Demonstration of a Resilient and Quantum-Secured Time-Shared Optical Network with Multi-Level Programmability

R. D. Oliveira, E. Arabul, R. Wang, G. T. Kanellos, R. Nejabati, D. Simeonidou
High Performance Networks Group, University of Bristol, Woodland Road, Bristol, United Kingdom
romerson.oliveira@bristol.ac.uk

Abstract: We have successfully implemented a multilevel programmable network resilience and security for Time-Shared Optical Networks (TSON). A SDN controller enables flexible control of FPGA-based network coding and encryption/decryption cores for secured and resilient TSON.

1. Overview

Optical Transport Networks (OTNs) have been rapidly growing as a research area and enabler for many on-demand technologies, such as 5G Networks, Internet of Things (IoT) and Smart Grids. With an increase in the amount of technologies transported over the networks, low-latency and high transmission capacity became essential for fronthaul/backhaul and metro/core network segments [1]. However, due to a vast number of technologies enabled by OTNs, a large variety of protocols has been used to access the network segments. The Time Shared Optical Networks (TSON) solution has been developed at the University of Bristol to address the growing interest in high bandwidth, low-latency, and flexible network access [2].

TSON is a proven multi-protocol access transport network solution which provides services such as Time Division Multiplexing (TDM), Wave Division Multiplexing (WDM) and Virtual Local Area Networks (VLANs) [2]. In its first iteration, TSON was designed to provide three levels of granularity based on networks requirements; allocation of sub-wavelength paths between two TSON Nodes; statistical multiplexing of the number of frames for connections; and division of frames into the smaller network resources defined as time-slices [3]. Later in the second iteration, TSON was evolved to support multi-protocol scenarios and synchronisation capabilities, and in this regard, xHaul and IEEE 1588v2 protocols were integrated into the TSON solution [4]. Moving to the third iteration of TSON, the Network Coding (NC) based protection had been implemented to improve the network resilience against base-band unit (BBU) failures, particularly for Cloud Radio Access Network (C-RAN) [5]. In the final two stages of the TSON's evolution, multi-haul support for TSON has been included and 100 Gbps Ethernet is dedicated for the long-haul network, whilst 10 Gbps Ethernet has been assigned for the metro/core [2].

In TSON architecture, a single 100 Gbps Ethernet connection between nodes and three 10 Gbps Ethernet connections for end points are provided. TSON can aggregate and dis-aggregate an arbitrary number of 10 Gbps clients and multiplex them onto its TDM and WDM enabled 10 Gbps or 100 Gbps flows. Furthermore, NC resilience is enabled for the metro/core network. Although TSON has been a resilient network solution, the optical security of TSON has not been considered to-the-date. Since a large amount of information is transferred by using TSON over the network, it cannot be denied that it is vulnerable to security threats.

In another research direction, previously, we have reported a Quantum Key Distribution (QKD)-aware 100 Gpbs programmable hardware encryptor [6, 7] and demonstrated the dynamic QKD control provided by a Software Defined Network (SDN) controller [8]. Our hardware encryptor solution has been unique in a way that its encryption scheme can be programmed by the SDN-controller on-the-fly for the network requirements. Therefore, based on the key refresh rates, throughput or any other network requirements, security could be dynamically adapted.

By applying the encryptor to secure the metro/core and long-haul flows of the TSON, this demo integrates TSON's resilient transport capabilities with the flexible security of a programmable hardware encryptor using a quantum key distribution system.

2. Demo Overview

In this demo, we show how network resilience and security can be achieved in optical domains by applying an Field Programmable Gate Array (FPGA)-based programmable encryptor to an environment hosting time-shared optical networks. The goal is to provide a quantum secured and resilient transport access for applications sharing the same infrastructure, and we aim to demonstrate that: *i)* TSON links are resilient, due to the Network Coding applied

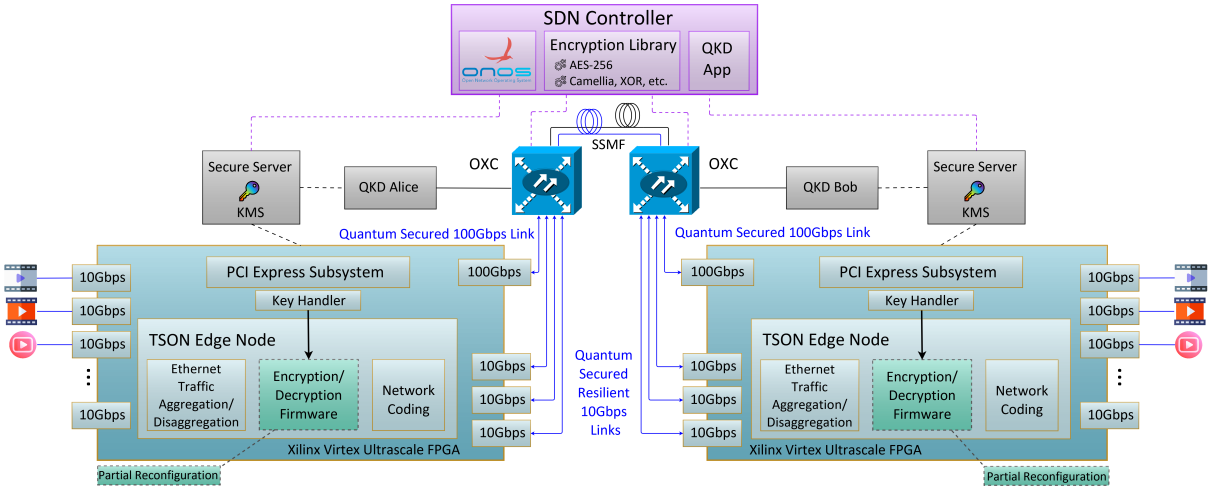

Fig. 1. Testbed Overview

to each data channel, in a way that the transmission persisting in case of link breakdown; *ii)* quantum hardware security can be added to the resilient links to achieve different levels of security according to the Security Policies; and *iii)* the traffic can be aggregated and transmitted over a quantum secured channel.

As a result, we create an environment with different and adjustable levels of security and resilience, which can be configured according to the quality of service agreed between clients and provider. Fig. 1 details the testbed for this demonstration. There are two similar communication sides, TSON edge node on the left acts as the server while the one on the right side holds the clients. In each node, there is a Xilinx VCU108 prototyping board with a Virtex UltraScale FPGA. Each board is connected to three clients through 10 Gbps optical Ethernet connections. The maximum number of clients is limited by the availability of SFP+ interfaces and the resource availability of the FPGA. There is an FPGA Mezzanine Card (FM-S18) which supports up to eight 10 Gbps clients. Also, there is one QSFP+ interface for the 100 Gbps channel. They are connected to Optical Cross-Connectors (OXC) that interconnects all the entities in the system. The OXCs are configured by the SDN controller which has access to all agents.

Two QKD units, Alice and Bob are connected to servers and they generate keys for the encryption process. The keys are managed by the Key Management Stores (KMS) and then sent to the FPGA via Peripheral Component Interconnect (PCI)-Express. Inside the FPGA, there is the core responsible for traffic aggregation and dis-aggregation; the programmable encryptor/decryptor; and the Network Coding, i.e., where the resilient links are coded to have the ability of recovering the transmission after failures. The connection between the two FPGAs is provided by four optical lanes. One of them operates at 100 Gbps and the others at 10 Gbps. In addition, all lanes can be quantum secured according to the requirement.

On the top of the Fig. 1, the SDN controller is a control plane's entity to orchestrate the software agents and forwarding hardware across the testbed. This is a distributed controller which uses Open Network Operating System (ONOS); a QKD App developed for our system; and hosts the Encryption Library with AES-128, AES-256, Camellia-256, XOR and PLAIN schemes of data encryption [7]. These algorithms can be dynamically embedded to the FPGA to change the encryption scheme based on demand. The data plane lies mainly within the FPGA, the optical Ethernet interfaces, OXCs and the streaming servers/clients in the edge of the network.

To validate the process, seven steps are assorted for addressing specific parts of the system. They are detailed in the following items and summarized according to Fig. 2.

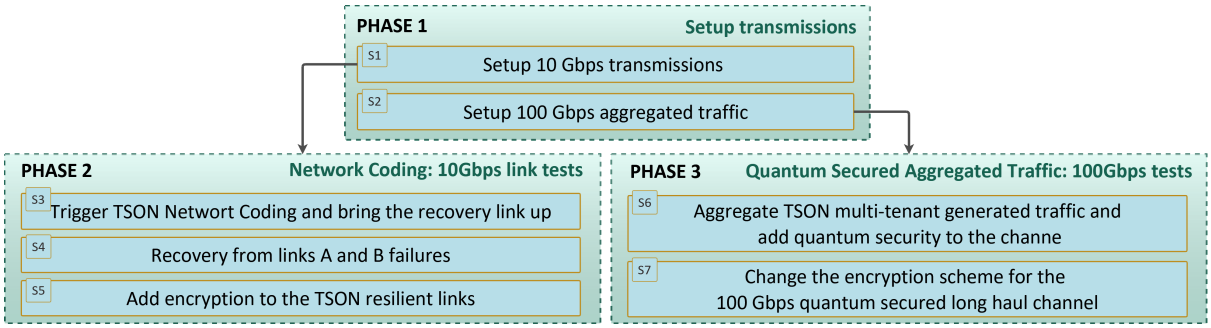

Fig. 2. Demo flowchart

1. *Setup 10 Gbps transmissions*: Transmissions are started among the 10 Gbps interfaces. Each inbound interface will be connected to one outbound interface (1:1) - and vice-versa at the receiver side. In this step, there is no encryption neither resilience is tested on the links and functioning paths are demonstrated.
2. *Setup 100 Gbps aggregated traffic*: All three inbound interfaces will be redirected to the 100 Gbps outbound interface to start the traffic aggregation proceeding. At this stage, there is no encryption running and plain transmissions will take place to certify the connectivity.
3. *Trigger TSON Network Coding and bring the metro core recovery link up*: Network Coding is enabled and the 10 Gbps link is activated and used to recover either A or B TSON flows in case of link breakdown.
4. *Recovery from links A or B failures*: Transmission is checked on the receiver's side and by applying modulo-2 sum (XOR) the link breakdown is recovered.
5. *Add encryption to the TSON resilient links to cope with Security Policies*: Security for the 10 Gbps links is enabled by encrypting the transmission using quantum keys and one encryption scheme from the library.
6. *Aggregate TSON multi-tenant generated traffic and add quantum security to the channel*: AES-256 is activated for the 100 Gbps long haul lane, and also, the time sharing multiplexing for the 10 Gbps metro core tenants is started. Then, the video's capture on the other side of the telecommunication system is checked.
7. *Change the encryption scheme for the 100 Gbps quantum secured long haul channel*: The SDN controller is able to change the encryption algorithm by sending instructions to the FPGA. In this step, by receiving the instruction, the FPGA update the firmware with a new *.bit file with no need to interrupt the system's operation.

3. Innovation

This demo showcases the deployment of a combined solution for long-haul and metro-core networks that offers multilevel programmability for network resilience and adjustable security. The current TSON architecture brings three key points of innovation: *i)* network coding combined with quantum security to provide a protection against network failures whilst, maintaining an unconditional security against eavesdropping; *ii)* different levels of security for different segments of the same transport network; and *iii)* a time shared optical infrastructure to support multi-tenancy protected by quantum security on the aggregated traffic. Currently, the system works with 10 Gbps channels for the metro-core and either 10 Gbps or 100 Gbps for the long haul, all orchestrated by an SDN-controller.

4. OFC Relevance

This demo is particularly designed for the OFC audience based on the ongoing trends of quantum networking, implementing advanced QKD applications, programmable networks, softwarised network functions and programmable hardware. Further to this, this work has a noticeable potential to attract industry interests, specially providers who are intent to improve the network security with quantum resources available and flexible their optical transport infrastructure by offering flows with adjustable levels of security and resilience according to the clients affordability. 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.

Acknowledgements

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

References

1. A. Al-Dulaimi et. al. , "Standardization: The Road to 5G " *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*, (Wiley-IEEE Press,2018),pp.691-708.
2. A. F. Beldachi et. al., "A Programmable Network Edge Solution for Multi-Access Support," *Appl. Sci.*, 9(22), pp.1-16, 2019.
3. G. S. Zervas et. al., "Time Shared Optical Network (TSON): a novel metro architecture for flexible multi-granular services," *Opt. Express* 19(26), pp.B509-B514, 2011.
4. Y. Yan et. al., "High performance and flexible FPGA-based time shared optical network (TSON) metro node,"*Opt. Express* 21(5), pp.5499-5504, 2013.
5. A. F. Beldachi et. al., "Resilient Cloud-RANs Adopting Network Coding,"*ONDM* 2019.
6. E. Arabul et. al., "Experimental Demonstration of Programmable 100 Gb/s SDN-Enabled Encryptors/Decryptors for QKD Networks," *OFC*, 2021.
7. E. Arabul et. al., "100 Gb/s dynamically programmable SDN-enabled hardware encryptor for optical networks," *J. Opt. Commun. Netw.* 14(1), pp.A50-A60, 2022 .
8. R. S. Tessinari et. al., "Demonstration of a Dynamic QKD Network Control Using a QKD-Aware SDN Application Over a Programmable Hardware Encryptor," *OFC*, 2021.