD link (880 nm, in our case). We assume that the QKD link is composed of two components. The QKD receiver is fixed and located at the center of the ceiling, while the QKD transmitter can be anywhere on the floor. We assume that at the receiver the unwanted light is filtered out by using a narrowband filter with bandwidth $1/T$, where T is the width of the transmitted pulses by the QKD user. In our simulation we assume $T = 100$ ps. We also assume that the decoy-state variation of the BB84 protocol is in use [7], and assume infinitely many decoy states for our analytical study of the secret key generation rate. In practice, one can approach the same limit with a finite number of decoy states [7]. The key advantage of the decoy-state protocol is to use weak laser pulses, instead of ideal single photon sources, while being immune to potential photon-number splitting attacks.

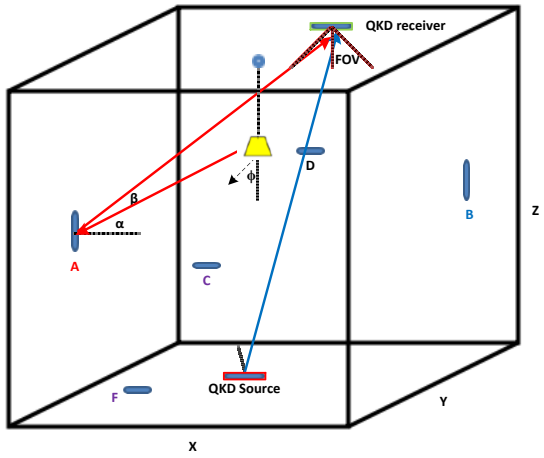

Fig. 1. A wireless QKD link in an indoor setup. The transmitter is mobile, while the QKD receiver is fixed on the ceiling.

A critical component of our key-rate analysis is the background noise that enters our QKD receiver. By accounting for the reflections from the floor and the walls [8], we calculate the background noise from the lighting source at the QKD receiver. The latter will go up with increase in S as well as the QKD receiver's field of view (FOV). The latter would determine how much mobility may be allowed. We therefore look at the trade-off between these two parameters in determining the secure versus insecure regimes of operations.

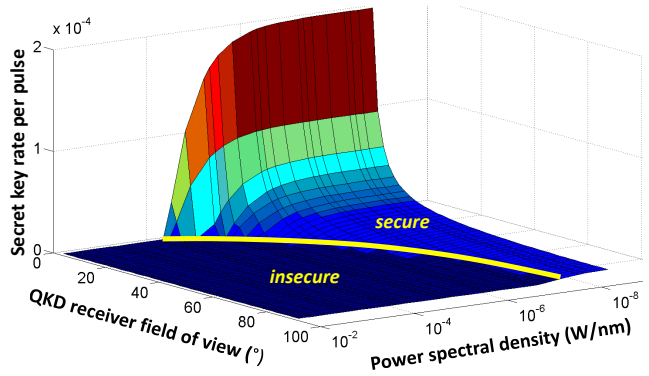

Fig. 2. Secret key generation rate versus the QKD receiver's FOV and the PSD of the lighting source. The QKD transmitter is located at the center of the floor, while the QKD receiver is at the center of the ceiling.

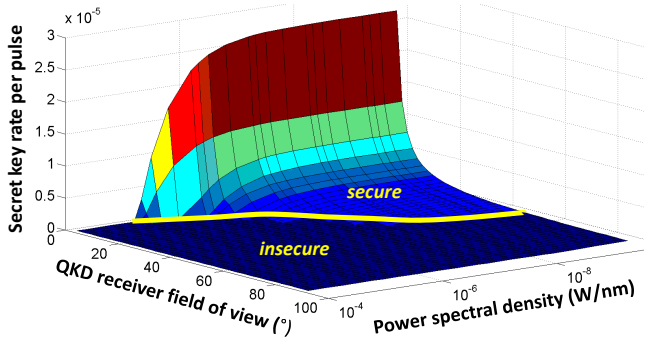

Fig. 3. Secret key generation rate versus the QKD receiver's FOV and the PSD of the lighting source. The QKD transmitter is located at the lower corner of the room, while the QKD receiver is at the center of the ceiling.

III. Numerical Results

We consider two scenarios that represent the best and the worst working conditions for the QKD link described above. In the fist scenario, we assume that the QKD transmitter, with a semi-angle at half power of 30°, is located at the center of the floor sending light upwards to the QKD receiver. In the second scenario, we assume that the same transmitter is located at the lower corner of the room (farthest distance) and it sends light vertically upward (loose beam steering). The reflection coefficient off the walls is 0.7 and off the floor is 0.1, assuming that the carpet or the potential furniture have less reflection than the walls. The employed single photon detectors are assumed to have a quantum efficiency of 0.8 and an effective area of 1 cm^2. Considering the short duration of the transmitted pulses, as compared to the delay in the reflected beams, we neglect to collect the reflected QKD signals off the walls. We also assume that none of these reflected pulses will interfere with the forthcoming QKD pulses. That would imply that the repetition rate of the QKD link must be on the order of 100 MHz or lower, which is suitable for our scheme.

Figures 2 and 3, respectively, show the secret key generation rates that can be achieved in the setup of Fig. 1 in the first and the second scenarios. The key rate is defined as the probability of obtaining a secret key bit per transmitted quantum signal. Both graphs roughly show in what regimes of operation, in terms of the QKD receiver's FOV and the lighting source's PSD, it is possible to exchange secret keys. For large values of PSD, the FOV must be reduced to accumulate less background noise, while in the other extreme, the QKD receiver can be kept wide open allowing to cover a larger area. The secure regime is also wider when the QKD transmitter is better aligned and closer to its receiver. The rather large semi-angle for the QKD transmitter would, however, allow us to communicate with the QKD receiver even from the corner of the room with little penalty in the generated key rate. These results imply that for a room lit by white LED bulbs, with PSD on the order of 10^{-6} W/nm at 880 nm, a large FOV can be employed for the QKD receiver, which, in turn facilitates the mobility of the transmitter device. Having large FOVs will also make the system less dependent on accurate beam steering, which reduces the complexity of the required modules. Given that, by adjusting the FOV, we can even tolerate PSDs on the order of 10^{-4} W/nm, one can be optimistic that such systems can even work in the presence of other sources of light. Proper beam steering may, however, be needed to minimize the background noise level in such cases.

IV. Conclusions

We showed that there exists a practical regime of operation within which a wireless QKD system can generate secret keys. Such systems can provide the first link within a larger quantum network or facilitate the use of QKD in common areas for many users. Our work provided a theoretical feasibility analysis for wireless and mobile QKD in its battle with the background noise. A practical demonstration of such systems will not be far away considering the extent of progress in implementing QKD modules with integrated optics [9] as well as the progress in beam steering in classical optical wireless communications [10]. Such work will result in high-rate wireless links for many QKD users.

The authors would like to thank Z. Ghassemlooy and D. Bitauld for fruitful discussions.

References

[1] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sept. 2009.

[2] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307km of optical fibre," *Nature Photon.*, vol. 9, pp. 163–168, Feb. 2015.

[3] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010504, 2007.

[4] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[5] B. Fröhlich *et al.*, "A quantum access network," *Nature*, vol. 501, pp. 69–72, Sept. 2013.

[6] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, 2012.

[7] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, July 2005.

[8] F. R. Gfeller and U. Bapst, "Wireless in-house data communication via diffuse infrared radiation," *Proc. IEEE*, vol. 67, pp. 1474–1486, Nov. 1979.

[9] P. Zhang *et al.*, "Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client," *Phys. Rev. Lett.*, vol. 112, p. 130501, Apr 2014.

[10] A. Gomez *et al.*, "Beyond 100-Gb/s indoor wide field-of-view optical wireless communications," *Photonics Technology Letters, IEEE*, vol. 27, no. 4, pp. 367–370, Feb 2015.