Future Generation Computer Systems 164 (2025) 107557

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Designing optimal Quantum Key Distribution Networks based on Time-Division Multiplexing of QKD transceivers: qTDM-QKDN

Juan Carlos Hernandez-Hernandez [a,*], David Larrabeiti [a], Maria Calderon [a], Ignacio Soto [b], Bruno Cimoli [c], Hui Liu [c], Idelfonso Tafur Monroy [c]

[a] Dept. of Telematic Engineering, Universidad Carlos III de Madrid, Av. de la Universidad, 30, Leganes, 28911, Madrid, Spain
[b] Dept. de Ingeniería de Sistemas Telemáticos, ETSI Telecomunicación, Universidad Politécnica de Madrid, Av. Complutense, 30, Madrid, 28040, Madrid, Spain
[c] Dept. of Electrical Engineering, Eindhoven University of Technology, De Groene Loper, 19, Eindhoven, 5612 AP, North Brabant, Netherlands

ARTICLE INFO

Keywords:
Quantum key distribution networks
Optimization
Efficient network deployment
Shared QKD transceivers

ABSTRACT

Time-sharing of Quantum Key Distribution (QKD) transceivers with the help of optical switches and a central Software-Defined Networking (SDN) controller is a promising technique to better amortize the large investments required to build a Quantum Key Distribution Network (QKDN). In this work, we investigate the implications of introducing Time-Division Multiplexing (TDM) in trusted-relay QKDNs at the wide-area network scale in terms of performance and cost-saving. To this end, we developed both a Mixed Integer Linear Programming (qTDM-MILP) model and a Heuristic Algorithm (qTDM-HA) to solve the allocation of QKD transceivers and network resources for a novel switched QKDN operating scheme: qTDM-QKDN. Our heuristic method provides a close-to-optimal resource planning for the offline problem that computes the minimum number of QKD transceivers and optical switch ports at each node, as well as the number of quantum channels on each link required to satisfy a target set of end-to-end secret-keyrate demands. Moreover, both the model and the heuristic provide the time fractions that each QKD transceiver needs to peer with each neighbor QKD transceiver. We compared our proposed model and heuristic algorithm for cost minimization with non-time sharing QKD transceivers (nTDM) as baseline. The results show that qTDM can achieve substantial cost-savings in the range of 10%–40% compared to nTDM. Furthermore, this work sheds light on the selection of the value for the working cycle T and its influence on network performance.

1. Introduction

Quantum technologies have emerged as viable tools with the potential to revolutionize various fields, ranging from secure communication and computing to precision measurement and sensing [1]. In the realm of security, the implications are profound. Quantum computers pose a substantial threat to data integrity, exposing the inherent vulnerability of existing security frameworks to their computational capabilities [2]. In turn, Quantum Key Distribution (QKD) promises security against such quantum threats.

QKD is a cryptography technique that leverages the principles of quantum mechanics to enable secure communication between two parties. It involves the transmission of quantum bits or qubits over a communication channel, where the properties of quantum particles ensure the detection of any eavesdropping attempts. QKD provides a secure exchange of cryptography keys to face the power of quantum computers that could compromise traditional encryption methods [3].

While quantum computing is in its initial stages, and its integration into industrial contexts will be a gradual process [2], it is imperative to advance research in QKD and its compatibility with existing network infrastructure. This proactive approach ensures a secure transition into the quantum era, safeguarding data integrity.

To implement QKD systems at a network scale, various techniques have been explored, including optical switching, quantum repeaters, trusted relaying, and untrusted relaying [3]. Optical switches are the natural tool to build cost-effective QKD networks (QKDNs) because they allow the sharing of devices at the QKD layer [4,5] by enabling the routing and reconfiguration of quantum channels (q-chs) as in [6,7]. Despite this, switches introduce impairments in the quantum channel (q-ch), mainly in the form of losses, which reduce the key generation capacity [8]. Addressing these challenges is crucial for the effective deployment of QKDNs.

In addition, the limited distances supported by q-chs necessitate a relay mechanism to enable secret-key exchanges between any pair

* Corresponding author.
E-mail address: juanhern@it.uc3m.es (J.C. Hernandez-Hernandez).

https://doi.org/10.1016/j.future.2024.107557
Received 10 November 2023; Received in revised form 9 March 2024; Accepted 12 October 2024
Available online 23 October 2024

of nodes in a network. This need has driven research into quantum repeaters as potential solutions [9–11]. Although quantum repeaters are promising, their maturity for real QKDN deployment is still a pending task. For the time being, the best practice implies relying on trusted relays [12]. Trusted relaying, combined with the use of the One-Time Pad (OTP) encryption [13], facilitates the generation of quantum keys by any pair of nodes in the network at acceptable rates.

Under trusted relays, intermediate nodes perform key storage and break the continuity of the q-ch, whereas untrusted relay schemes do not use key storage and simply extend the length of the q-ch [14]. However, this latter extension is not unbounded and cannot be cascaded, so trusted nodes remain necessary, in practice, in a network-wide extension. Therefore, most of the research on QKDN planning and optimization has focused on trusted relaying. This is also the target scenario of our work, supported by the use of optical switching.

On the other side, the past decade has witnessed experimental demonstrations of various QKD protocols, making significant progress towards realistic QKDN deployments. Existing QKD protocols, including Bennett–Brassard-1984 (BB84), Coherent One-way, Measurement Device Independent, and Twin Field, among others, have been comprehensively studied [3]. Numerous experiments, such as those highlighted in [15–19], attest to the feasibility of these protocols. However in our work, to avoid adding variables that can blur the real effect of shared QKD transceivers, we have used only BB84 in our simulations, although the model may easily be extended to consider other protocols, applying the principles of hybrid schemes like in [12].

However, the deployment of optical QKDNs is quite challenging from a techno-economic point of view [20], since the currently available commercial equipment required to establish a single q-ch features prices starting at 5-digit in dollars. This factor is likely to hinder the creation of large QKDNs and the rapid massive deployment of this technology. Therefore, ways to improve the utilization of the QKD transceivers[1] seem to be of great practical interest.

In a QKDN deployment, it is essential to take the target application scenario into account, as it dictates the necessary connectivity and secret-key demands. Our focus is focused on a specific use case illustrated in Fig. 1—the Quantum Virtual Private Network (qVPN) scenario. This scenario can include critical government or corporate data centers that host databases and applications requiring fully secure point-to-point connectivity across different locations. Applications in different locations can exchange data securely across the infrastructure, leveraging end-to-end secret-key-based communications.

For example, a network administrator may seek to replicate a database securely on three nodes while restricting access to the data solely to applications running on those specific nodes. The keys exchanged over the QKDN are employed to encrypt qVPN tunnels, tailored to the specific applications utilizing the encrypted connection. The security of each connection is determined by the key renewal rate. Consequently, different qVPN instances exhibit different key renewal rates, ensuring adaptability to the diverse requirements of different applications. This scheme allows for bundling several related applications into the same qVPN, thus making the QKD system more scalable. The requests for keys will be initiated at nodes marked with arrows going down in Fig. 1, with their destinations identified by nodes featuring arrows going up. Arrows, also, have been incorporated into the discontinuous lines within the Physical Layer, to offer a visual representation of how the Software Defined Networking (SDN) agents manage the relay paths for keys (the SDN controller coordinating the agents is not shown in the picture for the sake of clarity). Consequently, each q-ch facilitates key generation via hop-by-hop OTP as long as the capacity to generate an equivalent amount of keys that support the OTP process is guaranteed on the relay links. The direction in which the q-ch is established on each link, a decision made by our tool considering the network resource allocated, is independent of the direction of the key relay managed by the SDN agent.

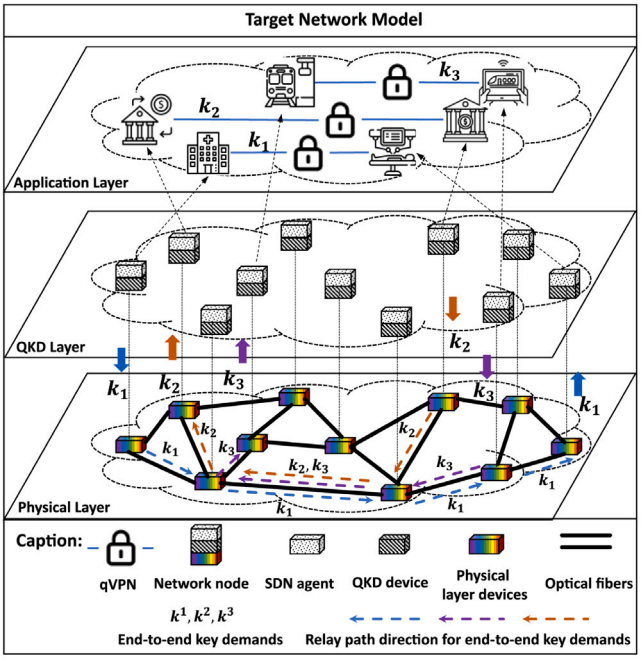


Fig. 1. qVPN: end-to-end key exchange over a QKDN.

Off-line QKDN resource planning requires determining in advance the target key rates intended to fulfill the security level for the communication among networked applications. This model operates under a pay-as-you-grow and fully guaranteed service framework, where the QKDN scales in response to the new demands of clients with no impact on the existing key rate reservations. In other words, the goal is to provide deterministic security levels in terms of key renewal rates.

Unlike scenarios that assume random dynamic requests, in our network model the QKDN manager pre-defines target key renewal rates (k in keys/s) between every pair of nodes. Transport Layer Security authentication and encryption within user applications are assumed to occur on top of the QKD Layer. Network performance control and orchestration are ensured by the SDN agent. Fig. 1 shows the routing of end-to-end secret key demands (k_1, k_2, k_3) among three pairs of nodes. On each link, the accumulative key demands of the relay paths traversing it must be generated, regardless of the path relay's direction. These keys will support a specific key relay mechanism (OTP), enabling the establishment of keys between non-adjacent end-to-end nodes [12]. The network designer and operator strategically allocate QKD-enabling resources, including QKD transceivers, optical switching devices, and q-chs, across the topology to meet every aggregated demand on the links.

In this paper, we introduce and study *qTDM-QKDN* (quantum transceiver TDM QKDN), a scheme in which QKD transceivers are shared over time by means of a pre-established periodic configuration. As originally proposed in [21], time-sharing QKD transceivers may be useful in reducing the cost of a QKDN with the help of configurable optical switches and QKD transceivers, via an SDN controller. This work develops the *qTDM-QKDN* concept thoroughly to understand the nature of the device-sharing problem on a periodic basis. We propose a practical model for planning and analyzing the potential cost-savings achievable under this approach. The problem is evaluated in the scenario of trusted key relaying, as the current best practice to make QKD scalable; however, the technique is also applicable to settings that include untrusted nodes. Although, in our work, we use BB84 as a

[1] The generic term *QKD transceiver* is used in this manuscript to refer to any of the endpoint devices in a q-ch, either transmitter (Tx) or receiver (Rx).

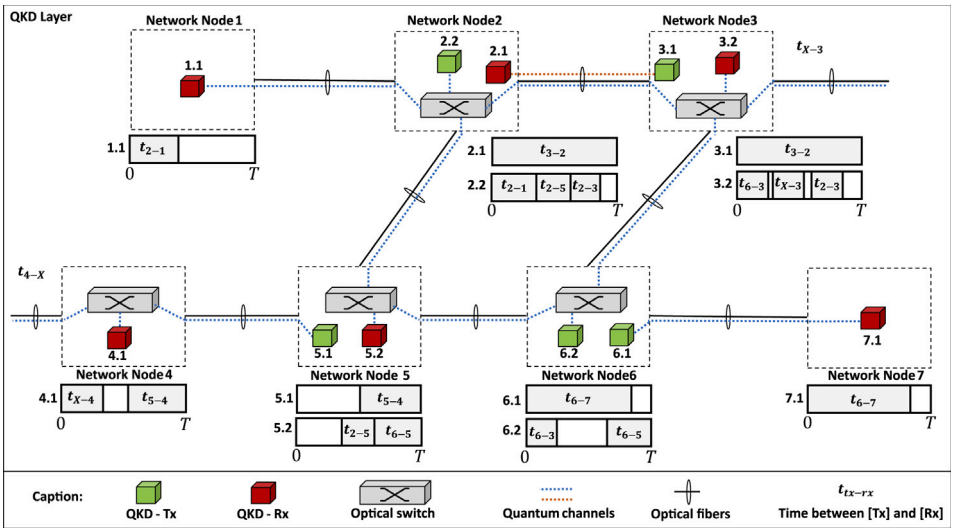


Fig. 2. Concept of Time-Division Multiplexing of quantum transceivers in a trusted-relay QKDN where the peering schedule is repeated each period T.

reference to compute the key generation rates on a q-ch, the planning technique introduced in this article is valid for any QKD protocol. The paper extends on two posters by the authors in [22,23] where the problem statement was made and some initial heuristic results were presented.

This article is organized as follows. Section 2 is a review of related work on QKDN design and optimization. Section 3 presents the time-sharing concept under study. Subsequently, the implications on the q-ch by using optical switches are analyzed in Section 4. Sections 5 and 6 introduce a mathematical programming model and a heuristic algorithm (HA) designed for planning and deploying QKDNs to meet the expected key renewal rates. The findings and conclusions are detailed in Sections 7 and 8.

2. Related work

The need to generate end-to-end secret keys within QKDNs has led to intense research in this area. Most approaches assume random arrivals of secret key requests or key exchange rate requests, as seen in works such as [6,24–28]. For instance, in [26], nodes maintain a pool of pre-generated keys, refilling it when their quantity falls below a pre-set threshold, in order to deal with the uncertainty of real-time request completion. The work in [29] suggests employing multiple disjoint paths simultaneously to carry the dynamic demands to increase the throughput and improve security. However, problems such as delays in key generation and the likelihood of blocking persist under all dynamic schemes despite enhancements, especially when resources are limited [26,28].

In contrast, this paper looks into a less-explored deterministic scheme, where target secret-key demands between non-adjacent nodes are predetermined as part of the QKDN's security policy [30–33] and applications consume, during a period T, the keys generated and stored in the precedent period T. This is an original key management scheme that we adopt in combination with periodic-based time-sharing.

The concept of time-sharing in QKDNs has been explored in past works, primarily in two forms: time-shared QKD transceivers [21,22,26,34] and time-shared QKD links [24,31,35]. While [21] introduced a field test of SDN-based resource scheduling mechanism for time-sharing a QKD receiver among multiple transmitters, applicable to point-to-point links and limited multi-hop paths, and [34] investigated recalibration time and key rate impacts of optical switches, these studies were conducted in small-scale laboratory settings. In contrast, our work addresses sharing at the network scale, aiming at programming large- and medium-scale QKDNs.

Moreover, the peculiar performance of the QKD technologies constrained by the q-ch length and the high device costs have fueled the research efforts in optimal deployment. Prior works [20,32,36] focused on optimizing QKD transceiver spatial distribution, minimizing the cost of deploying QKD-over Wavelength Division Multiplexing (WDM) backbone networks. While [12] proposed a hybrid deployment perspective using trusted and untrusted relays, and [37,38] advocated mixed ILP-based optimization, the approaches do not include periodic TDM-sharing for deployment cost optimization nor periodic key provisioning.

On the other hand, our work shares partially its objectives with [39], which investigates the reduction of QKD transceivers using optical switches. However, its emphasis is set on assessing the impact on key generation rates within a single path, lacking the scaling of the problem to a network environment with complex topologies. This involves accounting for the number of enabling resources such as switches or quantum channels, the number of transceivers for each node in the network, and how the relationships between them will be. These tasks are addressed in our work.

In summary, to the best of our knowledge, existing works have not comprehensively addressed the computation and minimization of the QKD-enabling resources required to support periodic secret-key demands on a time-sharing QKD transceiver scheme. The allocation of QKD-enabling resources is performed taking into due account the q-ch impairments that affect the key rate and the important overhead implied by re-starting QKD sessions when switching over, unlike previous works. Our contribution lies in providing a full mathematical model of the qTDM-QKDN concept, able to calculate for a target set of demands: (1) the minimum QKD transceivers at each node, (2) q-chs between every node pair, (3) quantum peerings and connection time between adjacent devices, and (4) required switch ports at each node.

3. qTDM-QKDN concept

Fig. 2 shows an overview of the qTDM-QKDN target network model. This scheme works based on a period T, during which a QKD transceiver may peer with some adjacent devices to generate keys, may be idle for some time, or even establish a directed connection without passing through an optical switch. For each end-to-end request of keys, one or even backup paths will be established to provide keys

for key relaying on the links that make up the selected paths. The key relay process is performed through trusted relays using OTP, as in conventional trusted relay schemes (for example, in [12]). For that, our network design must be able to provide as many keys in the relay links as end-to-end key requests are using it. In the case of key relaying, it occurs progressively on intermediate links as long as generated keys exist in the key storage at both ends of the link. Thus, when the cycle T ends, the end-to-end keys that need key relaying will be available on both non-neighbor network nodes.

The actions that take place during the period T are commanded by a central SDN controller which configures the optical switches and restarts the QKD process for each device whenever a switching event occurs. Optical switches are used to split T into time-windows (see Fig. 2) to enable the sharing of QKD transceivers. The SDN controller also drives the end-to-end key exchange with OTP and keeps the key store of each node filled at the pace required to satisfy the target demands. These key demands are set in advance by the QKDN manager according to the security level required between each pair of nodes. The SDN and key storage controllers needed to orchestrate the network are not shown in Fig. 2 for the sake of simplicity. They are common elements of time-shared and non-time-shared QKDN, and hence they do not make any difference in deployment costs.

The concept in Fig. 2 constitutes an example of what our tools pursue. For instance, node 5 needs two QKD transceivers to meet the key demands that traverse all its links according to the demands around it and computed by the tools. To this end, device 5.1 will peer with 4.1 during a time t_{5-4}, and device 5.2 will be shared by 2.2 and 6.2, for times t_{2-5} and t_{6-5}, respectively. In other words, the tools determined that the sum of all the service time needed at node 5 (t_{5-4}, t_{2-5}, t_{6-5}) is greater than T but less than $2 \cdot T$, and therefore two QKD transceivers were assigned to this node. To make it possible that Node 4 and 3 have exchange keys in the intermediate links of its path – let's say links (3,2), (2,5), (5,4) – within the time devoted to each connection t_{5-4}, t_{6-5}, t_{6-3} enough number of keys have to be available to apply OTP and relay the keys for the request from 4 to 3 and for all request that use this link. Thus, all key storage on the network will be filled before T finishes. In this way, the scheduler guarantees that during the current period T the keys generated are enough to match the demand for the next period T. Thus, in the next period, these keys will be consumed by the application running on each node, while on the QKD Layer, the keys for the next period are being generated.

For the sake of maximum efficiency, given the reduction in the effective key rate with distance and the use of the switches, our model also considers the possibility of having transceivers that avoid the switch when is not worth sharing. It occurs in cases where time sharing would not be efficient due to switching overhead or because the device has high utilization with a single connection. For example, device 5.1 is not attached to the switch to avoid additional switching impairments.

After the deployment phase or interruptions due to malfunctions, the proposed system requires a bootstrapping time for generating keys before the nodes can restart exchanging keys. If waiting for a bootstrapping time is not possible pre-shared keys, refreshed from time to time, might be a good strategy to overcome this issue.

In summary, our tools can calculate the number of QKD transceivers and q-chs needed to satisfy a required target set of demands. In addition, it can compute the share of T that the devices will devote to each neighbor transceiver and discriminate where to use optical switches to take advantage of reusing devices for multiple connections it is possible.

4. Practical issues of switched QKD channels

In the context of switched QKDNs, specifically within the qTDM-QKDN framework, two practical challenges arise. The first consideration is the switching and recalibration time t_s of a q-ch after a switching event [8]. A straightforward approach to minimize the relative impact of recalibration is to set the period for the TDM process T (an open design variable in our model) such that $T \gg t_s$. However, this approach discussed in-depth in Section 7, may result in a longer working cycle for the network. This would reduce the network's responsiveness to potential malfunctions or variations in key requests from the network administrator. In qTDM-QKDN, we assume the selection of T to be predefined before the solver or algorithm computes the paths for the end-to-end demands and the QKD-enabling resources.

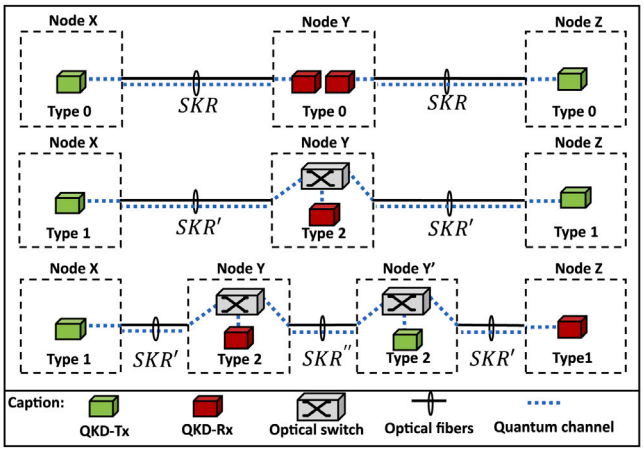


Fig. 3. The three possible settings for a q-ch in qTDM-QKDN regarding optical switch crossover.

The second aspect involves being aware that an optical switch within the q-ch introduces insertion loss and crosstalk, thereby reducing the secret key rate compared to an equivalent q-ch without a switch in the middle [8]. To mitigate these effects, our approach in qTDM-QKDN imposes constraints on the utilization of optical switches, as depicted in Fig. 2. This strategy ensures that the deployment does not introduce more QKD transceivers than a conventional setup without applying TDM, as illustrated in Section 7. Instead, it leverages the idle time of unshared transceivers for efficiency in the use of those expensive resources. However, if these advantages cannot be harnessed for certain nodes, unshared QKD transceivers implementation becomes necessary.

According to the cross-connection of a q-ch through a switch in qTDM-QKDN, three distinct settings can be identified, as illustrated in Fig. 3. At the top, a q-ch directly connects a pair of QKD transceivers, achieving a secret key rate (SKR). In the middle setting, q-chs facilitating peering with the central device (red square) must traverse the switch dedicated to sharing the central device. Here, both q-chs (X-Y and Z-Y) are affected by switch impairments, resulting in a lower secret key rate (SKR') compared to SKR. Finally, in the bottom setting, while q-chs from node X to Y and node Y' to Z mirror the middle case, the q-ch between node Y and node Y' must pass through two switches if a peering between connected devices is required. This leads to the lowest secret key rate (SKR'') among all settings. Therefore, the hierarchy follows $SKR > SKR' > SKR''$. Furthermore, QKD transceivers can be categorized into three possibilities. A QKD transceiver is labeled as type 0 when it establishes an unshared connection. If the output interface of a Tx or receiver Rx is not linked to a co-located optical switch but is connected at the other end, it falls into type 1 (illustrated by green squares in the SKR' case in Fig. 3). Lastly, devices are classified as type 2 if the transceivers at both ends of the q-ch have co-located an optical switch.

Therefore, to assess the impact of switching on the secret key rate (SKR) concerning the q-ch length (l) and the impairments introduced by the switch, we shall use as a reference the theoretical estimation given by [8,40] for a particular realization of decoy-state BB84 protocol where:

$$SKR = q \cdot \{Q_1^L - Q_1^L \cdot H_2(e_1^U) - Q_\mu \cdot f_{ec} \cdot H_2(E_\mu)\}, \quad (1)$$

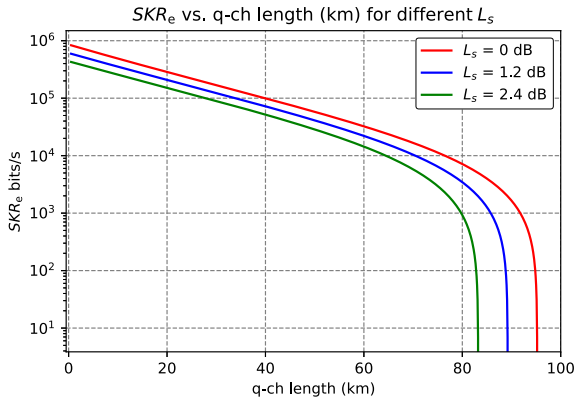


Fig. 4. Effective key rate estimation $SKR_e(bits/s)$ used for BB84.

where q is the basis reconciliation factor that depends on the implementation of the protocol, $q = 0.5$ for the standard BB84 protocol because the probability that the transceivers have chosen a compatible base is 50%. Furthermore, The subscript μ represents the intensity of signal states, and Q_μ corresponds to the gain of these signal states. E_μ is used to denote the overall quantum bit error rate (QBER), while Q_1^L is associated with the lower bound for the gain of single photon states. Additionally, e_1^U denotes the upper bound of the error rate of single photon states. H_2 is the binary Shannon entropy function given by $H_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$. The efficiency of error correction is f_{ec}.

Using optomechanical switches with crosstalk levels below −20 dB, as demonstrated in previous work [8], results in negligible penalties within the q-ch. Consequently, the transmittance of each q-ch is predominantly determined by the fiber loss coefficient, denoted as α, and the insertion loss of the optical switches L_s.

$$\eta = \eta_{Rx} \cdot 10^{-\frac{\alpha l + L_s}{10}} \tag{2}$$

The receiver intrinsic transmittance is η_{Rx}, α takes a standard monomode fiber value of 0.2 dB/km, l and L_s are the q-chs length, and the insertion loss of the switch, respectively. $L_s = \{0, 1.2, 2.4\}$ dB for each q-ch described in Fig. 3. According to [40] the lower bound for Q_1 and the upper bound for e_1 can be estimated by

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\upsilon - \upsilon^2}\left[Q_\upsilon \cdot e^\upsilon - Q_\mu \cdot e^\mu \frac{\upsilon^2}{\mu^2} - E_\mu \cdot Q_\mu \cdot e^{-\mu}\frac{\mu^2 - \upsilon^2}{0.5\mu^2}\right], \tag{3}$$

$$e_1^U = \frac{E_\mu \cdot Q_\mu}{Q_1^L}. \tag{4}$$

Finally, the overall gain in signal states and decoy states through the desired transmission path and the overall QBER in signal states can be described as [8]

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{5}$$

$$Q_\upsilon = Y_0 + 1 - e^{-\eta\upsilon} \tag{6}$$

$$E_\mu = \frac{e_0 \cdot Y_0 + e_d(1 - e^{-\eta\mu})}{Q_\mu} \tag{7}$$

Assuming $\mu = 0.48$, $\upsilon = 0.05$, $Y_0 = 6.8 \cdot 10^{-6}$, $e_d = 2.3$ %, $e_0 = 1/2$, $f_{ec} = 1.22$ and $\eta_{Rx} = 0.1$ like was described on the experiments of [8,40], we can obtain a function $SKR(l)$ in bits per pulse. To convert it to bits per second, we assume a typical value of the time window of 2.5 GHz [16]. However, the SKR estimation (shown in Fig. 4) includes also the privacy amplification process, which consumes several shared bits, so that only 1 out 3 are finally used for generating keys.

Table 1
Notation and definitions.

Notation	Definition
N	Set of optical/QKD nodes n
E	Set of available bidirectional links (i,j) with $i,j \in N$
$G(N,E)$	Optical/QKD network
L	Key length according to the encryption protocol used [bits]
k_r	Key rate for request r [keys/s]
R	Set of requests $r = (src, dst, k)$ $src, dst \in N$ $k \in \mathbb{R}$
X	Set of slots available in $n \in N$ to allocate devices of type 0
Y	Set of slots available in $n \in N$ to allocate devices of type 1
Z	Set of slots available in $n \in N$ to allocate devices of type 2
S	Set of switchable ports available in each optical switch
ρ	A path (sequence of links (i,j))
Ψ_r	Set of all candidate paths ρ for r
ρ^r	Candidate path ρ for a key request r
$l_{(i,j)}$	Length in kilometers of link (i,j)
$h_{(i,j)}$	Accumulated demand on the link (i,j) [keys/s]
$SKR_{(i,j)}$	Secret key rate of a q-ch (i,j) [bits/s]
t_s	Switching and re-calibration time of a q-ch [s]
m	Path multiplicity $\forall r \in R$. Normally $m = 1$ unless redundant backup paths are required
T	Time period for TDM [s]
β_n	Set of all neighboring nodes j of n where $h_{(i,j)} \neq 0, i = n$
$\bar{\epsilon}$	Average relative cost difference between MILP and HA
Ω_ρ	Set storing the rate $h_{(i,j)} \cdot L/SKR_{(i,j)} \forall (i,j) \in \rho, h_{(i,j)} \neq 0$
T_n^{total}	Number of Tx allocated at node n
R_n^{total}	Number of Rx allocated at node n
S_n^{total}	Number of optical switch ports allocated at node n
$Q_{ch_{(i,j)}}^{total}$	Number of q-ch needed to be placed on the link (i,j)
T_n, T_n', T_n''	Number of type 0, type 1 and type 2 Tx respectively, allocated at node n using qTDM-HA
R_n, R_n', R_n''	Number of type 0, type 1 and type 2 Rx respectively, allocated at node n using qTDM-HA
δ_{T_n}	Set of links peering the node n, which has Tx capability, with neighbor nodes with Rx capability
δ_{R_n}	Set of links peering the node n, which has Rx capability, with neighbor nodes with Tx capability
C_T^u	Cost of one Tx unit [cost units, cu]
C_T^{total}	Total cost of Tx allocated [cost units, cu]
C_R^u	Cost of one Rx unit [cost units, cu]
C_R^{total}	Total cost of Rx allocated [cost units, cu]
C_S^u	Cost of one switch port unit [cost units, cu]
C_S^{total}	Total cost of switch ports allocated [cost units, cu]
C_{Ch}^u	Cost of establishing one km of q-ch [cost units, cu]
C_{Ch}^{total}	Total cost for q-ch allocated in the network [cost units, cu]
$C_{nTDM}^{total}, C_{qTDM}^{total}$	Total cost of deployment with nTDM and qTDM respectively [cost units, cu]
$\Delta_{(i,j)}$	Time devoted to a q-ch on (i,j) that is using a shared device
$W_{(i,j)}$	Time devoted to all q-ch on (i,j) associated with pairs of transceivers of type 0
$F_T, F_{T'}, F_{T''}$	Accumulative factor that groups the sum of the time fractions devoted in type 0, type 1, and type 2 Tx devices
$F_R, F_{R'}, F_{R''}$	Accumulative factor that groups the sum of the time fractions devoted in type 0, type 1, and type 2 Rx devices
$RU_{qTDM}^{mean}(\%)$	Mean of resource utilization in a network under qTDM
$RU_{nTDM}^{mean}(\%)$	Mean of resource utilization in a network under nTDM

5. Mixed integer linear programming for qTDM-QKDN: qTDM-MILP

This section presents a cost-minimization model for deploying qTDM-QKDN over an optical network with spare fibers designated for QKD. The model can be seen as a WDM network employing shared QKD transceivers, with the optical switches serving as the WDM equipment. Table 1 defines the model's parameters and variables, while Table 2 introduces the decision variables used in this work. Objective functions, constraints, and auxiliary definitions will be explained throughout the section.

Table 2
Decision variables.

Variable	Definition
$p^{r}_{th,\rho}$	Binary variable indicating if, for request r, the nodes on path ρ have alternate Tx and Rx (1) or not (0)
$T_{n,x}(R_{n,x})$	Binary variable indicating if a type 0 Tx (Rx) is assigned to node n in slot x (1) or not (0)
$T'_{n,y}(R'_{n,y})$	Binary variable indicating if a type 1 Tx (Rx) is assigned to node n in slot y (1) or not (0)
$T''_{n,z}(R''_{n,z})$	Binary variable indicating if a type 2 Tx (Rx) is assigned to node n in slot z (1) or not (0)
$c_{(i,x),(j,x')}$	Binary variable indicating if a Tx at node i in slot x and an Rx at node j in slot x' establish a connection (1) or not (0)
$c'_{(i,z,s),(j,y)}$	Binary variable indicating if a Tx at node i in slot z through switch port s and an Rx at node j in slot y establish a connection (1) or not (0)
$c'_{(i,y),(j,z,s)}$	Binary variable indicating if a Tx at node i in slot y and a Rx at node j in slot z through switch port s establish a connection (1) or not (0)
$c''_{(i,z,s),(j,z',s')}$	Binary variable indicating if a Tx at node i in slot z through switch port s and an Rx at node j in slot z' through switch port s' establish a connection (1) or not (0)
$\alpha_{(i,x),(j,x')}$	Continuous variable representing the time devoted to key generation if $c_{(i,x),(j,x')} = 1$
$\alpha'_{(i,z,s),(j,y)}$	Continuous variable representing the time devoted to key generation if $c'_{(i,z,s),(j,y)} = 1$
$\alpha'_{(i,y),(j,z,s)}$	Continuous variable representing the time devoted to key generation if $c'_{(i,y),(j,z,s)} = 1$
$\alpha''_{(i,z,s),(j,z',s')}$	Continuous variable representing the time devoted to key generation if $c''_{(i,z,s),(j,z',s')} = 1$

Let $h_{(i,j)}$ represent the accumulative key demands k_r on the link (i,j) so that $h_{(i,j)} - h_{(j,i)} = 0$, accounting from quantum relay paths ρ that include both (i,j) and (j,i) (see Eq. (8)). This means that a key demand routed over the link $i \to j$ can be fulfilled by a q-ch set up from a Tx at node i to an Rx at node j or vice versa.

$$h_{(i,j)} = \sum_{r\in R}\sum_{\rho\in\Psi_r} k_r \cdot p^{r}_{th\,\rho} \quad \forall (i,j)\in E, (i,j)\vee(j,i)\in\rho \tag{8}$$

Eqs. (9) and (10) define T^{total}_n and R^{total}_n respectively, as the required number of Tx and Rx at each node n to fulfill the accumulated demand $h_{(i,j)}$ due to specific paths routed over (i,j). Both T^{total}_n and R^{total}_n include all types of transceivers mentioned in Section 4. In turn, S^{total}_n at Eq. (11) defines how to compute the number of allocated optical switch ports at node n, and $Q_{ch_{(i,j)}}$ at Eq. (12) determines the number of established q-chs on the link (i,j) following the rule that a Tx was allocated at i and a Rx at j otherwise $Q^{total}_{ch_{(i,j)}} = 0$.

$$T^{total}_n = \sum_{x\in X} T_{n,x} + \sum_{y\in Y} T'_{n,y} + \sum_{z\in Z} T''_{n,z} \quad \forall n\in N \tag{9}$$

$$R^{total}_n = \sum_{x\in X} R_{n,x} + \sum_{y\in Y} R'_{n,y} + \sum_{z\in Z} R''_{n,z} \quad \forall n\in N \tag{10}$$

$$S^{total}_n = \begin{cases} \sum\limits_{\substack{(i,j)\in E\\ i=n}}\sum\limits_{z\in Z}\sum\limits_{s\in S}\sum\limits_{y\in Y}\left[c'_{(i,z,s),(j,y)} + c'_{(j,y),(i,z,s)}\right] + \\ \sum\limits_{\substack{(i,j)\in E\\ i=n}}\sum\limits_{z\in Z}\sum\limits_{s\in S}\sum\limits_{z'\in Z}\sum\limits_{s'\in S}\left[c''_{(i,z,s),(j,z',s')} + c''_{(j,z,s),(i,z',s')}\right] + \\ \sum\limits_{z\in Z}\left[T''_{n,z} + R''_{n,z}\right] \end{cases} \quad \forall n\in N \tag{11}$$

$$Q^{total}_{ch_{(i,j)}} = \begin{cases} \sum\limits_{x\in X}\sum\limits_{x'\in X} c_{(i,x),(j,x')} + \\ \sum_{y\in Y}\sum_{z\in Z}\sum_{s\in S}\left[c'_{(i,z,s),(j,y)} + c'_{(i,y),(j,z,s)}\right] + \\ \sum\limits_{z\in Z}\sum\limits_{s\in S}\sum\limits_{z'\in Z}\sum\limits_{s'\in S} c''_{(i,z,s),(j,z',s')} \end{cases} \quad \forall (i,j)\in E \tag{12}$$

The cost model contemplates not just the cost for QKD transceivers (in Eqs. (13) and (14) respectively) but also the cost of enabling the qTDM-QKDN concept such as q-chs and switch ports (in Eqs. (15) and (16) respectively).

$$C^{total}_T = C^{u}_T \cdot \sum_{n\in N} T^{total}_n \tag{13}$$

$$C^{total}_R = C^{u}_R \cdot \sum_{n\in N} R^{total}_n \tag{14}$$

$$C^{total}_S = C^{u}_S \cdot \sum_{n\in N} S^{total}_n \tag{15}$$

$$C^{total}_{Ch} = C^{u}_{Ch} \cdot \sum_{(i,j)\in E} Q^{total}_{ch_{(i,j)}} \cdot l_{(i,j)} \tag{16}$$

The objective function (see Eq. (17)) is to minimize the total deployment cost for qTDM-QKDN (C^{total}_{qTDM}). It is calculated using the expression that gathers all the contributions mentioned before.

$$C^{total}_{qTDM} = C^{total}_T + C^{total}_R + C^{total}_S + C^{total}_{Ch} \tag{17}$$

The objective function is constrained by Eq. (18) to Eq. (35). Thus, Eq. (18) guarantees that each key demand between two end-to-end nodes $r \in R$ has a minimum multiplicity of m quantum paths. Path multiplicity is included in case path redundancy is required.

$$m - \sum_{\rho\in\Psi_r} p^{r}_{th,\rho} \leqslant 0 \quad \forall r\in R \tag{18}$$

In qTDM-QKDN, feasible paths include configurations such as [Tx] - [Rx] - [Tx], where Rx is shared by both Tx, or [Rx] - [Tx] - [Rx] when a Tx is shared by both Rx (QKD transceivers enclosed in [ ] represent network nodes with the corresponding transceivers allocated). Additionally, configurations like [Tx] - [Rx Tx] - [Rx], [Tx] - [Rx Rx] - [Tx], or [Rx] - [Tx Tx] - [Rx] are available to be implemented. The latter solutions mirror those provided for the benchmark non-time-sharing for QKD networks, as elucidated in Section 7. However, in these cases, the intermediate transceivers are unshared, and our objective is to minimize such instances while fulfilling the key demands.

In case a pair of QKD transceivers at both ends of the link (i,j) need to establish a connection all or only a fraction of the time T, then a q-ch has to be settled. This q-ch cannot be re-used for other pair of QKD transceivers to set a connection. This uniqueness is ensured by the Eq. (19) to Eq. (24).

$$\sum_{\substack{(i,j)\in E\\ i=n}}\sum_{x'\in X} c_{(i,x),(j,x')} \leqslant 1 \quad \forall x\in X, n\in N \tag{19}$$

$$\sum_{\substack{(i,j)\in E\\ j=n}}\sum_{x\in X} c_{(i,x),(j,x')} \leqslant 1 \quad \forall x'\in X, n\in N \tag{20}$$

$$\sum_{\substack{(i,j)\in E\\ i=n}}\sum_{z\in Z}\sum_{s\in S} c'_{(i,y),(j,z,s)} \leqslant 1 \quad \forall y\in Y, n\in N \tag{21}$$

$$\sum_{\substack{(i,j)\in E\\ j=n}}\sum_{z\in Z}\sum_{s\in S} c'_{(i,z,s),(j,y)} \leqslant 1 \quad \forall y\in Y, n\in N \tag{22}$$

$$\sum_{\substack{(i,j)\in E\\ i=n}}\sum_{y\in Y} c'_{(i,z,s),(j,y)} + \sum_{\substack{(i,j)\in E\\ i=n}}\sum_{z'\in Z}\sum_{s'\in S} c''_{(i,z,s),(j,z',s')} \leqslant 1 \qquad \begin{matrix}\forall s\in S,\\ z\in Z, n\in N\end{matrix} \tag{23}$$

$$\sum_{\substack{(i,j)\in E\\ j=n}}\sum_{y\in Y} c'_{(i,y),(j,z,s)} + \sum_{\substack{(i,j)\in E\\ j=n}}\sum_{z'\in Z}\sum_{s'\in S} c''_{(i,z',s'),(j,z,s)} \leqslant 1 \qquad \begin{matrix}\forall s\in S,\\ z\in Z, n\in N\end{matrix} \tag{24}$$

The constraints given by Eqs. (25) to (28) determine when a QKD transceiver must be allocated at the end of a link according to the q-chs established on that link or vice versa. For example if $c_{(i,x),(j,x')} = 1$, it just can be possible if $T_{n,x} = 1$ and $R_{n',x'} = 1$. The example can also be read starting from the end.

$$2\cdot c_{(i,x),(j,x')} - T_{n,x} - R_{n',x'} \leqslant 0 \qquad \begin{matrix}\forall (i,j)\in E,\\ x'\in X, x\in X,\\ n=i, n'=j\end{matrix} \tag{25}$$

$$2\cdot c'_{(i,z,s),(j,y)} - T''_{n,z} - R'_{n',y} \leqslant 0 \qquad \begin{matrix}\forall (i,j)\in E,\\ z\in Z, y\in Y, s\in S,\\ n=i, n'=j\end{matrix} \tag{26}$$

$$2 \cdot c'_{(j,y),(i,z,s)} - T'_{n,y} - R''_{n',z} \leqslant 0 \qquad \begin{matrix} \forall (i,j) \in E, \\ z \in Z, y \in Y, s \in S, \\ n = j, n' = i \end{matrix} \tag{27}$$

$$2 \cdot c''_{(i,z,s),(j,z',s')} - T''_{n,z} - R''_{n',z'} \leqslant 0 \qquad \begin{matrix} \forall (i,j) \in E, z' \in Z, \\ s \in S, z \in Z, s' \in S, \\ n = i, n' = j \end{matrix} \tag{28}$$

Constraints from (29) to (32) guarantee the allocation of dedicated time ($\alpha, \alpha', \alpha''$) for the establishment of a q-ch between QKD transceiver pairs. When a pair of QKD transceivers on a link is of type 0, the dedicated time for key generation is α (Eq. (29)). If one transceiver is type 1 and the other type 2, the devoted time for key generation is α'. Finally, if both are type 2, the connection will be established during a time α''. For α' and α'', the maximum time to be allocated to a q-ch must consider the overhead of switching and re-calibration time of QKD transceivers for every switching event, denoted as t_s.

$$\alpha_{(i,x),(j,x')} - T \cdot c_{(i,x),(j,x')} \leqslant 0 \qquad \begin{matrix} \forall x' \in X, x \in X, \\ (i,j) \in E \end{matrix} \tag{29}$$

$$\alpha'_{(i,z,s),(j,y)} - (T - t_s) \cdot c'_{(i,z,s),(j,y)} \leqslant 0 \qquad \begin{matrix} \forall s \in S, z \in Z, \\ y \in Y, (i,j) \in E \end{matrix} \tag{30}$$

$$\alpha'_{(j,y),(i,z,s)} - (T - t_s) \cdot c'_{(j,y),(i,z,s)} \leqslant 0 \qquad \begin{matrix} \forall s \in S, z \in Z, \\ y \in Y, (i,j) \in E \end{matrix} \tag{31}$$

$$\alpha''_{(i,z,s),(j,z',s')} - (T - t_s) \cdot c''_{(i,z,s),(j,z',s')} \leqslant 0 \qquad \begin{matrix} \forall s' \in S, z' \in Z, s \in S, \\ z \in Z, (i,j) \in E \end{matrix} \tag{32}$$

The key generation process in our approach is carried out within a period T on every QKD transceiver even for those that have to share their working time among others, as we mentioned in Section 3. To do so, we set the constraints (33) and (34), which restrict the time spent on each shared QKD transceiver to be less than or equal to the cycle T.

$$\left(\begin{matrix} \sum\limits_{\substack{(i,j)\in E \\ i=n}} \sum\limits_{y\in Y} \sum\limits_{s\in S} \left[\alpha'_{(i,z,s),(j,y)} + t_s \cdot c'_{(i,z,s),(j,y)} \right] + \\ \sum\limits_{\substack{(i,j)\in E \\ i=n}} \sum\limits_{s\in S} \sum\limits_{z'\in Z} \sum\limits_{s'\in S} \left[\alpha''_{(i,z,s),(j,z',s')} + t_s \cdot c''_{(i,z,s),(j,z',s')} \right] - T \end{matrix} \right) \leqslant 0 \quad \forall z \in Z, n \in N \tag{33}$$

$$\left(\begin{matrix} \sum\limits_{\substack{(i,j)\in E \\ j=n}} \sum\limits_{y\in Y} \sum\limits_{s\in S} \left[\alpha'_{(i,y)(j,z,s)} + t_s \cdot c'_{(i,y)(j,z,s)} \right] + \\ \sum\limits_{\substack{(i,j)\in E \\ j=n}} \sum\limits_{s\in S} \sum\limits_{z'\in Z} \sum\limits_{s'\in S} \left[\alpha''_{(i,z',s'),(j,z,s)} + t_s \cdot c''_{(i,z',s'),(j,z,s)} \right] - T \end{matrix} \right) \leqslant 0 \quad \forall z \in Z, n \in N \tag{34}$$

Last but not least, the constraint (35) ensures establishing as many q-chs as needed to fulfill the value of $h_{(i,j)}$ on a link (i,j) during a time T. As can be seen, this constraint is in charge of computing the times required for each type of channel established on the link (i,j) so that the accumulated key demand on the link $h_{(i,j)}$ is satisfied.

$$h_{(i,j)} - \left(\begin{matrix} \frac{SKR_{(i,j)}}{T \cdot L} \cdot \sum\limits_{x\in X} \sum\limits_{x'\in X} \left[\alpha_{(i,x),(j,x')} + \alpha_{(j,x),(i,x')} \right] + \\ \frac{SKR'_{(i,j)}}{T \cdot L} \cdot \sum\limits_{y\in Y} \sum\limits_{z\in Z} \sum\limits_{s\in S} \left[\alpha'_{(i,z,s),(j,y)} + \alpha'_{(j,z,s),(i,y)} \right] + \\ \frac{SKR'_{(i,j)}}{T \cdot L} \cdot \sum\limits_{y\in Y} \sum\limits_{z\in Z} \sum\limits_{s\in S} \left[\alpha'_{(i,y),(j,z,s)} + \alpha'_{(j,y),(i,z,s)} \right] + \\ \frac{SKR''_{(i,j)}}{T \cdot L} \cdot \sum\limits_{z\in Z} \sum\limits_{s\in S} \sum\limits_{z'\in Z} \sum\limits_{s'\in S} \left[\alpha''_{(i,z,s),(j,z',s')} + \alpha''_{(j,z,s),(i,z',s')} \right] \end{matrix} \right) \leqslant 0 \quad \forall (i,j) \in E \tag{35}$$

Moreover, a key point of our study is the Resource Utilization (RU) of these expensive QKD transceivers. A network with a high RU ratio is essential to achieve a balance between capital expenditure and operating efficiency. The RU for a QKD transceiver is defined as the ratio of the useful working time (excluding the contribution of t_s as it does not contribute to useful key generation time) to the total working cycle for each transceiver, which is T. In broad terms, the mean of RU in a network is computed as the sum of the time corresponding to each connection divided by the number of active QKD transceivers. If using the same data inputs, we compare two different approaches to deploy a QKDN, for instance, a lower RU indicates that resources (in this case, the expensive QKD transceivers) are being used less efficiently with one approach compared to the other.

To compute RU under the qTDM-QKDN concept, we use Eq. (36). The numerator of this expression includes multiple factors F that depend on the nature of the QKD transceivers.

$$RU^{mean}_{qTDM}(\%) = \frac{F_T + F_R + F_{T'} + F_{R'} + F_{T''} + F_{R''}}{\sum_{n\in N} \left(T^{total}_n + R^{total}_n \right)} \cdot 100 \tag{36}$$

Thus, Eqs. (37) and (38) gather all the contributions from connections established by QKD transceivers of type 0, being determined by the ratio of the time allocated for key generation to the cycle T if a q-ch is established from $i \rightarrow j$ for the link (i,j) (refer to Eq. (37)). Conversely, if the q-ch goes from $j \rightarrow i$, Eq. (38) is applied.

$$F_T = \frac{1}{T} \cdot \sum_{n\in N} \sum_{x\in X} \sum_{\substack{(i,j)\in E \\ i=n}} \sum_{x'\in X} \alpha_{(i,x),(j,x')} \tag{37}$$

$$F_R = \frac{1}{T} \cdot \sum_{n\in N} \sum_{x'\in X} \sum_{\substack{(i,j)\in E \\ j=n}} \sum_{x\in X} \alpha_{(i,x),(j,x')} \tag{38}$$

In the case of QKD transceivers of type 1, t_s should be excluded from the formulation, as is well reflected in α' which does not include this overhead. Despite t_s being a working time of QKD transceivers, it does not lead to the generation of keys. Including it would artificially inflate the value of RU (refer to Eqs. (39) and (40)). Thus, the factors $F_{T'}$ and $F_{R'}$ account for the contribution on itself, while the incidence of this time at the other end of the q-ch where it shares time on a shared device is accounted for by $F_{T''}$ and $F_{R''}$.

$$F_{T'} = \frac{1}{T} \cdot \sum_{n\in N} \sum_{y\in Y} \sum_{\substack{(i,j)\in E \\ i=n}} \sum_{z\in Z} \sum_{s\in S} \alpha'_{(i,y),(j,z,s)} \tag{39}$$

$$F_{R'} = \frac{1}{T} \cdot \sum_{n\in N} \sum_{y\in Y} \sum_{\substack{(i,j)\in E \\ j=n}} \sum_{z\in Z} \sum_{s\in S} \alpha'_{(i,z,s),(j,y)} \tag{40}$$

Finally, if a QKD transceiver is shared among others (type 2), its factor F to compute the RU is determined by the accumulative time devoted to the q-chs established through it. In this way, F includes the contribution from both q-chs those of transceivers of type 2 that connect to it, as well as those of type 1 that use the shared connection (see Eqs. (41) and (42)). Similar to the case before, t_s is not included in the value of α'' by definition.

$$F_{T''} = \frac{1}{T} \cdot \left(\begin{matrix} \sum\limits_{n\in N} \sum\limits_{z\in Z} \sum\limits_{\substack{(i,j)\in E \\ i=n}} \sum\limits_{s\in S} \sum\limits_{y\in Y} \alpha'_{(i,z,s),(j,y)} + \\ \sum\limits_{n\in N} \sum\limits_{z\in Z} \sum\limits_{\substack{(i,j)\in E \\ i=n}} \sum\limits_{s\in S} \sum\limits_{z'\in Z} \sum\limits_{s'\in S} \alpha''_{(i,z,s),(j,z',s')} \end{matrix} \right) \tag{41}$$

$$F_{R''} = \frac{1}{T} \cdot \left(\begin{matrix} \sum\limits_{n\in N} \sum\limits_{z\in Z} \sum\limits_{\substack{(i,j)\in E \\ j=n}} \sum\limits_{s\in S} \sum\limits_{y\in Y} \alpha'_{(i,y),(j,z,s)} + \\ \sum\limits_{n\in N} \sum\limits_{z\in Z} \sum\limits_{\substack{(i,j)\in E \\ j=n}} \sum\limits_{s\in S} \sum\limits_{z'\in Z} \sum\limits_{s'\in S} \alpha''_{(i,z',s'),(j,z,s)} \end{matrix} \right) \tag{42}$$

6. Heuristic algorithm for qTDM-QKDN: qTDM-HA

Given the scalability issues that integer programming models show to solve problems with a large number of variables, in this section, we propose an alternative heuristic algorithm, qTDM-HA, that let us find a close-to-optimal configuration for medium and large topologies in a short time.

Primarily, the newly defined sets δ_{T_n} and δ_{R_n} represent links (i,j) utilizing Tx or Rx capabilities at node n. If node n has a Tx capability, and adjacent nodes j with Rx capability use it, these links are stored

in δ_{T_n}; symmetrically, δ_{R_n} is utilized. For instance, in the configuration of QKD transceivers and optical switch ports in Fig. 2, that would be obtained using our proposed tools, examples of these sets (δ_{T_n} and δ_{R_n}) include $\delta_{T_2} = \{(2,1),(2,3),(2,5)\}$ and $\delta_{R_3} = \{(2,3),(6,3),(x,3)\}$.

The sets T_n, R_n, T'_n, R'_n, and sets of sets T''_n, R''_n indicate the type of QKD transceiver at any node, which may be of type 0, 1, or 2. Thus, T''_n and R''_n store groups of links (i,j) belonging to a shared device (Tx or Rx, respectively) at node n. In this manner, in T_n, R_n, T'_n and R'_n, links (i,j) are saved as QKD transceivers of type 0 and 1 using these links for which $n = i \vee n = j$. As an example in Fig. 2, some values would be $T_3 = \{(3,2)\}$, $R_2 = \{(3,2)\}$, $T'_5 = \{(5,4)\}$, $R'_1 = \{(2,1)\}$, $T''_2 = \{[(2,1),(2,5),(2,3)]\}$, $R''_5 = \{[(2,5),(6,5)]\}$. Lastly, $W_{(i,j)}$ represents the time dedicated to key generation, given that on link (i,j) one or more q-chs of type 0 are established. Similarly, $\Delta_{(i,j)}$ signifies the portion of time T for QKD transceivers of type 1 or 2 on link (i,j), including t_s, and $\Delta_{(i,j)} \leqslant T$.

In qTDM-HA, the central concept evolves around the selection of a path ($m = 1$) for each $r \in R$ and allocating a sequence of pairs Tx - Rx or Rx - Tx along those paths, but enabling time-sharing of QKD transceivers if possible. The qTDM-HA operations can be divided into three main steps outlined in a pseudo-code in Algorithm 1. Initially, qTDM-HA chooses the paths for routing key demands (lines 3 to 11 in Algorithm 1). Within these lines, a wise selection of quantum paths is conducted, emphasizing those that minimize the average network ($\overline{\Omega_\rho}$). Subsequently, qTDM-HA defines the connections of QKD transceivers and determines the required capability (Tx or Rx) for each node n (lines 12 to 25 in Algorithm 1). Finally, qTDM-HA calculates the necessary QKD transceivers and switch ports at each node, along with the number of q-chs on each link and the time allocated to each connection (lines 26 to 41 in Algorithm 1). Ultimately, the cost is computed.

The algorithm begins by initializing essential variables and sets. Note that a path is a sequence of links, and thus, the number of hops in any path is given by $|\rho| - 1$. Although this reasoning will not be explicitly mentioned in the subsequent analysis, it is considered in the formulation of the algorithm. Before this, the set of requests R is sorted on a decreasing key rate (k_r), prioritizing the analysis of high-demand requests. Subsequently, for each request r, candidate paths are identified using the hops-based shortest path ($\rho_{r,sp}$), allowing all paths for r (ρ_r) as long as $|\rho_{r,sp}| = |\rho_r|$. In cases of equal demands, we employ additional sorting criteria, prioritizing routes based on both the hops and length, thereby selecting paths with increased key generation capacity for significant key demands (see Line 2). Following this, qTDM-HA enters a loop, selecting each $r \in R$ and finding a suitable path ρ for it. To achieve this, the algorithm updates the value of $h_{(i,j)}$ for each path involving the link (i,j) or (j,i). The subsequent computation involves determining Ω for each ρ such that, among all the Ω_ρ values $\forall \rho \in \Psi_r$, the algorithm decides for the ρ resulting in the lowest network load. This iterative process concludes with an updated $h_{(i,j)}$, serving as input for the subsequent unanalyzed request r.

The rules for assigning Tx and Rx capabilities are detailed in lines 12 to 25. Initially, qTDM-HA assigns the Rx capability to the node with the highest degree according to β_n. Subsequently, a Tx capability is assigned to all its neighbor nodes. The algorithm then traverses the network topology, checking if each node has been analyzed or not, and assigns capabilities accordingly. The final step in lines 20 to 25 is essential in cases where a link with $h_{(i,j)} \neq 0$ lacks a pair of Tx and Rx capabilities at its ends, preventing the non-establishment of a q-ch for that link.

To differentiate between the three types of QKD transceivers (refer to Fig. 3), the initial step involves computing the number of dedicated q-chs (Line 26). Subsequently, lines 27 to 33 determine whether a q-ch can be a candidate to set a shared connection on a link through time-sharing QKD transceivers. For this purpose, it is crucial to introduce the new $SKR''_{(i,j)}$ (corresponding to the worst-case for which q-chs are established using transceivers of type 2 on Fig. 3) and the t_s in lines 28 and 29. One heuristic approach is applied on Line 34 to sort the links by $\Delta_{(i,j)}$ from smallest to largest, grouping them into sets where each contains as many q-chs as will fit on a QKD transceiver. The subsequent step involves creating a pool of shared QKD transceivers in each node, achieved by filling T''_n and R''_n with clusters of at least two q-chs on links (i,j) (from δ_{T_n} and δ_{R_n}) where introducing an optical switch at node n is considered useful for time-sharing implementation (lines 35 and 36). In each cluster, the sum of $\Delta_{(i,j)}$ must be less than or equal to 1. Line 37 ensures that if no q-chs are established over a shared transceiver on a link (i,j), then all QKD transceiver pairs on that link will be of type 0. Lines 38 and 39 specifically handle devices of type 1, with corresponding links saved in T'_n, R'_n. Before the final calculations, T_n and R_n are filled with the respective multiple links based on the value of $W_{(i,j)}$. Finally, qTDM-HA computes (lines 42 to 45) C^{total}_{qTDM}, and finally it returns all variables involved in the proposed deployment.

Algorithm 1 qTDM-HA

Require: $G(N,E)$, R, $l_{(i,j)}$, $SKR_{(i,j)}$, $SKR'_{(i,j)}$, $SKR''_{(i,j)}$, Ψ_r, T, t_s, L, C^u_T, C^u_R, C^u_S, C^u_{Ch}
Ensure: C^{total}_{qTDM}, T^{total}_n, R^{total}_n, S^{total}_n, $Q^{total}_{ch(i,j)}$

1: Initialize T_n, T'_n, T''_n, R_n, R'_n, R''_n in [ ]
2: Sort R by: 1st max(k_r), 2nd ρ_{sp} with fewest hops
3: **for** $r \in R$ **do**
4: **for** $\rho \in \Psi_r$ **do**
5: $h_{(i,j)} = h_{(i,j)} + k_r \ \forall (i,j) \in \rho$
6: $\Omega_\rho = \{h_{(i,j)} \cdot L / SKR_{(i,j)} | \ \forall (i,j) \in E\}$
7: $h_{(i,j)} = h_{(i,j)} - k_r \ \forall (i,j) \in \rho$
8: **end for**
9: $\rho_r \leftarrow \rho \in \Psi_r | \sum_{(i,j)\in E} \lceil \Omega_{\rho,(i,j)} \rceil$ and $\overline{\Omega_\rho}$ are minimum
10: $h_{(i,j)} = h_{(i,j)} + k_r \ \forall (i,j) \in \rho_r$
11: **end for**
12: Build $\beta_n = \{(i,j) | \ \forall (i,j) \in E, h_{(i,j)} \neq 0, n = i\} \ \forall n \in N$
13: Sort N by the highest $|\beta_n|$
14: **for** $n \in N$ **do**
15: **if** n has no assigned Rx or Tx capability **then**
16: Assign Rx capability to n by adding $\delta_{R_n} = \{(i,j) | \ \forall (i,j) \in \beta_n\}$
17: Assign Tx capability to the neighbor nodes of n adding $\delta_{T_i} = (i,j)$, $\forall (i,j) \in \beta_n$
18: **end if**
19: **end for**
20: **for** $(i,j) \in E$ **do**
21: **if** $h_{(i,j)} \neq 0$ and $\nexists$ Tx - Rx capacity pair in (i,j) **then**
22: Set Rx capability to $n, j = n$ by adding $\delta_{R_n} = \{(i,j)\}$
23: Set Tx capability to $n, i = n$ by adding $\delta_{T_n} = \{(i,j)\}$
24: **end if**
25: **end for**
26: Compute $W_{(i,j)} = \left\lfloor \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \right\rfloor \ \forall (i,j) \in E$
27: **for** $(i,j) \in E$ **do**
28: **if** $\left(\frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} - W_{(i,j)} \right) \frac{SKR_{(i,j)}}{SKR''_{(i,j)}} + \frac{t_s}{T} \leqslant 1$ and $h_{(i,j)} \neq 0$ **then**
29: $\Delta_{(i,j)} = \left(\frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} - W_{(i,j)} \right) \frac{SKR_{(i,j)}}{SKR''_{(i,j)}} + \frac{t_s}{T}$
30: **else**
31: $W_{(i,j)} = \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \cdot T \quad \forall (i,j) \in E$
32: **end if**
33: **end for**
34: Sort $(i,j) \in \delta_{T_n}$ and $(i,j) \in \delta_{R_n}, n \in N$ by the lowest value of $\Delta_{(i,j)}$
35: Scan $\delta_{T_n}, \forall n \in N$ starting by the first link, grouping them into sets so that the sum of their $\Delta_{(i,j)}$ is less or equal to 1, then add each set to T''_n, and $\Delta_{(i,j)} = \Delta_{(i,j)} \cdot T$
36: Scan $\delta_{R_n}, \forall n \in N$ starting by the first link, grouping them into sets so that the sum of their $\Delta_{(i,j)}$ is less or equal to 1, then add each set to R''_n, and $\Delta_{(i,j)} = \Delta_{(i,j)} \cdot T$
37: Links $(i,j) \in \delta_{T_n}$ and $\notin R''_n$ or $(i,j) \in \delta_{R_n}$ and $\notin R''_n$ set $\Delta_{(i,j)} = 0$ and $W_{(i,j)} = \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \cdot T$
38: Add to T'_n the link $(i,j), \forall (i,j) \in R''_n$ and $(i,j) \notin T''_n, \forall n \in N$, and $\Delta_{(i,j)} = \Delta_{(i,j)} \cdot T$
39: Add to R'_n the link $(i,j), \forall (i,j) \in T''_n$ and $(i,j) \notin R''_n, \forall n \in N$, and $\Delta_{(i,j)} = \Delta_{(i,j)} \cdot T$
40: Add to T_n the link $(i,j), \forall (i,j) \in \delta_{Tn} \forall n \in N$, X times, $X_{(i,j)} = \left\lfloor \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \right\rfloor$, if $\Delta_{(i,j)} = 0$
41: Add to R_n the link $(i,j), \forall (i,j) \in \delta_{R_n} \forall n \in N$, X times, $X_{(i,j)} = \left\lfloor \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \right\rfloor$, if $\Delta_{(i,j)} = 0$
42: Compute $T^{total}_n = |T_n| + |T'_n| + |T''_n|$ and $R^{total}_n = |R_n| + |R'_n| + |R''_n| \quad \forall n \in N$
43: Compute $S^{total}_n = \sum_{set \in T''_n} (|set| + 1) + \sum_{set \in R''_n} (|set| + 1) \quad \forall n \in N$
44: Compute $Q^{total}_{ch(i,j)} = \lceil W_{(i,j)} \rceil + \lceil \Delta_{(i,j)} \rceil \quad \forall (i,j) \in E$
45: Compute C^{total}_{qTDM} by Eq.(17)
46: **Return** C^{total}_{qTDM}, T^{total}_n, R^{total}_n, S^{total}_n, $Q^{total}_{ch(i,j)} \quad \forall n \in N, (i,j) \in E$

The reformulation of RU compared to qTDM-MILP maintains the essence. It represents the time of use of a QKD transceiver (not including t_s) divided by the time T. The formulas in Eqs. (43) and (44) describe the factor F due to QKD transceiver of type 0. In this formula, $W_{(i,j)}$ represents the total time devoted to a link for key generation attributed to transceivers not involved in a shared connection. The denominator corresponds to the amount of q-chs resulting from non-shared connections, multiplied by T.

$$F_T = \sum_{n\in N}\sum_{(i,j)\in T_n} \frac{W_{(i,j)}}{T\cdot\left(Q^{total}_{ch_{(i,j)}} - \lceil \Delta_{(i,j)}\rceil\right)} \tag{43}$$

$$F_R = \sum_{n\in N}\sum_{(i,j)\in R_n} \frac{W_{(i,j)}}{T\cdot\left(Q^{total}_{ch_{(i,j)}} - \lceil \Delta_{(i,j)}\rceil\right)} \tag{44}$$

While for those QKD transceivers that belong to a shared connection but do not have a co-located optical switch the accumulative factor F is computed by equations (45) and (46).

$$F_{T'} = \sum_{n\in N}\sum_{(i,j)\in T'_n} \frac{\Delta_{(i,j)} - t_s}{T} \tag{45}$$

$$F_{R'} = \sum_{n\in N}\sum_{(i,j)\in R'_n} \frac{\Delta_{(i,j)} - t_s}{T} \tag{46}$$

Finally, in the case of QKD transceivers of type 2, it is necessary to consider the whole contribution of connection passing through it ($set \in T''_n$ and $set \in R''_n$).

$$F_{T''} = \sum_{n\in N}\sum_{set\in T''_n}\sum_{(i,j)\in set} \frac{\Delta_{(i,j)} - t_s}{T} \tag{47}$$

$$F_{R''} = \sum_{n\in N}\sum_{set\in R''_n}\sum_{(i,j)\in set} \frac{\Delta_{(i,j)} - t_s}{T} \tag{48}$$

Then the mean of RU for qTDM-HA is calculated using Eq. (36).

7. Performance analysis

This section presents a performance analysis of our proposed model and algorithm for the cost-effective deployment of qTDM-QKDNs. We start by presenting the benchmark used to compare our approach. After that, the input data and the assumptions made on the design parameters to generate realistic numerical results through simulation will be provided. Then we obtain an estimation of the goodness of the heuristic qTDM-HA compared to the optimum qTDM-MILP on a small network. After that, qTDM-HA is applied to medium and large topologies, and the relative savings and other performance metrics w.r.t. non-time-sharing schemes are analyzed.

7.1. Non-time-sharing QKDN: nTDM

In the context of our discussion, the approach Non-time-sharing QKDN, abbreviated as nTDM, is a benchmark for us. This strategy establishes chains of Tx and Rx pairs along each relay path. Consequently, the feasible configurations involve dedicated pairs or sets of QKD transceivers for each link. The number of pairs is dictated by the key demands that the respective links must accommodate. This approach forms a pool of devices at each node, without the need for an identical number of transceiver pairs for each link. The preliminary definitions and the cost model for this approach are presented below. Note that the cost model does not include the cost of switch ports since time-sharing is not considered, then switches are not used.

$$T^{total}_n = \sum_{x\in X} T_{n,x} \quad \forall n\in N \tag{49}$$

$$R^{total}_n = \sum_{x\in X} R_{n,x} \quad \forall n\in N \tag{50}$$

$$Q^{total}_{ch_{(i,j)}} = \sum_{x\in X}\sum_{x'\in X} c_{(i,x),(j,x')} \quad \forall (i,j)\in E \tag{51}$$

$$C^{total}_T = C^u_T \cdot \sum_{n\in N} T^{total}_n \tag{52}$$

$$C^{total}_R = C^u_R \cdot \sum_{n\in N} R^{total}_n \tag{53}$$

$$C^{total}_{Ch} = C^u_{Ch} \cdot \sum_{(i,j)\in E} Q^{total}_{ch_{(i,j)}} \cdot l_{(i,j)} \tag{54}$$

$$C^{total}_{nTDM} = C^{total}_T + C^{total}_R + C^{total}_{Ch} \tag{55}$$

The nTDM-MILP is subject to constraints similar to the qTDM-MILP. Thus, the equations from Eq. (56) to Eq. (61) are in charge to meet the operation under nTDM. The flow and logic of the constraints mirror qTDM-MILP, with the distinction that the variables specifically pertain to QKD transceivers of type 0. (see Fig. 3).

$$m - \sum_{\rho\in\Psi_r} p^r_{th,\rho} \leqslant 0 \quad \forall r\in R \tag{56}$$

$$\sum_{\substack{(i,j)\in E\\ i=n}}\sum_{x'\in X} c_{(i,x),(j,x')} \leqslant 1 \quad \forall x\in X, n\in N \tag{57}$$

$$\sum_{\substack{(i,j)\in E\\ j=n}}\sum_{x\in X} c_{(i,x),(j,x')} \leqslant 1 \quad \forall x'\in X, n\in N \tag{58}$$

$$2\cdot c_{(i,x),(j,x')} - T_{n,x} - R_{n',x'} \leqslant 0 \qquad \begin{matrix}\forall (i,j)\in E,\\ x'\in X, x\in X,\\ n=i, n'=j\end{matrix} \tag{59}$$

$$\alpha_{(i,x),(j,x')} - T\cdot c_{(i,x),(j,x')} \leqslant 0 \qquad \begin{matrix}\forall (i,j)\in E,\\ x'\in X, x\in X\end{matrix} \tag{60}$$

$$h_{(i,j)} - \frac{SKR_{(i,j)}}{T\cdot L}\cdot\sum_{x\in X}\sum_{x'\in X}\left[\alpha_{(i,x),(j,x')} + \alpha_{(j,x),(i,x')}\right] \leqslant 0 \quad \forall (i,j)\in E \tag{61}$$

In cases where we need to use the qTDM-HA for larger networks, an nTDM-HA becomes essential to compare results on the same terms since heuristic algorithms leave solutions by the wayside in favor of the speed with which they deliver a result. In other words, it is not fair to compare qTDM-HA with nTDM-MILP. Thus arises the Heuristic Algorithm for nTDM-QKDN (nTDM-HA) with the pseudocode depicted at Algorithm 2.

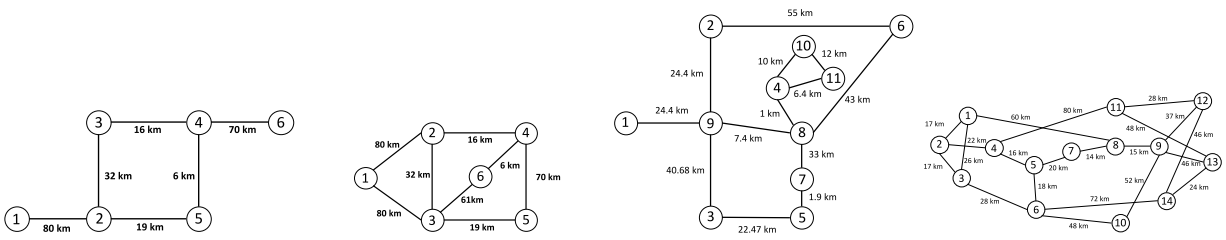
Algorithm 2 works similarly to Algorithm 1 when exploring candidate paths to determine the optimal selection for establishing the end-to-end key relay path. Once the paths are established, and the corresponding demands for each link are known, pairs of QKD transceivers are allocated to each link until the demand is fulfilled (lines 12 and 14). Subsequently, the cost of deployment is computed.

The mean of RU for the nTDM approach is calculated using Eq. (62). Notably, this calculation exclusively considers the contribution of QKD transceivers of type 0. This emphasis is evident in the inclusion only of the factors F_T (as per Eq. (37)) and F_R (as per Eq. (38)) in the numerator. In the case of nTDM-HA, the factors involved are the same but determined by different equations (F_T via Eq. (43) and F_R via Eq. (44)) where $\Delta_{(i,j)} = 0$ because they are unshared QKD transceivers.

$$RU^{mean}_{nTDM}(\%) = \frac{F_T + F_R}{\sum_{n\in N}\left(T^{total}_n + R^{total}_n\right)}\cdot 100 \tag{62}$$

7.2. Methodology, input data and assumptions

The topologies depicted in Fig. 5 will be used to analyze the performance of qTDM-QKDN and the proposed time-sharing computation tools. Thus, we have (a) the Vienna Quantum Key Distribution Network (SECOQC) [41], (b) A six-node graph (for testing purposes), (c) Madrid Quantum Communications Infrastructure (MadQCI) [21], and (d) the well-known National Science Foundation Network (NSFNET) scaled down to feature distances within 0–80 km. The key length is assumed



(a) Vienna QKDN (SECOQC). (b) Six-nodes graph. (c) Madrid QKDN (MadQCI). (d) National Science Foundation (NSFNET).

Fig. 5. Topologies used in the analysis.

Algorithm 2 nTDM-HA

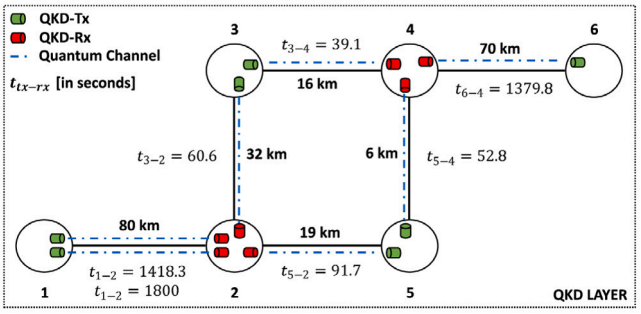
Require: $G(N,E)$, R, $l_{(i,j)}$, $SKR_{(i,j)}$, $SKR'_{(i,j)}$, $SKR''_{(i,j)}$, Ψ_r, T, L, C^u_T, C^u_R, C^u_{Ch}
Ensure: C^{total}_{qTDM}, T^{total}_n, R^{total}_n, $Q^{total}_{ch_{(i,j)}}$

Initialize T_n, R_n in [ ]
Sort R by: 1st $\max(k_r)$, 2nd ρ_{sp} with fewest hops
for $r \in R$ **do**
  for $\rho \in \Psi_r$ **do**
    $h_{(i,j)} = h_{(i,j)} + k_r \ \forall (i,j) \in \rho$
    $\Omega_\rho = \{h_{(i,j)} \cdot L / SKR_{(i,j)}| \ \forall (i,j) \in E\}$
    $h_{(i,j)} = h_{(i,j)} - k_r \ \forall (i,j) \in \rho$
  end for
  $\rho_r \leftarrow \rho \in \Psi_r | \sum_{(i,j)\in E} \lceil \Omega_{\rho,(i,j)} \rceil$ and $\overline{\Omega_\rho}$ are minimum
  $h_{(i,j)} = h_{(i,j)} + k_r \ \forall (i,j) \in \rho_r$
end for
Compute $W_{(i,j)} = \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \cdot T \quad \forall (i,j) \in E$
Add to T_n the link $(i,j), \forall (i,j) \in E$, X times, $X_{(i,j)} = \left\lceil \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \right\rceil$, if $h_{(i,j)} = 0, i < j$
Add to R_n the link $(i,j), \forall (i,j) \in E$, X times, $X_{(i,j)} = \left\lceil \frac{h_{(i,j)} \cdot L}{SKR_{(i,j)}} \right\rceil$, if $h_{(i,j)} = 0, i < j$
Compute $T^{total}_n = |T_n|$ and $R^{total}_n = |R_n| \quad \forall n \in N$
Compute $Q^{total}_{ch_{(i,j)}} = \lceil W_{(i,j)} \rceil \quad \forall (i,j) \in E$
Compute C^{total}_{qTDM} by Eq. (55)
Return C^{total}_{qTDM}, T^{total}_n, R^{total}_n, $Q^{total}_{ch_{(i,j)}} \quad \forall n \in N, (i,j) \in E$

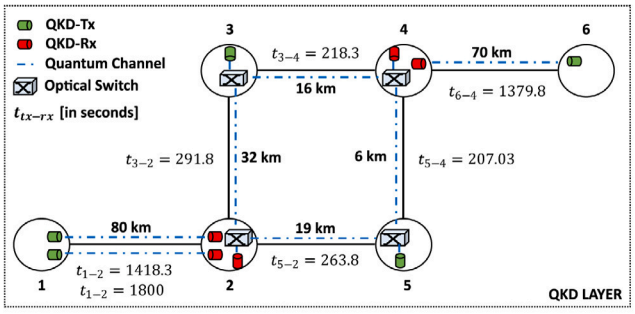
constant and set to $L = 256$ bits (e.g. for AES 256). Each request r includes all key demands between a pair of nodes (src, dst) in any direction; this means that a key rate k_r includes both the key demands originated at src and those originated at dst. Unless otherwise specified a single path must carry the whole demand ($m = 1$). The number of candidate paths to route a request r can vary depending on the difference in hops ($|\rho_r| - |\rho_{r,sp}|$) between any candidate path ($|\rho_r|$) and the hop-based shortest path ($|\rho_{r,sp}|$) between (src, dst) for r. Lastly, we consider that the q-chs through a link are truly isolated from each other, then only the impairments introduced by the optical switch and the attenuation of the q-ch fiber influence the key generation rate SKR as calculated in Section 4.

7.3. A small example on the SECOQC network

Fig. 6 allows us to compare both approaches (nTDM and qTDM) on a small topology: the SECOQC network. The set of end-to-end key demands R follows $R = \{(src, dst, k)| \ \forall src, dst \in N, src \neq dst, k = 10 \text{ keys/s}\}$. Fig. 6(a) shows the conventional non-time-sharing QKD transceivers deployment required to satisfy the predefined demands. Since QKD transceivers are unshared, each q-ch has a dedicated pair of transceivers, which leads to a high number of QKD transceivers (14 in total). Each link has been labeled with a time t_{tx-rx} that denotes the time devoted to key generation to fulfill the demand traversing the link. The time t_{tx-rx} also unveils that the quantum signal is generated on the side of the transmitter (tx) to the receiver (rx). Since there is no switching of quantum end-points at all, then there is no overhead t_s for switching and re-calibration. Thus, t_{tx-rx} does not include such overhead. The deployment depicted in Fig. 6 was achieved through



(a) Deployment using nTDM-MILP.



(b) Deployment using qTDM-MILP.

Fig. 6. Deployments obtained with the benchmark of dedicated QKD transceiver pairs per each link (a) vs. with shared QKD transceivers (b) ($C^u_T = 100$ cu, $C^u_R = 150$ cu, $C^u_S = 10$ cu, $C^u_{Ch} = 0.1$ cu, $T = 1800$ s, $t_s = 120$ s, $|\rho_r| - |\rho_{r,sp}| = 0$, $k_r = 10$ keys/s $\forall r \in R$).

the utilization of the MILP developed for both the nTDM and qTDM approaches.

Analyzing the deployment obtained by nTDM-MILP, the allocation of transceivers is not uniform. As can be seen, link $(1,2)$ is much longer than the others in terms of distance. This implies a lower secret key generation capacity on this link, making it necessary to provision two q-ch in parallel to satisfy the demand. Therefore, this link, in principle, will be a bad candidate for QKD transceiver sharing if the accumulated demand on it approaches the poor capacity of the key generation of the link.

For this particular deployment, the mean of RU is 38.43%. For this, there is very low utilization of the expensive QKD transceivers. For instance, q-chs on links $(3,2)$ and $(5,2)$ have dedicated transceivers that only use 3.3% (60.6 s out of 1800 s) and 5.1% (91.7 s out of 1800 s) each one respectively, of the total cycle T to satisfy the demands carried over those links.

On the other side, Fig. 6(b) shows the same scenario designed and operated with qTDM-QKDN. Under our approach, the number of deployed devices is 11 in total (making a difference to the 14 transceivers that are used with nTDM), thanks to the time-sharing of under-utilized transceivers like the ones used to serve the links

Table 3
Summary of metrics obtained to apply MILP and HA to randomly generated scenarios.

Label	Approach	$\bar{\epsilon}$ (%)	Avg. runtime (s)	
			MILP	HA
SECOQC	nTDM	3.24	0.20	0.002
Six-nodes graph	nTDM	1.89	0.25	0.003
SECOQC	qTDM	6.92	74.90	0.002
Six-nodes graph	qTDM	9.64	523	0.002

Table 4
Cost values used for savings analysis.

Label	C^u_T(cu)	C^u_R(cu)	C^u_S(cu)	C^u_{Ch}(cu)
Scenario # 1	100	150	10	0.1
Scenario # 2	150	300	10	0.1
Scenario # 3	150	300	20	0.1
Scenario # 4	150	300	50	0.1

$(3,2),(3,4),(5,2)$ and $(5,4)$. For this case, the time dedicated to each q-ch t_{tx-rx} labeling the links includes the overhead due to q-ch re-start time t_s, as the price to pay for switched quantum schemes. This time t_s cannot be underestimated with the state-of-the-art QKD technology (in the order of minutes), although it is expected to be reduced with new generations of QKD transceivers. On the other hand, t_{1-2} and t_{6-4} only include the necessary time for key generation (not include t_s), given that their transceivers are unshared. Thus, with qTDM-QKDN is possible to orchestrate a network performance combining dedicated and time-sharing QKD transceivers for the sake of savings on initial CAPEX expenses.

The metric of Relative Savings (RS) is introduced to compare in terms of deployment cost both approaches. It illustrates the potential savings achievable through the adoption of a shared transceiver (qTDM) strategy compared to the total investment required for deploying a non-time-sharing strategy (nTDM) to meet an equivalent set of demands.

$$RS(\%) = \frac{C^{total}_{nTDM} - C^{total}_{qTDM}}{C^{total}_{nTDM}} \cdot 100 \tag{63}$$

Comparing nTDM and qTDM in terms of cost for this small example, the deployment cost of a QKDN with nTDM is 1780.3 cost units, however, using qTDM-MILP it would be 1400.3 cost units, a 22% in terms of relative savings. In addition, it is remarkable that the mean of QKD transceiver utilization (RU) with qTDM-MILP becomes 56.65%, much higher than with nTDM: 38.43%.

The top-level deployment scheme shows that nTDM is a good approach for overloaded links. It means links that handle more traffic than their capacity can comfortably support, for example, links $(1,2)$ and $(4,6)$. The model qTDM-MILP as qTDM-HA can discriminate the cases where the load or key demand makes sharing transceivers convenient, from the cases where a dedicated connection of transceivers of type 0 is required because of its higher load. In this way, qTDM yields the best results in terms of savings and, in the worst case, the same results as nTDM.

To assess the goodness of the developed heuristic algorithms, simulations were conducted using randomly generated scenarios on both SECOQC and Six-node graph topologies. A summary is presented in Table 3. The simulations were performed 100 times over each network. Each execution is a different scenario for which the k_r $\forall r \in R$ and $l_{(i,j)}$ $\forall (i,j) \in E$ follow a uniform distribution. The set of key demands for each scenario was $R = \{(src, dst, k) | \forall src, dst \in N, src \neq dst, k \sim U(10,50)\}$, the length of the links was $l_{(i,j)} : (i,j) \rightarrow \{x | x \sim U(10,80)\}$ $\forall (i,j) \in E$. Finally, the ratios T/t_s, C^u_R/C^u_T and C^u_S took random values from predefined sets. In case of T/t_s from the set $\{2,3,8,12,24\}$, $C^u_R/C^u_T = \{1, 1.5, 2\}$ and $C^u_S = \{10, 20, 50\}$ for each generated scenario. Fixed values were chosen for the rest of parameters: $C^u_{Ch} = 0.1$ cu, $|\rho_r| - |\rho_{r,sp}| = 0$, $X = \{1,2,3,4\}$, $Y = \{1,2,3,4\}$, $Z = \{1,2,3,4\}$ and $S = \{1,2,3,4\}$. Tabla 3 reflects the good performance of the heuristics algorithms proposed, obtaining an average of relative deployment cost difference between MILP and HA $\bar{\epsilon} = 3.24\%$ and $\bar{\epsilon} = 1.89\%$ for nTDM and $\bar{\epsilon} = 6.92\%$ and $\bar{\epsilon} = 9.64\%$ in case of qTDM. The results with qTDM-HA were calculated for a mean of 0.002 s per simulation in both topologies, however, the runtime of TDM-MILP increases considerably as the topology becomes more complex as happened for the Six-nodes graph and qTDM. The simulations were carried out on an 11th Gen Intel(R) Core (TM) i7-11800H @ 2.30 GHz with 32 GB of RAM. From now on, the results calculated for both approaches will be given by using their respective heuristic algorithms. The source code of both the mixed integer linear programming models and the algorithms developed in this work can be consulted free of charge at any time at [42].

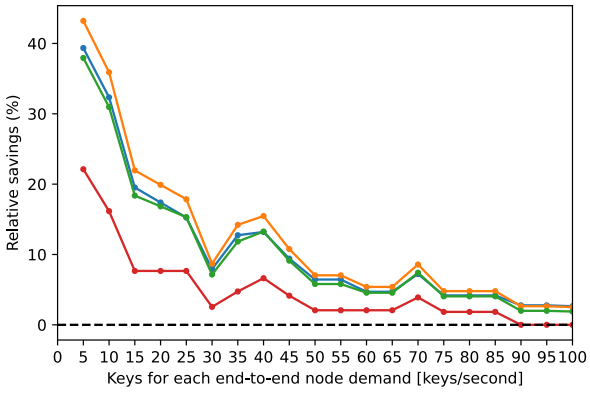
7.4. Cost-savings analysis

Cost-savings analysis is crucial to study the economic feasibility within a QKDN. It involves evaluating potential benefits from specific configurations and identifying cost patterns that minimize capital expenses. For that, four scenarios were defined in Table 4. The four scenarios follow the principle that a Tx is less complex and, consequently, less expensive than a Rx. Given that the prices of commercial products are generally not disclosed, it is well-known that single-photon detectors on the Rx side are generally expensive [43]. To explore the variable impact of these cost ratios, we propose scenarios where the relationship between these costs fluctuates. Additionally, an examination of how the cost of switching devices influences the utilization of shared devices

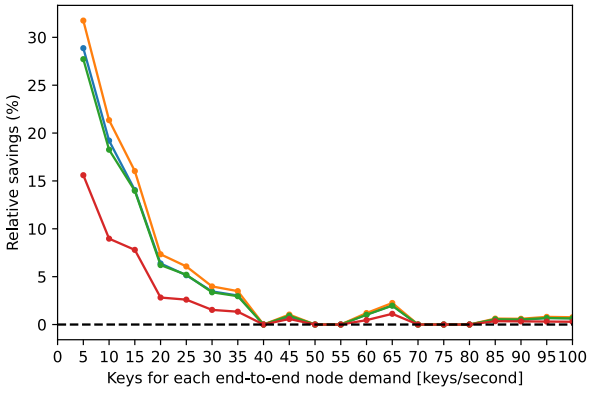
The simulations conducted on MadQCI and NSFNET for those scenarios, as depicted in Fig. 7, illustrate the RS. Notably, this relative savings consistently remains lower or equal to the established threshold set to 0 for both graphs. This validates the said before: qTDM yields the best results in terms of savings and, in the worst case, the same results as nTDM. The RS curves exhibit non-monotonic behavior, marked by subtle peaks, signifying the asymmetric responsiveness of both models to increased demand as can be seen in Fig. 8. These simulations underscore the efficacy of our qTDM approach, demonstrating savings exceeding 40% in Fig. 7(a) compared to nTDM, particularly under the most favorable cost-savings scenario (Scenario 2). In Fig. 7(b), the ratio exceeds 40% in low-load scenarios, especially in the optimal cost-effective scenario (depicted by the orange line). The distinctive characteristic of NSFNET, featuring a portion of links over 60 km (as observed in Fig. 4, where the key rate experiences a sharp decline), contributes to the gap for the RS compared to MadQCI. Unlike MadQCI, which lacks such links, the presence of key generation capacity-stressing q-chs in the network challenges the efficacy of qTDM. Nevertheless, its utility persists, as it strategically utilizes sharing opportunities, yielding savings wherever feasible.

In Scenario 2, characterized by a significant disparity between C^u_T and C^u_R, with C^u_S assuming a lower value in the analysis, remarkable savings are observed. The low cost of switch ports plays a pivotal role, as their relatively inexpensive nature encourages the qTDM approach. Moreover, when the cost difference between one unit of Tx and Rx is substantial, qTDM motivates the allocation of one type above the other. However, in general, we can conclude that the feasibility of qTDM depends on how cheap is the technology behind optical switches. This is the main reason to be Scenario 4 the worst one with $C^u_S = 50$ cu, fading the advantage of sharing QKD transceivers.

Fig. 8 compares, in terms of deployment costs and resource utilization, qTDM-HA and nTDM-HA applied to the topologies MadQCI (Fig. 5(c)) and NSFNET (Fig. 5(d)) for a specific input data. For these simulations, the worst-case scenario where every end-to-end key demand has the same value was chosen, thus k_r grows from 0 keys/s up to 100 keys/s in multiples of 10 per each x-value on the figure. The values

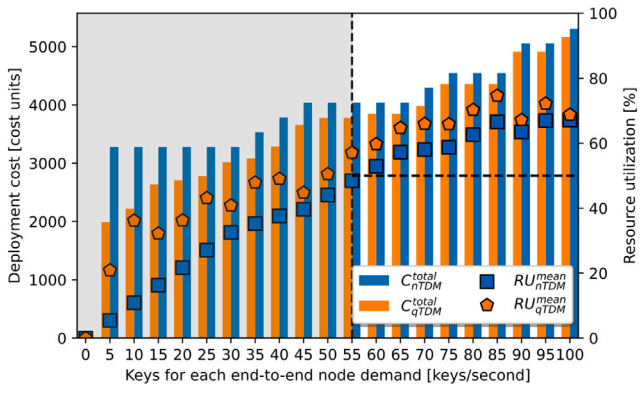


(a) Simulations using MadQCI.

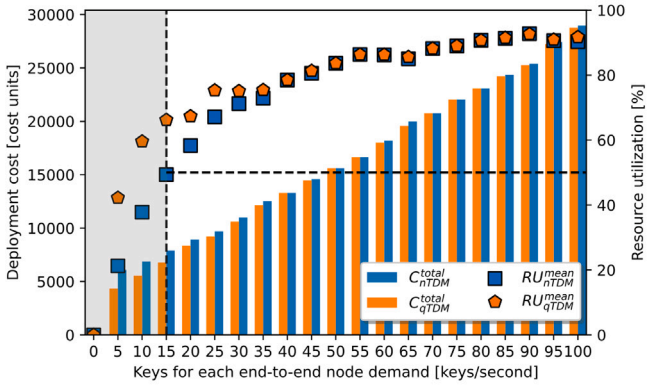


(b) Simulations using NSFNET.

Fig. 7. Relative savings evolution for every end-to-end key k_r demand with the same value varying from 0 to 100 bits/s ($T/t_s = 6$, $|\rho_r| - |\rho_{r,sp}| = 0$). The results were obtained using qTDM-HA and nTDM-HA.



(a) Simulations using MadQCI.



(b) Simulations using NSFNET.

Fig. 8. Deployment cost and resource utilization by both qTDM-HA and nTDM for different keys demand from 0 to 100 bits/s k_r ($C^u_T = 100$ cu, $C^u_R = 150$ cu, $C^u_S = 10$ cu, $C^u_{Ch} = 0.1$ cu, $T/t_s = 6$, $|\rho_r| - |\rho_{r,sp}| = 0$).

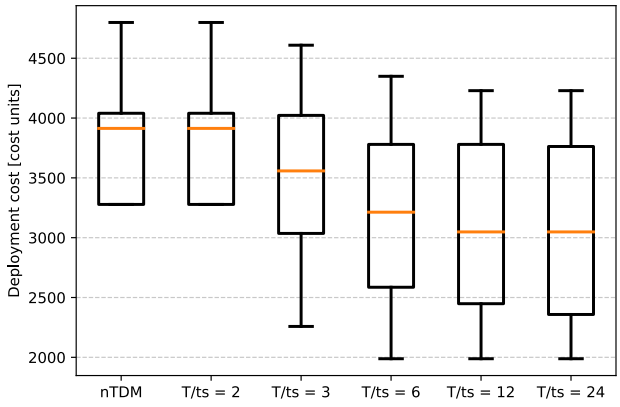
for the cost were $C^u_T = 100$ cu, $C^u_T = 150$ cu, $C^u_S = 10$ and $C^u_{Ch} = 0.1$ cu per kilometer. This election is consistent with the greater complexity of an Rx device compared to Tx, assuming using inexpensive optical switches and the cost of using a dedicated fiber or channel due to the maturity of such technology and their extended deploys. We refer to the range from $0\% \leqslant RU^{mean}_{nTDM} \leqslant 50\%$, as the low-load zone. Essentially, this zone delineates the boundary for optimal RS limits. Beyond it, we can see how the savings effect is blurred.

It can be observed in Fig. 8 that qTDM-HA consistently achieves lower costs than nTDM-HA, even with greater RU. Furthermore, as previously noted, the transition from one key demand on the x-axis to another does not consistently alter the cost on the y-axis for either or both approaches. This observation underscores that the nTDM and qTDM models exhibit a non-asymmetric response to increasing key demands.

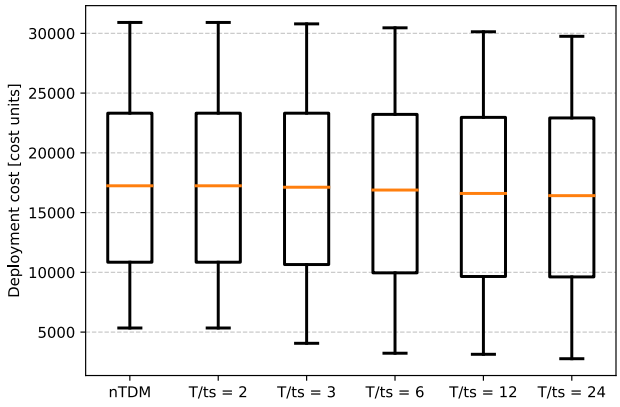
RS moves between 40% (5 keys/s) and 10% (55 keys/s) for low-load zones in Fig. 8(a). As demand grows, the smoother growth of qTDM-HA reveals a better pay-as-you-grow behavior. At high loads, the relative savings become lower as the fraction of shared devices is smaller because the links usually work at the limit of their capacity. The RU for both approaches experiences a fall every time the increases of k_r require the allocation of more QKD transceivers to fulfill the new demand.

The behavior in Fig. 8(b) is similar to the case with MadQCI. The low-load zone (30%–15% of relative savings) is narrower due to links over 60 km (as observed in Fig. 4, where the key rate experiences a sharp decline). Even for key demands beyond the low-load is possible to obtain savings wherever the device saturation permits it. However, it is remarkable that in case sharing QKD transceivers is not possible ($k_r = 70$ keys/s and $k_r = 75$ keys/s in Fig. 8(a)), qTDM-HA gives us the same deployment cost as nTDM-HA, therefore, there is no reason for its non-utilization. Furthermore, in this figure, one can appreciate the asymptotic behavior of RU to 100% and the coincidence in RU for qTDM-HA and nTDM-HA when $k_r = 70$ keys/s and $k_r = 75$ keys/s and sharing is not convenient. These outcomes, as anticipated, further validate our work, demonstrating that even under this scenario, our qTDM model provides similar results to those with nTDM.

As discussed in Section 3, the TDM period T is an important open design parameter. It has to be properly chosen since it drives the network bootstrapping time and permits or not the key generation over shared QKD transceivers because it dictates the overhead due to t_s. Given that t_s is intrinsic to the utilized QKD transceivers, network designers can influence the system by selecting the value of T. The simulations shown in Fig. 9 compute the evolution of the deployment cost due to the progressive increase in the value of k_r (as in Fig. 8), but now the process is repeated for different values of T/t_s. In Figs. 9(a) and 9(b) the nTDM tag on the x-axis corresponds to non-time sharing for which the QKD transceivers are unshared (t_s does not exist); then, the simulations are independent of T/t_s. In the case of MadQCI, it is noteworthy that setting a value of T close to t_s results in an undesirable situation similar to nTDM. This implies that introducing optical switches to leverage the underutilized time in nTDM is not feasible due to the high overhead t_s/T. Conversely, increasing the time T to its maximum does not necessarily lead to cost savings. Approaching $t_s/T = 0$ does not guarantee increased savings. Although the mean



(a) Simulations using MadQCI.



(b) Simulations using NSFNET.

Fig. 9. Box plots for the evolution of deployment cost for different ratios T/t_s (C^u_T = 100 cu, C^u_R = 150 cu, C^u_S = 10 cu, C^u_{Ch} = 0.1 cu, $|\rho_r| - |\rho_{r,sp}| = 0$).

cost significantly decreases for $T/t_s = 12$ compared to $T/t_s = 2$, setting $T/t_s = 24$ despite doubling the rate, still yields similar results to $T/t_s = 12$. Hence, for a qTDM deployment in a network resembling MadQCI's sharing pattern depicted in Fig. 9(a), the optimal selection for T aligns with $T = 12 \cdot t_s$.

However, for NSFNET in Fig. 9(b) increasing the values of T concerning t_s does not provide substantial additional savings. For this topology, many links are close in terms of length to the zone where key rate experiments a sharp decline, as illustrated in Fig. 4. However, as we pointed out before, although the overall performance looks similar in Fig. 9(b) is possible to obtain light savings in the deployment cost for each particular case.

8. Conclusions and future work

This work demonstrates that Time-Division Multiplexing of QKD transceivers (qTDM) at periodic intervals is a viable approach to designing and exploiting the first generations of real QKDNs in a cost-effective way. Sharing QKD transceivers employing inexpensive low-loss switches can yield substantial cost-savings, which we quantified for several topologies and with different secret-key renewal rates. To implement qTDM on QKDNs, we proposed a mixed integer linear programming model (qTDM-MILP) and a heuristic algorithm (qTDM-HA) to route end-to-end secret-key renewal rates through the network and compute the share of time, within a period, that each device needs to devote to peer with another device at adjacent nodes. Additionally, transmission impairments due to fiber and optical switching are also considered assuming the use of the BB84 QKD protocol, but the adaptation to other protocols is straightforward. Both the optimal model and the quasi-optimal algorithm accurately estimate how many QKD transceivers, optical switch ports, and q-chs are needed in a deployment. Both qTDM-MILP and qTDM-HA deal with dedicated and shared transceivers, considering the re-calibration time before key generation to make decisions on when sharing is feasible or not for the sake of deployment cost. The resulting QKD network deployments under qTDM achieve relative cost-savings up to 40% compared to the baseline non-time-sharing QKDN (nTDM) scheme. Furthermore, QKD transceivers are allocated only when they become strictly necessary, and their capabilities are leveraged to support multiple key-exchange routes right from the start, providing a smoother pay-as-you-grow scheme than with nTDM. Simulations show that proper adjustment of the period T of qTDM-QKDN is important because of its impact on cost saving and relative overhead. Pending questions, like time-alignment issues of the time shares computed for the QKD transceivers, is not addressed here due to lack of space, and will be described in a follow-up article. Leveraging genetic algorithms holds promise for addressing this kind of combinatorial problems [44,45], an approach also left for future work.

CRediT authorship contribution statement

Juan Carlos Hernandez-Hernandez: Conceptualization, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft. **David Larrabeiti:** Conceptualization, Methodology, Resources, Supervision, Writing – review & editing. **Maria Calderon:** Conceptualization, Investigation, Methodology, Supervision, Writing – review & editing. **Ignacio Soto:** Methodology, Supervision, Writing – review & editing. **Bruno Cimoli:** Conceptualization, Supervision, Writing – review & editing. **Hui Liu:** Conceptualization, Supervision, Writing – review & editing. **Idelfonso Tafur Monroy:** Resources, Supervision, Writing – review & editing.

Declaration of Generative AI and AI-assisted technologies in the writing process

Statement: During the preparation of this work the authors used chatGPT-3.5 in order to improve readability and language. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work has been partially supported by the Horizon EU Program under the ALLEGRO project (GA 101092766), KAT2 Quantum Delta NL, Netherlands, and the Spanish projects ACHILLES, Spain (PID2019-104207RB-I00) and FUN4DATE-REDES, Spain (PID2022-136684OB-C21).

Data availability

No data was used for the research described in the article.

References

[1] A. Sigov, L. Ratkin, L.A. Ivanov, Quantum information technology, J. Ind. Inf. Integr. 28 (2022) 100365.
[2] Y. Lu, A. Sigov, L. Ratkin, L.A. Ivanov, M. Zuo, Quantum computing and industrial information integration: A review, J. Ind. Inf. Integr. (2023) 100511.
[3] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.X. Ng, L. Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet, IEEE Commun. Surv. Tutor. 24 (2) (2022) 839–894.

[4] T. Chapuran, P. Toliver, N. Peters, J. Jackel, M. Goodman, R. Runser, S. McNown, N. Dallmann, R. Hughes, K. McCabe, et al., Optical networking for quantum key distribution and quantum communications, New J. Phys. 11 (10) (2009) 105001.
[5] P. Toliver, et al., Experimental investigation of quantum key distribution through transparent optical switch elements, IEEE Photonics Technol. Lett. 15 (11) (2003) 1669–1671.
[6] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, J. Zhang, Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD), Opt. Express 25 (22) (2017) 26453–26467.
[7] D. Earl, K. Karunaratne, J. Schaake, R. Strum, P. Swingle, R. Wilson, Architecture of a first-generation commercial quantum network, 2022, arXiv preprint arXiv: 2211.14871.
[8] X. Tang, Optically Switched Quantum Key Distribution Network (Ph.D. thesis), University of Cambridge, 2019.
[9] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, et al., Experimental quantum repeater without quantum memory, Nat. Photonics 13 (9) (2019) 644–648.
[10] S. Kumar, N. Lauk, C. Simon, Towards long-distance quantum networks with superconducting processors and optical links, Quantum Sci. Technol. 4 (4) (2019) 045003.
[11] Q. Ruihong, M. Ying, Research progress of quantum repeaters, J. Phys.: Conf. Ser. (2019) 052032.
[12] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, J. Chen, Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks, IEEE J. Sel. Areas Commun. (2021).
[13] G.S. Vernam, Cipher printing telegraph systems: For secret wire and radio telegraphic communications, J. AIEE 45 (2) (1926) 109–115.
[14] H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 108 (13) (2012) 130503.
[15] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, et al., Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. 117 (19) (2016) 190501.
[16] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, et al., Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. 121 (19) (2018) 190502.
[17] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, et al., Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics 15 (8) (2021) 570–575.
[18] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, et al., High-rate quantum key distribution exceeding 110 Mb s–1, Nat. Photonics 17 (5) (2023) 416–421.
[19] F. Grünenfelder, A. Boaron, G.V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, et al., Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photonics 17 (5) (2023) 422–426.
[20] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, J. Zhang, Cost-efficient quantum key distribution (QKD) over WDM networks, J. Opt. Commun. Netw. 11 (6) (2019) 285–298.
[21] A. Aguado, E. Hugues-Salas, P.A. Haigh, J. Marhuenda, A.B. Price, P. Sibson, J.E. Kennard, C. Erven, J.G. Rarity, M.G. Thompson, et al., Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources, J. Lightwave Technol. 35 (8) (2017) 1357–1362.
[22] J.C. Hernandez-Hernandez, D. Larrabeiti, M. Calderon, I. Soto, B. Cimoli, H. Liu, I.T. Monroy, Quantum key distribution resource sharing schemes for metropolitan area networks, in: Conference on Optical Network Design and Modelling, ONDM, 2022.
[23] J.C. Hernandez-Hernandez, D. Larrabeiti, M. Calderon, I. Soto, B. Cimoli, H. Liu, I.T. Monroy, Toward optimal orchestration of time-shared QKD infrastructure, in: European Conference in Optical Communications, ECOC, poster session, 2023.
[24] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, B. Mukherjee, Resource allocation in optical networks secured by quantum key distribution, IEEE Commun. Mag. 56 (8) (2018) 130–137.
[25] W. Ma, L. Liu, B. Chen, M. Gao, H. Chen, J. Wu, Routing, wavelength and time-slot assignment approaches with security level in QKD-enabled optical networks, in: 2020 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications, IPOC, IEEE, 2020, pp. 1–3.
[26] H. Wang, Y. Zhao, M. Tornatore, X. Yu, J. Zhang, Dynamic secret-key provisioning in quantum-secured passive optical networks (PONs), Opt. Express 29 (2) (2021) 1578–1596.
[27] M. Mehic, S. Rass, E. Dervisevic, M. Voznak, Tackling denial of service attacks on key management in software-defined quantum key distribution networks, IEEE Access 10 (2022) 110512–110520.
[28] Q. Zhang, O. Ayoub, A. Gatto, J. Wu, F. Musumeci, M. Tornatore, Routing, channel, key-rate and time-slot assignment for QKD in optical networks, IEEE Trans. Netw. Serv. Manag. (2023) 1–1.
[29] X. Yu, X. Liu, Y. Liu, A. Nag, X. Zou, Y. Zhao, J. Zhang, Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON), Opt. Express 29 (14) (2021) 21225–21239.
[30] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, A. Tomita, Technologies for quantum key distribution networks integrated with optical communication networks, IEEE J. Sel. Top. Quantum Electron. 15 (6) (2009) 1591–1601.
[31] Y. Cao, Y. Zhao, Y. Wu, X. Yu, J. Zhang, Time-scheduled quantum key distribution (QKD) over WDM networks, J. Lightwave Technol. 36 (16) (2018) 3382–3395.
[32] F. Pederzolli, F. Faticanti, D. Siracusa, Optimal design of practical quantum key distribution backbones for securing coretransport networks, Quantum Rep. 2 (1) (2020) 114–125.
[33] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, J. Chen, Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: a comparative study, IEEE Trans. Netw. Serv. Manag. 17 (2) (2020) 946–957.
[34] X. Tang, A. Wonfor, R. Kumar, R.V. Penty, I.H. White, Quantum-safe metro network with low-latency reconfigurable quantum key distribution, J. Lightwave Technol. 36 (22) (2018) 5230–5236.
[35] Y. Cao, Y. Zhao, R. Lin, X. Yu, J. Zhang, J. Chen, Multi-tenant secret-key assignment over quantum key distribution networks, Opt. Express 27 (3) (2019) 2544–2561.
[36] R. Alleaume, F. Roueff, E. Diamanti, N. Lütkenhaus, Topological optimization of quantum key distribution networks, New J. Phys. 11 (7) (2009) 075002.
[37] K. Assis, R.D. Oliveira, E. Arabul, R. Wang, R. Almeida, R. Nejabati, D. Simeonidou, Resources optimization for a resilient time-shared optical network, in: 2022 International Conference on Optical Network Design and Modeling, ONDM, IEEE, 2022, pp. 1–3.
[38] M. Wenning, M. Samonaki, S.K. Patri, T. Fehenberger, C. Mas-Machuca, Multi-layer optimization for QKD and key management networks, J. Opt. Commun. Netw. 15 (11) (2023) 938–947.
[39] A. Tayduganov, V. Rodimin, E.O. Kiktenko, V. Kurochkin, E. Krivoshein, S. Khanenkov, V. Usova, L. Stefanenko, Y. Kurochkin, A.K. Fedorov, Optimizing the deployment of quantum key distribution switch-based networks, Opt. Express 29 (16) (2021) 24884–24898.
[40] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A 72 (1) (2005) 012326.
[41] A. Poppe, M. Peev, O. Maurhart, Outline of the SECOQC quantum-key-distribution network in vienna, Int. J. Quantum Inf. 6 (02) (2008) 209–218.
[42] J.C. Hernandez-Hernandez, GitHub repository, 2024, URL https://github.com/jhhdez/fgcs_2024.
[43] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. 2 (1) (2016) 16025.
[44] Z. Abo-Hammour, O. Abu Arqub, S. Momani, N. Shawagfeh, et al., Optimization solution of Troesch's and Bratu's problems of ordinary type using novel continuous genetic algorithm, Discrete Dyn. Nat. Soc. 2014 (2014).
[45] O.A. Arqub, Z. Abo-Hammour, Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm, Inf. Sci. 279 (2014) 396–415.

Juan Carlos Hernandez-Hernandez is a Ph.D. student at the Department of Telematic Engineering at Carlos III University of Madrid (UC3M). He earned a B.S. in Telecommunications and Electronic Engineering and a M.S. in Telecommunications Engineering. The master studies was supported thanks to be awarded with a Santander Bank – UA Competitive Scholarships. Currently, the Ph.D. is funded by a grant from the Spanish State Agency of Research. Hernandez-Hernandez's research has primarily focused on optical networks and optimization.

David Larrabeiti is professor in Switching and Network Architectures at Universidad Carlos III de Madrid (UC3M) since 1998. He has participated in a number of EU research projects on next generation optical networks, like the Networks of Excellence e-Photon/One, e-Photon/One+, BONE, the H2020 project PASSION and 5G-PPP projects 5G-CrossHaul and BlueSPACE. His research interests include fast switching technologies, optical neworks and cyber-security in networking. He is currently participating in EU Horizon programme ALLEGRO project, which includes research in the design of QKD systems coexistent with conventional WDM networks. He has been a TPC member of ECOC, TPC co-chair of ONDM2021, ONDM2023 and General Chair of ONDM2024.

Maria Calderon is an associate professor at the Department of Telematics Engineering at Universidad Carlos III de Madrid (UC3M), currently visiting the Universidad Politécnica de Madrid (UPM). She received a Computer Science Engineering degree in 1991 and a Ph.D. degree in Computer Science in 1996, both from UPM. She has published over 90 papers in the fields of advanced communications, reliable multicast protocols, programmable networks and IPv6 mobility. He has participated in research projects funded by the European programs and different Spanish national programs. Her current work focuses on vehicular networks, Internet of Things Networks and QKD Networks.

Ignacio Soto received a Telecommunication Engineering degree in 1993, and a Ph.D. in Telecommunications in 2000, both from the Universidad de Vigo (UVigo), Spain. He was a Research and Teaching Assistant in telematics engineering at the University of Valladolid (UVA) from 1993 to 1999. In 1999, he joined Universidad Carlos III de Madrid (UC3M), where he was an Associate Professor from 2002 to 2021. In 2021, he joined Universidad Politécnica de Madrid (UPM) where he currently works as Professor in telematics engineering. His research activities focus on vehicular networks, future transportation systems, mobility support in packet networks, network security, software defined networks and network virtualization.

Bruno Cimoli received his B.Sc. degree on Information Engineering at the University of Padua (UNIPD) in 2012 and his M.Sc. degree on Telecommunications at the Technical University of Denmark (DTU) in 2014. He obtained his Ph.D. also from DTU in 2019 and he is currently a researcher at the Electrical Engineering department of the Eindhoven University of Technology (TU/e). His main research interests are in the area of wireless and optical communication systems and technologies for the physical layer of 5G and beyond mobile networks. Moreover, he is involved in multiple European research projects related to mm-waves and terahertz communication systems, quantum key distribution and edge computing to the fields of autonomous driving, industry 4.0 and smart healthcare.

Hui Liu received her B.Sc. degree in Nuclear Engineering and Nuclear Physics from the University of Science and Technology of China (USTC) in 2013 and her Ph.D. from USTC in 2020. Currently, Dr. Liu is a postdoctoral researcher in the Electrical Engineering department at Eindhoven University of Technology (TU/e). Her primary research interests lie in the practical aspects of QKD, where she focuses on the development and implementation of secure communication technologies in quantum networks.

Idelfonso Tafur Monroy obtained his M.Sc. from Saint Petersburg University of Telecommunications (Russia) in 1992 and his Ph.D. in Electrical Engineering from Eindhoven University of Technology (TU/e) in 1999. He also took courses at Stockholm University (Sweden), KTH Royal Institute of Technology (Sweden) and Utrecht University. Tafur Monroy worked as Assistant Professor in Electro-Optical Communications at TU/e from 1999 to 2006, after which he became Associate Professor and later Full Professor at DTU Fotonik (Denmark). In the meantime, Tafur Monroy also worked at Beijing University of Post and Telecommunications (China), UC Berkeley (USA) and ITMO University (Russia) as visiting professor. Tafur Monroy is Full Professor in the Electro-Optical Communication group and the Institute for Integrated Photonics. His research focuses on photonic terahertz systems. He is team leader in project 5G PPP blueSPACE, a European research project led by TU/e that will develop wireless technology for 5G wireless systems.