Quantum Key Distribution Resource Sharing Schemes for Metropolitan Area Networks

Juan Carlos Hernandez-Hernandez, David Larrabeiti, Maria Calderon
Dept de Ing. Telemática
Universidad Carlos III de Madrid
Madrid, Spain
juanhern@it.uc3m.es

Ignacio Soto
Dept. de Ing. de Sistemas Telemáticos
Universidad Politécnica de Madrid
Madrid, Spain
ignacio.soto@upm.es

Bruno Cimoli, Hui Liu, Idelfonso Tafur Monroy
Dept. of Electrical Engineering
Eindhoven University of Technology
Eindhoven, Netherlands
b.cimoli@tue.nl

***Abstract*—QKD networks are costly infrastructures. This paper introduces the concept of time-sharing of QKD resources, namely receivers, transmitters and quantum links. A number of strategies for resource sharing in QKD are described. The approach is valid for any point-to-point QKD system that implements end-to-end key exchange via one-time-pad-based trusted relay. A quick modelling and analysis of one of these strategies on a sample network proves the potential for QKD CAPEX saving. Coordinated smart scheduling of slices via SDN controllers is required.**

***Index Terms*—QKD, resource sharing, TDM, network design**

I. Motivation for resource sharing

Quantum key distribution (QKD) solves the problem of sharing cryptographic keys between two remote parties with absolute security, guaranteed by the fundamentals of quantum physics. The basic principle of QKD is exploiting the mere fact that observing quantum objects perturbs them in an irreparable way. These perturbations cause errors in the sequence of quantum bits (qubits) exchanged by a sender and a recipient. Therefore, by checking for the presence of such errors, the two parties can verify whether an eavesdropper was able to gain information over the exchanged qubits. In recent years, QKD has shown enormous potential for securing future networks, due to being theoretically safe against attacks from quantum computers, because it relies on quantum physic properties instead of on the computational complexity of the key exchange algorithm [13].

The QKD protocols allows to distribute between two points a symmetric key formed by random bits. This key is secure against an eavesdropper. The keys are generated in QKD modules, which are a transmitter module (QKD-Tx) and a receiver module (QKD-Rx). To generate a key between two QKD modules there must be a QKD link and a key management (KM) link. In general, a QKD link has a quantum channel that must be point-to-point and a classical logical channel for synchronisation and/or distillation (depending on whether it is a unidirectional or bidirectional communication) [2]. After, they are stored in a kind of internal memory of the modules known as a key manager. In this way, the keys are available to a higher level cryptography application that needs to make use of them. The keys are consumed by an encryption algorithm such as one time pad (OTP), advanced encryption standard (AES), hash based message authentication code (HMAC) among others, to be encrypted-decrypted at each end by the same chosen algorithm.

Experimental results have shown that the maximum key rate achievable by QKD systems rapidly decays with the distance between the two parties. Thus, to cover large-spatial areas and given the immaturity of quantum-relay technology, the deployment of trusted-relays is the most practical approach to develop QKD networks at the moment [1]. In this context, QKD can be used to continuously regenerate symmetric keys for AES-256 secured communications or other encryption protocol. Taking into account that the secure communication process between the end-to-end parties of a QKD network needs to consume the quantum keys generated by the point-to-point links [2], with these point-to-point keys being stored in the corresponding key pools until their consumption.

A quantum key distribution network (QKDN) is a network comprised of two o more QKD nodes connected through QKD links. It allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link [10]. Thanks to the progress in the study of the integration of QKD with current optical networks and wavelength division multiplexing (WDM) [7]–[9] there are different alternatives available to achieve this relaying [10]:

- Optical switching: These can switch QKD link traffic between pairs of QKD modules in the multi-point network, in order to form keys between different users. This form is limited by the distance between the QKD nodes.
- Trusted relaying: Keys are stored in QKD nodes (trusted nodes) and relayed to other distant QKD nodes via highly secure encryption, with one-time-pad (OTP) recommended. The QKD node (trusted node) is assumed to be secure against intrusion and attacks by any unauthorised parties.
- Quantum repeaters: Advances in the development of quantum repeaters have been reported but are not yet

Spanish Ministry of Science FPI grant number PID2019-104207RB-I00, ACHILLES project grant num AEI/10.13039/501100011033 and 6G-Xtreme MDI, H2020-ECSEL BRAINE project grant ID 876967, KAT2 Quantum Delta NL and Spanish Thematic Network Go2Edge (RED2018-102585-T)

978-3-903176-44-7

possible with current technology.

- Untrusted relaying: Measuring device independent QKD (MDI-QKD) and Twin-Field QKD (TF-QKD) are protocols that allow two QKD nodes (more specifically, two QKD-Tx) to establish a key thanks to a third party (this would be the QKD-Rx module). In this way, longer distances can be achieved and resources can be shared. The third node does not have to be trusted unlike the case with trusted repeaters.

To date, the use of trusted repeaters is the most tested and mature way to implement QKDN.

The deployment cost of metropolitan QKDN is still an open issue considering the high cost of QKD modules, mainly receiver components such as single photon detectors [3], even when considering the reuse of existing optical fibers. Several works in the past have investigated how to optimise the QKDN topology from different perspectives to improve security guarantees or QoS. Resource allocation has been studied with machine learning, with integer linear programming (ILP) models and with heuristic models. In [4] they propose a study of the topology to deploy a quantum network, in [5] a ILP models is proposed to minimize the deployment cost of a network with purely trusted relays and in [2] one with a hybrid network (trusted and untrusted repeater).

The common approach in deploying QKD networks has been that a QKD receiver and transmitter can only provide quantum keys for a pair of contiguous nodes. However, the possibility of sharing QKD resources (i.e., a transmitter or receiver is shared among the quantum channels connected to the node), and even use them as a pool to be multiplexed in time, has not been proposed nor explored so far to the best of our knowledge.

Figure 1 depicts the main concept proposed by this paper: TDM-based QKD resource sharing. As it can be seen, the introduction of optical switches in certain nodes enables the re-utilisation of transmission and reception devices. The idea of using a switch for resource sharing can be seen in [6] for MDI QKD, although it has not yet been analysed from the network planning perspective given the sharing alternatives identified next. The figure describes a series of strategies (A to C) that allow to save QKD exchange resources, starting from the baseline strategy-0, which has a dedicated pair of QKD-Tx (Transmitter) and QKD-Rx (Receiver) devices per QKD link. Lines in red depict sample key exchange point-to-point sessions to be serialised to perform time-sharing of resources. As it can be appreciated, the more re-utilisation is applied (from A to C), the more saving is obtained in terms of infrastructure, but the overall key exchange throughput of the network is expected to be lower, given the reduction of serving devices. Moreover, in the case of quantum link sharing by means of optical by-passing (which, on the other hand, can be seen as untrusted relaying), additional throughput loss w.r.t. the baseline strategy-0 comes from the reduction of key rates due to the use of longer optical paths. Due to space limitations, we constrain the scope of the following sections to show how strategy A can be applied to design a QKD network that shares QKD-Rx. Sharing QKD-Rx is the first strategy we propose to save resources because QKD-Rxs are significantly more costly than QKD-Txs in most technologies. However if this were not the case, the approach would still be valid by symmetry with QKD-Txs (start by reducing QKD-Txs instead of QKD-Rxs). The model can be applied to any point-to-point protocol either based on discrete or continuous variable QKD (DV-QKD and CV-QKD). In this paper we also let aside the possibility of using WDM as an additional dimension for resource multiplexing. If low-enough insertion loss ROADMs are available this possibility is also viable [11]. The optical switches considered in this article are supposed to be designed for Quantum applications, i.e. no amplification and no use of broadcast and select, and their impact on key rate and reach is assumed to be negligible for the sake of simplicity.

II. Heuristic for deployment of nodes in a QKD network

Algorithm 1: RESHAL (Receiver Sharing Algorithm)

Data: $G(N, L)$
Result: $sol[(n_{R_x}, n_{T_x})], num_{R_x}$ (all receiver-transmitter node pairs, number of receivers)

initialise $sol \leftarrow 0, node\_sol \leftarrow 0$;
Function `find_rx` (sp) **:**
  reachability $(n_i) \leftarrow 0$;
  reachability $(n_i) = \sum(n_j); \forall n_i, n_j \in G$;
  $max\_reach \leftarrow (n_i)$ with higher reachability;
  for $i \in sp$ **do**
    if $i == max\_reach$ **then**
      $sol \leftarrow (n_i, n_j)$;
      $node\_sol \leftarrow i, j$;
  $active\_boundary \leftarrow 0$;
  for $i \in node\_sol$ **do**
    for $j \in c_{ij}$ **do**
      if $i == j[0]$ *and* $j[1] \notin node\_sol)$ **then**
        $active\_boundary \leftarrow c_{ij}[j]$;
  if $active\_boundary \neq$ *empty* **then**
    $find\_rx(active\_boundary)$;
  else return sol, num_{R_x} ;
$find\_rx(G)$

We propose a heuristic algorithm that is able to allocate to each node of a QKD network QKD devices (transmitters and/or receivers) to allow secured communications between any pair of nodes in the network. The proposed Receiver Sharing Algorithm (RESHAL) reduces the cost of deploying the QKD network by enabling the sharing of QKD-Rx by several QKD-Tx.

The algorithm (see Algorithm 1) assigns a QKD-Rx to the node with the highest reachability (i.e., the node with more direct neighbors). Then, QKD-Tx are assigned to the direct

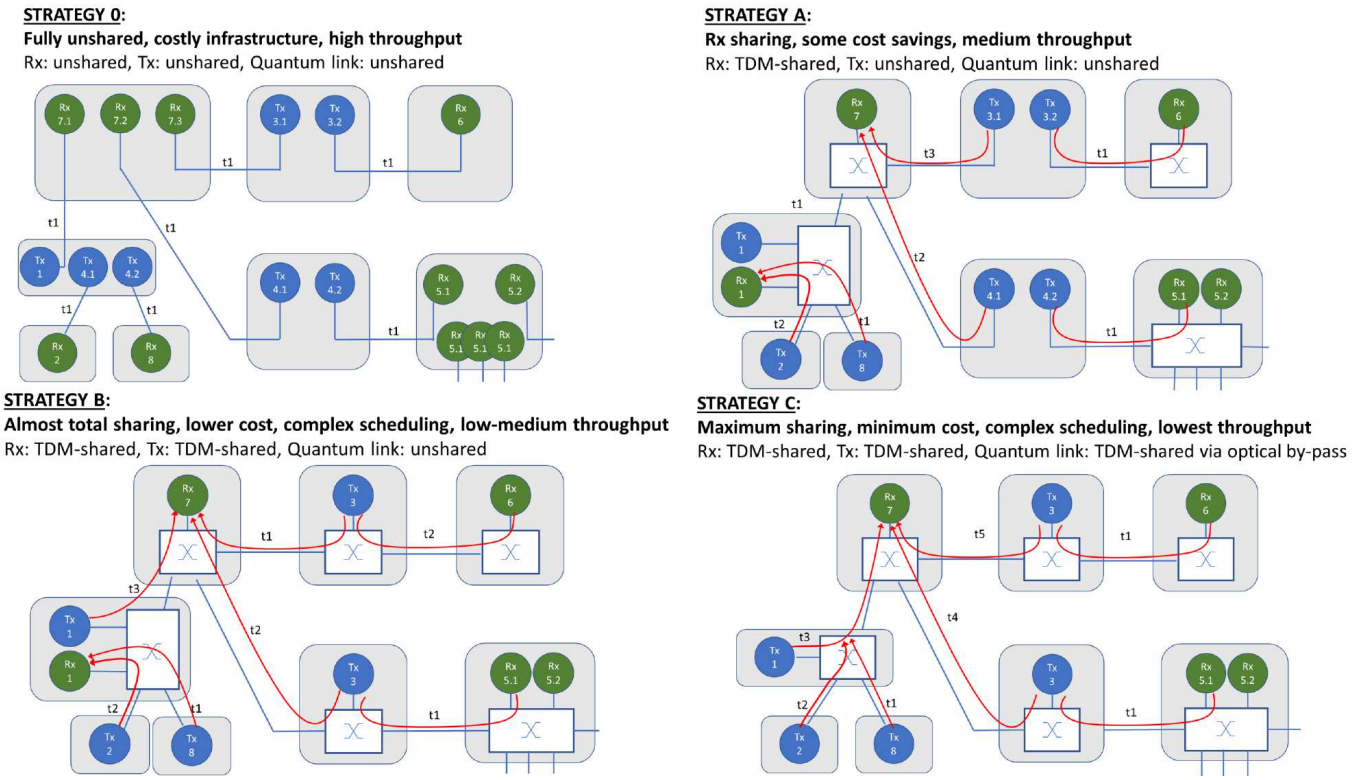

Fig. 1. QKD resource sharing strategies in a trusted-node-based key exchange scenario

neighbors of the QKD-Rx. The next QKD-Rx is assigned to the node with a QKD-Tx that has a direct connection with at least a neighbor that does not yet have a QKD-Rx nor a QKD-Tx (active boundary), and has the highest reachability. This process is repeated until all the nodes have a QKD-Rx, a QKD-Tx, or a QKD-Tx and a QKD-Rx.

To extend our results to a general topology, in which nodes that communicate can be several hops apart, the first step is to identify all the receiver nodes and the directly connected transmitter nodes to each receiver. In this way, each receiver node with its transmitters can be analysed independently applying the equations in this section. If a node has both a transmitter and receiver (in different links), the node appears in different sets of receiver-transmitters. Finally, the key rate demands R_{K_i} must be updated to include the keys needed for communications of any node in the network whose path to create keys goes through node *i* and its corresponding receiver node.

III. Example of Application

To demonstrate our concept, we use an example topology, shown in Figure 2. It is a metropolitan area network, where the distances between nodes are a random value. In the figure, this distance is the numerical label that appears between the nodes, given in kilometres.

Our purpose is to deploy a QKD network using the existing optical infrastructure. We assume that all nodes in the network want to establish quantum keys with any other node. Here we

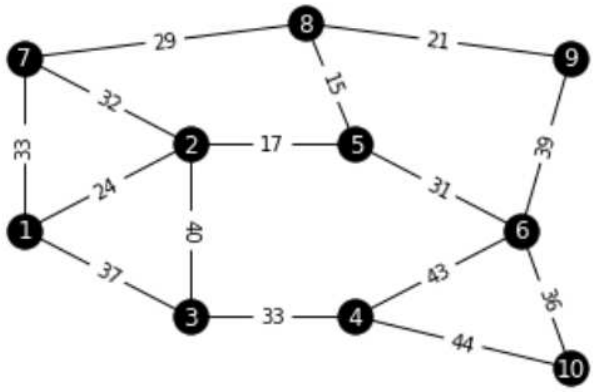

Fig. 2. Topology of the metropolitan optical network used in our example

consider CV-QKD protocols for network implementation as an example to show the feasibility of our concept. The CV-QKD protocol and its properties such as the secure key rate values were extracted from the state-of-the-art [12]. Note that our concept can also be used for DV-QKD protocol, such as the BB84 and distributed-phase-reference protocols.

Applying RESHAL (Algorithm 1) to the network in Figure 2, we obtain as a result three sets of one receiver and several transmitters. Set (1): at node 2 we allocate a QKD-Rx which serves the QKD-Tx located at node 1, node 3, node 5 and node 7; set (2): at node 5 we allocate a QKD-Rx which serves the QKD-Tx located at node 6 and node 8; and, finally, set (3):

at node 6 we allocate a QKD-Rx which serves the QKD-Tx located at nodes 4, 9 and 10. In this way we ensure that each pair of nodes in the network can exchange keys (those that are more than one hop away will employ secure relaying).

Once transmitters and receivers have been assigned to the nodes in the topology, we must determine the number of R_x and T_x needed in each node to address the key generation demands in the network. In this example, the key generation rate needed to secure the communications between any pair of nodes is 0.5 key/s. For example, in set (1), node 1 communicates directly with node 2 (QKD-Rx) and needs keys for communications with nodes 2 to 10. Therefore $R_{K_1} = 4,5$ key/s. A slightly more complex case is node 5, which is a transmitter, and node 2, which is a receiver. In this case, $R_{K_5} = 12$ key/s, since it has to provide keys for the communications of nodes 4, 5, 6, 8, 9, and 10, with nodes 1, 2, 3, and 7. The rest of the key rate demands can be calculated in a similar way, resulting in $R_{K_3} = R_{K_7} = R_{K_8} = R_{K_4} = R_{K_9} = R_{K_{10}} = 4.5$ key/s and $R_{K_6} = 12$ key/s.

Considering the previous demands, and with T=3600s, L=256 bits, and $t_{switching_i} = 600s$, we obtain that in the node 2, we need two QKD-Rx. The transmitter with more load is node 5, so we just need one transmitter at node 5. For the second set of receiver-transmitters, so we just need one Rx at node 5. The transmitter with more load is node 6, so only one transmitter is needed at node 6. Finally, in the third set of receiver-transmitters, two R_x are needed at node 6.

In summary, we obtain after applying strategy A a total of 5 QKD-Rx and 9 QKD-Tx, i.e. 15 devices. If we compare these values with the use of strategy-0 in which we would obtain 30 devices in total, of which 15 QKD-Rx and 15 QKD-Tx we have saved half of the devices. The result is even better if we compare with the amount of QKD-Rx. In applying our strategy A we have assumed that the QKD-Rx are more expensive than the QKD-Tx. In this way we obtain considerable savings because for our case study we only need 5 QKD-Rx to enable quantum key exchange between all nodes in the network instead of 15 QKD-Rx if we use strategy-0. In this way we have a functional QKDN with significant savings in terms of devices and therefore capital.

IV. Conclusions

The key exchange throughput of existing QKD devices (in the order of Kb/s) does not scale to support frequent key exchanges to secure end-user applications on a per-TLS connection basis. Thus in the next years, the practical application scope of QKD is the interconnection of servers or data centers via encrypted virtual private networks secured by QKD. This aggregate traffic encryption approach allows to think that there are scenarios where quantum key rates are enough to make the sharing of QKD resources possible via optical switching and pooling (when required). This paper introduced the concept of time-sharing of QKD resources, namely receivers, transmitters and quantum links. A quick modelling and analysis of one of the sharing strategies presented in this paper on a sample network proves the potential for QKD infrastructure saving. The analysis includes an example application that determines the amount of resources (number of QKD-Rx or QKD-Tx) to be deployed at each node and the proportion of time to be allocated to the demand. An heuristic to decide which type of node (QKD-Tx or QKD-Rx) maximising resource sharing is also presented. Then, with the key length data and mainly the key demand and the established switching times, we can determine the amount of equipment needed at each node. The resource savings obtained are considerable when compared to traditional resource allocation schemes in quantum key distribution as described in the strategy-0. SDN network controllers are needed to coordinate the setup of quantum sessions in order to carry the key distribution demands between pairs of nodes. The development of an SDN controller is the subject of future work.

References

[1] Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, 'Mathematical model and topology evaluation of quantum key distribution network', Optics Express, vol. 28, no. 7. The Optical Society, pp. 9419-9434, 2020.

[2] 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. Institute of Electrical and Electronics Engineers (IEEE), pp. 2701–2718, Sep. 2021.

[3] Y. Wang, Q. Li, H. Mao, Q. Han, F. Huang, and H. Xu, 'Topological optimization of hybrid quantum key distribution networks', Optics Express, vol. 28, no. 18/31. The Optical Society, pp. 26348, Aug. 21, 2020.

[4] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, 'Topological optimization of quantum key distribution networks', New Journal of Physics, vol. 11, no. 7. IOP Publishing, pp. 075002, Jul. 02, 2009.

[5] 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. MDPI AG, pp. 114–125, Jan. 30, 2020.

[6] H. Liu, W. Wang, K. Wei, X. Fang, L. Li, N. Liu, H. Liang, S. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H. Lo, T. Chen, F. Xu, and J. Pan, "Measurement-device-independent QKD over asymmetric channels," in Conference on Lasers and Electro-Optics, OSA Technical Digest (Optica Publishing Group, 2019), paper FM4C.3

[7] J. Zhihua, L. Shuhuai, W. Hao, and W. Yunlu, 'A novel WDM-PON based on quantum key distribution FPGA controller', International Journal of Embedded Systems, vol. 9, no. 3. Inderscience Publishers, p. 241, 2017. doi: 10.1504/ijes.2017.10005716.

[8] A. Wonfor et al., 'Quantum networks in the UK', Metro and Data Center Optical Networks and Short-Reach Links IV. SPIE, Mar. 05, 2021. doi: 10.1117/12.2578598.

[9] D. Lopez et al., "Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks," 2021 Optical Fiber Communications Conference and Exhibition (OFC), 2021, pp. 1-4

[10] ITU-T-Y3800, "Overview on networks supporting quantum key distribution," SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS,INTERNET OF THINGS AND SMART CITIES Y.3800(2020) https://www.itu.int/rec/T-REC-Y.3800/en.

[11] R. Wang 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. Institute of Electrical and Electronics Engineers (IEEE), pp. 139–149, Jan. 01, 2020. doi: 10.1109/jlt.2019.2949864.

[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nature Photonics, vol. 7, no. 5. Springer Science and Business Media LLC, pp. 378–381, Apr. 14, 2013.

[13] IDQuantique, "Understanding Quantum Cryptography", White Paper, May, 2020.