ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 12 N. 1 (2023), e30240
eISSN: 2255-2863
DOI: https://doi.org/10.14201/adcaij.30240

A Framework for Improving the Performance of QKDN using Machine Learning Approach

Arthi R[a], Saravanan A[b], Nayana J S[c], and Chandresh MuthuKumaran[d]

[a,c,d] Faculty of Engineering and Technology, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India
[b] Department of Computer Science and Engineering, Easwari Engineering College, Ramapuram, Chennai, India
arthir2@srmist.edu.in, dean.academic@srmrmp.edu.in, nj1672@srmist.edu.in, cm7061@srmist.edu.in

KEYWORDS

Qubits; Quantum Layer; Machine Learning; Quantum Key Distribution Network (QKDN); Cryptography

ABSTRACT

A reliable secure communication can be given between two remote parties by key sharing, quantum key distribution (QKD) is widely concentrated as the information in QKD is safeguarded by the laws of quantum physics. There are many techniques that deal with quantum key distribution network (QKDN), however, only few of them use machine learning (ML) and soft computing techniques to improve QKDN. ML can analyze data and improve itself through model training without having to be programmed manually. There has been a lot of progress in both the hardware and software of ML technologies. Given ML's advantageous features, it can help improve and resolve issues in QKDN, facilitating its commercialization. The proposed work provides a detailed understanding of role of each layer of QKDN, addressing the limitations of each layer, and suggesting a framework to improve the performance metrics for various applications of QKDN by applying machine learning techniques, such as support vector machine and decision tree algorithms.

1. Introduction

Communication technology is an essential part of our daily lives. Today's communication technologies depend on the infrastructure of the high-speed optical fiber communication network (Spurny *et al*., 2022). This is a serious threat to the critical information of the public, weakens

government confidentiality and can jeopardize business. This problem can be tackled by using encryption and decryption algorithm which can protect confidential information against the eavesdroppers by using either symmetric or asymmetric cryptography. To provide security, the key has to be designed in such a way that it cannot be decoded, so the computational complexity is what guarantees security. However, for the cipher/cryptographic transmission of highly confidential data, we must have an extremely secure method of crypto-key sharing between the remote parties Niemiec (2019).

The principles of quantum physics protect the data in QKD, making it a perfect solution for sharing crypto-keys securely between distant parties. In QKD, qubits (quantum information carriers/units of quantum information) are used to encode information that is sent from point to point on a quantum channel. Information can be theoretically secured with QKD technology by using one-time-pad encryption and detecting potential eavesdropping may also be possible (ITU-TY. supp., 2021). A QKDN is a technology that allows QKD to achieve greater reach and availability (Choi *et a*l., 2021). Keys between QKDN nodes can be exchanged through QKDN links, but when they are not connected, they are exchanged through key relays. Notwithstanding, QKDN is recognized from customary correspondence networks by QKD links and the structure of the actual network itself. QKDN can be applied in trustworthy networking technologies as well as artificial intelligence (AI)/machine learning (ML) techniques for 5G and beyond. There are multiple layers of QKDN, including a quantum layer for ensuring the establishment of secure symmetric keys, and QKD links are part of a quantum channel(Choi *et al*., 2021).

The key-management layer helps in key storage, verifying, routing and deleting of the previously established key, this layer is also in charge of quality of service (QoS).It has been suggested that QKDN management and controller layers are central to end-to-end QKD in the holistic control architecture (ITU-TY.3800, 2019; Zhao *et al*., 2021).Machine learning methods have been employed in the selection of optimal QKD protocol and applied random forest (RF) algorithm (Ren *et al*., 2021). The authors have compared RF with other machine learning algorithms and obtained an accuracy of 98 percent with the testing data set with a good receiver operating characteristic. The prediction speed distinguishes it and makes it strong in configuring the optimal QKD protocol and system parameters. The potential applications of QKD for future communication technology have been highlighted by the ongoing standardisation efforts essential for the sustainability and reliability of the near-future deployment (Liu *et al*., 2022).

Figure.1 shows the architecture of QKDN that explicitly describes the presence of various layers and its functions. The various layers present in the architecture of QKDN are the quantum layer, the key management layer, the QKDN control layer, the user network management layer, the quantum management layer, and the service layer. The key elements present in the quantum layer include the QKD links and the QKD module which are enabled to communicate to other layers conveniently. The parameters of the QKD links and the QKD module such as quantum key generation rate, transition power, receive power, could be adjusted in the QKDN control layer. The key management layer includes the functional elements such as the key management agent (KMA) and the key supply agent (KSA) which interchange the control and management messages.

The functional element of the QKDN control layer controls the variable resources to guarantee assured, steady, proficient, and healthy processes of QKDN. This layer unwraps the user interface to cryptographic applications in the service layer, empowering the provisioning of fast service for applications in QKDN. The role of the user network management layer is to perform fault, configuration, accounting, performance and security (FCAPS) management features of a user network. The key role

of the quantum management layer is to correspond and be aligned with information management. The service layer chooses the type of application that QKDN wishes to function. The cryptographic application has been chosen to exploit the distributed key pairs offered by the QKDN and accomplish encrypted contact between isolated parties. Three typical cryptographic applications in the service layer are point-to-point applications, point-to-multipoint applications, and multipoint-to-multipoint applications (ITU-TFGQIT4N, 2021).

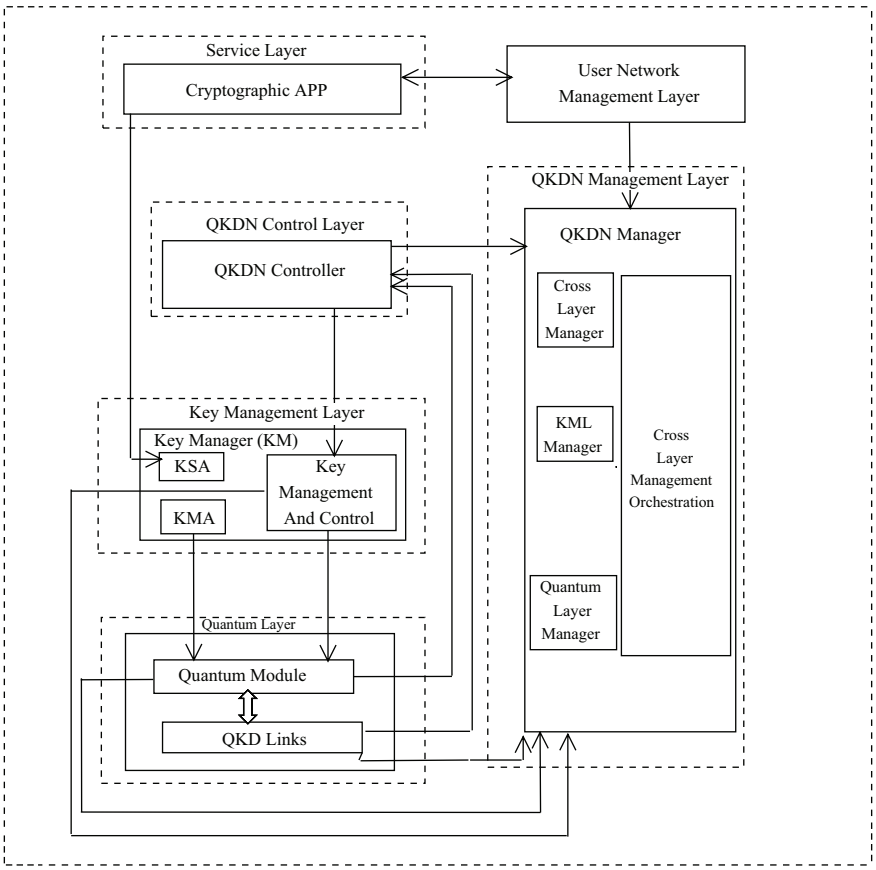

Figure 1. Architecture of QKDN

The detailed framework for improving the performance of the QKDN network using machine learning networks has been briefed in the following sections. Section 2 outlines the framework of QKDN using the machine learning approach which comprises various applications of the quantum layer, the key management layer, the control and management layer. Section 3 outlines additional applications of the machine layer in QKDN followed by conclusion in Section 4.

2. QKDN Framework using Machine Learning Approach

The framework for improving the performance of QKDN using machine learning is classified as the quantum layer, key management layer, control and management layer, and the role of machine learning in each layer of the QKDN is described briefly.

2.1. Role of Machine Learning in Quantum Layer

The initial layer of QKDN is the quantum layer, which is distinct from traditional communication layers. QKD's core components are the QKD transmitter (QKD-Tx) and receiver (QKD-Rx),that are referred to as QKD modules (Choi *et al*., 2021). The classical and quantum channels are included in the QKD link; the quantum channel is responsible for conveying quantum signals such as single photon level, coherent states of light, while the classical channel is responsible for synchronization data and data exchange between QKD modules. QKD protocols are implemented in the QKD modules of the quantum layer. The QKD link is used to connect QKD modules using a quantum relay point to relay quantum signals. As quantum layers play an important role in the robustness of the QKDN, the enhancement of channel performance and of the transmission environment of this layer is crucial to convert QKDN into a commercial product on a global scale (ITU-TY.3800, 2019). By having the best performing quantum layer, we can reduce the noise of the quantum signal which improves the transmission quality of the quantum signal. This can be achieved with quantum channel performance prediction which reduces the noise. The QKD system parameter optimization can convert QKD into a low power platform, and the remaining useful life (RUL) prediction can predict the operability of the components in QKD before they fail, guaranteeing the uninterrupted operation of the QKD system.

The role of machine learning in the quantum layer discusses the performance of the quantum channel, parameter optimization and remaining useful life prediction(Ren *et al*., 2021).

- Quantum channel performance: While transmitting the high-intensity quantum-encoded photons, noise induced by photon is a major challenge, this declines the quality of the quantum channel. As the optical signal to noise ratio (OSNR) decreases, the quantum bit-error-rate (QBER) rises. If QBER reaches the security threshold, the secure key rate (SKR), declines sharply and low SKR is a crucial practical problem for QKD. We can use the supervised machine learning techniques for the estimation of the quantum channel performance, the detailed analysis can be seen in Figure 2. This ML-based model predicts the signal to noise ratio (SNR) of the quantum state optical signal in the quantum channel under various noise conditions. By doing this, the channel environment can be improved and the loss brought on by decreased SNR can be reduced.
- Parameter optimization: Parameter optimization is an important step in the quick and accurate optimization of the QKD system and in the building of a low-power system in a changing, real time environment. Traditional methods require a lot of time and computational power, however, machine learning technology can quickly determine the optimal QKD system parameters based on a large amount of training data. A detailed analysis of the role of ML in parameter optimization is provided in Figure 2.
- RUL prediction: Remaining useful life (RUL) is a crucial factor in predicting the failure of a machine in the production line. The RUL of the QKD systems can be accurately predicted by applying the ML which assures the normal operation of the QKDN. In order to make the

LSTM-based RUL prediction, the raw data must first be collected, categorized, and pre-processed. The detailed flow diagram for RUL prediction using ML is given in Figure 2.

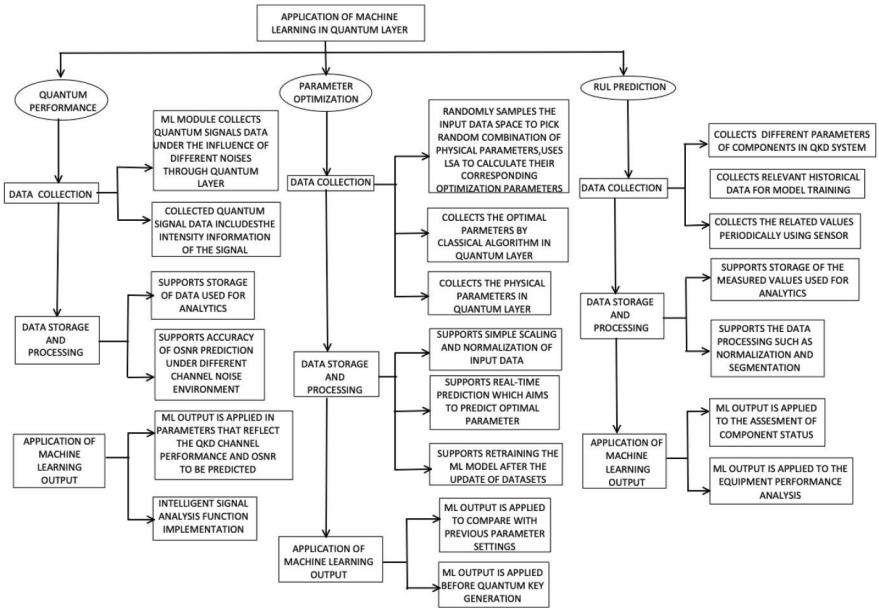

Figure 2. Role of Machine Learning in the Quantum Layer

2.2. Role of Machine Learning in Key Management Layer

This section first outlines the key management layer and then discusses the role of machine learning in the key management layer. The key management layer is an interface layer which is between the QKD protocol and various security applications. The function of the key management layer is to demultiplex the QKD key generated by the QKD protocol into separate groups. These groups can be synchronized between the two ends of the communication endpoints since they are independently ordered and used by programmers. After use, the QKD- keys are removed from the key management layer and are never revealed to anyone else. The key management layer is made up of a key manager (KM), which controls the key management agent (KMA), the key supply agent (KSA), and KM control and management (Ren *et al*., 2021). Each QKD module produces metadata, which is subsequently linked to the QKD-key to create a key file. The QKD-key file is then transferred to the appropriate KMAs. The KMAs combine and split QKD-keys into the prescribed keys known as KMA-keys, which are stored in the key management layer. The key supply interface receives the key request from the cryptographic application. Following authentication, the KSA notifies the KMA of requested information. Key encryption occurs at the source KMA, and decryption occurs at the destination KMA. It has been suggested that from KMA to KSA, the KMA-key supply is relayed until it reaches the key life cycle management, where each KMA stores data on the key management operations it performs, including receiving keys, key retention, key structuring, key imparting, key synchronization, key validation, key supply, and key deletion/preservation (ITU-TFGQIT4N, 2021).To improve the efficiency of the key management layer,

we have to find a solution for key formatting which saves time while also lowering the possibility of key synchronization failure. Improving key storage management allows for the ideal path for key distribution to be chosen, as well as acceptable scheduling and efficient use of key resources.

The role of machine learning in key management layer discusses about the key formatting, key storage management and anomaly detection (Ren *et al*., 2021).

- Key formatting: The key manager structures the keys for key supply and relay, which may involve merging and splitting if the lengths are insufficient. The different encryption algorithms and different security requirements need different key formats. To keep the QKDN interconnected and expandable, key data with supplementary metadata accommodating different types of information has to be properly key formatted. The massive service information could be used as input for ML module training by applying ML estimation techniques i.e., deep learning algorithm and Elman neural network. The statistical service features are determined by this training model. The analysis of key formatting using ML is shown in Figure 3.
- Key storage management: The QKD services cannot be carried out well if the key pool (KP) has inadequate/unnecessary key resources, severe jitter, and a prolonged storage time. The demand for keys from the user changes unpredictably with practical scenarios. Traditional solutions cannot perceive the actual needs, and the key supply cannot adjust dynamically when key requirements are changed dynamically. The ML model can be trained with a significant quantity of data, and a model can be developed using a classification algorithm. It can compare the outcomes and modify the model swiftly, enabling more accurate key requirement prediction. A detailed analysis can be seen in Figure 3.
- Anomaly detection: When key requirements are transmitted from cryptographic applications to key supply agents (KSA), the QKD controller facilitates the control of the reception of the key requests for the KSA. KSA authenticates this appropriately. The certificate is issued by the QKD controller's access control department. However, traditional methods cannot detect a mass attack effectively. ML algorithms such as artificial neural network (ANN) and recurrent neural network (RNN) can be applied for monitoring abnormalities and for authorizing cryptographic applications (ITU-TY.3800-series, 2021). The detailed analysis of anomaly detection using ML is shown in Figure 3.

2.3. Role of Machine Learning in Control and Management Layer

This section initially outlines the control and management layer and then discusses the role of machine learning in the control and management layer. The control and management layer contributes to the QKDN's safety, consistency, effectiveness, and dependability. It has been suggested that this layer is responsible for the administration of the QKDN as well as to support user network management (Choi *et al*., 2021). Control operations such as key generation regulation, route command for key replaying, session management for QKD systems, access control, and QoS regulation are all provided by this layer. It also manages several tasks that include fault management, configuration management, accounting, performance, and security management. This layer keeps track of the data from the quantum layer, the key management layer, and the control systems. Therefore, this layer maintains the overall performance of the QKDN, and also produces big data regarding network information, such as network topology, link load, the key consumption rate, real-time bandwidth requests etc., which can be used to implement optimization algorithms.

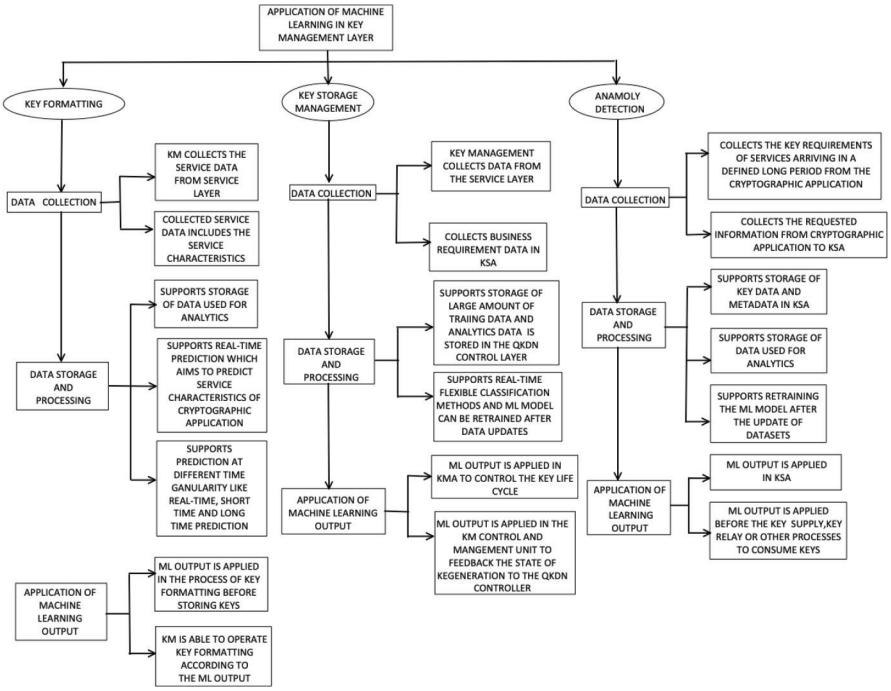

Figure 3. Role of Machine Learning in the Key Management Layer

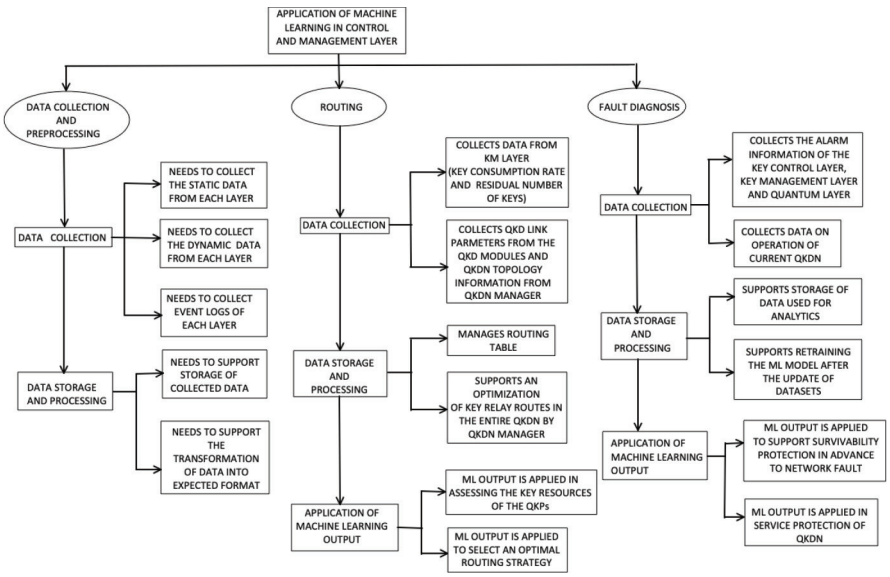

Figure 4. Role of Machine Learning in Control and Management Layer

The role of Machine Learning in Control and Management Layer discusses about data collection and preprocessing, as well as routing and fault diagnosis (Ren *et al*., 2021).

- Data collection and data pre-processing: The management layer collects information from each layer through reference points for anomaly detection and makes appropriate decisions to rectify it. As the QKDN has the multi-sourced data and is heterogeneous this type of data collection is not the best, and not suitable for data pre-processing. Data pre-processing can be applied for the dataset of all protocols that use the same features and values. Therefore, data processing methods that gather and organize the data into comprehensible, integrated, and simple structures have been proposed (ITU-TY.3800-series, 2021). Those methods can be utilized for data analysis with the aid of machine learning models. Figure 4 presents the detailed analysis of this case.
- Routing: Due to the service's dynamic and eruptive nature, there is an imbalance in the consumption and generation of essential resources. Whenever, the number of keys on the selected path is insufficient to satisfy the service encryption requirements, the success rate is decreased. We can use the data collected by the control and management layer to implement the optimization algorithm. In the categorization of routing parameters, ML classifiers such as reinforcement learning are implemented, resulting in the optimum routing scheme that is delivered to the QKDN control layer, where it is transformed into a cascade of rules. Figure 4 provides the analysis for this application.
- Fault diagnosis: Control and management layers collect the errors from all the three layers of the QKDN. To do this effectively, QKDN should be able to predict and locate errors timely according to the data provided to it from each layer. In order to assist this, the ML model can be used. This machine learning model extracts distress data from each layer of the QKDN and employs a convolutional neural network (CNN) for robust extraction and visualization. Figure 4 shows the detailed analysis of this use case regarding the data collection, data storage, data processing, and ML output.

3. Additional Applications of Machine Layer in QKDN

This section discusses quantum attacks on both continuous-variable and discrete-variable quantum key distribution. The additional applications touch upon previous work on error correction or key reconciliation as referred by Niemiec (2019).

Machine learning can be used to detect quantum attacks as a feasible defense method as suggested by (Mao *et al*., 2020). Using artificial neural networks (ANN), this research investigates the quantum attack in a continuous-variable quantum key distribution (CV-QKD). This work looked at different aspects of pulses as input to a machine learning model that predicts attack detection and classification. The results identify the majority of attacks while cutting the cost. By monitoring the properties of the pulses and understanding the sort of attack, it gives a universal attack prediction algorithm.

Machine learning framework for enhanced QKD network is shown in Figure 5. The various layers present in the quantum layer act as a source input to machine learning pipeline processing to obtain output at a destination for the QKDN network. As we are aware, machine learning pipeline processing consists of acquiring the data, validating the data, cleaning the data, training the machine learning model, evaluating the model, validating the model and again triggering the re-training in accordance with the accuracy and efficiency obtained on the chosen model.

The machine learning model can be supervised, unsupervised or reinforcement learning. The well-known algorithms under supervised learning techniques include decision trees (DTs), support vector machine (SVM), K-nearest neighbors (KNN), support vector regression (SVR) and gaussian process regression (GPR) algorithms. The well-known algorithms under unsupervised learning techniques include K-means clustering, hierarchical clustering algorithms, principal component analysis (PCA), and ISOmetric MAPping (ISOMAP). The techniques for reinforcement learning are Markov decision process (MDP), Q-learning, policy learning, actor critic (AC) and multi-armed bandit (MRB) algorithms. Depending on the type of chosen application, various algorithms can be carefully trained on machine learning models to fully support QKDN.

Measurement device-independent quantum key distribution (MDI-QKD) systems provide an untappable quantum key distribution system that resolves many of the QKD's practical concerns while also being effective. When dealing with noise from the external environment and internal components, the feedback controls keep the system stable. For reference frame calibration, scanning and transmitting or inserting an extra device is commonly employed, although this increases system complexity and reduces transmission efficiency. This issue has been addressed in a research by Zhang *et al*. (2021) in which the authors use a long short-term memory (LSTM) based ML model for the very first time on MDI-QKD for reference frame calibration (2021). Error correction or key reconciliation in quantum cryptography has been addressed by Niemiec (2019), which is essential for obtaining the high level of security that QKD offers. The authors used the mutual synchronization of the ANN to correct the errors occurring during transmission in quantum channel. This shows the synchronization process is faster compared with the parallel cases using neural cryptography.

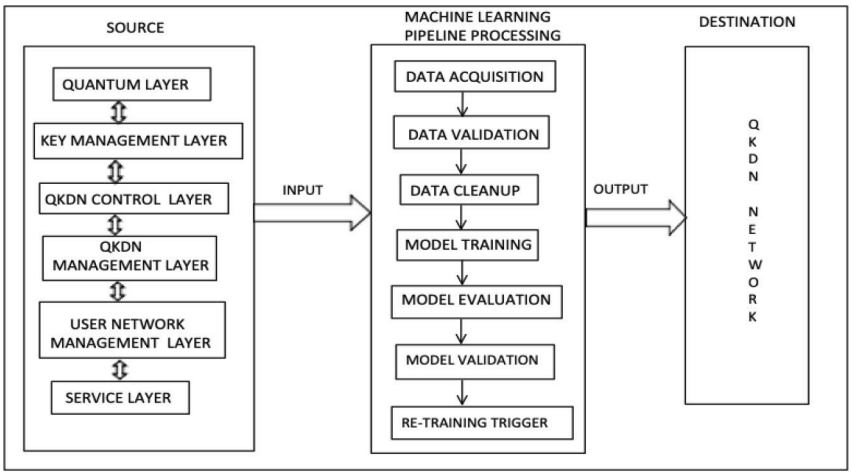

Figure 5. Machine Learning Framework for Enhanced QKDN

Biswas *et al*. (2022) proposed a modified key sifting scheme for quantum cryptography that utilizes the artificial neural network based key reconciliation for future quantum key distribution. Djordjevic (2020) has employed the joint QKD-post-quantum cryptosystems which consider the complexity of the algorithm that employs the raw-key algorithm and this subsystem uses transmit parity bits for information reconciliation. Sun *et al*. (2022) have employed sending or not sending twin-field QKD by

considering the practical imperfections of the detection device. This work has provided practical references for long term quantum communication. Cai *et al*. (2021) have done a theoretical study on the issues of QKD in long-distance transmission, along with classical signals. It was found that multicore fiber was effective for long distance transmission of QKD and dense wavelength division multiplexing system. Yu *et al*. (2021) have worked on free-space phase-matching QKD where the real time practical version would be able to surpass the linear bound without quantum repeaters. First the authors secured the key rate and later employed the simulated performance of QKD in free space and ideal circumstance to study the effect of the atmospheric turbulence.

4. Conclusion

A framework for improving the performance of QKDN using the machine learning approach has been proposed in this article by looking at how machine learning can help the quantum key distribution network function better. The proposal addresses various layers in quantum computing to make it easier to use ML to resolve issues and facilitate the role of the framework. It can be seen that artificial intelligence and machine learning models play a vital role in each layer of QKDN for enhancing channel performance, optimization, prediction, management, and classification of machine learning parameters. To consider a definitive objective of quantum-safe interchange frameworks, a multi-disciplinary methodology is required, going from the hypothetical investigation of the QKD use cases to the actual execution of QKD gadgets. It is evident that machine learning plays a crucial factor in the commercialization of the QKDN. The additional application of quantum cryptography helps to identify the attacks with the machine learning approach through practical concern of QKDN. Although there is plenty of research and development in the area of QKDN, directing the effort towards standardisation that meets industrial goals, will guarantee the near future reliability and sustainability of QKDN. Corrective measures have to be taken to collaborate with academia, industry and government in order to accelerate the progress towards the deployment of QKDN.

References

Biswas, C., Haque, M. M., and Das Gupta, U., 2022. A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography. *IEEE Access, 10*, 72743-72757. https://doi.org/10.1109/ACCESS.2022.3188798

Cai, C., Sun, Y., & Ji, Y., 2021. Simultaneous long-distance transmission of discrete-variable quantum key distribution and classical optical communication. *IEEE Transactions on Communications, 69*(5), 3222-3234. https://doi.org/10.1109/TCOMM.2021.3056528

Choi, T., Kim, H., Kim, J., Yoon, C. S., & Lee, G. M., 2021. Quantum key distribution networks for trusted 5g and beyond: An itu-t standardization perspective. In *2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K)*, pp. 1-9. IEEE. https://doi.org/10.23919/ITUK53220.2021.9662098

Djordjevic, I. B., 2020. Joint QKD-post-quantum cryptosystems. *IEEE Access, 8*, 154708-154712. https://doi.org/10.1109/ACCESS.2020.3018909

ITU-TFGQIT4N, 2021. FG QIT4N D2.3 quantum key distribution network protocols: Key management layer, QKDN control layer and QKDN management layer.

ITU-TY.3800, 2019. Recommendation ITU-T Y.3800 specifies an overview on networks supporting Quantum Key Distribution (QKD).

ITU-TY.3800-series, 2021. Y. Sup70: ITU-T Y.3800-series - Quantum Key Distribution Networks - Applications of Machine Learning.

ITU-TY.supp, 2021. Draft supplement itu-t y.supp.qkdn-mla : Quantum key distribution networks - applications of machine learning.

Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., and De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Communication, 3*(3), 151-163. https://doi.org/10.1049/qtc2.12044

Mao, Y., Huang, W., Zhong, H., Wang, Y., Qin, H., Guo, Y., & Huang, D., 2020. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New Journal of Physics, 22*(8), 083073. https://doi.org/10.1088/1367-2630/aba8d4

Niemiec, M., 2019. Error correction in quantum cryptography based on artificial neural networks. *Quantum Information Processing, 18*(6), 1-18. https://doi.org/10.1007/s11128-019-2296-4

Ren, Z.-A., Chen, Y.-P., Liu, J.-Y., Ding, H.-J., & Wang, Q., 2021. Implementation of machine learning in quantum key distributions. *IEEE Communications Letters, 25*(3), 940-944. https://doi.org/10.1109/LCOMM.2020.3040212

Spurny, V., Munster, P., Tomasov, A., Horvath, T., & Skaljo, E., 2022. Physical layer components security risks in optical fiber infrastructures. *Sensors, 22*(2), 588. https://doi.org/10.3390/s22020588

Sun, M.-S., Zhang, C.-H., Ma, X., Zhou, X.-Y., & Wang, Q., 2022. Sending-or-not-sending twin-field quantum key distribution with measurement imperfections. *IEEE Communications Letters, 26*(9), 2004-2008. https://doi.org/10.1109/LCOMM.2022.3181984

Yu, Y., Wang, L., Zhao, S., & Mao, Q., 2021. Free-space phase-matching quantum key distribution. In *2021 13th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1-4. https://doi.org/10.1109/WCSP52459.2021.9613412

Zhang, S., Liu, J., Zeng, G., Zhang, C., Zhou, X., & Wang, Q., 2021. Machine learning-assisted measurement device-independent quantum key distribution on reference frame calibration. *Entropy, 23*(10), 1242. https://doi.org/10.3390/e23101242

Zhao, Y., Zhang, K., Zhu, Q., Wang, H., Yu, X., & Zhang, J. 2021. Applications of machine learning in quantum key distribution networks. In *2021 IEEE 6th Optoelectronics Global Conference (OGC)*, pp. 227–229. IEEE. https://doi.org/10.1109/OGC52961.2021.9654412