Quantum services architecture in softwarized infrastructures

J. P. Brito[1], D. R. López[3], A. Aguado[1], C. Abellán[4], V. López[3], A. Pastor-Perales[3], F. de la Iglesia[3], and V. Martín[1]

[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]Quside Technologies S.L., Castelldefels 08860 Barcelona, Spain
email: juanpedro.brito@upm.es

ABSTRACT

Quantum computing is posing new threats on our security infrastructure. This has triggered a new research field on quantum-safe methods, and those that rely on the application of quantum principles are commonly referred as quantum cryptography. The most mature development in the field of quantum cryptography is called Quantum Key Distribution (QKD). QKD is a key exchange primitive that can replace existing mechanisms that can become obsolete in the near future. Although QKD has reached a high level of maturity, there is still a long path for a mass market implementation. QKD shall overcome issues such as miniaturization, network integration and the reduction of production costs to make the technology affordable. In this direction, we foresee that QKD systems will evolve following the same path as other networking technologies, where systems will run on specific network cards, integrable in commodity chassis. This work describes part of our activity in the EU H2020 project CiViQ in which quantum technologies, as QKD systems or quantum random number generators (QRNG), will become a single network element that we define as Quantum Switch. This allows for quantum resources (keys or random numbers) to be provided as a service, while the different components are integrated to cooperate for providing the most random and secure bit streams. Furthermore, with the purpose of making our proposal closer to current networking technology, this work also proposes an abstraction logic for making our Quantum Switch suitable to become part of software-defined networking (SDN) architectures. The model fits in the architecture of the SDN quantum node architecture, that is being under standardization by the European Telecommunications Standards Institute. It permits to operate an entire quantum network using a logically centralized SDN controller, and quantum switches to generate and to forward key material and random numbers across the entire network. This scheme, demonstrated for the first time at the Madrid Quantum Network, will allow for a faster and seamless integration of quantum technologies in the telecommunications infrastructure.

Keywords: Quantum key distribution; Service automation; Software-defined networking; Open Interfaces.

1. INTRODUCTION

Typical network infrastructure is complex and difficult to manage. It usually comprises various types of network elements, such as routers, switches, firewalls, etc. that are usually managed through proprietary solutions. Under these conditions, adding new services could require much time and effort, if it is possible at all without changing the hardware itself.

The rapid evolution of applications and services needs flexible networks that can cope with this dynamicity, being able to integrate new services in an agile and easy way. In that sense, different software paradigms have emerged, where certain functions, actions, and operations that used to run internally in a network device in the past model, are now abstracted and executed as software processes.

One of these novel network paradigms is Network Function Virtualization (NFV). This technology employs IT virtualization technology, where the functionality or services of the network are separated from the capacity of the network. Operators can orchestrate networks by deploying virtual functions onto standard hardware appliances, without the need for upgrading the network with new dedicated equipment.

Another new paradigm is known as Software Defined Networking (SDN) [1]. This approximation allows software developers to control network resources in the same simple way as ordinary computing resources [3]. The key element to support this programmability freedom is the decoupling of the control plane (control/management protocols and actions) from the data plane (forwarding), using open interfaces between a centralized controller and packet forwarding devices. This separation allows dynamic management of infrastructure and network services, for example, new services to increase the network security.

Quantum key distribution (QKD) technologies [2,3] exploits quantum mechanics to allow the generation of synchronized keys (random bits) between two separated parties. One of the strongest points of this technology is

that it is Information Theoretically Secure (ITS), which means that the maximum information leaked out of these parties can be upper-bounded, independently of the computational power available to the attacker. The security of the QKD-produced keys relies on the physical layer and, therefore, this security method is immune to any computing-based cryptanalysis algorithm.

Although QKD technology has a high level of maturity, in many cases QKD devices are highly experimental and their Technology Readiness Level is not enough for mass market production. Different vendors follow different approaches in the design of their devices, making the integration on real networks a really complex task, especially when these systems must communicate in a vendor independent manner, providing a secure end-to-end (E2E) QKD service in a transparent way.

To ease the integration of QKD as a service, we propose a single network element that we define as Quantum Switch. This highly customizable SDN element is based on open interfaces and protocols that transform any QKD device or a set of them into a network element. This element is what we refer as SD-QKD node, which has a very simple interface able to establish the Quality of Service (QoS). This approximation allows quantum resources (keys or random numbers) to be provided as a service, integrating a set of different cooperative software components to provide secure bit streams.

2. QUANTUM SWITCH

The Quantum Switch network element allows quantum resources to be provided as a service. At this moment, the design is focused on QKD services, because is the most mature field of quantum communications, but it is easily extensible to other Quantum services in the future, for example QRNG. The Quantum Switch is based on the SDN principles, with which we increase the network elasticity and heterogeneity, allowing, for example, the seamless integration of new QKD systems and the dynamic routing of QKD keys.

The integration of QKD as a service in production networks requires basically two entry points. On the one hand, an interface that allows to obtain Keys from the QKD devices, that we solve through the use of a simple API capable of establish sessions with an associated QoS. On the other hand, how to control all the necessary resources (quantum or classical channels for key generation/delivery, incoming applications, etc.) and all the necessary logic to accomplish a QKD network. We have solved this with a model-driven central controller that communicates with the SD-QKD node using standard protocols.

2.1 Application Interface

The Application Interface describes a minimal interface to provide Keys to the application that request the QKD service. Note that applications that call this API do it within the user's local security perimeter. With this API, manufacturers shall supply and implement function calls when a QKD service is present in the network infrastructure. This API could be combined with other manufacturers API that may provide additional and expanded functionality. The Application Interface is designed to be simple yet powerful. It is formed by three functions with a minimal set of parameters on each call as you can see in Figure 1.

```
Interface QKD{
        OPEN_CONNECT (in source, in destination, in QoS, in-out Key_stream_ID, out status);
        GET_KEY (in Key_stream_ID, in-out index, out Key_buffer, out status);
        CLOSE (in Key_stream_ID, out status);
}
```

Figure 1. Application Interface. (ETSI QKD-ISG 004 AppInt)

Here we present the details of the Application Interface:

- **OPEN_CONNECT:** Generate a Key_stream_ID (an association for a set of future keys) and its associated resources at both E2E QKD link and establish a set of parameters that define the expected levels of key service (QoS). This function is autoblocking until both peers are identified
- **GET_KEY:** Obtain the required amount of key material requested for this Key_stream_ID. Each call shall return the fixed amount of requested keys or an error message if it failed. Together with the requested key, the QKD Local Key Manager System (a system in charge of all generated keys) shall return a unique index for each chunk -of predefined length- of retrieved key, so that they are univocally determined. Other characteristics of this process (e.g. maximum size, jitter) is set through the QoS parameters.

- **CLOSE:** This terminates the association established for this Key_stream_ID, and no further keys will be associated to it.

2.2 QKD Control Interface for Software Defined Networks

The QKD Control Interface defines the management interface for one or multiple QKD systems placed in a secure area connected to a SDN controller. This interface is based on a YANG model, designed to be the base for the integration of QKD technologies in softwarized networks. Still, the nature of this model is to be open, so further extensions can be incrementally integrated, especially with experimental purposes or to cope with special characteristics that are relevant to a certain QKD implementation. YANG models also offer the possibility to use any of the well-accepted network management protocols used in SDN architectures, such as NETCONF, RESTCONF or recently gNMI.

Through this open interface, the architectural design, shown in Figure 2, allows a central controller to orchestrate the QKD resources to optimize the key allocation per link. This is done by automating the creation of physical QKD channels and of virtual (multi-hop-based) QKD links and having a network wide visibility. The connection between node and controller allows retrieving information from the QKD domain and dynamically and remotely configuring the behaviour of the QKD systems to create, remove or update key associations between remote secure locations.

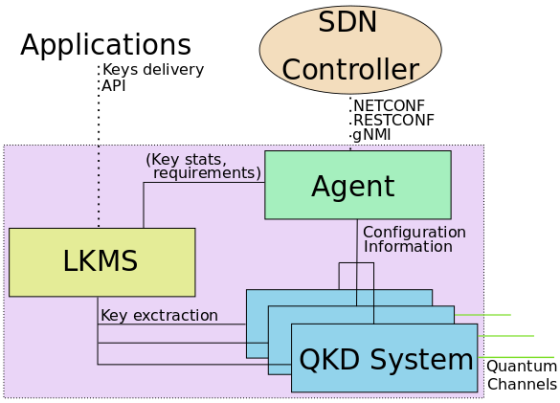

Figure 2. Main logical components of SD-QKD node.

The components of the SD-QKD architecture are the controller and the SD-QKD node. The SD-QKD node has also several internal components (the apps themselves, the LKMS, the SDN Agent and the Quantum services, like a QKD system or a QRNG):

- **Controller:** It has all the information of the Network topology, features and states of the devices and it has the ability to modify any component of the network dynamically. It is in charge of the control plane and is logically regarded as the core of the network intelligence. The communication with the Quantum Switch is done through open interfaces based on YANG models.
- **App:** It makes use of the Application Interface proposed on section 2.1 and it is in charge of the key consuming, encrypt the data and send it through the classical channel.
- **LKMS:** The Local Key Management System is the place where the keys are stored and prepared to be used. This component not only store and serve keys, but is also in charge of the key-relay between multi-hop links.
- **Agent**: The agent is the connection point between the controller, LKMS and the QKD Systems. The communication with the controller is made through standard protocols (Eg. NETCONF) using the proposed YANG models, for example when an App (through the LKMS) makes a request for Key. The Agent acts as an adaptation layer to communicate with the QKD Systems, adapting the data structures sent by the controller to the QKD System requirements.
- **QKD System:** The physical quantum devices that are continuously generating keys

The proposed model, combined with the YANG-based interfaces provides an abstracted view of the QKD domain. It can abstract the QKD systems within a secure location as interfaces of a network element, simulating a building-block with QKD capacities. This network element, the SD-QKD node, is able to communicate with its neighbours and with the central controller to create end-to-end services. This makes the introduction of our proposal for an SDN-enabled QKD networks completely transparent to any upper layer service.

3. USE CASE: MADRID QUANTUM NETWORK

This proposal has been successfully implemented in the Madrid Quantum Network [4, 5] at a physical and a logical level, showing the integration potential of quantum communications (QKD) in a real telecommunications environment. The network was also used in combination with traditional carrier use cases, from traditional end-to-end security, to next-generation NFV-based services.

The Madrid Quantum Network shows the application of the Open Switch into real world capabilities, specifically in production facilities of Telefónica of Spain, and using the same protocols than the ones used to install standard communications equipment. The Madrid Quantum Network was running continuously during 4 months and is currently being enlarged.

4. STANDARIZATION

Both, the Application Interface and QKD Control Interface for Software Defined Networks are the subject of standardization by the European Telecommunications Standards Institute, under the Industry Specification Groups 004 and 015 respectively. They permit to operate an entire quantum network using a logically centralized SDN controller and Quantum Switches to generate and to forward key material and random numbers across the entire network, while providing a standard way for applications to access QKD-derived keys.

5. CONCLUSIONS

QKD is one of the most active research areas in Quantum Communications, that can be seen as a physical layer to secure current network infrastructures. The highly experimental and prototypical nature of the QKD devices, focused in single point-to-point links, does not fit well with current networks. Nevertheless, we demonstrate that it is possible to integrate these new technologies into real production network using our approximation for SDN-enabled QKD systems abstracted as a single network element, the Quantum Switch, that is completely technology and vendor independent and hide the low level details of the devices through the use of standard interfaces and protocols, easing the integration of QKD services into real networks. We demonstrate that 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. This approximation has been tested in the Madrid Quantum Network allowing a faster and seamless integration of quantum technologies in real telecommunications infrastructure, through the use of standard interfaces and the programmability freedom offered by SDN. The adoption of these techniques into the telco infrastructures implies that the integration of new (quantum) services must be done using tools already available in softwarized networks.

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. QUITEMAD: Comunidad de Madrid P2018/TCS-4342,

REFERENCES

[1] N. McKeown *et al.*: *OpenFlow: enabling innovation in campus networks*, SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Mar. 2008.

[2] N. Gisin *et al.*: *Quantum cryptography*, Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, Mar. 2002.

[3] V. Martin *et al.*: *Quantum key distribution, introduction*, in Wiley Encyclopedia of Electrical and Electronics Engineering, Wiley, 2017, pp. 1–17.

[4] 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 .

[5] V. Martín et al.: "Quantum aware SDN nodes in the Madrid Quantum Network". ICTON 2019. IEEE - See this same issue.