Dynamic DV-QKD Networking in Fully-Meshed Software-Defined Optical Networks

Obada Alia, Rodrigo Stange Tessinari, Emilio Hugues-Salas, George T. Kanellos, Reza Nejabati, Dimitra Simeonidou

Abstract—We demonstrate for the first time a trusted node free fully meshed metro network with dynamic discrete-variable quantum key distribution DV-QKD networking capabilities across four optical network nodes. A QKD-aware centralised SDN controller is utilised to provide dynamicty in switching and rerouting. The feasibility of coexisting a quantum channel with carrier-grade classical optical channels over field-deployed and laboratory-based fibres is experimentally explored in terms of achievable quantum bit error rate, secret key rate as well as classical signal bit error rate. Moreover, coexistence analysis over multi-hops configuration using different switching scenarios is also presented. The secret key rate dropped 43% when coexisting one classical channel with 150 GHz spacing from the quantum channel for multiple links. This is due to the noise leakage from the Raman scattering into the 100 GHz bandwidth of the internal filter of the Bob DV-QKD unit. When coexisting four classical channels with 150 GHz spacing between quantum and the nearest classical channel, the quantum channel deteriorates faster due to the combination of Raman noise, other nonlinearities and high aggregated launch power causing the QBER value to exceed the threshold of 6% leading the SKR to reach a value of zero bps at a launch power of 7 dB per channel. Furthermore, the coexistence of a quantum channel and six classical channels through a field-deployed fibre Test Network is examined.

Index Terms—Quantum Key Distribution (QKD), Optical Switching, Software Defined Networking, Quantum and Classical Channel Coexistence, Bandwidth Variable Transceivers

I. INTRODUCTION

Quantum communication networks present a revolutionary step in the field of quantum communication [1]. In the last two decades, quantum networks evolved from relayed point-to-point quantum communication links - with main focus in quantum security applications such as QKD - to multiserver quantum networks with partial or full connectivity beyond point-to-point links functioning in real life environment [2]. However, ultimately the goal of quantum communication is to provide a worldwide connectivity via complex networks – similar to the current internet – with an ultimate security based on the on the laws of physics rather than computational complexity [3]. The Quantum Internet vision is moving towards interconnecting seamlessly multiple nodes and enable applications beyond QKD such as blind and distributed quantum computing [4]. For such applications to reach their maximum capabilities, fully dynamic quantum networks [5] need to be deployed overcoming the relayed point-to-point quantum links approach and allowing the coexistence of classical and quantum channels over the same fibre in optical networks with the ability to switch between different nodes providing multi-hops connectivity.

QKD provides information-theoretic security by utilising quantum mechanics to encrypt and decrypt key information. Thus it can be regarded as the ultimate technology for physical layer communication security [1]. However, for QKD networks to become functional for the future Internet use cases such as 5G, the integration of QKD with classical optical networking infrastructure and adaptation the dynamic environment to the metro and edge part of optical networks are crucial; hence dynamic QKD could be considered as a potential security candidate for such networks [6].

Table I summarises the main features of the major QKD networks. Although the first field-trial of a QKD network was the DARPA QKD demonstrated in 2004 [7], it did not provide any practical implementation of the QKD system. The SECOQC was a subsequent demonstration of a QKD network aiming at implementing practical applications of the QKD technologies [8], [9]. Moreover, Tokyo QKD network was similar to the SECOQC in terms of infrastructure and was based on point-point links using trusted nodes topology. However, it included the implementation of the first Key Management Server (KMS) for centralised key management [10]. The most recent network demonstration is the integrated space-to-ground quantum communication network in China [11]. This QKD network consisted of a long-distance fibre backbone network and two satellite–ground links and four quantum metropolitan area network where the backbone link covers over 2000km. A trusted node–free eight-user metropolitan quantum communication using a polarisation-entangled photon source has been implemented in the city of Bristol [12].

Based on the coexistence of quantum and classical channels, several field-trials were undertaken in different parts of the world. The Cambridge-Ipswich QKD network was one of these demonstrations in which a COW DV-QKD system in the O-band (IDQuantique Clavis3 system [13]) was integrated with 5x100 G classical DWDM channels in the C-band. Having the quantum and classical channels in different frequency bands eliminates any challenge in coexisting. The QKD network consisted of five nodes on a bus topology where the three intermediate nodes were used as trusted nodes [14]. Other demonstration was the Cambridge Quantum Metro network consisting of coexistence between DV-QKD channels implementing a BB84 protocol with two decoy states and 2x100G classical DWDM channels on a single link. The network consisted of 3 nodes acting as trusted nodes forming in a ring topology [15].

Classical and quantum channels coexistence highly benefit from intelligent control of resources, and SDN is a
perfect technology to accomplish that. SDN automation in QKD networks since automatic provision of channels can be achieved on different parts of the network, based on real-time monitoring of quantum parameters. Efforts to implement the first automated switching of the quantum channel in an SDN-controlled QKD network were reported in [18], [19]. In [20], a real-time monitoring of QKD parameters in an SDN-controlled QKD network was used to switch the quantum channel into a different fibre route under a physical-layer attack mitigation experiment. In the Madrid Quantum Network, the demonstration of a dynamic Software-defined CV-QKD quantum network was undertaken using commercial optical switches [16], [17]. All of the previous mesh DV-QKD networks used trusted nodes or did not coexist quantum and classical channels in the same fibre. A trusted node is an intermediate node containing a pair of QKD devices, which establishes a connection between the original end-to-end QKD system. These nodes are used to extend the reach of the QKD system and to enable the distribution of secure keys between the end points. Having a pair of QKD devices allow the quantum generated keys to be extracted and XORed with the keys of the QKD system in the next node. Trusted node networks tend to use the same sender and receiver hardware at each intermediates nodes which add the cost prohibitively. Furthermore, since all the nodes in the network including intermediate trusted nodes are assumed to be safe from eavesdropping, any access to a trusted node cause a potential security risk and relinquish the strong security offered by quantum cryptography [21]. Therefore, a trusted node free network does not only reduce the cost tremendously but also require less equipment and maintenance. To this end, we have recently demonstrated an end-to-end quantum-secured inter-domain 5G service orchestration over a dynamically-switched optical network [19]. Also a 5G network slicing with QKD using a SDN orchestrator has been verified in [22]. However, the dynamic QKD approach requires investigations in deployed optical fibre networks and aiming at this research, we have demonstrated a first field trial of a fully-meshed network with dynamic QKD networking capabilities across four nodes in the 5GUK testbed in Bristol [5].

In this paper, we present the first dynamic trusted-node free fully-meshed DV-QKD network in a field trail (in 5GUK deployed fibre in Bristol) as well as laboratory-based testbeds for extensive analysis of quantum impairments considering the coexistence of carrier-grade classic channels and a quantum channel over switched network. Coexistence over multiple-hops using OXC switches and a comparison between different switching scenario are also presented. Additional findings of the coexistence over the deployed links of the 5GUK network are also evaluated. Moreover, new results of the SDN control implementation are also included in this communication. This paper is organized as follows: in Section II we discuss the overall network architecture. In Section III-A we discuss the experimental system setup for the dynamic QKD network laboratory testbed followed by Section III-B where we discuss the SDN control plane implementation. In Section IV we present the results of the data and control plane and finally, in Section V we conclude the paper.

II. Network Architecture

This section describes the overall network concept used in this paper. As shown in Fig. 1 the network is divided into control and data planes. The control plane contains the SDN controller and the required connectivity to the data plane equipment whereas the data plane represents the optical fibre infrastructure, optical equipment and QKD-related devices.

The SDN controller is responsible for the computation, creation, and management of the complete path that traverses optical and SDN switches between the nodes. The SDN Controller is individually controlling the switches, QKD terminals, and encryption/application server in each node to create secure channels. The SDN controller utilises a quantum aware path computation mechanism, that calculates the best path for QKD and classical channel including power and losses, for minimal effect on the quantum channel. The SDN controller is also responsible for the establishment and management of paths that traverses between the nodes, including both classical and quantum channels and requires an L2 network to communicate with the data plane devices.

To be able to perform the aforementioned tasks, the controller requires some essential components, such as databases to store network data (e.g. routing and connection tables), driver modules needed to control multiple different vendor devices, communication modules that understand different protocols (e.g. gRPC and Netconf), and finally intelligent algorithms that could use both heuristics or machine learning to optimise the usage of the network resources.

Next, on the data plane, each node is composed by several components, including but not restricted to, optical switches, transponders, QKD equipment, data encryptors, computational servers, and filtering devices. Sharp filters are required to partly isolate the noise generate from the high power classical channels (orders of magnitude higher than quantum channels)
to provide a sufficient isolation for the quantum channel; hence improving its performance.

The computational units host the software needed to communicate and control the equipment, including the Key Management System (KMS). The KMS is an entity that manages keys in a network in cooperation with one or more other KMS. When new cryptographic keys are generated by a QKD device, the keys are securely stored in a database (also called as key store) managed by the KMS. Such key stores provide a "key buffer" within the network, effectively decoupling the key generation process from the key consumption applications, allowing greater tolerance to bursts of key usage as also to temporary unavailability of the key-generation devices. Additionally, the KMS is responsible for monitoring and recording the usage and generation of keys, thus providing valuable statistics that can be used by the SDN controller. In the next section we describe the implementation of this architecture, as we describe the experimental setup.

III. Experimental System Setup

A. Data Plane

Fig. 1 shows the fully-meshed network used to demonstrate the dynamic QKD-networking. The network comprises four nodes interconnected via standard multiple single-mode fibre (SSMF) links. Each node is equipped with optical cross-connects (OXC), a bandwidth variable transponder (BVT), a QKD device, an encryption unit, data servers and a secure server. The testbed was designed to provide flexibility enabled by the SDN Controller. It is possible to transmit classical data using the BVT, coexisting or not with the quantum channel, while it is also possible to transmit encrypted data. This section describes the testbed in details.

The BVT includes four ports at 100 Gbps (25 Gbaud) data rate each with PM-QPSK modulation format. Each of the ports can be tuned to any of the 100 wavelengths in the C-band included in the ITU-T grid with 50 GHz offset. The QKD unit used is a commercially available IDQ Clavis2 DV-QKD system with an auto compensating interferometric setup and quantum random number generators (QRNGs) to create secret keys. These Clavis 2 systems support fully automated sifting for the BB84 protocols and key distillation. The last equipment included in each node is a software encryption unit Dell PowerEdge server, responsible for the software encryption and used to secure the user data transmission with AES – 256 encryption.

As shown in Fig. 1 in Node 1 and Node 2, the four coherent output ports of the BVT are coupled using a 1x4, 6-dB coupler, for a total throughput of 400 Gbps. A controllable q-ROADM is used to enable classical data channels and QKD signal routing and switching functionality. The q-ROADM provides low loss switching capability for the quantum channel due its 10 dB limited power budget and it consists of the filtering...
stages and the OXC devices \[19\]. The output is again coupled via a 95/5 ratio and insertion loss of 13 dB for the 5% port used to enable low power loss in the quantum channel. The second port of this 95/5 coupler is used to exchange the encoded photons of the discrete-variable DV-QKD Alice unit considering a power loss of less than 0.5 dB for the 95% port. The output of the 95/5 coupler is connected to the OXC and the coexisting QKD and classical signals are injected into the optical link via the suitable cross-connection. The OXC used is a SDN-enabled optical fibre switch with typical optical losses per cross-connection of 1 dB.

In these nodes, the encryption server will interface to the IDQ Clavis 2 unit for the QKD protocol and an optical output of 10 Gbps data rate will transport the encrypted data towards the optical link via the OXC. In Node 3 and Node 4, the OXC will cross-connect the incoming coexisting signal to an optical band pass and rejection (stop) filter (BPRF) with 0.8 dB of loss for the band pass port, before connecting to the the IDQ Clavis 2 Bob unit. The band pass port of the BPRF has an optical bandwidth of 100 GHz centered at the 1551.7 nm wavelength of the QKD units. For the rejection port of the BPRF, the quantum channel is blocked and the combined classical signals are optically amplified by an erbium-doped fibre amplifier (EDFA) to boost the optical power to an acceptable level for detection. The output of the EDFA feeds a 1x4, 6 dB splitter and its four different optical ports are each connected to a coherent receiver of the BVT. Finally, in these nodes, the decryption server will extract the data received after processing the key. Table II summarises the main parameters of the implemented fully-meshed QKD dynamic network.

### B. Control Plane

As Fig. 1 shows, each node has several components that need to be monitored and controlled by the SDN controller. To provide connectivity between the SDN controller and all the controllable devices in our deployed network we devised a supporting management network. One particular component is the Secure Server, that connects to L2 switches and other Secure Servers (using 10 Gbps SPFIs), thus accounting for the control plane logical and electrical connections described in Fig. 1.

The Secure Servers also host the Key Manager System (KMS) that doubles down as a key database and as an agent to manage and control the QKD devices. The KMS software of choice was the CQP Toolkit, developed in-house \[23\]. Additionally, the Secure Servers also hosts the OXC agent and the encryption unit agent.

As can be seen in Fig. 1, Node 1 also hosts the SDN controller used in our testbed, in addition to all the described components. The SDN controller is responsible for the establishment and management of the complete path that traverses the optical SDN switches between the nodes. It can handle paths for the quantum channel, classical channels, and coexisting QKD and Classical channels. Additionally to the switches, the QKD terminals and the encryption units are also controlled.

In the current controller state, the routes are calculated offline using the network information and then uploaded to the controller. This network information includes the OXC ports, link connections and losses, and available routes. Therefore, the path assignment consists in selecting the most suited route available for the incoming request (e.g. fibres with smaller losses for a quantum channel). Classical channels can be established between any two nodes and quantum channels between any two matching devices (i.e. one Alice and one Bob) as per the user’s request.

Fig. 2 summarises the flow when a new request arrives to the SDN controller. The start connection request identifies a source and a destination site and retrieves all the information pertaining to that particular pair from the routing table. This information includes the cross connections (e.g. OXC’s input and output ports) needed to fulfil the path between sites. The SDN controller utilises the information to install the flow rules in the OXC.

After the OXC devices are configured, the controller issues the start QKD message towards to the KMS agents, triggering the start of the key generation process. Thereafter, the monitoring of the Quantum Bit Error Rate (QBER) starts, raising an event within the controller in case there is a deviation the QBER values. If the QBER is below a QBER threshold (6% by default), it is deemed as acceptable and the encryption unit is set to initiate the encryption software, creating an encrypted tunnel between the endpoints. However, if at any moment the QBER monitored is above the threshold, the current quantum

### TABLE II: Parameters for Dynamic QKD Networking Testbed

| Parameters                          | Value                          |
|-------------------------------------|-------------------------------|
| Number of Channels                  | 4                             |
| Classical Channel                   | 1550.52 nm, 1550.12 nm,       |
| Wavelengths                         | 1549.72 nm, 1549.32 nm         |
| Classical Channel Frequency         | 193.35 THz, 193.40 THz,        |
| Frequencies                         | 193.45 THz, 193.50 THz         |
| Grid Spacing                        | 50 GHz                         |
| Modulation Format                   | PM-QPSK                        |
| Optical Signal-to-Noise Ratio       | 20 dB                          |
| Capacity per Channel                | 100 Gbps                       |
| Total Capacity                      | 400 Gbps                       |
| Pre-FEC Level                       | 15%                            |
| Detector sensitivity*               | -35 dB                         |
| EDFA                                |                                |
| Noise Figure                        | 5 dB                           |
| Operation Mode                      | Continuous optical power       |
| Encryption technique                | AES-256                        |
| Encryption data rate                | 10 Gbps                        |
| Optical band pass/Rejection Filter  |                                |
| Insertion loss                      | 0.5 dB                         |
| band pass port                      |                                |
| Center wavelength                   | 1551.7 nm                      |
| band pass port                      |                                |
| Bandwidth band pass port            | 100 GHz                        |

*Corresponding to PM-QPSK Modulation @100 Gbps and back-to-back
channel quality is noted as unsatisfactory and therefore the controller proceeds to fetch the next available route in the routing table connection and the aforementioned process starts again.

Once the whole system is running, the quantum keys are generated by the IDQClavis2 and stored on databases managed by the KMS system. In addition to the KMS, CQPToolkit software suite also encompasses an interface to control the Clavis devices and an encryption application. This controlling interface allows the SDN controller to start/stop IDQClavis2 devices and subsequently to request statistics to monitor the quantum channel parameters. All communication between CQPToolkit and the SDN controller is done using gRPC as communication protocol. As encryption application, CQPToolkit suite ships with the QTunnelServer software which implements one solution to the problem of sending encrypted data from one site to another. It creates an encrypted tunnel thus allowing secured data transfer by using AES-256 encryption.

IV. RESULTS
A. Results of the Fully-Meshed Dynamic Network without Coexistence

Table III shows the main parameters of the dynamic QKD network of Fig. 1. The parameters of the optical fibre links are described such as fibre lengths and end-to-end power losses. Also, Table III depicts the number of cross-connections per link required for dynamically switch to the quantum channel requested. The quantum parameters of quantum bit error rate (QBER) and secret key rate (SKR) are represented in this table without coexisting with classical channels. In addition, the combination of links for multihop scenarios is included to show the performance of the dynamic QKD network without coexistence. As observed, the link L1 with the lowest power budget (5.19 dB) achieves the lowest QBER of 1.02% and highest SKR of 2575.69 bps. However, for the combination of L3 and L4, with the highest power budget of 10.62 dB and three crossconnections, results show a QBER of 4.51% and a SKR of 194.16 bps, being at the power budget limit of the QKD system used.

B. Results of the Fully-Meshed Dynamic Network with Coexistence

To investigate the effect of Raman noise over the DV-QKD channel, the testbed of Fig. 1 is used considering links L1, L2, L3 and L4 and one classical channel centered at the frequency of 193.35 THz with 150 GHz spacing from the quantum channel. Fig. 3a shows the measured SKR and QBER of the quantum channel at different launched optical power levels of the classical channel. As observed, when the launching power is more than 1 dBm, the QBER and SKR deteriorate due to the noise leakage into the 100 GHz bandwidth of the internal filter of the Bob DV-QKD unit. Moreover, the close QBERs achieved by the DV-QKD channel over all the links reflect the small variation of optical attenuation of 2 dB for each link. In addition, at the BVT highest possible launch power of 9 dB, the lowest SKR achieved is 350 bps with continuous key generation for link L4. Fig. 3b shows the impact of coexisting four classical channels (193.35 THz, 193.40 THz, 193.45 THz and 193.50 THz) over the quantum channel (193.20 THz). As observed from Fig. 3a, the quantum channel deteriorates faster compared to Fig. 3a due to the combination of Raman noise and other nonlinearities. Considering the two frequencies 193.35 THz and 193.50 THz as f1 and f2 respectively, one product of the four wave mixing would be f3 = 2f1 − f2 = 193.20 THz which is the quantum channel frequency which degrade the performance of the quantum channel due to the additional noise from such phenomena. Therefore, more noise leakage into the Bob DV-QKD unit occurs due to higher aggregated launch power (16 dB when transmitting four classical channels at 9 dB), higher Raman noise and other nonlinear effects such as four wave mixing. It also observed that at a launch power of 7 dB per channel, the QBER values exceed the threshold of 6% causing the SKR to be zero bps.

Fig. 3c and Fig. 3d show the SKR and QBER over the combined links of L1+L2 and L1+L3. In both figures, increasing the number of classical channels is presented to reflect the impact of incremental channels over the quantum channel. As observed, similar trends of QBER and SKR deterioration...
appear for both cases of links due to the optical power budgets in the vicinity of 8 dB. Also, it is clear in both links that by adding a classical channel, the total aggregated power is increased and the Raman noise effect is proportional to the power added, worsening the quantum channel performance. It can also be observed that the QBER values exceed the threshold of 6% causing the SKR to be zero bps at a launch power of 5 dB per channel which is different comparing to Fig. 3b. This is due additional losses of links L1+L2 and L1+L3 and the additional cross-connection in the optical

Fig. 3: (a) Coexistence of quantum channel and one classical channel ($F_c 193.35 \text{THz}$) for four different links. (b) Coexistence of quantum channel and four classical channels for four different links. (c) Coexistence of quantum channel and four classical channels for link L1+L2 (d) Coexistence of quantum channel and four classical channels for link L1+L3

Fig. 4: (a) Coexistence of quantum channel and six classical channels in a 1.9 km field-deployed fibre (HPC-WTC) (b) Coexistence of quantum channel and six classical channels in a 2.7 km field-deployed fibre (NSQI-WTC)
C. Coexistence over Bristol City 5GUK Testbed

To further explore the coexistence of a DV-QKD channel with classical carrier-grade channels, two links of the Bristol City 5GUK testbed were used [5]. One link connects the site HPN to the WTC node, with a fibre length of 1.9 km total optical fibre attenuation of 4.68 dB. The other link interconnects the sites NSQI to the node WTC passing through the node HPN (2 hops) with a fibre length of 2.7 km total optical fibre attenuation of 5 dB. Fig. 4a shows the QBER and SKR for the link HPN-WTC. A quantum DV-QKD channel coexisted with 6 PM-QPSK 100 Gbps channels with 50 GHz spectrum space difference between them (from 193.5 THz to 193.75 THz). To evaluate the performance of the coexistence over these channels, the bandwidth of the optical band pass filter of Section III is tuned to gradually allow noise proliferation into the quantum channel. As observed, when the filter bandwidth is in the range of 500 GHz to 725 GHz, the SKR obtained is higher than 890 bps and the QBER is lower than 2.8%. However, for filter bandwidths higher than 750 GHz, the noise leakage over the quantum channel will impede the key generation due to high QBERs of more than 5.9% causing the SKR to plummet to zero bps. For the classical channels, the BER measured was $3.5 \times 10^{-9}$ average for the channels selected. Fig. 4b shows the QBER and SKR curve with respect to the filter bandwidth for the link NSQI-WTC. Compared to the link HPN-WTC (Fig. 4a), the SKR and QBER obtained degrade faster. This is due to the additional crossconnection for the extra hop in the link which increases the power budget of the link.

V. Conclusion

We have demonstrated for the first time a trused node free dynamic QKD networking implementation over a testbed that spanned across four optical nodes interconnected in mesh topology. The coexistence of a DV-QKD channels and $4 \times 100$ Gbps classical channel was successfully demonstrated over multiple links with the ability to switch between the links using a centralised SDN controller. For the coexistence over the longest link (L3) with 5.8km, a minimum QBER of 2.7% and a maximum SKR of 650 bps was demonstrated for the DV-QKD simultaneously with a minimum average pre-FEC BER of $1.28 \times 10^{-8}$ for the error free classical channels. Investigations also prove that when coexisting four classical channels with 150 GHz spacing from the quantum channel, a minimum power of 7 dB per channel is required to deteriorate the key generation process with a SKR of zero bps. Moreover, this work also demonstrated the coexistence of a quantum channel and six classical channels through a field-deployed fibre in the 5GUK Test Network. The key generation process is maintained when the bandwidth of the optical band pass filter which is centred at 193.625 THz and is lower than 750 GHz. When the filter bandwidths is tunned to higher than 750 GHz, the noise leakage over the quantum channel will impede the key generation due to high QBER of more than 6% causing the SKR to plummet to zero bps.

ACKNOWLEDGEMENT

This work acknowledges the EU funded project UNIQORN (820474), the EPSRC EP/T001011/1: UK QHub for Quantum Communications, and Facebook for the Voyager switches utilised in the experiment.

REFERENCES

[1] S. Pirandola et al., “Advances in quantum cryptography,” Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, 2020.
[2] M. Mehic et al., “Quantum key distribution: a networking perspective,” ACM Computing Surveys (CSUR), vol. 53, no. 5, pp. 1–41, 2020.
[3] S. Valerio et al., “The security of practical quantum key distribution,” Rev. Mod. Phys., Sep 2009.
[4] R. V. Meter et al., “The path to scalable distributed quantum computing,” Computer, vol. 49, no. 9, pp. 31–42, 2016.
[5] 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,” in 45th European Conference on Optical Communication (ECOC 2019). IET, 2019, pp. 1–4.
[6] D. Zavitsanos et al., “On the qkd integration in converged fiber/wireless topologies for secured, low-latency 5g/h5q fronthaul,” Applied Sciences, vol. 10, no. 5, p. 5193, 2020.
[7] C. Elliott et al., “Current status of the darpa quantum network,” in Quantum Information and computation III, vol. 5815. International Society for Optics and Photonics, 2005, pp. 138–149.
[8] M. Peev et al., “The secqoe quantum key distribution network in vienna,” New Journal of Physics, vol. 11, no. 7, p. 075001, 2009.
[9] A. Poppe et al., “Outline of the secqoe quantum-key-distribution network in vienna,” International Journal of Quantum Information, vol. 6, no. 02, pp. 209–218, 2008.
[10] M. Sasaki et al., “Field test of quantum key distribution in the tokyo qkd network,” Optics express, vol. 19, no. 11, pp. 10387–10409, 2011.
[11] Y.-A. Chen et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” Nature, pp. 1–6.
[12] S. K. Joshi et al., “A trusted node-free eight-user metropolitan quantum communication network,” Science advances, vol. 6, no. 36, p. eaba0959, 2020.
[13] Id quantique clavis3 qkd platform. [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/clavis3-qkd-platform-rd
[14] A. Wonfor et al., “Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x 100g dwdm transmission system,” in 45th European Conference on Optical Communication (ECOC 2019). IET, 2019, pp. 1–4.
[15] J. Dynes et al., “Cambridge quantum network,” npj Quantum Information, vol. 5, no. 1, pp. 1–8, 2019.
[16] V. Martin et al., “The madrid quantum network: A quantum-classical integrated infrastructure,” in Photonic Networks and Devices. Optical Society of America, 2019, pp. QW3E–5.
[17] A. Aguado et al., “The engineering of software-defined quantum key distribution networks,” IEEE Communications Magazine, vol. 57, no. 7, pp. 20–26, 2019.
[18] R. Nejabati et al., “First demonstration of quantum-secured, inter-domain 5g service orchestration and on-demand tsv chaining over flexi-wdm optical networks,” in Optical Fiber Communication Conference. Optical Society of America, 2019, pp. Th4C–6.
[19] R. Wang et al., “End-to-end quantum secured inter-domain 5g service orchestration over dynamically switched flex-grid optical networks enabled by a q-roadmap,” J. Light. Technol., vol. 38, no. 1, pp. 139–149, 2019.
[20] E. Hugues-Salas et al., “Monitoring and physical-layer attack mitigation in sdn-controlled quantum key distribution networks,” IEEE/OSA Journal of Optical Communications and Networking, vol. 11, no. 2, pp. A209–A218, 2019.
[21] Q. Zhang et al., “Large scale quantum key distribution: challenges and solutions,” Opt. Express, vol. 26, no. 18, pp. 24260–24273, Sep 2018.
[22] P. Wright et al., “5g network slicing with qkd and quantum-safe security,” Journal of Optical Communications and Networking, vol. 13, no. 3, pp. 33–40, 2021.
[23] Richard Collins. CQPToolkit: A QKD toolkit library, University of Bristol, Bristol, UK, 2018. [Online]. Available: https://github.com/QComms