Quantum aware SDN nodes in the Madrid Quantum Network

V. Martin[1], A. Aguado[1], J.P Brito[1], A.L. Sanz[2], P. Salas[2], D. R. López[3],V. López[3], A. Pastor-Perales[3], A. Poppe[4] and M. Peev[4].

[1]*Center for Computational Simulation and ETSI Informáticos, Universidad Politécnica de Madrid 28660 Madrid, Spain*
[2]*Center for Computational Simulation and ETSI Telecomunicación, Universidad Politécnica de Madrid 28660 Madrid, Spain*
[3]*Telefónica Investigación y Desarrollo, Ronda de la Comunicación s/n 28050 Madrid. Spain*
[4]*Huawei Technologies Duesseldorf GmbH, European Research Institute, Riesstrasse 25-C3, 80992 München. Germany*
email: vicente@fi.upm.es

ABSTRACT

QKD technology is mature enough to be used beyond the usual single, point to point, link by creating networks. Quantum ad hoc networks, where a separate, quantum-only network, is running in parallel to a classical network have been demonstrated in several occasions. Having to, essentially, duplicate the network to introduce quantum communications is very expensive and, beyond niche use-cases, fully integrated quantum-classical networks is what the industry demands to accept quantum technologies as a serious networking technology, ready for a broad market uptake.

Recently we have reported on the successful deployment of the Madrid Quantum Network. This network is novel because it has been the first installed in production sites of a Telecommunications operator and moreover it is managed through a Software Defined Networking (SDN) structure that integrates classical and quantum channels. The network was operating for four months and we could demonstrate several technologies utilizing the integration of quantum and classical networks. Here we report on some implementation aspects and its usage in several use cases, in particular to secure the management of the SDN control plane as a critical infrastructure.

Keywords: Quantum communications, software defined networking, cryptography, passive optical networks.

1. INTRODUCTION

Quantum Key Distribution (QKD) is a method for distant key generation employing quantum principles. The latter allow unprecedented security of the generated key material. This is certainly Quantum Safe (i.e. the key generation method cannot be broken by prospective quantum computers) in contrast to the presently used methods (e.g. RSA, Elliptic Curves, etc.) that are embedded in most of the of the protocols used to secure the communications nowadays, and whose security is based on the computational complexity of a mathematical problem. The security of QKD is independent of the computational power of an attacker, therefore it can, in principle, reach the level of Information Theoretic Security (ITS). It is, however, a matter of fact that such an extreme level of key generation security comes at a price. QKD is a physical layer technology and requires the use of single photon-level intensity quantum signals – loosely qubits. It is the unavoidable disturbance that a possible attacker produces in a qubit that guarantees the security of a QKD transmission. However, this also means that amplifiers would destroy these signals and cannot be used. Also, such a delicate signal, means that many pulses are lost or suffer errors -that cannot be differentiated from the action of an attacker- during transmission and that the co-propagation with classical signals, many orders of magnitude stronger, produces noise in the quantum channel. As a result, the total error increases and, beyond some threshold, it is impossible to distill a secret key. Although some promising results with new protocols have demonstrated in the lab to tolerate losses close to 60 dB, is currently not realistic to have a reasonable key rate (at least a few kbps) if channel losses exceed 25 to 30 dB in the field and using non-forbiddingly demanding technology. Since optical fiber losses are about 0.2 dB/km at 1550 nm, this would translate into a maximum distance of about 150 km. In practice, however, losses due to connectors, fiber bending or passive components like splitters, wavelength filters and couplers, AWGs, etc. mean that realistic distances are much lower, although still adequate for metro area networks. There exists the promise of quantum repeaters, which would get rid of the distance/losses limitations but, unfortunately, this is a future technology, yet to be developed.

To reduce these problems, QKD networks have been implemented in the past using a separate infrastructure i.e. dark fiber exclusively used for the qubit transmission, and trusted nodes, where the secret key is extracted and retransmitted. Having to build a parallel infrastructure is very expensive, arguably more costly that the QKD devices themselves, and requires a large up-front investment. This has reduced the appeal of the technology except for some niche applications, and heavily limited its wide-spread adoption. To solve this issue it is essential to share infrastructure, so that adding QKD capabilities to a communications network should be as seamless and straightforward as it is to add standard communications equipment. In this paper we give a short overview of the Madrid Quantum Communications network [1], present its main characteristics and one of its main architectural components, namely the Quantum SDN Node.

2. THE MADRID QUANTUM NETWORK

The main objective of the Madrid Quantum Network [1] was to enable the integration of quantum communications in a telecommunications network, both at the physical and logical level. In order for the technology to be accepted, this is done using tools and schemes that are familiar to the telecommunications industry. In the past, such an integration had not been achieved, deploying instead a network specialised in the quantum part and running in parallel to the standard communications one [2,3,4]. The communication network paradigms prevalent just a few years ago were designed more for capacity and robustness of data transmission, while flexibility and the capacity to offer new services were not the main driving force. Network Softwarization [5] came as a response to the fast evolution of networks that was necessary to support new services. Whereas in the old paradigm, to add a quantum channel required the careful ad-hoc modification, reconfiguration and fine-tuning, step by step, of the existing devices and communications channels, network softwarization, through the use of standard interfaces and programmability allows for a flexible design and evolution. A new device can advertise its capabilities to the network and be properly configured and managed through a logically centralized control scheme. This opens completely new possibilities to integrate quantum communications in telecommunications networks, avoiding large deployment costs and adding these capabilities where they are needed. Moreover, the quick adoption of these techniques among the telco operators, also implies that the integration is done using tools that are already familiar in networks, facilitating the assimilation and deployment of quantum communications and cryptography in the large ecosystem of networks and security infrastructures.

The Madrid Quantum Network, was built around this paradigm, using SDN as a basis to deploy QKD in a telecommunications network and Network Function Virtualization (NFV) to demonstrate relevant use cases. Also, to show real-world capabilities, well beyond lab demonstrations, the network was installed in production facilities of Telefónica of Spain, by using the same deployment protocols that are used to install standard communications equipment. The layout of the network, with distances and losses, is shown in Fig. 1. It was operating continuously during 4 months and currently an enlargement is underway.

Figure 1: The Madrid SDN QKD Network layout installed in Telefónica of Spain production network. The distances and losses between the Points of Presence used are given in the white boxes. The additional losses in some of the links correspond to additional fibre (spool) used to artificially increase the distances in some experiments. Note that losses are much higher than the expected because of the distance, since additional connectors, bending of the fiber and crossing of intermediate PoPs (not shown) have an important impact.

3. IMPLEMENTATION

The QKD systems used were based on Continuous Variables (CV) QKD and designed to be driven from the network [5]. They were provided by Huawei Research Technologies Duesseldorf. CV-QKD systems have the advantage that the detection system is based on homodyne detection and does not require the usual bulky and expensive single photon detectors. This is an important aspect of the implementation, since it naturally opens the possibility of mass production based on extensions of available telecommunications technology, whereas the same is not true when traditional single photon detectors are needed. Also, CV-QKD is more resistant to the noise in the fibre due to co-propagating classical channels. On the other hand, key distillation in the CV case is computationally very costly and the tolerance to losses is more limited. In Madrid, two receivers and one emitter were installed. The emitter could be switched by the SDN controller to communicate with either of the receivers. This basic set up was sufficient to demonstrate several use cases of importance for Telefónica. A scheme, showing also the SDN QKD nodes, is presented in Fig. 2.

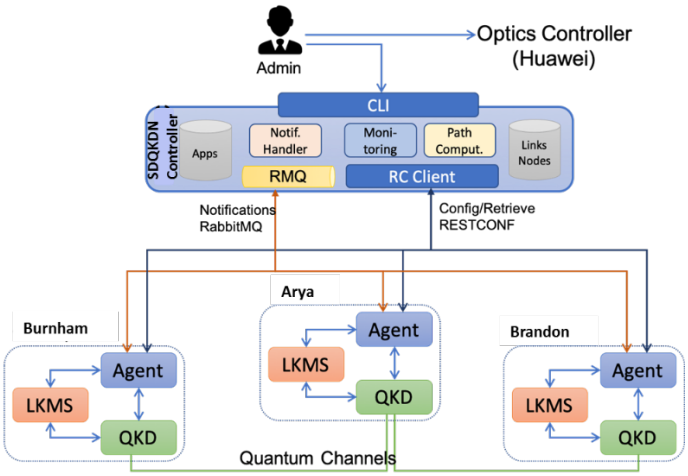

Figure 2: SW structure of the network. A SDN Controller with all the logic to manage the different nodes is connected with the three SDN-QKD Nodes. Arya is the emitter, while Brandon and Burnham are the receivers. Each node has an SDN Agent that collects the node info and statistics from the secret key management subsystem (Local Key Management System – LKMS) and the QKD device itself. The agent also acts as a single entry point for the SDN controller that knows the whole state of the network (e.g. Apps and Links information) and can optimize the behaviour of both, the classical and quantum part of the network, at the same time.

Each node connects the QKD system to the optical network using standard optical equipment (in this case, Huawei OSN-1800) that is also equipped with a link encryptor that can use the keys provided by a QKD system. In fact, our protocols allow to use the standard Diffie-Hellman symmetric key negotiation together with the key obtained by the QKD by X-ORing them. This keeps the standard level of security and complements it with QKD, preparing for a quantum-safe infrastructure that is also compliant with current security practice.

The SDN controller can gather information from each SDN-QKD node and set the optical connections appropriate to serve the application requests in the different nodes. Note that the applications obtain the keys from the corresponding LKMS and that the SDN controller is not used as a storage of key material. This structure allows a QKD device to advertise its capabilities and to the SDN controller to learn what is available and what the status of the network is, such that its logic can optimize the joint usage of the quantum and classical segments of the network. In Fig. 3 sample messages from the controller to gather information from a SDN-QKD node and to set an appropriate link among two network nodes are shown.

Note that the interfaces to perform these actions, including the information models, have to be fixed and standardized. The control interface between the SDN controller and the SDN-QKD agent in this network has been proposed for standardization at ETSI (European Telecommunications Standards Institute). Other interfaces between the different elements of the SDN-QKD node have also been standardized [6].

```
GET /restconf/data/etsi-qkdn:sdqkd_node HTTP/1.1
Host: example.com
Accept: application/yang-data+json

{
"sdqkd_node": {
    "location_id": "Almagro",
    "node_id": "F0EFF695-C54C-47B8-A4E4-0F14980D2547",
    "qkd_capabilities": {
        "application_stats_support": "True",
        "key_relay_mode_enable": "True",
        "link_stats_support": "True"
    }
}
```

```
POST /restconf/data/etsi-qkdn:sdqkd_node/qkd_links HTTP/1.1
Host: example.com
Accept: application/yang-data+json

{
"etsi-qkdn:qkd_link": [
    {
        "enable": "True",
        "link_id": "166567E0-F251-4944-8C7F-64CD0B678F37",
        "local": {
            "interface": "1",
            "qkd_node": "51447CE8-06A3-4BD8-9AD4-8189FE10C7E0"
        },
        "remote": {
            "interface": "1",
            "qkd_node": "AA7EEA2D-93DE-4AAA-98F2-AEF4A81F99F0"
        },
        "type": "Physical",
        "wavelength": "1550"
    }
]
}
```

Figure 3: Sample messages from the quantum-enabled SDN controller to an SDN-QKD node. On the left a Restconf message is sent to collect basic information about the SDN-QKD node. On the right, another one is sent to set a physical link between two of the nodes.

Using these structures, we have implemented several use cases that are mainly relevant to a telecommunications company. Note that network softwarization increases the flexibility, but also introduces new security problems, that QKD can mitigate. As such, these techniques are not only enablers of quantum communications in telco networks, but are also consumers of their services. An interesting point here is that network softwarization requires that the PoPs were the SW instances and apps are running must be secure locations. This means that the co-location of trusted QKD-nodes in these points keeps additional trusted locations at a minimum. In certain cases, the limited reach problem of QKD devices can be solved without additional trusted locations.

The implemented use cases cover the security of the SDN control plane, the security of the data plane -where we are not limited to the typical ITS One Time Pad encryption, but have optimized for high throughput by using the OSN-1800 AES line cards with a fast key renewal rate through the QKD devices. The security of NFV services, by instantiating several VPNs in the different locations and linking them through a modified IPsec protocol that, on top of a Diffie-Hellman key exchange makes an XOR with a QKD key [7,8]. We have also been experimenting with new protocols for network attestation, in particular an Ordered Proof of Transit protocol based on QKD keys [9].

Most importantly, note that although these use cases are geared towards the telco operator, once there is a flow of high quality secret key in a network, it is straightforward to use these as a service for any user application that needs an extra, quantum-safe, security layer. In this case, the final user would maintain its security mechanisms and policies, and the telco can transparently cypher all the user's traffic, such that if it is captured on transit, the QKD layer must be also broken in addition to the user's security layer.

As an additional feature, we have populated the available OSN channels with classical communications in order to test the co-propagation of classical and quantum communications in the same fibre. The co-propagation was tested up to the maximum number of free slots in the set-up (17 classical channels using 10 and 100 Gbps transceivers in the same C-band). While the power of the classical channels needed to be reduced, this was done so that the classical BER did not increase. The QKD CV scheme operated very robustly, with an uninterrupted quantum transmission and demonstrating the potential of up to 17 Tbps of classical data co-propagation.

4. CONCLUSIONS

With the deployment of a SDN-based QKD network in production facilities, the Madrid Quantum Network has demonstrated the possibility of converging quantum-classical communications infrastructure in real world settings. While the coexistence of both technologies is bound to have limits, it is more flexible than previously thought when using the appropriate technology. This contributes to reducing the barriers to the broad adoption of QKD as a valuable addition to the tools used to secure the communications and the infrastructure itself and paves the way for future product-level implementations of the technology.

ACKNOWLEDGEMENTS

Supported by FET QT-Flagship, EU H2020 grant agreement 820466 CiViQ: Continuous Variable Quantum Communications, and the Spanish Ministry of Economy MINECO/FEDER, CVQuCo, TEC2015-70406-R

REFERENCES

[1] A. Aguado *et al.*: *The Engineering of an SDN Quantum Key distribution Network*. IEEE Comms. Mag. Jul. 2019 (Special issue *"The Future of Internet"* DOI: 10.1109/MCOM.2019.1800763 ArXiV: 1907.00174
[2] M. Peev *et al.*: *SECOQC*, New Journal of Physics **11** 075001 (2009).
[3] M. Sasaki *et al.*: *The Tokyo QKD network*, Optics Express, **19**, 10387 (2011).
[4] A. Ciurana *et al.*: *Quantum metropolitan optical network based on wavelength division multiplexing*. Opt. Express, 22(2):1576 (2014) doi:10.1364/OE.22.001576.
[5] H. H. Brunner *et al.*: *"A low-complexity heterodyne CV-QKD architecture"* in ICTON 2017. IEEE, Jul. 2017.
[6] P. Brito *et al*.: *"Quantum services architecture in softwarized infrastructures"*. ICTON 2019. IEEE - See this same issue.
[7] A. Aguado, *et al.*: "*Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks"*, in JOCN **9**, 819-825 (2017).
[8] A. Aguado, *et al.*: "*Quantum Technologies in Support for 5G services: Ordered Proof-of-Transit*", Accepted: ECOC 2019.
[9] A. Aguado, *et al.*: "VNF Deployment and Service Automation to Provide End-to-End Quantum Encryption," JOCN **10**, 421 (2018).