Toward Optimal Orchestration of Time-shared QKD Infrastructure

Juan Carlos Hernandez-Hernandez[(1)], David Larrabeiti[(1)], Maria Calderon[(1)], Ignacio Soto[(2)], Bruno Cimoli [(3)], Hui Liu[(3)], Idelfonso Tafur Monroy[(3)]

[(1)] Dept. de Ingeniería Telemática, Universidad Carlos III de Madrid, Spain, juanhern@it.uc3m.es
[(2)] Dept. de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid, Spain
[(3)] Dept. of Electrical Engineering, Eindhoven University of Technology, Netherlands

Abstract *Orchestrating Time-multiplexed QKD (Quantum Key Distribution) infrastructure is a complex task which, properly performed, can substantially reduce QKD service deployment costs. This work provides the basis to orchestrate near-optimal key exchange routing and time-sharing; furthermore, cost saving as a function of key rate is quantified.*

Introduction

Deploying Quantum Key Distribution service both by means of a standalone network (QKDN) and on top of a WDM infrastructure is a technological and economic challenge given (a) the current cost of commercial QKD equipment[1], (b) the physical layer requirements of quantum channels and (c) the complex orchestration of QKD infrastructure. From all available QKDN schemes, trusted-relay-based QKD seems to be the widest accepted pragmatic approach to make QKD feasible in a multi-hop scenario. In[2] a mathematical programming (MP) model is proposed to minimize the deployment cost of a network with purely trusted relays and in[3] a hybrid one with trusted and untrusted relays. This approach allows some degree of sharing of devices (Transmitters (Tx) and Receivers (Rx)) for the end-to-end exchange of keys as outlined in the next section. However, in this architecture, a device is statically allocated to a quantum link. However, additional sharing gain can be obtained if a single device can be shared in time over multiple quantum links with the help of an optical switch. This concept is implicitly present in the experiment settings of[4]–[7], which prove the technical viability of this approach (especially if an optical fiber switch is employed, like in[8]). In particular[5] predicts the existence of some cost savings and demonstrates how virtualized network functions can be secured using time-shared QKD devices using an SDN network controller.

However, to the best of our knowledge, the generalization of this approach to a whole network, how this time sharing can be scheduled and how key exchange requests should be routed through the network to minimize the number of devices to deploy has not been explored. Furthermore, the cost saving envisaged in[5] has not yet been quantified. In this work, we address all these important open issues which need to be taken into account by the smart control plane in charge of allocating the time shares of QKD devices to quantum links by re-configuring the attached switches.

Network model and overall concept

Key generation in conventional trusted-node QKDNs is sketched at the top of Figure 1. The management and storage of the keys are carried out by the management entity (ME) and by the key storage (KS) respectively. In TDM trusted-node QKDNs key generation works in the same way, except for the fact that there is no need to deploy a pair of QKD transceivers per quantum link. The concept of TDM trusted-node QKDNs is shown at the bottom of figure 1 where Node 2 has a single QKD-Rx, which is shared between neighbouring nodes (nodes 1 and 3). The size of each time slot assigned to the shared devices depends on the key demands on the links. To share a QKD device over multiple optical channels requires an additional low-insertion loss and crosstalk optical switch element, for instance, an optomechanical switch[7].

In our model, time is structured in periods of duration T. T should be much greater than the re-calibration time required by the QKD devices every time they switch over from one quantum channel to another. Our work's aim is to deploy a QKDN with the minimum number of devices that can meet the key demands (known in advance) between every pair of nodes. For this purpose, we applied the following methodology. Firstly, we defined the network model to be equipped with QKD devices; then we developed a heuristic algorithm for QKDN with TDM (HAQTDM) getting the

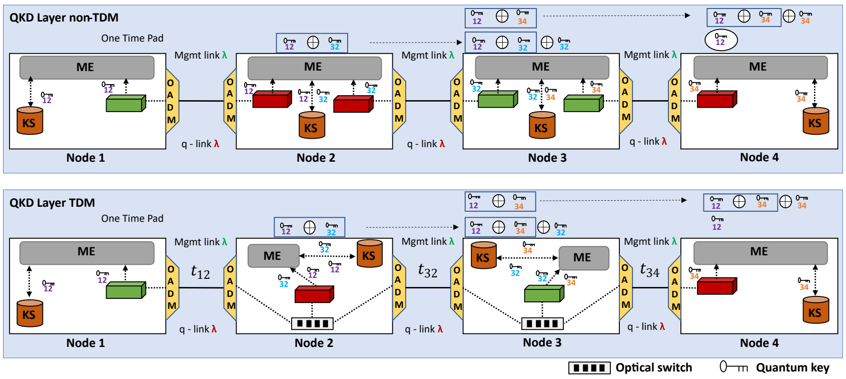

Fig. 1: Non-TDM scheme (top) vs TDM trusted-node QKD networks (bottom)

close-to-optimum set of resources and scheduling needed in the deployment and orchestration process respectively; and, finally, we applied the heuristic method to a real topology, MadQCI, to evaluate the implications and viability of our approach compared to a shortest-path balanced algorithm non-TDM (SP-nTDM).

Deploying QKDNs: HAQTDM heuristic algorithm

Let t_n and r_n be the number of QKD-Tx and QKD-Rx devices respectively, required to be allocated at each node $n \in N$ which are given by equations 1 and 2. The number of switch ports $\forall n \in N$ is calculated by equation 3. The total deployment cost is provided by equation 5 and depends on the QKD transceivers allocated, the optical switch ports, the number of quantum channels and their length. HAQTDM determines the fraction of time a device needs to devote to a quantum link to satisfy all the demands traversing this link. Because lack of space, this version of the algorithm does not deal with concrete time slot alignments. A simple time slot alignment procedure not included in the figure is required.

$$t_n = \left\lceil \frac{\sum\limits_{(i,j)\in\delta_{t_n}} \left(\frac{h_{(i,j)}\cdot L\cdot T}{\mu_{(i,j)}} + t_s\right)}{T} \right\rceil \qquad \forall n \in N \qquad (1)$$

$$r_n = \left\lceil \frac{\sum\limits_{(i,j)\in\delta_{r_n}} \left(\frac{h_{(i,j)}\cdot L\cdot T}{\mu_{(i,j)}} + t_s\right)}{T} \right\rceil \qquad \forall n \in N \qquad (2)$$

$$s_n = \begin{cases} t_n + r_n + |\beta_n| & \text{if } t_n + r_n + |\beta_n| \geqslant 3 \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

Tab. 1: Notation and Definitions

Notation	Definition
$G(N,E)$	Optical/QKD network
N	Set of optical/QKD nodes
E	Set of available edges
L	Key length [bits]
$l_{(i,j)}$	Set of all link length
R	Set of all secret-key demands
$r_{(s,d,k)}$	Secret-key demand $r \in R$
$h_{(i,j)}$	Accumulated demand on (i,j)
$\mu_{(i,j)}$	Key rate on (i,j) [bps]
$c_{(i,j)}$	Number of q-ch at link (i,j)
p_{th}^{r}	Set of all possible paths for r
β_n	Set of neighbors nodes of n
δ_{t_n}	Set of connected links of Tx at n
δ_{r_n}	Set of connected links of Rx at n
t_s	Switching time [seconds]
r_n	Number of Rxs at node n
t_n	Number of Txs at node n
s_n	Number of switch ports at node n
$\mathrm{C_r}$	Cost of one Rx
$\mathrm{C_t}$	Cost of one Tx
$\mathrm{C_s}$	Cost of one switch port
$\mathrm{C_c}$	Cost of each channel
$\mathrm{C_T}$	Total deployment cost

$$c_{(i,j)} = \left\lceil \frac{\frac{h_{(i,j)}\cdot L\cdot T}{\mu_{(i,j)}} + t_s}{T} \right\rceil \qquad \forall n \in N \qquad (4)$$

$$\begin{aligned} \mathrm{C_T} = & \sum_{n\in N} \mathrm{C_r}\cdot r_n + \sum_{n\in N} \mathrm{C_t}\cdot t_n \\ & + \sum_{n\in N} \mathrm{C_s}\cdot s_n + \sum_{(i,j)\in E} \mathrm{C_c}\cdot c_{(i,j)}\cdot l_{(i,j)} \end{aligned} \qquad (5)$$

Results analysis

To evaluate our proposal, the topology of Madrid Quantum Network (MadQCI, see Figure 3)[9] was considered. We have assumed $L = 256$ bits, $\mathrm{C_r} = 150$ units, $\mathrm{C_t} = 100$ units, $\mathrm{C_s} = 10$ units, $\mathrm{C_c} = 0.1$ units/km, with $\mathrm{C_r}/\mathrm{C_t} = 1.5$ thinking in a scenario

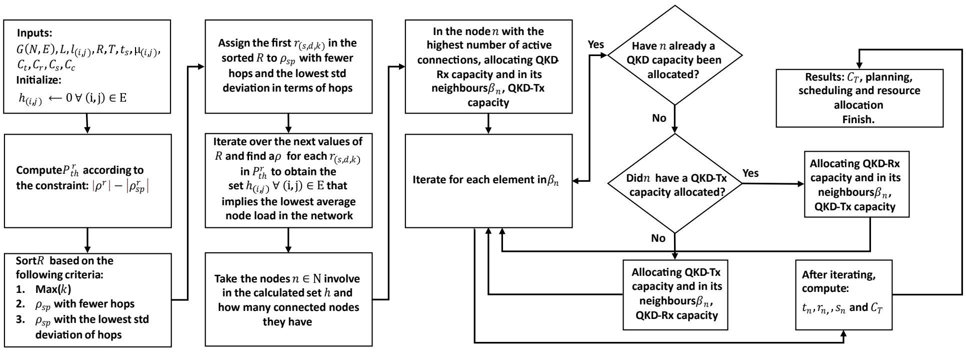
Inputs:
$G(N,E), L, l_{(i,j)}, R, T, t_s, \mu_{(i,j)}, C_t, C_r, C_s, C_c$
Initialize:
$h_{(i,j)} \leftarrow 0 \; \forall \, (i,j) \in E$
Compute P^r_{th} according to the constraint: $|\rho^r| - |\rho^r_{sp}|$
Sort R based on the following criteria:
1. Max(k)
2. ρ_{sp} with fewer hops
3. ρ_{sp} with the lowest std deviation of hops
Assign the first $r_{(s,d,k)}$ in the sorted R to ρ_{sp} with fewer hops and the lowest std deviation in terms of hops
Iterate over the next values of R and find a ρ for each $r_{(s,d,k)}$ in P^r_{th} to obtain the set $h_{(i,j)} \; \forall \, (i,j) \in E$ that implies the lowest average node load in the network
Take the nodes $n \in N$ involve in the calculated set h and how many connected nodes they have
In the node n with the highest number of active connections, allocating QKD-Rx capacity and in its neighbours β_n, QKD-Tx capacity
Iterate for each element in β_n
Yes
Have n already a QKD capacity been allocated?
No
Did n have a QKD-Tx capacity allocated?
Yes
No
Allocating QKD-Rx capacity and in its neighbours β_n, QKD-Tx capacity
Allocating QKD-Tx capacity and in its neighbours β_n, QKD-Rx capacity
After iterating, compute:
$t_n, r_{n,}, s_n$ and C_T
Results: C_T, planning, scheduling and resource allocation
Finish.

Fig. 2: Flowchart of HAQTDM, the proposed heuristic algorithm

with BB84 QKD protocol where the single photon detector at receivers side is more expensive than the transmitter. For simplicity, the value of t_s is assumed to be 300 seconds based on the state-of-the-art[7]. We chose the worst case for $\mu_{(i,j)}$ where the q-ch goes via two optical switch ports interpolating the values in[7] to obtain the secret-key generation rate as a function of distance. We compare our HAQTDM with a Shortest Paths Balanced Algorithm without TDM (SP-nTDM), since no previous works exist in the state-of-the-art for optimizing QKD network deployment with TDM. SP-nTDM only considers candidate paths for a given request r with the same number of hops as the shortest path ($|\rho^r| - |\rho^r_{sp}| = 0$). QKD transceivers must be allocated at each link to meet the demands in h, similar to HAQTDM. The number of QKD transceivers on each link is determined by the upper integer value of $h_{(i,j)} \cdot L/\mu_{(i,j)}$.

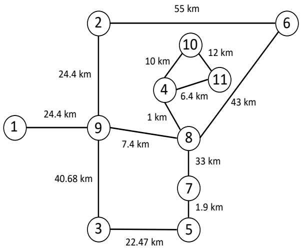

Fig. 3: MadQCI topology

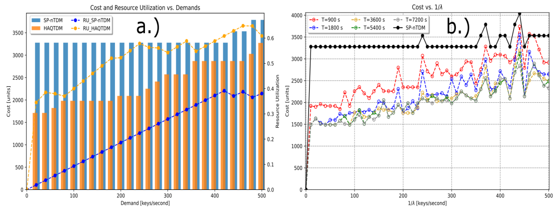

Fig. 4: Simulations on MadQCI with demands: symmetric (a) and exponential distribution (b)

The simulation reveals, as shown in Figure 4 for symmetric and exponentially distributed key generation demands, that at low quantum link loads, HAQTDM achieves savings of about 50 % and keeps on being substantial (25 %) up to high link loads. As expected, the higher the link utilization by the demands the higher the amount of devices to install at the nodes and the absolute benefit of TDM sharing fades out. The continuous growth at low loads of TDM is due to the incremental saturation of the most central links. The absolute throughput figures show real practical applicability of this technique even to scenarios requiring hundreds of keys per second.

Conclusions

This work addressed for the first time fundamental issues in the design and orchestration of time-shared QKD infrastructure at a network scale. The work proposed a heuristic to route key exchange requests through the network that minimizes the cost of required QKD devices and provides the SDN orchestrator with the time shares that each QKD device needs to devote to each quantum link it is serving. Our work estimated for the first time that device sharing by employing inexpensive low-loss switches can yield substantial cost savings as high as 50 % at low-to-medium loads. Simulations prove that overall throughput in a real QKDN topology and commercial technology at those loads is large enough (hundreds of keys/sec) to provide high levels of security.

Acknowledgements

This work has been partially supported by Horizon EU Program under the ALLEGRO project, the Spanish project ACHILLES (PID2019-104207RB-I00) and CAT2 Quantum Delta NL.

References

[1] K. Klink, “Quantum key distribution in a pan-european network of national research and education networks, qualitative and quantitative aspects of implementing a quantum key distribution network”, M.S. thesis, University of Twente, 2022.

[2] F. Pederzolli, F. Faticanti, and D. Siracusa, “Optimal design of practical quantum key distribution backbones for securing coretransport networks”, *Quantum Reports*, vol. 2, no. 1, pp. 114–125, 2020.

[3] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks", *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 9, pp. 2701–2718, 2021.

[4] Y.-L. Tang, H.-L. Yin, Q. Zhao, *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network", *Phys. Rev. X*, vol. 6, p. 011 024, 1 Mar. 2016.

[5] A. Aguado, E. Hugues-Salas, P. A. Haigh, *et al.*, "Secure nfv orchestration over an sdn-controlled optical network with time-shared quantum key distribution resources", *J. Lightwave Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[6] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution", *Journal of Lightwave Technology*, vol. 36, no. 22, pp. 5230–5236, 2018.

[7] X. Tang, "Optically switched quantum key distribution network", Ph.D. dissertation, University of Cambridge, 2019.

[8] R. Wang, R. S. Tessinari, E. Hugues-Salas, *et al.*, "End-to-end quantum secured inter-domain 5g service orchestration over dynamically switched flex-grid optical networks enabled by a q-roadm", *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 139–149, 2020.

[9] V. Martin, A. Aguado, J. P. Brito, *et al.*, "Quantum aware sdn nodes in the madrid quantum network", in *2019 21st International Conference on Transparent Optical Networks (ICTON)*, IEEE, 2019, pp. 1–4.