Towards a Smooth Integration of Quantum Key Distribution in Metro Networks

Slavisa Aleksic[(1)], Senior Member, IEEE, Dominic Winkler[(1)], Florian Hipp[(2)], Andreas Poppe[(2)], Gerald Franzl[(1)], and Bernhard Schrenk[(2)], Member, IEEE
[1] *Institute of Telecommunications, Vienna University of Technology, Favoritenstrasse 9-11/E389, 1040 Vienna, Austria*
[2] *Safety & Security Department, AIT Austrian Institute of Technology GmbH, Donau-City-Strasse 1, 1220 Vienna, Austria*
e-mail: Slavisa.Aleksic@tuwien.ac.at

ABSTRACT
Quantum key distribution (QKD) systems have already reached a reasonable level of maturity. However, a smooth integration of commercial QKD systems in metropolitan area networks has still remained challenging because of technical and economical obstacles. Mainly the need for dedicated fibers and the strong dependence of the secret key rate on both loss budget and background noise in the quantum channel hinder a practical, flexible and robust implementation of QKD in current and next-generation optical metro networks.

In this paper, we discuss these obstacles and present approaches to share existing fiber infrastructures among quantum and classical channels. Particularly, a proposal for a smooth integration of QKD in optical metro networks, which implies removing spurious background photons caused by lasers, amplifiers and nonlinear effects in optical fibers, is presented and discussed.
Keywords: Quantum Key Distribution (QKD), Metropolitan Area Networks, Raman Scattering.

1. INTRODUCTION

Current commercially available QKD systems generally presume dedicated point-to-point fiber links connecting two network terminals that exchange keys. For simplicity and in accordance with network security literature, the two terminals are called Alice and Bob. The challenge of QKD is to exchange quantum bits (qubits) between Alice and Bob that yield the encryption key used to secure their communication. Photons received by Bob not originating from Alice reduce the secret key-rate and indicate a potential intruder. However, if noise photons exceed a certain level, a secret key exchange becomes impossible.

In this paper, we analyse how Raman scattering challenges the integration of QKD in metropolitan area networks, assuming the so-called co-existence scheme, where quantum and classical communication channels share the same fiber to reduce the associated costs. In Section 2, we briefly outline integration options and challenges, explain the Raman scattering problem and present the setup used to measure Raman scattering. Section 3 presents estimated performance of the proposed method for the integration of QKD in a legacy DWDM system. Finally, Section 4 summarises our findings and concludes the paper.

2. INTEGRATION OF QKD IN METRO NETWORKS

Two deployment options for QKD in the metropolitan area are sketched in Figure 1. The traditional one, depicted in Figure 1a), uses two dedicated fibers to transmit the faint quantum signals on one fiber and any other (conventional) signals on the other, including the key distillation channel needed to perform error correction and privacy amplification required to establish the quantum key distribution [1].

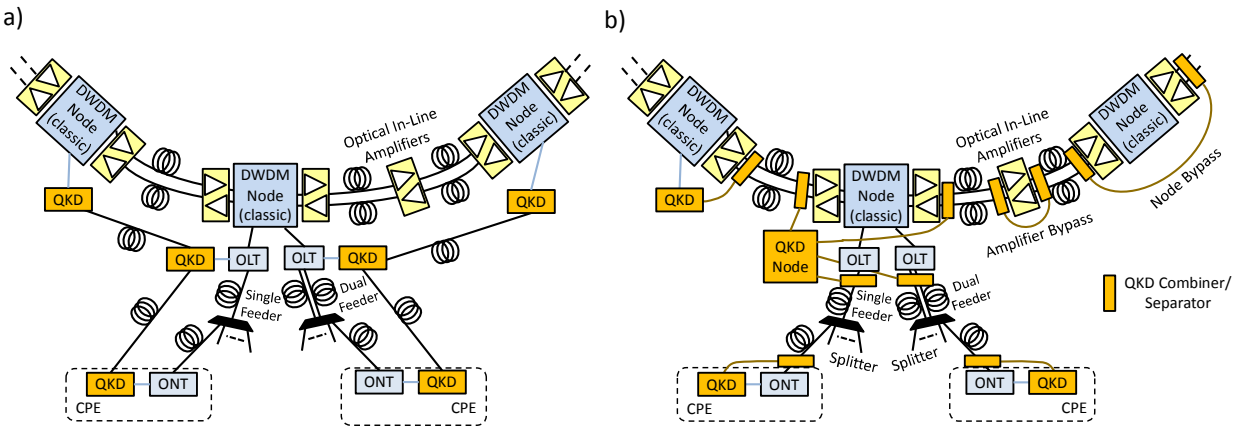

Figure 1. Deployment options for QKD in metropolitan area networks: a) dedicated fibers for QKD and b) smooth integration of QKD in the co-existence scheme.

The second deployment option is depicted in Figure 1b). It envisages the integration of QKD assuming the co-existence scheme, where the quantum channel, the key distillation channel and classical communication channels are multiplexed/demultiplexed using the so called QKD combiner/separator and transmitted over the same fiber.

Several studies have shown that co-existence architectures are in principle possible [2 - 8], but impairments strongly limit the performance of QKD systems. It has been estimated recently that the optical noise power in a quantum channel should be below about -100 dBm to not severely impact the performance of a typical QKD system using the BB84 protocol [8]. Some more advanced QKD schemes are slightly more resistant to background noise. Using the current QKD technology, limiting the number of conventional WDM channels to four and reducing the launched power far below the standardized levels, a reach up to 50-90 km is achievable [3]. However, these restrictions on the system parameters are hardly achievable with common WDM metro network designs.

2.1 Extending QKD encrypted links towards QKD secured networks

The limited reach of weak quantum signals binds its distribution to a rather small range. To become scalable, means to cascade QKD encrypted links into a QKD secured network need to be defined. If all network nodes provide no other than QKD based ports, the entire network can be assumed protected against outsider attacks. However, first the integration in the physical layer needs to be solved and based thereon potential QKD architectures evaluated. Topologies to be considered are: point-to-point, as depicted in Figure 1, and point-to-multipoint in the access part of metropolitan networks, as well as ring and meshed topologies interconnecting the QKD terminals to achieve a QKD based secure metropolitan area network. When multiple terminals use the same quantum channel, the utilisation of additionally needed optical components can be improved by transporting different quantum signals in parallel, i.e., using a feasible multiplexing technique to separate quantum signals. To extend QKD from point-to-point to any other topology, various optical components are needed to realize a QKD node such as optical filters (muxes/demuxes), splitters and switches (e.g. micro-electro-mechanical systems – MEMS). Their influence on the quantum channel needs to be considered in the system design. In case the degradation caused by any component is more than what a by-pass causes, the bypass is to be foreseen in order to maximise the achievable secret key rate. Amplifiers generally have to be bypassed.

2.2 Challenges in Integrating QKD

QKD systems are extremely sensitive to losses and noise. Strong conventional signal levels may therefore constitute severe impairments on the weak quantum signals [3]. These impairments have been identified and analysed in [4, 5, 8]. The 3rd transmission window around 1.5 μm (C-band) is most widely used for long-range communications due to the low attenuation down to 0.2 dB/km. Attractive also for QKD systems, but co-existing classical signals within the same band cause serious impairments [8]. The band around 1.3 μm (O-band) shows higher attenuation of about 0.3 dB/km and is traditionally used for local area and access networks. Recent trends in optical access technology indicate that high data rates above 10 Gbit/s and the DWDM technology available for the C-band will increasingly be used also in the access area. Therefore, we focus on the 1.3 μm region (O-band) and assume all conventional channels to reside in the C-band (around 1.5 μm). The influence of numerous nonlinear effects such as four-wave mixing, Brillouin and Rayleigh scattering can be avoided by allocating the quantum channel spectrally far away from any classical data channels. However, Raman scattering still represents a source of bothersome noise photons in the quantum channel, even if the spectral separation between the quantum and classical channels is 200 nm and more.

2.3 Raman Scattering

An accurate consideration of the impairments caused by Raman scattering and an effective noise filtering in the O-band are essential. We first concentrated on defining and analysing the method for combining and separating of QKD and classical signals by spectral filtering. A cascade of two band multiplexers/ demultiplexers (WDM couplers/splitters) is used as shown in Figure 2, because with a single typical band filter sufficient band separation was not achieved. Additionally, a narrow-band filter (0.1 nm) is needed in front of the QKD receiver to further reduce the noise level. The experimental setup depicted in Figure 2 is applied to experimentally analyse the combining/separating of quantum and classical channels and also to evaluate the influence of Raman scattering. Because noise levels below -90 dBm are hard to measure with conventional optical spectrum analysers (OSA), we count the noise photons using a single-photon avalanche diode (SPAD). An 1550.12 nm CW laser source with 3.5 dBm optical output power is used as Raman pump. The measured forward Raman scattering in standard single mode fiber (SSMF) at lengths of 14.3 km and 17.1 km is shown inset in Figure 2 (continuous lines) together with simulation results (dashed lines). For obtaining the simulation results we used the fiber model of the commercial tool VPI TransmissionMaker with adapted Raman gain spectrum. At 1250 nm the noise level is as low as -120 dBm and increases toward longer wavelengths. Above 1360 nm and 1400 nm the optical noise power rises above -100 dBm and -95 dBm, respectively, which prohibits reliable exchange of quantum keys. Experimental and simulation results fit very well over the wavelength range considered, i.e., from 1250 nm to 1400 nm.

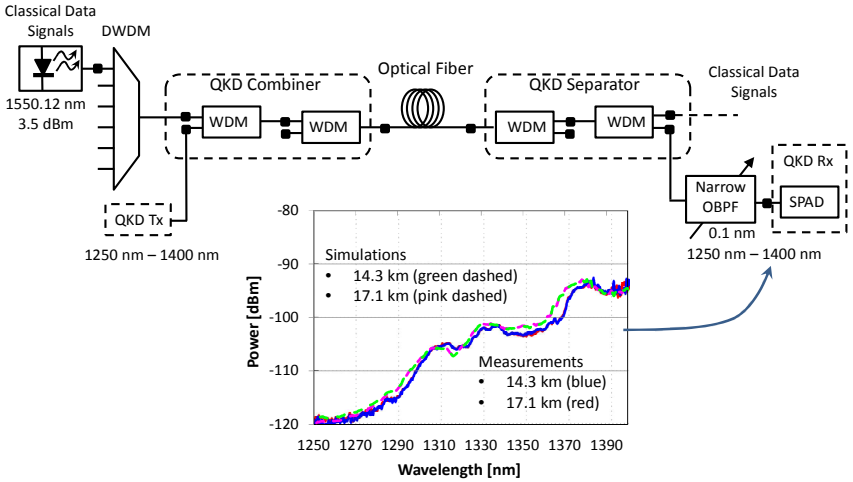

Figure 2. Experimental and simulation setup for analysing the influence of forward Raman scattering on integrated QKD systems in metropolitan area networks. Inset measurement and simulation results for 4.3 km and 17.1 km of standard single mode fibers (SSMF) and the wavelength range from 1250 nm to 1400 nm.

3. QKD PERFORMANCE

To analyse the performance of QKD integration options in the metropolitan area we apply a combined experimental and simulation approach. First, we analyse a commercial DWDM system (Wave Star OLS400G) configured to provide 20 DWDM channels (classical data channels). The measured optical spectrum of the 20-channel DWDM signal after the DWDM multiplexer, an optical amplifier (EDFA) and 5 km (blue line) or 14 km (red line) of standard single mode fiber (SSMF) is shown inset in Figure 2a). Additional to the 20 data channels we see at 1510 nm an optical supervisory channel (OSC). The measured data is used to set the simulation parameters for estimating the achievable secret key rate (R_{sec}) over a co-existing quantum channel integrated using the QKD combiners/separators depicted in Figure 2. To calculate the achievable secure data rate for two QKD protocols, BB84 and SARG, we apply the analytical model proposed in [2]. The configurations analysed comprise a plain point-to-point link, a single bypass of an optical amplifier and a bypass of an entire DWDM node, as shown in Figure 3.

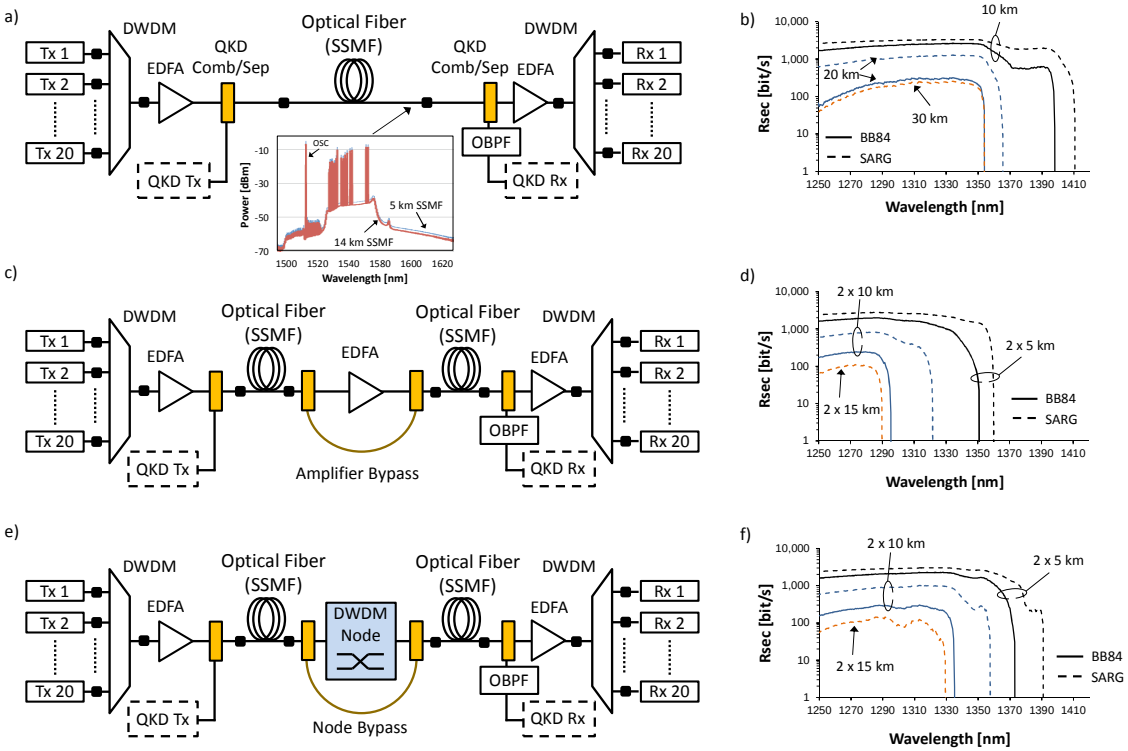

Figure 3. a) Integrated QKD/DWDM link - inset measured spectra of a 20-channel DWDM link after 5 km (blue line) and 14 km (red line) of standard single mode fiber (SSMF), OSC: Optical Supervisory Channel- b) secret key rate (R_{sec}) for three link lengths:10km, 20km und 30km, c) amplifier bypass, d) R_{sec} for amplifier bypass, e) node bypass, and f) R_{sec} for node bypass.

The point-to-point configuration depicted in Figure 3a) yields a secret key rate (R_{sec}) of several kbit/s for 10 km long links and wavelengths up to about 1400 nm. Figure 3b) shows that an R_{sec} as high as 1 kbit/s is possible up to 20 km when using the SARG scheme, while the BB84 scheme achieves no more than some hundreds bit/s. Using the SARG scheme an R_{sec} of about 100 bit/s can be expected for link lengths as long as 30 km. When bypassing an optical amplifier as shown in Figure 3c), similar values for R_{sec} can be obtained, but the usable wavelength range is remarkably reduced, as shown in Figure 3d). The increased losses on the QKD path due to the insertion of the QKD combiner/separator pair and the higher noise level due to the stronger Raman scattering and the amplified spontaneous emission (ASE) from the amplifier jointly cause the reduction of the usable wavelength range by about 50 nm. The influence of bypassing a DWDM node as depicted in Figure 3e) is shown in Figure 3f). It reduces the usable wavelength range by about 20 nm, compared to the point-to-point link without bypass, while providing similar secret key rates in the usable range. Hence, when allocating the quantum channel in the O-band between 1260 nm and 1290 nm, reliable secret key exchange can be achieved at rates of several kbit/s up to 10 km of SSMF and at about 100 bit/s over 30 km links, both in co-existence with many classical channels in the same fiber and if inline-amplifiers and conventional network nodes are carefully bypassed.

4. CONCLUSIONS

A smooth integration of quantum key distribution (QKD) systems in deployed metropolitan area networks is an important step towards a practical and economical use of quantum cryptography. In this paper, we proposed and investigated a method for reliable quantum key exchange over existing fiber infrastructures in co-existence with classical (conventional) data channels operated at usual power levels. To realize a QKD network utilizing the co-existence scheme, methods for filtering and switching of quantum signals have to be further evaluated. In this paper particularly, the influence of Raman scattering on a quantum channel allocated in the O-band (around 1.3 µm) has been investigated and the expectable performance of QKD systems integrated in metropolitan area networks evaluated considering the essential bypassing of in-line amplifiers and conventional network nodes.

The simulation study based on parameters obtained by measurements on a DWDM system operated at default power levels proved that a QKD reach up to 30 km is achievable without a change of the DWDM system's operation parameters. However, the secret key rate achievable at such distances is rather low. For shorter distances, such as 10 km, the secret key can be exchanged at rates of several kbit/s.

ACKNOWLEDGEMENTS

This work was supported in part by the project "QKD-Telco: Practical Quantum Key Distribution over Telecom Infrastructures" (contract No. 835926), within the FIT-IT programme funded by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT) in coordination with the Austrian Research Promotion Agency (FFG).

REFERENCES

[1] ETSI, "Quantum key distribution (QKD): components and internal interfaces," ETSI Industry Specification (ISG) Group Quantum Key Distribution, Tech. Rep., 2010.

[2] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New Journal of Physics, vol. 12, no. 6, p. 063027, 2010.

[3] K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, and A. J. Shields "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Physical Review X*, vol. 2, p.041010, 2012.

[4] A. Poppe, B. Schrenk, F. Hipp, M. Peev, S. Aleksic, G. Franzl, A. Ciurana and V. Martin, „Integration of Quantum Key Distribution in Metropolitan Area Networks", in Proceedings of the 2014 OSA Optics & Photonics Research in Optical Sciences Congress, Quantum Information and Measurement, Berlin, Germany, March, 2014, pp. 1 - 3.

[5] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk and F. Hipp, „Quantum Key Distribution over Optical Access Networks", 18th European Conference on Networks and Optical Communications (NOC 2013), June 2013, pp. 11-18.

[6] R. J. Runser, et al., "Progress toward quantum communications networks: opportunities and challenges," *Optoelectronic Integrated Circuits IX*, vol. 6476, p. 6476OI, 2007.

[7] P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," in *Electronics Letters*, vol. 33, no. 3, 1996.

[8] S. Aleksic, D. Winkler, A. Poppe, G. Franzl, B. Schrenk and F. Hipp, „Distribution of quantum keys in optical transparent networks: issues and challenges", 15th International Conference on Transparent Optical Networks (ICTON 2013), IEEE; Cartagena, Spain, June 23-27, 2013, paper We.B1.3.