Data acquisition and simulation tools for virtual QKD testbed access – examples from the OPENQD project

Florian Kutschera[(1)], Emir Dervisevic[(2)], Ladislav Behan[(3)], Diego López[(4)], Miralem Mehic[(2)], Miroslav Voznak[(3)], Hannes Hübel[(1)] Antonio Pastor[(4)] and Luis Cepeda[(4)]

[(1)] AIT Austrian Institute of Technology GmbH, 1210 Vienna, Austria, florian.kutschera@ait.ac.at
[(2)] Department of Telecommunications, Faculty of Electrical Engineering, University of Sarajevo, Zmaja od Bosne bb, Kampus Univerziteta, 71000 Sarajevo, Bosnia and Herzegovina
[(3)] VSB-Technical University of Ostrava, 17.listopadu 15, 708 00 Ostrava-Poruba, Czech Republic
[(4)] Telefónica Investigación y Desarrollo, Madrid, Spain

The OPENQKD project is demonstrating deployed QKD networks in several European cities. We present a virtual QKD testbed that allows the user to monitor live data but also to re-enact the past QKD exchange over the various links, together with a QKD network simulation tool.

The OPENQKD project

Our ICT based society relies heavily on secure encryption methods to transmit data and messages. Due to the advent of quantum computers the current methods (e.g. public key infrastructure) are vulnerable and must be replaced soon. Quantum Key Distribution (QKD) is an information theoretic secure method to generate symmetric keys and can therefore secure communication links in the future. The developments of QKD over the last two decades have now cumulated in robust and mature technology, that is ready for deployment. Large network demonstrations have been initiated with more to come[1,2]. In Europe, the OPENQKD[1] project will show-case QKD applications in various testbeds around the continent working with end-users to demonstrate the maturity and readiness of this technology in real-world use cases. Since not every potential user takes part in these trials, the project aims to provide a virtual testbed interface that can be used to interactively extract data from the different test-sites and use-case demonstrations. In addition to that a QKD simulator tool was also developed and can be accessed by the public. We present here details of the virtual QKD Testbed and QKD Simulator tool.

Virtual Testbed Description

Data from the devices deployed in the use-cases are collected in a central database. With these data, visualizations are created and hosted on the specially developed web interface with different granularity for different user groups (public, project stakeholders, use-case and test-bed admins, etc.). Since it is not feasible to have a permanent data connection from each device in the project to the central database a local collector machine will be used on each location to locally collect data in device-specific ways and formats. All local collectors send the collected data in an OPENQKD project specific format to the central collector.

Roles of the Local Data Collector

The main roles of the local data collectors are as followed: Connecting to the local devices over SNMP, NETCONF, REST, CLI or any other connection. Collecting all data from the different devices used, what includes the QKD links, encryptors and application devices. These data sets will be received in totally different, device-specific formats and need to be converted into the OpenQKD project specific message format. Transfer data to the Kafka[2] instance hosted at AIT. To cache messages in case of internet outages a local Kafka instance can be used. Local messages are sent to the local Kafka instance and will be forwarded to the central Kafka whenever a connection is available. This message transport over the Internet is encrypted and authenticated. The local data collector is the only place with access to the local devices and knowledge about locally used data formats.

Roles of the Central Data Collector

The main roles of the central data collectors are as follows: Collecting and storing data from all devices used in the project into a database. Provide a Web GUI showing different representations of the data for different user groups. Provide all the information for later processing as required for error tracking, reports and scientific papers. Data in the central data collector is in a device-independent format to enable project-wide comparisons and evaluations.

Transferred message

Messages sent over Kafka are transmitted together with a key. The key is used to describe the message format, the sender and a timestamp. For Kafka, the message is just a byte array with a maximum size of 1 MB. The key provides the possibility to add more message formats in the future if necessary. This key describes that the message holds a

[1] https://openqkd.eu

[2] https://kafka.apache.org

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

measurement value formatted in JSON[3]. The sender should be the actual hostname of the collector, which should be unique within OPENQKD.

Web Interface

The main page of the web interface shows an overview map, Fig. 1, with all use-case numbers coloured corresponding to their current state (planned, active, completed).

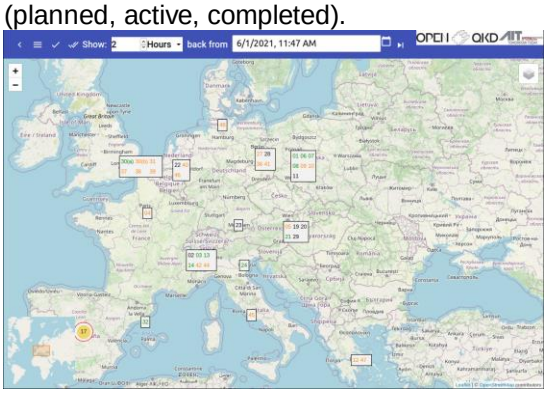


Fig. 1: Testbed Overview

From there, a use-case can be selected to get to the specific use-case information, status-map or graphics page for detailed information. On the top right on the "Status Map", Fig. 2 is a list of selectable items that can be shown which can differ from use-case to use-case depending on the data provided by the use-case coordinator.

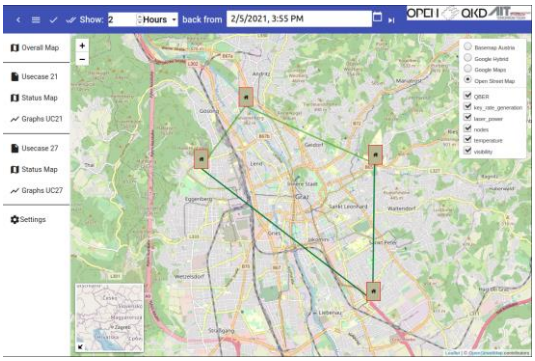


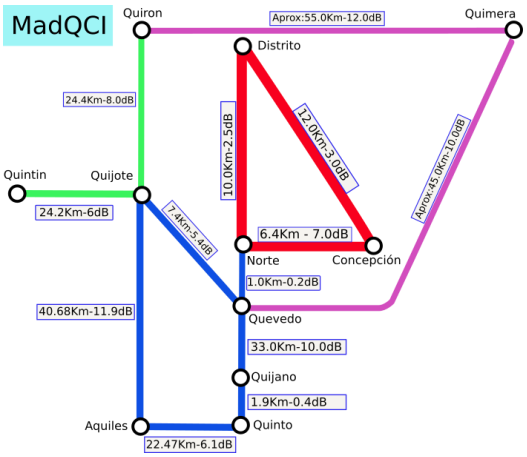
Fig. 2: Status Map of the use-cse demonstration in Graz, Austria

While hovering over the links all selected information is shown for the time range which can be defined in the header. On the graphics page visualizations of the collected performance data can be found. These visualizations are created using the Grafana plotting tool.

Madrid QKD testbed – The MadQCI

The data acquisition shown for the virtual testbed will be the one generated by the MadQCI network in Madrid. As depicted in REF, the MadQCI has two components: a ring of about 28 km installed in the Telefónica Spain production network (in red), and the other is part of the Madrid Research Network (REDIMadrid). The Points of Presence (PoPs) are shown as circles. The part in the production network is ideal for testing high Technological Readiness Level devices since the systems installed must follow the standard procedures for telco equipment and comply with operator constraints. On the other hand, the ring is of exclusive use for the quantum testbed, and the fibres are not lit, which makes it ideal for testing new services.

Fig. 3: Schematic representation of the Madrid Quantum Communication Infrastructure



The rest of the network (blue, green and purple lines) is part of the Madrid Research Network. The PoPs in this network are more open to experimentation and are adequate for devices with lower TRL. The fibres are typically shared with classical channels, which can be used to demonstrate quantum/classical channel co-propagation. The current number of PoPs is nine, although more (3-4 more) can be easily added in the production ring. The network connects several campuses with the Spanish National Research and Education Network (NREN) RedIRIS point of presence, and from there it is connected to the European academic network GÉANT. The MadQCI has been designed with several salient features that makes it unique worldwide. It also connects the infrastructures of two independent network service providers (Telefonica and REDIMadrid). This shared tenancy enables to connect nodes which are further apart in the metropolitan area. The full network is currently designed with 13 links and 11 PoPs, each one with their trusted zone and denoted by their own name most of them using production facilities and sharing most of the nodes and fibre simultaneously for classical and QKD communications.

Applying QKD for B2B and 5G networks.

The demonstrated use-case focuses on the application of QKD in next-generation networks. As the network is evolving towards flexible and scalable architectures, it enables a higher granularity when managing network services.

[3] https://datatracker.ietf.org/doc/html/rfc8259

This means that new technologies and services can be seamlessly integrated into the network within very few days, while networks can be sliced, and their management left for the end-users be changed on demand. One of the most desired and demanded capabilities is to have an enhanced layer for securing the transport segment, traditionally seen as a "black box" from the end-user perspective.

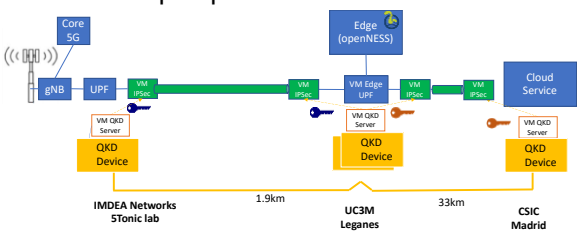


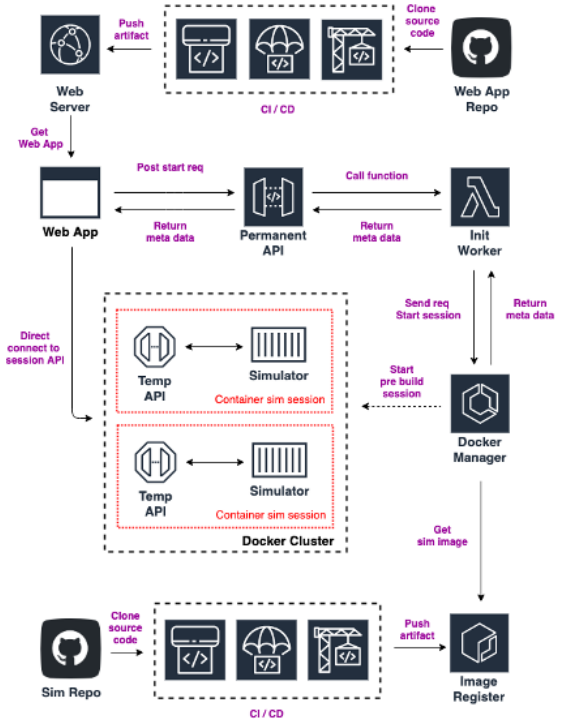
Fig. 4: Applying QKD to 5G edge scenarios at MadQCI

QKD will play an important role when securing the network, as traditional transport services (e.g., virtual private networks-VPNs, label switched paths-LSPs or tunnels) can additionally integrate QKD for securing end-to-end communications. This will allow services on top of the transport network, such as VPNs for business to business (B2B) or connectivity from radio base stations to core or data centre premises (e.g., for 5G), to incorporate quantum-safe security for end-user communications.

QKD Simulator

The quantum key distribution network simulator (QKDNet-Sim) is a simulation module designed to expand the NS-3 network simulator with QKD network functionalities[3]. Its primary purpose is to analyze different approaches to QKD network organizations, simulate networking technologies considering integrating QKD systems into existing telecommunications networks concerning network security[4]. The current stable version of QKDNetSim is compatible with the 3.33 version of the NS-3 simulator. During the QKDNetSim module development, no modifications were made to the core components of the NS-3 simulator[4]. QKDNetSim follows the well-accepted organization of QKD node implementing components such as QKD key, QKD buffer (storage), QKD post-processing applications, and QKD encryptors[5]. Also, it is equipped with a Key Manager System (KMS) that supports both ETSI GS QKD 014[6] and ETSI GS QKD 004[7] standard API interfaces for key delivery to the applications and implements functionalities that currently can support point-to-point communications. To verify KMS functionalities, dedicated QKD applications are developed, each employing a different API interface to communicate with the KMS. The QKD applications allow simulations of the QKD-enabled secure communications in various cryptography or network organization settings. All realized components are independently developed, enabling their installation on separate nodes and realizing large-scale network simulations using Message-Passing Interface (MPI) libraries on High-Performance Computing (HPC) platforms.

Fig. 5: QKDNetSim Web Interface Back-end Organization Scheme



QKDNetSim Web Interface

QKDNetSim is a console-oriented simulator that allows visualization of network topologies using the NS-3 tools NetAnim and PyViz. The web interface consists of two main parts, the graphical user interface (GUI) and the back-end. Through the web interface, the user can select points on the map, between which the distance is automatically calculated, and adjust simulation parameters such as the key generation rate, type of cryptographic techniques, and ETSI 014 parameters such as the number of keys requested from KMS entities in a single request, application and KMS operation time settings. After entering all the parameters correctly, the application sends an API request to initialize the QKD simulator docker application. After completing the simulation process, the user is informed about the achieved results.

Acknowledgments

This work was supported by the H2020 project (OPENQKD) https://www.openqkd.eu under grant agreement No. 857156

[4] More details can be found at www.qkdnetsim.info

References

[1] YA. Chen et al., ”An integrated space-to-ground quantum communication network over 4,600 kilometres”. Nature 589, 214–219 (2021).

[2] European Quantum Communication Infrastructure (EuroQCI) initiative; https://digital-strategy.ec.europa.eu/en/news/technical-agreement-signed-european-plan-quantum-communication-infrastructure

[3] M. Mehic et al, “Implementation of Quantum Key Distribution Network Simulation Module in the Network Simulator NS-3,” Quantum Information Processing, vol. 16, no. 10, p. 253, oct 2017. [Online]; http://link.springer.com/10.1007/s11128-017-1702-z

[4] M. Mehic et al., “Quantum Key Distribution,” ACM Computing Surveys, vol. 53, no. 5, pp. 1–41, oct 2020. [Online]; https://dl.acm.org/doi/10.1145/3402192

[5] V. Martin et al., “A components based framework for quantum key distribution networks,” International Conference on Transparent Optical Networks, vol. 2020-July, no. 2004, pp. 2018–2021, 2020.

[6] ETSI ISG QKD, “Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API (ETSI GS QKD 014 V1.1.1),” vol. 1, pp. 1–22, 2019. [Online]; https://www.etsi.org/deliver/etsi_gs/QKD/001099/014/01.01.01 60/gs qkd014v010101p.pdf

[7] ETSI ISG QKD, “Quantum Key Distribution (QKD); Application Interface,” vol. 2, pp. 1–22, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/QKD/001099/004/02.01.01 60/gs qkd004v020101p.pdf