Optical Network Architecture Supporting Dynamic and End-to-End Quantum Secure Networking

Reza Nejabati, Rui Wang, George T. Kanellos, Dimitra Simeonidou

HPN Group, Smart Internet Lab, University of Bristol, UK, reza.nejabati@bristol.ac.uk

Abstract This paper proposes an optical network architecture including physical layer and control plane supporting dynamic networking and co-existence of quantum and classical channels over the same fibre infrastructure. It will discuss technological challenges for realising the proposed architecture and potential solutions for addressing them.

Introduction

No cloning principle of quantum physics makes it impossible to create an identical copy of an arbitrary unknown quantum state. This has a profound impact in the field of network security and has been the founding principle for quantum secure communication as the ultimate network security solution.

Over the past two decades quantum secure transponder technologies and various quantum key distribution (QKD) protocols have been studied by research communities [1] with some commercial products are becoming available. So far, most efforts have been dedicated to developing technologies for point-to-point QKD links using dedicated fibre, satellite, or optical wireless links [2-4].

Despite the existing progress, still there is a need for significant research to develop solutions that allow deployment of quantum security in a dynamic networking scenario. It is until then that we can claim quantum security is a realistic physical layer security solution for the Internet infrastructure.

This paper aims to discuss an optical network architecture supporting dynamic end-to-end quantum secure communications. It will also discuss challenges and the required technologies for realising such an architecture.

Architecture

An architecture blueprint for a dynamic optical network supporting quantum secure communication is shown in Fig. 1, including physical layer connectivity and a control and management plane. Similar to a classical optical network, it includes access quantum secured network, metro quantum secured network and core quantum secured network. It is aimed to provide quantum secured communications in existing fibre infrastructure with various physical layer connectivity ranges and different QKD technologies. Importantly, in this architecture quantum channels can be transported over a dedicated fibre link or in co-existence with classical channels sharing the same fibre.

Physical layer

In access quantum secured networks, due to its short range both Continuous Variable-QKD (CV-QKD) [5] and Discrete Variable QKD (DV-QKD) [6] techniques can be deployed in a star-like topology to encrypt the classical point-to-point communication link, such as QKD over PON [7].

At the metropolitan regional level, an optical mesh [8] or ring metro [9] quantum network interconnects several small access networks, to enable the quantum key distribution and key exchange between them. The border nodes between the access network and metro network not only originate and terminates the quantum signal, but may also support dynamic routing for both quantum and classical channels co-existing in the same fibre. This can be achieved by utilising a quantum-enabled reconfigurable optical add and drop multiplexer (q-ROADM).

In small metro or access quantum secured networks with fibre span of less than 50km both CV-QKD and DV-QKD can be deployed but for large metro network with long fibre spans DV-QKD technique will be a suitable technology [3].

At the national or regional level, an optical mesh core quantum secured network interconnects multiple metro quantum secured networks. Such a network must support dynamic high key-rate QKD links with quantum enabled optical switches such as q-ROADMs. Furthermore, it is anticipated that the q-ROADM in a core network must have low-loss characteristics, posing a limited even negligible impact to the reach distance of the QKD system. Quantum repeaters may also be required to extend the ranges of the existing quantum system.

Quantum repeaters are at their early stage of the development with most of the existing research are focusing on their theory. In the absence of quantum repeaters, some of the network nodes (e.g. q-ROADMs) can also act as trusted nodes to extend the reach distance for large-scale core quantum networks. These nodes not only can facilitate end-to-end quantum secure communication for long distances but also can

978-1-6654-3868-1/21/$31.00 ©2021 IEEE

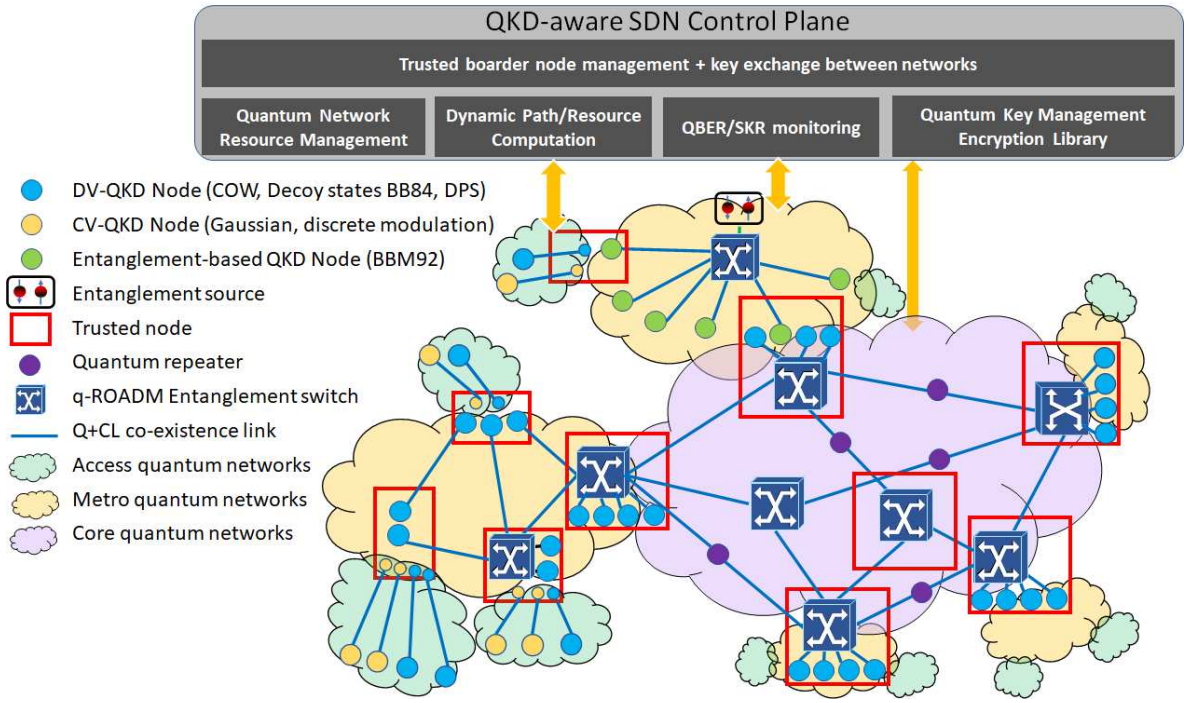

Fig 1. Optical network architecture supporting dynamic QKD networking

act as a gateway or boarder nodes interconnection multiple domains each utilising their own QKD protocol. The trusted nodes perform the relay-function for p2p QKD systems and can be co-located with amplifiers for classical signals and or optical switching nodes in long-haul fibre links.

Entanglement-based quantum networking

In a high-density network with high degree of connectivity between end points, DV-QKD or CV-QKD techniques won't be efficient. They require large number of quantum transponders and complex network management to support simultaneous secure communication between any two end points. Instead, entanglement-based networking scheme, can efficiently support large-scale QKD networks, interconnecting multiple nodes simultaneously or even new schemes of quantum conference key agreements [17].

Quantum entanglement is a property in which the quantum states of two or more particles, e.g. photons, are highly (perfectly) correlated, even when they are separated by a large distance. When two photons are entangled, measurements performed on one photon will instantaneously influencing the other one. This property can be utilised to create a resource efficient QKD network. A broadband entangled photon source[10] together with a suitable QKD protocol such as BBM92 [11] can be utilised to create entangled pair of wavelengths for establishing quantum secure channels between any pair of end nodes (users) in a network. In an entanglement-based quantum network, the physical layer consists of several end points connected to a single entanglement source in a star topology [12]. When two users share different halves of the entangled state, they share entanglement and can use it as a QKD channel. The effort is now shifted towards active entanglement distribution for dynamic allocation of the photon-pairs that create the QKD links [13].

q-ROADM

A dynamic quantum secured network should support the switching of both classical data channels and QKD channels that may co-exist in the same fibre. The conventional ROADM designed for switching classical data channels with relatively large insertion loss is not feasible for QKD channel switching. Apart from high loss, the ASE noise generated from pre-amplifiers and post-amplifiers of the ROADM would fall into the quantum channel, posing a significant challenge to the QKD receiver.

To overcome these drawbacks and since QKD systems operate at single/few photons level, a q-ROADM must be able to operate at low loss switching regime. It should also include tuneable flexi grid wavelength selective switching (WSS) with very high Q factor filtering capability to allow dynamic and independent switching of quantum and classical channel from any incoming fibre to any outgoing fibre. For quantum and classical channels co-existence scheme, the q-ROADM needs to amplify only classical channels while

allowing high-extinction filtering of out-band noise to prevent ASE noise in quantum channels. Internal architecture of the switch must also allow perseveration of polarization of quantum channels. This is especially important for polarisation-entanglement-based QKD networks. Fig 2. shows two possible variations of q-ROADM architecture proposed by authors, supporting (a) DV-QKD [14], and (b) polarisation entanglement-based quantum networking [15].

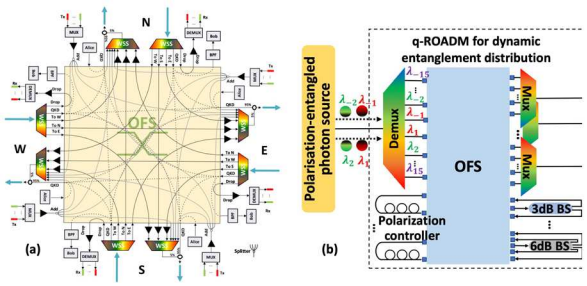

Fig 2. q-ROADM architecture supporting (a) DV-QKD; (b) polarisatio- entanglement-based QKD.

Control and management plane

A quantum secured optical network, as depicted in Fig. 1, is a heterogeneous network comprising a mixture of quantum and classical communication technologies often from different vendors. Such a network architecture requires multi-technology and vendor agnostic control and management mechanisms. As such, a control plane utilising software-defined networking (SDN) technology is the most suitable solution. There have been large body of works reporting on SDN controller architectures and functionalities for optical networks. Recent efforts of the international community [ETSI, ITU] have managed to propose standardised interfaces for connecting QKD equipment to the SDN controllers. A SDN controller supporting quantum security requires extra functionalities and capabilities in order to be QKD aware and support provisioning of quantum secured optical connectivity services [14]. A QKD-aware SDN controller for the quantum network should be able to support quantum key management, monitoring of Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR). More importantly, it should support path computation and co-optimization of channel spacing between quantum and classical channels, supporting their co-existence in the same fibre in a dynamically switched optical network. Finally, it should be able to coordinate trusted border nodes (gateway nodes) to enable key exchange between different network domains with different QKD protocols as well as facilitating end-to-end secured connectivity for long distances.

Algorithms and intelligence

One of the main functionalities of a QKD aware SDN controller is end-to-end path computation for both quantum and classical channels. In addition to impairments introduced by q-ROADM such as loss and crosstalk, impairments introduced by classical channels due to fibre nonlinearities such as four-wave mixing, and Raman noise can have significant adverse effect on quantum channels. These issues make the path computing a very complex algorithm. Additionally, since quantum channels behave according to quantum mechanics principles, existing impairments-aware heuristic and analytical algorithms or models cannot be utilised for path computation. The problem become even more complex in entanglement-based network where combination of a broadband entanglement source and q-ROADM enable flexible creation QKD channels between any pairs of end nodes in the network.

One possible solution to overcome this complexity, is development of path computing algorithm utilising supervised machine learning techniques such as artificial neural networks and regression techniques.

Recent study by authors has shown Random Forest regression techniques is a suitable method for path computation and especially for wavelength allocation and minimizing channel spacing between quantum and classical channels in the fibre[16] for a DV-QKD network. Further study by authors has shown deep neural network with 5 hidden layers is a suitable candidate to predict the quantum link performance for path computation and wavelength allocation in an entanglement-based QKD network [15].

Conclusions

Any realistic solution for deployment of internet-wide quantum security requires architecture and technologies that can facilitate the deployment of quantum security in dynamic optical network and in co-exitance with classical optical communication. This paper discussed an optical network architecture for such an end-to-end dynamic quantum secure optical networking. It also provided insight about associated technical challenges and the required technologies for realisation of the proposed architecture.

Acknowledgements

We acknowledge support from Engineering and Physical Science Research Council (EPSRC), UK National Quantum Technologies Programme, Quantum Communications Hubs EP/T001011/1 and EU funded project UNIQORN (820474).

References

[1] Pirandola, Stefano, et al. "Advances in quantum cryptography." Advances in Optics and Photonics 12.4 (2020): 1012-1236.Fdds

[2] Liao, SK., Yong, HL., Liu, C. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nature Photon 11, 509–513 (2017).

[3] Lucamarini, M., Yuan, Z.L., Dynes, J.F. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 557, 400–403 (2018).

[4] Liao, SK., Cai, WQ., Liu, WY. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017)

[5] S. L. Braunstein, and P. Van Loock, “Quantum information with continuous variables,” Rev. Mod. Phys. 77, 513 (2005)

[6] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Int. Conf. on Computers, Systems & Signal Processing, Ban98 galore, India, Dec 9-12, 1984. Also at Theor. Comput. Sci. 560, 7 (2014)

[7] Fröhlich, B., Dynes, J., Lucamarini, M. et al. Quantum secured gigabit optical access networks. Sci Rep 5, 18121 (2016).

[8] 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," 45th European Conference on Optical Communication (ECOC 2019),

[9] Dynes, J.F., Wonfor, A., Tam, W.W.S. et al. Cambridge quantum network. npj Quantum Inf 5, 101 (2019).

[10] Fan, Jingyun, and Alan Migdall. "A broadband high spectral brightness fiber-based two-photon source." Optics express 15.6 (2007): 2915-2920.

[11] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” Phys. Rev. Lett. 68, 557 (1992).

[12] S.K. Joshi, et al, ‘A trusted node–free eight-user metropolitan quantum communication network’, Sci. Adv., Vol. 6, no. 36, Sep. 2020.

[13] Lingaraju, Navin B., et al. "Adaptive bandwidth management for entanglement distribution in quantum networks." Optica 8.3 (2021): 329-332.

[14] 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-ROADM’, J. Light. Technol., vol. 38, no. 1, pp. 139–149, Jan. 2020.

[15] R. Wang et al., ‘AI-Enabled Large-Scale Entanglement Distribution Quantum Networks’, in Optical Fiber Communication Conference 2021, (Optical Society of America, 2021), paper Tu1I.4.

[16] Y. Ou et al., "Field-Trial of Machine Learning-Assisted Quantum Key Distribution (QKD) Networking with SDN," 2018 European Conference on Optical Communication (ECOC), 2018.

[17] M. Proietti et. al “ Experimental quantum conference key agreement.” In: Science Advances. 2021 ; Vol. 7, No. 23.