Qiskit-Based Simulation of HAP-Enabled Multi-User Entanglement QKD over FSO Channels

Yuma Kaminaga, Hoang D. Le, Cuong T. Nguyen, and Anh T. Pham
Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan

Abstract—In this paper, we propose and simulate a high-altitude platform (HAP)-based quantum key distribution (QKD) network architecture using free-space optics (FSO) links to enable one-to-many key generation. The quantum key exchange is based on the entanglement-based BBM92 protocol, integrated with a time division multiple access (TDMA) scheme to efficiently manage multi-user communication. To evaluate the performance and feasibility of the proposed system, we develop a simulation framework using Qiskit that incorporates a realistic FSO quantum channel model, taking into account key physical factors such as atmospheric attenuation, beam divergence, misalignment, and turbulence. Using this framework, we analyze the system's performance in terms of the achievable secret key rate (SKR) under various conditions. Our simulation results show a high degree of consistency with the theoretical models, confirming both the validity of our approach and the accuracy of the simulation environment. These findings confirm the potential of HAP-based QKD systems for secure, scalable quantum communications.

Index Terms—Free-space optics (FSO), quantum key distribution (QKD), high-altitude platforms (HAP), BBM92, multiple users, Qiskit.

I. Introduction

With the rapid growth of the Internet of Things (IoT), a wide range of devices, from smartphones and tablets to distributed sensor networks, are now interconnected, raising significant security concerns. However, due to their diverse operating environments and resource constraints, such as processing power, traditional security approaches may be insufficient. Furthermore, the development of quantum computers poses a risk of compromising current cryptographic technologies in the future. In this context, quantum key distribution (QKD) has emerged as a promising candidate for future-proof information-theoretically secure communication. It is a technology that applies the fundamental principles of quantum mechanics to enable the generation and sharing of secret keys between legitimate parties, guaranteeing security even in the presence of a powerful eavesdropper. Despite its potential, integrating QKD into IoT systems presents substantial challenges, primarily due to hardware and scalability limitations.

To overcome these barriers, prior research, such as [1], proposed the use of unmanned aerial vehicles (UAVs) for QKD key distribution. In this approach, UAVs serve as physical carriers of quantum keys, and it is assumed that there exist optical fiber links between the central server and various gateway nodes (GNs). This assumption becomes infeasible in geographically remote or difficult-to-access areas (e.g., mountainous regions or islands), where laying and maintaining optical fiber infrastructure is costly and impractical.

To address this limitation, our study proposes a free-space optics (FSO)-based QKD network architecture using high-altitude platforms (HAPs) as an alternative to fiber-optic links. HAPs, which operate in the stratosphere at altitudes around 20 km, offer several advantages over satellite-based systems. Due to their proximity to the Earth's surface, HAPs exhibit lower latency, reduced transmission losses, and improved link stability—critical properties for real-time communication. Moreover, HAPs are more cost-effective to deploy and maintain compared to satellites, which require expensive rocket launches and challenging spaceborne maintenance [2].

Several previous studies have explored HAP-based QKD systems [2]–[5], typically adopting a prepare-and-measure protocol (e.g., BB84) where the HAP acts as a relay between the ground node and a trusted network. However, such architectures often involve multiple sequential key distribution steps and increased system complexity, reducing overall efficiency. In contrast, the scheme proposed in this study utilizes entanglement-based QKD (BBM92 protocol) for key generation. In this setup, the HAP functions as a central entangled photon source, simultaneously distributing entangled photon pairs to multiple ground-based users. This one-to-many transmission capability reduces the need for intermediate trusted nodes and significantly improves scalability and system performance.

The motivation for this study is that the limitations of fiber-based QKD, which lack the flexibility, scalability, and cost-efficiency required for global or large-scale IoT deployment. In contrast, HAP-based FSO QKD systems offer secure, high-capacity communication across diverse and remote environments. A key challenge is efficiently distributing keys to a large number of GNs within the network, which is essential for scalable IoT security. To address this, the study proposes an HAP-based FSO architecture, develops a Qiskit-based simulation framework with realistic FSO quantum channel models to evaluate system performance, especially in terms of the achievable secret key rate (SKR), and designs a time-division multiple access (TDMA)-compatible, entanglement-based QKD protocol supporting multiple users.

II. System Description

A. System Model

Figure 1 depicts the system model, where a central server (Alice) aims to establish secret keys with N gateway nodes, denoted as Bob_i, for $i \in [1, N]$. To achieve that, the system employs (1) the BBM92 protocol [6] for QKD between Alice
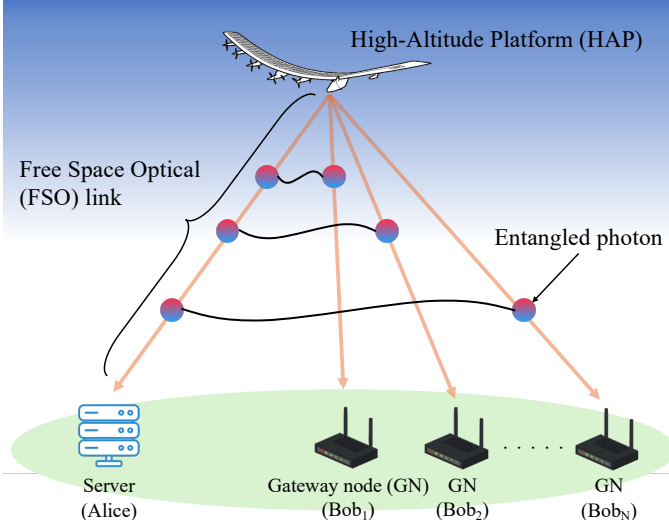
Fig. 1. The system model of HAP-aided FSO/QKD system for multiple users.

and each gateway node, using an HAP as a trusted relay to distribute entangled photon pairs; and (2) a TDMA scheme to coordinate the key distribution across the multiple gateway nodes. In the BBM92 protocol, the HAP first generates polarization-entangled photon pairs, with quantum states given by

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_\mathrm{A}|V\rangle_\mathrm{B} - |V\rangle_\mathrm{A}|H\rangle_\mathrm{B}\right), \quad (1)$$

where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization, respectively, and their subscript denote the recipient of the single photon. Then, one photon from the pair will be sent to Alice, and the other one will be transmitted to Bob_i via the FSO channels. If the photon can arrive at its corresponding user, it will be measured by a randomly selected basis, which is either a rectilinear or a diagonal one. After a period of time, both sides announce their time-tagged values of the received photon count and the corresponding choice of basis via a public channel. Based on that information, Alice and Bob_i will keep the bits with the same time-tagged values and measured by the same basis. Finally, both sides perform key reconciliation and privacy amplification on these bits to generate the secret key [7].

It is worth noting that an entangled photon pair can be shared only between Alice and a single gateway node at a time. To enable coordinated key distribution among multiple users, we adopt a TDMA scheme. In this approach, time is partitioned into fixed-duration timeslots, and each Bob is assigned specific timeslots during which they receive key materials. Fig. 2 describes an example of the TDMA scheme involving Alice and two gateway nodes, Bob_1 and Bob_2. As seen, Bob_1 is assigned the first and the third timeslots, while Bob_2 uses the second and the fourth. For this scheme, we assume perfect synchronization among entities, which is achieved by the global positioning system (GPS) [7].
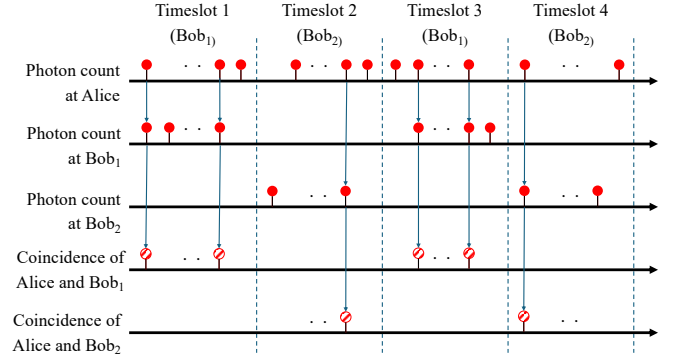

Fig. 2. Example of the TDMA scheme with Alice and two gateway nodes.

B. FSO Channel Model

We denote the transmittance of the quantum channel from the HAP to Alice/Bob_i as η_U, $U \in \{\mathrm{A}, \mathrm{B}_i\}$. This value can be formulated as $\eta_U = \eta_{\ell,U} I_{\mathrm{a},U} \eta_{\mathrm{p},U}$, where $\eta_{\ell,U}$ denote the atmospheric loss, $I_{\mathrm{a},U}$ denotes the random fluctuation due to atmospheric turbulence, and $\eta_{\mathrm{p},U}$ is the beam spreading loss and misalignment-induced fluctuations. *As for the atmospheric loss,* the value of $\eta_{\ell,U}$ can be computed as [5]

$$\eta_{\ell,U} = \tau_{\mathrm{zen},U}^{\sec(\xi_U)}, \quad (2)$$

where ξ_U denotes the zenith angle, and $\tau_{\mathrm{zen},U} \in [0,1]$ is the transmittance efficiency at $\xi_U = 0°$.

Regarding the atmospheric turbulence, we consider the log-normal distribution to model the random variable $I_{\mathrm{a},U}$ in weak turbulence condition. Therefore, the probability density function (PDF) of $I_{\mathrm{a},U}$ can be given as

$$f_{I_{\mathrm{a},U}}(I_{\mathrm{a},U}) = \frac{1}{I_{\mathrm{a},U}\sqrt{2\pi\sigma_{\mathrm{R},U}^2}} \exp\left[-\frac{\left(\ln I_{\mathrm{a},U} + \frac{\sigma_{\mathrm{R},U}^2}{2}\right)^2}{2\sigma_{\mathrm{R},U}^2}\right], \quad (3)$$

where $\sigma_{\mathrm{R},U}^2$ presents the Rytov variance, which can be calculated as

$$\sigma_{\mathrm{R},U}^2 = 2.25 k_{\mathrm{wave}}^{\frac{7}{6}} \sec^{\frac{11}{6}}(\xi) \int_{H_{\mathrm{g},U}}^{H_{\mathrm{atm}}} C_{\mathrm{n}}^2(h)(h - H_{\mathrm{g},U})^{5/6}\,\mathrm{d}h, \quad (4)$$

where $k_{\mathrm{wave}} = \frac{2\pi}{\lambda_{\mathrm{f}}}$ is the optical wave number, H_{atm} is the atmospheric altitude, $H_{\mathrm{g},U}$ is the altitude of the user U, λ_{f} denotes the optical wavelength, and $\sec(\cdot)$ is the secant function. In addition, $C_{\mathrm{n}}^2(h)$ is the refractive index structure parameter, and can be calculated as a function of the ground turbulence level $C_{\mathrm{n}}^2(0)$ and the root-mean-squared wind speed v_{wind} as in [5, (14)].

For the beam spreading loss and misalignment-induced fluctuations, we consider the four-parameter Beckmann distribution to model all cases of pointing errors. As a result, the PDF of $\eta_{\mathrm{p},U}$ can be expressed as [8]

$$f_{\eta_{\mathrm{p},U}}(\eta_{\mathrm{p},U}) = \frac{\varphi_{\mathrm{mod},U}^2}{A_{\mathrm{mod},U}^{\varphi_{\mathrm{mod},U}^2}} \eta_{\mathrm{p},U}^{\varphi_{\mathrm{mod},U}^2 - 1}, \quad (5)$$
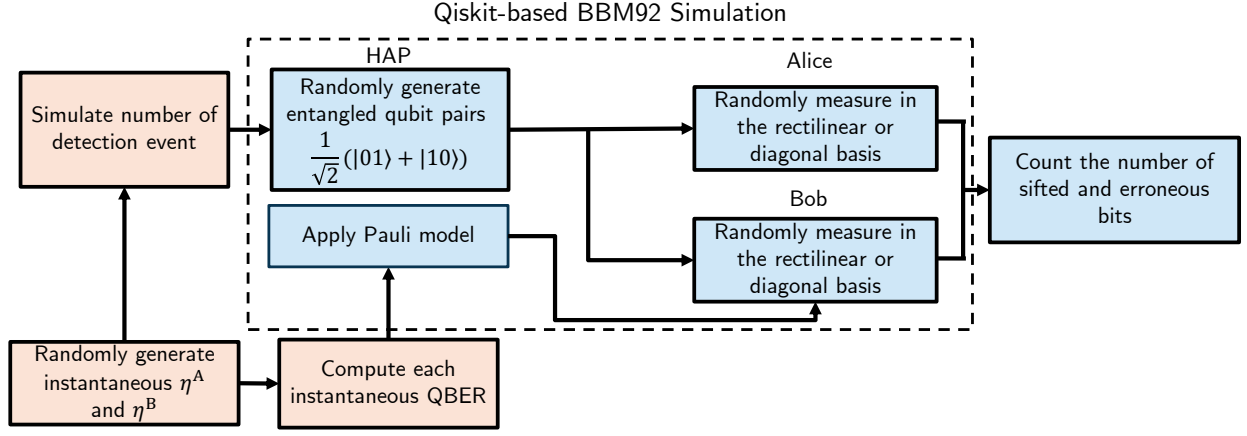
Fig. 3. Block diagram of the simulation framework with the Qiskit-enabled BBM92 simulation.

where $\varphi_{\mathrm{mod},U} = w_{L_{\mathrm{eq}},U}/2\sigma_{\mathrm{mod},U}$, $w_{L_{\mathrm{eq}},U}$ is the equivalent beam width of user U and can be computed as

$$w_{L_{\mathrm{eq}},U} = \sqrt{w_{L,U}^2 \frac{\sqrt{\pi}\mathrm{erf}\,(\nu_U)}{2\nu_U \exp\left(-\nu_U^2\right)}}, \qquad (6)$$

where $w_{L,U}$ is approximated as $w_{L,U} \simeq \theta_{\mathrm{div}}L_U$, $L_U = (H_{\mathrm{HAP}} - H_{\mathrm{g},U})\sec\left(\xi_U\right)$ is the slant distance of user U, H_{HAP} is the altitude of the HAP, θ_{div} is the beam divergence half-angle, $\nu_U = \frac{\sqrt{\pi}a_U}{\sqrt{2}w_{L,U}}$, and a_U is the aperture radius of user U. Additionally, $\sigma_{\mathrm{mod}} = \left(\frac{3\mu_{x,U}^2\sigma_{x,U}^4 + 3\mu_{y,U}^2\sigma_{y,U}^4 + \sigma_{x,U}^6 + \sigma_{y,U}^6}{2}\right)^{1/3}$ is the modified beam-jitter variance approximation, in which $\mu_{x,U},\mu_{y,U},\sigma_{x,U},\sigma_{y,U}$ are the means and the standard deviations of the Gaussian-distributed jitters along the x and y axes, respectively. Therein, $\sigma_{x,U}$ and $\sigma_{y,U}$ can be computed via the standard deviations of angle-jitter $\sigma_{\theta_{x,U}}$ and $\sigma_{\theta_{y,U}}$ as $\sigma_{x,U} \simeq L_U\sigma_{\theta_{x,U}}$ and $\sigma_{y,U} \simeq L_U\sigma_{\theta_{y,U}}$. Moreover, $A_{\mathrm{mod},U} = A_{0,U}G_U$, where $A_{0,U} = \left[\mathrm{erf}\,(\nu_U)\right]^2$ is the maximum transmittance if there is no misalignment, and G_U can be found in [8].

Combining all these factors, the PDF of η_U can be written as

$$
\begin{aligned}
f\left(\eta_U\right) = {} & \frac{\varphi_{\mathrm{mod},U}^2}{2\left(A_{\mathrm{mod},U}\eta_{\ell,U}\right)^{\varphi_{\mathrm{mod},U}^2}}\eta_U^{\varphi_{\mathrm{mod},U}^2-1} \\
& \times \mathrm{erfc}\left[\frac{\ln\left(\frac{\eta_U}{A_{\mathrm{mod},U}\eta_{\ell,U}}\right) + \chi_U}{\sqrt{2}\sigma_{\mathrm{R},U}}\right] \qquad (7) \\
& \times \exp\left[0.5\sigma_{\mathrm{R},U}^2\varphi_{\mathrm{mod},U}^2(1 + \varphi_{\mathrm{mod},U}^2)\right],
\end{aligned}
$$

where $\mathrm{erfc}(x)$ is the complementary error function, and $\chi_U = 0.5\sigma_{\mathrm{R},U}^2\left(1 + 2\varphi_{\mathrm{mod},U}^2\right)$.

III. QISKIT SIMULATION AND ANALYSIS

A. BBM92 Simulation with Qiskit

To evaluate the performance and feasibility of the proposed system, we develop a simulation platform incorporating the modelled quantum channel and a BBM92 protocol implementation enabled by Qiskit, as shown in Fig. 3. Qiskit is an open-source, Python-based software development kit (SDK) introduced by IBM for building and simulating quantum circuits. For each simulated channel coherence time, we generate two instantaneous transmittance values of η_{A} and η_{B_i}, sampled from the PDF given in Eq. (7). These values are then used to calculate the number of coincident detection events and the corresponding instantaneous QBER, which serves as inputs to the Qiskit-based BBM92 simulation.

In this work, we consider a type-II parametric down-conversion (PDC) source that can emit states containing multiple photon pairs. In particular, the probability that the source emits an n-photon-pair state is given by [9]

$$P\left(n\right) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \qquad (8)$$

Here $\lambda = \mu/2$, where μ is the average number of photon pairs generated per pump pulse [9]. Accordingly, the coincidence detection probability and error rate of n-photon-pair states are computed based on [9, (9)] and [9, (A6)], respectively. After simulating 10^6 channel coherence times, the total number of sifted bits and erroneous bits is used to compute the secret key rate, as described in the following section.

B. Theoretical Secret Key Rate

To assess the system's performance, we consider the secret key rate, which is defined as the average number of secure key bits that Alice/Bob$_i$ can generate per second via the quantum channels. Specifically, the secret key rate of Bob$_i$ can be expressed as

$$\mathrm{SKR}_{\mathrm{Bob}_i} = \frac{\mathcal{R}}{N}s\langle Q_{\lambda,i}\rangle\left[1 - (f+1)H_2\left(\langle E_{\lambda,i}\rangle\right)\right], \qquad (9)$$

where $\mathcal{R}$ is the repetition rate, s is the sifting coefficient, which equals 0.5 in case of the BBM92 protocol, f is the key reconciliation efficiency, and $H_2\left(\cdot\right)$ denotes the binary entropy function [9]. Additionally, $\langle Q_{\lambda,i}\rangle$ is the probability of
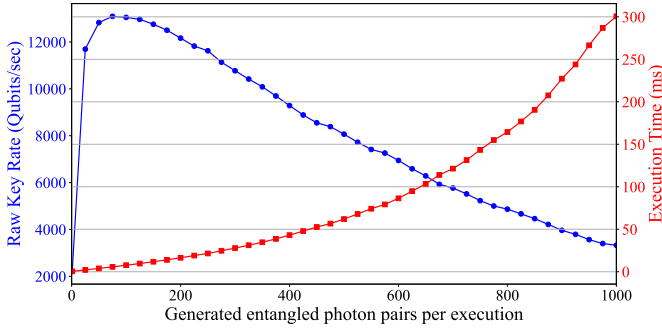
Fig. 4. Raw key rate and execution time of the Qiskit-based simulation versus the number of generated entangled photon pairs.

Fig. 5. Secret key rate versus the average number of generated photon pairs.

a coincident detection event between Alice and Bob_i, which can be calculated as

$$\langle Q_{\lambda,i}\rangle = \int_0^1 \int_0^1 Q_\lambda(\eta_\text{A}, \eta_{\text{B}_i}) f_{\eta_\text{A}}(\eta_\text{A}) f_{\eta_{\text{B}_i}}(\eta_{\text{B}_i}) \, d\eta_\text{A} d\eta_{\text{B}_i}, \tag{10}$$

where $Q_\lambda(\eta_\text{A}, \eta_{\text{B}_i})$ is the conditional coincident detection probability given the instantaneous values of η_A and η_{B_i}, and can be computed as [9]

$$Q_\lambda(\eta_\text{A}, \eta_{\text{B}_i}) = 1 - \frac{1 - Y_{0A}}{(1 + \eta_A\lambda)^2} - \frac{1 - Y_{0B_i}}{(1 + \eta_{B_i}\lambda)^2} + \frac{(1 - Y_{0A})(1 - Y_{0B_i})}{(1 + \eta_A\lambda + \eta_{B_i}\lambda - \eta_A\eta_{B_i}\lambda)^2}, \tag{11}$$

where Y_{0A} and Y_{0B_i} are the background count rates on Alice's and Bob_i's sides. Moreover, $\langle E_{\lambda,i}\rangle$ is the average quantum bit-error rate (QBER) and can be expressed as

$$\langle E_{\lambda,i}\rangle = \frac{\int_0^1 \int_0^1 E_\lambda Q_\lambda(\eta_\text{A}, \eta_{\text{B}_i}) f_{\eta_\text{A}}(\eta_\text{A}) f_{\eta_{\text{B}_i}}(\eta_{\text{B}_i}) d\eta_\text{A} d\eta_{\text{B}_i}}{\langle Q_{\lambda,i}\rangle}, \tag{12}$$

where $E_\lambda Q_\lambda(\eta_\text{A}, \eta_{\text{B}_i})$ is the erroneous detection probability per pulse conditional on the instantaneous values of η_A and η_{B_i}, and can be calculated as [9]

$$E_\lambda Q_\lambda(\eta_A, \eta_{B_i}) = e_0 Q_\lambda - \frac{2(e_0 - e_d)\eta_A\eta_{B_i}\lambda(1 + \lambda)}{(1 + \eta_A\lambda)(1 + \eta_{B_i}\lambda)(1 + \eta_A\lambda + \eta_{B_i}\lambda - \eta_A\eta_{B_i}\lambda)}, \tag{13}$$

where e_0 is the error rate from background counts(random noise), e_d is the intrinsic detector error. Finally, the secret key rate of Alice is given as

$$\text{SKR}_\text{Alice} = \sum_{i=1}^N \text{SKR}_{\text{Bob}_i}. \tag{14}$$

IV. RESULTS AND DISCUSSIONS

This section evaluates the performance of the proposed systems using both a theoretical framework and Qiskit-based simulations. The system parameters are as follows: aperture radius $a = 0.75$ m,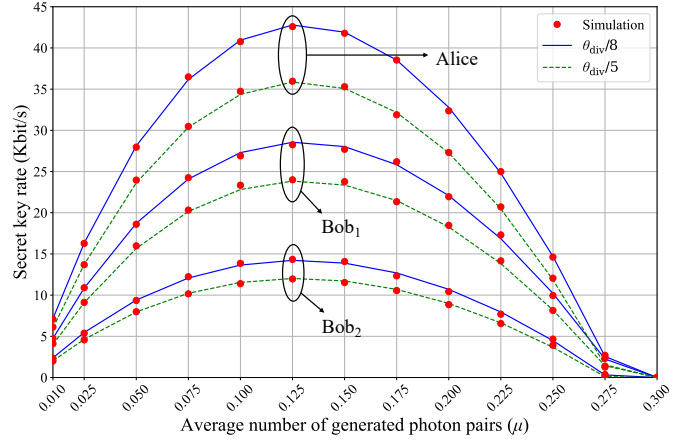 wavelength $\lambda_\text{f} = 0.85\mu$m, receiver altitude $H_{\text{g},U} = 10$ m, HAP altitude $H_\text{HAP} = 20$ km, atmospheric altitude $H_\text{atm} = 20$ km, beam divergence half-angle $\theta_\text{div} = 0.2$ mrad, wind speed $v_\text{wind} = 5$ m/s, ground turbulence level $C_\text{n}^2(0) = 10^{-13}\text{m}^{-2/3}$, means of horizontal and vertical jitters $\mu_{x,U} = \mu_{y,U} = 0$, key reconciliation efficiency $f = 1.1$, pulse repetition rate $\mathcal{R} = 10^9$ pulses/s, the background count rates on Alice's and Bob_i's sides $Y_{0A} = Y_{0B_i} = 10^{-5}$, the error rate from background counts $e_0 = 0.5$, the intrinsic detector error $e_d = 1\%$. Other parameters are similar to those in [9].

Fig. 4 shows the relationship between the number of entangled photon pairs generated per execution in the IQX simulator and the resulting raw key rate and execution time. The raw key rate, shown by the blue line, initially increases sharply with the number of photon pairs, peaking at approximately 13,000 qubits/sec when 75 photon pairs are generated. Beyond this point, the raw key rate begins to decline. Meanwhile, the execution time, indicated by the red line, increases steadily with the number of photon pairs. These results are crucial for assessing the efficiency of QKD protocols in the IQX environment. Selecting the optimal number of generated photon pairs is essential to maximizing the raw key rate.

Next, we simulate the SKR as a function of the average number of generated photon pairs with results shown in Fig. 5 for two pointing misalignment levels: $\theta_\text{div}/8$ and $\theta_\text{div}/5$. The simulation involves Alice and two receivers, Bob_1 and Bob_2, performing key distribution using the BBM92 protocol with TDMA. Alice is located at a zenith angle of 30 degrees, while Bob_1 is at 10 degrees, and Bob_2 is at 45 degrees. Each Bob is assigned specific timeslots in the TDMA scheme, and the SKR for Bob_1 and Bob_2 reflects the key rates from their individual links with Alice. Alice's SKR represents the total combined SKR of both Bobs.

As shown in Fig. 5, the SKR between Alice and each Bob exhibits a tendency: it increases with the average number of generated photon pairs μ, reaches an optimal point, and then gradually decreases. An optimal value of approximately $\mu = 0.125$ is consistently observed across all cases. The impact of pointing misalignment is clearly evident. Under
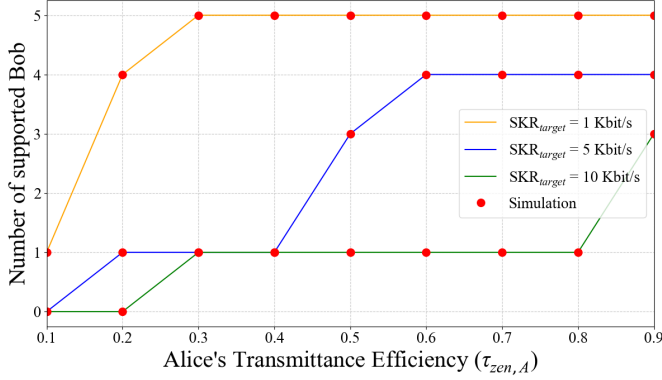
Fig. 6. Number of supported Bobs versus the transmittance efficiency.

the $\theta_{\mathrm{div}}/8$ condition, representing smaller angular deviations, higher SKRs are achieved across all scenarios compared to the larger misalignment condition of $\theta_{\mathrm{div}}/5$. This observation suggests that increased pointing errors directly reduce the photon reception efficiency. Additionally, the influence of the zenith angle on the SKR is apparent when comparing Bob_1 and Bob_2. Bob_1, positioned at a zenith angle of 10 degrees, consistently achieves higher SKRs than Bob_2, who is located at 45 degrees. This reduction in SKR with increasing zenith angle is attributed to greater atmospheric path loss, which diminishes the transmittance of the quantum channel. In all scenarios, the simulation results and the theoretical model show very close agreement. This strong agreement indicates that the proposed simulation model accurately captures the theoretical model, thus validating the precision of the simulation.

Fig. 6 investigates the effect of atmospheric transmittance efficiency on the number of supported gateways at a time. In this figure, we consider the scenarios where the HAP attempts to support five pairs of Alice and Bob. The zenith angles of Alice (ξ_A) and five Bob ($\xi_{B_i}, i \le 5$) is set as $30°, 10°, 20°, 30°, 40°, 50°$, respectively. The atmospheric transmittance for the Bobs was held constant at 0.91, and the average number of generated photon pairs is set as 0.125. Moreover, we define that a supported user is one who can achieve a target level of SKR, SKR_{target}. In this regard, we consider three target levels of SKR, i.e., 1 Kbit/s, 5 Kbit/s, and 10 Kbit/s. The results show that, across all three target SKR levels, an improvement in Alice's transmittance efficiency leads to an increase in the number of supported Bobs. In particular, when the target SKR is 1 Kbit/s, an increase of $\tau_{\mathrm{zen, A}}$ from 0.1 to 0.3 results in a sharp rise in the number of supported Bobs, from one to the maximum of five. This is because a high value of transmittance efficiency results in a high coincident detection probability. Moreover, as the required SKR increases, a higher $\tau_{\mathrm{zen, A}}$ is necessary. In the case of the highest target SKR of 10 Kbit/s, no Bob can be supported under conditions where $\tau_{\mathrm{zen, A}} \le 0.2$. Only when

$\tau_{\mathrm{zen, A}}$ reaches 0.3 does it become possible to support a single Bob, and supporting three Bobs requires an extremely high transmittance of $\tau_{\mathrm{zen, A}} = 0.9$.

V. CONCLUSIONS

We proposed and evaluated a HAP-based QKD network designed for scalable one-to-many key generation over FSO communication links. The system architecture employs the entanglement-based BBM92 protocol integrated with a TDMA scheme to support multiple ground nodes efficiently. To assess the feasibility and performance of the proposed approach, we developed a robust Qiskit-based simulation framework that incorporates a realistic FSO quantum channel model, capturing critical physical factors such as atmospheric attenuation, turbulence, and beam divergence. Simulation results revealed a strong correlation with theoretical performance predictions, particularly in terms of the SKR under various realistic FSO conditions. This consistency confirms the validity of both our system model and the underlying simulation framework.

REFERENCES

[1] P.-Y. Kong, "UAV-assisted quantum key distribution for secure communications with resource limited devices," *IEEE Trans. Veh. Technol.*, vol. 73, no. 8, pp. 11 923–11 933, Aug. 2024.

[2] Y. Chu, R. Donaldson, R. Kumar, and D. Grace, "Feasibility of quantum key distribution from high altitude platforms," *Quantum Sci. Technol.*, vol. 6, no. 3, p. 035009, Jun. 2021.

[3] M. Q. Vu, T. V. Pham, N. T. Dang, and A. T. Pham, "Design and performance of relay-assisted satellite free-space optical quantum key distribution systems," *IEEE Access*, vol. 8, pp. 122 498–122 510, Jul. 2020.

[4] N. Alshaer and T. Ismail, "Exploring quantum key distribution for secure communication in high-altitude platforms," in *Proc. 24th Int. Conf. Transp. Opt. Netw. Conf.*, 2024, pp. 1–5.

[5] P. V. Trinh, S. Sugiura, C. Xu, and L. Hanzo, "Optical RISs improve the secret key rate of free-space QKD in HAP-to-UAV scenarios," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 8, pp. 2747–2764, Aug. 2025.

[6] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557, Feb. 1992.

[7] M. Q. Vu, H. D. L, T. V. Pham, and A. T. Pham, "Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/direct detection," *IEEE Access*, vol. 10, pp. 113 260–113 274, Oct. 2022.

[8] P. V. Trinh *et al.*, "Statistical verifications and deep-learning predictions for satellite-to-ground quantum atmospheric channels," *Commun. Phys.*, vol. 5, no. 1, p. 225, Sept. 2022.

[9] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, no. 1, p. 012307, Jul. 2007.