QUANTUM KEY DISTRIBUTION IN OPTICAL NETWORKS

Francesco Matera
Fondazione Ugo Bordoni, via del Policlinico 147, 00161, Rome, Italy, fmatera@fub.it

This paper reports an investigation about the incorporation of Quantum Key Distribution systems into existing telecommunications infrastructures, analysing the solutions and performance in each network segment to define safe end-to-end physical paths compatible with the 5G slicing concept.
Keywords: QKD, WDM, Access, FSO

1. Introduction

Technology innovation is bringing quantum computing out of laboratories towards the real word. Quantum computing could make current cryptographic algorithms obsolete, putting data and communication protection at risk, leading to a speed up of the adoption of quantum-safe technologies, especially to protect critical data and infrastructures.
It is widely recognized that is paramount to start thinking about future-proof security infrastructures and developing a quantum risk managemnt plan now. Currently Quantum Key Distribution (QKD) is recognized as one of the most important quantum safe communication approach [1-2], and it adoptes a Quantum Photon channel to encrypt the information.
QKD systems are already operating in several contests [1], connecting places over long distances in P2P configurations. However for its complete introduction, in all the telecommunication networks, from the access to the core, several technological steps are still necessary and several problems must be solved.

2. Overview of QKD operating in existing networks

QKD exploits a quantum channel only to produce and distribute keys to encrypt (and decrypt) a message exchanged on a standard communication classical channel, not to transmit any message data. Unbreakable key distribution to strengthen existing network communications is based on the laws of physics, not mathematics. QKD systems are now commercially available and point-to-point QKD links are already operating in several cities and standardization is under investigation in ITU and ETSI (ETSI ISG-QKD) organisms.
Such systems operate with very low power, and therefore any source of loss and noise (classical and quantum) strongly degrades their performance.
Currently the bit rate permitted by QKD is extremely lower than conventional optical transmission systems and therefore many efforts are necessary to increase the transmission speed, but also the maximum propagation distance and making QKD systems low cost, compact and robust.
QKD systems have been shown to coexist with intense data traffic in the same fibre [1-2], thus eliminating the need for dark fibres that are not only expensive but also often unavailable. Therefore QKD-over-WDM backbone has become a promising and feasible solution for future quantum secure networks, even though precautions must be taken into account to limit the degradations due to optical noise contributions (ASE, nonlinear effects,…).

Access network architectures based on optical propagation can exploit the QKD properties and in this contest Gigabit Passive Optical Networks (GPON) appear as much appealing, even though the splitter losses reduce the number of QKD users.
QKD over Free Space Optics (FSO) is another way to exploit optical propagation for quantum security avoiding fiber installation and therefore this approach results much important for QKD introduction both in the access and backhaul segment.

3. Network infrastructures based on QKD

Based on these brief considerations, Fig. 1 illustrates a complete network including QKD systems operating from the core to the access, up to the radio access antenna.

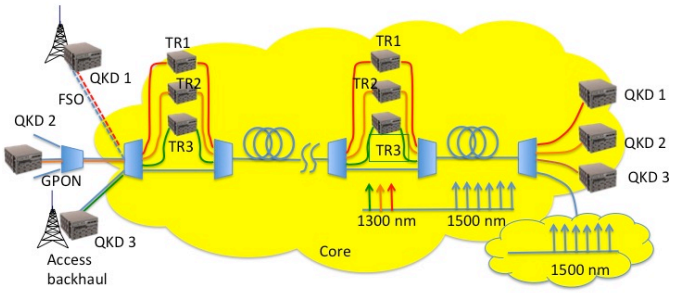

Fig. 1: Wide Geographical Area network operating with QKD communications. TR Trusted Repeater

At the core level, considering that quantum repeaters are beyond current technology, at the moment one interesting solution to transmit QKD signals over long and very long distances is based on the introduction of *trusted repeaters* [1] adopting a propagation of QKD channels in the fiber spectrum not used for conventional channels (1300 nm); at each amplifier spacing optical filters separate the QKD channels to be processed by means of trusted repeaters. Optical filters can be also be used in GPON architectures to reduce the limitations due to splitter losses.
In this paper, for each network segment, we describe the technical issues for the adoption of a quantum security based on QKD in optical networks, evaluating the capacity versus network sizes, and analyzing the compatibility with the novel architectures designed for 5G infrastructures, defining a *Quantum Slice,* and operating with software defined network approaches.

References

1. E. Diamanti et al, "Practical challenges in quantum key distribution" Nature Partner Journal 2016, 2.
2. Y. Cao et al, J. Opt. Comm. Netw. 2019, 11 n. 6