Stange Tessinari, R., Bravalheri, A. C., Hugues Salas, E., Silva Guimaraes, R. S., Alia, O., Kanellos, G., ... Simeonidou, D. (2019). *Field Trial of Dynamic DV-QKD Networking in the SDNControlled Fully-Meshed Optical Metro Network of the Bristol City 5GUK Test Network*. Paper presented at ECOC 2019, Brussels, Belgium.

Peer reviewed version

Field Trial of Dynamic DV-QKD Networking in the SDN-Controlled Fully-Meshed Optical Metro Network of the Bristol City 5GUK Test Network

Rodrigo S. Tessinari[1], Anderson Bravalheri[1], Emilio Hugues-Salas[1], Richard Collins[2], Djeylan Aktas[2], Rafael. S. Guimaraes[1], Obada Alia[1], John Rarity[2], George T. Kanellos[1], Reza Nejabati[1], and Dimitra Simeonidou[1]

[1]*High Performance Network Group, University of Bristol, UK*
[2]*Quantum Engineering Technology Labs, University of Bristol, UK*
**gt.kanellos@bristol.ac.uk*

Keywords: QUANTUM KEY DISTRIBUTION, OPTICAL SWITCHING, OPTICAL NETWORK

Abstract

We demonstrate for the first time a field trial of a fully meshed metro network with dynamic QKD networking capabilities across four optical network nodes in the 5GUK Test Network, where the DV-QKD quantum channels co-exist with classical channels and are dynamically switched and rerouted utilising QKD-aware SDN control.

1 Introduction

Emerging 5G services are high-bandwidth, low-latency cloud-based services that often require optical network connectivity between end-users and compute resources at the edge of the network (MEC or FOG computing paradigms [1]) and in remote data centres. However, in the distributed and highly dynamic environment of the emerging 5G services now raises security as a critically important aspect that must be provided in an end-to-end fashion.

QKD technology has been brought into perspective as the ultimate physical layer security. However, in order to become functional for practical 5G scenarios, it must be integrated with the classical optical networking infrastructure and adapt to the dynamic environment on the metro/edge part of the 5G networks. Current filed-deployed QKD secured networks are mainly based on point-to-point, static links on dedicated fibre connectivity [2]. These QKD network deployments have so far relied on the use of trusted nodes [3], where the content of QKD channels from one link has to be connected using some form of key management [3] with the next link. In a recent field trial demo in Madrid [4], dynamic QKD networking in a metro ring network scenario has been demonstrated with CV-QKD technology going through a commercial optical switch.

However, to the best of authors knowledge, there is no field trial reporting on dynamic networking with DV-QKD. DV-QKD scheme poses significantly more technical challenges in switching and co-existence with classical optical channels. This is mainly due to DV-QKD protocol requirement for few/single photon based QKD [5]. Furthermore, Dynamic QKD in a meshed network scenario (for both DV and CV QKDs) still is a major challenge and there is no previous reported field trial.

Recently authors have demonstrated in the lab a quantum-ROADM implementation with the ability to simultaneously mix and route any combination of classical and DV-QKD channels in any of the four ROADM degrees [6], as the ultimate switching element towards quantum-secured WDM optical networks for inter-domain 5G services.

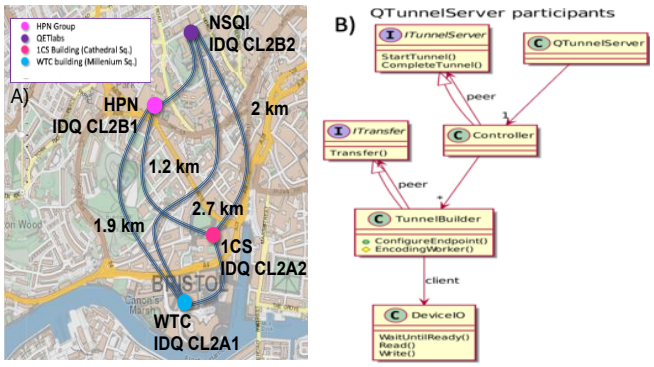


Fig. 1. A) Bristol City map with the location of each node and distance of the fibre links. B) Block diagram of *QtunnelServer* application to encrypt/decrypt data with AES using quantum keys.

In this paper, we take advantage of the low optical losses of fibre transmission in the metro network and combine it with ultra-low losses of optical MEMS switching technologies [7], to demonstrate that the limited power budget of DV-QKD technologies can still be efficiently applied with dynamic metro optical networking scenarios to provide quantum secure communication between computing resources at the edge and 5G access points. We demonstrate for the first time a field trial of a fully meshed network with dynamically switched DV-QKD capabilities supporting the co-existence of classical optical channels in the same fibre as QKD channel. The network comprises four optical network nodes across Bristol city, including the 5G access point in Millennium Square (WTC) and in 1 Cathedral Sq. as well as the University of Bristol campus nodes of HPN Group and QETLabs (NSQI), as depicted in figures 1.A and 2A. The four sites are connected through the metro optical network (with dynamic optical switching capabilities) of 5GUK Test Network in a meshed topology. We demonstrate simultaneous classical/quantum dynamic switching for continuous transmission of quantum-encrypted data using a QKD-aware Software Defined Network (SDN) Control Plane that provides continuous and optimal quantum secured connectivity in the meshed network scenario.

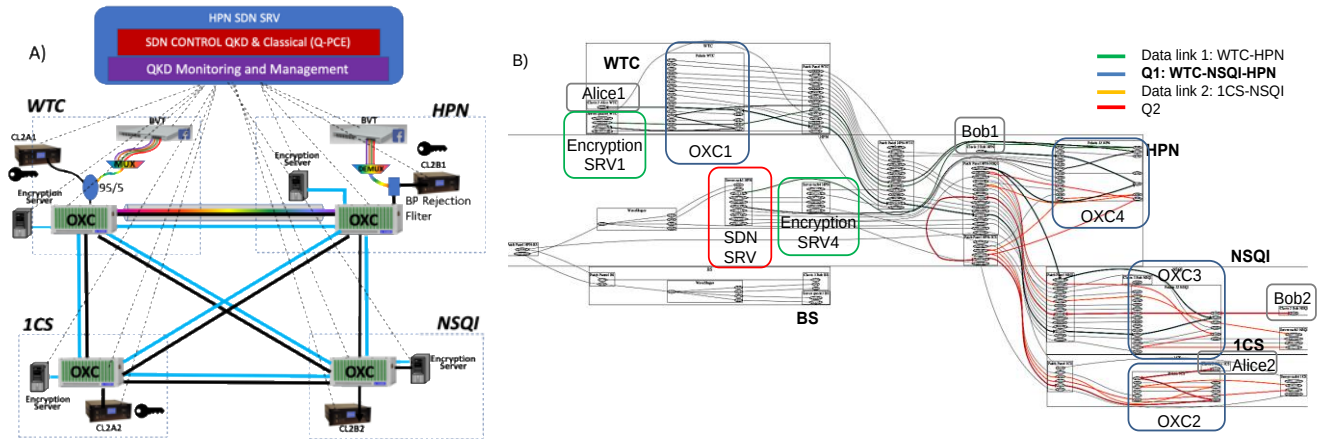


Fig. 2. A) Block diagram of the field-trial dynamic QKD network. B) Actual filed trial network topology as print-screen of the interactive map (for Demo Step1). Coloured links are the data plane active links for quantum and classical data channels.

2. The testbed

2.1 Data Plane Connectivity

The network comprises four nodes in a full mesh physical topology across the Bristol City metro area as shown in Fig. 1.A. All four nodes are equipped either with an Alice (WTC, 1CS) or Bob (HPN, NSQI) terminals of the commercially available IDQClavis2 DV-QKD system that implements the BB84 protocol. Each node employs a low loss optical switch with less than 2dB of optical losses while all fibre links are <10km, leading to a total link power budget of <7dB for all mesh links, safely within the 10dB power budget dynamic range of the IDQClavis2. The use of an optical switch in each node guarantees quantum and parallel classical data link for any-to-any node interconnection. Scalability of the network is determined by the number of switch ports that for MEMS based switches can scale to 100's of ports [7]. In case of link failure or Denial of Service (DoS) attack, an additional maximum 1-hop may be required in such mesh-topology to re-establish the broken link, leading to a maximum cascade of three switches. Each link also employs a parallel fibre for the classical data channel (10Gb/s SFP+ C-band interfaces) that is connected to the encryption server through a NIC card. This is in addition to the capability for co-existence of classical and quantum channel in the same fibre. WTC node also employs a BVT switch (Facebook Voyager) that provides 4x100Gb/s 25 Gbaud PM-QPSK channels in the C-band. The BVT channels are coupled through a 95/5 coupler in the same fibre with the IDQClavis2 quantum channel in a co-existing configuration. A second BVT switch in HPN node receives the BVT channels after a band-pass rejection filter (BPRF) with 0.8dB of loss before the IDQClavis2 Bob1, thus establishing a co-existing link between WTC-HPN. Additional parallel fibres are used for the quantum channels service links and for providing the control channels interconnection with the SDN server (HPN). Fig. 2.B shows the full complexity of the network topology.

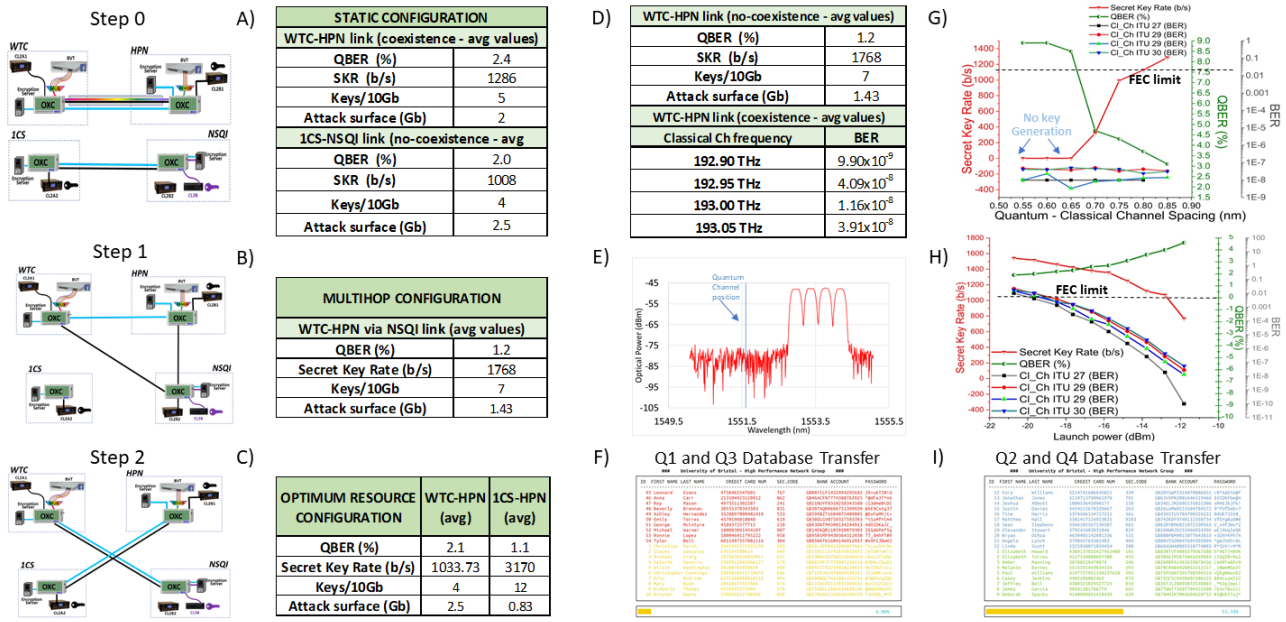
2.2. SDN Control Plane

The SDN Control Plane is responsible for the computation, creation, and management of the complete path that traverses optical and SDN switches between the nodes. SDN Controller is individually controlling the switches, QKD terminals, and encryption/application server in each node (Fig. 2.A) to create secure channels. The SDN controller utilises a quantum aware path computation mechanism, Q-PCE Fig. 2.A, that calculates the best path for QKD and classical channel, including power and modulation format for minimal effect on the QKD channel [10]. The quantum keys generated by the IDQClavis2 are managed by the SDN Control QKD Management blocks responsible for the creation of the quantum key tunnel using the in-house CQP toolkit [9]. The embedded *QTunnelServer* application is a working implementation of a Virtual Private Network (VPN) service which uses an interface that directly incorporates key cycling on a configurable basis (e.g., based on time or data usage) and encrypts data with AES (Fig. 1.B). Once the end-to-end path is established, the Quantum Key management Block sends the quantum key information to the SDN Control Plane. Subsequently, the SDN Control Plane authorizes the end-to-end transmission between the nodes and encrypts the classical channel with GCM-AES-256 encryption scheme using the quantum keys. The application server awaits permission in the form of a publish-subscribe asynchronous message from the Control Plane to initiate or terminate publishing confidential information.

On the application side, the confidential information of 2000 customers is stored in a database. This database is sent as publish-subscribe asynchronous messages through a QKD-secured channel previously established by the SDN Control Plane. The confidential information is displayed on the GUI screen in a colour-coded format, where each colour represents messages pertaining to a specific server (Fig. 3.F and 3.I).

3 Results

To evaluate the performance of the full-mesh dynamic QKD network, we implemented several dynamic configurations of the topology (Fig. 3, Steps 0, 1, and 2) with the classical data in co-existence or in parallel and monitored the performance of the QKD channel(s) in terms of QBER and SKR when the AES-GCM 256 encrypted data channel(s) were sustained. In particular, Fig. 3.A presents the static results for the quantum channels Q1 and Q2 (A1→B1, A2→B2) while Q1 is co-existing with 4x100Gb/s QPSK channels (Fig. 3.E spectrum). The tables in figures 3.A and 3.D show the SKR variation between Q1-no-co-existence and Q1-co-existence while Q2 SKR is reduced due to increased link losses. During co-existence, the classical channels are coupled after a 1x4 coupler with an aggregated optical power of -12dBm together



STATIC CONFIGURATION	
WTC-HPN link (coexistence - avg values)	
QBER (%)	2.4
SKR (b/s)	1286
Keys/10Gb	5
Attack surface (Gb)	2
1CS-NSQI link (no-coexistence - avg	
QBER (%)	2.0
SKR (b/s)	1008
Keys/10Gb	4
Attack surface (Gb)	2.5

MULTIHOP CONFIGURATION	
WTC-HPN via NSQI link (avg values)	
QBER (%)	1.2
Secret Key Rate (b/s)	1768
Keys/10Gb	7
Attack surface (Gb)	1.43

OPTIMUM RESOURCE CONFIGURATION	WTC-HPN (avg)	1CS-HPN (avg)
QBER (%)	2.1	1.1
Secret Key Rate (b/s)	1033.73	3170
Keys/10Gb	4	12
Attack surface (Gb)	2.5	0.83

WTC-HPN link (no-coexistence - avg values)	
QBER (%)	1.2
SKR (b/s)	1768
Keys/10Gb	7
Attack surface (Gb)	1.43
WTC-HPN link (coexistence - avg values)	
Classical Ch frequency	BER
192.90 THz	9.90×10^{-9}
192.95 THz	4.09×10^{-8}
193.00 THz	1.16×10^{-8}
193.05 THz	3.91×10^{-8}

Fig. 3. A) Q1 and Q2 parallel secure links with Q1 in co-existence with 4x100G channels, B) three-hop quantum secure channel, C) Q3 and Q4 secure channels established after switching, D) performance of co-existent channels, E) spectrum of 4x100G co-existent channels, F) , I) GUI for encrypted database transmission for Q1, Q2, Q3, Q4 secure links, G), H) Co-existence analysis vs. channel spacing and input power.

with the quantum channel. On the HPN site, the unamplified classical channels are directed to the Voyager BVT for coherent detection after the BPRF via a 1x4 optical splitter, and with a 15% FEC, the channels are recovered within FEC acceptable limits ($<10\text{x}10^{-8}$) and with OSNRs of 27.04dB, figures 3.D and 3.H. Fig. 3.H details the performance of classical and quantum channels vs. the classical channels aggregated power at the co-existence level and reveals an additional power tolerance of 3dB for acceptable channels reception. Fig. 3.G shows the tolerance of quantum channel to the classical channels' wavelengths up to 0.5 nm of spacing.

Fig. 3.B provides a comparison for the secure link when the quantum channel is transmitted over two and three nodes respectively. Q-channel rerouting may occur in case of link failure or if a Denial-of-Service (DOS) attack is launched over the vulnerable quantum channel [8]. We used the WTC-HPN secure link as a reference for this comparison and compared the quantum channel as 1) a direct link and 2) when it is redirected through the NSQI node, while the classical encrypted data channel is not redirected. To test the SDN controller, at an arbitrary time the Q1 link was manually unplugged and the SDN controller automatically detected the loss of the quantum signal and commanded the rerouting of the quantum channel through NSQI. SDN decision was based on the new link overall losses that were manually configured. In both cases, the Q2 secure link between 1CS and NSQI remains unaffected. The SKR comparison for one and two hops (figures 3.D and 3.B) reveals a 20% drop due to the additional link losses induced by the optical switch.

At this point, it should be mentioned that the nodes in our mesh-network implementation are not considered trusted nodes. Rerouting of the quantum channel relies only on passive optical beam-steering devices (e.g., mirrors) and once the optical path is established, the quantum channel initialization and authentication rely only on the information exchanged between the end nodes of the link. This is a significant benefit to the approach of trusted nodes. Fig. 3.C presents the QBER and SKR results when the two new secure links Q3 and Q4 have been established. In this case, A1 from WTC node establishes a QKD channel with B2 in NSQI, providing a new QKD channel Q3 that would normally require and additional pair of QKD devices if the mesh network was not in place, highlighting the optimization of resource usage as a benefit of the dynamic network approach. In a similar way, a fourth quantum channel Q4 establishes a fourth secure link between A2→B1. In order to achieve successful authentication for the new quantum secure channels, B1 and B2 have to share the same pre-shared key. Figures 3.F and 3.I shows the GUI that monitored the progress of the encrypted databases been transmitted only when the quantum-secure channels were sustained. Messages from Q1 (WTC-HPN) are displayed in red (Fig. 3.F), whereas the messages from Q2 (1CS-NSQI) are displayed in blue (Fig. 3.I). When the Control Plane implements the switching to setup Q3 (WTC-NSQI) and Q4 (1CS-HPN), the messages appear in yellow (Fig. 3.F) and green (Fig. 3.I) respectively indicating the initialization of the new secure channels. The progress bar shows the status of data transmission based on the number of customers and gives the percentage of pending messages.

4 Conclusion

We have demonstrated for the first time a dynamic QKD networking implementation over a field-trial testbed that spanned across four optical nodes interconnected in full-mesh topology. Indicative results of dynamic setup for quantum-secure optical channels transmission were presented revealing the resource allocation and rerouting advantages for QKD networking.

5 Acknowledgements

This work acknowledges EU-H2020 UNIQORN, the EPSRC EP/M013472/1: UK QHub for Quantum Communications, and Facebook for the Voyager switches in the experiment.

6 References

[1] Q. Pham et al. “A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art,” arXiv:1906.08452, Jun 2019

[2] A. Wonfor, et. al. “High performance field trials of QKD over a metropolitan network,” QCrypt 2017, Cambridge, UK

[3] Q. Zhang, et. al., “Large scale quantum key distribution: challenges and solutions,” Optics Express, Vol. 26, Issue 18, pp. 24260-24273(2018)

[4] V. Martin, et. al., “The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure,” in OSA Advanced Photonics Congress (AP) 2019 (), paper QtW3E.5

[5] R. Asif et. al., “Seamless Cryptographic Key Generation via Off-the-Shelf Telecommunication Components for End-to-End Data Encryption”, iThings-GreenCom-CPSCom-SmartData.2017.140

[6] R. Nejabati, et al., “First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining over Flexi-WDM Optical Networks,” In Optical Fiber Communication Conf., 2019, pp. Th4C-6.

[7] Polatis - Optical Switch Modules, https://www.polatis.com/switch-modules-for-oem-all-optical-switch-module-solutions-original-equipment-manufactures.asp, accessed 08 September 2019.

[8] E. H. Salas, et. al, “Monitoring and Physical-Layer Attack Mitigation in SDN-Controlled Quantum Key Distribution Networks,” J. Opt. Commun. Netw. 11, A209-A218 (2019)

[9] R. Collins and D. Aktas, “QComms QKD Software Toolkit,” Journal of Open Source Software, Jun 2019.

[10] Y. Ou et al., “Field-Trial of Machine Learning-Assisted Quantum Key Distribution (QKD) Networking with SDN,” 2018 European Conference on Optical Communication (ECOC), Rome, 2018, pp. 1-3.