Fair and Efficient Scheduling Strategies for Satellite Assisted Quantum Key Distribution Systems

Ronald Maule*, Nitish K. Panigrahy¶, Naga Lakshmi Anipeddi§, Prajit Dhara‡, Deirdre Kilbane§
Md. Zakir Hossain*, Walter O. Krawec*, Don Towsley†, Bing Wang*
*School of Computing, University of Connecticut, Storrs, CT, USA
†Manning College of Information & Computer Sciences, University of Massachusetts, Amherst, MA, USA
‡Wyant College of Optical Sciences, University of Arizona, Tucson, AZ, USA
§Walton Institute, South East Technological University, Waterford, Ireland
¶Department of Computer Science, Binghamton University, Binghamton, NY, USA

***Abstract*—Satellite-based quantum key distribution (QKD) systems use constellations of satellites to assist secret key generation among ground station pairs that are far away from each other. In this paper, we study satellite scheduling to establish secret keys among ground station pairs in a fair and efficient manner. While satellite scheduling has been considered in the past, existing scheduling algorithms are not for QKD, and have not explicitly accounted for fairness of resource allocation among ground station pairs. We propose three satellite scheduling strategies that have different tradeoffs in fairness and computational overhead. Using extensive simulation, we evaluate these strategies in a wide range of settings, while considering realistic environmental conditions (time-of-day, cloud coverage). Our results demonstrate that they achieve significantly better fairness at the cost of slightly lower overall number of keys when compared to a baseline strategy that has no fairness considerations.**

***Index Terms*—Quantum key distribution (QKD), Satellite Assisted QKD, Satellite scheduling, Fairness**

I. Introduction

Quantum Key Distribution (QKD), where two entities, Alice and Bob, establish secret keys using the principles of quantum mechanics, is one of the most remarkable quantum technologies. It achieves information theoretic security [1]–[3], without relying on computational assumptions, unlike classical public key cryptographic systems. Long-distance QKD where Alice and Bob are at locations far away from each other can be achieved through ground-based fiber connection (with the aid of a sequence of quantum repeaters) or a satellite-based system. The latter has the advantage that it leverages free-space satellite communication that has much lower loss than fiber channels, and hence is well recognized as one of the most promising technologies to achieve global-scale QKD [4]–[8]. Indeed, several experimental studies have demonstrated the technological feasibility of this approach [9]–[12].

In a satellite-based QKD system, a constellation of satellites communicate with ground stations to assist secret key establishment among the ground stations. While multiple architectures have been proposed in the literature [8], we consider *dual-downlink* entanglement distribution architecture (see §II), where a satellite equipped with entanglement sources distributes entanglements to a pair of ground stations simultaneously. This architecture is more efficient than an uplink-based architecture that suffers from early atmospheric diffraction [13]. In addition, coupled with entanglement-based QKD (e.g., E91 [14]), it can be readily used to generate secret keys between the two ground stations.

In the settings with a constellation of multiple satellites and a set of ground station pairs, a satellite can be in view of multiple ground station pairs in a time slot; similarly, a ground station pair can be in view of multiple satellites. With limited number of transmitters at each satellite and receivers at each ground station, *satellite scheduling* determines which satellite to serve which ground station pairs in each time slot.

One satellite scheduling strategy is to maximize the total number of secret keys that are generated among the ground station pairs in each time slot, similar in spirit to maximizing the number of entanglements distributed among the ground station pairs in [15]. Such strategies, however, have no fairness considerations, and hence can cause some ground station pairs, particularly those under unfavorable conditions (e.g., those that are far away from each other), to have low key generation rate. This is undesirable since for such ground station pairs, it is particularly important to achieve as high key rate as possible, because for them the only viable way for performing QKD may be through the satellite system due to their distance.

In this paper, we consider fair and efficient scheduling for dual-downlink based satellite-assisted QKD systems. Specifically, our goal is to achieve fair key allocation among the ground station pairs, while not sacrificing much in terms of the total number of secret keys. We first propose a fairness index that considers the different maximum number of keys that can be generated for each ground station pair. We then propose three satellite scheduling strategies, *slot-based weighted-sum*, *slot-based max-min*, and *window-based max-min*, that exhibit different tradeoffs in terms of fairness and computational overhead. All the strategies account for the finite resource constraints of each satellite and ground station, as well as various dynamics present in satellite-based QKD systems (e.g., key rate affected by time of day and weather conditions).

Using extensive simulations, we evaluate these strategies in a wide range of settings (satellite constellation, satellite altitude), while considering realistic environmental conditions (time-of-day, cloud coverage). Our results demonstrate that,

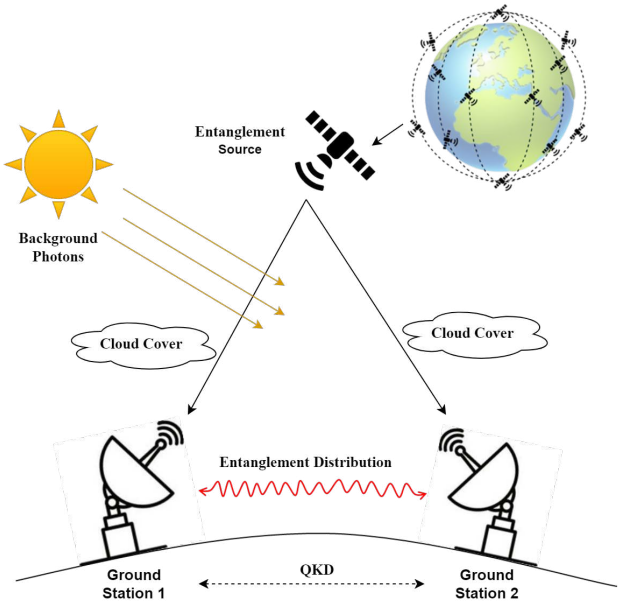


Fig. 1. Dual-downlink satellite-assisted QKD.

compared to a baseline strategy that has no fairness considerations, our proposed strategies achieve significantly better fairness at the cost of slightly lower overall numbers of keys over a time period (a day in our simulations). Among the three proposed strategies, slot-based max-min achieves the best tradeoffs in terms of total number of secret keys, fairness index, and computational overhead. The baseline strategy leads to zero or close to zero fairness index in some cases. For the rest of the cases, slot-based max-min leads to up to 28.7× higher fairness index than the baseline strategy, while only up to 16.9% less secret keys.

The rest of the paper is organized as follows. In Section II, we present problem setting and background. In Section III, we present the scheduling framework and three strategies. In Section IV, we present our evaluation results. In Section V, we briefly review related work. Last, Section VI concludes the paper.

II. Problem Setting and Background

A. Dual-downlink Satellite-assisted QKD

We consider a constellation of satellites that orbit around the Earth at a certain altitude. Specifically, we consider polar constellation as shown in the top right of Fig. 1; our approach can be easily extended to other types of constellation (e.g., Polar, Walker, Iridium, Starlink, and Kuiper [4]). We focus on low-earth-orbit (LEO) satellites, i.e., altitude between 250 to 2000 km. Such LEO satellites benefit from proximity to Earth's surface, and their technological feasibility has been demonstrated experimentally [8], [16], [17]. Each satellite has photon sources that generate entangled pairs and uses downlink optical channels to transmit entanglement pairs to a pair of ground stations simultaneously, as shown in Fig. 1. We consider a set of ground stations. Each pair of ground stations run an entanglement based QKD protocol to establish secret keys between them. We consider one QKD protocol, E91 [14], in the rest of the paper, though our approach can be applied to other entanglement based QKD protocols.

In E91, a source (in our case a satellite) prepares entangled Bell states, sending one qubit to Alice and one qubit to Bob. Alice and Bob, individually, choose a random basis to measure their particle in either the computational Z basis or the Hadamard X basis. This measurement result translates to a raw key bit for each party: if either party receives a $|0\rangle$ or $|+\rangle$, this will be considered a raw key bit of zero; otherwise it will be a raw key bit of one. Clearly, if a true Bell state is held by Alice and Bob and both parties choose the same basis, they will have a correlated outcome; otherwise, they will have a random outcome. The two parties then use an authenticated classical channel to reveal their basis choice. If their choices do not match, this round is simply discarded. The process repeats until the two parties share a suitably large number of raw keys.

These raw keys produced through the quantum communication stage of E91 are only partially correlated (there may be errors, either naturally induced or adversarial) and partially secret (the adversary Eve may have some information on these raw key bits). Thus, they must be further processed before they can be used as a secret key. First, an error correction protocol is run (which leaks additional information to Eve). Second, a privacy amplification protocol is run, which essentially hashes the error corrected raw keys down to a smaller secret key.

Let N denote the number of rounds performed by the QKD protocol. Let ℓ denote the size of the final secret key (after error correction and privacy amplification). Then the *key rate* is defined to be the ratio: $r = \ell/N$. In this paper, we are interested in asymptotic results, i.e., when N approaches infinity. Under these conditions, we use the standard E91/BB84 key-rate expression: $r = 1 - 2h(Q)$, where Q is the error rate in the raw key, and $h(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function [18], [19].

B. Entanglement Sources

We assume each satellite utilizes spontaneous parametric down-conversion (SPDC) based dual-rail polarization entanglement sources that are well-studied and widely used [20]–[22]. In such entanglement sources, a two-qubit entangled Bell state requires four orthogonal modes (i.e., two pairs of mode) to encode. The expression of the output is a quantum state as follows [22], [23]:

$$|\varphi^{\pm}\rangle = N_0\Bigg[\sqrt{p(0)}\,|0,0;0,0\rangle + \sqrt{\frac{p(1)}{2}}(|1,0;0,1\rangle \pm |0,1;1,0\rangle) + \sqrt{\frac{p(2)}{3}}(|2,0;0,2\rangle \pm |1,1;1,1\rangle + |0,2;2,0\rangle)\Bigg], \tag{1}$$

where N_0 is a normalization factor:

$$N_0 = \frac{1}{\sqrt{p(0)+p(1)+p(2)}} = \frac{(N_s+1)^2}{\sqrt{6N_s^2+4N_s+1}} \quad (2)$$

and $p(n)$ is the probability of generating a n-photon term in each pair of mode, given by

$$p(n) = (n+1)\frac{N_s^n}{(N_s+1)^{n+2}}\,, \quad (3)$$

where N_s is *pump power*, i.e., the mean photon number per mode. The entangled pair from the SPDC dual-rail polarization source is

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|1,0;0,1\rangle \pm |0,1;1,0\rangle)\,. \quad (4)$$

The vacuum state is $|0,0;0,0\rangle$, and all the other terms are spurious two-photon states. In Eq. (1), we assume that N_s is low (e.g., below 0.2) and hence $p(n)$ for $n \geq 2$ is negligible and is omitted in the quantum state. In our evaluation (§IV), we set $N_s = 0.01$.

C. Loss and Noise Models

The satellite quantum communication channel via free space optical (FSO) transmission must account for the characteristics of the optical channel in its underlying analysis. Transmission loss for each qubit (comprising of a pair of modes) scales quadratically with free space propagation length and exponentially with aerial propagation length [23]. We incorporate the effect of transmission loss by treating FSO transmission as a Bosonic pure loss channel acting on each mode of the quantum state described in Eq. (1). Most generally, the Bosonic pure loss channel leads to a reduction in the mean photon number of the input state; additionally an input pure quantum state becomes a mixed state for non-zero loss. In the present context, this reduces the probability of successfully delivering the entangled pairs to both ground stations, as well as affecting the fidelity (to the ideal Bell state) of the delivered entangled photons [23]. See more details of the loss model in [23].

Using MODTRAN (Moderate Spectral Resolution Radiative Transfer Model) [24] with the assumption of a clear sky with complete visibility and zero cloud cover, we first compute the *atmospheric transmissivity*, denoted as $\hat{\eta}_{s,g}^{(a)}(t)$, for downlink configuration between satellite s and ground station g at zenith. We subsequently calculate the actual atmospheric transmissivity using the following expression [25]

$$\eta_{s,g}^{(a)}(t) = \hat{\eta}_{s,g}^{(a)}(t)^{\operatorname{cosec}(\theta_{s,g}(t))}\,, \quad (5)$$

where $\theta_{s,g}(t)$ represents the *angle of elevation* between satellite s and ground station g at time t.

To investigate the effect of seasonal variations of atmospheric profiles and weather patterns on atmospheric transmissivity, we selected a single day from each of four different months equally distributed throughout a year. Specifically, using MODTRAN AGT, we generated atmospheric profiles for various locations for the 15^{th} day of March, June, September and December respectively. We used weather data from online resource called Visual Crossing [26], that is widely used for earth observation and climate studies providing global historic weather data records. The cloud coverage data of the year 2022, as per the location and time of the day is taken into account, which is used in our evaluation in §IV. We denote $c_{t,g}$ as the cloud coverage for ground station g at time t. The value of $c_{t,g}$ falls within range of $[0,1]$, where $c_{t,g} = 0$ indicates clear sky above ground station g at time t, and $c_{t,g} = 1$ signifies the opposite (i.e., complete cloud coverage).

In this work, we consider unfiltered background photons as a source of noise within Atmospheric FSO transmission channels. The presence of background photons in the channel impacts the fidelity of entanglement distribution. The background photon flux varies drastically depending on time of the day. The level of background photon flux is at its highest during clear daylight, and at its lowest during clear nighttime. In our work, we consider four time points throughout the day, 12:00 AM, 6:00 AM, 12:00 PM, and 6:00 PM, to measure the background photon flux at each ground station and compute the fidelity of the generated entangled state between two ground stations by modeling the arrival of unfiltered background photons as detector dark click events.

III. Satellite Scheduling Framework and Strategies

In this section, we first present a satellite scheduling framework and fairness index, and then present three scheduling strategies.

A. Scheduling Framework

Let $\mathcal{S}$ denote a set of satellites, and $\mathcal{G}$ denote a set of ground stations. Let $M_s \geq 1$ denote the number of transmitters at satellite s and $R_g \geq 1$ denote the number of receivers at ground station g. We consider the problem of scheduling satellites to ground station pairs in a time period, T (e.g., a day). The basic time unit for scheduling is a time slot (e.g., 1 second). The scheduling problem determines, for any slot t, which satellite $s \in \mathcal{S}$ will serve a ground station pair, $g, g' \in \mathcal{G}$ so as to optimize an objective function (see below). Let binary decision variable, $x_t^{s,g,g'}$, represent the scheduling decision for satellite s and ground station pair (g,g') in slot t. Specifically, $x_t^{s,g,g'} = 1$ when satellite s serves (g,g') at time t, and $x_t^{s,g,g'} = 0$ otherwise.

Our goal is to find a schedule that maximizes the number of keys generated, while satisfying fairness among the ground station pairs. In the following, we define a fairness index based on key generation demand. Specifically, for a given satellite constellation, we introduce *key generation demand*, $d_{1:T}^{g,g'}$, for ground station pair (g,g') over time interval $[1,T]$ as the maximum number of secret keys that can be generated, assuming that (g,g') is the *only* pair that needs to be served by the satellite constellation. A satellite scheduling strategy only needs to consider ground station pairs that have positive key generation demand; the ground station pairs with zero demand can be ignored (since no scheduling strategy can lead

to positive key rate for them). For a given satellite scheduling strategy, let $k_{1:T}^{g,g'}$ denote the total number of secret keys generated for ground station pair (g, g') during interval $[1, T]$ under this strategy. Then the *fraction of demand satisfied* for (g, g') is $k_{1:T}^{g,g'}/d_{1:T}^{g,g'} \in [0, 1]$.

Ideally, we want the ground station pairs to have the same fraction of demand satisfied. We therefore define a fairness index, F, as the minimum fraction of demand satisfied across all ground station pairs with positive demand. That is,

$$F := \min_{g,g' \in \mathcal{G}, d_{1:T}^{g,g'} > 0} (k_{1:T}^{g,g'}/d_{1:T}^{g,g'}) \tag{6}$$

The above fairness index is in $[0, 1]$, and the higher the better.

To determine the satellite schedules for period T, we divide T into *windows*, where each window contains L slots, $1 \leq L \leq T$. When $L = 1$ slot, we refer to the schedule as *slot-based schedule* since it determines the schedule for each slot individually. When $L > 1$, we refer to the schedule as *window-based schedule*, which considers the slots in a window jointly to determine the schedule for each slot in the window. As the window size increases, more constraints are considered jointly, and hence can potentially lead to better schedules. On the other hand, larger window size leads to more decision variables and constraints in an optimization formulation, which can lead to higher computation overhead.

We assume that the loss and noise characteristics of the channels from the satellites to the ground stations are known beforehand. This is a reasonable assumption since short-term weather and cloud coverage can be predicted accurately (e.g., when T is one day). As such, the schedule for all the satellites will be determined beforehand, and transmitted to the satellites using classical communication channels before the start of a scheduling time period.

B. Scheduling Strategies

In the following, we present three scheduling strategies. All three strategies consider both fairness and total number of keys generated, and use different designs to trade off these two metrics. In all the strategies, let $\lambda_t^{s,g,g'}$ denote the number of entanglements that satellite s distributes to ground station pair (g, g') successfully in slot t, and let $\mathsf{R}_t^{s,g,g'}$ denote the corresponding key-rate. We estimate $\lambda_t^{s,g,g'}$ using the loss model in §II-C beforehand. Similarly, we estimate $\mathsf{R}_t^{s,g,g'}$ by estimating the error using the noise model in §II-C and key rate expression in §II-A beforehand. Let $c_{t,g}$ and $c_{t,g'}$ denote respectively the cloud coverage for ground station g and g' in slot t, which can also be estimated beforehand based on weather prediction as described in §II-C. Then we set the cloud coverage for ground station pair (g, g') as $c_{t,g,g'} = \max(c_{t,g}, c_{t,g'})$. Therefore, for slot t, following the linear approximation in [27], the number of secret keys that is generated by satellite s serving ground station pair (g, g') is $(1 - c_{t,g,g'})\lambda_t^{s,g,g'}\mathsf{R}_t^{s,g,g'}$. In the rest of the paper, for ease of exposition, let $n_t^{s,g,g'} := (1 - c_{t,g,g'})\lambda_t^{s,g,g'}\mathsf{R}_t^{s,g,g'}$ denote the number of secret keys that can be generated in slot t for ground station pair (g, g') by satellite s.

We next present the three strategies. Two of them are slot-based with window size $L = 1$ slot, and the other is window-based with $L > 1$ slot. All three strategies are described as solutions to mixed-integer programming (MIP) problems, which can be solved using standard MIP solvers (e.g., CPLEX [28]).

1) Slot-based Weighted-sum: For each slot t and ground station pair (g, g'), this strategy considers two factors: (i) the demand $d_t^{g,g'}$ for slot t, i.e., the maximum number of secret keys that can be generated for (g, g') using the satellite constellation assuming no competition with other ground station pairs, and (ii) estimated number of secret keys that has already been created for a ground station pair (g, g') so far (i.e., from slot 1 to the end of slot $t - 1$), denoted as $k_{1:t-1}^{g,g'}$. Both of them can be estimated beforehand using the channel models and key rate expression in §II; the estimation of $k_{1:t-1}^{g,g'}$ further uses the scheduling decisions up to slot $t - 1$.

This strategy takes $d_t^{g,g'}$, $k_{1:t-1}^{g,g'}$, $n_t^{s,g,g'}$ as input and maximizes a *weighted sum*, subject to the satellite constraints (number of transmitters at each satellite) and ground station constraints (number of receivers at each ground station). Specifically, the optimization problem for each slot t is

$$\max \sum_{s \in \mathcal{S}} \sum_{g,g' \in \mathcal{G}} x_t^{s,g,g'} \left(\frac{d_t^{g,g'}}{k_{1:t-1}^{g,g'}} + \frac{n_t^{s,g,g'}}{d_t^{g,g'}} \right) \tag{7}$$

$$\text{s.t.} \sum_{g,g' \in \mathcal{G}} x_t^{s,g,g'} \leq M_s, \forall s \in \mathcal{S} \tag{8}$$

$$\sum_{s \in \mathcal{S}} \sum_{g' \in \mathcal{G}} x_t^{s,g,g'} \leq R_g, \forall g \in \mathcal{G} \tag{9}$$

$$x_t^{s,g,g'} \in \{0, 1\}, \forall s \in \mathcal{S}, g, g' \in \mathcal{G} \tag{10}$$

The binary decision variable $x_t^{s,g,g'}$ determines whether satellite s distributes entanglements to ground station pair (g, g') in slot t or not, $s \in \mathcal{S}, g, g' \in \mathcal{G}$. In the objective function, the first term in the sum, $d_t^{g,g'}/k_{1:t-1}^{g,g'}$, gives higher weight to a (g, g') pair that has received less secret keys. The second term in the sum, $n_t^{s,g,g'}/d_t^{g,g'}$, gives higher weight to scheduling decisions which satisfy more of the demands in the slot. In (7), we give the two terms in the sum equal weights, and leave other forms of weight settings to future work.

Henceforth, we refer to the above strategy as *slot-based weighted-sum*. Since the decision for slot t depends on the decisions in earlier slots (due to $k_{1:t-1}^{g,g'}$), we solve the optimization problem sequentially one slot at a time.

2) Slot-based Max-min: The above weighted-sum formulation does not incorporate the fairness index explicitly. We next enhances it to incorporate the fairness index explicitly. Specifically, we set the objective function as

$$\max \alpha\Lambda + \frac{1 - \alpha}{\gamma} \sum_{s \in \mathcal{S}} \sum_{g,g' \in \mathcal{G}} x_t^{s,g,g'} \left(\frac{d_t^{g,g'}}{k_{1:t-1}^{g,g'}} + \frac{n_t^{s,g,g'}}{d_t^{g,g'}} \right) \tag{11}$$

where $\alpha \in (0,1)$ is a pre-determined constant, and γ is a normalization term defined as follows, so that the second term is no more than 1.

$$\gamma := \sum_{s\in\mathcal{S}} \sum_{g,g'\in\mathcal{G}} \left(\frac{d_t^{g,g'}}{k_{1:t-1}^{g,g'}} + \frac{n_t^{s,g,g'}}{d_t^{g,g'}} \right)$$

In (11), α represents the relative weight between the two terms in the objective function: the first is related to the fairness index (see below) and the second is the same term in (7). We use both terms since the first term is only about the the fairness index, and considering it solely can lead to pessimistic results in terms of key rate. We use $\alpha = 0.9$ in our evaluation (see §IV) to give the first term (on fairness) a higher weight.

The constraints are slot-based, including the constraints on the number of transmitters for each satellite, the number of receivers for each ground station, and the binary variable constraints, the same as in (8)-(10). In addition, we have a constraint on Λ as the minimum fraction of demands that has been satisfied until end of slot t (i.e., $d_{1:t}^{g,g'}$) across all the ground station pairs, i.e.,

$$k_{1:t-1}^{g,g'} + \sum_{s\in\mathcal{S}} x_t^{s,g,g'} n_t^{s,g,g'} \geq \Lambda d_{1:t}^{g,g'}, \forall g,g' \in \mathcal{G} \text{ s.t. } d_{1:t}^{g,g'} > 0$$

Note that the above constraint considers the cumulative demand, $d_{1:t}^{g,g'}$, which differs from the demand in slot t, $d_t^{g,g'}$, in the objective function in (11).

Henceforth, we refer to this strategy as *slot-based max-min*, since it aims to maximize the minimum of fraction of demands that has been satisfied so far in each slot. Again, we solve it sequentially one slot at a time due to $k_{1:t-1}^{g,g'}$ in the formulation.

3) Window-based Max-min: We next extend the above slot-based max-min to a window-based strategy, referred to as *window-based max-min*. This strategy considers a window of L slots, and reduces to slot-based max-min when $L = 1$. In the following, we present the formulation for the scheduling for the k-th window, i.e., from slot $kL+1$ to $(k+1)L$. For ease of notation, let b_k and e_k denote the beginning and ending slot of the k-th window, respectively. Then the formulation is

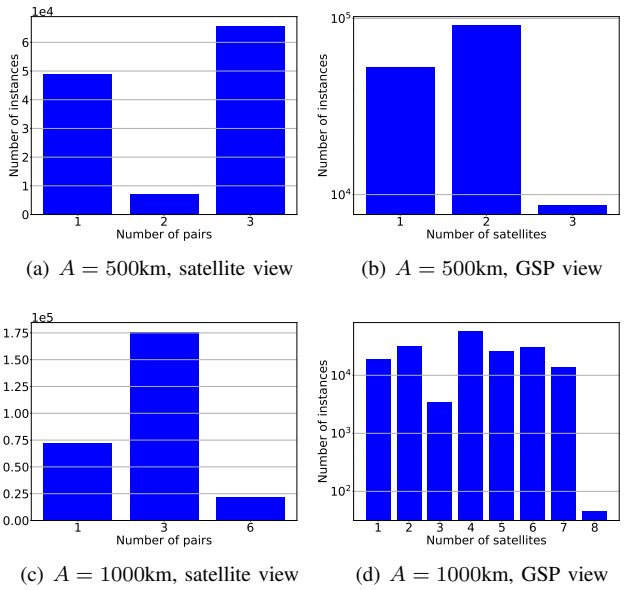
$$\max \alpha\Lambda + \frac{1-\alpha}{\gamma} \sum_{t=b_k}^{e_k} \sum_{s\in\mathcal{S}} \sum_{g,g'\in\mathcal{G}} x_t^{s,g,g'} \left(\frac{d_t^{g,g'}}{k_{1:b_k-1}^{g,g'}} + \frac{n_t^{s,g,g'}}{d_t^{g,g'}} \right) \tag{12}$$

$$\text{s.t.} \sum_{g,g'\in\mathcal{G}} x_t^{s,g,g'} \leq M_s, \forall s \in \mathcal{S}, t = b_k, \ldots, e_k \tag{13}$$

$$\sum_{s\in\mathcal{S}} \sum_{g'\in\mathcal{G}} x_t^{s,g,g'} \leq R_g, \forall g \in \mathcal{G}, t = b_k, \ldots, e_k \tag{14}$$

$$k_{1:b_k-1}^{g,g'} + \sum_{t=b_k}^{e_k} \sum_{s\in\mathcal{S}} x_t^{s,g,g'} n_t^{s,g,g'} \geq \Lambda d_{1:e_k}^{g,g'}, \quad \forall g,g' \in \mathcal{G} \text{ s.t. } d_{b_k:e_k}^{g,g'} > 0 \tag{15}$$

$$x_t^{s,g,g'} \in \{0,1\}, \forall s \in \mathcal{S}, g,g' \in \mathcal{G}, t = b_k, \ldots, e_k \tag{16}$$



(a) $A = 500$km, satellite view (b) $A = 500$km, GSP view

(c) $A = 1000$km, satellite view (d) $A = 1000$km, GSP view

Fig. 2. (a) Satellite view: for a satellite, the number of ground station pairs that can potentially be served by the satellite, and (b) ground station pair (GSP) view: for a GSP, the number of satellites that can potentially serve it. All the plots are for the day in September.

where as in slot-based max-min, $\alpha \in (0,1)$ is a pre-determined constant, and γ is a normalization term, defined as

$$\gamma := \sum_{t=b_k}^{e_k} \sum_{s\in\mathcal{S}} \sum_{g,g'\in\mathcal{G}} \left(\frac{d_t^{g,g'}}{k_{1:b_k-1}^{g,g'}} + \frac{n_t^{s,g,g'}}{d_t^{g,g'}} \right)$$

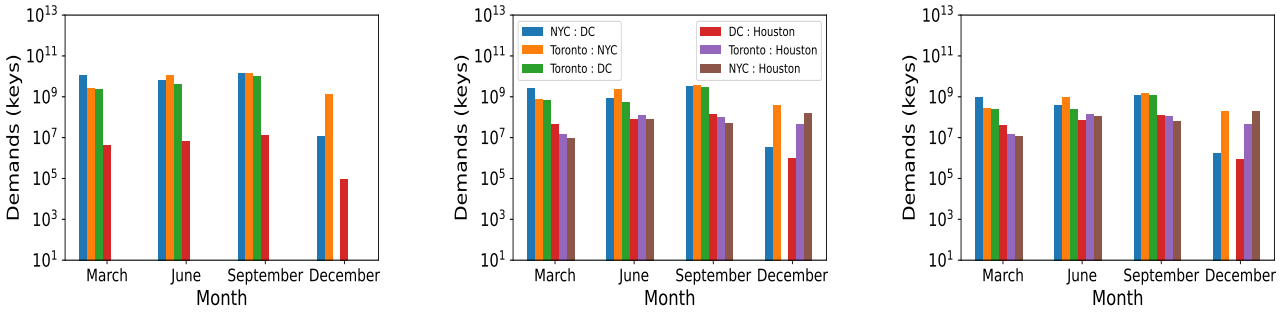
The running time of the above formulation increases with L. For the evaluation settings in §IV, we vary L from 1 to 240 slots; we do not use larger L values due to their higher computational overhead.

IV. Performance Evaluation

In this section, we evaluate our proposed scheduling strategies using extensive simulations. In the following, we first describe the evaluation setup and then the results.

A. Evaluation Setup

We consider a polar constellation of LEO satellites in 20 rings, each ring with 20 satellites as in [4], [15]. Let A denote the attitude of the satellites. We consider three altitudes, $A = 500$km, 800km, and 1000km. The orbit time (the amount of time for a satellite to finish one orbit) is 5668, 6044, and 6298 seconds, for satellite altitudes of 500km, 800km and 1000km, respectively. Each satellite is equipped with a SPDC entanglement source (see §II-B) that operates at a 1 GHz rate, i.e., generating 10^9 entangled photons per second. The pump power of each source is set to a low value ($N_s = 0.01$) so that high-order-photon contributions are negligible. We consider 4 ground stations in North America: New York City (NYC), Washington D.C. (DC), Toronto, and Houston, forming a total of 6 ground station pairs. Considering the constraints of the current technologies, we focus on the setting where each



(a) $A = 500$km (b) $A = 800$km (c) $A = 1000$km

Fig. 3. The demand of each ground station pair for each of the four days and three satellite altitudes. Only non-zero demands are plotted.

satellite has a single transmitter and each ground station has a single receiver, i.e., $M_s = 1$, $R_g = 1$. We also explore the case when each satellite has three transmitters, i.e., $M_s = 3$; the results are very close to those when $M_s = 1$ due to constraints of the ground stations. Henceforth, we only present the results when $M_s = 1$.

As described in §II-C, we consider four days, the 15^{th} day of March, June, September, and December in 2022, with channel models following the actual weather and background photon measurement data. For each day, we obtain the satellite schedules using our proposed strategies, i.e., $T = 1$ day. Each slot is one second. Therefore, $T = 86,400$ slots. The elevation angle threshold is set to 20°, i.e., a satellite can only serve a ground station pair when the elevation angles to both ground stations are larger than 20°.

We compare our three proposed approaches with a baseline scheduling strategy that only aims to maximize the total number of keys in each slot, with no fairness considerations. Specifically, it differs from slot-based weighted-sum in that the objective function is maximizing $\sum_{s\in\mathcal{S}}\sum_{g,g'\in\mathcal{G}} x_t^{s,g,g'} n_t^{s,g,g'}$. Henceforth, we refer to this baseline strategy as *slot-based max-key*. The solutions of all the strategies are obtained using CPLEX [28], a widely used MIP solver.

We evaluate the various scheduling strategies using two performance metrics: (i) total size of received secret keys (i.e., number of generated keys through QKD) across all the ground station pairs at the end of a day, and (ii) fairness index, F, as defined in (6).

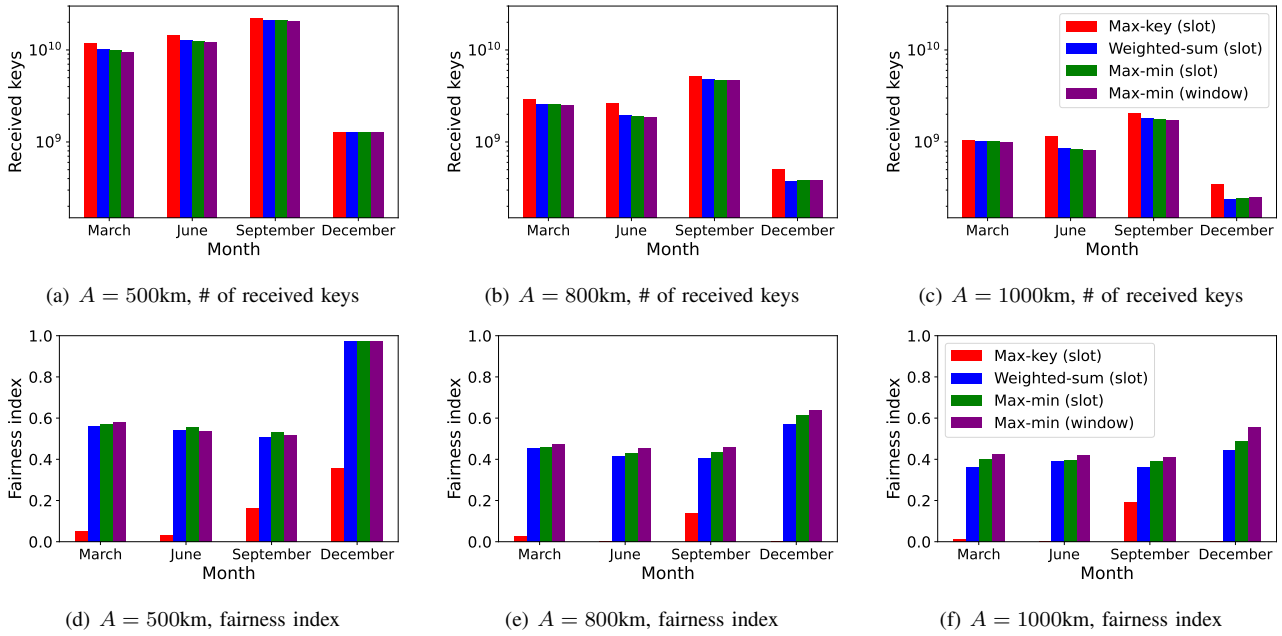
B. Need for Satellite Scheduling

We first show the need for satellite scheduling. Fig. 2a plots the histogram of the number of pairs that a satellite can choose to serve in a slot, considering all the satellites and slots in a day, for $A = 500$km and the day in September. The y-axis represents the number of instances, considering all the 20×20 satellites in the constellation and all the slots in a day. We see a significant number of instances in which a satellite can choose from two or three ground station pairs to serve in one slot. Fig. 2b shows the corresponding results from the perspective of the ground station pairs, i.e., for a ground station pair, the number of satellites from which it can choose to be served, considering all the ground station pairs and slots in a day. We see a significant number of instances in which a ground station pair can be served by two or three satellites. Fig. 2c and d show the corresponding results for $A = 1000$km, and again for the day in September. We see more choices for this higher altitude: there are a large number of instances in which a satellite can choose from 3 or 6 ground station pairs in a slot, while a ground station pair can choose from up to 8 satellites in a slot. Since a satellite has a single transmitter, it can choose one ground station pair to serve in a slot; since a ground station only has a single receiver, it can only be served by one satellite, and can only be in one pair that is served. Therefore, a satellite scheduling strategy is needed that considers the possible set of scheduling choices, and selects the one that satisfies a certain optimization goal.

C. Demands of Ground Station Pairs

Before presenting the results of the various satellite scheduling strategies, we first present the demand of each ground station pair under various settings. Recall that the demand of a ground station pair is the maximum number of secret keys that can be generated for a ground station pair, assuming that it is the only pair that is served by the satellite constellation. Fig. 3 shows the demands of the various ground station pairs for $A = 500$km, 800km, and 1000km, and each of the four days that we consider. For each setting, only the pairs with positive demands are shown in the figure. We see more pairs have positive demands as the altitude increases since more pairs can be served by the satellite constellation at higher altitudes. For a given altitude and ground station pair, the demand of the ground station pair can vary significantly across the days due to different weather conditions (solar radiance and cloud coverage). The demand for the day in December is particularly low due to high cloud coverage (sometimes close to full cloud coverage in an entire day). In contrast, the demand for the day in September tends to be higher than the other three days. We also observe that for a given ground station pair and day, the demand is lower for a higher altitude, even though more satellites are in view of this ground station pair as altitude increases. This is due to the higher loss and noises for higher altitudes.

Four pairs, (NYC, DC), (Toronto, NYC), (Toronto, DC), and (DC, Houston), have positive demands in most cases for



(a) $A = 500$km, # of received keys (b) $A = 800$km, # of received keys (c) $A = 1000$km, # of received keys

(d) $A = 500$km, fairness index (e) $A = 800$km, fairness index (f) $A = 1000$km, fairness index

Fig. 4. Performance comparison: the three proposed scheduling strategies vs. the baseline max-key strategy. For window-based max-min, $L = 240$ slots.

all altitudes ($A = 500$km, 800km and 1000km). Due to close geography distance, (NYC, DC) pair tends to have the highest demand, except for December due to high cloud coverage. Two other close-by pairs, (Toronto, NYC) and (Toronto, DC), also tend to have high demands. One special case is (Toronto, DC) in the December day for all altitudes, where the maximum cloud coverage of the two ground stations is one for all the time periods, leading to zero demand for the day (i.e., no key can be generated). The pair (DC, Houston) has much lower demand than the above three pairs. The remaining two pairs, (NYC, Houston) and (DC, Houston), only have positive demand when the altitude is 800km or 1000km.

Since the demand for a ground station pair represents the maximum number of keys that can be generated for the pair, if the goal of satellite scheduling is simply to maximize the total number of keys, the pairs with lower demand will be served at lower priority. Therefore, for better fairness, it is important to take demands into consideration, and serve the ground station pairs with lower demand with higher priority.

D. Evaluation Results

Fig. 4 compares the performance of our proposed scheduling strategies and the baseline slot-based max-key strategy in all the settings of satellite altitudes and days. The performance of window-based max-min depends on the window size L. The results below are for $L = 240$ slots; the impact of window size L on the performance of window-based max-min is deferred to §IV-F.

The top row of Fig. 4 shows the total size of secret keys across the ground station pairs in a day. For all the schemes, we see that, consistent with the results for demands (see §IV-C), the total size of secret keys decreases with increasing altitude, even though more pairs can be served by the satellite constellation at a higher altitude. In addition, for a given altitude, the total size of secret keys is the highest for the day in September and lowest for the day in December, consistent with the demands for these two days.

For each setting, as expected, the slot-based max-key strategy leads to more secret keys than our proposed strategies, since its optimization goal is maximizing the total number of secret keys. For the three strategies that we propose, in most cases, slot-based weighted-sum leads to slightly (up to 3.0%) more keys than slot-based max-min strategy, while slot-based max-min leads to slightly (up to 7.2%) more keys than window-based max-min. across the various settings, the baseline max-key strategy leads to 0.02% to 43.0% more keys than slot-based weighted-sum strategy.

The bottom row of Fig. 4 shows the fairness index. We see that the max-key strategy leads to significantly lower fairness index than our proposed strategies in all the settings. For our proposed strategies, slot-based max-min leads to slightly higher (up to 4.0% higher) fairness index than slot-based weighted-sum, while window-based max-min leads to slightly higher (up to 13.4% higher) fairness index than slot-based max-min in most cases, except for two cases when $A = 500$km, a point that we will return to in §IV-F.

In the bottom row of Fig. 4, the baseline max-key strategy leads to zero or close-to-zero fairness index in four setting ($A = 800$km and 1000km, and the days in June and December). For the rest of the eight settings, slot-based max-min leads to up to 28.7$\times$ higher fairness index than the max-key strategy, while only up to 16.9% less keys (the reduction in number of keys is up to 39.9% considering all the twelve settings).

Summarizing the above results, slot-based max-min might be a preferred strategy in balancing the two performance metrics (fairness index and number of secret keys) and computational overhead. Compared to slot-based weighted-sum, it leads to slightly higher fairness index at the cost of slightly less secret keys. Compared to window-based max-min, it can lead to more secret keys, slightly lower fairness index, and significantly lower computational overhead (see more discussion in §IV-F).

E. Secret Keys across Ground Station Pairs

In the above, the fairness index is the minimum of the fraction of demand satisfied across all the ground station pairs. We next show the key distribution across the ground station pairs, i.e., the fraction of demand satisfied for each ground station pair with positive demand, in various settings under our proposed strategies. Fig. 5 shows the results, where each row corresponds to a strategy. Comparing the first and second rows of Fig. 5, we see that the results for slot-based weighted-sum and max-min are similar, while slot-based max-min leads to slightly more uniform distribution of keys than slot-based weighted-sum (e.g., when $A = 500$km). Comparing the second and third rows of Fig. 5, we further see that window-based max-min leads to more uniform distribution of keys than slot-based max-min.

The more uniform distribution of keys in window-based max-min compared to slot-based max-min is because it considers the slots in a window jointly. To gain more insights into the scheduling strategies, Fig. 6 presents a time series plot that shows the ratio of the number of received keys over the demand for each hour for the three strategies (each column corresponds to a strategy). It is for two settings, $A = 500$km and 1000km, both for the day in March. When $A = 500$km, while the decisions of the three strategies are similar for two pairs, (DC, Houston) and (NYC, DC), i.e., the two pairs with the minimum and maximum demands, respectively, their decisions for the other two pairs, (Toronto, NYC) and (Toronto, DC), are clearly different: in window-based max-min, their ratios are smooth over time and almost overlap with each other; while they interleave in slot-based max-min, and in slot-based weighted sum, one pair has consistently higher ratio than the other. When $A = 1000$km, we again see four pairs have very similar ratio over time, while their differences is larger in slot-based max-min, and even larger in slot-based weighted-sum.

F. Impact of Window Size on Window-based Max-min

Last, we evaluate the impact of window size on performance in window-based max-min strategy. Fig. 7 shows the two performance metrics for various settings with the window size L varies from 1 to 240 slots (seconds), where the case when $L = 1$ corresponds to slot-based max-min. In general, we see that increasing L leads to less secret keys, while higher fairness index. Two exceptions are $A = 500$km, for the days in June and September, where $L = 1$ has slightly higher fairness index than $L = 240$. For all the other settings, the fairness index of $L = 240$ is higher (0.3% to 13.4% higher) than that of $L = 1$. The computational overhead increases with L, and when $L = 240$s, it already leads to more than 10 times more running time than when $L = 1$ in some settings (e.g., for $A = 1000$km and the day in September) due to more decision variables and constraints in the optimization problem. The running time will be even larger for a larger number of satellites and ground station pairs. Therefore, considering both performance and computational overhead, slot-based max-min (i.e., $L = 1$) might be a preferred strategy in practice.

V. Related Work

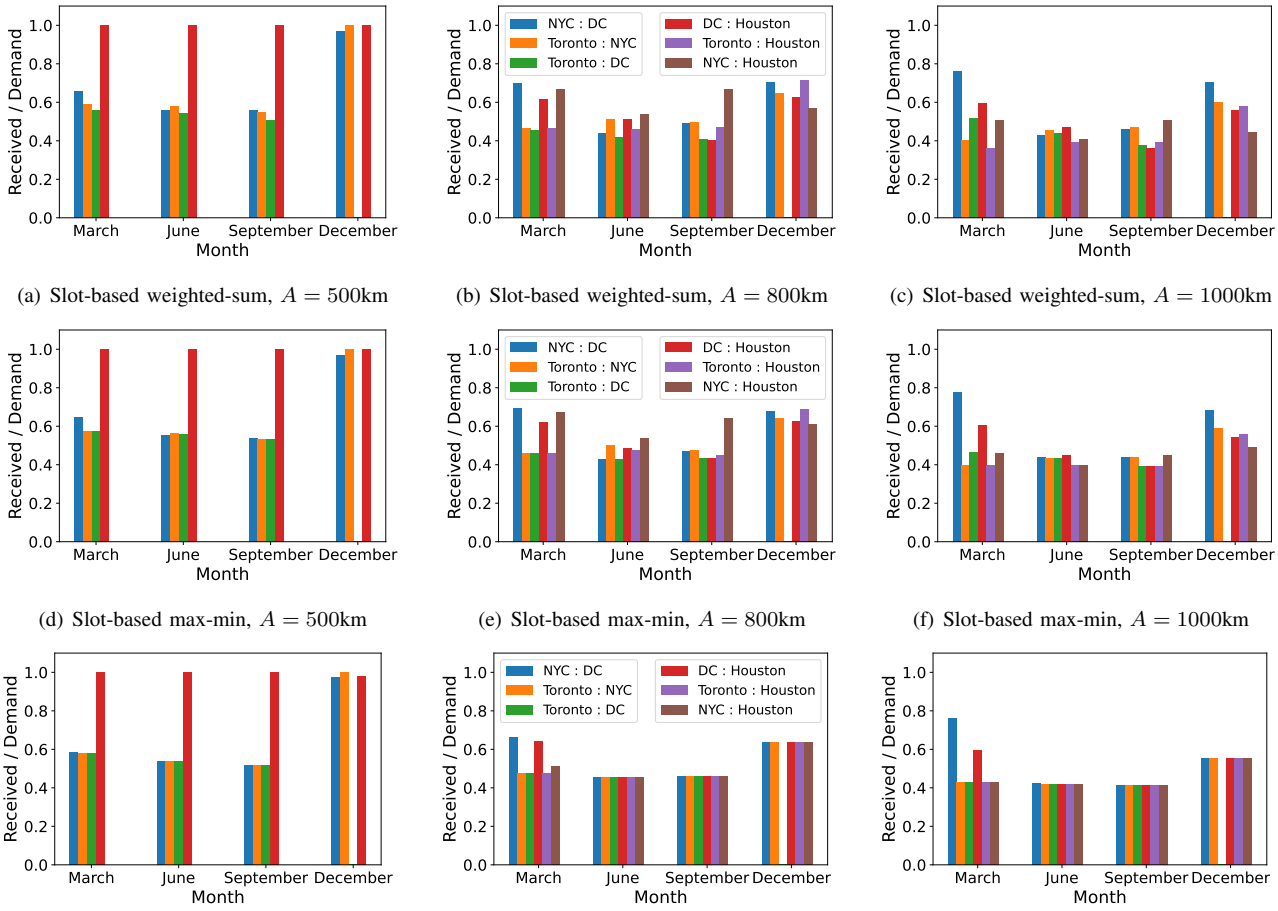
There are several proposals for design considerations and component specifications of a quantum satellite network [29]–[31]. In particular, authors in [31] proposed the use of quantum memory equipped satellites for memory assisted QKD systems to enhance the key rates. Authors in [32] quantified the performance limits of satellite QKD systems, examining factors such as link efficiency, background light, and source quality while considering finite-block size effects. These studies do not explore the scheduling aspect of quantum satellite communication.

The study in [4] studied several satellite configurations to minimize the number of satellites and maximize the overall entanglement generation rate in a polar satellite constellation. The work that is closest to ours is [15] where the authors designed satellite scheduling algorithms for entanglement distribution in dual-downlink settings. The authors proposed an optimization approach to maximize entanglement distribution in each slot considering the constraints at the satellites and ground stations. Their scheduling algorithm is for entanglement distribution, not for QKD. In addition, their design assigns weights to different ground station pairs, unlike our design that aims to optimize the fairness metric and the total number of received keys.

The study in [27] schedules a single satellite to serve multiple ground stations. While the authors also formulated optimization problems, their study differs from ours in two important aspects. First, they consider a single satellite, unlike satellite constellation in our study. Second, the satellite performs QKD with each ground station individually, instead of with a ground station pair as in dual-downlink architecture as in this study.

VI. Conclusion

We studied satellite scheduling to establish secret keys among ground station pairs in a fair and efficient manner. We proposed three satellite scheduling strategies that have different tradeoffs in fairness and computational overhead. Using extensive simulations, we evaluate these three strategies in a wide range of settings, while considering realistic environmental conditions (time-of-day, cloud coverage). Our results demonstrate that they achieve significantly better fairness at the cost of slightly lower overall number of keys when compared to a baseline strategy that has no fairness considerations.



(a) Slot-based weighted-sum, $A = 500$km (b) Slot-based weighted-sum, $A = 800$km (c) Slot-based weighted-sum, $A = 1000$km

(d) Slot-based max-min, $A = 500$km (e) Slot-based max-min, $A = 800$km (f) Slot-based max-min, $A = 1000$km

(g) Window-based max-min, $A = 500$km (h) Window-based max-min, $A = 800$km (i) Window-based max-min, $A = 1000$km

Fig. 5. Fraction of demand satisfied for the various settings. The three rows compare the results from the three strategies that we propose. For window-based max-min, $L = 240$ slots.

ACKNOWLEDGEMENT

This research was supported in part by the NSF grants CNS-1955744, CCF-2143644, NSF-ERC Center for Quantum Networks grant EEC-1941583, and the MURI ARO Grant W911NF2110325. The opinions expressed in this paper are those of the researchers and not of funding sources.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019.

[3] E. Diamanti, H.-k. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Quantum Inf.*, vol. 2, no. 16025, 2016.

[4] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling, "Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet," *npj Quantum Inf*, vol. 7, no. 4, 2021.

[5] C. Simon, "Towards a global quantum network," *Nat. Photonics*, vol. 11, pp. 678–680, 2017.

[6] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *IEEE J. Selected Top. Quant. Electron.*, vol. 9, pp. 1541–1551, 2003.

[7] T. Jennewein and B. Higgins, "The quantum space race," *Phys. World*, vol. 26, no. 52, 2013.

[8] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quant. Inf.*, vol. 3, no. 30, 2017.

[9] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, *et al.*, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013.

[10] J. Yin, Y. Cao, S.-B. Liu, G.-S. Pan, J.-H. Wang, T. Yang, Z.-P. Zhang, F.-M. Yang, Y.-A. Chen, C.-Z. Peng, *et al.*, "Experimental quasi-single-photon transmission from satellite to earth," *Optics express*, vol. 21, no. 17, pp. 20032–20040, 2013.

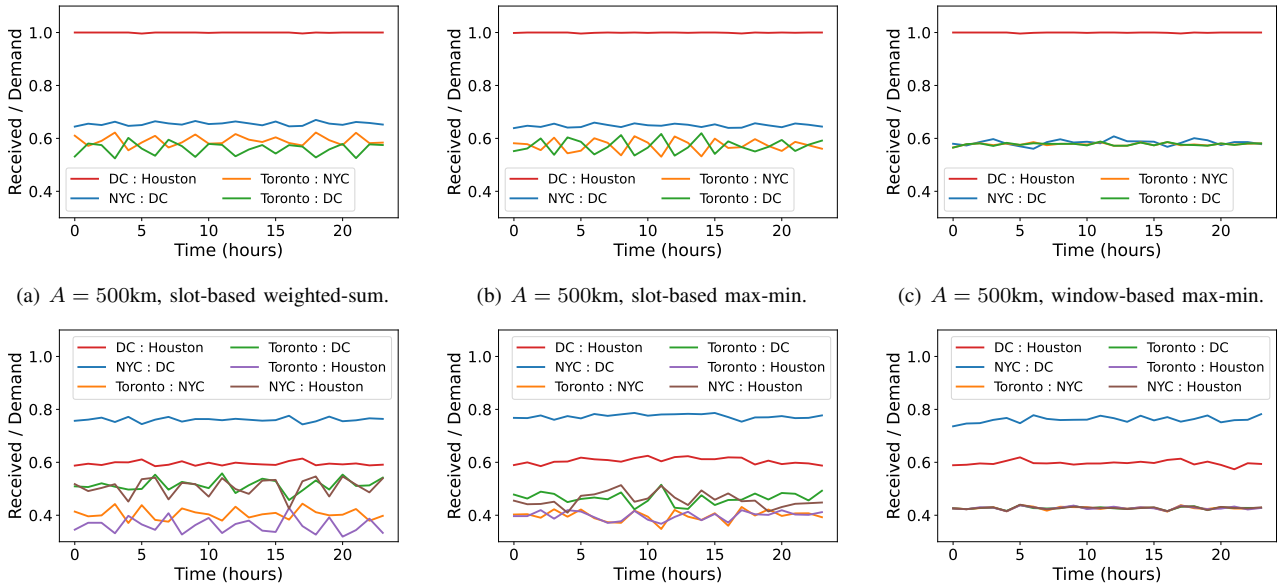
[11] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, p. 040502, 2015.

[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[13] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, February 2013.

[14] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[15] N. K. Panigrahy, P. Dhara, D. Towsley, S. Guha, and L. Tassiulas, "Optimal entanglement distribution using satellite based quantum networks," in *NetSciQCom: Network Science for Quantum Communication Networks, in conjunction with Infocom*, May 2022.



(a) $A = 500$km, slot-based weighted-sum. (b) $A = 500$km, slot-based max-min. (c) $A = 500$km, window-based max-min.

(d) $A = 1000$km, slot-based weighted-sum. (e) $A = 1000$km, slot-based max-min. (f) $A = 1000$km, window-based max-min.

Fig. 6. Time series plot of received packets in one hour divided by the demand in that hour for the four ground station pairs, $A = 500$km or 1000km for the day in March. For window-based max-min, $L = 240$ slots.

[16] S.-K. Liao and et al., "Ground test of satellite constellation based quantum communication," *ArXiV preprint 1611.09982v1*, 2016.

[17] J. Yin and et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, pp. 1140–1144, 2017.

[18] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000.

[19] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, p. 012332, Jul 2005.

[20] H. Krovi, S. Guha, Z. Dutton, J. Slater, C. Simon, and W. Tittel, "Practical quantum repeaters with parametric down-conversion sources," *Appl. Phys. B.*, vol. 122, 2016.

[21] P. Kok and S. Braunstein, "Post-selected versus non-post-selected quantum teleportation using parametric down-conversion," *Phys. Rev. A.*, vol. 61, 2000.

[22] P. Dhara, S. J. Johnson, C. N. Gagatsos, P. G. Kwiat, and S. Guha, "Heralded multiplexed high-efficiency cascaded source of dual-rail entangled photon pairs using spontaneous parametric down-conversion," *Physical Review Applied*, vol. 17, no. 3, p. 034071, 2022.

[23] N. K. Panigrahy, P. Dhara, D. Towsley, S. Guha, and L. Tassiulas, "Optimal entanglement distribution using satellite based quantum networks," in *IEEE INFOCOM Workshops*, 2022.

[24] "MODTRAN®." http://modtran.spectral.com/.

[25] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Inf*, vol. 7, no. 3, 2021.

[26] "Visual Crossing: Weather Data & API, Global Forecast & History Data." https://www.visualcrossing.com/weather-data.

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

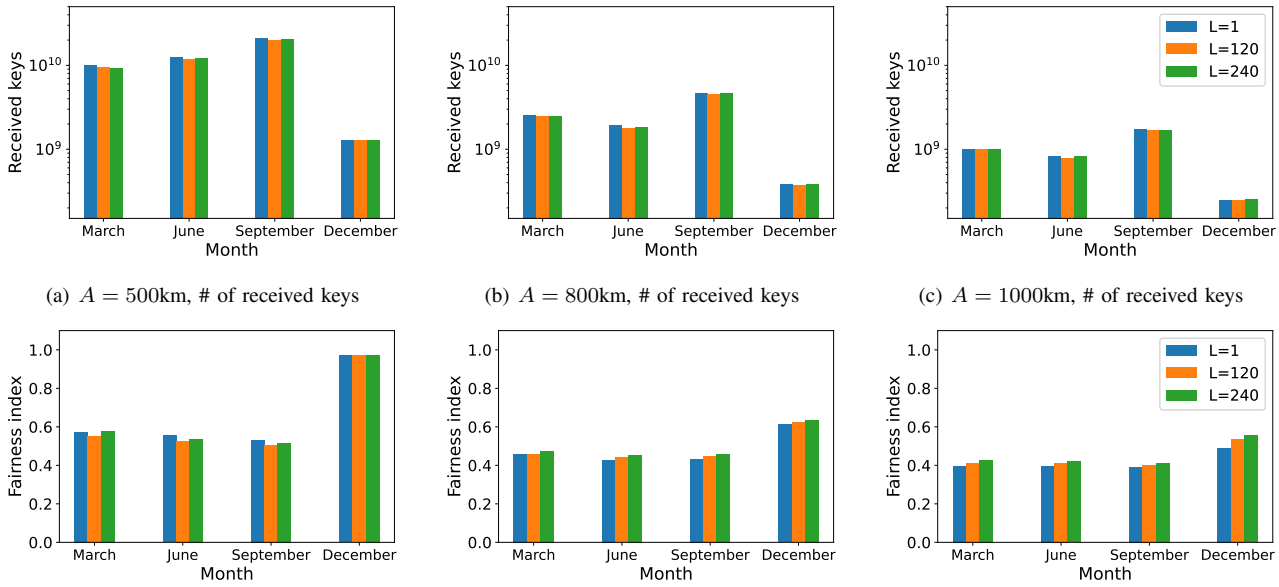
[28] "CPLEX." https://www.ibm.com/products/ilog-cplex-optimization-studio.

[29] L. de Forges de Parny, O. Alibart, J. Debaud, S. Gressani, A. Lagarrigue, A. Martin, A. Metrat, M. Schiavon, T. Troisi, E. Diamanti, P. Gélard, E. Kerstel, S. Tanzilli, and M. Van Den Bossche, "Satellite-based quantum information networks: use cases, architecture, and roadmap," *Communications Physics*, vol. 6, no. 1, pp. 1–17, 2023.

[30] C. Y. Lu, Y. Cao, C. Z. Peng, and J. W. Pan, "Micius quantum experiments in space," *Reviews of Modern Physics*, vol. 94, no. 3, 2022.

[31] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, D. K. Oi, and M. Krutzik, "Proposal for space-borne quantum memories for global quantum networking," *npj Quantum Information*, vol. 7, no. 1, pp. 1–11, 2021.

[32] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, "Finite key effects in satellite quantum key distribution," *npj Quantum Information*, vol. 8, no. 1, 2022.



(a) $A = 500$km, # of received keys (b) $A = 800$km, # of received keys (c) $A = 1000$km, # of received keys

(d) $A = 500$km, fairness index (e) $A = 800$km, fairness index (f) $A = 1000$km, fairness index

Fig. 7. Impact of window size on performance in window-based max-min strategy; L varies from 1 to 240 slots.