IOP Publishing New J. Phys. 27 (2025) 043021 https://doi.org/10.1088/1367-2630/adce24

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
2 November 2024

REVISED
14 April 2025

ACCEPTED FOR PUBLICATION
17 April 2025

PUBLISHED
24 April 2025

PAPER

Machine learning for optimal parameter prediction in free space continuous-variable quantum key distribution

Dong Chen*, Cheng Jin, Liu Ao, Chen Lanjian, Chen YuJie, Yin Peng and Wu TianYi

Information and Communication College, National University of Defense Technology, Wuhan, People's Republic of China
* Author to whom any correspondence should be addressed.

E-mail: dongchengfkd@163.com

Keywords: continuous-variable quantum key distribution, parameter optimization, machine learning

Abstract

For a practical continuous-variable quantum key distribution (CV-QKD) system, the optimization of modulation variance is crucial for promoting protocol performance. The optimization relies on algorithms like local search in general. But the efficiency of local search methods is limited in low latency and limited computing power scenarios due to their high computational consumption. Hence, this optimization approach is infeasible for satellite-based CV-QKD due to satellites' low power feature. In this paper, a neural network model that directly predicting the optimal modulation variance in nearly real time is proposed for free space gaussian modulated CV-QKD protocols. This work enhances the feasibility of implementing CV-QKD in low-Earth-orbit satellite scenarios, where typical link durations of few seconds demand rapid parameter optimization. Moreover, a simulation platform for free space CV-QKD protocol, which employs the precise orbital model to extract the elevation angle and the transmission length, is designed and developed to generate training sets that make the neural network model more practical. Our work can be used as a foundation to support parameter prediction for future quantum communication satellite missions.

1. Introduction

Quantum key distribution (QKD) [1, 2], based on its security characteristics under the framework of quantum mechanics and information theory, can distribute security keys between two communication parties to achieve secure and confidential communication in the sense of information theory. Driven by the grand vision of an integrated quantum secure communication network, space quantum secure communication with high-stability and high-bit-rate under all-weather conditions has become a research hotspot in the field of quantum information.

Generally, QKD protocols can be divided into discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD) according to the information encoding method. According to the channel transmission medium, it can be classified as optical fiber channel and free space channel. The 'Micius' quantum science experiment satellite has verified the feasibility of satellite-to-ground DV-QKD, entanglement distribution and teleportation experiments [3–5], and the UAV QKD experiment has verified the feasibility of air-to-ground DV-QKD [6]. However, the feasibility research of free space CV-QKD is still in the preliminary stage of theoretical research and experimental exploration [7, 8]. Compared with the theoretical and experimental scheme of DV-QKD, which is composed of single photon quantum state, polarization/phase/orbital angular momentum modulation and single photon detection, CV-QKD protocol adopts Gaussian/discrete modulation of coherent optical quantum state and homodyne detection processing to transmit the key information. Coherent measurement of quantum states using homodyne or heterodyne detectors in fiber channel CV-QKD has demonstrated the ability to obtain higher security bit rates and greater compatibility with existing optical communication systems. Therefore, under the background of the gradual maturity of terrestrial fiber QKD technology and the success of space based DV-QKD experiment, the feasibility theory and experimental research of CV-QKD are explored by referring to the spatial DV-QKD

theory and experimental development path, which relying on the physical realization technology basis such as classical laser communication link and acquisition, tracking and aiming system.

Different from the relatively fixed transmission efficiency of fiber channel, the transmission efficiency of fading channel in free space not only changes dynamically with orbit altitude, elevation angle and the excess noise, but also is affected by random disturbance such as turbulence. Hence it is crucial to optimize the protocol parameters to fit the dynamical satellite-to-ground link. However, the limited access window time of the satellite-to-ground link is in conflict with the relatively long calculation time using the traditional global search or local search algorithm, which needs a high-efficiency parameter optimization method that can realize parameter optimization with faster computing speed and fewer computing resources.

As to our knowledge, machine learning methods are widely used to optimize parameters and channel compensation in QKD systems. Wang and Lo [9] presented a simple way to train a neural network that accurately and efficiently predicts the optimal parameters for a given QKD protocol, such as symmetric and asymmetric MDI-QKD, BB84, and TF-QKD. Liu *et al* [10] integrated machine learning to achieve an automatic parameter prediction for practical continuous-variable QKD by tuning the intensity of the LO pulse with feedback which is obtained via machine learning. Liu *et al* [11] developed a neural network model combined with Bayesian optimization to directly extract key rates with high reliability, considerable tightness and great efficiency. Jin *et al* [12] proposed key-sifting algorithms for CV-QKD protocol using a machine-learning framework based on the isolation forest to provide better feasibility in noisy environments. Liao *et al* [13] proposed a multi-label learning-based scheme to predict the unknown signal state for discretely-modulated CVQKD. Mao *et al* [14] introduced and experimentally addressed a quantum attack defense strategy for CV-QKD protocols by using artificial neural network. However, an implementation of machine learning is even more urgent for free space CV-QKD where fast and accurate parameter optimization based on a changing environment in real time is a difficult task on low-power platforms. Long *et al* [15] proposed a convolutional neural network for estimating phase corrections for an real local oscillator by using only intensity measurements for satellite-to-ground CV-QKD.

In this paper, we present a neural network model for free space Gaussian-modulated CV-QKD protocols directly to predict the optimal modulation variance in nearly real time. A ResNet-18 network [16] framework is used to replace the convolutional layer with a fully connected layer in this paper. This enables efficient training of deeper networks while leveraging residual learning, thereby maintaining high accuracy and stability. Moreover, a simulation platform for free space CV-QKD protocol, which employs the precise orbital model to extract the elevation angle and the transmission length, is designed and developed to generate training sets for the neural network model. Compared to the traditional local search algorithms, our method is more suitable for satellite-to-ground communication scenarios, where only have an access duration window of a few seconds to implement key distribution. Our work can be used as a pathfinder to support parameter prediction for the selection of the future quantum communication satellite missions.

2. Methods

Fast and accurate parameter optimization in dynamic channel is challenging on low-power platforms like satellites. This paper proposes a neural network framework capable of predicting the optimal modulation variance V_A in nearly real time for free-space Gaussian-modulated CV-QKD. In this section, we systematically describe the neural network architecture, dataset generation methodology, and training the neural network specifically designed for free-space Gaussian modulation of CV-QKD. Figure 1 illustrates the framework of the parameter optimization in satellite-to-ground CV-QKD based on machine learning. The Alice locates on satellite to generate coherent optical quantum states and chooses the parameter optimized by machine learning. The Bob locates at the ground station to receive signals and performs measurements of quantum states to implement key distribution.

2.1. Design and training of network

In this section, we briefly describe the design and training process of the neural network used to predict the optimal parameters. The key rate calculation for CV-QKD is highly dependent on various system parameters. To optimize the modulation variance, other parameters are categorized into experimentally variable parameters and device-specific fixed parameters respectively. The variable parameters set $\vec{s}$ (H, R, θ, ξ) comprises four dynamic variables: quantum channel excess noise (ξ), satellite orbital altitude (H), real-time slant range (R) representing the instantaneous satellite-to-ground distance, and zenith angle (θ) characterizing the geometric relationship between satellite terminal and ground station. The fixed parameters denoted as, include the receiver telescope size a, the beam spot size w_0, the detector efficiency η, the electronic noise v_{el}, and the reconciliation efficiency β. We demonstrate the feasibility of employing the neural network to find the optimal parameters of $V_{A\,\mathrm{opt}}(\vec{s})$ based on any input $\vec{s}$ and P_{fix} here. The

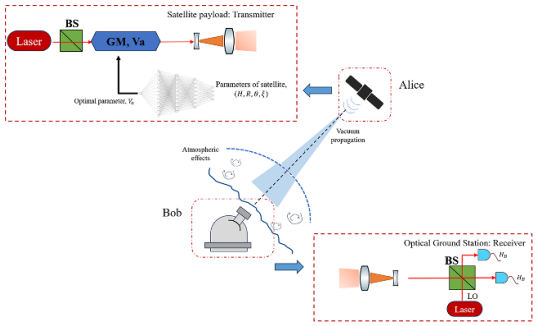


Figure 1. The framework of the optimal parameter prediction in satellite-to-ground CV-QKD base on machine learning. Main parameters include the orbital altitude (H), the real-time distance (L) between the ground station (Bob) and the satellite (Alice), and the zenith angle (θ) between them, as well as the excess noise (ξ) in the channel. The system incorporates a local oscillator (LO), the beam splitter (BS), the Gaussian modulator GM, and heterodyne detector.

relationship among $V_{A\text{opt}}(\vec{s})$, $\vec{s}$ and P_{fix} is discussed in appendix A.1. In this study, we develop a model named the ResFCN18 neural network to predict the optimal modulation variance, which combines the benefits of fully connected layers with the residual learning capabilities. Fully connected layers in the network offer the flexibility to accommodate various input and output configurations, effectively mapping the relationships between the experimental and optimal parameters. The residual module based on the ResNet18 mitigates vanishing gradients and network degradation in deeper architectures. This model receives the experimental parameters $\vec{s}$ at the input layer, while the hidden layers extract and process the underlying features. Finally, the output layer predicts the optimal modulation variance V_A. Additionally, techniques like batch normalization are employed to stabilize and accelerate training. The activation function ReLU [17] introduces non-linearity into the network, enabling it to learn complex patterns more effectively and helping to address the vanishing gradient problem.

Figure 2 illustrates the architecture of the ResFCN18 neural network model. The input layer consists of four neurons to receive the experimental parameters $\vec{s}$ and the output layer with a single neuron produces the predicted modulation variance V_A. The core of the network is a fully connected structure that incorporates multiple residual blocks, which enhance the network's ability to learn complex mappings between the input and output layers. The ResFCN18 is divided into two components: the main block and the residual block as depicted in figures 2(a) and (b). The main block is structured as a fully connected neural network with a residual framework, comprising four stages of residual blocks that contain 64, 128, 256, and 512 neurons, respectively. Each stage includes two residual blocks, and each residual block is made up of two fully connected layers. Due to a data size mismatches between residual blocks at different levels, a resized fully connected network layer is employed to ensure proper alignment. The last output fully connected layer maps the features to the target dimension. Each fully connected layer within the residual block is followed by batch normalization and a ReLU activation function. The mean squared error (MSE) is chosen as the cost function for the optimization of network weights, which is described in more detail in appendix A.2.

2.2. Dataset generation

To obtain more realistic satellite-to-ground communication data and enhance the model's practical applicability, we develop a simulation platform for the free-space CV-QKD based on the satellite tool kit (STK) software. More implementation details are listed in appendix B. Datasets for network training are generated through simulation platform aforementioned. A dataset around 10 000 samples is generated for parameters $(H,\ R,\ \theta)$, where H ranges from 400 to 800, R spans 400×10^3 to 2000×10^3, and θ covers 10° to 90°. Each $(H,\ R,\ \theta)$ combination was subsequently augmented with 12 distinct random noise components ξ $(0.01 \leqslant \xi \leqslant 0.03)$, ultimately yielding a comprehensive dataset of 126 575 samples containing $\vec{s}(H, R, \theta, \xi)$ quadruples.

We set the values of the fixed parameters P_{fix} in the satellite-to-ground CV-QKD protocol based on realistic experimental data. These include the receiver telescope size $a = 1.2\,\text{m}$ [18], the beam spot size $w_0 = 0.2\,\text{m}$, the detector efficiency $\eta = 0.4$, the electronic noise $v_{\text{el}} = 0.1$ $S.N.U.$, and the reconciliation efficiency $\beta = 0.96$ [19].

Here, we choose the no-switching Gaussian-modulated CV-QKD [20] as the representative protocol used by Alice and Bob. At the same time, we employ the free-space channel model with the weak turbulence assumption established in [21] to simulate the satellite-to-ground communication links. The turbulence refractive index structure constant of the weak turbulence is $C_n^2 \leqslant 10^{-15}\,\text{m}^{-\frac{2}{3}}$. Its affect on the variance of the

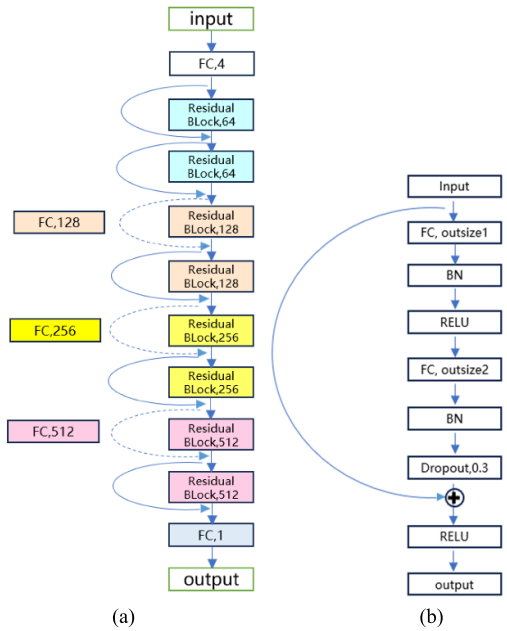


Figure 2. The ResFCN18 network layer architecture, where the input layer was used to receive the experimental parameter $\vec{s}(H,R,\theta,\xi)$, the residual block is used to extract the feature information of $\vec{s}$, and the output layer is used to predict the optimal modulation variance $V_{A\text{opt}}$. (a) The main block contains a fully connected neural network with a residual structure; (b) the residual block contains two fully connected layers, each of layers is followed by batch normalization and ReLU activation functions.

beam center is $\sigma^2 \approx 1.919 C_n^2 R^3 (2w_0)^{-\frac{1}{3}}$. According to this protocol and channel model, we can calculate the key rate under any set of parameters $\vec{s}(H,R,\theta,\xi)$.

The maximal key rate under the same set of $\vec{s}$ corresponds to the optimal V_A. Since the optimal V_A is the label of a $\vec{s}$ set, we search the maximal key rates of all $\vec{s}$ sets by local search algorithm [22] to determine the labels $V_{A\text{opt}}(\vec{s})$ for them.

To further optimize the input of the neural network, the parameters $\vec{s}$ are normalized by setting:

$$s_1 = \frac{H}{100},\ s_2 = \frac{R}{10^6},\ s_3 = \theta \times \frac{\pi}{180^\circ},\ s_4 = -\log_{10}(\xi). \tag{1}$$

Following normalization, the parameters s_1, s_2, s_3, and s_4 are constrained to the ranges $[4,\ 8]$, $[0.4,\ 2]$, $[0.06,\ 1.57]$, and $[1.52,\ 2]$ respectively. The normalization of the parameters reduces the impact of outliers and stabilizes the variance across the dataset. This pre-processing step enables the model to effectively capture the underlying relationships within the data, while maintaining the intrinsic characteristics of the experimental data. The output parameters for the optimal modulation variance fall within the range $(0,\ 4)$, which is of the same order of magnitude as the normalized data.

Finally, we generate 126 575 sets of normalized data with corresponding labels. Five percent of the dataset is allocated as the validation set and the remainder comprises the training set. The dataset generation utilized over 2300 core hours on a computer equipped with a 13th Gen Intel(R) Core (TM) i9-13900HX processor. Although the phase of data generation and model training is time-intensive, such efforts are performed offline. Once training is completed, the model can efficiently process data in real-time. The trained network can be deployed into the hardware system, achieving rapid online computation of datasets on the millisecond scale.

3. Numerical results

The training details of ResFCN18 are elaborated in appendix A3. After training is completed, the trained network is applied to the satellite-to-ground CV-QKD to assess its performance in predicting the optimal modulation variance using test data. In figure 3(a), the red points represent the $V_{A\text{opt}}$ values computed via the local search algorithm, while the green points correspond to the $V_{A\text{pred}}$ values predicted by the ResFCN18 network. The test sets $V_{A\text{opt}}$ and $V_{A\text{pred}}$ values are predominantly concentrated within the 0.5–2 range. The close alignment of the green points with the red points indicates good agreement between the neural network's predictions and the local search outcomes. To further assess the performance of the neural

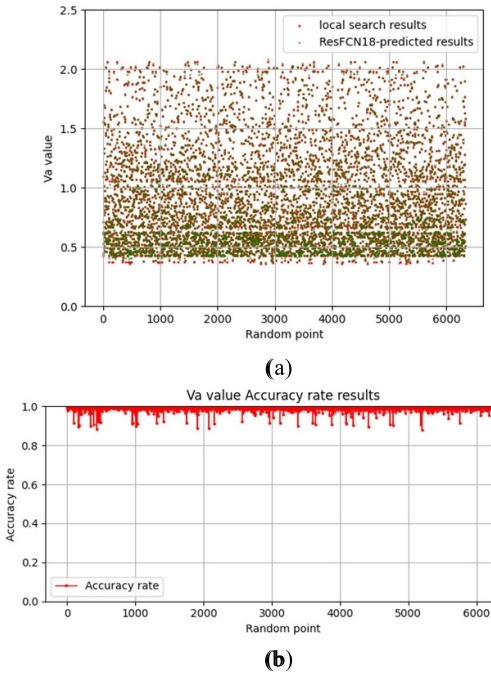


Figure 3. The results of testing data using the ResFCN18 network for no-switching CV-QKD protocols in satellite-to-ground communication systems are shown. (a) The red and green scatter points in the chart represent the results obtained via a local search algorithm and the neural network, respectively. (b) The accuracy rate of the neural network's predicted $V_{A\text{pred}}$ values compared to those calculated by the local search algorithm.

network, the accuracy rate is calculated by comparing the predicted parameter $V_{A\text{pred}}$ with the optimal parameter using the formula $1-\left|V_{A\text{pred}}-V_{A\text{opt}}\right|/V_{A\text{opt}}$. As shown in figure 3(b), the optimal and average accuracy rates are approximately 99.7% and 99.54% for the modulation variance respectively and the standard deviation is around 0.008 564 across all test points. This high accuracy rate demonstrates the model's ability to generate highly precise predictions for the majority of the test data.

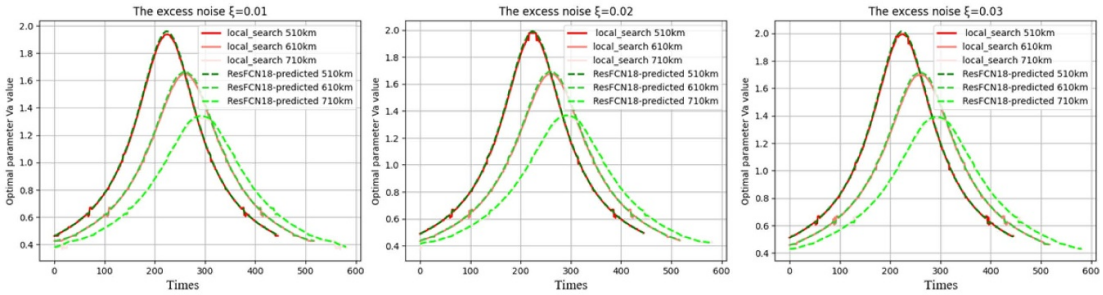
Additionally, the performance comparison between the ResFCN18 network and the local search algorithm is presented on four datasets. The test data containing 6328 sets is randomly selected from the sample sets. Test datasets Orbit1, Orbit2, and Orbit3 are generated from three different satellite orbit altitudes (510 km, 610 km, 710 km). All three datasets comprise three data subsets corresponding to excess noise levels of 0.01, 0.02, and 0.03, respectively, while the fixed parameters remain unchanged. This comparison results of four datasets are recorded in table 1, where four datasets include 446, 518, 582, and 6328 sets, respectively. The mean accuracy of the neural network approach across all test sets is 99.54%, 99.39%, 99.23%, and 99.21%, demonstrating that the neural network effectively approximates the optimal solutions identified by the local search method.

Furthermore, the ResFCN18 network exhibits a significant reduction in computation time. When evaluated on the same test dataset, the neural network approach shows a remarkable improvement in efficiency, reducing computation time by approximately 3–4 orders of magnitude compared to the local search method. The local search approach takes 14 754.3 s to complete the analysis for the test data, whereas the ResFCN18 network only consumes 1.08 s, highlighting the substantial advantage of the neural network in computation efficiency. Similarly, for another three datasets, the ResFCN18 network consistently demonstrated superior computational efficiency. The computation times of the network are 0.508 s, 0.512 s, and 0.523 s for each dataset, respectively. In contrast, the local search approach required considerably longer times of 1031.4 s, 1185.5 s, and 1330.9 s for the corresponded datasets. This comparison outstands that the ResFCN18 network is much faster than the local search method in the parameter prediction of CV-QKD. High accuracy is also maintained across different orbital altitudes, providing reliable parameter estimates for varying conditions.

To demonstrate the validity of the neural network approach, the optimal parameter prediction results of the ResFCN18 network is compared with those of the local search method for different satellite orbital altitudes and excess noise levels. In figure 4, the x-axis represents the communication point sets for different satellite orbit altitudes of 510 km, 610 km, and 710 km, while the y-axis shows the optimal parameter V_A values. Each value i on the x-axis represents the ith set of parameters (R,θ) sampled at the corresponding orbital altitude. The data sampling interval is 1 s. Thus, the x-axis actually represents the communication

Table 1. The performance comparison between the ResFCN18 network and the local search algorithm. These sets include data from three different satellite orbit altitudes (510 km, 610 km, 710 km) and test data. Here, ξ is the excess noise in the communication channel, H is the satellite orbit altitudes, $a = 1.2$ m is the receiver telescope size, $w_0 = 0.2$ m is the beam spot size, $\eta = 0.4$ is the detector efficiency, $v_{el} = 0.1$ (S.N.U.) is the electronic noise, and $\beta = 0.96$ is the reconciliation efficiency.

Set	Method	ξ (S.N.U.)	H(km)	Size	Rate (%)	Times(s)
Test data	Local search	0.01–0.03	400–800	6328	99.54	14 754.3
Test data	ResFCN18	0.01–0.03	400–800	6328		1.08
Test orbit1	Local search	0.01, 0.02, 0.03	510	446	99.39	1031.4
Test orbit1	ResFCN18	0.01, 0.02, 0.03	510	446		0.508
Test orbit2	Local search	0.01, 0.02, 0.03	610	518	99.23	1185.5
Test orbit2	ResFCN18	0.01, 0.02, 0.03	610	518		0.512
Test orbit3	Local search	0.01, 0.02, 0.03	710	582	99.21	1330.9
Test orbit3	ResFCN18	0.01, 0.02, 0.03	710	582		0.523



(a) (b) (c)

Figure 4. This figure visually compares the optimal modulation variances predicted by the local search method and the ResFCN18 network approach for the satellite-to-ground CV-QKD. The green dotted line represents the $V_{A_{\text{pred}}}$ values predicted by the ResFCN18 network, while the red dotted line represents the $V_{A_{\text{opt}}}$ values determined by the local search method. The x-axis represents the communication time and the y-axis shows the optimal parameter V_A values. Figures (a)–(c) illustrate the impact of different levels of excess noise ξ in the communication channel, with values of 0.01, 0.02, and 0.03, respectively.

time. Figures 4(a)–(c) demon-states simulation results under successively increasing excess noise levels ($\xi = 0.01$, 0.02, and 0.03).

In figure 4, the green dotted line represents the $V_{A_{\text{pred}}}$ values predicted by the ResFCN18 network, while the red line represents the $V_{A_{\text{opt}}}$ values obtained through the local search method. The green and red curves exhibit a close overlap, demonstrating strong consistency between results of the two methods. The optimal modulation variance $V_{A_{\text{opt}}}$ decreases with increasing satellite orbit altitude. Specifically, under the excess noise of 0.01, the optimal modulation variance decreases from 1.95 to 1.33. This downward trend is also observed under the excess noise level of 0.02 and 0.03. As the satellite orbit altitude increases from 510 km to 710 km, the distribution range of $V_{A_{\text{opt}}}$ values becomes slightly narrower, suggesting that the best performance at lower satellite orbit altitudes should be achieved under a wider range of optimal parameters. In figures 4(a)–(c), the peak $V_{A_{\text{opt}}}$ values show slight variations depending on the excess noise level. Specifically, the optimal modulation variance $V_{A_{\text{opt}}}$ shows an increase with orbital altitude. It increases from 1.95 to 2.09 at the orbital altitude of 510 km; it rises from 1.65 to 1.71 at 610 km, and it goes from 1.34 to 1.39 at 710 km. These results confirm the excellent adaptability of the ResFCN18 network approach across different scenarios.

In the previous section, we demonstrated that the ResFCN18 network approach can be trained to accurately predict the optimal parameter function $V_{A_{\text{opt}}}(\vec{s})$ for the satellite-to-ground CV-QKD. In the satellite-to-ground CV-QKD, it is crucial to generate a sufficient number of secure keys within the communication window. As shown in figure 5, the key rates are derived from three different V_A values: the empirical V_A ($V_{A_{\text{emp}}} = 2$), V_{A} predicted by the ResFCN18 network ($V_{\text{A}_{\text{pred}}}$), and V_A computed by the local search method ($V_{\text{A}_{\text{opt}}}$). These are represented by the blue solid, green dashed, and red solid lines, respectively. The key rates based on the $V_{A_{\text{emp}}}$ parameter are relatively lower, particularly at the start and end of the communication session. In contrast, the key rates under the optimal $V_{\text{A}_{\text{pred}}}$ parameter are higher, particularly in the middle part of the communication window. Notably, the green dashed lines almost completely overlap with the red solid lines, indicating that the key rates predicted by the ResFCN18 network are nearly the same as those from the local search method ($V_{A_{\text{pred}}} \approx V_{A_{\text{opt}}}$). This demonstrates the high prediction accuracy of the ResFCN18 network in practical applications.

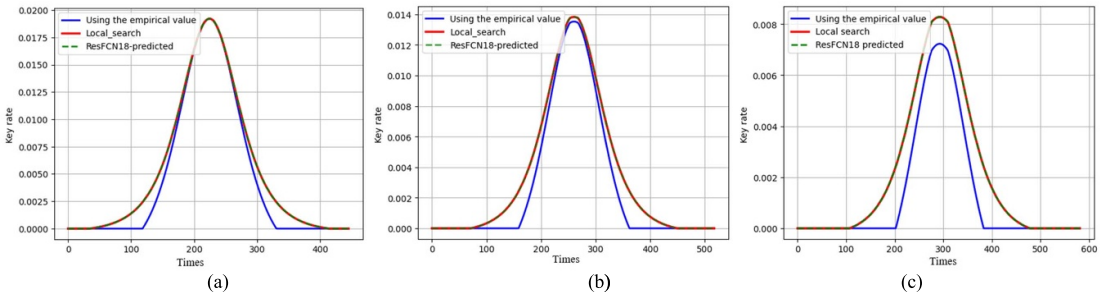


Figure 5. The results of the key rate comparison results under different satellite orbit altitudes when the excess noise is 0.01. The blue solid line represents the key rates calculated using the empirical $V_{A_{\text{emp}}}$, the red solid line represents the key rates under the local search found optimal value, and the green dashed line represent the key rates under the ResFCN18 network predicted $V_{A_{\text{pred}}}$. Figure (a)–(c) represent satellite orbit altitudes of 510 km, 610 km, and 710 km, respectively. The *x*-axis represents the communication time and the *y*-axis depicts the key rate, with higher values signifying more efficient key generation at that point.

In the satellite-to-ground CV-QKD, the duration of secure communication is associated with the quantity of secure keys generated, with longer durations resulting in more key generation. The key rate analysis in figures 5(a)–(c) reveals a significant enhancement in communication duration through optimized $V_{A_{\text{pred}}}$ parameters. At the orbital altitude of 510 km, the duration increases from 210 s ($V_{A_{\text{emp}}}$) to 378 s ($V_{A_{\text{pred}}}$), corresponding to a 168 s extension. This improvement becomes more substantial with increasing altitude: 176 s extension at 610 km (total 416 s) and 192 s extension at 710 km (total 468 s). Therefore, using the optimal $V_{A_{\text{pred}}}$ parameter has a significant impact on communication duration as the satellite's orbital altitude increases.

The key rate results at an orbital altitude of 510 km show a significant enhancement when the optimal modulation variance parameters V_{Apred} are used. Notably, the key rate demonstrates peak enhancements of 17.08 dB (average gain: 1.56 dB), with this improvement intensifying at elevated orbital altitudes. Specifically, maximum enhancements reach 22.43 dB (average: 1.89 dB) at 610 km and 15.89 dB (average: 2.5 dB) at 710 km. The simulation results demonstrate that employing the optimal modulation variance parameter V_{Apred} significantly affects communication duration and effectively improves the satellite-to-ground CV-QKD communication performance as the satellite orbit altitude increases. In contrast, the $V_{A_{\text{emp}}}$ parameter reduces communication efficiency and may degrade security or cause communication failure.

The ResFCN18 network approach has shown remarkable effectiveness in optimizing the modulation variance parameter $V_{A_{\text{pred}}}$. Compared with traditional local search algorithms, it improves computational speed by three to four orders of magnitude. This advancement enables the satellite-to-ground CV-QKD to leverage machine learning-assisted parameter tuning, thereby significantly optimizing the secret key rate.

4. Discussion

The dataset size is an important factor affecting the performance of neural networks. The training performance of the ResFCN18 across various dataset sizes is compared in appendix A.4. It reveals that once the training set size exceeds 100 000, the mean accuracy rate of the neural networks does not exhibit a significant increase. Therefore, training the neural network with 120 000 samples is deemed reasonable, as it strikes a balance between computational efficiency and model precision.

It is evident in figure 3(b), where most test points demonstrate high accuracy, yet certain data points remain relatively lower accuracy. The low accuracy of points may come from bad prediction of neural network due to rough model and poor data quality, or wrong calculation of the local search. Our accuracy may be improved further by improving neural network. In order to improve the performance of neural network, we can improve data quality through data preprocessing methods. We have performed data normalization in this work to make the neural network more stable. Data cleaning may be required if realistic satellite-to-ground data is available in future work.

Intending to implement proposed method on low-power platforms, we make a rough evaluation to illustrate the possible power consumption of our neural network. Since neural networks are calculated layer by layer, power may depend primarily on how many neurons (computing units) there are per layer on average. Wang and Lo [9], used 2 layers with an average of 300 neurons per layer and maximally 400 neurons in a single layer for calculation. The power deployed on the Raspberry Pi 3 is <5 W. Ignoring the jump structure, our neural network has 16 layers, with an average of 240 neurons per layer and maximally 512

neurons in a single layer. Therefore, the power is estimated to be only about 5 W, although the calculation time will be slightly increased.

In addition to power, two important indicators of predictive performance are accuracy and calculation time. For the trained neural network, the accuracy does not change with the platform. Due to the limitation of low-power platforms, the computation time will be extended. For instance, the computation time of the neural network in [9], has a computation time of 0.5–1 ms on the desktop and 3 ms on the Raspberry Pi 3. Our neural network takes about 1.3 ms to compute on the desktop, so even if deployed on a low-power platform, it should not require more than 10 ms of computation time. Hence, developed neural network here is promising in being deployed on low-power platforms without significant performance deterioration and relate experiments will be launched in the future.

5. Conclusion

In this paper we proposed a general approach for training neural networks to accurately and efficiently predict the optimal parameters of modulation variance for gaussian modulated satellite-to-ground CV-QKD protocol, which is applicable to general CV-QKD protocols, such as discrete modulation CV-QKD, CV-MDI-QKD etc.

Our approach can solve the optimal parameter optimization problem with low latency and limited computing power, which is more suitable for satellite-to-ground quantum protocols where only have an access duration window of few seconds to implement key distribution. Moreover, a simulation platform for satellite-to-ground CV-QKD protocol, which employs the precise orbital model to extract the elevation angle and the transmission length, is developed and designed to generate training sets to make the neural network model more practical.

Our results showed that the proposed approach could achieve three to four orders of magnitude faster optimization speed compared to traditional local search algorithm and the secret key rate of the satellite-to-ground CV-QKD protocol can be optimized by tuning the modulation variance V_A with feedback via machine learning.

The proposed method would reduce complexity and increase the feasibility of a global satellite-based CV-QKD protocol and would be used as a pathfinder to support parameter prediction involving as the selection of the future quantum communication satellite missions.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgment

This work is supported by the National Natural Science Foundation of Hubei Province.(No. 2024AFB991).

Appendix A

A.1. Parameters optimization analysis

To optimize the modulation variance V_A, other parameters are categorized into experimentally variable parameters $\vec{s}\,(H, R, \theta, \xi)$ and device-specific fixed parameters P_{fix}. Consequently, the CV-QKD key rate $\mathcal{R}$ can be expressed as:

$$\mathcal{R} = R\left(\vec{s}, V_A, P_{\text{fix}}\right). \tag{A1}$$

$\mathcal{R}$ is a function of the variable experimental parameters $\vec{s}$, the fixed experimental parameters P_{fix} and the parameters of modulation variance V_A, where the $\vec{s}$ is determined by the satellite-to-ground communication parameters and the V_A is determined by the user.

Given a set of experimental parameters $\vec{s}$ under fixed conditions P_{fix}, there exists an optimal modulation variance V_A that maximizes the key rate. The maximum key rate is denoted as:

$$R_{\max}\left(\vec{s}\right) = \max_{V_A \epsilon V} R\left(\vec{s}, V_A, P_{\text{fix}}\right). \tag{A2}$$

Hence, to determine the optimal modulation variance, V_A can be expressed as a function of $\vec{s}$:

$$V_{A_{opt}}\left(\vec{s}\right) = \underset{V_A \epsilon V}{argmax} R\left(\vec{s}, V_A, P_{fix}\right). \tag{A3}$$

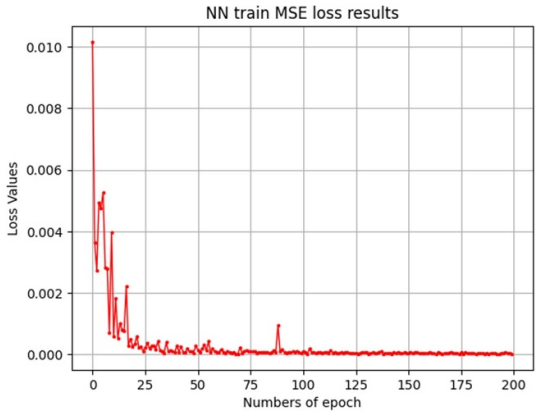


Figure A1. The results in the MSE loss throughout the 200 epochs of training for the ResFCN18 network is illustrated. The network was trained using the Adam optimizer with an initial learning rate of 0.001 over 200 epochs. As shown in the figure, the initial loss, approximately 0.01, quickly decreased to around 0.0002 and ultimately converged to a final value of 0.000025.

The relationship between $V_{A\mathrm{opt}}(\vec{s})$ and $R_{\max}$ is defined by the mathematical forms argmax and max, but $V_{A\mathrm{opt}}(\vec{s})$ cannot be obtained analytically. The optimal parameters are generally determined through local search algorithms, which perform extensive computations on the function $R(\vec{s}, V_A, P_{\mathrm{fix}})$ with different parameters value to locate the maximum value. However, the computational processes in this method are resource demanding and time-consuming for satellite-to-ground CV-QKD systems with constrained payload and power supply.

The universal approximation theorem for neural networks [23] guarantees that net architectures can approximate any continuous function on a defined domain, provided the network possesses adequate parameters and proper basis functions in its hidden layer. This fundamental theory enables our model to establish complex nonlinear mappings between time-varying channel parameters and optimal modulation variances. Therefore, this suggests that it might be possible to use a neural network to fully described the behavior of the aforementioned optimal parameter's function $V_{A\mathrm{opt}}(\vec{s})$. By inputting the parameters $\vec{s}$ and P_{fix}, the network can directly predict the optimal modulation variance V_A to calculate the corresponding key rate R. compared with the local search algorithms, this method avoids conducting numerous calculations on the function R across a range of parameter values to identify the maximum key rate. Meanwhile, the neural network computation method significantly reduces the computation time, which benefits real-time modulation variance optimization as the satellite-to-ground channel rapidly changes.

A.2. Cost function

MSE calculates the average of the squared differences between the predicted and actual values, thereby amplifying the impact of errors. This characteristic renders MSE particularly sensitive to outliers and large deviations in the prediction results. Due to its sensitivity, MSE is instrumental in training the model, as it emphasizes the minimization of significant errors, steering the model towards more accurate parameter optimization and enhancing its overall predictive performance. MSE can be expressed as:

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}\left(\hat{V}_{Ai} - V_{Ai}\right)^2. \tag{A4}$$

where N denotes the total count of samples, $\hat{V}_{Ai}$ refers to the predicted modulation variance for the ith sample as determined by the model and V_{Ai} is the actual modulation variance for the ith sample.

A.3 Training details of ResFCN18 neural network

The ResFCN18 network is trained for 200 epochs with the Adam optimizer [24], the initial learning rate is set to 0.001, and the batch size to 64. The whole train process takes roughly 40 min on an Nvidia GeForce RTX 4060 Laptop GPU 8G.

Figure A1 demonstrates the training results of the ResFCN18 network in the form of the MSE loss function values (The loss value reflects the discrepancy between the predicted and label values, with lower values indicating better model performance). During the first 25 epochs, the rapid drop in loss suggests that the model quickly learns the underlying features of the data, significantly reducing prediction error. As training continues, the rate of loss decrease slows, and the curve begins to level off, indicating that the model tends toward stability. From approximately the 175th epoch onward, the loss value fluctuates around

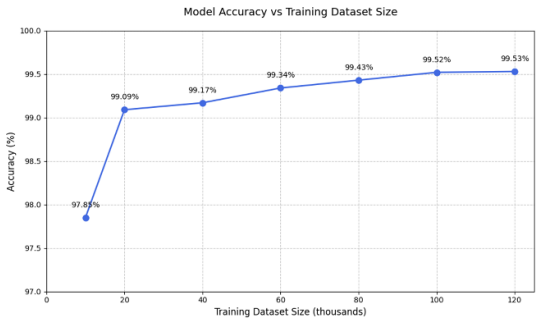


Figure A2. The figure demonstrates the relationship between the number of training samples and prediction accuracy.

0.000025, signifying that the model has effectively converged. Further training yields minimal improvement. The converged loss values demonstrate that the model possesses strong learning capabilities and is able to fit the training data effectively.

A.4. Performance of different dataset sizes

To examine the relationship between model accuracy and training dataset size, we train the ResFCN18 across various dataset sizes and present the results in figure A2.

The results show that accuracy improvements plateau beyond 100 000 samples. This observation is consistent with relevant literature, which indicates that datasets of approximately 10^5 samples are sufficient for training robust and efficient neural networks in quantum communication systems (e.g. [9, 11] use 4×10^5 and 7.7×10^5 samples, respectively).

Appendix B

The simulation scenarios are based on the communication between the Micius satellite and the Delingha ground station. The parameters of the Micius satellite are obtained from CelesTrak [25], as shown in table 2.

Table 2. The two-line element set (TLE) data from CelesTrak.

Parameter	Description	Value
Epoch	TLE epoch time	16 354.569
Inclination	Angle between the orbital plane and the equatorial plane (degrees)	97.3698°
Right ascension of ascending node	Longitude of the ascending node (degrees)	268.1064°
Eccentricity	Shape of the orbit (decimal point assumed)	0.001 3349
Argument of perigee	Angle between the ascending node and the perigee (degrees)	175.8929°
Mean anomaly	Position of the satellite in its orbit at the epoch (degrees)	309.019°

The parameters of the Delingha ground station we need include longitude and latitude (43°28′40.4976” N, 87°11′15.7518” E) and elevation (2050 m). We input these parameters into the STK simulation software and change the mean motion value (the number of orbits per day) to generate simulation scenarios for different satellite orbital altitudes ranging from 400 km to 800 km.

ORCID iD

Dong Chen https://orcid.org/0000-0003-2745-0258

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (*Bangalore, India*) pp 175–9
[2] Mayers D 2001 Unconditional security in quantum cryptography *J. ACM* **48** 351–406.2001
[3] Liao S K *et al* 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43
[4] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5
[5] Ren J G *et al* 2017 Ground-to-satellite quantum teleportation *Nature* **549** 70–73
[6] Dubey U *et al* 2023 A review on practical challenges of aerial quantum communication (arXiv:2309.13417)

[7] Villaseñor E, Malaney R, Mudge K A and Grant K J 2020 Atmospheric effects on satellite-to-ground quantum key distribution using coherent states *GLOBECOM 2020–2020 IEEE Global Communications Conf.* (IEEE) pp 1–6
[8] Harney C, Fletcher A I and Pirandola S 2022 End-to-end capacities of hybrid quantum networks *Phys. Rev. Appl.* **18** 014012
[9] Wang W and Lo H K 2019 Machine learning for optimal parameter prediction in quantum key distribution *Phys. Rev. A* **100** 062334
[10] Liu W, Huang P, Peng J, Fan J and Zeng G 2018 Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution *Phys. Rev. A* **97** 022316
[11] Liu Z P, Zhou M G, Liu W B, Li C-L, Gu J, Yin H-L and Chen Z-B 2022 Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution *Opt. Express* **30** 15024–36
[12] Jin D, Guo Y, Wang Y, Li Y and Huang D 2021 Key-sifting algorithms for continuous-variable quantum key distribution *Phys. Rev. A* **104** 012616
[13] Liao Q, Xiao G, Zhong H and Guo Y 2020 Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution *New J. Phys.* **22** 083086
[14] Mao Y, Huang W, Zhong H, Wang Y, Qin H, Guo Y and Huang D 2020 Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution *New J. Phys.* **22** 083073
[15] Long N K, Malaney R and Grant K J 2024 Phase correction using deep learning for satellite-to-ground CV-QKD *Proc. SPIE* **13106** 1310602
[16] He K, Zhang X, Ren S and Sun J 2016 Deep residual learning for image recognition *Proc. IEEE Conf. on Computer Vision and Pattern Recognition* pp 770–8
[17] Nair V and Hinton G E 2010 *Proc. 27th Int. Conf. on Machine Learning, Haifa, 2010* (*Omnipress, Madison*) pp 807–14
[18] Liao S K *et al* 2017 Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab *Chin. Phys. Lett.* **34** 090302
[19] Pirandola S 2021 Satellite quantum communications: fundamental bounds and practical security *Phys. Rev. Res.* **3** 023130
[20] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Quantum cryptography without switching *Phys. Rev. Lett.* **93** 170504
[21] Dequal D, Trigo Vidarte L, Roman Rodriguez V, Vallone G, Villoresi P, Leverrier A and Diamanti E 2021 Feasibility of satellite-to-ground continuous-variable quantum key distribution *npj Quantum Inf.* **7** 3
[22] Katoch S, Chauhan S S and Kumar V 2021 A review on genetic algorithm: past, present, and future *Multimedia Tools Appl.* **80** 8091–126
[23] Hornik K, Stinchcombe M and White H 1989 Multilayer feedforward networks are universal approximators *Neural Netw.* **2** 359
[24] Kingma D P and Ba J Adam: a method for stochastic optimization (arXiv:1412.6980)
[25] Kelso D T S 2008 CELESTRAK-TLE (available at: https://celestrak.com/)