Quantum-Aware Software Defined Networks

A. Aguado[1], V. Martin[2], D. Lopez[3], M.Peev[4], J. Martinez-Mateo[2], J.L. Rosales[2],
F. de la Iglesia[3], M. Gomez[3], E. Hugues-Salas[1], A. Lord[5], R. Nejabati[1] and D. Simeonidou[1]
[1]High Performance Networks, University of Bristol, Woodland Road, Bristol BS8 1UB. UK
[2]Center for Computational Simulation - UPM. Campus de Montegancedo. Boadilla del Monte, 28660 Madrid. Spain
[3]Telefónica Investigación y Desarrollo, Ronda de la Comunicación s/n 28050 Madrid. Spain
[4]Huawei Technologies Duesseldorf GmbH, Riesstrasse 25, 80992 Munchen. Germany
[5] Optical Research Unit, British Telecom, UK
(a.aguado@bristol.ac.uk, vicente@fi.upm.es, diego.r.lopez@telefonica.com, momtchil.peev@huawei.com)

ABSTRACT.— Software Defined Networks (SDN) represent a major paradigm change in communications networks. It provides a level of abstraction and independence from the traditional networking practice that allows for a fast path of innovation, opening new opportunities for Quantum Key Distribution (QKD) networks. In this contribution we explore the implications of this paradigm for the deployment of QKD in practice from the point of view of telecommunications' providers, network equipment manufacturers and applied research and development. We propose a generic quantum-aware SDN architecture and two applications, a generic end to end encryption one and other for the network infrastructure itself.

Statement of the problem.— Quantum Key Distribution is a difficult technology. Beyond its intrinsic point to point nature, the creation, transmission and detection of quantum signals impose very stringent requirements on the physical implementation. Its difficulty increases in the case of QKD networks (NW), where new requirements, such as addressability, physical media sharing between classical and quantum channels or the use of common infrastructure come into play. Although its limits and restrictions are reasonably well understood, a full integration of QKD in a telecommunication NW is still an open problem. Either switched or trusted node NW currently rely in propietary equipment that need to be modified to support a quantum channel. No manufacturer is going to invest heavily in modifications that have yet to prove its commercial success.

SDN Networks.— Software Defined Networks separate the control and data planes. Fig. 1 shows the canonical diagram of SDN networks. The key point is that this decoupling allows for a rapid evolution of the NW, opening the infrastructure to new devices that can interact between them and the control plane through SW and open interfaces.

The control plane provides a set of APIs to applications managing network behavior and services, or to end-user applications willing to use and shape the services they require from the NW.

The SDN model is currently being widely and quickly adopted in communications networks. Having a software-based centralized control of network state has many advantages for QKD: The quantum layer is made explicit to the control plane. The entry point for manufacturers is unique; the controller manages requirements and interactions taking into account its capabilities. Keys can be used directly to secure the control plane. The controller runs in a trusted environment that facilitates the creation of trusted node NW. Reduced CAPEX through incremental deployment and sharing of quantum capabilities. Hybrid usage of quantum and conventional crypto...

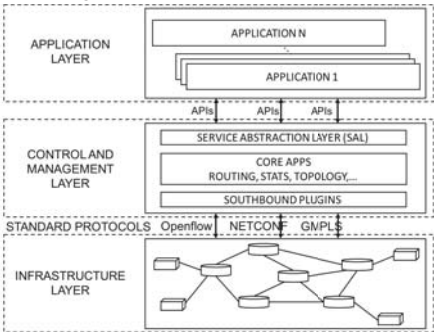

Fig. 1. Structure of an SDN network depicting the three layers: infrastructure, control/management and application. The QKD devices are installed within the infrastructure layer. A control/management layer oversees the infrastructure using a common set of open protocols. From a QKD perspective this decoupling allows to develop a true integration of QKD in networks: neither the devices are required to comply with the requirements of other, classical, appliances nor classical appliances have to be necessarily aware of quantum devices. Their functionality and coordination is managed in software by the upper layer depending on the functionality exposed by the devices in the infrastructure layer.

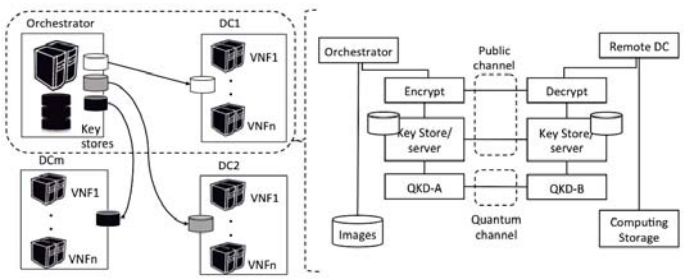

Fig. 2. Architecture for the Network Function Virtualization use case. A NFV orchestrator, the manager of virtualized images in the network, is connected to several datacenters (DC) with quantum links. The DCs provide the servers and connectivity for the NW services implemented by the VNFs, through end to end encryption. These keys allow to secure the NFV services (e.g. a distributed router), and functions image installation, attestation, etc.

The Network Function Virtualization Case.— An important case is when the NW itself is the user of the QKD keys. Since authentication, forward and backward security are granted in QKD, it can secure the control plane. A supply of symmetric keys is very convenient to secure data plane workloads in specific network paradigms, like in NW function virtualization (NFV). NFV intends the deconstruction of current network appliances (routers, firewalls, etc.) into specific network functions implemented as software images running on a homogenous infrastructure. This adds new problems that can be alleviated by pools of symmetric keys, that also serve the high encryption bandwidth that is needed (e.g.: virtual image distribution, VNF attestation). A scheme of this use case is described in Fig. 2.

SDN Node Architecture.— Bringing quantum encryption awareness and the capability of providing inline encryption into a logically centralized control plane requires a modification of the existing protocols and to develop some necessary extensions, in particular to perform routing and status dissemination that nowadays, depending on the type of network, is performed by different sets of protocols. Fig. 3 shows two integration possibilities of end to end encryption services using QKD.

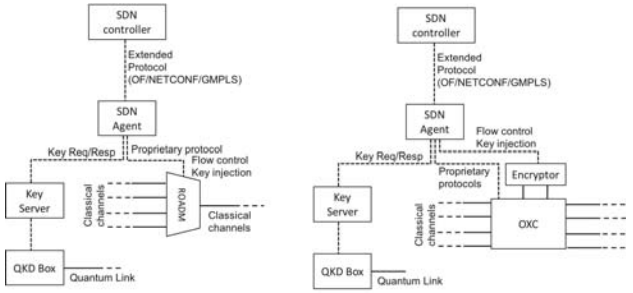

Fig. 3. Two SDN node architecture examples for the end to end encryption using QKD case. Note how the SDN agent is a client to the QKD system, using symmetric keys produced by QKD devices. The upper layers view the infrastructure layer with QKD in the same way that a VPN: all data travelling through the selected classical channels is seamlessly cyphered, without having to work out any ad-hoc compatibility solution.

CONCLUSIONS. A huge effort aiming to standardise different protocols and models for network management is currently underway.

The fundamental point is to make QKD services available to the control plane. For this, extensions allowing the following features are required:

- Features dissemination, in the shape of node capabilities or link reachability information.
- Inline encryption flow configuration. explicit route object structure and management modification.
- Key ID streaming to the control plane.

Note that these extensions have to be also supported from the QKD device side, exporting the appropriate features. Note also that these extensions have impact beyond the network itself since there can be direct security implications. For example, a trusted repeater could be built keeping the actual key inside the QKD device as long as it has the ability to manage two quantum channels. Forwarding managed by the control plane and a database of key IDs would be enough for the key forwarding operation. Actual keys will be only delivered to the applications at the endpoints.

The combination of SDN and QKD technologies is just starting, the definition and development of these protocols will be an enabler for operators to offer and capitalize new encrypted network services powered by QKD technologies and automated from a logically centralized control plane. This will allow for a real convergence of quantum and classical networks very difficult in the old NW paradigms. QKD as we know it today is just the starting point, but the SDN model allows for the evolution and adaptation of other capabilities and devices, like the yet to come quantum repeaters.

ACKNOWLEDGMENTS.— This work has been partially supported by the project CVQuCo, TEC2015-70406-R, funded by the Spanish Ministry of Economy and Competitiveness, QUITEMAD+, S2013-IC2801, funded by Comunidad Autónoma de Madrid and EPSRC EP/M013472/1: UK Quantum Technology Hub for Quantum Communications Technologies.