First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining over Flexi-WDM Optical Networks

R. Nejabati, R. Wang, A. Bravalheri, A. Muqaddas, N. Uniyal, T. Diallo, R. S. Tessinari, R. S. Guimaraes, S. Moazzeni, E. Hugues-Salas, G. T. Kanellos and D. Simeonidou
High Performance Network Group, Department of Electrical and Electronic Engineering, University of Bristol,UK
reza.nejabati@bristol.ac.uk

Abstract: First demonstration of quantum-secured end-to-end VNS composition through dynamic chaining of VNFs from multiple-domains. We rely on a novel quantum-switched flexi-grid WDM network and q-ROADM for inter-connectivity and on-demand selection of transport functions for quality-of-service.
OCIS codes: (060.2330) Fiber Optics Communications; (060.4250) Networks, (060.4253) Networks, circuit-switched

1. Introduction

The evolving 5G architecture needs to focus in developing solutions for managing disaggregation and cloudification of network functions and guarantee security of end-to-end 5G network services. Managing disaggregation and cloud-ification at large scale is fundamental, as it will enable new types of 5G services including cross-domain network slicing and neutral hosting scenarios, therefore delivering the true value promised by 5G. These new services will rely on composition of complex chains of disaggregated and distributed virtualized functions, often residing in technologically different and administratively independent 5G infrastructures. Optical networks will be a key enabler for such service delivery, offering high-bandwidth, fundamentally low-latency and relatively mature solutions for virtualizing and flexibly managing infrastructure. In addition, Quantum Key Distribution (QKD) promises ultimate physical layer network security and can be used to secure interconnections of distributed virtual functions. In this paper, for the first time, we experimentally demonstrate a quantum-secured multi-domain 5G network, using an orchestrator, the **5G-Exchange**, for end-to-end service composition with the following novel features: 1- On-demand composition of Virtual Network Services (VNSs) by chaining distributed Virtual Network Functions (VNFs) hosted in data centers belonging to different 5G network domains 2- Utilizing QKD for quantum-securing the VNSs via a quantum meshed network enabled by a novel **quantum switched flexi-grid ROADM (q-ROADM)**. 3- On-demand optimization of the service quality of VNSs (BW and connectivity) by dynamically adjusting the optical parameters such as modulation format and path selection.

2. Quantum Secured 5G Exchange Architecture, Concept and Experimental Setup

Fig1. shows the proposed quantum-secured 5G-Exchange architecture and the experimental setup including the physical optical network that supports co-existence and independent switching of quantum channels and classical flexi-WDM channels. In order to demonstrate on-demand composition of quantum-secured VNSs that each comprises a dynamic chain of VNFs, we have implemented four individual 5G network islands. Each 5G Island is an autonomous domain with representative radio access and optical fronthaul interconnected to an SDN enabled layer 2 network (Corsa switch), a data center (servers hosting VNFs), SDN enabled optical network (Voyager switch with multiple Bandwidth Variable Transponders-BVTs), QKD generator and receiver (IDQ Clavis 2), encoder and decoder.
2.1 Experimental scenario: we demonstrate three scenarios with multiple VNSs. Each VNS is defined by its composing VNFs, latency, Bandwidth, security requirements as well as its service start-time and Time To Live (TTL). Two experimental scenarios include VNSs where each comprises two VNFs with different network connectivity topologies, while the third scenario is a VNS comprising four VNFs. To demonstrate chaining of distributed VNFs using optical network, VNFs belonging to the same VNS are hosted in different islands and interconnected with a flexi-WDM channel and a QKD channel (if VNS is quantum secured i.e., SVNS), where the modulation format and center frequency are defined according to the required quality of service.
2.2. Orchestrator, control plane and workflow: Each of four 5G islands has its own independent SDN controller (based on OpenDaylight) and a NFV orchestrator (based on ETSI Open Source MANO (OSM)). An overlay orchestrator, the 5G-Exchange, is facilitating multi-domain orchestration across the four SDN and four OSM domains (one of each for each island) [1]. The 5G-Exchange is also based on OSM and has been extended with the following novel functionalities: 1- VNS Composer: which allows VNS description by defining the chain of desired VNFs, with or without defining the location of VNFs, but with the capability to define BW, latency and security for connectivity service in a VNF chain. 2- Network Service Manager: which is responsible for the life-cycle management and operation of a VNS. In this experiment, this functionality is limited to instantiation, operation and termination of a VNS and its VNFs. 3- Quantum-Aware Network Service Broker (QNSB): In this experiment, to reduce complexity we have preloaded compute nodes in each island with a set of VNFs. The QNSB will choose islands with unallocated VNFs and with suitable network connectivity capability (i.e. available ports and BW). If a VNS requires secured VNF chaining (indicated in

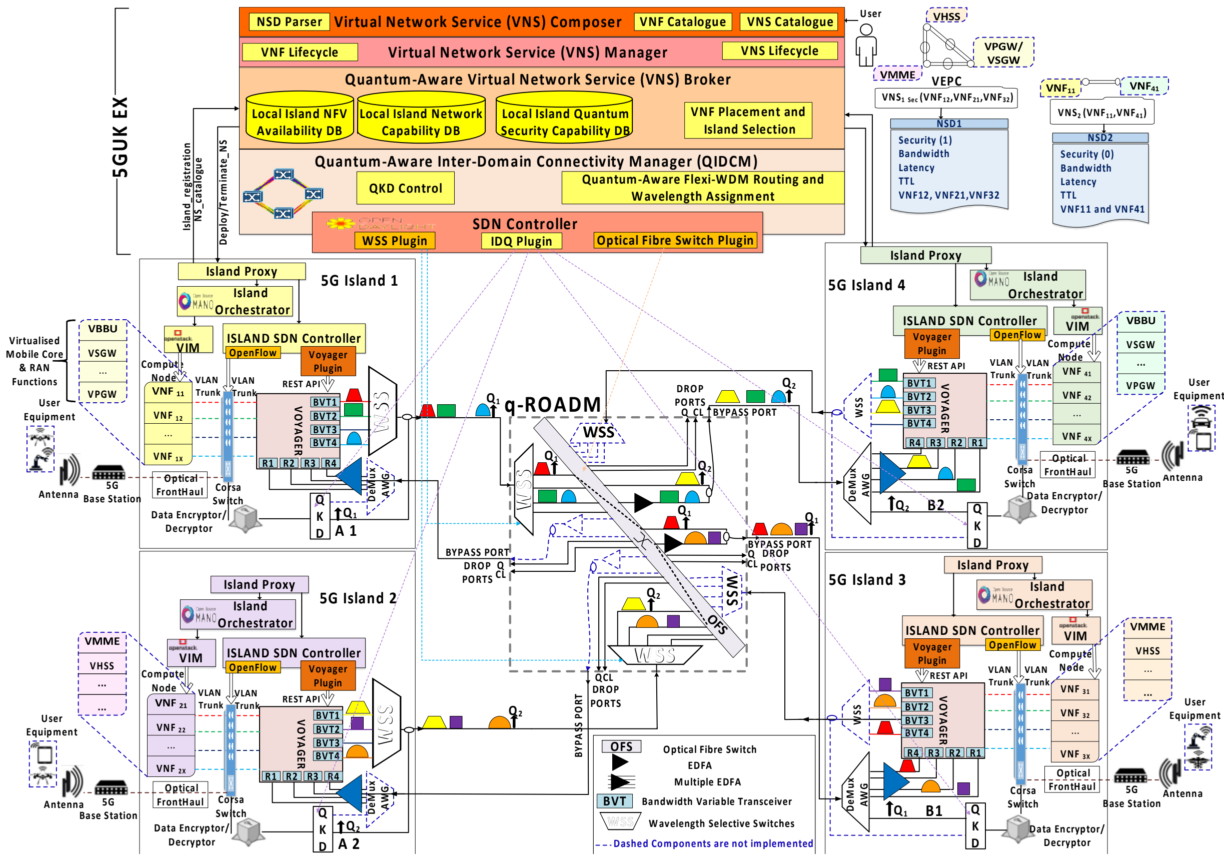

Fig. 1: Experimental setup: 4 5G islands connected over a quantum secured flexi-WDM network enabled by a q-ROADM.

the Network Service Descriptor - NSD), the QNSB must choose islands that have capability for QKD. Once island and VNF allocations are successful, the QNSB will request connectivity service. <u>4- Quantum-Aware Inter Domain Connectivity Manager (QIDCM)</u> is responsible for providing connectivity between VNF chains in a VNS. After selection of Islands and placement of VNFs, the QNSB requests the QIDCM to establish connectivity service for VNF chain of a VNS. In the proposed scenario each island has it is own local SDN controller, controlling intra-island layer 2 (Corsa) and optical network (BVT, Voyager). QIDCM uses an SDN controller to control the optical network that interconnects different islands (inter-island optical network). The QIDCM directly configures the q-ROADM for inter-island connectivity. It also acts as a parent controller for the SDN controller of each island (via the local island proxy). The QIDCM selects path, modulation format and center frequency for the optical channels between VNFs hosted in different islands. It also takes into account channel spacing (between data and quantum channels) needed for correct operation of QKD channel, in case of SVNS. Finally, the QIDCM is responsible to initiate quantum key generation between QKD devices of two separate islands that host VNFs of the SVNS.

<u>*2.4 Physical Layer:*</u> The experiment implements for the first time a quantum-switched optical network that allows: 1- to dynamically control and assign wavelength, BW and modulation format of each optical channel interconnecting the VNFs 2- a co-existent scheme of quantum and classical channels where any combination of mixed or independent quantum and classical signals arriving from one island can be destined to any other island providing a full 4-degree q-ROADM functionality that seamlessly interconnects the four islands 3- dynamic configuration of different pairs of DV-QKD transmitters (Alices) and receivers (Bobs) enabling provisioning/creation/use of new quantum paths. Specifically, each VNF is assigned in a particular VLAN, all VLANs are aggregated in a VLAN trunk through the Corsa switch and fed into the Voyager switch where the available 200Gb/s coherent BVT assigns each VLAN to a respective coherent link with controlled bit-rate and modulation format (QPSK, 8-QAM, 16-QAM) (see QIDCM). The four BVT ports of the Voyager are then multiplexed in a WSS (Finisar) and coupled to the island's DV-QKD quantum channel generated by an IDQ Clavis 2. An additional server that interfaces the Clavis 2 with the QIDCM is also responsible for providing the quantum keys to software encryptors (ChaCha20) that encrypt NFV data. The multiplexed quantum and classical signals are transmitted over the same fiber in a co-existing scheme to a novel fully functional low-loss, a 4-degree q-ROADM where the mixed signals arriving from each island are first demultiplexed through a WSS and coupled to an optical space switch (Polatis), both controlled by QIDCM. For the output ports of the q-ROADM, we have two options: 1- quantum- and classical channels are multiplexed again in the Bypass output ports 2- quantum

and classical channels are separated and dropped locally from the Drop ports. On the Bypass port of the q-ROADM, un-amplified mixed quantum- and classical channels and amplified classical channels are coupled through a 95/5 coupler respectively. The coupled amplified and un-amplified branches scheme was explicitly designed to minimize the optical losses for the quantum channel. For the Drop ports quantum and classical channels are separately driven to the island. On the Islands receiver side, the mixed channels from the Bypass ports are demultiplexed through fixed AWG. For both cases, total quantum channels losses over the q-ROADM do not exceed 5dB, while worst case end-to-end power budget is -8.9dB.

3. Results

Fig. 2 shows the experimental results. Fig. 2 (a), (b), (c) depict the physical layer characterization of classical and quantum channels co-existence scheme over the shared optical network, revealing the operational windows for single (a) and multiple (b) channels optical power and modulation formats (c) in order to sustain both the classical and quantum channels (secret key rate (SKR)>0). A maximum of 375 b/s SKR can be achieved on the bypass channel for 1 co-existing classical channel with a –24.5dBm co-existence power. For two classical channels, slightly worse performance with 250b/s SKR at -23dBm/channel co-existence power is achieved. The effect of modulation formats is investigated in the Drop ports, revealing that the minimum operational co-existence power for 16-QAM is -23dBm. Only QPSK and 8-QAM are considered in the following scenarios, allowing a broader operational power range. Fig. (d), (e), and (f) detail the three dynamic scenarios implemented for composition of SVNS: scenario 1 and 2 implement 4 parallel VNS each chaining 2 VNFs with 1 wavelength, while 2 VNS are quantum secured with the respective quantum channels in cross and bar states respectively. Scenario 3 implements a VNS with chaining 4 VNFs, in which 2 VNF chains are quantum secured with Q1 and Q2 respectively. Inset Tables provide the operational characteristics when scenarios deployment is stable. Average VNF chain delays of ~1ms include the negligible optical network delay and the VNF software stack delay indicating the low-latency potential. Fig. 2. (g, h) depict the implementation timings for management, control and data plane functions for the three scenarios. They start by setting up the inter-island datapath using IDCM. Follows the QKD key exchange in parallel with setting up intra-island flows and the VNFs deployment. Fig.2 (g) shows the execution and transition timings from scenario 1 to scenario 2 without redeploying the VNFs and local island networking but only changing the inter-island networking and QKD channel.

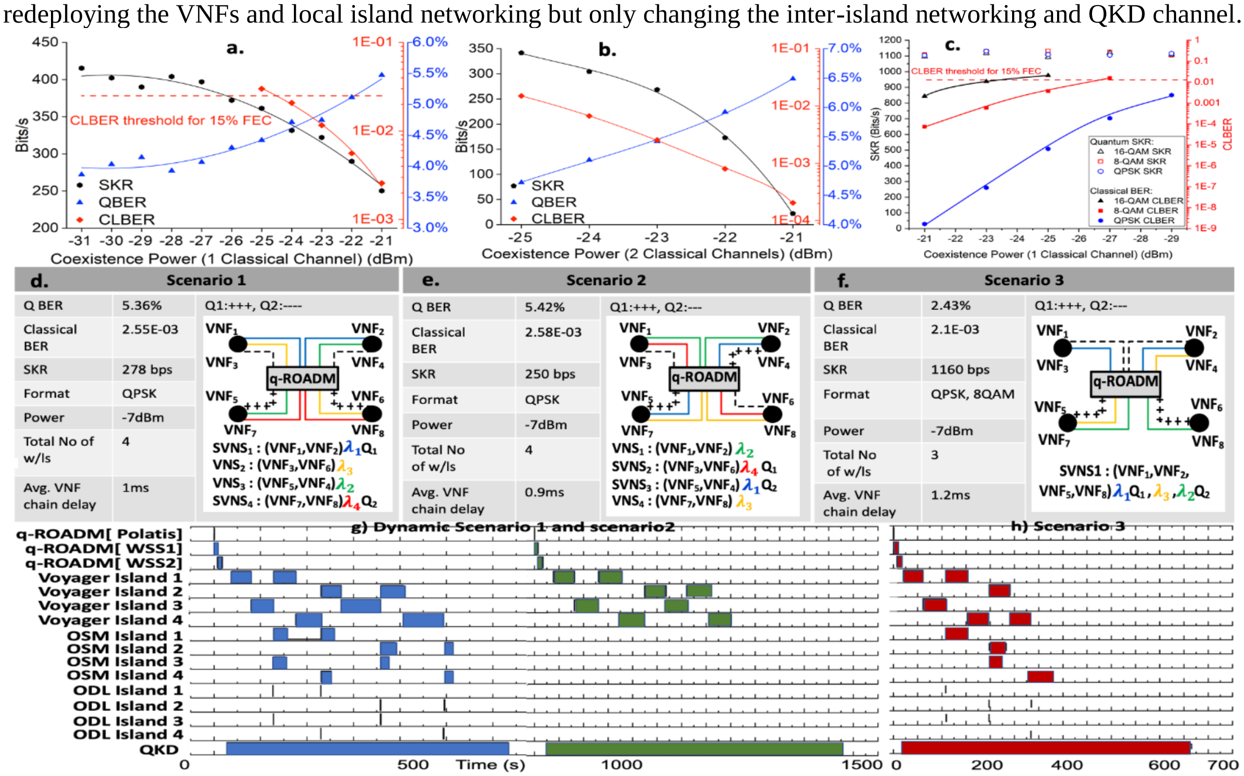

Fig. 2: Experimental results

4. Conclusion

We have experimentally demonstrated for the first time on-demand composition of quantum secured VNSs with adjustable BW by chaining distributed VNFs over an optical network employing a quantum switched WDM q-ROADM.

Acknowledgment: EU Funded Projects UNIQORN, Metro-Haul. UK EPSRC Funded Projects: TOUCAN, INITIATE, QUANTUM COMM. HUB

References: [1] D Gkounis, et. al., TuDS.14, ECOC 2018, Rome, Italy