Aguado, A., Martin, V., Lopez, D., Peev, M., Martinez-Mateo, J., Rosales, J. L., ... Simeonidou, D. (2016). Quantum-Aware Software Defined Networks. In 6th International Conference on Quantum Cryptography (QCRYPT 2016): Washington, DC, September 12-16, 2016. [188] QCrypt.

Peer reviewed version

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 and, specifically, opens 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.**

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. This is difficult already in the typical point to point links over which most of QKD research has been done and it gets worse in the case of QKD networks, where new requirements, such as addressability, physical media sharing between classical and quantum channels or the use of common infrastructure come into play. The last items also imply that now losses and noise in the channel are even more relevant, since the quantum channel has to pass through optical devices that are common in the nowadays prevalent paradigm of passive optical networks. These issues have been studied in many networks and testbeds [1]–[3] but although the limits and restrictions are now reasonably well understood, a full integration of QKD in a telecommunication network is still an open problem.

Two QKD Network architectures have been put forward, one being the switched QKD Network, where uninterrupted and non-amplified, point to point optical paths supporting a quantum channel are created in a passive optical network. This architecture allows for end to end Information Theoretically Secure (ITS) links, but is heavily penalized by the absorptions in the path through the optical components in the network, thus limiting its applicability to metropolitan areas. The other QKD Network architecture paradigm is that of the trusted node (repeater) network, in which the end to end paths cross intermediate nodes where the quantum channel ends and the key material is extracted and used to create node to node secure communication connections. By chaining these with as many trusted nodes as needed, the distance limitation is avoided at the expense of the security of the end to end key material. This is still ITS albeit with the additional assumption that all intermediate nodes are trustworthy. Without quantum repeaters, this is actually the only way to solve the absorption problem and allow quantum key generation that is not limited by distance.

From a practical network perspective, however, neither option is actually a good one. Both architectures pose in practice a problem of running two separate networks in parallel (the classical communication and the QKD one) and not integrating the quantum and classical channels into a single one. In the case of a trusted node network, actually the only real contact point between these two is at the application level, when the keys produced in the quantum network are handled to be used in the classical communication one. A common management can be expected only when, like in a switched network, a physical link (i.e: a strand of fiber) is shared for quantum and classical purposes, but then the management is usually an ad-hoc choice of wavelengths and power such that the noise in the quantum channel is minimized. Otherwise, the QKD and the classical networks can be seen as completely separated ones. This makes a large scale deployment of quantum networks non-practical, since either many devices in an optical network need to be modified (e.g.: quantum aware ROADMs, OLTs, ONTs, switches, etc.) and made mutually compatible, as is the case in classical communications, or a separated quantum network has to be deployed and run in parallel.

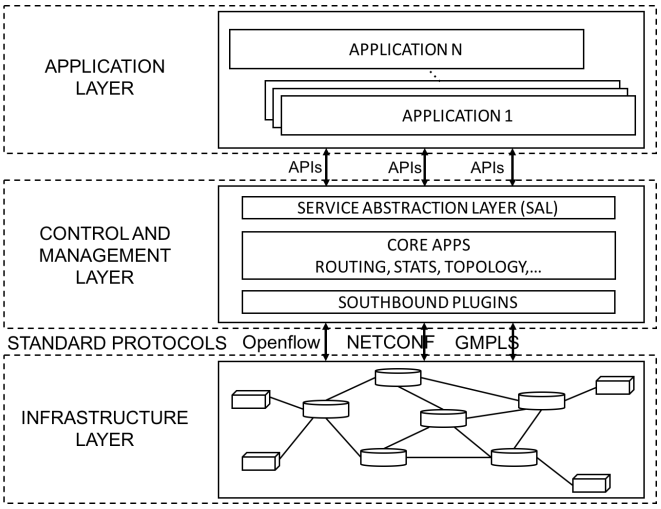

Fig. 1. General structure of an SDN network depicting the three main layers: infrastructure, control/management and application. The QKD devices will be installed within the infrastructure layer. A control/management layer will oversee the infrastructure using a common set of open protocols. From a QKD perspective (and from a more general network evolution 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.

Software Defined Networks separate the control and data planes. Fig. 1 shows the canonical diagram of SDN networks. A lower layer, the data plane, composed of forwarding elements (either sw components or physical devices) is abstracted to the upper layers that control the flow of data (and services) in a centralized way.

This logically centralized control/management plane uses open interfaces to access the elements in the data plane. This 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 network.

The elements in the data plane can also provide control functions beyond pure switching or forwarding, so that a dynamic environment is set up such that a manufacturer can add new functionality and expose it to the controller/manager that, in turn, can easily evolve to accommodate this new functionality. As compared with the traditional approach, where the network configuration and management interfaces are typically proprietary and tied to a specific manufacturer, this represents a revolution that opens the network to potentially disruptive technologies like QKD and quantum technologies in general. More over, the SDN model is currently being widely and quickly adopted in communications networks.

Under this new paradigm of software-based centralized control of network state the integration of QKD is, in principle, much more easy since:

- It can be made explicit to the control plane (i.e: as a new service, on equal footing with many others, either supported natively by the network control protocol or introduced thanks to the protocols extension capabilities) that then can manage its special characteristics in a centralized way for the whole network or part of it.
- The entry point for the manufacturers is unique: it is only the device that they manufacture. There is no need for other network devices to be "quantum-aware". The controller manages the special requirements and their interactions, taken into account their capabilities.
- The specific data that QKD produces -keys- can be managed by the control plane itself (e.g. if it is a "forwarding key" or keys to secure the control plane) or handled to another entity (e.g. a key manager, that is seen as an northbound App from the control plane perspective) transparently.
- From a telecommunication point of view, the controller runs inside a trusted domain (a secured environment from the physical and logical point of view), hence using these nodes as trusted repeaters does not involve an extra security assumption. However, different QoS can be still distinguished (ITS when a direct link is available and ITS with additional trust assumptions when key forwarding is required) and managed accordingly.
- There is no need to deploy a full quantum network. It can be installed in an incremental way without problems. The upfront cost is greatly reduced.
- The quantum part of the network can be upgraded to new technologies when available (e.g. quantum repeaters can be installed instead of forwarding devices) easily and independently of other network devices.
- More optical paths are available, hence opening the possibility to use network coding techniques to increase the security (e.g. several paths have to be compromised at the same time)
- An hybrid usage of quantum and classical crypto techniques can be easily implemented.
- From an operator perspective, the integration of SDN into a QKD network could reduce CAPEX, as the deployment of a QKD pair for each point-to-point (p2p) won't be necessary if a transmitter can be 'time-shared' among different receivers and, therefore, the number of QKD devices could be reduced.

Beyond this, an important case in point is the fact that the network itself can be a user of the QKD keys. The fact that authentication is granted after a first correct installation of a QKD device and that an attacker must be continuously attacking the network after a breach to ensure subsequent key possession (forward and backward security) are desirable characteristics to secure the control plane. A continuous flow of symmetric keys is also very convenient to secure data plane workloads in specific network paradigms, from generic p2p encryption services to the new architectural concept of network function virtualization (NFV), which 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 a new set of problems for the network security that can be alleviated by pools of symmetric keys, which are quite convenient to 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

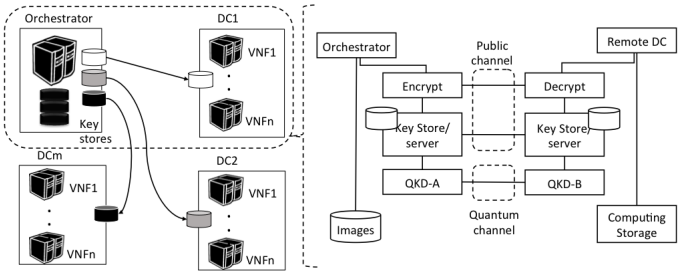

Fig. 2. Architecture for the Network Function Virtualization use case. A NFV orchestrator, the entity that manages all virtualized images in the network, is connected to several datacenters (that provide the servers and connectivity for the network services that will be implemented by the VNFs) through an end to end encryption service. This implies inter-datacenter quantum connectivity to share symmetric keys with the orchestrator. These keys can be used to encrypt and authenticate critical data in the network (e.g. routing tables, firewall information, VNF images...) that would allow various network services (e.g. a distributed router), image installation, attestation, etc.

The usage of SDN technologies to build a unified classical-quantum network will enable more flexibility and reduce the cost of deployment and management of the quantum channels. The combination of these two technologies has to be seen as a mutually beneficial arrangement. Enabling the secure working of the network control plane or a NFV infrastructure, which is a clear advantage to their operation, is possible when a continuous supply of secure key material is available. Simultaneously, QKD can be seen as a new opportunity for the operators and infrastructure providers as it can enable the provision of new, high security encryption end-to-end services. In this context, a network device with quantum capabilities should be able to expose to the control plane, beyond a standard interface and through an open one, these additional characteristics. In our case, those related to QKD are:

- Generate keys to perform symmetric encryption using quantum key distribution.
- Expose key IDs to network controllers and/or applications (northbound interface)
- Perform switching and inline encryption.

Note that we do not consider at this stage of the development the access from the control/management plane to lower level functionality of the QKD card, like specific parameters of the protocol being performed (e.g.: decoy states parameters for a card performing BB84). We are rather assuming that the device brings some intelligence to adapt these when the characteristics of the quantum channel changes (e.g. in the case of the switching). Also, although inline encryption is not strictly required, it is the kind of functionality that is very

convenient to have directly accessible. In any case, note that the versatility of the SDN model makes these interfaces relatively easy to evolve.

Bringing quantum encryption awareness and the capability of providing inline encryption into a logically centralized control plane will require a modification of the existing protocols and to develop some necessary extensions, in particular to perform routing and status dissemination. Note that although the SDN model is being adopted at a very fast pace, there is not yet a unified and standardized set of protocols to solve all problems in the network. Of particular interest to QKD is the routing and status dissemination that nowadays, depending on the type of network, is performed by different set of protocols. In this sense, to start as soon as possible with, at least, a minimal and functional set of modifications enabling quantum aware SDN networks is important to have a real chance. Fig. 3 shows two integration possibilities of end to end encryption services using QKD.

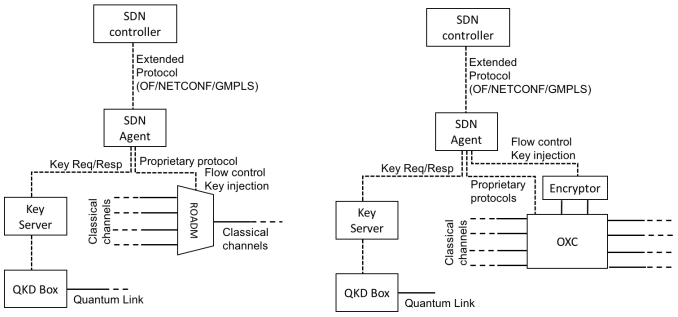

Fig. 3. Two SDN node architecture examples for the end to end encryption using QKD case. Note how the SDN agent is a client to the QKD system, using symmetric keys produced by QKD devices. To the upper layers this allows to view the infrastructure layer with QKD in the same way that a VPN is seen: all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

A huge effort aiming to standardise different protocols and models for network management is currently underway. Some legacy networks are functional using GMPLS as the protocol suite to exchange link reachability information and provide path configuration over the network. Apart from GMPLS, those that we consider more relevant to the QKD case include YANG, that has been pushed as the dominant model for networking, providing an structure than can be used to define NETCONF [4] (xml/rpc-based) interfaces. OpenFlow [5] has also gained a lot of popularity among the SDN community. Even though it was originally defined as a protocol for the packet domain, it is also popular in domains such as optical and wireless and the last versions contains the definition of experimental fields, thus facilitating the extensions to include new capabilities.

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 (rpc-reply to a hello message in NETCONF, features-reply in Openflow) or link reachability information (ISIS, OSPF-TE, BGPLS).
- Inline encryption flow configuration. YANG will require a model definition. Openflow will need flow-mod extension. GMPLS protocols will need explicit route object structure and management modification.
- Key ID streaming to the control plane. Several mechanisms could be implemented here (using rpc-reply in NETCONF, in Openflow barrier synchronization and flow-stats action field extension, and inline injection of the key in the RSVP path message.) or even the inclusion of a key management system.

Note that these extensions have to be also supported from the QKD device side, that has to export the appropriate features. Note also that these extensions can have impact beyond the network itself in the sense that there are also direct security applications. 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 opens the road for a real convergence of quantum and classical networks. 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.

Brief Glossary.

BGPLS : Border Gateway Protocol with Link State (LS) extensions.
GMPLS : General Multiprotocol Label Switching. Encapsulation technique for fast data routing avoiding routing tables.
ISIS : Intermediate System to Intermediate System routing protocol.
NETCONF : Network Configuration Protocol.
NVF : Network Function Virtualization.
OpenFlow : Communications protocol to access the forwarding plane of the network devices (switches, routers...). It is a key SDN enabler.
OSPF-TE: Open Shortest Path First routing protocol for Traffic Engineering. Used to describe the topology of a network.
SDN : Software defined network.
VNF : Virtualized Network Function. Describes an instance of a software image performing a network function in the NVF paradigm.
YANG : Yet Another Next Generation. Data modeling language for NETCONF.

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

References

[1] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, and B. et al., "The SECOQC quantum key distribution network in vienna," *New J. Phys.*, vol. 11, no. 7, p. 075001, July 2009.
[2] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "Qkd in standard optical telecommunications networks," in *Quantum Communication and Quantum Networking*, vol. 36, no. 11, 2010, pp. 142–149.
[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, and T. et al., "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.
[4] E. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network configuration protocol (netconf)," RFC6241, June 2011. [Online]. Available: https://tools.ietf.org/html/rfc6241
[5] M. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, April 2008.