Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things

Alex Mavromatis[(1)], Foteini Ntavou[(1)],
Emilio Hugues Salas[(1)], George T. Kanellos[(1)], Reza Nejabati[(1)], Dimitra Simeonidou[(1)]

[(1)] High Performance Networks Group (HPN), University of Bristol, a.mavromatis@bristol.ac.uk

Abstract *A software-defined IoT network is integrated with fibre-based QKD technology to provide the IoT devices with quantum-secure keys to enhance their battery lifetime. Experimental demonstration reveals an 18% energy efficiency improvement compared to the standard device key generation.*

Introduction

As Internet of Things (IoT) is rapidly growing to a predicted connectivity of over 30 billion devices by 2020[1], network security emerges as the major challenge in IoT since one attack can affect millions of devices. To adequately address the need for increased security in IoT, complex software-based data encryption schemes have been recently adapted employing a lightweight hardware-depended AES encryption. However, such schemes rely on locally generating the encryption keys at the expense of intense computational power and energy resources from the devices. Research now focuses on optimizing the encryption methods to enhance energy efficiency and allow for prolonged battery lifetime and autonomy of the IoT[2].

On the other hand, Quantum Key Distribution (QKD) technology has proved to be a strong candidate for future-proof secure communications with recent field trials being successfully demonstrated in a network scale[3]. QKD enables the sharing of a secure key between two remote entities (Alice and Bob) while quantum mechanics prevent an eavesdropper (Eve) from measuring the encoded photons. Current implementations rely on complex QKD systems[3] but the increased interest on chip-based QKD[4] may soon lead in low cost QKD devices and systems, that would allow their massive deployment with IoT.

In this paper we demonstrate, for the first time, to the best of our knowledge an experimental integration between a Software-Defined IoT network of devices and a fibre-based QKD system, as a first proof-of-concept implementation to showcase that QKD can serve a significantly increased number of IoT devices with the same level of security while drastically improving energy savings for the IoT infrastructure. In this work QKD serves both as an enhanced key source mechanism relying on quantum true random generation and as a secure mechanism to distribute the keys through the optical network to the IoT gateways and then to the IoT devices, thus completely replacing the embedded key generation processes otherwise present in current IoT networks. For the wireless part of the key transmission, we relied on conventional HTTPS connection where the key is encrypted and securely passed to the device prior to being decrypted and used by the device. However, the fact that implementation on wireless QKD is progressing[5], brings closer the potential for true end-to-end QKD to the IoT devices and prompts for further research on this field.

For this experiment, we launch our QKD system (IDQ-Clavis2) through our field trial fibre network infrastructure to establish a secure connection between a server that represents the data centre and our IoT devices, and compare this to our standard IoT network configuration over 24h experiments. While network performance in terms of latency and packet loss is not compromised, results show significant reduction on energy consumption, with an 18% improvement of the Radio Duty Cycle(RDC) of the devices in comparison to the typical device-key-generation, resulting to a battery lifetime extension.Finally, analysis of the capabilities of the QKD system reveals that for the given optical losses of the fibre network a massive 9000 IoT devices could be served considering the same length and frequency of secret keys to conventional implementations[6].

QKD for Software Defined IoT

In the IoT world several encryption mechanisms propose a lighter way of encrypting data, commonly known as Lightweight Cryptography[7]. A commonly used encryption technique is the Elliptical Curve Cryptography (ECC), where keys are locally generated by utilizing the properties

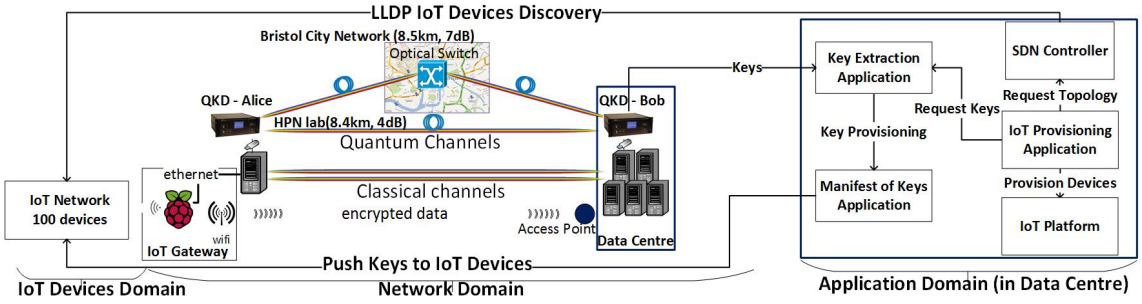

Fig. 1: Architecture of the integrated optical QKD system and IoT network

of the elliptic curve equation. Our concept relies on removing this additional processing overhead for the key generation from the devices by implementing a wake up mechanism to get out of sleep mode and fetch a key provided by the QKD system from a specific HTTPS address. Fig.1 presents the experimental setup of the proposed integrated Quantum-IoT architecture, where QKD is used as a continuous pool of symmetric keys for the IoT Network.

In the physical layer, Alice resides in the IoT Network while Bob is connected to a server emulating the Data Centre(DC). The QKD pair operates over 2 channels: the classical(ClCh) that forms a public and authenticated channel between the 2 parties, and the quantum(QCh) through which the encoded photons are transmitted. For the purpose of this experiment and to investigate the effect of the QCh parameters in the IoT network performance, the QCh is implemented in two different ways. Firstly, we implement the QCh with an 8.4km-long dedicated single mode fibre, exhibiting a total optical loss of 4dB. In the second case, we launch the QCh over the Bristol City Network (BCN) in the city of Bristol, UK, through an optical switch and 8.5km-long dedicated dark fibre with overall optical losses of 7dB. The ClChs in both cases are also optical fibre links. The IoT Gateway is a Raspberry Pi with an Ethernet interface connected to the optical QKD network and a wireless interface used for the transmission of the encrypted data between the IoT network and the DC.

In the Network and Application Domains, the core building block is the IoT platform which is the element retrieving and providing the data from the devices. To establish communication between the devices and the IoT platform, a process is launched through the IoT provisioning application utilizing the SDN controller, to provision the devices based on their MAC address[8]. When the SDN controller discovers the entire network, the application requests keys equal to the total amount of the IoT devices. The QKD system generates 256bit-keys after several steps, including error correction and privacy amplification happening in the ClChs. The keys are saved to the Key Buffer(KB)(1Mbits), approximately 3900 256bit-keys, and are accessible from the Key Extraction Application (Fig.1) which makes a request over UDP to extract them. Fig.2e shows one of the UDP response packets from Bob's server containing a requested 256bit-key. When the KB is full, the system replaces the keys with newly generated ones. Furthermore, the generated keys are available through a REST API to facilitate a secure GET request for all the devices. In our experiments the keys are updated once every 30 min.

Performance Evaluation

To evaluate the benefits of the integration between QKD and the IoT infrastructure, as well as the impact to the networking performance, a series of experiments is conducted. We use the network emulator Mininet and the IoT MQTT data protocol and average results obey to a confidence interval of 95%. The IoT devices are emulated based on the out-of-shelf Pycom-Pysense-fipy. This section presents a comparative performance evaluation for both QKD key generation and device key generation (DKG) for data encryption.

In Fig.2a the average RDC is presented to evaluate the overall workload of each device revealing a significant decrease of 18% when the devices encrypt using QKD keys. The decrease in RDC is due to the fact that key generation process is not performed locally anymore, however some power is consumed in the decryption of the keys needed for their wireless transmission. Thus, in case of end-to-end QKD transmission, RDC would be further decreased. Fig.2b plots the average Battery Lifetime observed in the experiments, to reveal that the QKD technique outperforms the embedded key generation by extending the device lifetime in excess of 18%, drastically enhancing the devices autonomy. While the energy efficiency

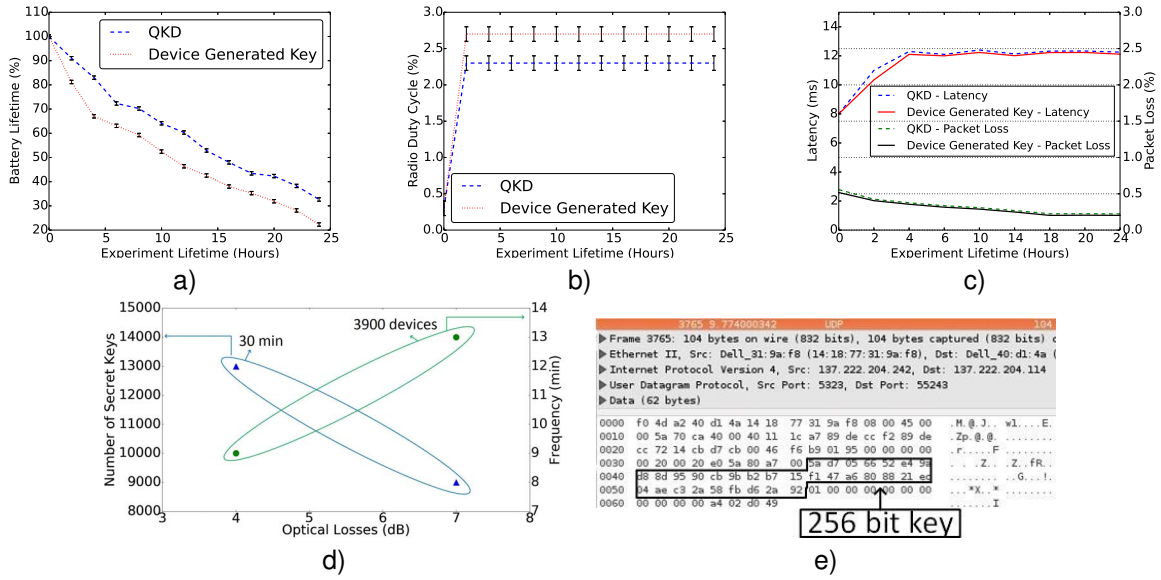

Fig. 2: a) RDC over 24h using the QKD key and the DKG,b) Battery Lifetime over 24h of the IoT devices using the QKD key and the DKG,c) Latency/Packet loss over 24h using the QKD key and the DKG,d) Number of keys and frequency that the devices can be served as a function of the optical losses in the two QCh cases,e) UDP response packet containing a 32byte key (Wireshark)

benefits are evident, the networking overhead for the QKD approach is negligible. Fig.2c plots the average latency and packet loss for the two approaches, revealing insignificantly higher latency and packet loss when QKD is introduced.

Fig.2d shows the capabilities of the QKD system in the number of the IoT devices to be provisioned or the frequency they can be served and the effect of the optical losses in the QCh. Specifically, Fig.2d plots the optical losses of the two different link setups (HPN lab link, BCN network link) versus the number of secret keys generated within 30min of timespan in the left axis of the figure, and the frequency in which the devices can be served with new secret keys in the right axis. Since the average secret key rate for the case of the HPN lab fibre and the BCN network links was found to be 1880bps and 1220bps respectively, the number of secret keys and thus the number of devices to be served within 30min timespan is approximately 13000 and 9000 respectively. Alternatively, considering that the minimum time to update the secret keys is the time required to fill in the KB(1Mbit), the QKD system can serve 3900 devices every 9min or 13min respectively. Both results highlight the capacity to massively serve a very high number of IoT devices with the QKD system while these numbers can be further improved by minimizing the optical losses.

Conclusions

In this work we investigate the DKG impact to the energy consumption in IoT. We propose a key generation using QKD to increase the IoT device battery lifetime. The proposed scheme outperforms the DKG and presents energy efficiency improvement of 18% without compromising the network reliability.

Acknowledgements

This work acknowledges EPSRC EP/M013472/1 UK Quantum Hub and H2020 REPLICATE

References

[1] D. Evans, “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,” Cisco Systems, 2011, Accessed March (2018)

[2] U. Banerjee, et al., “Energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications,” ISSCC (2018)

[3] M. Peev et al., “The SECOQC quantum key distribution network in Vienna,” New J. Phys., Vol. 11, 075001 (2009)

[4] P. Sibson et al., “Chip-based quantum key distribution,” Nature Communications, 8, 13984 (2017)

[5] O.Elmabrok et al., “Wireless quantum key distribution in indoor environments,” JOSA B, Vol. 35, Issue 2, pp. 197-207 (2018)

[6] Meena Singh et al., “Secure MQTT for Internet of Things (IoT),” Communication Systems and Network Technologies (2015)

[7] Himja Agrawal1, Prof.P.R.Badadapure., “A Survey Paper On Elliptic Curve Cryptography,” International Research Journal of Engineering and Technology (2016)

[8] Alex Mavromatis et al., “A Software Defined Device Provisioning Framework Facilitating Scalability in Internet of Things,” to be presented at World Forum 5G, Santa Clara, California (2018)