Quantum Secured Control Plane Communications

Carlos Rubio García[1], Idelfonso Tafur Monroy[1], J.J. Vegas Olmos[2], Simon Rommel[1]

[1] Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, The Netherlands

[2] Software Architecture, NVIDIA Corporation, Yokneam, Israel

In current networks, the security of critical information depends primarily on a mix of conventional public key encryption (PKE) whose security is based on very complex mathematical models. Nonetheless, as proven by Shor's algorithm, the rapid development of quantum computers is seriously threatening PKE schemes. This is something that exposes new security issues on Software Defined Networks (SDN), where the control plane is separated from the data plane. Since the behavior of the network is based on the information collected and transmitted by the control plane, it is of high importance that these communications remain secure against any attacker. This paper explains the problem that SDN networks are facing in the advent of quantum computers and the reason why quantum key distribution (QKD) and post-quantum cryptography (PQC) need to be combined for enabling quantum secured control plane communications. Finally, we describe a user scenario in which a strategy is proposed for integrating QKD and PQC into the control plane.

Introduction

Over the last few years, there has been an unexpected growth in quantum technologies. The need for more powerful machines in some areas of research is leading the industry to strongly push for the development of quantum computers [1]. In such a case, current cryptography algorithms will no longer be secure. The development of Shor's polynomial-time algorithms for prime factorization and discrete logarithms transform problems that were thought to be hard for classical computers, into something doable with a mature-enough quantum computer [2]. The National Institute of Standard and Technology (NIST) predicts that by 2030, a quantum computer built with a budget of around 1 billion dollars will be able to break 2000-bit Rivest-Shamir-Adleman (RSA) cryptography. Moreover, this report also predicts that by 2036, sufficiently large quantum computers will be able to break all public key schemes that are currently in use within communication systems [3], [4]. The reason to address this now is commonly known as the "harvest now, decrypt later" problem, in which a quantum-mature adversary can collect encrypted versions of long-lived private information to decrypt it later in the future. This implies a critical need for implementing quantum-safe communications [4].

Software Defined Networks

Increasingly demanding cloud services, network virtualization and Internet of Things (IoT) applications demand service providers to develop new services that can keep up with high quality of service (QoS) requirements [5]. While this is rather difficult to do in conventional network architectures [6], Software Defined Networking (SDN) has emerged as the network paradigm that provides the programmability and flexibility long needed. As depicted in Fig. 1, since the behavior of the network is logically centralized in an entity called SDN controller, service providers can easily manage, configure and optimize network resources with dynamic, automated and open-source programs [5]. SDN is enabled by four key features [6]:

- Separation of control plane from the data plane
- Centralized controller that has a global view of the network
- Open interfaces between the control plane (controller) and the data plane (network devices)
- Programmability of the network by external applications

Although SDN allows more simple, flexible and dynamic network deployments, there are also several challenges that need to be addressed, such as performance, scalability, security and interoperability. While all of them are of capital importance, this paper focuses on the security vulnerabilities of SDN. We propose a strategy on how to augment the security of the SDN control plane communications by means of QKD, and thus, explain how SDN can remain secure in the advent of quantum computing.

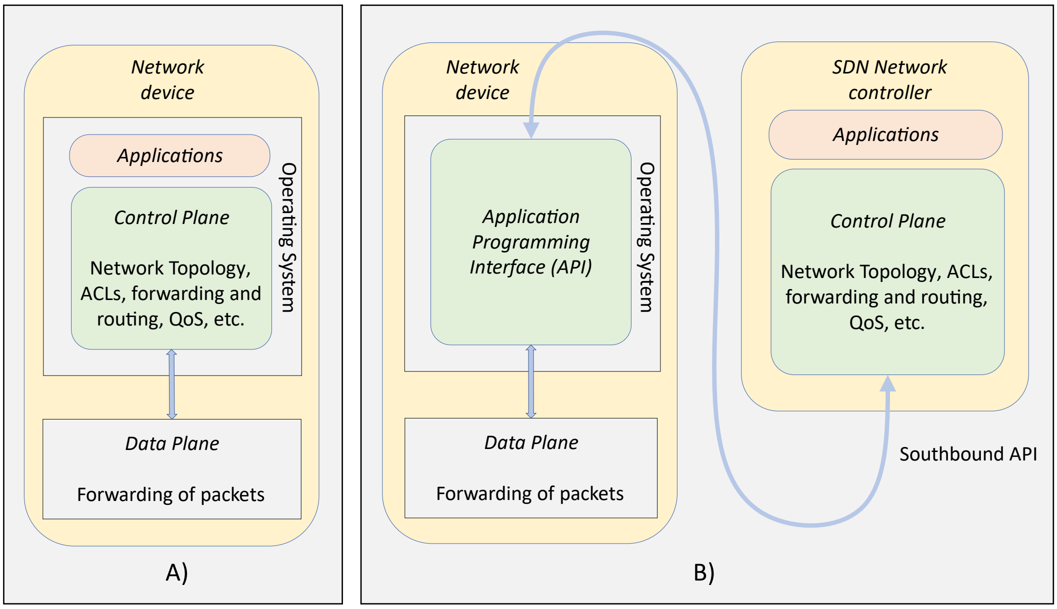

Figure 1. A) Traditional control approach; B) SDN control approach [6].

Quantum Key Distribution

A solution to overcome this challenge is by employing Quantum Key Distribution (QKD). This technology allows establishing a secure communication channel whose security is guaranteed by the laws of quantum physics, instead of a challenge on how to solve a complex mathematical problem. Due to the uncertainty principle and the no-cloning theorem, the observation of a quantum signal causes a perturbation in its state. That means, if a third party (Eve) wants to obtain any information about the message exchanged in the quantum channel, it causes a perturbation to the sequence of qubits, which changes its final state. After the transmission of the encoded message, both transmitter and receiver can estimate how much of the message has been leaked. If the difference between the first and final state of the qubits surpasses a certain threshold, the secret quantum key cannot be distilled. The fact that the integrity of the messages can be guaranteed following quantum physics suggests the unconditional security of the messages, independently of Eve's computational resources [7].

Architecture of quantum secured networks

It is vital that the introduction of quantum technologies in the data plane can coexist with current optical infrastructure. As it happens with traditional equipment, QKD networks need an effective management and control plane that can coordinate the QKD resources, support the dynamic allocation of quantum links among nodes, and orchestrate the integration with already existing telecommunications infrastructure. The data plane must ensure the correct forwarding of the quantum keys. On the other hand, QKD can be implemented to secure control plane communications against quantum-mature attackers. Therefore, SDN-QKD is considered a mutually beneficial relationship. In order to enable the integration of QKD within SDN control plane, we propose the architecture shown in fig. 2:

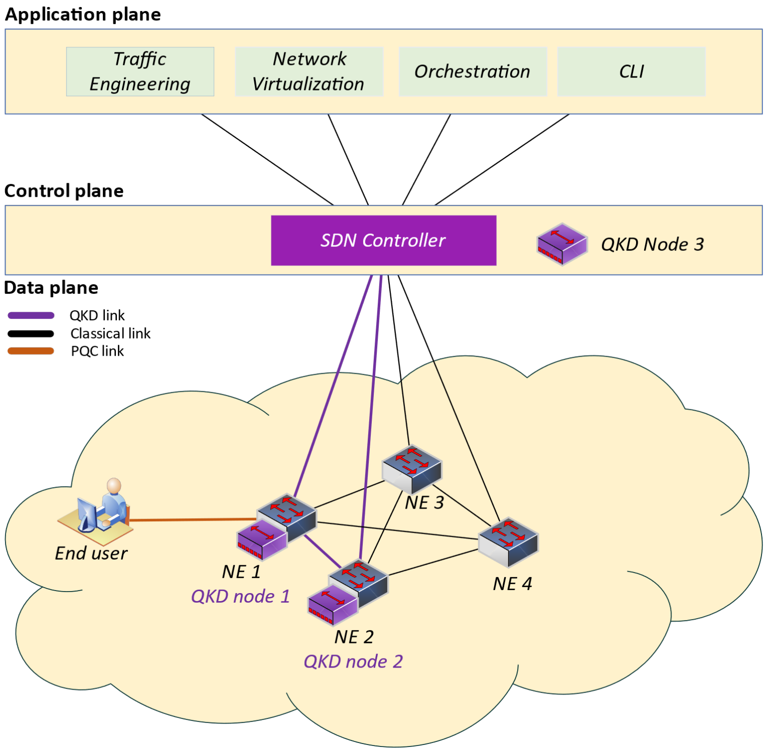

Figure 2. SDN-QKD-PQC architecture

- For implementing fully secure QKD-based communications, there needs to be an authentication phase in which both applications using QKD keys can use PKE (certificates) to identify themselves as the rightful endpoints of the communication. Authentication is a task that QKD cannot address, and thus, another quantum safe alternative needs to be used. We propose the use of post-quantum cryptography (PQC) for the authentication of multiple parties. While there are many different post-quantum algorithms that can handle authentication, the use of Crystals-Dilithium [8] algorithm is recommended by NIST [9].
- While QKD has established itself as the most secure option for key distribution, it is a relatively “new” technology that also brings constraints to the networks (limited distance, expensive equipment, complex integration with traditional infrastructure, etc.). It is recommended that QKD should be combined with other cryptographic algorithms for augmented security. Here, we propose that network security protocols such as Transport Layer Security (TLS) could be modified, so that they combine classical cryptography (Elliptic Curve Diffie-Hellman) with QKD. On top of that,

since there are also PQC alternatives for the key exchange such as Crystals-Kyber [10], PQC can also be integrated into authenticated key exchange (AKE) mechanisms. We propose the implementation of a quantum-safe TLS, which combines classical cryptography, PQC and QKD. Hence, achieving a level of security backed up by three different cryptographic assumptions.

- Although free space QKD is also an alternative for implementing QKD in wireless scenarios, it is still a challenging subject. In implementations where end-to-end quantum security must be achieved, we propose to implement PQC (i.e. Crystals-Kyber) as the AKE mechanism in those areas of the networks where optical fiber links are not available.

Conclusions

Since SDN allows more flexible, programmable and dynamic networks, it remains the technology of choice while introducing QKD for securing communications. This adds requirements on the QKD equipment, which needs: (i) be equipped with interfaces that can interpret and respond to the network controller commands, and (ii) be able to react accordingly to these commands. At the same time, QKD is one of the best options to secure control plane communication. Its integration/combination with classical cryptography, as well as PQC, will give SDN networks the security needed to guarantee and provide ultra-safe communications in the 6G and beyond era, where quantum computers will already be a mature technology.

Acknowledgements

This work was supported by the EC H2020 MSCA ITN-ETN IoTalentum (grant no. 953442) and Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

References

[1] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018, doi: 10.22331/q-2018-08-06-79.

[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[3] L. Chen *et al.*, "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, NIST IR 8105, Apr. 2016. doi: 10.6028/NIST.IR.8105.

[4] D. Ott, C. Peikert, and other workshop participants, "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility." arXiv, Sep. 16, 2019. doi: 10.48550/arXiv.1909.07353.

[5] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in Software-Defined Networking (SDN)," *Comput. Netw.*, vol. 112, pp. 279–293, Jan. 2017, doi: 10.1016/j.comnet.2016.11.017.

[6] S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013, doi: 10.1109/MCOM.2013.6553676.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/RevModPhys.81.1301.

[8] P. Schwabe, "Dilithium." https://pq-crystals.org/dilithium/ (accessed Nov. 09, 2022).

[9] "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," *NIST*, Jul. 2022, Accessed: Nov. 09, 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[10] P. Schwabe, "Kyber." https://pq-crystals.org/kyber/ (accessed Nov. 09, 2022).