Securing Communication with Quantum Key Distribution

Securing Communication with Quantum Key Distribution: Implications and Impact on Network Performance

Catalina Stan,[1] Carlos Rubio Garcia,[1] Bruno Cimoli,[1] Juan José Vegas Olmos,[2] Idelfonso Tafur Monroy,[1] Simon Rommel[1]

[1] *Department of Electrical Engineering, Eindhoven University of Technology, 5600MB Eindhoven, Netherlands*
[2] *NVIDIA Corporation, Ofer Industrial Park Yokneam, Israel*

{*c.i.stan,c.rubio.garcia,b.cimoli,i.tafur.monroy,s.rommel*}*@tue.nl, juanj@nvidia.com*

Abstract: With a fully functional point-to-point quantum key distribution link, we demonstrate secret key retrieval by a pair of encryptors and investigate how their addition impacts key network performance indicators on a 10 Gbit/s data channel.

1. Introduction

Quantum key distribution (QKD) enables exchange of encryption keys between two remote nodes. By relying on the properties of quantum information, QKD guarantees information-theoretic secrecy against an all-powerful eavesdropper considering that a quantum bit cannot be copied [1], and correctness since the communication between the two nodes will result in storing the same key on both transmitter and receiver. The encryption key exchanged according to a chosen QKD protocol can be used in a symmetric cipher scheme such as the Advanced Encryption Standard (AES) [2], therefore ensuring secure communication between two nodes. Although point-to-point QKD links have seen significant improvements in terms of performance over the past years, such links can provide secure communication for a limited number of users. Consequently, moving beyond point-to-point towards quantum networks has become a challenge since there is need for technological development, such as quantum repeaters or trusted relays, that can overcome the range limits of QKD and allow scalability of the network while ensuring enough key material for different practical applications [3]. In this paper, we present a fully functional point-to-point link consisting of QKD equipment, layer 2 encryptors and end users and experimentally evaluate how adding new network elements impacts performance. The experimental setup was build as part of the Eindhoven QKD testbed [4] that is currently being developed.

2. Experimental setup

Figure 1 shows the experimental setup comprised of one QKD transmitter (Tx), one QKD receiver (Rx), a pair of encryptors (Encryptor A and Encryptor B), two servers representing the end users (Server A and Server B) for traffic generation and one switch. The QKD layer is based on DV-QKD where the two QKD modules communicate via two fiber-based channels – the service channel which is responsible for authentication, key sifting, privacy amplification and information reconciliation and the quantum channel at 1550 nm which is responsible for sending qubits. The encryptors are configured to obtain the secret key material based on application programming interface (API) calls, as defined in ETSI GS QKD 014 [5]. In order to evaluate the impact of adding new network elements on the 10 Gbit/s data channel, such as encryptors and switch, four scenarios are proposed: 1. Server A – Encryptor A – Encryptor B – Server B, 2. Server A – Server B, 3. Server A – Encryptor A – Switch – Encryptor B – Server B, 4. Server A – Switch – Server B. When the encryptors are included in the configuration, the data channel is encrypted at layer 2 with AES (256 bit key length) as opposed to when they are not connected. For each configuration, a series of latency and throughput tests were performed in order to observe the differences from one scenario to another. For latency tests, 10 000 ping commands were run, while for throughput tests, iPerf3 was used to send Transmission Control Protocol (TCP) data streams (100 simultaneous connections with 100 Mbit/s bandwidth each) for 10 min for configurations 1 and 2 and 5 min for configurations 3 and 4, with a number of streams configured to fully occupy the total 10 Gbit/s capacity of the links.

3. Results and discussion

When adding encryptors, the frame order has to be preserved, therefore a shim of 8 bytes is added to the packet header. During the tests, the shim was added for every frame (shim rate 1) or every 32 frames (shim rate 32) in scenario 3. This means that the maximum payload per frame is smaller as all the headers have to be accounted for

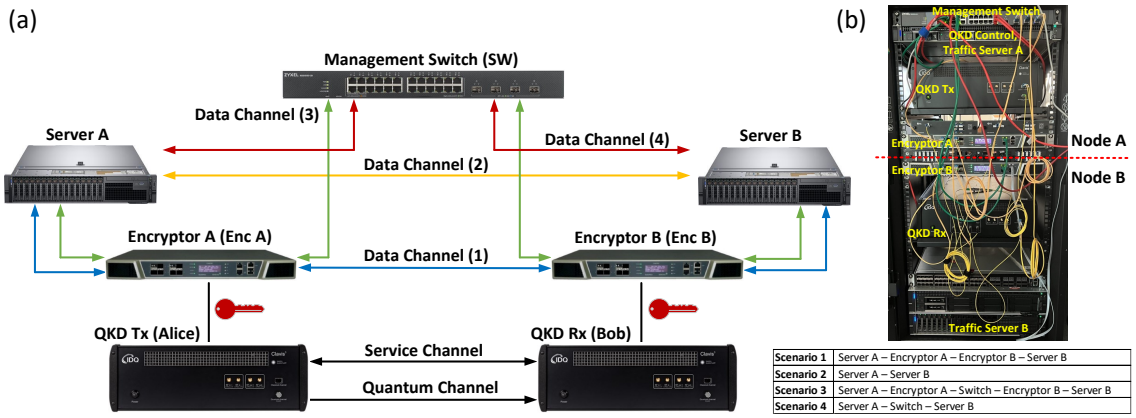


Fig. 1. (a) Experimental setup representing the four data channels. (b) Photograph of the QKD setup consisting of QKD Tx and Rx, switch and encryptors; it should be noted that for convenience the two nodes are housed in the same rack, while for deployment they would of course be separated.

within the fixed Ethernet maximum transmission unit (MTU), making the maximum segment size (MSS) equal to 1452 bytes for the throughput measurements – showing the latency impact of the encryption to be comparable to that of a simple switch. In Fig. 2, we show the latency and throughput for each scenario described in Fig. 1(a). The round trip time (RTT) increased by up to 11 % for scenario 3 with both encryptors and switch, while separate addition of the switch or encryptors result in a delay of 5 % and 6 % respectively, compared to a mean RTT of 0.2177 ms in scenario 2 where the two traffic servers are directly connected. Throughput was the most affected in scenario 3 where both encryptors and switch are added, with a decrease of 5.39 % due to the added shim on every frame, compared to scenario 4 where the average throughput is 9.4145 Gbit/s.

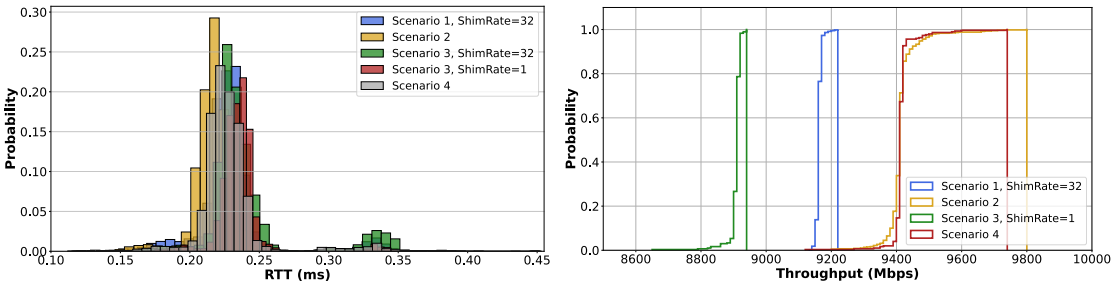
4. Conclusion

We showed a data channel encrypted with QKD-exchanged key material and evaluated throughput and latency impact when adding encryption, finding a small impact on both, resulting from the overhead and processing delay added by encryption.

Acknowledgments The authors would like to thank Thales for providing the encryptors. This work was partially funded by EU MSCA ITN-ETN IoTalentum (grant 953442), ECSEL BRAINE (grant 876967) and NGF Quantum Delta CAT2.

References

1. Wootters, W., et al., “A single quantum cannot be cloned,” Nature 299, 802–803 (1982).
2. Diamanti, E., et al., “Practical challenges in quantum key distribution,” npj Quantum Inf 2, 16025 (2016).
3. Wehner, S., et al., “Quantum internet: A vision for the road ahead,” Science 362, 6412 (2018).
4. Raddo, T. R., et al., “Quantum Data Encryption as a Service on Demand: Eindhoven QKD Network Testbed,” 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019, pp. 1-5.
5. ETSI GS QKD 014, “Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API,” V1.1.1 (2019).



(a) Latency (b) Throughput

Fig. 2. (a) Latency comparison for each scenario and shim rate. (b) Throughput decreased as encryptors are added on the data path.