Joint Routing, Channel, and Key-Rate Assignment for Resource-Efficient QKD Networking

Qiaolun Zhang*, Omran Ayoub†, Alberto Gatto*, Jun Wu‡§,
Xi Lin‡§, Francesco Musumeci*, Giacomo Verticale*, Massimo Tornatore*
* Politecnico di Milano, Italy ‡ Shanghai Jiao Tong University, China
† University of Applied Sciences of Southern Switzerland, Lugano, Switzerland
§Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai, China

***Abstract*—Quantum Key Distribution (QKD) is a recent technology for secure distribution of symmetric keys, which is currently being deployed to increase communications security against quantum attacks. However, the key rate achievable over a weak quantum signal is limited by the link performance (e.g., loss and noise) and propagation distance, especially in multi-node QKD networks, making it necessary to design a scheme to efficiently and timely distribute keys to the various nodes. In this work, we formulate, using a Mixed Integer Linear Programming (MILP) model, a novel Routing, Channel, and Key-rate Assignment (RCKA) problem for QKD with Quantum Key Pool (QKP), which exploits the opportunity of using trusted relays and optical bypass. Our formulation accounts for the possibility to build a *quantum key distribution path* that combines both quantum channels and trusted relays to increase the acceptance ratio of key rate requests. Leveraging different versions of the proposed MILP model, we evaluate several strategies exploiting different combinations of trusted relays and optical bypass for the RCKA problem. Results show how different trade-offs between security and resource-efficiency (expressed in terms of acceptance ratio of key rate requests vs. key storing rate in QKP) can be achieved when adopting trusted-relay and/or optical-bypass technologies. Trusted relays can provide a higher acceptance ratio when the number of QKD modules (transmitters or receivers) is sufficiently large, while optical bypass, which does not require the implementation of expensive trusted relays, is preferable when the number of QKD modules is a limiting factor.**

***Index Terms*—Quantum key distribution, quantum key pool, trusted relay, optical bypass, key rate.**

I. Introduction

Fifth-generation (5G) and beyond communication networks will distribute a large amount of private and sensitive data to support new applications (e.g. e-health application) that needs to be encrypted [1]–[3]. However, the rapid development of quantum computing technologies is threatening traditional cryptography [4]–[6], making data exchange over communication networks no longer secure against the attack of a large-scale quantum computer. To address this challenge, Quantum key distribution (QKD) schemes are being investigated and deployed in optical networks, which can provide keys for the application layer, IP layer, or Optical Transport Network (OTN) layer [7], [8]. Since QKD is based on the transmission of single-photon states, this technology holds the potential to share Information-Theoretic Secure (ITS) symmetric keys, thanks to the fundamental principles of quantum physics [4]. Unlike classic bits, in fact, the no-cloning theorem prevents passive eavesdropping of the quantum signal, leading to an unconditionally secure information exchange, which is theoretically immune to any algorithmic cryptoanalysis [4].

A QKD network consists of multiple QKD nodes, QKD links, and a Quantum Key Pool (QKP) [4]. The QKP is a repository, maintained in each QKD node, of the keys generated in the QKD network. Each node has several QKD modules, each of which can work either as a transmitter or as a receiver. Each link has multiple quantum channels where qubits are transmitted at different wavelengths. Each quantum channel requires a QKD module at its end nodes to transmit the quantum signal. Since no optical manipulation is permitted at the intermediate nodes, as shown in Fig. 1(c), the quantum information exchange process is intrinsically limited to point-to-point connections between adjacent nodes, which is a significant limitation when secret keys need to be generated between non-adjacent nodes. To enable the sharing of quantum keys in such cases, as shown in Fig. 1 (d) and (e), two practical approaches exist[1]: (1) Using a *trusted relay*, i.e. an intermediate, uncompromised node, which is *trusted* to relay the keys between two other nodes. The main limitation of this approach is that it fails if the intermediate node is compromised. (2) Adopting an *optical bypass*, which allows establishing a quantum channel between non-adjacent nodes bypassing any intermediate nodes at the optical domain. Note that the optical bypass node does not require any QKD module in the intermediate node. The main limitation of the optical bypass approach is that the optical signal of the quantum channel fades with distance, lowering the key rate, making it potentially not applicable over long paths.

Although QKD network can distribute keys for non-adjacent nodes using trusted relays or optical bypass, the most limiting factor in its field deployment is the low key rate, which is defined as the amount of key bits distributed between two nodes per second. The low key rate derives from fiber attenuation, which strongly impacts the transmitted single-photon states, reducing their number at the receiver end. The fiber attenuation affects the QKD performance in terms of the key length, the time needed to generate a key, and

[1]Note that another scheme, quantum repeater, exists, which creates entanglement to enable key transmission over long distances [9]. However, it is not considered since the field trial of it is still not available.

978-1-6654-3540-6/22/$31.00 © 2022 IEEE

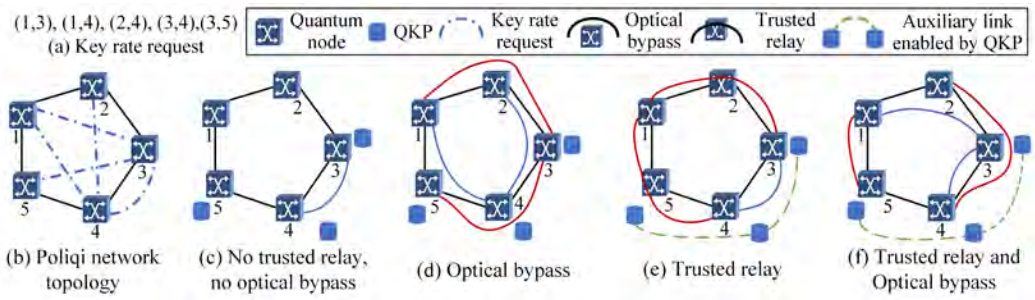

Fig. 1: Example of how requests are served under different settings of trusted relay and optical bypass

ultimately, the achievable key rate. To mitigate such a problem, it is crucial to design a key management scheme (KMS) for efficient key generation, distribution, and usage in the QKD network. QKP is one of the most important mechanisms to effectively manage the keys generated in the QKD network. In fact, if we consider dynamically-evolving key rate requests between pairs of quantum nodes, it may occur that some of the keys generated are not immediately used [4], particularly in low-load periods. In these periods, unused keys can be stored in the QKP for later use, i.e., for future key demands. Past works for QKD networks mainly consider storing the keys in the QKP for encrypting and securing data [10]. However, how to jointly assign routing, key-rate, and channel resources using the keys in the QKP to share keys for other pairs of nodes has not been systematically defined and discussed. Moreover, to the best of our knowledge, there is no existing work considering the joint use of optical bypass and trusted relays for QKD networking.

The main novelties of this work are as follows.

- For the first time, to the best of our knowledge, we define a novel joint routing, channel, and key-rate assignment problem to achieve resource-efficient QKD networking, that considers optical bypass, trusted relays, and QKP.
- We formulate a Mixed Integer Linear Programming (MILP) model to solve the RCKA problem to efficiently distribute keys. Our formulation accounts for the possibility to build QKD paths that utilize both quantum channels and stored keys in the QKP.
- We provide illustrative numerical evaluations to compare different settings of optical bypass and trusted relays to quantify the trade-off between security and resource-efficiency.

The rest of the paper is organized as follows. Sec. II discusses related work. Sec. III formally states the RCKA problem statement, clarifying the new concept of QKD path. Sec. IV proposes the MILP model to solve the RCKA problem. Sec. V discusses numerical results. Finally, Sec. VI concludes the paper and discusses future work.

II. Related Work

Quantum technology is rapidly evolving, offering new enabling technologies for QKD networks, including advances for both point-to-point QKD connectivity as well as for QKD connectivity between non-adjacent nodes. Regarding to point-to-point QKD, in [5], a state-of-the-art QKD network is implemented, which supports physical links of over $4,600$ kilometers, while Ref. [6] demonstrates the coexistence of QKD transmission and classical transmissions in already deployed WDM networks, which would enable much more cost-effective QKD deployments. To extend QKD connectivity to non-adjacent nodes, three schemes have been investigated, namely, trusted relay [11], optical bypass [12], and quantum repeater [9]. Since quantum signal degrades over long distances, the key rate of the link decreases with the distance, and trusted relays have to be adopted to extend the transmission distance [11]. Specifically, in [11], a novel routing scheme using trusted relay is proposed to achieve quality-of-service provisioning. As an alternative to trusted relays, approaches such as device-independent QKD (DI-QKD) can also relay keys using untrusted nodes [13], but the realizations of these approaches are either not mature or not available in practice [7]. Thus, the approaches using untrusted relays are not considered in this work. Optical bypass achieved with optical switches has also been demonstrated in QKD networks, which utilized SDN-controlled nodes to bypass itself [12]. Unlike trusted relay and optical bypass, quantum repeater is not yet available for large-scale deployment of quantum networks although there are small-scale experiments of quantum repeater using techniques such as long-lived quantum memories [9].

To improve the key rates offered in a QKD network, the research community is investigating novel schemes to efficiently distribute keys. Ref. [4] proposes a layered QKD network in which a KMS layer collects demands for keys and determines how to use network resources to generate keys. In [10], a routing, wavelength, and time-slot assignment problem to store keys in the QKP. However, this work does not consider optical bypass and the keys in QKP are only used for the node pair that manages it rather than for other node pairs that require keys. Different from previous work, we systematically compared different strategies exploiting trusted relays and/or optical bypass. Based on the proposed strategies, we define a novel RCKA problem for resource-efficient QKD networking. Another strength is that our model can utilize keys in the QKP to establish a QKD path, is more efficient to distribute keys than only using quantum channels.

III. Routing, Channel, and Key-Rate Assignment Problem

A. Problem Statement

The RCKA problem for QKD networking can be stated as follows: **Given** a QKD network topology and a set of key rate requests during time period T, **decide** the routing, channel, and key rate assignment for each key rate request (i.e. also how each channel using trusted relay and/or optical bypass), **constrained to** the limited number of QKD modules and quantum channel capacity, trusted-relay constraint, key-rate capability of quantum channels, and quantum-channel uniqueness, with the **objective** of maximizing the number of served requests and the key storing rate (defined as the rate of storing keys in QKP).

To clarify the role of optical bypass and trusted relays in the provisioning of secret keys over a QKD network, let us consider the example in Fig. 1, which refers to PoliQi network topology (5-node ring topology), a QKD network currently being deployed in Milan (Italy) [14]. Fig. 1(a) shows a sequence of key rate requests, where notation (a, b) means that a key stream with a given key rate must be set up between nodes a and b for a time period of 10 seconds. The key rate for all requests is 5 kb/s except the one for $(3, 5)$, which is 3 kb/s. Fig. 1(b) shows the 5 requests listed in Fig. 1(a) as dotted lines over the 5-node ring topology. The secret keys stored in the QKP are managed in a pair-wise fashion between any two nodes. For instance, if node 1 distributes keys to node 2, nodes 1 and 2 both maintain a copy of keys in their QKP. Assume that, before the requests arrive, the QKP of nodes 3 and 5 already stored 30 and 80 kb of key bits, respectively, to communicate with node 4, which also maintained corresponding replicas of keys in its QKP. Each node has 2 QKD modules and we consider each link to have 2 quantum channels in this example. The key rate achievable between two adjacent nodes and non-adjacent nodes are 12 kb/s and 8 kb/s, respectively. The quantum channels are marked with red and blue curved lines in this figure to show the transmission of signals at different wavelengths. Fig. 1(c) represents the case of point-to-point quantum communications, i.e., when neither trusted relay nor optical bypass for sharing keys is used. In this case, only request $(3, 4)$ is served as it is the only request between adjacent nodes. Fig. 1(d) represents the case when optical bypass is allowed. In this case, 4 requests can be served, namely, $(1, 3)$ (bypassing node 2), $(1, 4)$ (bypassing node 5), $(2, 4)$ (bypassing node 3), and $(3, 5)$ (bypassing node 4). Request $(3, 4)$ is not served since it cannot be served with either quantum channels (all two QKD modules in nodes 3 and 4 are used) or QKP (the keys stored in QKP are not enough to serve the request). In Fig. 1(e) we show the case where only trusted relays are used (optical bypass is not allowed). By using trusted relays, 4 requests are served, $(1, 3)$, $(1, 4)$, $(3, 4)$, and $(3, 5)$. In this case, request $(3, 5)$ is served with the auxiliary link enabled by QKP, which utilized the keys in QKP to distribute keys between nodes 3 and 5. Request $(2, 4)$ is not served since no node has vacant QKD modules, making it impossible to enable new QKD links using trusted relays. Finally, in Fig. 1(f), we show the case when both optical bypass and trusted relays are exploited. In this case, all five key rate requests are served. Specifically, request $(3, 5)$ is served with the auxiliary link enabled by QKP and request $(1, 4)$ is served with quantum channel between node pair $(1, 5)$ and auxiliary link $(5, 4)$ enabled with QKP. In summary, we have simply demonstrated how different numbers of key rate requests can be served when optical bypass and trusted relay (or a combination of the two) are used.

B. Quantum Key Distribution (QKD) Path

Fig. 2 shows an example of QKD path, which utilizes quantum channels *and* keys in QKP to distribute keys in the QKD network. Each link in the QKD path is called *QKD relay link* and can be either a quantum channel or an auxiliary link enabled by QKPs. Fig. 2 shows an example of 6 nodes in which nodes 2 and 4 serve as trusted relays. In the example, node 1 distributes keys to node 6. The QKD path between nodes 1 and 6 consists of three QKD relay links, $(1, 2)$, $(2, 4)$, and $(4, 6)$. The QKD relay link $(2, 4)$ is an auxiliary link, which uses the keys in the QKP to relay keys directly. QKD relay link $(4, 6)$ uses optical bypass and it does not consume QKD modules in the nodes traversed (in this case, node 5). Note that, although optical bypass may reduce the key rate of the quantum channel, it allows traversing untrusted nodes, which makes key distribution more secure. The maximum key rate of the QKD path is less or equal to the maximum key rate among all the QKD relay links in the QKD path (the maximum key rate between node pair $(1, 6)$ in Fig. 2 is 5 kb/s).

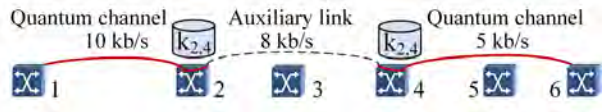

Fig. 2: Example of a QKD path using QKP.

IV. Mixed Integer Linear Programming Model for RCKA problem

This section presents the proposed MILP model for RCKA problem, and then extends the MILP model considering different settings of optical bypass and trusted relay.

A. Decision Variables and Objective Function

Sets, parameters, and variables are listed in Table I and Table II, respectively. We denote $\delta^+(i)$ and $\delta^-(i)$ as the set of outgoings links and the set of incoming links from i, respectively. The initial node and the end node of a path p are denoted with $a(p)$ and $b(p)$, respectively. Besides, the opposite direction of link e is denoted with $\overline{e}$.

Objective: Maximizing the number of served requests, as a first priority and, as a second priority, the key storing rate. Weight $\alpha_{1,e}$ and $\alpha_{2,e}$ are set to give higher priority to serving key rate requests. The weight of $\alpha_{1,e}$ is set to be much larger than $\alpha_{2,e}$ to give priority to serving requests.

TABLE I: Sets and Parameters for the MILP Model

Parameter	Description
N_p	Set of physical nodes
E_p	Set of unidirectional physical links
E_a	Set of unidirectional links in the fully connected graph of nodes in N_p
P	Set of possible node pairs for managing QKP
R	Set of node pairs with key rate requests
N_t	Set of trusted relays in N_p
W	Set of quantum channels
T	Time period of the RCKA problem
C_i	Number of QKD modules in node $i \in N_p$
r_d	Key rate requests for $d \in R$
h_e^w	Maximum key rate of quantum channel $w \in W$ between node pair $e \in E_a$
M	A large constant number which equals to the upper bound of key rate in a path
C_i	Number of QKD modules in node $i \in N_p$
Q_p	Current available keys in quantum key pool between node pair $p \in P$
Q_p^m	Capacity of the QKP between node pair $p \in P$
$\alpha_{1,d}$	Weight for the served request of node pair $d \in R$
$\alpha_{2,p}$	Weight for storing keys in QKP of node pair $p \in P$

TABLE II: Variables for the MILP Model

Variable	Description
$q_{e,w}^p$	Binary, equals to 1 if QKD path between node pair $p \in P$ uses link $e \in E_a$ in quantum channel $w \in W$
f_w^p	Binary, equals to 1 if QKD path between node pair $p \in P$ uses quantum channel $w \in W$
$u_{e,w}^p$	Binary, equals to 1 if the QKD path between node pair $p \in P$ uses the quantum channel w for QKD relay link $e \in E_a$
$\overline{u}_{e,w}^p$	Binary, equals to 1 if the path between node pair $p \in P$ uses the QKP for QKD relay link $e \in E_a$
$x_{e_1,e_2}^{p,w}$	Binary, equals to 1 if the QKD relay link $e_1 \in E_a$ for QKD path between node pair $p \in P$ uses the quantum channel $w \in W$ in physical link $e_2 \in E_p$
$\hat{k}_w^p$	Key rate provided from quantum channel $w \in W$ for the node pair $p \in P$
$\overline{k}_{e,w}^p$	Key rate provided from QKP for QKD relay link $e \in E_a$ in QKD path of node pair $p \in P$ in quantum channel $w \in W$
k_p	Key storing rate in QKP for node pair $p \in P$
y_d	Binary, equals to 1 if key rate request between node pair $d \in R$ is served
g_p	Amount of stored keys for node pair $p \in P$ during T

$$\max \quad \sum_{d \in R} \alpha_{1,d} * r_d * y_d + \sum_{p \in P} \alpha_{2,p} * k_p \tag{1}$$

B. Constraints

We first describe the constraints for the RCKA problem with both optical bypass and trusted relay.

1) Flow conservation constraints for QKD path: Eqn. (2) is the flow constraint for QKD path for all node pairs $p \in P$.

$$\sum_{e \in \delta^+(i)} q_{e,w}^p - \sum_{e \in \delta^-(i)} q_{e,w}^p = \begin{cases} f_w^p & i = a(p) \\ -f_w^p & i = b(p) \\ 0 & otherwise \end{cases} \quad \forall p \in P, i \in N_p, w \in W \tag{2}$$

2) Link formation of QKD path: Eqn. (3) ensures that the QKD path p can use a QKD relay link e only if the quantum channel or QKP can provide keys.

$$q_{e,w}^p = u_{e,w}^p \wedge \overline{u}_{e,w}^p \quad \forall p \in P, e \in E_a, w \in W \tag{3}$$

3) QKD module capacity constraints: Eqn. (4) ensures that the number of quantum channels enabled in node i cannot exceed the number of QKD modules in the node.

$$\sum_{p \in P} \sum_{e \in \delta^+(i) \cup \delta^-(i)} \sum_{w \in W} u_{e,w}^p \leq C_i \quad \forall i \in N_p \tag{4}$$

4) Trusted relay constraint: Eqn. (5) ensures that the QKD relay link can only use trusted relay as an intermediate node.

$$q_{e,p}^{w,t} = 0 \quad \forall p \in P, e \in P, w \in W, t \in T : (a(p) \neq a(e) \wedge a(e) \notin N_{tr}) \vee (b(p) \neq b(e) \wedge b(e) \notin N_{tr}) \tag{5}$$

5) Key supply constraints: Eqn. (6) ensures that the key rate of the QKD path should be less than or equal to the key rate of all the QKD relay links, which is provided by the quantum channel and the QKP. Eqn. (7) ensures no key can be provided from the QKD path if this path is not enabled. Eqn. (8) ensures QKP does not provide keys if it is not used.

$$\hat{k}_w^p \leq h_e^w * u_{e,w}^p + \overline{k}_{e,w}^p + M * (1 - q_{e,w}^p) \quad \forall p \in P, e \in E_a, w \in W \tag{6}$$

$$\hat{k}_w^p \leq M * f_w^p \quad \forall p \in P, w \in W \tag{7}$$

$$\overline{k}_{e,w}^p \leq M * \overline{u}_{e,w}^p \quad \forall p \in P, e \in E_a, w \in W \tag{8}$$

6) Flow conservation constraint for QKD relay link: If a QKD relay link uses a quantum channel, it may traverse several physical links, which forms a path. Eqn. (9) finds the path between the end points of a QKD relay link e_1 that uses quantum channel. Eqn. (10) ensures that a quantum channel is used for QKD relay link e_2 only if there is a flow passing through it.

$$\sum_{e_2 \in \delta^+(i)} x_{e_1,e_2}^{p,w} - \sum_{e_2 \in \delta^-(i)} x_{e_1,e_2}^{p,w} = \begin{cases} u_{e_1,w}^p & i = a(e_1) \\ u_{e_1,w}^p & i = b(e_1) \\ 0 & otherwise \end{cases} \quad \forall p \in P, e_1 \in E_a, i \in N_p, w \in W \tag{9}$$

$$x_{e_1,e_2}^{p,w} \leq u_{e_1,w}^p \quad \forall p \in P, e_1 \in E_a, e_2 \in E_p, w \in W \tag{10}$$

7) Quantum channel uniqueness constraints: Eqn. (11) ensures a quantum channel can only be used for at most one pair of nodes to distribute keys.

$$\sum_{p \in P} \sum_{e_1 \in E_a} (x_{e_1,e_2}^{p,w} + x_{e_1,\overline{e}_2}^{p,w}) \leq 1 \quad \forall e_2 \in E_p, w \in W \tag{11}$$

8) Key storing rate constraint: Eqn. (12) ensures that the key storing rate cannot exceed the difference between the key rate of generating keys and the key rate of using keys. Eqn. (13) and Eqn. (14) gets the keys stored in the QKP of node pair (i, j) at the end of time period T.

$$k_{p_2} \leq \sum_{w \in W} \hat{k}_w^{p_2} - \sum_{p_1 \in P} \sum_{w \in W} (\overline{k}_{p_2,w}^{p_1} + \overline{k}_{\overline{p}_2,w}^{p_1}) - y_{p_2} * r_{p_2} \quad \forall p_2 \in P \tag{12}$$

$$g_p \leq Q_p + k_p * T \quad \forall p \in P \tag{13}$$

$$0 \leq g_p \leq Q_p^m \quad \forall p \in P \tag{14}$$

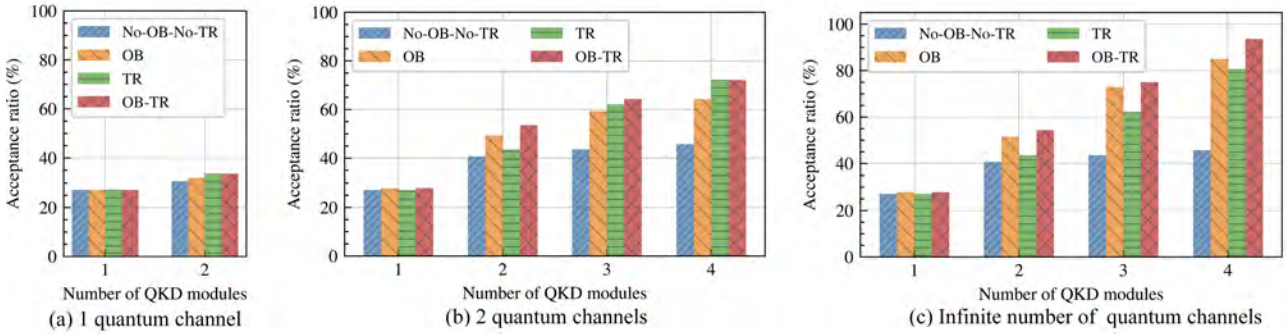

Fig. 3: Acceptance ratio vs. number of QKD modules under different number of quantum channels in each link.

C. Extension of the MILP formulation to Different Settings

The MILP formulation models a scenario where all nodes support both trusted relay and optical bypass (we refer to this scenario as OB-TR). Here, we extend the MILP model above to the following different settings.

1) No optical bypass and no trusted relay (No-OB-No-TR): Eqn. (15) and (16) disable optical bypass and trusted relay, respectively.

$$u^p_{e,w} = 0 \quad \forall p \in P, e \in E_a - E_p, w \in W \tag{15}$$

$$\overline{u}^p_{e,w} = 0 \quad \forall p \in P, e \in E_a, w \in W \tag{16}$$

2) With optical bypass (OB): This case only requires (16) to ensure that trusted relay is not allowed.

3) With trusted relay (TR): This case only requires Eqn. (15) to ensure that optical bypass is not possible.

V. Numerical Results

A. Evaluation Setting

We implement the MILP formulation using AMPL and solve it with CPLEX MIP solver. The simulations are performed on a workstation with Intel(R) Xeon(R) Gold 5217 CPU (8 cores @ 3.00GHz) processor and 128 GB of memory. We consider PoliQi network topology as in Fig. 1. The maximum key rates between each adjacent quantum node pair and non-adjacent quantum node pair are 12 kbit/s and 8 kbit/s, respectively. The number of key rate requests in each time period is 5. The key rate requests are uniformly distributed in [3,6]. We report averaged results over 7 different problem instances.

B. Discussion

We first compare the acceptance ratio of key rate requests with different settings of trusted relay and optical bypass.

Fig. 3 compares the acceptance ratio of the four network settings introduced in Section IV, for an increasing number of QKD modules for the case of one quantum channel (Fig. 3(a)), two quantum channels (Fig. 3(b)) and an infinite number of quantum channels (Fig. 3(c)). Since infinite number of quantum channels would result in infinite constraints, a sufficiently large number of channels (20) is selected, which is enough for the small topology considered. We only show the results of up to 2 QKD modules in Fig. 3(a) because at most 2 QKD modules are used with only 1 quantum channel in each link. In all cases, OB-TR achieves the highest acceptance ratio while No-OB-No-TR has the lowest acceptance ratio. Specifically, OB-TR achieves a higher key rate request acceptance ratio ranging between $0\% - 12\%$ and $0\% - 25\%$ than OB and TR, respectively. The comparison between OB and TR settings is less trivial. When there is only one quantum channel, TR requires 2 QKD modules to have a higher acceptance ratio than OB. As shown in Fig. 3(a), the acceptance ratio of TR is up to about 4% higher than that of OB when there are 2 QKD modules. When the number of quantum channels increases, TR needs more QKD modules in a node to have a higher acceptance ratio than OB. This happens because TR requires more QKD modules to establish quantum channels than OB. For example, when the number of quantum channels increases to 2, as shown in Fig. 3(b), TR can have the same acceptance ratio as OB-TR when there are 4 QKD modules, and OB is about 11% worse than OB-TR. When there is an infinite number of QKD channels, even when there are 4 QKD modules, TR is still about 5% worse than OB. In conclusion, OB can have a better acceptance ratio than TR when there is a limited number of QKD modules. TR can outperforms OB when increasing the number of QKD modules. Moreover, when increasing the number of quantum channels, TR needs more QKD modules in each node to have a higher acceptance ratio than OB.

We now focus on the key storing rate. Fig. 4 shows the key storing rate when increasing the number of QKD modules under a different number of quantum channels in each link. For all cases, No-OB-No-TR has the highest key storing rate since it consumes the least keys for key rate requests and instead generates keys between adjacent nodes, which have also a higher maximum key rate than non-adjacent nodes. On the contrary, OB-TR has the lowest key storing rate in most cases because it consumes the largest number of keys to achieve the highest acceptance ratio of key rate requests among the four network settings. For most cases, when acceptance ratio increases, the key storing rate in QKP decreases because more keys are used to serve the key rate requests. However,

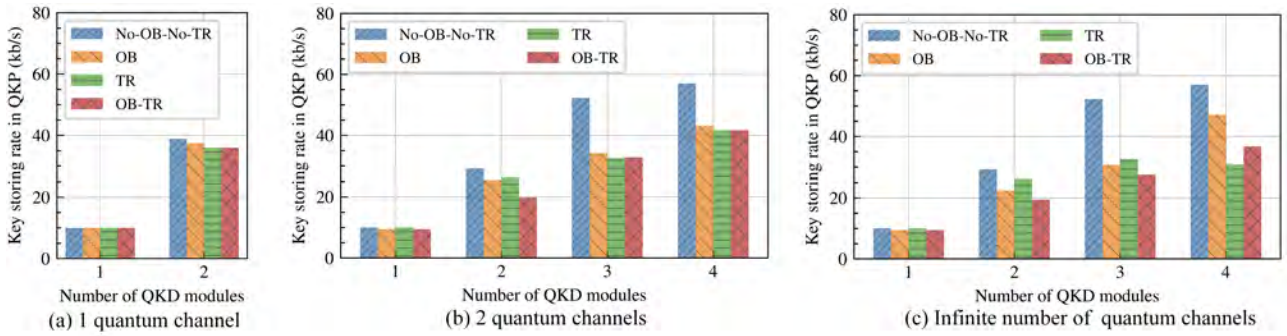

Fig. 4: Key storing rate in QKP vs. number of QKD modules under different number of quantum channels in each link.

it is worth noting that when there are 4 QKD modules and an infinite number of quantum channels, OB and OB-TR have a higher key storing rate than TR, by about 53% and 19%, respectively, and, in the meantime, a higher acceptance ratio than TR by about 5% and 16%, respectively. This is because OB can have more QKD paths enabled in the same link as it requires fewer QKD modules, which reduces the number of hops of a QKD path and the keys consumed while relaying keys for a node pair. In conclusion, although one network scenario may have a lower acceptance ratio, our scheme can utilize the idle quantum channel and QKD modules to store keys in the QKP, which can be used for the key rate requests later. Besides, since OB consumes fewer quantum channels for a QKD path, it may have both a higher acceptance ratio and key storing rate in QKP than TR.

VI. Conclusion and Future Work

In this work, we proposed a novel routing, channel, and key-rate assignment (RCKA) problem to distribute keys resource-efficiently. To solve the RCKA problem, we designed a quantum key distribution (QKD) path scheme and formulated a Mixed Integer Linear Programming (MILP) model for all different settings of optical bypass and trusted relay. We found that, with a limited number of QKD modules, optical bypass (OB) outperforms trusted relay (TR) in terms of acceptance ratio, while TR is preferable when the number of QKD modules is not a limiting factor. Moreover, using optical bypass and trusted relays (OB-TR) combines the benefits of both OB and TR. For the tested scenarios, OB-TR leads to up to about 12% and 25% higher acceptance ratios than OB and TR, respectively. As a future work, we plan to evaluate the behavior of the solution to the RCKA problem in a real-time scenario under dynamic traffic.

Acknowledgment

This work was supported by the Italian Ministry of University and Research (MUR) and the European Union (EU) under the PON/REACT project. It is also partly funded by the National Natural Science Foundation of China under Grants U21B2019 and 61972255 and MUR PON2014_2020 "QUANCOM" Project (MIUR ARS01_00734). Moreover, this work was sponsored by Program of Shanghai Academic Young Research Leader under grant 20XD1422000.

References

[1] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[2] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6g: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[3] Q. Zhang, J. Wu, M. Zanella, W. Yang, A. K. Bashir, and W. Fornaciari, "Sema-iiovt: Emergent semantic-based trustworthy information-centric fog system and testbed for intelligent internet of vehicles," *IEEE Consumer Electronics Magazine*, 2021.

[4] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, "The Engineering of a Scalable Multi-Site Communications System Utilizing Quantum Key Distribution (QKD)," *Quantum Science and Technology*, 2017.

[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[6] A. Gatto, M. Brunero, M. Ferrari, A. Tarable, D. Bodanapu, J. P. Brito, R. B. Mendez, R. J. Vicente, F. Bianchi, and M. Frittelli, "A BB84 QKD Field-Trial in the Turin Metropolitan Area," in *Photonics in Switching and Computing*. Optical Society of America, 2021, pp. Tu1A–2.

[7] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys & Tutorials*, 2022.

[8] C. Wang and A. Rahman, "Quantum-enabled 6g wireless networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58–69, 2022.

[9] Y.-F. Pu, S. Zhang, Y.-K. Wu, N. Jiang, W. Chang, C. Li, and L.-M. Duan, "Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments," *Nature Photonics*, vol. 15, no. 5, pp. 374–378, 2021.

[10] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3382–3395, 2018.

[11] M. Mehic, P. Fazio, S. Rass, O. Maurhart, M. Peev, A. Poppe, J. Rozhon, M. Niemiec, and M. Voznak, "A Novel Approach to Quality-of-Service Provisioning in Trusted Relay Quantum Key Distribution Networks," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 168–181, 2020.

[12] K. Dong, Y. Zhao, X. Yu, A. Nag, and J. Zhang, "Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure," *Optics Express*, vol. 28, no. 5, p. 5936, Mar. 2020.

[13] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y.-Z. Tan, R. Wolf, V. Scarani, and C. C.-W. Lim, "Device-independent quantum key distribution with random key basis," *Nature Communications*, vol. 12, no. 1, p. 2880, 2021.

[14] "Rigene Project - POLIQI - POLItecnico Quantum Infrastructure." [Online]. Available: https://sites.google.com/view/rigene/news/poliqi-politecnico-quantum-infrastructure