Demonstration of a Dynamic QKD Network Control Using a QKD-Aware SDN Application Over a Programmable Hardware Encryptor

R. S. Tessinari, E. Arabul, O. Alia, A. S. Muqaddas, G. T. Kanellos, R. Nejabati, D. Simeonidou

High Performance Networks Group, University of Bristol, Woodland Road, Bristol, United Kingdom

rodrigo.tessinari@bristol.ac.uk

Abstract: We successfully implemented a QKD-Aware SDN application capable of real-time monitoring and controlling a quantum secure network paired with a programmable FPGA encryption/decryption technology to provide on-demand encryption algorithms for network services between different sites.

1. Overview

Recently, commercial high throughput encryption solutions were developed to work with Quantum Key Distribution (QKD) to answer the increased interest for quantum-secure networking, leading to many collaborations in the field. One of these collaborations was Nokia, SK Telecom and ID Quantique in 2018, where an IDQ QKD system was used for encryption with Nokia's Optical Transport Network systems on SKT's commercial network [1]. Moreover, in 2019, IDQ and ADVA partnered to produce the first commercial QKD encryption solution, where IDQ's Cerberis3 QKD System was combined with ADVA's FSP3000 encryptors to achieve quantum secure AES based 100 Gb/s encryption data line with dynamic Diffie-Hellman key exchange [3].

Data encryption rates have also been significantly increasing using hardware encryption, as it was demonstrated in [4] where an AES-based FPGA encryptor achieved a remarkable throughput of 482 Gb/s. Also in [5], a quasi-reconfigurable FPGA based encryptor has been demonstrated having a throughput of 200 Gb/s with limited 48.38 Gb/s AES rate.

However, all high-throughput and quantum secure hardware encryptor solutions available in the literature and market exhibit very limited reconfigurability, either locked within the firmware or non-existing [5]. Therefore, the encryption/decryption schemes on these implementations cannot be controlled dynamically to adjust, for example, the encryption scheme or the key consumption rate to fit the application or network operation requirements. Recently, a dynamic QKD network configuration was demonstrated in a field deployment [6] to offer enhanced rerouting capabilities in the distribution of keys, highlighting the potential for highly programmable networks with the use of reconfigurable hardware encryptors.

We recently reported on the implementation details of a new programmable FPGA-based encrpytor and discussed its performance in [7] (submitted in OFC 2021[1]). However in this paper, we demonstrate the implementation of a quantum SDN application, built on top of ONOS SDN Controller that takes advantage of its programmability to control multiple software agents and provides added flexibility to the network while leveraging the hardware encryptor to offer on-demand encryption. We also demonstrate network operation with on-demand choices of instigating QKD links while offering re-configurable on-the-fly encryption scheme changes and dynamic key consumption rates for different secured Virtual Network Services (VNSs) based on chained Virtual Network Functions (VNFs).

2. Demo Overview

The demonstration validates two main points of the system: i) that the SDN controller can establish QKD connections, monitor relevant parameters, and take actions accordingly, and ii) the FPGA-based encryptor adapts to the SDN controller commands in adjusting the encryption scheme and controlling the key consumption rate. On the next paragraphs, we describe the testbed details, followed by a workflow of the demonstration.

The testbed is detailed in Fig. 1 and is partitioned into three layers; the data layer, agent layer, and control layer. Starting from the bottom-up, the data plane is composed of compute servers, Optical Cross Connectors

[1]submission id: 3560910; N3: Architecture and software-defined control for metro and core networks, Key distribution and quantum networking

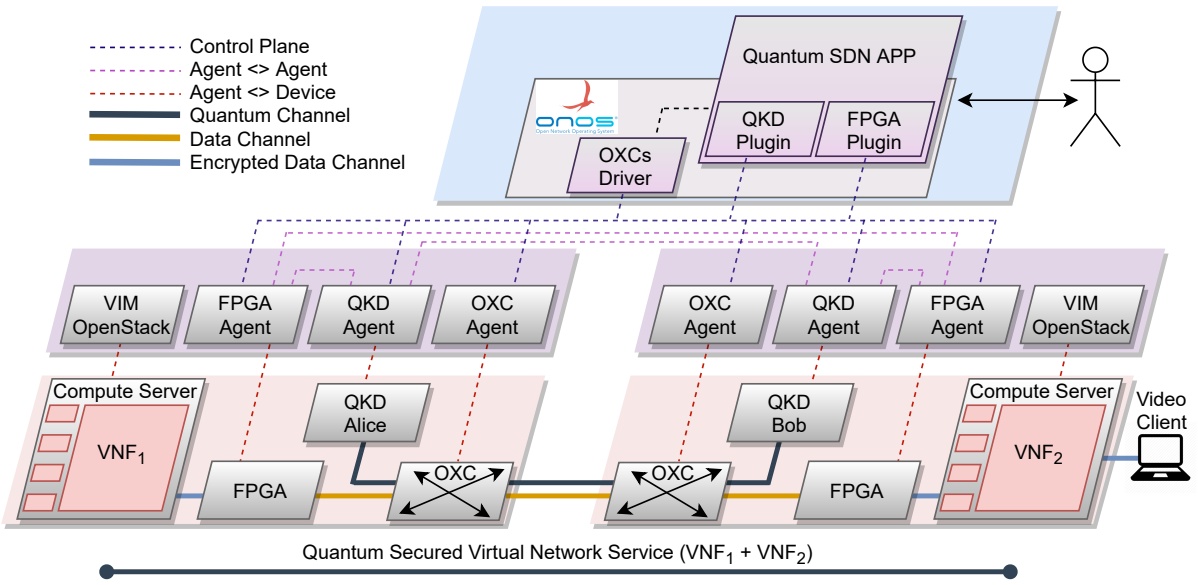


Fig. 1. Testbed setup

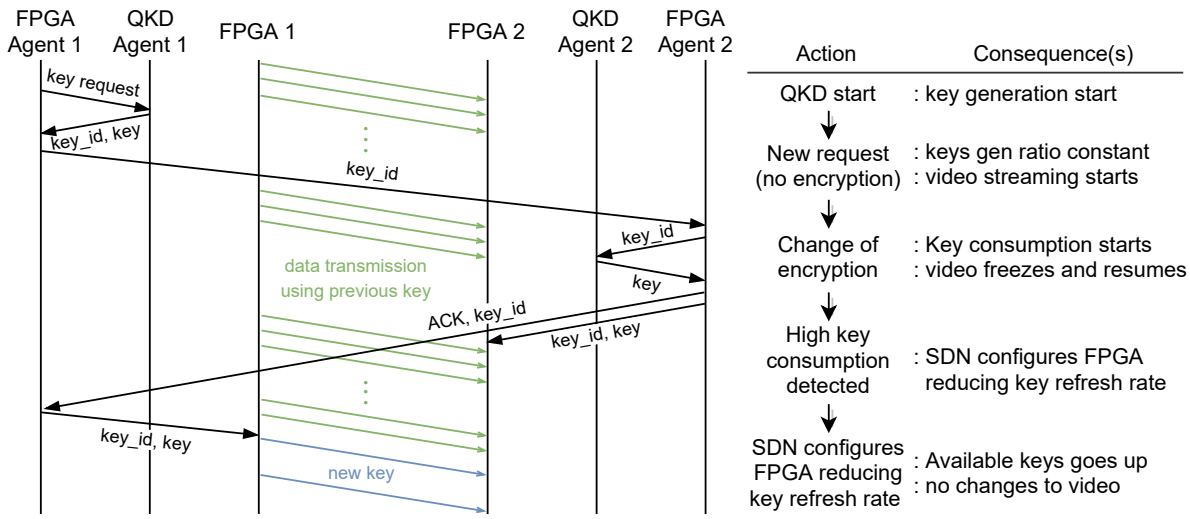
(OXCs), QKD devices, and FPGAs. The compute servers host VNFs including, but not restricted to, firewalls, deep packet inspectors, authentication servers, and video servers. Two or more VNFs are chained together to form a VNS which can be secure or not, according to the agreed Quality of Service (QoS). Next, the OXCs connect the devices inter- and intra-sites, where the ID Quantique Clavis 2 QKD devices generate 256-bit sized quantum symmetric keys. For encryptors, we used an FPGA implementation that can be programmed in real-time by the SDN controller with various encryption algorithms. The encryptor supports 10 Gb/s clients and can transmit up to 100 Gb/s encrypted traffic bidirectionally [7].

Each device has a companion agent that facilitates the communication with the SDN Controller. For instance, the QKD Agent (CQP Toolkit [8]) interfaces with QKD devices, stores the generated keys and can be controlled via gRPC; the OXC Agent applies the received flows from the SDN controller; and the FPGA Agent pushes keys and loads encryption algorithms. Moreover, there is a public communication channel between some of the agents to its peers, mainly for key synchronisation purposes. As an example, Fig. 2. a) illustrates how the FPGA agents synchronise keys, thus guaranteeing that the decryptor party always has the matching key, mitigating a potential problem of missing keys. It is important to mention that although instances of OpenStack as the reference Virtual Infrastructure Manager (VIM) are also part of our testbed, for the purpose of this demonstration, the VNF orchestration is outside the scope of this demo and is shown in more detail in [9, 10].

To conclude, on the control layer we take an advantage of ONOS southbound to install flows on classical equipment (i.e. the OXC devices in this particular demo). We also leverage internal ONOS gRPC and REST libraries to communicate with the other devices. Additionally, we created a Quantum SDN App to monitor both the QKD and encryption parameters. This application enables us to interact with the system during the demo, via ONOS northbound REST API interface.

In Fig. 2. b), the main aspects of the demonstration are highlighted. First, the QKD system will generate keys, being perceived as a continuous increase in the number of available keys. Following this, the Quantum SDN App is requested to provision an (insecure) connection between VNF_1 and VNF_2. Although the traffic is flowing through the FPGA, there is no encryption, hence no impact on the key consumption rate. Next, a change in the QoS of the connection is issued, resulting in the SDN controller sending a command to change the encryption algorithm. During the configuration time, the video stream freezes and resumes shortly after the configuration is done. Moreover, the encryptors start to consume keys, consequently decreasing the number of available keys. Finally, the SDN controller detects a high key consumption rate, thus it automatically intervenes by reducing the encryptors' key refresh rate to a more suitable value. This configuration occurs seamlessly to the application, and as a result, the number of available keys in the database stabilises.

The experimental validation will be conducted remotely at the University of Bristol, and all the software components will be accessed from the OFC premises. We will start the demo with a working QKD system producing keys and then show its operation by terminating the existing connection. The ONOS SDN controller and other VNFs will run on Ubuntu-based virtual machines. The logging of the software components will be visible to show all the relevant events. Custom software will show the available keys and key consumption levels. Furthermore, the video client will be accessed to show the end-to-end video streaming for verifying the connectivity status.



a) b)

Fig. 2. a) Key synchronisation diagram. b) Demonstration workflow.

3. Innovation

The demo showcases the deployment of 100 Gb/s FPGA-based encryptors, that supports varied encryption algorithms and can be programmed real-time by an application built on top of ONOS SDN Controller. The SDN controller itself brings three innovations: i) a QKD-aware module capable of controlling the QKD operation and managing the key generation process, ii) control the encryption application's key consumption rate and balance it based on real-time key generation rates, and iii) access a library of encryption algorithms which can be pushed to the FPGAs according to the requirements of the network operator or the resource optimisation algorithms. Currently, our system supports six encryption modes: AES (128, 192, 256), Camellia-256, XOR, and no encryption.

4. OFC Relevance

This demo is tailored particularly for the OFC audience, based on the ongoing trends of quantum secure networks, network control and secure applications/devices. This work may be of great interest for industry players who are thinking ahead and looking for ways to improve security in face of the new dawn of quantum computers and the vulnerability of current encryption solutions. Additionally, this work is also of interest of hardware manufactures, interested in novel designs for encryption devices. The OFC demo zone is a relevant venue for showcasing the results achieved under cooperation of UNIQORN, 5G-COMPLETE and UK Quantum Communication Hub projects, so the audience can learn more about the contributions of these projects towards the optical networks community. Furthermore, we use ONOS as the state-of-the art open source SDN controller, aiming to make our implementation more compatible with current community efforts.

Acknowledgements

This work was funded by EU funded projects 5G-COMPLETE (871900) and UNIQORN (820474); and part of the research leading to this work has been supported by the Quantum Communication Hub funded by the EPSRC grant ref. EP/T001011/1.

References

1. ID Quantique SA, "ID Quantique, SK Telecom & Nokia Secure Optical Transport System Using Quantum Key Distribution (QKD)," *Press Release*, 2018.
2. ADVA, "ADVA FSP 3000 powers UK's first quantum network," *Press Release*, 2018.
3. ID Quantique SA, "ID Quantique partners with ADVA to commercialise a quantum-safe encryption solution," *Press Release*, 2019.
4. B. Buhrow et. al., "A highly parallel AES-GCM core for authenticated encryption of 400 Gb/s network protocols," *ReConFig*, 2015.
5. Z. Martinasek et. al., "200 Gbps Hardware Accelerated Encryption System for FPGA Network Cards," *ASHES*, 2018.
6. R. S. Tessinari et. al., "Field Trial of Dynamic DV-QKD Networking in the SDN-Controlled Fully-Meshed Optical Metro Network of the Bristol City 5GUK Test Network," *ECOC*, 2019.
7. E. Arabul et. al., "Experimental Demonstration of Programmable 100 Gb/s SDN-Enabled Encryptors/Decryptors for QKD Networks," submitted to OFC, 2021.
8. R. Collins et. al., "QComms QKD Software Toolkit" *Journal of Open Source Software*, 4(38), pp.1119, 2019.
9. A. Aguado et. al., "Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources," J. Lightwave Technol. 35(8), pp. 1357-1362, 2017.
10. R. Nejabati et. al., "First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks," OFC, Th4C.6, 2019.