Resource Allocation for Satellite QKD Networks with Atmospheric Forecast

Sun Gyu Park*, Qiaolun Zhang†‖, Raul C. Almeida Jr.‡, Mehdi Bolourian*, Massimo Tornatore†, Raouf Boutaba*
* University of Waterloo, Canada † Politecnico di Milano, Italy ‡ Federal University of Pernambuco
‖ Corresponding author: qiaolun.zhang@polimi.it

***Abstract*—Quantum Key Distribution (QKD) is a foundational technology for future secure communications, and several QKD networks have been already deployed and tested around the world using optical fibers. However, these networks cannot scale in size due to the inefficiency of fiber QKD networks with increasing distances, making satellite networks a major candidate for long-distance QKD networks. In satellite QKD networks, satellites and ground stations can act as *trusted relays*, distributing keys between satellite-ground station pairs to serve requests among ground stations. Satellite QKD networks face fundamental challenges due the time-varying nature of the connection between ground stations and satellites, caused by both the satellite's orbital movement and fluctuating atmospheric attenuation. Thus, it is necessary to design novel schemes to dynamically allocate resources for satellite QKD networks that adapt to evolving network conditions in different time intervals. In this work, we investigate the problem of resource allocation in satellite QKD networks taking into account the changing key generation rates, calculated according to evolving weather conditions and satellite visibility. We first model the achievable key rate of connections between satellite and ground stations under different weather conditions, which is used as an input for optimization. We formulate a Mixed-Integer Linear Programming (MILP) model to allocate resources in satellite QKD networks, which decides both *link assignments* (i.e., deciding which ground to connect to for satellites) and the appropriate routing path for the trusted relay. In addition, the MILP models multiple time-slots and considers keys stored in the quantum key pool (QKP), allowing keys generated during low-load periods to be used later during high-load periods. Moreover, we propose to decide the link configuration with heuristic algorithms and then utilize ILP to decide the appropriate routing path for the trusted relay, which significantly reduces the execution time. The numerical results show that incorporating link configuration within the ILP achieves up to 20% more total served keys compared to heuristic-based baseline approaches, but with an execution time up to 700x longer.**

***Index Terms*—Quantum key distribution, quantum key pool, Mixed-Integer Linear Programming, Satellite networks**

I. Introduction

Quantum Key Distribution (QKD) offers an information-theoretically secure solution against quantum attacks (enabled by recent advances in quantum algorithms that can break classical encryption schemes [1, 2]). QKD protocols are classified mainly into continuous-variable QKD (CV-QKD) and discrete-variable QKD (DV-QKD). Among DV-QKD, the BB84 protocol [3] has been demonstrated to provide theoretical security [3, 4] and is the most imminent in widespread network adoption.

QKD has already been implemented over optical fiber networks in several countries [5–7], but these networks cover relatively short (mostly, metro) distances, spanning at most a few hundred kilometers, as optical fibers experience exponential signal loss over long distances. Hence, it becomes problematic to utilize fiber-based QKD for global-scale networks, where distances between communication nodes span several thousand kilometers. Larger signal loss leads to increase in quantum bit error rate (QBER), and in turn to the failure of establishing secret keys between two nodes.

Satellite QKD networks have emerged as a potential solution to overcome the limitations of fiber-based QKD networks, particularly for long-distance secure communication, as satellites can effectively bridge distances far beyond what optical fibers can achieve [8–10]. In satellite QKD networks, ground satellites and ground stations can work as *trusted nodes* to relay the keys to serve requests among ground stations. Specifically, keys can be first generated between ground stations and satellites, and then the keys can later be combined (e.g., via one-time pad operations) to relay secure messages between distant endpoints. Besides, satellite QKD networks may utilize Quantum Key Pools (QKPs) at ground stations, which cache keys during periods of low traffic and use the keys during future periods of high demand. The effectiveness of a satellite QKD link is heavily influenced by various factors related to atmospheric transmission [11]. The main sources of signal loss include diffraction due to the large distance between the satellite and the ground station (GS), atmospheric absorption and scattering, as well as imperfections in the receiver and transmitter systems. Addressing these challenges through proper network-level resource allocation is crucial to improving the reliability of global satellite QKD networks, as key generation rate is limited both by the capricious nature of the weather and by the constant change in satellite visibility over time. As shown in Fig. 1, the pair of Ground Stations in Melbourne and the given satellite of RAAN $80°$ and anomaly of $0°$ is not always visible to each other. Under evolving weather conditions and satellite-to-ground visibilities, a problem formulation that adapts resource allocation to current satellite link state is needed to attain an effective resource utilization.

The main contributions of this work are as follows:

- We propose a mixed-integer linear programming (MILP) model to allocate network resources considering the

978-3-903176-75-1 ©2025 IFIP

changing conditions of the satellite-ground links (non-constant key generation rates).
- We demonstrate the limitations of assuming constant atmospheric conditions, showing the effect of real weather variations.
- We evaluate the performance of the MILP model in comparison with that of simplistic heuristics of link selection.

II. Related Works

A. Satellite QKD Network Demonstrations and Architectures

Satellite-based QKD is being investigated to overcome the distance limitations of fiber-based QKD networks worldwide [12–14]. A notable early demonstration was carried out by the *Micius* mission in China [12] in 2017, which successfully established downlink BB84 QKD with multiple ground stations. In 2025, satellite QKD successfully generated secret keys between sites in China and South Africa, spanning a terrestrial distance of over 12,900 kilometers [13]. Similar efforts are being carried out globally. Specifically, Canada started the QEYSSat project to establish a technology roadmap to build a satellite quantum network for Canada [14]. Besides, Europe also started investigating how to build a quantum-safe space communication network with satellite QKD networks [15].

B. Resource Allocation for Satellite QKD Networks

With the worldwide deployment of satellite QKD networks, researchers started to extend resource allocation studies from fiber-based quantum communication networks [16] to satellite quantum networks [8–10]. However, since the satellite QKD networks are still being deployed, the resource allocation for satellite QKD networks is still largely underexplored. Most of the works [8, 10] simplify the modeling of satellite QKD networks and do not account for the varying key generation rate caused by weather conditions. Specifically, Karavias et al. [8] formulated an MILP model that abstracts satellite paths as logical nodes and assumes static link capacities to determine the minimum number of satellites needed to serve the key requests. Maule et al. [10] proposed fairness-aware slot allocation strategies in dual-downlink satellite systems, balancing total throughput with equitable distribution across station pairs. In addition to the works that optimize directly satellite QKD networks, some other works investigate entanglement-based resource scheduling for satellite quantum networks, where the distributed entanglements can be used to retrieve keys. Specifically, Panigrahy et al. [17] modeled the distribution of entangled pairs using integer programming across LEO constellations. Williams et al. [18] focused on scalable scheduling heuristics that optimize fidelity-aware delivery in large-scale constellations. All the previously mentioned works do not consider the varying link capacity due to varying weather conditions. The only work that considers varying weather conditions is Ref. [9], which formulated an MILP model to optimize the connection between a single satellite and multiple ground stations in the UK in orbital geometry and historical weather conditions. However, Ref. [9] does not consider optimization of resource allocation with multiple satellites.

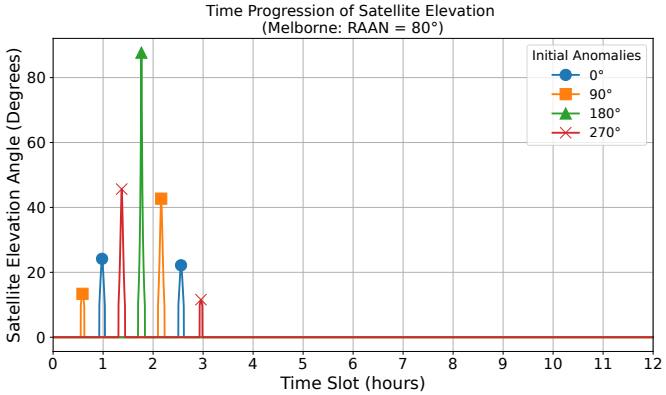

Fig. 1. Elevation angles of 4 satellites in right ascension of the ascending node (RAAN) of 80° from Melbourne GS. In a circular orbit without a defined periapsis, the initial anomaly or the starting angle is considered the satellite's angular position relative to the ascending node at the start of the simulation. This demonstrates that the satellites are not visible to a given GS most of the day. Consistent satellite quantum links throughout the day are difficult.

In contrast to previous works, we optimize resource allocation in satellite QKD networks by explicitly accounting for time-varying link capacities caused by both satellite visibility and atmospheric conditions. Specifically, we propose a joint optimization framework that determines the assignment of satellites to ground stations and the operation of trusted relays to maximize secure key distribution under these dynamic conditions.

III. System Model and Problem Statement

A. System Model

We model the satellite QKD network topology as a time-varying undirected graph composed of both ground stations and satellites. Each node represents either the satellite or the ground station, and each edge represents the maximum key generation capacity of that given time slot. Every possible satellite-ground pair can have quantum key pool (QKP) to cache the keys for later use. All quantum channel links and virtual links spanned from the QKP are fundamentally bidirectional: once a key is generated, it can be used to relay secure communication in either direction (e.g., satellite to ground or ground to satellite), but its source of consumption is the same shared link capacity of both quantum and QKP.

We model the achievable key rate (i.e., quantum link capacity) as a function of satellite visibility, atmospheric conditions at the ground stations, and the elevation angles between satellites and ground stations. The atmospheric transmittance is computed using libRadtran [19], and the key rates are calculated using SatQuMA, which implements the connection model from Sidhu et al. [11] with region-specific elevation angles and weather-dependent transmittance. See the Appendix for details on transmittance estimation.

Once the keys are generated and stored in the QKP, the keys can be consumed later for trusted relay [20] through classical channels, even when the satellite is no longer visible to the ground station. In this case, the QKP acts as a virtual link between the nodes. The directionality of key usage in the flow representation indicates which ground station or satellite is sending to which destination, but this does not imply physical directionality in the quantum channel.

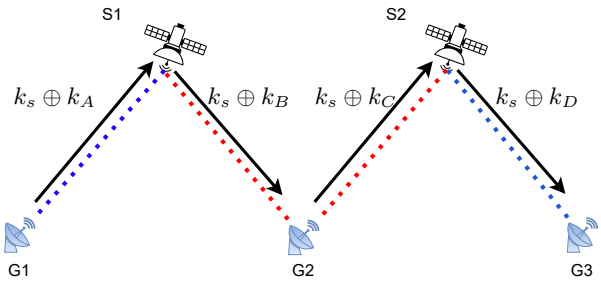

Fig. 2. Key distribution scheme from G1 to G3.

In this model, we assume that the ground stations are far away and cannot generate keys among themselves. The allowed key generation is only between a satellite and a ground station. The key generation between non-adjacent nodes is illustrated in Fig. 2. Specifically, the communication between two ground stations in G1 and G3 may be given by G1-S1-G2-S2-G3, but we do not allow connections such as G1-G2-S1-G3 or G1-S2-S1-G3. In other words, inter-ground or inter-satellite QKD links are not considered.

The general key relay scheme follows Fig. 2. Each of the colored edges represents either the quantum link (red) or the virtual link from QKP (blue) generated by the satellites and the respective ground stations. A single ground station is permitted to create quantum link with as many satellites it requires but a satellite is limited to a single ground station for a quantum link in a single time slot because of the difficulties in the satellite-ground alignment.

Fig. 2 demonstrates an example where the ground station G1 wants to communicate to G3 by passing on a shared key k_s. G1-S1 and S2-G3 already have generated a key length ready for k_s. Multi-hop is permitted, and each relay requires the same length of key bits as k_s. If k_s is a shared secret of n bits, the rest of the keys used for relaying the keys (k_A, k_B, k_C, k_D) should be of n bits to guarantee the same level of security for the One-time Pad. Then, if ground station G1 wants to communicate with ground station G2 through satellite path S1, the amount of keys used between G1 and S1 has to equal to the one between G2 and S1 to carry the shared key. In our problem, this is represented as the flow conservation in (2). The flow of logical key incoming to a satellite should equal the total amount that is outgoing of the satellite to the next destination. In other words, if we are to expand a problem where we have a logical key flow G1-S1-G2-S2-G3, each edge traverse of the flow requires the same amount of key that reaches from G1 to G3.

TABLE I
INPUT PARAMETER DEFINITIONS FOR THE MILP

Parameter	Description
$\mathcal{G} = (G \cup S, E)$	Graph defining connectivity of GS to satellites
G	Set of ground stations
S	Set of satellite orbits
E	Set of quantum-channel links
Λ	Set of all key rate demands
$\mathcal{T}$	Set of all time slots
$a(d)$ and $b(d)$	Source and destination GS of demand d
$\Gamma^{d,t} \in \mathbb{R}^+$	Total key transmission rate demanded between ground stations $a(d)$ and $b(d)$ at time slot t
$\zeta^t_{j,i} \in \mathbb{R}^+$	Key generation rate at time slot t between satellite orbit $j \in S$ and ground station $i \in G$
$n_c \in \mathbb{R}^+$	Total number of link for each satellite per time slot
$\mathcal{N}(i)$	Set of adjacent nodes to node i
θ	Duration of each time slot

B. Problem Statement

The investigated resource allocation problem for satellite QKD networks can be stated as follows: **given** network topology, key rate demands, and pre-calculated key generation rates calculated using SatQuMA through the connection model from [21], we **decide** assignment of generated or stored keys to serve key demands and the storage of keys by unused generated keys. These are **constrained by** flow conservation, link capacities (maximum key generation) and the amount of stored keys. The **objective** is to primarily maximize total served keys, while maximizing the residual keys that would be stored after the final time slot as secondary.

IV. MILP MODEL

This section introduces the proposed MILP which incorporates time-varying quantum link, time progression, and QKP.

A. Objective Function

The following MILP aims to primarily maximize the total served key rate $r^{d,t}$ between GS pairs throughout a set of time slots $\mathcal{T}$, and maximize the final amount of the stored key bits $h^{t_f}_{s,g}$ after the last time slot t_f. The variable β acts as a weighting factor ($\beta < 1$), ensuring that the second term of the objective function is treated as secondary. The input parameters are defined in Table VI, and the variables are defined in Table II. At each time slot, the key flow consists of a combination of newly generated keys in the link and keys consumed from the QKP.

$$\textbf{Max} \sum_{d\in\Lambda}\sum_{t\in\mathcal{T}} r^{d,t}\theta + \beta \sum_{s\in S}\sum_{g\in G} h^{t_f}_{s,g} \tag{1}$$

TABLE II
VARIABLE DEFINITIONS FOR THE MILP

Variable	Description
$x_{u,v}^{d,t} \in \mathbb{R}^+$	Key rate expended directly from link u-v generation rate for demand d at time slot t
$y_{u,v}^{d,t} \in \mathbb{R}^+$	Key rate expended from the virtual link spanned by QKP associated with nodes u-v for demand d at time slot t
$h_{s,g}^t \in \mathbb{R}^+$	Stored keys at time slot t in the QKP for transmissions between $g \in G$ and $s \in S$
$Z_{s,g}^t \in \{0,1\}$	Binary, representing link establishment between satellite s and GS g at time slot t
$r^{d,t} \in \mathbb{R}^+$	Total rate of keys served between source and destination ground stations for demand $d \in \Lambda$ at time slot t

B. Constraints without Internal Link Selection

In this subsection, we present the constraints used when satellite–ground link assignments are fixed in advance. This setup removes the internal link selection from the optimization and instead relies on external link heuristics. The purpose is to evaluate how well the model performs under constrained link choice strategies presented in section IV-D against the one with internal link selection.

1) Flow Conservation for the Serving Path:

$$\sum_{j\in\mathcal{N}(i)} \left(x_{i,j}^{d,t} + y_{i,j}^{d,t}\right) - \sum_{j\in\mathcal{N}(i)} \left(x_{j,i}^{d,t} + y_{j,i}^{d,t}\right) = \begin{cases} r^{d,t} & i = a(d) \\ -r^{d,t} & i = b(d) \\ 0 & \text{otherwise} \end{cases}, \forall\, d \in \Lambda,\, t \in \mathcal{T},\, i \in G \cup S \tag{2}$$

where:

$$r^{d,t} \leq \Gamma^{d,t} \tag{3}$$

The logical flow of key serving is defined in two parts. The first part ($x_{i,j}^{d,t}$) is the key bits used directly from the link capacity, whereas the second ($y_{i,j}^{d,t}$) is the key bits used from QKP. Equation (2) addresses the flow constraints at any node in the network, either a source or destination ground station or an intermediate ground station or satellite path. If the current node is the source of the key demand d, then the output should be the resulting transmission key. However, if the current node is the destination of the key demand d, then the total net key is negative, representing an incoming flow. Otherwise, the total incoming flow must be equal to the total outgoing flow. No key should be generated in or consumed by any satellite or ground station that is neither the source nor the destination of the key flow. Also, with (3), any key served will be consumed immediately. As a result, the amount served does not exceed the demand.

2) Constraint for Link Capacity:

$$\sum_{d\in\Lambda} \left(x_{i,j}^{d,t} + x_{j,i}^{d,t}\right) \leq \zeta_{j,i}^t, \forall\, j \in S, \forall i \in \mathcal{N}(j), \forall t \in \mathcal{T} \tag{4}$$

The total key consumption rate from the current time slot's quantum channel should be limited by link capacity $\zeta_{j,i}^t$. This applies to all possible pairs of GS and satellite in both directions of the key flow.

3) Constraint for QKP:

$$h_{j,i}^t \geq \sum_{d\in\Lambda} \left(y_{i,j}^{d,t} + y_{j,i}^{d,t}\right)\theta \tag{5}$$

$$h_{j,i}^{t+1} \geq h_{j,i}^t - \sum_{d\in\Lambda} \left(y_{j,i}^{d,t} + y_{i,j}^{d,t}\right)\theta \tag{6}$$

$$h_{j,i}^{t+1} \leq h_{j,i}^t - \sum_{d\in\Lambda} \left(y_{j,i}^{d,t} + y_{i,j}^{d,t}\right)\theta + \zeta_{j,i}^t\theta - \sum_{d\in\Lambda} \left(x_{j,i}^{d,t} + x_{i,j}^{d,t}\right)\theta \tag{7}$$

$$\forall j \in S,\ \forall i \in \mathcal{N}(j),\ \forall t \in \mathcal{T}$$

Equation (5) indicates that the key consumption from the QKP should be limited to QKP capacity $h_{j,i}^t$ of the current time slot. This also applies to all possible pairs of GS and satellite in both directions of the key flow. Equation (6) sets the minimum value of key bits in QKP carried over to the next time slot which is the remaining size after assigning the key bits from the current time slot. Then, equation (7) constrains the maximum increase in key bits within the QKP to the residual capacity of the quantum channel after serving current demand d.

4) Cycle Prevention:

$$\left(x_{i,j}^{d,t} + y_{i,j}^{d,t}\right) \leq r^{d,t}, \forall i \in G \cup S, \forall j \in \mathcal{N}(i) \tag{8}$$

$$\sum_{j\in\mathcal{N}(i)} x_{j,i}^{d,t} + y_{j,i}^{d,t} = 0, \quad i = a(d) \tag{9}$$

$$\sum_{j\in\mathcal{N}(i)} x_{i,j}^{d,t} + y_{i,j}^{d,t} = 0, \quad i = b(d) \tag{10}$$

$$\forall\ d \in \Lambda, \forall t \in \mathcal{T}$$

In any case, unintended consumption of keys should be prevented. Equation (8) states that consumed key bits do not exceed the number of served key bits. Equations (9) and (10) declare that no keys should go into the demand source node $(a(d))$ and no keys should come out of the demand destination node $(b(d))$. However, these do not fully prevent meaningless loops among intermediate nodes that are not part of the actual path. Equations (11) to (12) exist to prevent a solution with possible over-consumption and cyclic flow that serves no purpose to the served key rate. The following fragment (where $p < 0$) is added to the objective function to reduce the risk of such an event and discourage overuse of keys:

$$p \sum_{d\in\Lambda} \sum_{i\in G} \sum_{j\in\mathcal{N}(i)} \sum_{t\in\mathcal{T}} I_{x_{i,j}^{d,t}} + I_{x_{j,i}^{d,t}} + I_{y_{i,j}^{d,t}} + I_{y_{j,i}^{d,t}} \tag{11}$$

Where:

$$I_{x_{i,j}^{d,t}} \geq \frac{x_{i,j}^{d,t}}{\Gamma^{d,t}}, \quad I_{y_{i,j}^{d,t}} \geq \frac{y_{i,j}^{d,t}}{\Gamma^{d,t}}, \quad I_{x_{j,i}^{d,t}} \geq \frac{x_{j,i}^{d,t}}{\Gamma^{d,t}}, \quad I_{y_{j,i}^{d,t}} \geq \frac{y_{j,i}^{d,t}}{\Gamma^{d,t}}, \tag{12}$$

$$\forall d \in \Lambda,\ \forall t \in \mathcal{T},\ \forall i \in G,\ \forall j \in \mathcal{N}(i)$$

The reason for the division by parameter $\Gamma^{d,t}$ is that we have (8) which already prevent both $x_{i,j}^{d,t}$ and $y_{i,j}^{d,t}$ to be no greater than $\Gamma^{d,t}$. The value of $\Gamma^{d,t}$ normalizes the division on the right-hand side to be $[0, 1]$. The variables in equation (12): $I_{x_{i,j}^{d,t}}, I_{x_{j,i}^{d,t}}, I_{y_{i,j}^{d,t}}, I_{y_{j,i}^{d,t}}$ are defined as binary variables, which means each can only take values 0 or 1.

C. Constraints with Internal Link Assignment

In this subsection, we present an alternative formulation of the MILP model in which quantum link assignment is determined internally by the optimization process itself, labeled "ILP" in the plots. This is in contrast to the previous model in which all existing links are assumed to be simultaneously connected.

1) Constraint for Link Capacity:

$$\sum_{d\in\Lambda}\left(x_{i,j}^{d,t} + x_{j,i}^{d,t}\right) \leq \zeta_{j,i}^{t} Z_{j,i}^{t}, \forall j \in S, \forall i \in \mathcal{N}(i), t \in \mathcal{T} \quad (13)$$

Constraint set (13) extends (4) by including binary variable $Z_{j,i}^{t}$, which causes the effective link capacity to be zero if the given link is not selected.

2) Constraint for QKP:

$$\begin{aligned} h_{j,i}^{t+1} \leq\ & h_{j,i}^{t} - \sum_{d\in\Lambda}\left(y_{j,i}^{d,t} + y_{i,j}^{d,t}\right)\theta \\ & + \zeta_{j,i}^{t} Z_{j,i}^{t}\theta - \sum_{d\in\Lambda}\left(x_{j,i}^{d,t} + x_{i,j}^{d,t}\right)\theta \qquad (14) \\ & \forall j \in S,\ \forall i \in \mathcal{N}(j), \forall t \in \mathcal{T} \end{aligned}$$

Similarly, constraint set (14) extends equation (7). There is an addition of the binary variable $Z_{j,i}^{t}$ to the link capacity $\zeta_{j,i}^{t}$. Although satellite and ground station may be visible to each other (i.e. $\zeta_{j,i}^{t} > 0$), the restrained number of transmitters may limit key generation in such link. In this case, no new keys are generated (see Eq. 13) nor added to the QKP.

3) Constraint for Maximum Links:

$$\sum_{i\in\mathcal{N}(j)} Z_{j,i}^{t} \leq n_c, \forall\ j \in S, \forall i \in \mathcal{N}(j), \forall t \in \mathcal{T} \quad (15)$$

The cumulative number of connections for the satellite should not exceed the number that it can support in a single time slot. Based on existing studies on the time required for links [12, 22], which can range between approximately 2 to 5 minutes but require few more minutes extra for alignment with the GS, we choose the duration of a single time slot to be 10 minutes. Finally, n_c was kept as the value of 1 during each time slot.

D. Heuristics for Link Assignment

As mentioned earlier, for the model without internal link assignment, we pre-assign links prior to optimization. We evaluated three heuristics for link assignment: *Greedy*, *Path*, and *Random*. These heuristics for link assignment decide the assignment of satellites to ground stations. First, in **Greedy**, each satellite selects the single link with the highest key generation rate in each time slot, while all other link capacities are set to zero. Second, in **Path**, the satellite also selects one link per time slot, but prioritizes avoiding repeated use of the same ground station across adjacent time slots and overlapping links in the current time slot, unless no other options exist. Last, **Random** selects one link per satellite and time slot, with all others set to zero. This method is repeated in eight randomized runs, and average performance is reported. After determining the assignment of satellites to ground stations, we solve the resource allocation problem to serve requests with the MILP in Sec. IV-B. The solutions of heuristics combined with MILP are named as *Greedy-ILP*, *Path-ILP*, and *Random-ILP* for heuristics with *Greedy*, *Path*, and *Random* respectively.

TABLE III
PROBLEM SETTINGS

Setting	Description
Simulation Start	December 14, 2024 (UTC+0)
Duration	12 hours
Size of time slot t	10 minutes
Orbital Path	RAAN of 80° and 90°
Satellites per Path	4
Initial Angular Positions	$0°, 90°, 180°, 270°$
Satellite Altitude	567 km
Inclination Angle	97.7°
Signal Wavelength	785 nm
Min. Visibility Angle	10°
Dark Count Probability	$5 \cdot 10^{-7}$ (Night)
	$1 \cdot 10^{-5}$ (Day)
Connection Limit n_c	1

TABLE IV
GROUND STATION SETS FOR DIFFERENT TOPOLOGIES

Topology Name	**Ground Stations**
Global	Graz, Johannesburg, Sao Paulo, Tokyo, Auckland, Mumbai, Xinglong, Melbourne, Denver
Regional Clusters	London, Frankfurt, Graz, New Delhi, Mumbai, Bangalore, Melbourne, Perth, Brisbane
Europe	London, Madrid, Athens, Paris, Nantes, Bern, Florence, Naples, Berlin

V. ILLUSTRATIVE NUMERICAL RESULTS

A. Simulation Setup

The simulations were performed on a server equipped with AMD EPYC 7302 16-Core Processor (16 Cores @ 3.04GHz) and 504 GB of memory. Our proposed solutions were implemented on Python 3.8 and solved using CPLEX V22.1 [23] to evaluate the mentioned heuristics with their respective link assignment methods.

We consider three different satellite network topologies, each with 9 ground stations and 2 orbital paths with 4

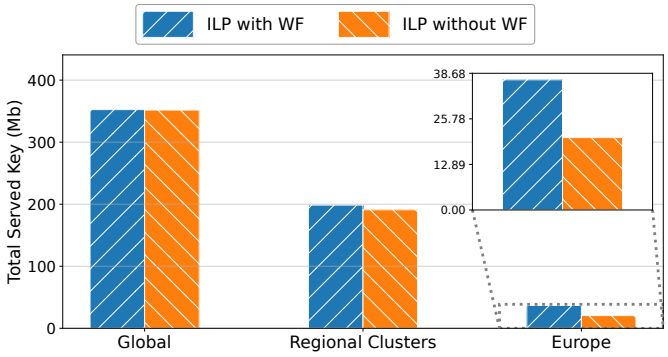

Fig. 3. Total served key with and without weather forecast (WF) considered.

satellites, and with different geographical coverage, as detailed in Table III. The satellite orbit trajectories and altitude were based on [24]. The MILP models were executed under two different atmospheric settings: uniform clear weather and realistic historical hourly cloud coverage per region starting December 14, 2024 (UTC+0) according to Visual Crossing [25].

We evaluate our model in three different GS topologies: **Global**, **Regional Clusters**, and **Europe**, as summarized in Table IV. In the **Global** topology, the GS pairs are at least separated by 2,000 km, thus making the sparsest configuration, reducing simultaneous satellite visibility among ground stations. In Regional Clusters, there are subgroups of regions: Europe, India, and Australia. This setup enables satellites to access multiple nearby nodes when passing over a region, though inter-region communication still spans large distances. The **Europe** topology consists of ground stations located entirely within Europe. This configuration represents a dense continental network with the highest simultaneous satellite visibility among the three configurations.

All secret-key demand rates between every GS pair were set to be equal and constant throughout each time interval. Each topology and heuristic was evaluated under varying levels of key demand rates. At the higher demand levels, the demands were large enough that the solutions were expected to leave the key storage fully empty at the end of the 12-hour period, even in a scenario with cloud coverage. Conversely, at the lowest demand level, the demands were relatively modest, hence residual keys in the QKP were anticipated in the solutions, even under moderate cloud coverages.

B. Performance Comparison with and without forecast

We first compare our solution, considering changing weather conditions using weather forecasting (labeled as *ILP with WF*), to the solutions in Ref. [8] without weather forecasting (labeled as *ILP without WF*). Specifically, the case without weather forecast was done by applying the MILP solution for all quantum connections in each time slot in clear skies to those in real weather scenarios, and then the optimization decisions are applied to the scenarios with real weather conditions.

The total served keys are shown in Fig. 3. In Global topology, this is not very apparent as all GS pairs are very distant from each other, so the satellites do not have many links to decide from. Regional Clusters and Europe topologies, however, show more differences as link options of each satellite are now more than it did with Global topology. The mentioned problem is mostly noticeable in the Europe topology with almost twice the served keys. The deviating results suggest that the choice of satellite-GS connections may not apply the same when we are situated in real weather conditions. Although this depends on what kind of network topology the satellites serve in Fig. 3, the consideration of weather seems inevitable in topologies with closely neighboring regions.

C. Performance Evaluation for each Topology

1) Global: We have compared the performance of the complete MILP formulation and the three presented heuristics as presented in Figs. 4 and 5. In Global topology, the differences in the performances between different methods of link assignment are not evident. As mentioned in the previous section, the reason for this is that the satellites eventually pass each ground station, but there were not many options for the satellite to choose which ground station to establish the QKD link. Given the lack of possible choice of GS selection, the performance of each method is very similar to the optimum MILP solution.

2) Regional Cluster: The Regional Cluster topology has some locations of ground stations that are close to each other, hence the satellites have some options to intelligently select the ground station to assign the QKD link. ILP, as expected, provides the highest amount of served key, but Greedy-ILP and Path-ILP show quite close performance. In clear skies, the Greedy-ILP outperforms Path-ILP. But in real weather, Path-ILP outperforms Greedy-ILP in lower demands. This is because Greedy-ILP commits to a single best link, resulting in possible lost opportunities to serve keys. Random-ILP is significantly worse than both Greedy-ILP and Path-ILP. This trend also occurs in a similar way in the topology of Europe.

3) Europe: The European topology is smaller in distance between each pair of ground stations than the first two topologies. Here, the link selection method significantly affects the final result. The Greedy-ILP outperforms the Path-ILP in higher demands, while in lower demands, the Path-ILP performs better.

Greedy-ILP does not limit establishing a quantum link with the same ground station as the previous time slot. Some regions might constantly have bad weather relative to other regions or the satellite visibility might be only advantageous for a narrow set of locations. So, there is a possibility to have a scenario where the pre-assigned links in Greedy-ILP do not necessarily form a complete path for the keys to relay the shared key in proceeding time slots, while Path-ILP focuses more on creating a complete immediate flow path between two ground stations.

To elaborate further, Greedy-ILP might lead to a greater amount of stored keys in QKP, where there are fewer complete

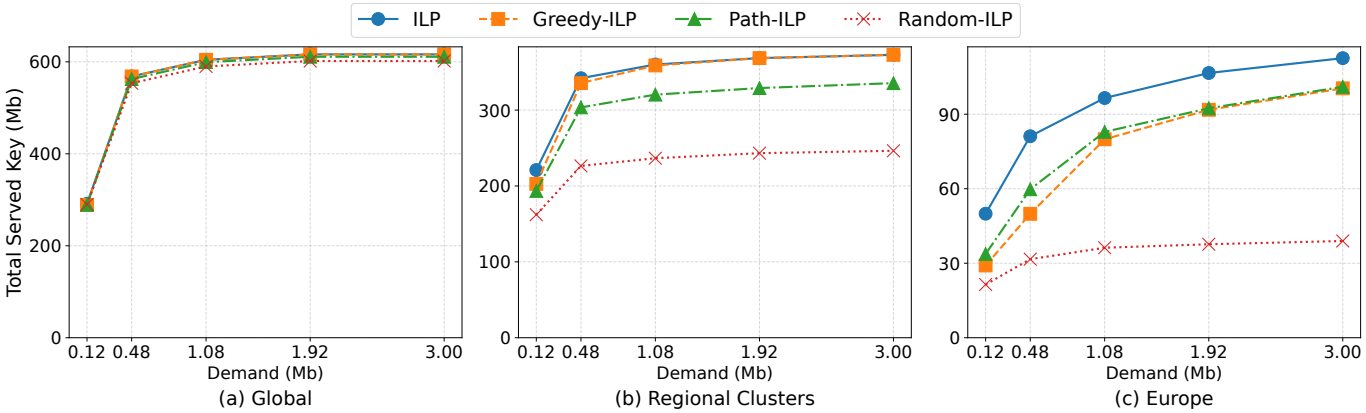

Fig. 4. Total served key in each topology under optimistic weather condition (0% cloud cover).

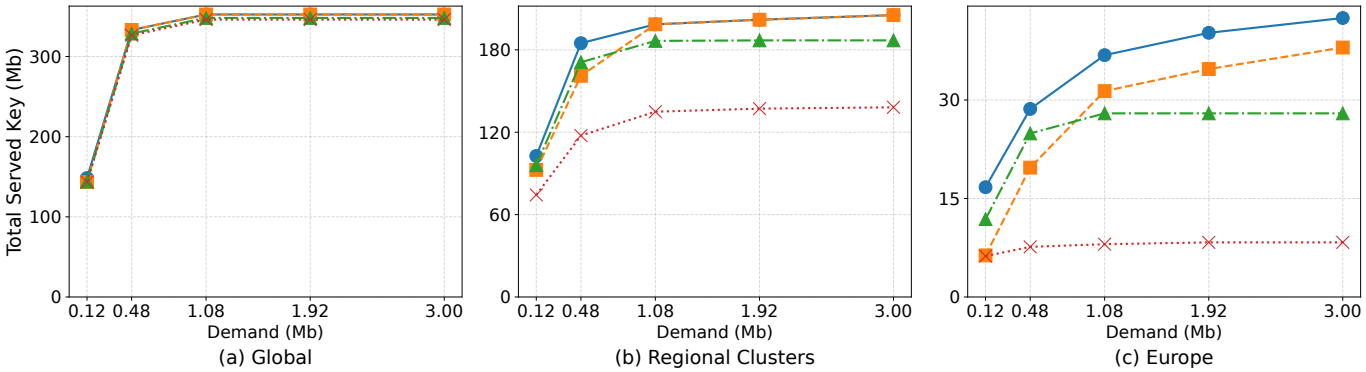

Fig. 5. Total served key in each topology under real weather condition of December 14, 2024 (UTC+0).

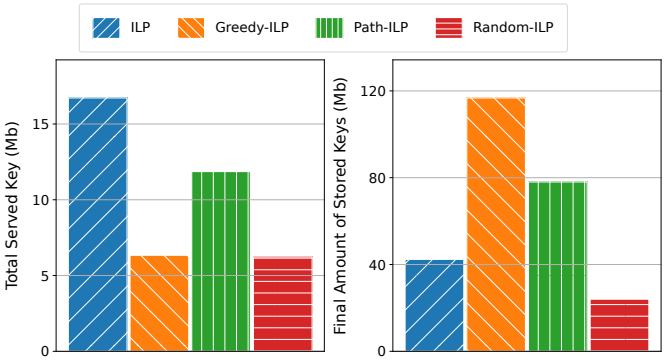

Fig. 6. Total served key and final stored keys with demand 0.12 Mb in Europe.

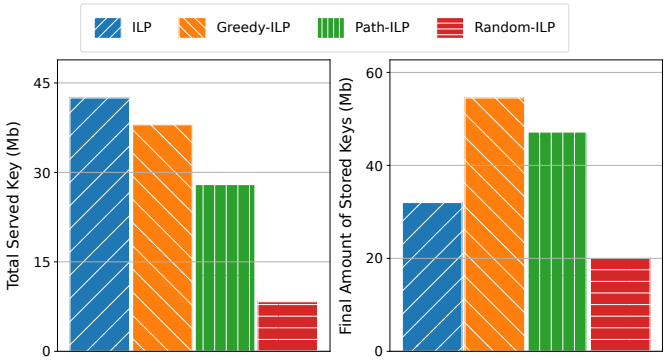

Fig. 7. Total served key and final stored keys with demand 3.00 Mb in Europe.

paths that can be fully utilized. This is evident from Fig. 6. There is a very high accumulation of stored keys in QKP at the end of the simulation, but a smaller amount of key served. Since demand between GS pairs is quickly satisfied, the optimization does not prioritize routing additional keys beyond what is needed. This bottleneck is somewhat resolved for larger demands as more keys can be served for consumption even by fewer set of ground stations.

The scale of the final stored keys in QKP in Fig. 7 has gone down greatly compared to Fig. 6 in a higher demand setting. The ground stations could just get more keys served instead of leaving them in QKP. On the other hand, the increase in total key served in Path-ILP is not as great as Greedy-ILP increase. Path-ILP in fact should have more possible paths as Fig. 6 suggests. The links that are selected for Path-ILP are not necessarily as great as the ones selected for Greedy-ILP. This leads to a situation where the capacity bottleneck of a path is not necessarily big and shows small change even if we

are to increase the demand size to serve more keys.

TABLE V
OPTIMIZATION RUNTIMES IN SECONDS FOR EUROPE TOPOLOGY UNDER REAL WEATHER CONDITION.

Method/Demand (Mb)	0.12	0.48	1.08	1.92	3.00
ILP	93009	4795	2428	2769	5141
Greedy-ILP	135	58	54	56	153
Path-ILP	167	58	56	63	169
Random-ILP	303	75	66	169	262

D. Runtime

Table V presents the runtimes to solve the optimization instances for each of the proposed approaches. Overall, the runtimes remain within a reasonable range for all models. However, we observe significant reductions in the runtime with pre-assigned heuristics by one to two orders of magnitude from the ILP model with link selection. Interestingly, the ILP model with internal link selection takes longer to solve in low-demand scenarios. The ILP experiences difficulty in attaining solutions for lower demands as multiple combinations allow for a greater number of near-optimal link combinations. As demand increases, the solution space narrows and leads to a shorter runtime. Despite this, ILP with link selection can take several hours to reach optimality in larger network instances. The cost of runtime for the increased network scale would be more expensive than the pre-assigned heuristics.

VI. CONCLUSION

This work addresses the resource allocation problem for Quantum Key Distribution (QKD) networks that consider both satellite visibility and changing weather conditions. By modeling the achievable key rates and formulating the problem as a Mixed-Integer Linear Program, we enable efficient scheduling of link selection for satellite-to-ground key generation and end-to-end key routing. Our results demonstrate that adaptive link selection can significantly improve key distribution performance, and an optimal link selection obtained with ILP achieves up to 20% more total served keys than solutions with link selection obtained using heuristics. In the future, we plan to develop a scalable heuristic algorithm for resource allocation for satellite QKD networks.

APPENDIX A
MODELING OF TRANSMITTANCE

SatQuMA assumes a downlink channel. Signal traverses from the top of the atmosphere to the ground level. Throughout transmission, the photon loss from diffraction and detector faults remains relatively predictable compared to atmospheric conditions, which can range greatly from clear skies to complete loss of horizontal visibility. The calculation of radiation attenuation by libradtran [19] in Table VII shows that there is a noticeable attenuation in the transmittance of 785-nm signal radiation to the ground when encountered with water droplets in the clouds based on [26], even though 785-nm is considered within low-loss windows [27]. With less cloud cover, there is a better chance that the signal can reach ground level without encountering the clouds directly. When the cloud cover is close to 100%, the transmittance generally results close to zero. This is evident from the following equations:

TABLE VI
VARIABLE DEFINITIONS FOR APPENDIX A

Variable	Description
I_0	Initial intensity of the radiation
τ	Optical thickness
T_{clear}	Transmittance through clear atmosphere
T_{cloud}	Transmittance through cloudy atmosphere
c	Cloud coverage of the atmosphere

$$I = I_0 e^{-\tau} \tag{16}$$

$$T = (1-c)T_{clear} + cT_{cloud} \tag{17}$$

$$T_{cloud} \propto e^{-\tau} \tag{18}$$

$$0 < T_{cloud} << 1 \tag{19}$$

$$T \approx (1-c)T_{clear} \tag{20}$$

Equation (16) is called Beer-Lambert's Law. It is stating that the intensity of the radiation reaching the bottom is proportional to the original intensity and is inversely correlated with τ, "optical thickness." The optical thickness is dependent on the density and the average radius of the water droplets. Table VII has a list of optical thicknesses and the respective attenuation factor for each of the cloud types. The attenuation is computed by assuming direct radiation from the atmosphere. Even if we take stratocumulus, the link efficiency is 291.87 dB. The high attenuation leads to a total reduction factor of 10^{29}, close to zero. At the end, the average encounter of the radiation with the cloud leads from Equation (17) to an approximation at (20). With less clear horizontal visibility, a more noticeable reduction in signal transmittance is expected to occur on average.

TABLE VII
CLOUD TYPES AND OPTICAL THICKNESS OF 1-KM CLOUDS

Cloud Type	τ	Attenuation (dB)
Stratocumulus	$6.72 \cdot 10$	291.87
Stratus	$1.06 \cdot 10^2$	458.76
Nimbostratus	$2.40 \cdot 10^2$	1042.67
Cumulonimbus	$7.42 \cdot 10^2$	3222.22

ACKNOWLEDGMENT

This work was supported in part by funding from the Innovation for Defence Excellence and Security (IDEaS) program from the Canadian Department of National Defence (DND), and in part by CNPq and Facepe.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," pp. 124–134, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[4] G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, and M. Curty, "Security of quantum key distribution with imperfect phase randomisation," *Quantum Science and Technology*, vol. 9, p. 015025, Dec. 2023.

[5] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, and et al., "Long-term performance of the swissquantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, p. 123001, Dec. 2011.

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, and et al., "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[7] J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, and et al., "Cambridge quantum network," *npj Quantum Information*, vol. 5, Nov. 2019.

[8] V. Karavias, C. White, A. Lord, and M. C. Payne, "Optimizing satellite and core networks for a global quantum network," *J. Opt. Commun. Netw.*, vol. 16, no. 4, pp. 504–515, Apr 2024.

[9] M. Polnik, L. Mazzarella, M. Di Carlo, D. K. L. Oi, A. Riccardi, and A. Arulselvan, "Scheduling of space to ground quantum key distribution," *EPJ Quantum Technology*, vol. 7, no. 1, p. 3, 2020.

[10] R. Maule, N. K. Panigrahy, N. L. Anipeddi, P. Dhara, D. Kilbane, M. Z. Hossain, and et al., "Fair and efficient scheduling strategies for satellite assisted quantum key distribution systems," in *IEEE International Conference on Quantum Communication, Measurement and Computing (QCMC)*, 2024.

[11] J. S. Sidhu, T. Brougham, D. McArthur, and et al., "Finite key performance of satellite quantum key distribution under practical constraints," *Communications Physics*, vol. 6, p. 210, 2023.

[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, and et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, p. 43–47, Aug. 2017.

[13] Y. Li, W.-Q. Cai, J.-G. Ren, C.-Z. Wang, M. Yang, L. Zhang, H.-Y. Wu, L. Chang, J.-C. Wu, B. Jin *et al.*, "Microsatellite-based real-time quantum key distribution," *Nature*, pp. 1–8, 2025.

[14] T. Jennewein, C. Simon, A. Fougeres, F. Babin, F. K. Asadi, K. B. Kuntz, M. Maisonneuve, B. Moffat, K. Mohammadi, and D. Panneton, "Qeyssat 2.0—white paper on satellite-based quantum communication missions in canada," *Canadian Journal of Physics*, 2025.

[15] T. Hiemstra, D. Hasler, D. Paone, F. Reichert, F. Heine, and J. Struck, "The european satellite-based qkd system eagle-1," in *Free-Space Laser Communications XXXVII*, vol. 13355. SPIE, 2025, pp. 216–222.

[16] Q. Zhang, N. Di Cicco, M. Ibrahimi, R. C. Almeida, A. Gatto, R. Boutaba, and M. Tornatore, "Link configuration for fidelity-constrained entanglement routing in quantum networks," in *IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2025, pp. 1–10.

[17] N. K. Panigrahy, P. Dhara, D. Towsley, S. Guha, and L. Tassiulas, "Optimal entanglement distribution using satellite based quantum networks," in *IEEE INFOCOM Network Science for Quantum Communication Workshop*, 2022.

[18] A. Williams, N. K. Panigrahy, A. McGregor, and D. Towsley, "Scalable scheduling policies for quantum satellite networks," in *IEEE International Conference on Quantum Communication, Measurement and Computing (QCMC)*, 2024.

[19] C. Emde, R. Buras-Schnell, A. Kylling, B. Mayer, J. Gasteiger, U. Hamann, and et al., "The libradtran software package for radiative transfer calculations (version 2.0.1)," *Geoscientific Model Development*, vol. 9, p. 1647–1672, May 2016.

[20] Q. Zhang, O. Ayoub, A. Gatto, J. Wu, F. Musumeci, and M. Tornatore, "Routing, channel, key-rate, and time-slot assignment for qkd in optical networks," *IEEE Transactions on Network and Service Management*, vol. 21, no. 1, pp. 148–160, 2023.

[21] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Finite key effects in satellite quantum key distribution," *npj Quantum Information*, vol. 8, no. 1, p. 18, Feb. 2022, open Access, CCBY4.0.

[22] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photonics*, vol. 11, no. 8, pp. 502–508, Jul. 2017.

[23] IBM Corporation, *IBM ILOG CPLEX Optimization Studio Version 22.1.1.0*, 2022, documentation available online. [Online]. Available: https://www.ibm.com/docs/en/icos/22.1.1

[24] R. J. Boain, "A-b-c's of sun-synchronous orbit mission design," Jet Propulsion Laboratory, National Aeronautics and Space Administration, Pasadena, CA, Preprint (Draft being sent to journal) Document ID 20210001902, February 2004, acquired by NASA Technical Reports Server on February 1, 2004; publicly available.

[25] V. C. Corporation, "Visual crossing weather api," 2025, accessed: 2025-01-31.

[26] G. L. Stephens, *Optical Properties of Eight Water Cloud Types*. Aspendale, Victoria, Australia: CSIRO Division of Atmospheric Physics, 1979.

[27] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, and et al., "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, vol. 15, no. 2, p. 023006, feb 2013.