2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)
31 July – 2 August 2025, Rangpur, Bangladesh

Greedy Optimization for Enhancing Satellite-Based Quantum Key Distribution Performance

Asif Akhtab Ronggon[1], Tuhin Hossain[2]
[1]Department of Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology
Dhaka, 1000, Bangladesh
[2]Department of Computer Science and Engineering, Jahangirnagar University
Savar, 1342, Bangladesh
Email: [1]asifaftab172@gmail.com, [2]tuhin97.hossain@gmail.com

***Abstract*—Quantum Key Distribution (QKD) is a fundamental technology to ensure secure communication between distant points on the Earth, leveraging the principles of quantum mechanics (QM) to provide an unconditionally secure method for distributing cryptographic keys. In this paper, we investigate the optimization of QKD systems in low Earth orbit (LEO) through a simulation-based approach, utilizing a Greedy Optimization Agent (GOA) that dynamically adjusts key system parameters in response to changing atmospheric and orbital conditions. The agent adjusts the beam pointing, transmission loss, and coherence factors to maximize the quantum key rate while accounting for signal degradation due to atmospheric turbulence and misalignment. The experimental results demonstrate that the optimization of the QKD system significantly outperforms the baseline system. The optimization system outperformed the baseline by 13.82%, with an average reward of 95.80 ± 72.63 compared to 84.07 ± 70.31. In the same way, there was a 13.22% rise in the average key rate, with the optimized system reaching 98.37 ± 71.80, rather than the baseline's 86.95 ± 69.52. In addition, the modified system significantly improved alignment by lowering the beam pointing error from 0.0456 in the baseline to 0.0170. These findings confirm that real-time dynamic adjustment is an effective strategy for improving the performance of satellite-based quantum communication systems.**

***Index Terms*—Quantum Cryptography, Quantum key distribution (QKD), Dynamic parameter adjustment, Greedy optimization agent (GOA), Quantum key rate, Satellite-based quantum communication.**

I. Introduction

Quantum cryptography ensures secure information processing through the use of quantum physics principles. Future applications will rely on it because, in the face of emerging quantum technology, it guarantees a level of protection not feasible with standard cryptographic methods. Conventional cryptographic methods are vulnerable to prospective advancements in quantum computing, as they rely on mathematical problems that quantum algorithms could resolve easily. When it comes to communication security, quantum cryptography, QKD, provides an unparalleled level of protection that classical systems simply cannot. QKD protocols, such as BB84 [1] and E91 [2], utilize quantum entanglement and the no-cloning theorem to detect eavesdropping and guarantee the confidentiality of the exchanged keys. With the advent of quantum networks and the development of quantum computers, the importance of QKD has grown exponentially as it provides the only known method of encryption that is theoretically invulnerable to computational attacks.

Traditional terrestrial QKD systems, based on fiber-optic cables, are limited by the distance over which secure keys can be distributed. In wide-coverage networks, fiber-optic QKD is difficult to use and extend due to signal attenuation and loss from long distances and fiber failures. The lack of quantum repeaters, a technically challenging issue, limits QKD's practical range [3]. However, QKD systems operating from orbit have the potential to overcome the physical limitations of ground-based systems. Since LEO satellites operate very close to the Earth's surface, they can cover great distances with negligible delay, making them a great choice for foundation QKD systems. Their normal range is 500 to 2000 km. Carrying QKD on board LEO satellites enables a secure link between faraway earth stations and worldwide quantum communication networks. With low-latency and high-throughput LEO satellites, quantum cryptography technology can finally find a home in the world's communication networks.

However, satellite QKD transmission has considerable challenges. Turbulence, absorption, and scattering are environmental phenomena that significantly diminish the transmission of optical communication systems. Research suggests that variations in the integrity of optical free-space communication channels are mostly caused by air turbulence [4]. A number of factors, including the satellite's velocity in relation to the ground station, tracking device aiming errors, and beam misalignment, may reduce the signal intensity and increase the probability of significant errors. Therefore, optimization will be required to resolve these problems and keep QKD operating correctly. Precise beam aiming is essential for satellite-based QKD since satellite movement and air disturbances may result in signal degradation [5]. Recent research has focused on greedy algorithms and machine learning (ML) methods to increase quantum key rate with low errors [5]. This technique enables real-time adjustments to transmission power, beam alignment, and other system parameters. In some cases, greedy algorithms optimize well. It focuses on local minima and settles for suboptimal global solutions. It suggests a viable method of controlling QKD systems in real time when computing capabilities are limited [3]. The greedy method improves how dynamic QKD systems work by constantly correcting

979-8-3315-9694-1/25/$31.00 ©2025 IEEE

aiming errors, lowering transmission losses, and changing coherence factors. The study contributions listed below are:

- This paper presents a GOA-based optimized QKD system that can modify critical system parameters depending on orbital and atmospheric conditions.
- It focuses on improving quantum key rates, reducing errors, and enhancing system efficiency by adjusting parameters like beam pointing and transmission loss.
- The study highlights the importance of real-time dynamic adjustments to system parameters based on atmospheric and orbital changes.

After the study overview in Section 2, the methodology is elaborated in Section 3. Section 4 contains an in-depth assessment of the experimental findings and evaluation. Finally, Section 5 concludes the work by addressing its limitations and suggesting avenues for future research.

II. Literate Review

A machine learning-based method is suggested to create a real-time, ubiquitous detection tool for eavesdropping risks and device vulnerabilities. They created a comprehensive mathematical model of real-world QKD systems by considering device defects and potential eavesdropping attacks. To prove this, they employed the popular BB84 QKD time-bin phase-coding approach. Thereafter, they use ML approaches like the random forest algorithm to detect device faults and attacks in real time with 98% accuracy [6]. A different study introduced a deep learning-based detection method that is capable of successfully detecting denial-of-service attacks on the parameter estimation method of CVQKD. Before feeding the large amount of data into the suggested attack-aware neural network model, a set of feature vectors tagged by DoS attacks is constructed for training. According to simulated results, the trained AMM-CNN model can identify DoS attacks in a CVQKD system with 98.7% accuracy using a single forward propagation computation process in a complicated communication environment [7]. Another study examined an ANN-based CVQKD quantum defensive mechanism. They developed feature vectors identified by attack categories as inputs to an ANN model after considering how existing attack techniques affect signal and LO pulse measurable attributes. The focus is on three homodyne detection attacks on GMCS CVQKD, such as saturation, LO intensity, and calibration. They assessed performance using training and testing data based on realistic attack assumptions. Simulation results indicate that their trained ANN model can automatically detect and categorize most known attacks, with up to 99% recall and precision, while lowering transmission distance and secret keys [8]. IoT and encryption key theft were examined in a separate study on QKD. They propose a QKD architecture for networks beyond 5G IoT that incorporates train network sensors and offloads computationally heavy tasks to IoT controllers. They suggested an NN-based attacker detection mechanism for QKD without disrupting key distribution. The approach successfully identifies attackers 99% of the time [9]. A separate study examined how ML could improve QKD protocol security, robustness, and efficiency. Their deep learning-based approach improves photon polarization states and boosts key generation. They detect and prevent eavesdropping attempts via unsupervised learning, increasing quantum communications security while considering the BB84 protocol. Their ML-enhanced technology speeds communications by 25%. Since its anomaly detection methods are better, it detects suspicious activity 7.8% more effectively. Besides a 30% increase in system resilience, this system reduces errors in transmitting quantum bits by 33.3%, where overall system efficiency is 8.2% greater [10]. AI doorkeepers and QKD were used in another study to identify quantum channel eavesdropping. They propose an LSTM-based RNN and an SVM-based doorkeeper to secure the BB84 protocol. Each doorkeeper detects eavesdropping well. The trained models can detect security breaches perfectly on QKD nodes running the same application without interrupting the data flow between the server and IoT devices [11].This technique offered QML algorithms for QKD protocol applications. They developed and investigated the QML challenge to optimize eavesdropping attacks on quantum circuits in the BB84 protocol. Along with optimization, their methods explicitly express attacks as quantum circuits, providing a structured framework for analyzing QKD. Their research demonstrated a collective attack using normal data from QKD post-processing in quantum machine learning (QML). The new cloning method outperforms the old ones in noisy settings [12]. Another work proposed a channel-amplification physical attack for optical fiber CV-QKD. They created a decision tree classifier model that uses LO intensity to differentiate CA and DoS attacks on the channel. Finding channel tampering attacks makes CV-QKD better, and using ML classification to choose quantum data helps improve the security key rates (SKRs) that were attacked [13]. ML-driven QKD protocol improvements were proposed in another study to improve efficiency and security. Adaptive, entanglement-based, and hybrid methods will be tested under varying key lengths, noise levels, and channel stability. ML models will leverage ensemble learning methods like Random Forest and XGBoost. The adaptive protocol had an accuracy of 0.80 for a 2500-bit key, compared to 0.24 and 0.26 for the entanglement-based and hybrid protocols, respectively. In terms of detection probability, they find that the adaptive protocol is the best option, with 0.84 to 0.85 and 0.43 to 0.45 for eavesdropping [14]. A subsequent study used a robust and stable four-photon entanglement generator to show Third-Man Quantum Cryptography (TQC) and Quantum Secret Sharing (QSS). Entangled GHZ states can be generated, requiring teamwork during key reconstruction in QSS and allowing a third party to produce keys in TQC without knowing the messages. Their secure key sharing reduced errors by 0.35% using error correction. The experiment proved that multi-party quantum communication is possible and that secure communication can be controlled without compromising privacy using entanglement [15]. Realistic QKD is presented in another research

investigation. This approach facilitates safe key creation with 27.6% bit error rates, enhancing error tolerance. With adaptive privacy amplification and two-way classical communication, the system builds on six-state QKD. The combination of entanglement purification and majority-vote error correction enhances error tolerance without quantum computing. Their approach is more durable than standard BB84 systems, making QKD perform in noisy conditions much better [16]. One more study used ML to optimize twin-field quantum key distribution (TF-QKD) parameters to outperform local search. They test BPNN, RBFNN, and GRNN to predict the best intensities and probabilities in symmetric and asymmetric TF-QKD. Their results indicated that the neural networks can reduce calculation time without compromising accuracy. While BPNN is faster and real-time, RBFNN is the most accurate model. This method makes TF-QKD deployment simple and flexible [17]. This article discusses why the BB84 QKD system uses quantum error-correcting codes, notably CSS codes, and entanglement purification for security. By correcting quantum noise and eavesdropping errors, these systems let Alice and Bob safely exchange keys. The authors guarantee a high-fidelity and interference-resistant protocol by purifying entanglement. Using CSS codes, which make earlier proofs easier, is a useful and efficient way to communicate securely using quantum computers without quantum computation [18].The paper enhances quantum network authentication with post-quantum cryptography (PQC) and QKD. It addresses pre-shared symmetric key restrictions with the Aigis-Sig lattice-based digital signature system. By giving each user one digital certificate for safe authentication, this system simplifies key management and improves scalability and security. In the context of future quantum-safe communication networks, the utilization of PQC for authentication offers a quantum-resistant solution [19]. For secure communication, the paper introduces QKD and quantum coin tossing using quantum mechanics' uncertainty principle. It shows how polarized photons can distribute random keys across users to detect eavesdropping due to transmission disturbance. The paper also provides a quantum coin-tossing system that maintains fairness even against unlimited computing power opponents. Using quantum cryptography to create safe ways to communicate that can't be broken by normal cryptography threats is also shown in this paper [20].

III. Methodology

The current research analyzes the optimization of QKD in LEO utilizing a simulation-based strategy, employing GOA for dynamic system parameter adaptation. In order to accomplish its goal of improving key rate output, this agent makes use of transmission loss, beam aiming inaccuracy, and adjustment of coherence parameters. It takes into account external factors, including air conditions, satellite motion, and beam misalignment. The workflow architecture of our suggested solution is shown in Figure 3.

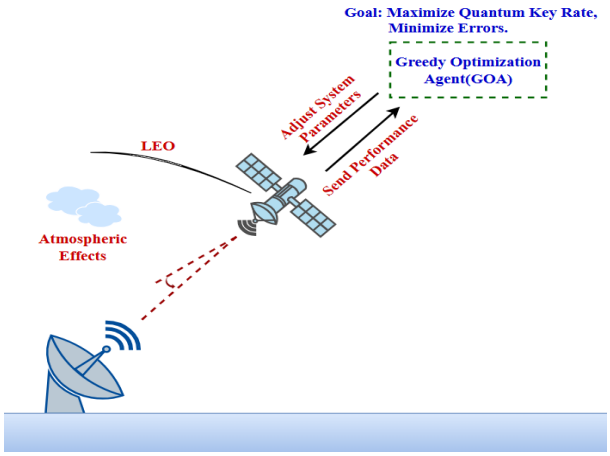

Fig. 1: Workflow architecture.

A. System Model

A LEO satellite communication system is studied in which air loss, beam misalignment, and weather are among the variables impacting quantum communication. We will presume that the satellite has a 90-minute orbital period, is 1000 km above the ground surface, and travels at the speed $v = 7340$ m/s. The next parts provide a detailed discussion about the model's stochastic and deterministic components.

B. Atmospheric and Channel Models

The communication channel undergoes attenuation as a result of atmospheric effects that encompass Rayleigh scattering, aerosol scattering, and atmospheric turbulence. The total transmission loss L_{trans} at a given time t is modeled as:

$$L_{\text{trans}} = \alpha \exp\left(\beta \frac{d(t)}{10000}\right)(1 + \text{Turbulence}) + \text{Rayleigh} + \text{Aerosol} \quad (1)$$

where α and β are atmospheric loss constants typically derived from empirical measurements [4], and $d(t)$ is the path length between the transmitter and receiver, where the path loss model can be founded [21]. Also, the Rayleigh scattering component and aerosol scattering component depend on the distance and atmospheric conditions (via weather).

For the weather conditions, we model a diurnal and seasonal variation in atmospheric turbulence. The function is defined as:

$$w(t) = 0.6 \cdot \sin\left(\frac{2\pi t}{86400}\right) + 0.3 \cdot \sin\left(\frac{2\pi t}{365 \times 86400}\right) + \epsilon \quad (2)$$

Where ϵ is a random fluctuation representing unpredictable weather, and the diurnal and seasonal cycles follow patterns observed in meteorological models [22].

C. Satellite and Orbital Dynamics

The satellite's position in its orbit is described using Keplerian mechanics. Given the orbital period T_{orb} and eccentricity e, the orbital position $P(t)$ of the satellite at any time t can be

calculated from the semi-major axis a and eccentric anomaly $E(t)$:

$$P(t) = a\,(1 - e\cos(E(t))) \tag{3}$$

where $E(t)$ is derived from the mean anomaly $M(t)$, which is given by:

$$M(t) = \frac{2\pi t}{T_{\text{orb}}} \tag{4}$$

and $E(t)$ is obtained numerically through the Kepler equation:

$$E(t) = M(t) + e\sin(E(t)) \tag{5}$$

This orbital model is derived from Kepler's Laws of Planetary Motion and is extensively utilized in satellite communication models [23].

The zenith angle $\theta(t)$ and beam pointing error $\varepsilon(t)$ are modeled to account for misalignments due to thermal effects and orbital dynamics:

$$\begin{aligned}\theta(t) &= 0.2\sin\left(\frac{2\pi t}{T_{\text{orb}}}\right) + 0.1\\ \varepsilon(t) &= \text{periodic error} + \text{random error} + \text{thermal drift}\end{aligned} \tag{6}$$

These factors impact the route length $d(t)$, which is utilized to determine the transmission loss and communication quality.

D. Quantum Key Rate and Error Rate Models

The quantum key rate R_{key} serves as a critical metric for assessing the performance of the quantum communication channel. The outcome is contingent upon the quality factor $\mathcal{Q}$, which includes the influences of distance attenuation, beam misalignment, weather conditions, and quantum coherence. The quality factor is calculated as:

$$\begin{aligned}\mathcal{Q} = \frac{1}{1 + \left(\frac{d(t)}{5000}\right)^2} \cdot \exp(-\gamma\varepsilon(t)^2)\\ \cdot \exp(-w(t) \cdot \text{Turbulence}) \cdot \text{Coherence} \cdot \text{Efficiency}\end{aligned} \tag{7}$$

where γ is the beam misalignment error factor, derived from optical communication models [24], and $w(t)$ is the weather condition based on meteorological data [22]).

The error rate e_λ for the communication channel, including misalignment, turbulence, and detector errors, is modeled as:

$$\begin{aligned}e_\lambda = \text{detector error} + \text{misalignment error} + \text{turbulence error}\\ + \text{decoherence error} + \text{timing jitter}\end{aligned} \tag{8}$$

where, as often occurs in real-life quantum communication contexts [3], each error component is weighted correctly and the overall error is clipped between 0.01 and 0.5.

Finally, the quantum key rate is given by:

$$\begin{aligned}R_{\text{key}} = q \cdot \mathcal{Q} \cdot \text{sifting factor} \cdot (1 - \text{error correction})\\ - \text{privacy amplification}\end{aligned} \tag{9}$$

where q is the quantum bit rate, error correction and privacy amplification are efficiency terms affecting the rate for QKD protocols [1].

E. Reward Calculation for Optimization

A reward function is defined to direct the agent's decision-making procedure, which incorporates the quantum key rate along with different costs. Coherence, transmission loss, error rate, and beam-directing inaccuracy are all factors that go into these expenses. The reward function is as follows:

$$\begin{aligned}\text{reward} = R_{\text{key}} - \lambda \cdot (L_{\text{trans}} + E_{\text{error}} + S_{\text{steering}})\\ - C_{\text{coherence}}\end{aligned} \tag{10}$$

where L_{trans} is the transmission loss, E_{error} is the error cost, S_{steering} is the steering cost, and $C_{\text{coherence}}$ is the coherence cost. The parameter λ is a scaling factor that adjusts the importance of cost components [3].

F. Optimization Agent

The greedy agent in this study considers all of its options before deciding how to respond in order to maximize the reward function. The agent picks the action that maximizes reward by meticulously examining a spectrum of alternative actions that modify the system's beam aiming inaccuracy, coherence factor, and transmission loss.

Taking into account the current condition, the greedy agent determines the best action a^* from a discrete action space:

$$a^* = \arg\max_a \text{reward}(s'|s, a) \tag{11}$$

The current state is denoted by s while the new state, created by action a, is shown by s'. The agent takes action to modify the system parameters, which enhances the quantum key rate while decreasing errors and losses.

IV. Results Analysis

Detailed outcomes from the GOA simulation of QKD-related low-Earth orbit satellite systems will be discussed in this section of the research. The baseline system, which did not undergo any dynamic parameter changes, was used to evaluate the GOA. The two systems were tested with key performance indicators including reward, quantum key rate, transmission loss, beam aiming inaccuracy, and coherence factor. We conducted statistical significance tests to look at how reliable the stated benefits were.

A. Performance Comparison: Optimized vs. Baseline

Table I highlights the main performance benchmarks for the GOA and the baseline system. The 13.82% increase in reward and 13.22% increase in key rate shown by the optimal system over the baseline indicate that the real-time corrections performed by the GOA greatly improve the system's efficiency. The reason for these enhancements is that the GOA can adjust the coherence factor, transmission loss, and beam focusing to suit dynamic circumstances.

TABLE I: Performance metrics for Greedy Optimization and Baseline systems. The optimized system yields significant improvements in both reward and key rate.

Metric	Greedy Optimization	Baseline
Average Reward	95.80 ± 72.63	84.07 ± 70.31
Average Key Rate	98.37 ± 71.80	86.95 ± 69.52
Reward Improvement	13.82%	N/A
Key Rate Improvement	13.22%	N/A

B. Statistical Significance

Using t-tests on key rate indicators and incentive measures, we were able to confirm that the enhancements were solid. The observed improvements in performance are confirmed to be statistically significant and not due to random fluctuations, since the p-values for both measures are substantially under the 0.05 threshold. Specifically-
- Reward p-value: 0.000236 and
- Key Rate p-value: 0.000244

These findings provide credence to the idea that dynamic parameter modification might be useful in real-time environments, as the GOA considerably improves the QKD system's performance.

C. Key Rate and System Efficiency

The quantum key rate is a crucial measure of QKD system performance, directly affecting the efficiency of secure key generation. As shown in Figure 2, the optimized system consistently achieves higher key rates compared to the baseline. The maximum key rate achieved by the optimized system was 223.87 bits/s, compared to 176.32 bits/s for the baseline system, demonstrating the effective optimization of the QKD system.

D. Beam Pointing Error and Transmission Loss

Figures 3 and 4 display the significant improvements in beam pointing error and transmission loss achieved by the GOA. The optimized system reduced the beam pointing error to 0.0170, compared to 0.0456 for the baseline. Similarly, the optimized system minimized transmission loss by dynamically adjusting system parameters in response to orbital and atmospheric changes, leading to more stable and efficient communication.

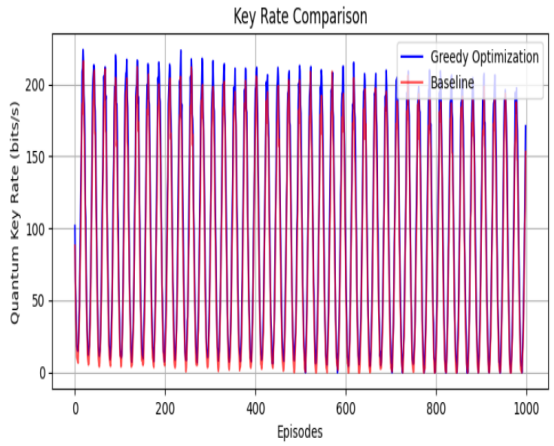

Fig. 2: Key rate comparison between Greedy Optimization and Baseline. The optimized system outperforms the baseline in key rate generation.

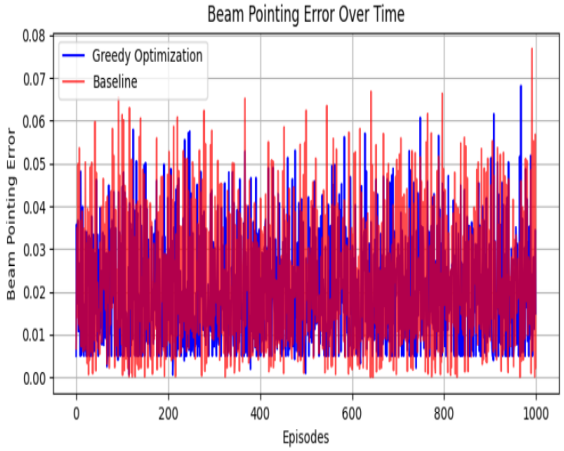

Fig. 3: Beam-pointing error comparison between greedy optimization and baseline. The optimized system reduces beam misalignment, improving performance.

E. Coherence Factor

The coherence factor is a critical parameter for quantum systems, as it indicates the level of quantum coherence maintained during transmission. As illustrated in Figure 5, the optimized system maintains a coherence factor of 1.0000, ensuring better quantum state integrity and more secure key distribution. In contrast, the baseline system experiences a reduced coherence factor due to misalignments and environmental disturbances.

The findings indicate that the GOA significantly enhances the performance of satellite-based QKD systems. In comparison to the baseline, the enhanced system demonstrates reduced error rates, superior quantum key rates, and increased overall system efficiency. The t-tests indicate that these enhancements statistically substantiate the robustness of the optimization method. The findings indicate that real-time dynamic parameter adaptation greatly enhances the effectiveness of satellite-based quantum communication systems, positioning the GOA

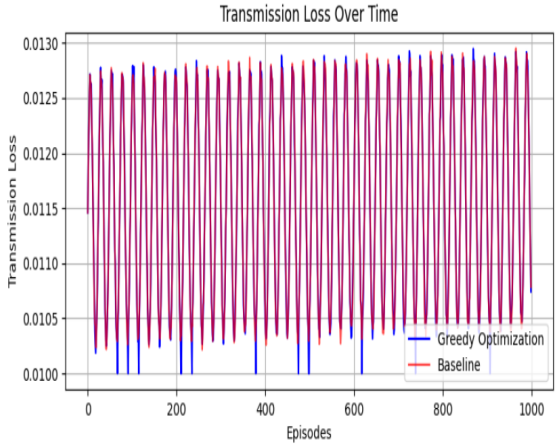

Fig. 4: Transmission loss comparison between Greedy Optimization and Baseline. The optimized system achieves lower transmission loss.

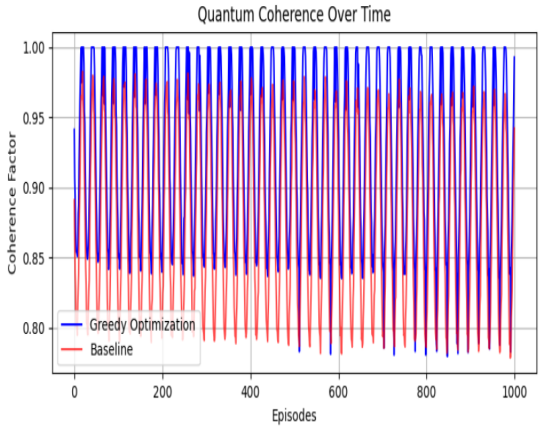

Fig. 5: Coherence factor comparison between Greedy Optimization and Baseline. The optimized system maintains better coherence, ensuring more secure key distribution.

as a viable strategy for future QKD deployments.

V. Conclusion and Future Work

The QKD approach serves as a tool for secure key exchange in quantum cryptography that works across an unsecured channel. To improve QKD systems utilizing satellites, this study presents a new approach based on the GOA. By adjusting critical parameters such as beam targeting, transmission loss, and coherence dynamically, the ideal system outperforms baseline models. Experimental results demonstrated that our proposed optimized system performs much better than the baseline, with the average reward improving by 13.82% and the average key rate increasing by 13.22%. Furthermore, the optimized system eliminated transmission loss and reduced beam directing error from 0.0456 to 0.0170, resulting in more robust and efficient communication. This leads to the best possible quantum key rates with the fewest possible errors. The findings suggest GOA-based optimization could be a promising method for satellite-based quantum communication systems.

Future research will investigate the incorporation of machine learning for optimization to augment system flexibility, enhance energy efficiency, and strengthen security protocols. The improvements in satellite quantum key distribution are projected to accelerate the creation of secure, long-distance communication networks, furthering the field of global quantum communication.

References

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

[2] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[3] S. Pirandola et al. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.

[4] T. S. Rappaport et al. Free-space optical communication: Propagation and system performance. *Proceedings of the IEEE*, 84(4):502–510, 1996.

[5] T. Zhang et al. Machine learning for quantum key distribution in space. *Quantum Information Processing*, 19:30, 2020.

[6] Jiaxin Xu, Xiao Ma, Jingyang Liu, Chunhui Zhang, Hongwei Li, Xingyu Zhou, and Qin Wang. Automatically identifying imperfections and attacks in practical quantum key distribution systems via machine learning. *Science China Information Sciences*, 67(10):202501, 2024.

[7] Wenhao Yin, Yuhan Zhou, and Duan Huang. Denial-of-service attack defense strategy for continuous variable quantum key distribution via deep learning. *Mathematics*, 11(12):2681, 2023.

[8] Yiyu Mao, Wenti Huang, Hai Zhong, Yijun Wang, Hao Qin, Ying Guo, and Duan Huang. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New Journal of Physics*, 22(8):083073, 2020.

[9] Hasan Abbas Al-Mohammed, Afnan Al-Ali, Elias Yaacoub, Khalid Abualsaud, and Tamer Khattab. Detecting attackers during quantum key distribution in iot networks using neural networks. In *2021 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2021.

[10] RM Bommi, M Nalini, N Vijayaraj, and A Mary Joy Kinol. Enhancing quantum key distribution protocols with machine learning techniques. In *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, pages 1–4. IEEE, 2023.

[11] Hilal Sultan Duranoglu Tunc, Yingjian Wang, Riccardo Bassoli, and Frank HP Fitzek. Machine learning based attack detection for quantum key distribution. In *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, pages 1–6. IEEE, 2023.

[12] T Decker, M Gallezot, SF Kerstan, A Paesano, A Ginter, and W Wormsbecher. Qkd as a quantum machine learning task. *arXiv preprint arXiv:2410.01904*, 2024.

[13] Sebastian P Kish, Chandra Thapa, Mikhael Sayat, Hajime Suzuki, Josef Pieprzyk, and Seyit Camtepe. Mitigation of channel tampering attacks in continuous-variable quantum key distribution. *Physical Review Research*, 6(2):023301, 2024.

[14] Naim Ajlouni, Abdelrahman Almassri, and Rasha Ragheb Atallah. Enhancing quantum key distribution efficiency and security. 2025.

[15] Yu-Ao Chen, An-Ning Zhang, Zhi Zhao, Xiao-Qi Zhou, Chao-Yang Lu, Cheng-Zhi Peng, Tao Yang, and Jian-Wei Pan. Experimental quantum secret sharing and third-man quantum cryptography. *Physical review letters*, 95(20):200502, 2005.

[16] Hoi Fung Chau. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Physical Review A*, 66(6):060302, 2002.

[17] Jia-Le Kang, Ming-Hui Zhang, Xiao-Peng Liu, and Jia-Hui Xie. Machine learning with neural networks for parameter optimization in twin-field quantum key distribution. *Quantum Information Processing*, 22(8):309, 2023.

[18] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[19] Liu-Jun Wang, Kai-Yi Zhang, Jia-Yong Wang, Jie Cheng, Yong-Hua Yang, Shi-Biao Tang, Di Yan, Yan-Lin Tang, Zhen Liu, Yu Yu, et al. Experimental authentication of quantum key distribution with post-quantum cryptography. *npj quantum information*, 7(1):67, 2021.

[20] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[21] M. Hata. Empirical formula for propagation loss in land mobile radio services. *IEEE Transactions on Vehicular Technology*, 29(3):317–325, 1980.

[22] A. Chandler et al. Meteorological data for atmospheric modeling. *Journal of Atmospheric and Solar-Terrestrial Physics*, 73(1):16–30, 2011.

[23] A. Bertin and F. Siffert. *Orbital Mechanics and Satellite Communications*. Springer, 2001.

[24] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.