Routing and Wavelength Assignment with Minimal Attack Radius for QKD Networks

Mengyao Li*, Qiaolun Zhang*, Zongshuai Yang*, Stefano Bregni*, Alberto Gatto*,
Raouf Boutaba†, Massimo Tornatore*
*Politecnico di Milano, Italy †University of Waterloo, Canada
Corresponding author: qiaolun.zhang@polimi.it

***Abstract*—Quantum Key Distribution (QKD) can distribute keys with guaranteed security but remains susceptible to key exchange interruption due to physical-layer threats, such as high-power jamming attacks. To address this challenge, we first introduce a novel metric, namely Maximum Number of Affected Requests (maxNAR), to quantify the worst-case impact of a single physical-layer attack, and then we investigate a new problem of Routing and Wavelength Assignment with Minimal Attack Radius (RWA-MAR). We formulate the problem using an Integer Linear Programming (ILP) model and propose a scalable heuristic to efficiently minimize maxNAR. Our approach incorporates key caching through Quantum Key Pools (QKPs) to enhance resilience and optimize resource utilization. Moreover, we model the impact of different QKD network architectures, employing Optical Bypass (OB) for optical switching of quantum channels and Trusted Relay (TR) for secure key forwarding. Moreover, a tunable parameter is designed in the heuristic to guide the preference for OB or TR, offering enhanced adaptability and dynamic control in diverse network scenarios. Simulation results confirm that our method significantly outperforms the baseline in terms of security and scalability.**

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

I. Introduction

Quantum Key Distribution (QKD) allows to exchange cryptographic keys with guaranteed information-theoretic security, relying on the laws of quantum mechanics to ensure resilience against quantum-capable adversaries [1], [2]. Initially applied in point-to-point configurations, recent advances have enabled the development of more scalable multi-point QKD networks over optical infrastructures [3]. These scalable QKD networks, composed of interconnected QKD nodes, links, and QKD modules, are now transitioning from experimental systems to practical deployments, which can protect highly sensitive domains such as financial transactions and defense communications [4].

To support these mission-critical applications, prior research has focused on optimizing network performance, particularly through efficient resource provisioning and routing strategies [1], [5]. However, comparatively little attention has been paid to the resilience of QKD networks against targeted attacks. Various threat vectors can disrupt key distribution, including out-of-band attacks that interfere with classical control channels or inject unauthorized signals to compromise quantum channels [6]–[8]. Such attacks are the key reasons why important institutions (e.g. NSA, NIST) remain skeptical about the practicality of QKD [9], [10]. However, our approach offers a concrete step toward mitigating these vulnerabilities. For instance, an adversary may utilize high-power jamming malicious signals to attack a single quantum link, which may disrupt not only the intended transmission but also all other requests sharing the same fiber. The impact of the above-mentioned attacks is closely related to the technologies used for QKD networking as discussed below.

In this work, we consider QKD networks equipped with three critical technologies: (i) Quantum Key Pools (QKPs), which act as key caches at each node, storing pre-distributed keys for future use; (ii) Trusted Relays (TR), which can forward keys, in case maximum signal reach is insufficient, through intermediate, trusted nodes using one-time pad encryption schemes [1]; and (iii) Optical Bypass (OB), enabling direct key delivery between non-adjacent nodes using ROADMs (OB reduces the amount of QKD modules per path but incurs significant attenuation [5]). OB and TR enable efficient key routing over paths connecting non-adjacent nodes, while QKPs add a further degree of freedom to key distribution, facilitating key retrieval between node pairs that can be represented via auxiliary paths. Note that these technologies represent logical capabilities rather than specific physical components. Fig. 1 shows four key requests. Request 1, between nodes (1,3), is served using cached QKD keys and marked with a purple line. Request 2, between nodes (2,4), is served via trusted relay and shown in orange. Requests 3 and 4, also between (1,3) and (2,4), are served via bypass and represented by green and blue lines, respectively. Fig. 1 also illustrates how a single attack on one physical link can disrupt multiple requests, even those that traverse different links. Specifically, a high-power jamming attack on link (1,2) disrupts Request 3, but, since Request 3 uses OB, the attack causes the high-power signal to be propagated also to link (2,3), affecting Request 2. Since Request 1 uses pre-stored keys from the QKP, it remains unaffected.

To mitigate the impact of these jamming attacks, we formulate in this study the *Routing and Wavelength Assignment with Minimal Attack Radius (RWA-MAR)* problem, which seeks to minimize the worst-case impact of a single physical-layer jamming attack. We propose a metric called maxNAR (Maximum Number of Affected Requests), i.e., an extension of the NAR (Number of Affected Requests) tailored to the unique characteristics of QKD systems. maxNAR captures the worst-case service disruption from a single compromised link, factoring in QKD-specific features such as wavelength sharing and specialized transmission mechanisms.

Our proposed approaches address the temporal dynamics of QKD networks by dividing time into discrete slots, during which key availability fluctuates based on the current QKP storage. Unlike conventional optical networks that utilize the Lightpath Attack Radius (LAR) metric [6], we adopt the NAR as a more suitable indicator for QKD scenarios.

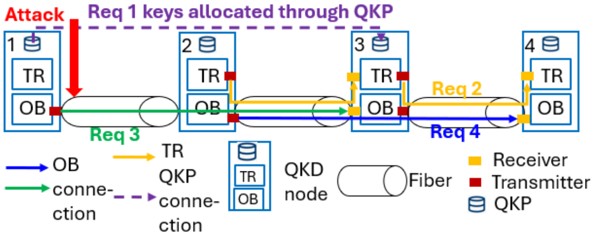


Fig. 1. Example of QKD-specific technologies

A. Related work

QKD networks have been successfully demonstrated in testbeds in various countries, including Switzerland and Italy [1], demonstrating their potential for secure communication. The feasibility of co-existence between QKD and conventional communication signals in optical fiber networks has also been validated [11]. A QKD network architecture is commonly organized into three hierarchical layers: the Quantum Point-to-Point (or Link) layer, the Quantum Network Layer, and the Quantum Transport Layer [12]. Within this framework, keys can be generated and distributed through QKD nodes and modules, utilizing advanced technologies such as TR and OB [3]. TR is a foundational component in many existing QKD testbeds [1], enabling long-distance key distribution, including a demonstration extending up to 4,600 kilometers [2]. OB has been explored both experimentally and analytically [13]. The authors of [14] proposed a quantum-node representation in graphs that facilitates OB using auxiliary graphs to capture quantum-node logical adjacencies enabled by OB. The authors of [5] examined OB and TR integration through a network-wide optimization lens. In our prior work [15], we employed a combination of OB and TR with QKP to support progressive recovery from large-scale network disruptions.

With the growing deployment of QKD networks, an important next research question is how to ensure QKD networks resiliency against physical-layer attacks. Physical-layer attacks can be launched against QKD networks, potentially disrupting key generation [7], [8], [16]. While resilience to such attacks has been studied in classical optical networks [6], solutions specifically tailored to the unique properties of QKD networks remain unexplored.

In contrast to classical optical networks, the presence of technologies introduced for QKD networks, such as QKP caching, OB, and TR, significantly reshapes how disruption propagates. In this paper, we propose a new approach for solving the attack-aware routing problem in QKD networks.

B. Contribution

The main technical contributions of this work can be summarized as follows:

- We formulate a new problem, RWA-MAR, as an ILP, and define a new maXNAR metric to quantify the worst-case impact of a single physical-layer attack.
- We develop a scalable heuristic algorithm and a baseline method, to solve large-scale maxNAR instances efficiently where ILP is computationally infeasible.
- We provide comprehensive numerical evaluations to assess the impact of OB/TR architectures on security and resource utilization.

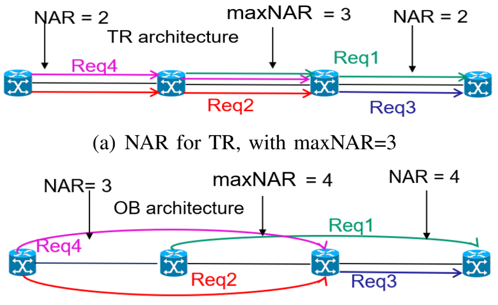
The rest of the paper is organized as follows. Section II formally defines the problem definition, its ILP formulation, and heuristic solution approach. Section III presents and discusses simulation results under various architectural configurations. Finally, Section IV concludes the paper.

II. RWA-MAR PROBLEM

A. System model

We model the QKD network as a weighted directional graph $G_p = (N_p, E_p)$, where N_p and E_p are the sets of nodes and links, respectively. maxNAR as the maximum number of requests any one request is link-sharing with, where link-sharing is defined as a property indicating whether two requests traverse at least one common physical link in the same direction. We assume time is divided in timeslots. We then construct a fully-connected auxiliary graph $G_p = (N_p, E_a)$ where each link denotes the opportunity for key distribution between adjacent and non-adjacent nodes. Key distribution between adjacent nodes can use a physical quantum channel or a logical auxiliary link enabled by QKP. A quantum channel is where qubits are transmitted at different wavelengths. Key distribution between non-adjacent nodes can use a quantum channel with OB/TR or an auxiliary link enabled by QKP key caching (i.e., stored keys in advance for future use). Each node is equipped with a limited number of QKD modules, including both transmitters and receivers. An OB connection requires 2 modules in total, whereas a TR path consumes two modules (a QKD receiver and a QKD transmitter) at each intermediate node to enable key forwarding. Our evaluations are grounded in realistic QKD key rate models [5], and incorporate both OB and TR mechanisms within the system architecture.

Figure 2 illustrates how NAR is computed under OB and TR architectures. Arrows indicate the position of an attack and the resulting number of affected requests. The maximum value among them defines the maxNAR. In Fig. 2(a), all the requests are served using TRs. Due to the characteristics of TR, in this case, the NAR only calculates how many requests traverse the same physical link. TR consistently results in a low NAR (in this case, maxNAR is equal to 3), but requires a higher amount of QKD modules. In Fig. 2(b), requests 1, 2, and 4 use OB, while request 3 is served on a quantum



(a) NAR for TR, with maxNAR=3

(b) NAR for OB, with maxNAR=4

Fig. 2. Example of NAR calculation

channel between two adjacent nodes. Requests using OB are vulnerable to attack propagation because OB allows signals to pass through multiple nodes without regeneration, enabling interference to spread across downstream links. If there is an attack on the middle link, it affects requests 1, 2, and 4, with OB propagating the impact to request 3, keeping the NAR at 4. Note that the quantum channels are directional; thus, an attack in the reverse direction will not affect the served requests. Since keys distributed via QKP are always unaffected by physical-layer attacks (as shown in Fig. 1), we omit further examples involving QKP.

B. Achievable Key Rate and QKP Capacity

The achievable key rate in our model is derived from Ref. [5]. With this model, we can calculate the maximum achievable key rate for different reaches reported in Table I. These key rates decrease by 11% for each crossed node when using optical bypass. The QKP capacity is estimated based on AES256 encryption in Cipher Block Chaining mode. Since each key can securely encrypt up to 2^{48} AES blocks (=36000 Tb), a 100-channel fiber (1 Tb/s per channel) requires a 256-bit key rotation every 360 seconds. Thus, the minimum QKP capacity per one-hour stage is 2560 bits [15].

TABLE I
KEY RATE FOR DIFFERENT REACHES

Reaches	10km	20km	30km	40km	50km
Key rate	23 kb/s	13 kb/s	7 kb/s	3.5 kb/s	1.9 kb/s

C. Problem Statement

The RWA-MAR problem can be stated as follows: **Given** a QKD network topology, number of QKD modules and quantum channels, key requests, achievable key rates for different reaches, timeslots, **decide** the routing, wavelength, and key-rate assignment for key requests, **constrained** by the maximum achievable key rates on given paths, the maximum number of quantum channels and quantum modules, with the **objective** to minimize the sum of the maxNAR across all timeslot. We solve the RWA-MAR problem under three network architectures depending on the availability of optical bypass and trusted relay: 1) OB-TR, 2) OB, 3) TR.

D. Integer Linear Programming (ILP) model

The sets, parameters, and variables for the ILP model are listed in TABLE II.

TABLE II
SETS, PARAMETERS, AND VARIABLES DESCRIPTION FOR ILP MODEL.

Sets	**Description**
G_p	Physical network topology
N_p	Set of physical nodes in network
E_p	Set of physical links in network
E_a	Set of links in the fully-connected graph
P	Set of node pairs of requests in the network
W	Set of QKD channels
T	Set of timeslots
Φ_e	Set of physical routes that use the same end nodes as auxiliary link $e \in E_a$
D	Set of requests
$S^+(i)$	Set of outgoing links from node i
$S^-(i)$	Set of incoming links for node i
Para	**Description**
O_n	Integer, number of QKD modules on node n
$h_{\phi,e}$	Binary, equals to 1 if link $e \in E_p$ in the route ϕ
k_d	Integer, required key rate of request $d \in D$
l_ϕ	Integer, key rate that can be supplied by route ϕ
Var	**Description**
$f_{e,w}^{p,t}$	Binary, equals to 1 if quantum channel w on link $e \in E_a$ is allocated for path between node pair p at timeslot t
$x_{e,w}^{p,t,\phi}$	Binary, equals to 1 if route ϕ is selected for connection between the end nodes of link $e \in E_a$ in QKD path between node pair p at channel w at timeslot t
$xx_{e'}^{p,t}$	Binary, at timeslot t, the routing of node pair p used physical link e' in E_a
$p_{e,w}^{p,t}$	Binary, equals to 1 if link $e \in E_a$ used quantum channel in between node pair $p \in P$ on channel $w \in W$ at timeslot $t \in T$
$q_{e,w}^{p,t}$	Binary, equals to 1 if path p contains auxiliary link $e \in E_a$ based on QKP on channel w at timeslot t
$u_{p,w}^t$	Integer, key rate generated for path p on channel w at timeslot t
$z_{p,w}^t$	Binary, equals t if QKD path between node pair $p \in P$ uses quantum channel $w \in W$ at timeslot t
B_ϕ^t	Binary, at timeslot t, the routing ϕ has been used
$C_\phi^{p,t}$	Binary, at timeslot t, any attack on routing ϕ will affect the routing of node pair p
g_p^t	Integer, stored keys in QKP for path between node pair p at timeslot t
y_d^t	Binary equals to 1 if request d is served at timeslot t
$\gamma_{e,w}^{p,t}$	Integer, key rate provided from QKP for link e in QKD path between node pair p in channel w
$maxNAR_t$	Integer, the maxNAR of timeslot t

Objective function: to minimize the maxNAR.

$$min \sum_{t \in T} maxNAR_t \tag{1}$$

1) Flow, link, and modules constraints: Eqs. (2), (3) show the flow constraint for the QKD path, and it can be either a quantum channel (OB/TR) or an auxiliary link (QKP enabled link). Eq. (4) ensures the number of used modules is smaller than or equal to the number of available nodules in a node. For each link in a fully connected graph E_a, it may consist of several physical links $e \in E_p$ in physical topology. Eq. (5) determines the physical route $\phi \in \Phi$ for auxiliary links $e \in E_a$. Eqs. (6) and (7) ensure that multiple QKD paths cannot use the same channel and the same route.

$$\sum_{e \in S^+(i)} f_{e,w}^{p,t} - \sum_{e \in S^-(i)} f_{e,w}^{p,t} = \begin{cases} z_{p,w}^t \ if \ i = a(p) \\ -z_{p,w}^t \ if \ i = b(p) \\ 0 \ others \end{cases} \tag{2}$$

$$\forall p \in P, i \in N_p, t \in T, w \in W$$

$$f_{e,w}^{p,t} = q_{e,w}^{p,t} \vee p_{e,w}^{p,t} \quad \forall e \in E_a, p \in P, t \in T, w \in W \tag{3}$$

$$\begin{aligned}\sum_{p \in P, e \in S^+(n), w \in W} p_{e,w}^{p,t} + \sum_{p \in P, e \in S^-(n), w \in W} p_{e,w}^{p,t} \\ \leq O_n \quad \forall n \in N_p, t \in T\end{aligned} \tag{4}$$

$$\sum_{\phi \in \Phi_e} x_{e,w}^{p,t,\phi} = q_{e,w}^{p,t} \quad \forall p \in P, e \in E_a, w \in W, t \in T \tag{5}$$

$$\sum_{p \in P} x_{e,w}^{p,t,\phi} \leq 1 \quad \forall e \in E_a, t \in T, w \in W, \phi \in \Phi_e \tag{6}$$

$$\sum_{p \in P, e' \in E_a, \phi \in \Phi_e} x_{e,w}^{p,t,\phi} * h_{\phi,e'} \leq 1 \forall e \in E_p, w \in W, t \in T \tag{7}$$

2) Key rate constraints: Eq. (8) ensures the key rate of QKP path p is less than the sum of the key rate provided by a quantum channel and from QKP in each edge of the path. Eq. (9) ensures that keys are distributed only when the corresponding path p is active and available for use.

$$\begin{aligned}u_{p,w}^{t} \leq \sum_{\phi \in \Phi_e} (x_{e,w}^{p,t,\phi} * l[\phi]) + \gamma_{e,w}^{p,t} + \\ M * (1 - f_{e,w}^{p,t}) \ \forall e \in E_a, p \in P, w \in W, t \in T\end{aligned} \tag{8}$$

$$u_{p,w}^{t} \leq M * z_{p,w}^{t} \quad \forall p \in P, t \in T, w \in W \tag{9}$$

3) QKP storage constraints: Eq. (10) ensures that the stored keys in QKP are not less than 0. Eq. (11) expresses that the amount of keys stored in the QKP at stage t equals the remaining keys from the previous stage $t-1$, plus the newly generated keys supplied by the quantum channel, minus the keys consumed by all requests routed through path p. Eq. (12) ensures that the variable $\gamma_{e,w}^{p,t}$ equals to 1 only when QKP is being used for path $p \in P$.

$$g_p^t \geq 0 \quad \forall p \in E_a, t \in T \tag{10}$$

$$\begin{aligned}g_p^t \leq g_p^{t-1} + \sum_{w \in W} u_{p,w}^{t} - \sum_{p' \in E_a} \sum_{w \in W} (\gamma_{p,w}^{p',t} + \gamma_{\bar{p},w}^{p',t}) \\ -k_p * y_p^t \ \forall p \in P, t \in T\end{aligned} \tag{11}$$

$$\gamma_{e,w}^{p,t} \leq M * q_{e,w}^{p,t} \quad \forall p \in P, e \in E_a, t \in T, w \in W \tag{12}$$

4) NAR constraints: Eq. (13) ensures that the variable $xx_{e'}^{p,t}$ equals to 1 when path p uses physical link e'. Eq. (14) defines if route ϕ is used on timeslot t. Eq.(15) ensures route ϕ has been used for request d at timeslot t. Eq.(16) calculates NAR at each timeslot t.

$$\begin{aligned}xx_{e'}^{p,t} \geq x_{e,w}^{p,t,\phi} \cdot h_{\phi,e'} \forall t \in T, w \in W, p \in P, \\ e \in E_a, e' \in E_p, \phi \in \Phi_e\end{aligned} \tag{13}$$

$$B_\phi^t \geq x_{e,w}^{p,t,\phi} \forall \ t \ \in \ T, w \ \in \ W, p \ \in \ P, e \ \in \ E_a, \phi \ \in \ \Phi_e \tag{14}$$

$$\begin{aligned}C_\phi^{d,t} \geq \left(xx_{e'}^{d,t} \cdot h_{\phi,e'} \right) \ \wedge \ B_\phi^t \\ \forall \ t \in T, d \in D, e' \in E_p, e \in E_a, \phi \in \Phi_e\end{aligned} \tag{15}$$

$$maxNAR_t \geq \sum_{d \ \in \ D} C_\phi^{d,t} \forall \, t \ \in \ T, e \ \in \ E_a, \phi \ \in \ \Phi_e \tag{16}$$

E. Min-maxNAR Algorithm

Algorithm 1 Min-maxNAR Algorithm

Input:N_p, E_p, G_p, T, D, k_d, J_d^p, α, W, O_n
Output:maxNAR, average NAR

```
 1: for $t \in T$. At timeslot t=0, input $J_d^p$ = 0 do
 2:     for each unserved request $J_d^p < k_d$, $d$ = 1 to $|D|$ do
 3:         Get shortest path $P_d$ for all the requests. For OBTR architecture,
            set a tunable parameter $\alpha\%$ to select the initial shortest path.
 4:         if Path $P_d$ for request $d$ routing from $d_s$ to $d_d$ exists. then
 5:             Distribute keys $g_d^p$ from path $P_d$, and stored keys in QKP
 6:             Update quantum channel and modules utilization.
 7:             $J_d^p = J_d^p + g_d^p$
 8:         end if
 9:     end for
10:     while QKPs is not full and network resources are not exhausted do
11:         Find the routing path and store more keys for the future
12:         Update quantum channel and QKD modules utilization
13:     end while
14:     for iteration $\leq \theta$ do
15:         Randomly select a lightpath to reroute
16:         Find the K-shortest paths as the neighborhood of the lightpath
17:         Find the best neighbor which is not in the Tabu list
18:         Update quantum channel and modules utilization
19:         Update the maxNAR, and average NAR
20:     end for
21: end for
22: return maxNAR, and average NAR
```

To solve the RWA-MAR problem, we developed a scalable heuristic algorithm. The details of the Min-maxNAR algorithm are reported in Alg.1. Min-maxNAR algorithm constructs a topology G_t for each stage, which contains nodes and links. J_p^d is an array whose elements contain the achievable key rate from path p for each request d. We develop the Min-maxNAR Algorithm based on the Tabu Search Algorithm (TSA) [17], as TSA has proven powerful in solving min-max problems like ours [18].

At lines 1-2, the topology is initialized, and the system checks the current time-slot while identifying all unserved requests. From lines 3-9, the algorithm first finds the shortest path as the initial routing for serving all the requests from $d = 1$ to $|D|$. For OBTR architecture, initial paths are selected using TR or OB based on a tunable priority parameter α. A lower α favors OB for reduced module cost at the expense of a slightly higher maxNAR, while a higher α prioritizes TR to minimize maxNAR, accepting higher resource usage. OBTR0 refers to the OBTR architecture with $\alpha = 0$, meaning the algorithm initially prioritizes OB paths during path selection and stores them in the Tabu list as the starting solution. Even under OBTR0, however, the system can still have the possibility to select TR during

Tabu-search iterations. Note that α only influences the initial solution; afterward, the heuristic uses Tabu-Search to iteratively optimize routing, often incorporating more TR paths to improve maxNAR. Then the algorithm stores the distributed keys in the QKP while updating the network resource usage, including quantum channels and modules. Moving to lines 10-13, the algorithm examines whether redundant resources are available to serve future requests, allowing for storage of keys in advance using the QKP, following the same logic applied in lines 3 to 5. In lines 14–21, the heuristic optimizes routing by exploring neighboring solutions of the current path, selecting the one with the lowest maxNAR, and updating both the TABU list and the resource utilization (quantum channels and module) accordingly.

III. Illustrative Numerical Results

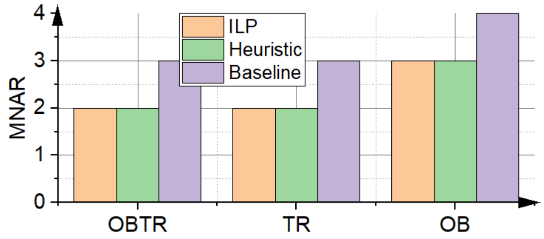


Fig. 3. Results for PoliQi topology.

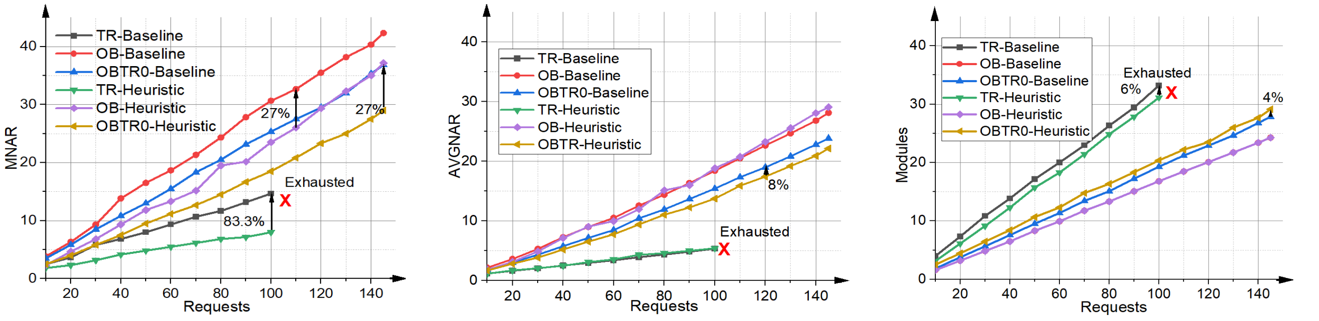
We evaluate the performance of the Min-maxNAR algorithm under three different architectures (*OB-TR*, *OB*, and *TR*). We first benchmark the performance of the in-maxNAR algorithm compared to the ILP in a five-node ring topology (as in the PoliQi QKD testbed currently being deployed in Milan [5]). Each node has ten modules. We consider 7 requests, and each request requires 10kb/s during each timeslot. We then evaluate the Min-maxNAR algorithm also in the NSF topology [19], which has 14 nodes (70 modules) and 21 links. We scale down the link distance as [5, 15]km to be suitable for QKD reaches. Due to the lack of scalability, ILP can not be solved for the NSF topology. For the NSF topology, we consider a demand matrix in which requests are generated for 80% of all node pairs. 80% of the requests have key rate distributed in [5-10] kb/s, and 20% of requests have key rate distributed in [15-25] kb/s. We evaluate our heuristic's performance based on three key metrics: maxNAR, average NAR (avgNAR), and average modules cost for each node, comparing it against a baseline that utilizes depth-first search for shortest path routing between node pairs in the network graph. Note that we also use a tunable parameter α to adjust the initial TABU list in our Min-maxNAR algorithm.

We first discuss results on the PoliQi topology. As shown in Fig. 3, the proposed heuristic achieves the same (optimal) maxNAR of the ILP, with OB-TR and TR architectures reaching a maxNAR of 2 (note that TR consumes more QKD modules than OB-TR, and here $\alpha = 0$). As expected, OB yields the highest maxNAR. Notably, the ILP requires over ten hours to converge, while the heuristic achieves the same results in about five seconds.

Next, we consider the NSF topology and we analyze the performance of the Min-maxNAR algorithm compared to the baseline across the three architectures. In Fig. 4(a), for OB and OBTR0 configurations (meaning $\alpha = 0$), the heuristic reduces maxNAR by approximately 27% compared to the baseline. In contrast, TR exhausts resources after 100 requests due to its higher module consumption. As expected, OB exhibits the highest maxNAR, while TR achieves the lowest. Figure 4(b) presents the avgNAR, which represents the average NAR across all physical links and requests in the network. Compared to the maxNAR results, the gap between the heuristic and baseline approaches is narrower. For both OB and TR architectures, the heuristic yields a higher avgNAR. This is because the heuristic reduces the maxNAR by distributing the requests more evenly across the network, which in turn slightly raises the average number of affected requests. However, in the OBTR architecture, the flexibility of the heuristic allows for a more optimized allocation, resulting in both lower maxNAR and avgNAR compared to the baseline. Specifically, the heuristic achieves up to 8% reduction in avgNAR. Among the architectures, TR consistently achieves the lowest avgNAR, while OB results in the highest, as expected. Finally, Fig. 4(c) illustrates module utilization. TR consumes the most modules, and OB the least (only costs two per lightpath). For OB, both heuristic and baseline use the same number of modules, as expected. In TR, the baseline uses about 6% more modules than the heuristic, while in OBTR, the heuristic consumes 4% more modules to achieve better maxNAR and avgNAR, reflecting a deliberate trade-off for improved routing flexibility.

Moreover, we analyze the impact of the priority parameter α on maxNAR, avgNAR, and module utilization, as shown in Fig. 5. OBTR80 corresponds to $\alpha = 80$, meaning an 80% preference for initially selecting TR paths, while OBTR0 fully prioritizes OB paths. As shown in Fig. ref fig:14-2(a), OBTR80 achieves a 23% maxNAR reduction compared to OBTR0 and a 60% reduction relative to OB. Even OBTR0 provides a 34% improvement over OB. In terms of avgNAR (Fig.5(b)), OBTR80 outperforms OBTR0 by 36.6%, while OBTR0 achieves a 34% gain over OB. TR consistently yields the lowest avgNAR, exhibiting an 84% gap compared to OBTR80. Module utilization results are shown in Fig. 5(c). TR exhausts resources due to its heavy module demand, while OBTR80 consumes 27% fewer modules than TR but 29% more than OBTR0. OBTR0 increases module utilization by 20% compared to OB, while achieving maxNAR and avgNAR gains. These results show that α is a critical tuning parameter: lower α is preferred with limited modules, while higher α improves security and costs more resources.

Finally, we evaluate the impact of QKPs across multiple timeslots using the OBTR0 configuration in the NSF topology with 145 requests. As shown in Fig. 6, both baseline and heuristic start with high maxNAR, but the heuristic reduces it from 37 to 32, while avgNAR shows smaller differences. The usage of key caching leads to a sharp drop in NAR during the

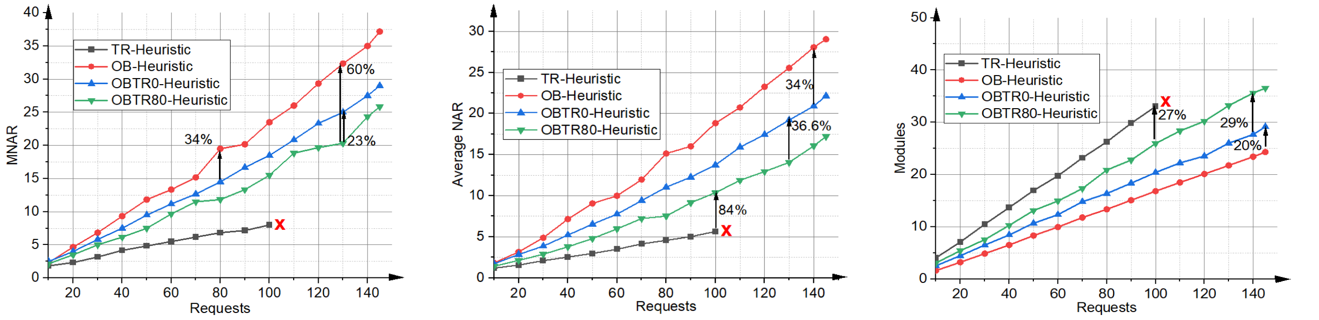


(a) maxNAR

(b) avgNAR

(c) Average number of cost modules for each node

Fig. 4. Result in NSF topology: compared with baseline with $\alpha = 0$



(a) maxNAR

(b) avgNAR

(c) Average number of cost modules for each node

Fig. 5. Result in NSF topology with $\alpha = 0$ & $\alpha = 80$

second timeslot. By the third and fourth timeslots, maxNAR stabilizes around 1 to 2 as QKP reserves meet demand. A slight rise occurs in the final slot as keys are nearly depleted, but the heuristic still outperforms, demonstrating efficient dynamic key allocation.

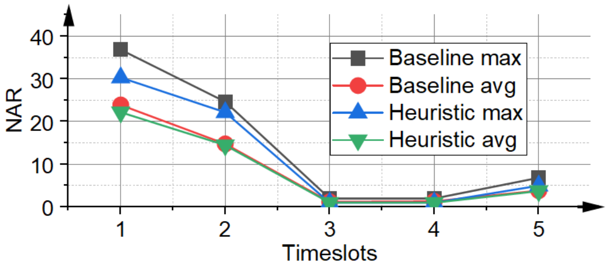


Fig. 6. Result for 5 timeslot with 145 requests

IV. Conclusion

This paper addresses QKD network vulnerability to physical-layer attacks by formulating the RWA-MAR problem and developing both an ILP model and a scalable TABU-based heuristic to solve it. The ILP and heuristic are applicable in three different technological scenarios, namely, OB, TR, and OBTR. Simulation results demonstrate that our heuristic outperforms a baseline solution by about 27% in terms of maxNAR and average NAR. To our knowledge, this is the first work to model and optimize maxNAR for improving QKD network resilience.

Acknowledgment

This work was supported in part by funding from the Innovation for Defence Excellence and Security (IDEaS) program from the Department of National Defence (DND). This work was partially supported by the PRIN project ZeTON funded by Italian Ministry of University and Research.

References

[1] Y. Cao *et al.*, “The evolution of quantum key distribution networks: On the road to the qinternet,” *IEEE CST*, 2022.

[2] Y.-A. Chen *et al.*, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, 2021.

[3] Y. Cao *et al.*, “Time-scheduled quantum key distribution ...,” *J. Light. Technol*, 2018.

[4] M. Sena *et al.*, “Deploying the qline system for a qkd metropolitan network on the berlin openqkd testbed,” *IEEE Photonics J*, 2024.

[5] Q. Zhang *et al.*, “Routing, channel, key-rate, and time-slot assignment for qkd in optical networks,” *IEEE TNSM*, 2024.

[6] M. Furdek *et al.*, “Physical-layer attacks in all-optical wdm networks,” in *2011 MIPRO*, IEEE, 2011.

[7] P. Smith *et al.*, “Out-of-band electromagnetic injection attack on a quantum random number generator,” *Physical Review Applied*, 2021.

[8] A. Alomari *et al.*, “Securing iot systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions,” *IoT*, 2024.

[9] R. Renner and R. Wolf, “The debate over qkd: A rebuttal to the nsa’s objections,” *arXiv preprint arXiv:2307.15116*, 2023.

[10] W. Beullens, “Breaking rainbow takes a weekend on a laptop,” in *CRYPTO*, Springer, 2022.

[11] A. Gatto *et al.*, “A bb84 qkd field-trial in the turin metropolitan area,” in *Photonics in Switching and Computing*, 2021.

[12] M. Dianati *et al.*, “Architecture and protocols of the future european quantum key distribution network,” *SCN*, 2008.

[13] H. H. Brunner *et al.*, “Demonstration of a switched cv-qkd network,” *EPJ Quantum Technology*, 2023.

[14] K. Dong *et al.*, “Auxiliary graph based routing, wavelength, and timeslot assignment...,” *Optics express*, 2020.

[15] M. Li *et al.*, “Drl-based progressive recovery for quantum-key-distribution networks,” *JOCN*, 2024.

[16] V. Mani, “Security challenges to iot and cloud-based systems in the era of quantum attacks,” Springer, 2024.

[17] F. Glover, “Tabu search: A tutorial,” *Interfaces*, vol. 20, no. 4, pp. 74–94, 1990.

[18] H. Youssef *et al.*, “Evolutionary algorithms, simulated annealing and tabu search: a comparative study,” *Eng. Appl. Artif. Intell.*, 2001.

[19] X. Dong *et al.*, “On the energy efficiency of physical topology design for ip over wdm networks,” *J. Light. Technol.*, 2012.