Increasing network reliability by securing SDN communication with QKD

Paolo Comi
Innovation Lab and Research
Italtel S.p.A
Milan, Italy
paolomaria.comi@italtel.com

Paolo Martelli
Dipartimento di Elettronica
Informazione e Bioingegneria
Politecnico di Milano
Milan, Italy
paolo.martelli@polimi.it

Vicente Martin
Center for Computational Simulation
and Dept. LSIIS
Universidad Politécnica de Madrid
Madrid, Spain
vicente@fi.upm.es

Juan P. Brito
Center for Computational Simulation
and Dept LSIIS
Universidad Politécnica de Madrid
Madrid, Spain
juanpedro.brito@upm.es

Alberto Gatto
Dipartimento di Elettronica
Informazione e Bioingegneria
Politecnico di Milano
Milan, Italy
alberto.gatto@polimi.it

Rubén B. Méndez
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
ruben.bmendez@upm.es

Rafa J. Vicente
Center for Computational Simulation
Universidad Politécnica de Madrid
Madrid, Spain
rafaelj.vicente@upm.es

Fabrizio Bianchi
Innovation Lab and Research
Italtel S.p.A
Milan, Italy
fabrizio.bianchi@italtel.com

Marco Brunero
Cohaerentia S.r.L.
Milan, Italy
marco.brunero@cohaerentia.com

***Abstract*—Modern communication networks can be flexibly shaped and controlled using Software Defined Networking (SDN) paradigm. However, besides unprecedented functional benefits, this solution exploits an architectural single point of failure. Securing the communication among SDN functional element is therefore a critical requirement for improving the network reliability. A novel approach to secure communications is provided by Quantum Key Distribution (QKD) that is a physical layer technology capable to securely deliver symmetric encryption keys leveraging on quantum physic properties. Our research demonstrates how to provide unconditionally secure communication at SDN level dramatically improving the reliability of the communication network itself.**

Keywords—SDN, QKD, symmetric encryption, secure communications

I. Software Defined Networking Reliability

SDN [1] is a new paradigm for network control based on decoupling data and control plane. However, the internal communication among the functional elements of the control plane represents a single point of failure from an architectural perspective.

A. Software Defined Networking

Current network architectures are evolving towards new principles based on softwarization and virtualization, such as Software Defined Networking (SDN), where the fundamental concept is the decoupling between the Control Plane and the Data Plane. The Control Plane is the set of elements (hardware or software) that creates a local dataset for configuring the device, while the Data Plane is in charge of handling the incoming traffic and forwarding it towards the correct destination. In a SDN environment, the Data Plane is bounded by the network devices, while all the control and management features are moved into the logic layer of the Control Plane. This simple decision permits a high degree of freedom that reduces the integration and management costs of communication networks. The Control Plane permits a large degree of freedom in the network, devices and services, and this is where the flexibility of the SDN approach shines. However, this flexibility comes at the cost of a centralized control, which implies the creation - at least conceptually - of a single point of failure with potentially catastrophic consequences for the whole network. Increasing its robustness is a must for a critical infrastructure.

B. SDN reliability

The main functional elements of a SDN network are the logically centralized SDN controller, that implements the network logic, and the SDN agents, that control the network plane elements at each node. The correct communication and coordination among them are key aspects for the operation of the data plane.

Any attack or unauthorized manipulation of the internal SDN communication can dramatically damage or also break the functioning of the entire network. Therefore, to improve the reliability of SDN it is mandatory to secure the communication of SDN protocol messages. The approach we have investigated consists in adopting encrypted communication in the Control Plane. Due to the high rate of messages and the need of strong security, the best choice is to use symmetric encryption keys. Indeed, public key cryptography incurs in a large computing (time) overhead; therefore, symmetric cryptography is more attractive to secure a high speed and high throughput data channel. Having a channel integrated with the network, where high quality

symmetric keys are continuously distributed, can be used for both control and data encryption. This opens the opportunity for a QKD network integrated with a classical one to be used for both: high speed data encryption and secure control communications. The SDN paradigm, thanks to its flexibility, opens the possibility to do such an integration and, at the same time, it can benefit from the QKD service. In this sense, SDN and QKD are paradigms that complement each other. On the other hand, the use of QKD as a basic security technology at the physical level ensures that the network is resistant against any computational attack, even that from a quantum computer.

C. SDN communication to be secured

An SDN network can use encryption for both the Data and the Control plane. For the Data plane, this is generally a service for the users of the network, while for the Control plane keys are consumed on behalf of the network itself, to increase its robustness and resiliency against attackers.

In SDN networks there are several points in the Control Plane where QKD security-enhanced communication can be used:

- Between SDN central controller and SDN agent (in node) and network devices, usually via OpenFlow/NETCONF, to establish the flow configuration, device parameters, status requests and gathering statistics.
- Between the different components in a QKD-enabled disaggregated SDN node, especially in the inter-node communications (e.g. between the local key management components, see Fig. 3 and [2]).
- Between a network orchestrator and an SDN controller, typically via SSH and to establish end-to-end communications between points under different controllers, stats requests, etc.

Modifications to the SSH protocol appears as the most important ones. In this case, the SSH protocol is modified to check for the availability of QKD-derived keys for the specific connection and to use them together with the initial Diffie-Hellman key establishment procedure. Note that this is an election. QKD alone keys could be used, but it is preferable to use a final key obtained as a combination of the traditional D-H and the QKD. Indeed, the combination of both ensures the legal requirement of certification while the QKD certification process is still in development. The demonstration presented in this paper is a first step towards securing all these communications with the help of QKD.

II. Securing SDN with Quantum Key Distribution

QKD technology is recently becoming available for distributing symmetric encryption keys. QKD guarantees that the information leakage on a symmetric key created between two QKD devices can be bounded as tightly as needed. This bound is independent of the computational power of the adversary. Therefore, the adoption of QKD can improve the reliability of SDN networks by making the communication in the SDN control plane unconditionally secure.

A. Quantum Key Distribution

QKD provides unconditional security of communication services based on quantum physics property that makes it impossible to eavesdrop data transmitted over a quantum channel (optical fiber or free-space satellite link). The keys created in this process do not require any kind of computational complexity assumption, as is the case of Rivest–Shamir–Adleman (RSA) or elliptic curves used today. This makes the keys also resistant to any computational attack, either classical or quantum. The symmetric keys provided by a QKD system are thus quantum-safe. Symmetric encryption keys can then be used to provide unconditionally secure communications guaranteed by the laws of physic.

B. Quantum Secure Networking Prototype

The QKD prototype presented in this paper is called QSN (Quantum Secure Networking) and represents the result of an innovation project supported by EIT Digital and led by Italtel [5,6]. QSN is designed to be integrated in current metropolitan optical communication networks and supports the SDN being able to adapt to any network topology. The specific application of QSN prototype is to secure the internal communication among the functional entities of an SDN network.

QSN solution is composed by two stations: transmitter unit (Alice) and receiver unit (Bob). Whenever Alice needs to establish a secure communication with Bob, they shall generate a shared secure symmetric encryption key through the QKD communication over a quantum channel, realized as transmission of polarization-encoded photons over a standard optical fiber. Now Alice and Bob share the same key, which is unconditionally secure, meaning that they are sure that nobody was able to intercept it, thanks to the quantum physics principles exploited in QKD [7,8]. Finally, Alice can send a message to Bob and vice versa using mathematically secure encrypted communication over any communication channel, such as the usual Internet.

III. Demonstration

A. QSN prototype

For realizing the QSN prototype, it has been exploited the BB84 protocol [7] with polarization-encoded qubits over four linear states of polarization (with orientation angles 0°, 45°, 90°, 135°). A cost-effective configuration has been implemented, using just one single-photon avalanche detector (SPAD), instead of the standard one with two SPADs, placed after a polarization transformer (giving a polarization azimuth variation among the four possible values 0°, 45°, 90°, 135°) and a fixed-angle polarizer, according to the principle of operation described in [9]. In view of the co-propagation of the QKD channel with other classical traffic wavelength-division multiplexing (WDM) channel in C band (from 1530 to 1565 nm) in the same fiber, we have chosen for the QKD a wavelength of 1310 nm (i.e. the center of O band) for the quantum channel, in order minimize the crosstalk of the classical WDM channels with the QKD channel. The schemes of transmitter and receiver are shown in Figs. 1 and 2.

We have tested the performance of the QKD prototype in terms of quantum bit error rate (QBER) of the sifted key for

several values of link attenuation, up to a maximum of 11 dB, that are the typical conditions of optical links in urban area not longer than 20 km. We have always measured a QBER less than 6%, therefore lower than the theoretical threshold (about 11%) for guaranteeing unconditional security of the BB84 protocol [8].

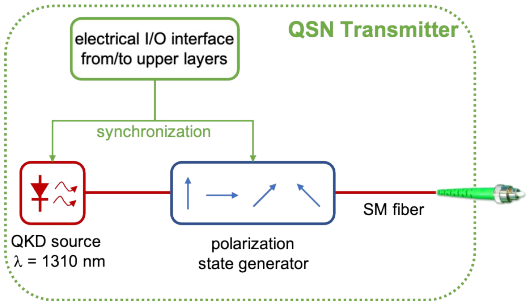

Fig. 1. Scheme of the QKD transmitter.

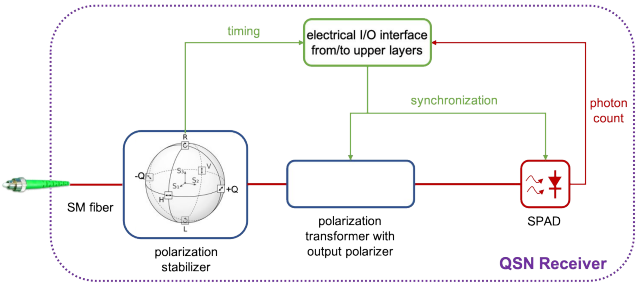

Fig. 2. Scheme of the QKD receiver.

B. *Content of the demonstration*

The novel idea to use QKD to secure SDN for improving the network reliability will be demonstrated securing the communications among the disaggregated components of a QKD-enabled SDN network, including both the intra-node and inter-node communications. A SDN QKD-enabled node in a SDN network is shown in Fig. 3. The demonstration secures the communication using keys extracted from the QKD devices.

Since at this stage we are mostly concerned with control information, which is usually short but has repetitions, the logical choice is to use a One Time Pad (OTP) scheme, where the keys are never reused and encrypts information of the same length than the key itself, in contrast to use an Advanced Encryption Scheme (AES) or a session key to secure a channel for a given length of time. While this might seem overkill, in principle, the expected number of keys needed are not that many, since control messages are usually short and the bandwidth used is small. In this situation, the production of keys by the QKD devices should be enough to cope with these demands. However, this is still a matter of debate, since it might vary much depending on the situation (e.g. in large nodes) and the performance of the QKD systems, which might also vary a lot depending on, e.g. the length of the links. For these reasons, the scalability of the scheme might be compromised. In this demonstration we implement a first version that does not enforce OTP encryption and use other techniques (e.g. AES or key expansion) to cope with these situations. The keys are thus automatically refreshed when needed from the QKD systems (e.g. at least one per message, whenever key production is sufficient). Note that a general requirement is that each disaggregated component has access to a QKD device.

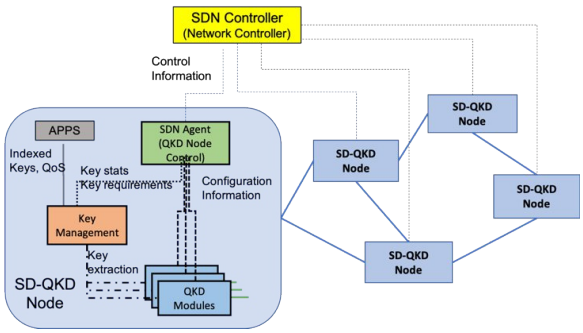

Fig. 3. QKD-enabled SDN node in a network and type of nformation flow

ACKNOWLEDGMENT

We want to acknowledge EIT Digital Q-Secure Net innovation activity that made it possible to realize the QDK prototype. QUITEMAD-CM P2018/TCS-4342, the FET Flagship on Quantum Technologies, EC Horizon 2020 research and innovation programme under grant agreement No 820466: Continuous Variable Quantum Communications (CiViQ), and ICT grant agreement No 857156: Open European Quantum Key Distribution Testbed (OpenQKD).

REFERENCES

[1] D. Kreutz et al. “Software-Defined Networking: A Comprehensive Survey”, Proceedings of the IEEE 103, pp. 14-76 (2015) DOI: 10.1109/JPROC.2014.2371999.

[2] A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martin, “The engineering of software-defined quantum key distribution networks,” IEEE Communications Magazine, vol. 57, no. 7, pp. 20–26, July 2019.

[3] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, “Hybrid conventional and quantum security for software defined and virtualized networks,” J. Opt. Commun. Netw., vol. 9, no. 10, pp. 819–825, Oct 2017.

[4] V. Martin (Rapporteur) et al. ETSI ISG GS QKD 015: “Quantum Key Distribution (QKD); Control Interface for SDN”. Approved Specification, Dec. 2020. (to be published www.etsi.org).

[5] https://research.italtel.com/projects/q-secure-net/

[6] https://www.eitdigital.eu/fileadmin/files/2020/factsheets/digital-tech/EIT-Digital-Factsheet-Q-Secure-net.pdf

[7] C.H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proc. IEEE Internat. Conf. Computers, Systems and Signal Processing 1984, Bangalore, 175.

[8] P. W. Shor and J. Preskill, “Simple proof of the security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett. 85, 441-444 (2000).

[9] P. Martelli, M. Brunero, A. Fasiello, F. Rossi, A. Tosi, and M. Martinelli, “Single-SPAD implementation of quantum key distribution,” Internat. Conf. on Transparent Optical Networks, Angers, 9-13 July 2019, We.C5.

.