DEPLOYING QKD IN STANDARD OPTICAL NETWORKS

D. Lancho[1], J. Martinez-Mateo[1], D. Elkouss[1], A. Ciurana[1], M. Soto[2] and V. Martin[1]*
[1] *Facultad de Informática, Universidad Politécnica de Madrid, Campus de Montegancedo, Madrid 28660, Spain*
[2] *Depto. Seguridad en Redes y Servicios, Telefónica Investigación y Desarrollo, Emilio Vargas 6, Madrid 28043, Spain.*

Introduction: QKD is a promising technology. It provides a mechanism to grow symmetric keys safe from any hypothetical algorithmic weaknesses in the form of unproven computational complexity. Long term secrecy, backward and forward security or even the fact that is a fundamentally different paradigm are desirable characteristics. However, its practical implementation is rather cumbersome, requiring the manipulation of extremely weak signals traveling through noise-free quantum channels that couple emitters and receivers in pairs. In order to deploy QKD in a cost effective and scalable way, its integration with already installed optical networks is a logical step. If, for the sake of security, we require that no intermediate trusted nodes would be needed, the maximum distance/absorptions allowed by QKD systems, limit ourselves to metropolitan area networks. Current metro networks are mostly all optical and passive, hence a transparent link can be established among any two points and this link can be used to transport the quantum channel. The purpose of the present communication is to report on our findings studying the problems arising when integrating QKD systems in standard telecommunications networks.

Network Testbed and Results: The testbed setup is depicted in Fig. 1. Enclosed in dashed line is the core part and in dotted line, the access. The core has a ring topology and the access is of the GPON type, although DWDM-PON studies are under way. QKD equipments are id Quantique Clavis 3000 and 3100 two way systems using BB84. Mean photon number was set to simulate a decoy state protocol with signal plus one decoy. The optimal mean number for our setup was 0.79. A full protocol stack, including specifically designed LDPC error correction codes with 1.05 efficiency and privacy amplification was used. The core testbed uses CWDM technology and is composed of three standard ROADMS. Two wavelengths, 1510 and 1470 nm are used for classical signals, while 1550 is reserved for the quantum channel. Beyond power management, extra filtering to further isolate the quantum channel was needed and standard DWDM 50 GHz (0.4 nm) filters were used. Losses in this scenario, without the fiber are 8 dB.

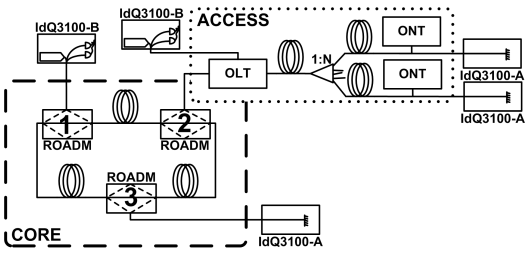

Fig. 1: Network testbed scheme.

The access network uses the GPON standard. In this experiment, a continuous data flux was established among the OLT (core side) and ONT (client side) using the 1490 nm (downstream) and 1310 nm (upstream) channels. Again, QKD used the 1550 nm channel. In this set up, the launch power is fixed and only a small attenuation can be introduced in the OLT. The filtering used was the same (50 GHz) and the splitting factor was four. Losses without fiber are 9 dB.

Other experiments that we will be reporting include to multiplex several quantum channels on the same fiber and the crossing of the core plus the access network in just one jump, both without classical channels.

The top part of Fig. 2 shows the results for the core. Extrapolated data to a 5.6 GHz filtering scheme are included. QBER (left scale) and key rate (right) are presented as a function of the fiber length connecting ROADM nodes 1 and 2, an almost worst case configuration for QKD. The net key throughput is greatly enhanced using the narrower filter, more markedly at the higher distances because the Raman scattering reaching the detectors is still increasing with distance for that fiber length.

The bottom part of Fig. 2 presents the results for the access network. QBER and key rate is presented as a function of fiber length connecting the OLT with the splitter, again an almost worst case configuration for QKD. In this scenario, the narrower filter is more important because of the unattenuated upstream classical channel. In both scenarios a secure key throughput of over 100 bits/sec. is achievable at the longest distances. This is able to sustain an AES256 with a key change rate higher than is usual today and supports the view that the integration of QKD in modern optical networks, although not free from problems, is a real possibility.

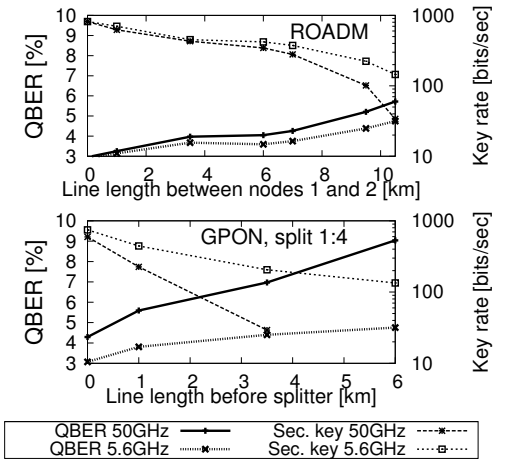

Fig. 2: Core and access network results.

*vicente@fi.upm.es