IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 June 2024, accepted 4 August 2024, date of publication 15 August 2024, date of current version 2 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3444268

RESEARCH ARTICLE

Deep Learning-Based Optimization of Underwater QKD Systems With Time-Gated SPADs

MOSTAFA NOZARI[1], (Student Member, IEEE), AND MURAT UYSAL[2], (Fellow, IEEE)
[1]Department of Electrical and Electronics Engineering, Özyeğin University, 34794 Istanbul, Türkiye
[2]Engineering Division, New York University Abu Dhabi (NYUAD), Abu Dhabi, United Arab Emirates
Corresponding author: Mostafa Nozari (mostafa.nozari.st@gmail.com)

ABSTRACT In this paper, we consider underwater quantum key distribution (QKD) systems with time-gated single photon avalanche photodiodes (SPADs) and present a comprehensive performance analysis and optimization. We utilize a deep learning model for the system optimization. We first perform Monte Carlo simulations for a subset of possible scenarios and train the deep learning model on them. Then, we use this model to instantly extract the optimum values for possible underwater scenarios. Our study provides critical insights on determining the optimal bit time, field of view (FoV), and gate time in underwater QKD. Through a meticulous analysis of the propagation delay and angle of arrival results, we determine the bit time and FoV, respectively, by striking a balance between the average number of received photons and background noise. Afterwards, using the proper bit time and FoV from the previous steps, we determine the optimal gate times in the sense of minimizing the quantum bit error rate (QBER). Our findings reveal that the proposed method significantly improves QBER, with enhancements reaching up to two orders of magnitude across different link lengths.

INDEX TERMS Quantum key distribution, single photon avalanche diode, deep learning, underwater quantum communication, quantum bit error rate.

I. INTRODUCTION

The rapid advancements on quantum computers with high computational capabilities have raised concerns regarding the use of classical cryptography methods. In the post-quantum era, classical asymmetric key generation techniques commonly employed in wireless systems will face significant security risks [1]. These methods build upon some computational complexity assumptions and can be susceptible to attacks by powerful computers. Quantum Key Distribution (QKD) relies on the principles of quantum mechanics and provides theoretically unconditional security [2], [3]. The initial QKD protocol introduced by Bennett and Brassard back in 1984, commonly referred to as BB84 [4], is a prepare-and-measure protocol. In this protocol, a qubit state is prepared and subsequently transmitted to the receiving party. Subsequently, entanglement-based protocols were developed, wherein both parties possess a shared state and perform measurements on it. While entanglement protocols provide an added layer of security by eliminating the need to trust the quantum source, BB84 and its variants protocols have gained greater popularity primarily due to their simplicity.

QKD was successfully applied to fiber optic, satellite, and terrestrial wireless links [5], [6]. Another potential QKD application area is underwater communications. Quantum-secure communication is critical for maritime surveillance sensor networks and strategic applications such as submarine-to-submarine communication, autonomous underwater vehicle (AUV) data offloading, etc. There has been a growing literature on the underwater QKD, see e.g., [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], and [17]. For example, in [7] and [8], based on the Beer–Lambert path loss model, the maximum secure communication distance for the BB84 protocol in underwater environments was derived to achieve a desired level of quantum bit error rate (QBER) and

The associate editor coordinating the review of this manuscript and approving it for publication was Fang Yang.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

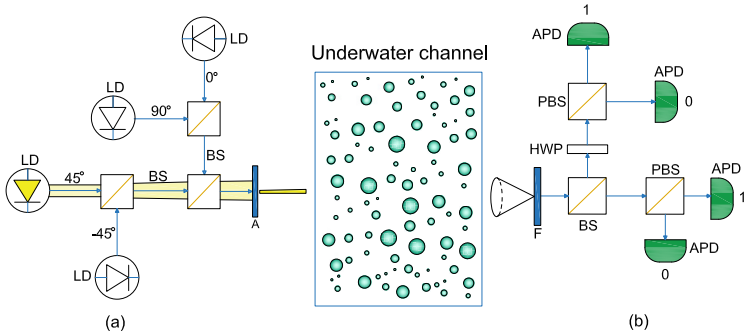


FIGURE 1. Underwater QKD system under consideration a) transmitter, b) receiver. Transmitter components are laser diode (LD), beam splitter (BS) and attenuator (A). Receiver components are filter (F), beam splitter (BS), polarizing beam splitter (PBS), half wave-plate (HWP), and avalanche photodiode (APD).

the secret key rate (SKR). While initial works ignore the effects of turbulence, later works have demonstrated the effect of turbulence via computer simulations and analytical derivations [9], [10], [11] as well as experimental means [12], [13]. Various protocols such as decoy state BB84 [14], BB92 [15], entanglement [16] were further investigated in underwater environments. Absorption, scattering, and turbulence experienced in underwater channels severely limit the range of quantum communication links. As a potential solution to overcome range limitations, multi-hop underwater QKD where intermediate nodes (i.e., relays) between the source and destination nodes help the key distribution was also explored in [17].

In the practical implementation of the BB84 protocol, InGaAs or InP single photon avalanche photodiodes (SPADs) working in the Geiger mode are commonly employed as detectors [18]. To mitigate the effect of background noise, they are operated typically in the gate mode. However, selecting an inappropriate gate time can filter out a significant number of photons count and lead to performance degradation. The optimal design of time-gated single photon detection system depends on the propagation medium and has been recently studied for underwater links in [19] and [20]. In [19], the underwater channel impulse response was estimated through Monte Carlo simulations. Based on the developed channel model, optimal selection of the gate time was discussed to minimize the QBER. This evaluation was conducted for given values of receiver field of view (FoV) and bit time. In [20], the bit time was first determined to avoid the inter symbol interference (ISI) arising from multiple scattering, i.e., an emitted photon within the previous bit time can arrive late due to scattering and therefore recorded in the next bit time. Then, based on the angle of arrival (AoA) of the received photons, the proper value of FoV was selected to restrict the received background noise. Finally, the SPAD gate time was optimized to minimize the QBER for the selected values of FoV and bit time.

In this paper, we re-visit the problem in [20] in an effort to have further insight into underwater QKD system design and optimization. Our contributions are three-fold:

- Selection of bit time and FoV were carried out independently in [20]. They are in fact related to each other and must be optimized jointly. The FoV value plays a significant role in limiting the reception of photons which deviate from the direct path between transmitter and receiver and therefore require a longer time to reach the detector due to the extended path. Consequently, the selected FoV value directly affects the required bit time. In this study, we consider the interdependence of bit time and FoV and jointly optimize these two system parameters.
- In [20], to minimize the ISI, the minimum bit time was selected as the required average time for receiving a sufficiently large number of photons. Specifically, a threshold of 99.9% of the total received photons was considered. Similarly, the FoV was selected in [20] as the angle needed to capture a significant number of photons, i.e., a threshold of 99.9%. However, the effect of background noise is ignored during these selections [20]. In this study, we mitigate the degrading effects of noise by properly adjusting the bit time and FoV with respect to QBER. However, this adjustment may result in a higher level of ISI. Consequently, we consider ISI effect in our optimization as an additional constraint.
- Conducting an interdependence analysis of bit time and FoV with respect to QBER for every variation in the system or channel parameters is computationally expensive. Instead, we utilize a deep learning model for the system optimization. We first perform simulations for a subset of possible scenarios and train the deep learning model on them. Then, we use this model to extract the optimum values for other possible underwater scenarios.

The rest of the paper is organized as follows: In Section II, we describe the underwater QKD system under consideration. In Section III, we investigate the interdependency of the SPAD parameters and their impact on the QBER. In Section IV, we discuss the QKD system optimization based on supervised learning. In Section V,

we present the numerical results and finally conclude in Section VI.

II. SYSTEM MODEL

We consider a QKD system that utilizes the BB84 protocol for underwater communication over a distance of L. For underwater QKD, an operation wavelength of λ in blue and green region is commonly preferred. The QKD BB84 protocol establishes a secure key between two trusted partners, traditionally named as Alice and Bob, to ensure that an eavesdropper (Eve) can not obtain significant information during the key exchange. At the transmitter (see Fig. 1a), Alice uses a laser diode followed by a set of four distinct filters to align the light's polarization in certain orientations, e.g., $0°$, $90°$, $-45°$, and $+45°$. She randomly selects a filter for each bit time, denoted by Δt, and transmits either 0 or 1 using a beam splitter. The laser is assumed to have a maximum beam divergence of $\theta_{0,\max}$ and a beam width of r_0. While the initial position of photons on the transmitter plane is determined by the beam width, beam divergence affects the departure direction of photons. The directed light goes through an attenuator to ensure proper reduction in light energy and is transmitted through the underwater channel.

At the receiver side (see Fig.1b), a filter is used to distinguish the photon signal from the background noise. The filter spectral width, denoted by $\Delta\lambda$, determines the range of wavelengths allowed by the optical filter for receiving photons. After that, a beamsplitter randomly directs the photon to one of two arms, each corresponding to a different polarization basis. To linearly polarize light, a half-wave plate is used. The photon is then redirected to one of the APDs through a polarizing beam splitter based on its polarization state. APDs have an aperture area of A that represents a surface area over which the incoming light is collected. SPADs working in the Geiger mode are commonly employed as APDs. The gate time of $\Delta t'$ represents a time window ($0 \leq \Delta t' \leq \Delta t$) in which Bob performs measurements on the quantum states sent by Alice, and any reception outside the gate window will cause the photon rejection. The FoV of the SPADs, denoted by Ω, determines the angular extent of the region over which the detector can effectively capture incoming photons. As a result, photons that fall outside the angular region of FoV will not be counted.

Assume that Alice wishes to send a bit string to Bob over the quantum channel to establish a key. Bob randomly selects a combination of polarization bases to measure the light in each bit time interval. A "sift" event is triggered when both Alice and Bob use the same polarization basis. Alice and Bob exchange their basis strings over the classic channel and eliminate bits where bases do not match. In the presence of imperfections like interception, noisy channels, or detector issues, sift events may yield different bit values. To verify the equality of the shared key, Alice and Bob reveal a portion of their key over the classic channel. If the number of incorrect bits exceeds a predetermined threshold, the shared key is deemed unreliable. Otherwise, error correction techniques can be applied. Once Alice and Bob have agreed upon the key, they can use it for encryption over the classical channel.

III. INTERDEPENDENCY OF SYSTEM PARAMETERS AND THEIR EFFECT ON QBER

Let γ denote the fraction of received photons [21]. QBER is defined as the error rate in the sifted key and can be calculated as [21]

$$QBER = \frac{n_N}{\gamma \frac{n_S}{2} + 2n_N} \tag{1}$$

where n_S represents the expected number of received photons during each bit time interval and the factor of 1/2 is introduced as a result of sifting process. Based on the well-known Beer-Lambert law, the number of photons is a function of the extinction coefficient depending on the water type.

Background noise is calculated by

$$n_N = n_D + \frac{n_B}{2} \tag{2}$$

where the first and second terms respectively arise from the dark current of the SPADs and environment irradiance. The first term is calculated as

$$n_D = I_{dc}\Delta t \tag{3}$$

where I_{dc} is the dark current count. It determines the average rate of dark current events in the absence of incident light and relates to the sensitivity of SPAD detectors. The second term is given as

$$n_B = \frac{\pi R_d A \lambda \Delta\lambda (1 - \cos(\Omega))\Delta t'}{2h_p c_0} \tag{4}$$

where, h_p is Planck's constant, c_0 is the speed of light, and R_d is the irradiance of the environment whose primary source is the refracted sunlight from the surface of the water [22].

It can be readily checked from (1) that increasing the value of n_N can result in a higher QBER. Therefore, it is crucial to limit the effect of background noise. Based on (3), it is observed that the level of background noise arising from dark current only depends on the bit time (Δt). On the other hand, as can be seen from (4), the level of background noise due to irradiance is dependent on several system parameters including FoV, gate time, aperture area and filter spectral width. In the following, for given values of maximum beam divergence, beam width and aperture area, we will discuss how bit time and FoV values affect the QBER performance and how they interplay with each other.

A straightforward approach to determine the bit time, as adopted in [20], is based on the required time to guarantee the reception of a very high percentage of photons (99.99%). Such a conservative approach ensures reliable transmission by avoiding ISI, however requires large values of the bit time. This, in turn, increases the amount of background noise as a result of the dark current from SPADs. Similarly, the value of FoV can be selected as in [20] to allow for the inclusion of a significant number of photons. However, increasing the FoV leads to a greater number of background photons, which in

turn can increase the noise as a result of the irradiance from environment. Moreover, FoV and bit time are dependent on each other. Choosing a large FoV (e.g., 180°) allows for more photons to be taken into account and deals with the worst case scenario of ISI. This helps to even capture the photons that deviate significantly from the direct propagation line. However, this increases the propagation time and accordingly necessitates a larger value of bit time, eventually leading to further increase in the background noise. As a summary, we need to carefully weigh the benefits of considering a higher percentage of photon reception against the potential drawbacks of longer required reception times and a larger FoV to achieve best QBER performance.

IV. SUPERVISED LEARNING-BASED QKD SYSTEM OPTIMIZATION

As discussed in the previous section, many system and channel parameters are related to each other and have direct or indirect effects on the QBER. Optimal underwater QKD system design taking into interdependence for every variation in the system or channel parameters is computationally expensive. To overcome this challenge, we utilize supervised learning [23] for optimization. This type of machine learning is analogous to human learning from past experiences to gain new knowledge in order to improve our ability to perform real-world tasks [23]. Since computers lack their own experience, we rely on labeled datasets in supervised learning. These datasets consist of multiple data samples. Each data sample is denoted as $(x^{(m)}, y^{(m)})$, where $x^{(m)}$ represents a feature vector for the m^{th} sample (representing the causes leading to a particular experience) and the label $y^{(m)}$associated with feature $x^{(m)}$ to reflect the experience itself.

The goal of supervised learning is to learn the underlying relationship between the features and their corresponding labels. For this purpose, it employs an appropriate deep learning architecture and trains it using a proper cost function to make accurate predictions for new combination of input features. Deep neural networks (DNNs) can capture intricate nonlinear relationships within the data, which can be particularly valuable in use cases where there may be complex interactions among the input features. A DNN is composed of multiple layers, including an input layer and an output layer, along with intermediate layers referred to as hidden layers. Neurons within each layer receive inputs from multiple neurons in the preceding layer and perform computations. This typically involves a weighted sum followed by a nonlinear activation function. Mathematically speaking, it is given by

$$A_j^{[l]} = \sigma_j^{[l]}\left(\sum_i w_{ji}^{[l]} z_i^{[l]} + b_j^{[l]}\right) \tag{5}$$

where $A_j^{[l]}$ represents the output of the j^{th} neuron in the l^{th} layer, $\sigma(.)$ represents an activation function utilized to introduce non-linearity in the modeling process, $z_i^{[l]}$ represents an input from the i^{th} neuron of the preceding layer (in the first layer, this corresponds to the i^{th} feature from $x^{(m)}$), $w_{ji}^{[l]}$ corresponds to the weight between that input and the j^{th} neuron in the l^{th} layer, and $b_j^{[l]}$ denotes the bias term associated with the j^{th} neuron in the l^{th} layer.

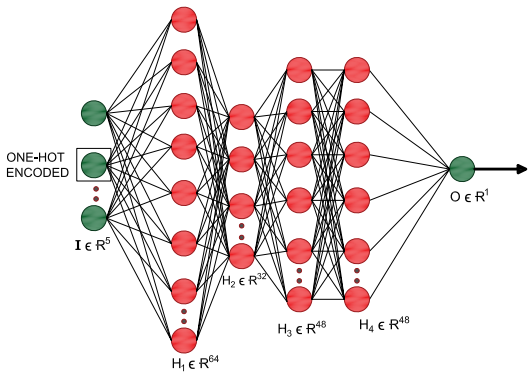


FIGURE 2. DNN with five features and four fully connected hidden layers with 64, 32, 48, 48 units, respectively, and utilizing the Rectified Linear Unit (ReLU).

Assume that the DNN includes L layers. Based on the inputs of the last layer, i.e., $z_j^{[L]} = A_j^{[L-1]}$, the predicted label value for the m^{th} sample can be calculated as

$$y_{\text{pred}}^{(m)} = \sum_i w_{1i}^{[L]} z_i^{[L]} + b_1^{[L]} \tag{6}$$

where $w_{1i}^{[L]}$ is the weight between i^{th} neuron in the $(L-1)^{th}$ layer and the single neuron in L^{th} layer, and $b_1^{[l]}$ is the bias term associated with the neuron in the L^{th} layer. The mappings in (5) and (6) are learned from the labeled data by adapting each neuron's weights and bias using forward-backward propagation sequences through a proper cost function [24]. The cost function compares the predicted value in (6) with the actual label across all the training data samples. The cost function averaged across the entire training set can be envisioned as a landscape with hills and valleys in the high-dimensional space of weight parameters. The negative gradient vector of the cost function indicates the direction of the steepest descent within this landscape, guiding the optimization process toward a minimum where the average output error is minimized [25]. This process is commonly referred to as backpropagation and is accompanied by forward propagation, where the updated weights are used to calculate the output. This iterative process of adjusting weights through backpropagation and calculating output through forward propagation is called the training process and continues until convergence is achieved or predetermined condition met.

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we employ a DNN and train it to determine the optimal underwater QKD parameters with sufficient

TABLE 1. System and channel parameters.

Parameter	Definition	Numerical Value
p	Photon power	1W
λ	Wavelength	532 nm [16]
I_{dc}	Dark current count rate	60 Hz [16]
$\Delta\lambda$	Filter spectral width	30 nm [16]
K_∞	Asymptotic diffuse attenuation coefficient	0.08 m^{-1} [26]
z_d	Depth	100 m [16]
$R_d\,(\lambda, 0)$	Irradiance of the underwater environment at sea surface	10^{-3} W/m^2 [16]
r_0	Transmitter beam width	3, 6 mm
$\theta_{0,\max}$	Maximum beam divergence	20°, 30°
A	Receiver aperture diameter	10, 20, 30 cm
L	Link length	5, 10, 15, 20, 25, 30, 35, 40 m
ζ	Extinction coefficient (water type: Pure sea, Clear ocean, Coastal water, Harbor water)	0.056, 0.15, 0.305, 2.17 m^{-1} [22]

precision. For training, we first need to collect data samples of bit time and FoV values. Due to the lack of an off-the-shelf dataset for our specific purpose, we need to create our own by identifying the suitable feature vectors and their corresponding labels. For this purpose, we conduct a comprehensive exploration of the parameter space, meticulously examining the interdependencies among the bit time and FoV, and their impact on QBER performance as earlier described in Section III.

A. DATA SET GENERATION

In this section, we explain how we generate dataset to train our DNN model. Through earlier discussions in Section III, the major parameters that notably affect the bit time and FoV include beam width, beam divergence, receiver aperture diameter, link length, and water type. These constitute the elements of the five-dimensional feature vector which is the input to the DNN. As illustrated in Fig.2, we utilize a DNN comprising an input layer (denoted as I) with five features. In the input layer, we employ one-hot encoding to distinctly represent each water type feature, thereby avoiding any imposition of ordinal relationships between them. Following the input layer are four hidden layers (denoted as H_i, where i ranges from 1 to 4 for the first through fourth hidden layers, respectively), which contain 64, 32, 48, and 48 neurons, respectively. A Rectified Linear Unit (ReLU) activation function is utilized in the neurons of these hidden layers. The output layer (denoted as O) represents either bit time or FoV values.

In our study, we use the Monte Carlo modeling of light transport in the multi-layered tissues (MCML) method [27]. In this simulation method, the photons are launched from the transmitter based on initial beam divergence and departure direction, which are derived from a uniform distribution [27]. A photon propagates through the underwater channel and travels a random distance before interacting with a particle in the medium. Upon collision with a particle, the photon undergoes energy reduction based on the absorption and scattering coefficients. Then it scatters with a new direction which is determined randomly based on the two-term Henyey–Greenstein (TTHG) model [20]. This process continues iteratively until the photon either reaches the receiver or is lost due to multiple scattering. The inherently random trajectory of the photon during this process can introduce ISI at the receiver side if the bit time is chosen based on a portion of received photons instead of considering roughly all the received ones. To model the ISI, let t_p denote the arrival time of a photon belonging to one of the bit times in the interval of $[1, m-1] \in \mathbb{N}$. Here, m denotes the bit time where the ISI occurs within that interval and is given by $m = \left\lfloor \frac{t_p}{\Delta t} \right\rfloor$, where $\lfloor . \rfloor$ represents the floor function. ISI occurs if the arrival time of a photon is greater than the bit time, i.e., $t_p > \Delta t$ and the inequality $m\Delta t < t_p < \left(m\Delta t + \Delta t'\right)$ is satisfied. This inequality indicates that the arrival of a photon belongs to a bit time within the range of [1, m-1] and inside the gate window of the m^{th} bit time.

We partition both datasets of bit time and FoV into training and validation, with a ratio of 80:20, respectively. In other words, we dedicate 80% of the dataset for training purposes and 20% for the test of the model. In the simulations, we assume beam width of $r_0 = 3, 6$ mm, initial divergence of $\theta_{0,\max} = 20°, 30°$, receiver aperture diameter of$A = 10, 20, 30$ cm, link length of $L = 5, 10, 15, 20, 25, 30, 35, 40$ m and extinction coefficient of $\zeta = 0.0056, 0.15, 0.305, 2.17$ m^{-1} that correspond to pure sea, clean ocean, coastal water, and harbor water. The ranges of the parameters under consideration are provided in Table 1 which leads to a dataset of 384 samples.

We train the model using the adaptive moment estimation (Adam) optimizer [28] and use the mean squared error (MSE) as our cost function

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}\left(y_{\text{pred}}^{(i)} - y^{(i)}\right)^2 \tag{7}$$

where n is the number of samples and $y_{pred}^{(i)}$, $y^{(i)}$ are respectively the predicted value and the actual value corresponding to the i^{th} sample. In the training, we adopt early stopping [29] with a learning rate schedule to prevent divergence and to reduce the learning time. In addition, we use model checkpointing [30] to save the best-performing model during training.

To describe the goodness of our model, we consider the R-squared criterion [31]

$$R^2 = 1 - \frac{\sum_{i=0}^{n-1} \left(y^{(i)} - y_{\text{pred}}^{(i)}\right)^2}{\sum_{i=0}^{n-1} \left(y^{(i)} - \bar{y}\right)^2} \tag{8}$$

where $\bar{y}$ represents the mean value of labels $y^{(i)}$, i=0,1...N−1. This is upper bounded by unity which is reached in the case of fitting a perfect model. The R-squared criterion is unable to check the bias in the model and is typically utilized in conjunction with residual plots [31] for model evaluation. A residual is a measure of the vertical deviation of dependent variables from the prediction model and can be calculated as $r = y - y_{pred}$. To estimate the probability density function (PDF) of residuals and obtain smoothed representation of histogram shape of residuals, we employ kernel density estimation (KDE) as

$$\widehat{f}(r) = \frac{1}{nh} \sum_{i=0}^{n-1} k\left(\frac{r - r^{(i)}}{h}\right) \tag{9}$$

where h is smoothing parameter and k is a Gaussian kernel function given by

$$k(x) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) \tag{10}$$

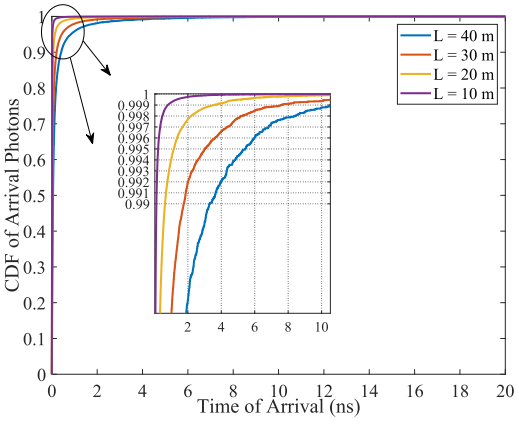


FIGURE 3. CDF of arrival photons versus time of arrival.

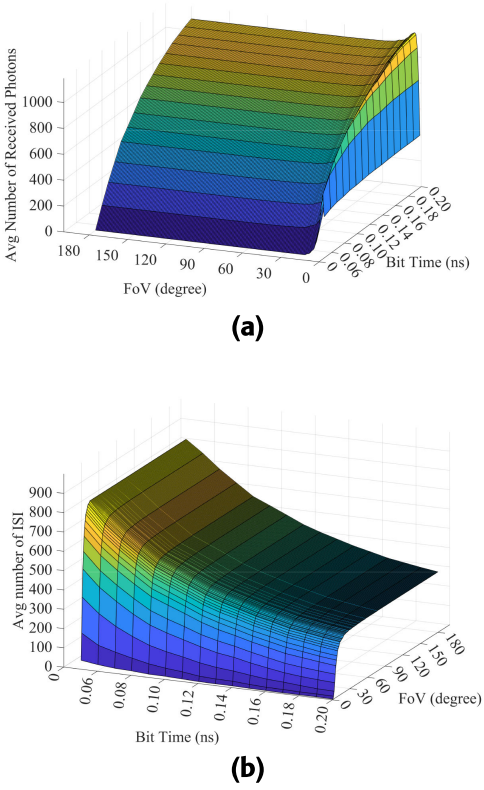


FIGURE 4. Effect of bit time and FoV on the a) average number of received photons, b) average number of ISI.

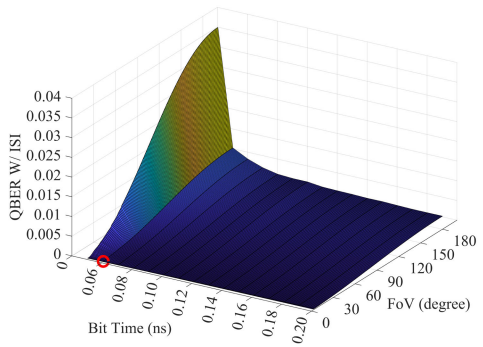


FIGURE 5. QBER versus bit time and FoV for optimized gate time.

B. OPTIMIZATION RESULTS

In our simulation study, we generate 3×10^7 photons that travel from the transmitter to the receiver through the underwater channel. For each scenario, we consider the interdependency of bit time and FoV and analyze the joint effect of them on the QBER performance to determine their appropriate values.

As the first example, we consider a scenario where we assume coastal water, $\theta_{0,\max}$ =20°, r_0=3 mm, and A = 20 cm. In order to highlight the tradeoff between ISI and noise, we investigate the propagation delay of received photons for various link distances. Fig. 3 presents the CDF of received photons for L=10, 20, 30, and 40 meters under the assumption of using a FoV of Ω=180°. It is observed that propagation times for 99% of the received photons for link lengths of L=10, 20, 30, and 40 m, are respectively Δt =0.11, 0.68, 1.7, and 3.3 nanoseconds (ns). By increasing the threshold from the 99% to the 99.9%, the required bit time values increase to Δt=0.8, 3.5, 7.5, and 10.5 ns. Determining the bit time based on the threshold of 99.9% of photons instead of 99% of photons can reduce the probability of ISI

occurrences. However, the significant increase in the bit time leads to much higher dark noise.

In our above example, we consider FoV of $\Omega = 180°$ to account for the worst case of ISI. In Fig.4, we illustrate the influence of both the bit time and the FoV on the reception count and the occurrences of ISI for a link length of $L = 40$ m. It is evident from Fig. 4a that by increasing the bit time, the count of received photons (see Fig. 4b) increases as the ISI decreases. As expected, increasing the FoV also increases the number of received photons. However, after a certain value of FoV, the number of received photons decreases as the count of ISI increases. For example, consider a bit time of $\Delta t = 0.05$ ns. It is observed from Fig. 4a that the maximum number of received photons is 482 and achieved with a FoV of $\Omega = 2°$. However, with a further increase in FoV, the reception count steadily declines, ultimately reaching zero at a FoV of $\Omega = 10°$. The decrease in photon reception with an increase in FoV can be explained by referring to Fig. 4b. Due to the short bit time of $\Delta t = 0.05$ ns considered in this example, the system experiences high ISI. Expanding the FoV for this particular bit time leads to more photons reaching the receiver plane, and this results in increase of ISI, ultimately corrupting all received photons at the FoV of $\Omega = 10°$. In summary, increasing the FoV necessitates the selection of a longer bit time value. However, failing to properly adjust the bit time when expanding the FoV leads to a rise in ISI levels, potentially causing the system performance to deteriorate to the point of non-functionality.

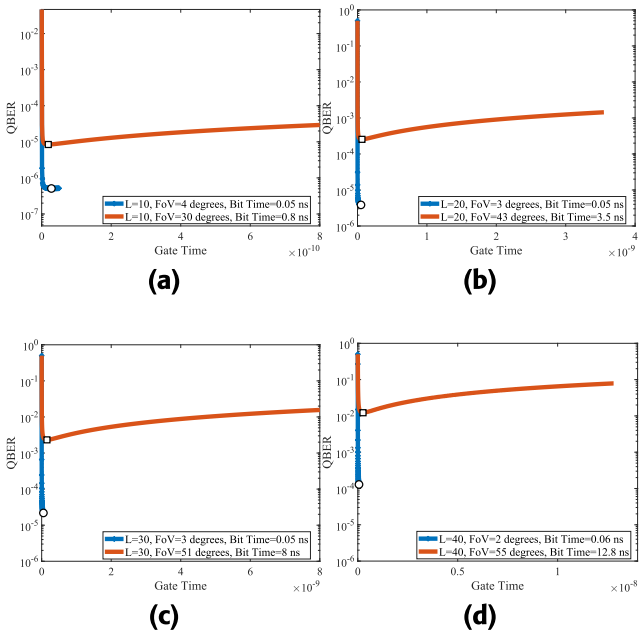


FIGURE 6. QBER performance with respect to the gate time for link distances of (a) L = 10 m, (b) L = 20 m, (c) L = 30 m, and (d) L = 40 m.

In Fig. 5, we illustrate the combined effect of bit time, FoV, and gate time on the QBER performance while the ISI is taken into account. We assume a link length of L = 40 m. For each selected bit time and FoV, the optimized gate time is determined through the exhaustive search and is used to calculate the corresponding QBER. The interdependency of optimum bit time and FoV values can be realized by assessing the figure. For example, for a $\Omega = 1°$, the optimum bit time (in sense of QBER minimization) is $\Delta t = 0.05$ ns. For a FoV of $\Omega = 10°$, the optimum bit time shifts to $\Delta t = 0.13$ ns. For $\Delta t = 0.05$ ns, increasing the FoV significantly reduces the number of received photons as a result of ISI, and the QBER reaches around 0.046 for $\Omega = 180°$. This implies that the system requires a larger bit time if a larger FoV will be selected to avoid performance degradation. The red circle in the figure indicates the optimal point where the joint selection of bit time and FoV results in the minimum QBER. The bit time and FoV corresponding to this optimal point are $\Delta t = 0.06$ ns and $\Omega = 2°$, respectively, and the corresponding minimum QBER value is 1.25×10^{-4}.

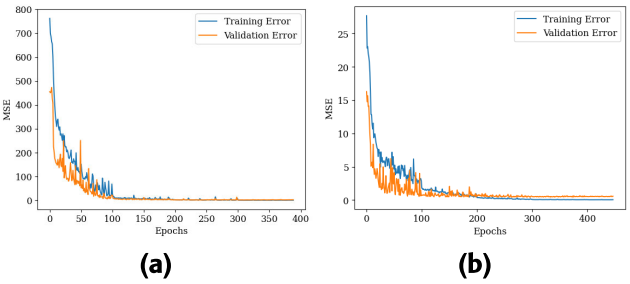


FIGURE 7. MSE for a) bit time, b) FoV.

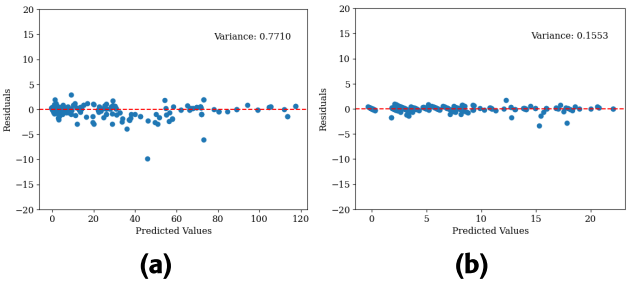


FIGURE 8. Residual for a) bit time, b) FoV.

In Fig. 6, we present the QBER as a function of gate time and provide a comparison of the achieved performance in our study with that reported in [20] for various link distances. Note that the attained QBER values in [20] for link lengths of L=10, 20, 30, and 40 meters, are respectively 8.4×10^{-6}, 2.5×10^{-4}, 2.2×10^{-3}, and 1.0×10^{-2}. In our case, for the same link lengths, we achieve QBER values of 5×10^{-7}, 3.8×10^{-6}, 2.1×10^{-5}, and 1.2×10^{-4}, respectively, indicating significant improvements up to 2 order magnitudes. Specifically, in our study, we are able to transmit a larger proportion of photons in a shorter time interval with judicious choices of bit time and FoV, thereby significantly enhancing the system's efficiency. Specifically, in our study, we use optimized bit times of Δt =0.05, 0.05, 0.05, and 0.06 ns for link lengths of $L = 10$, 20, 30, and

40 meters. The corresponding dark current noise for $I_{dc} = 60$ Hz are calculated as $n_D = 3 \times 10^{-9}$, 3×10^{-9}, 3×10^{-9}, and 3.6×10^{-9}. The irradiance background noise with the optimized FoVs of $\Omega = 4°$, $3°$, $3°$, and $2°$ and optimized gate time values of $\Delta t' = 28$, 50, 50, and 60 picoseconds (ps) can be further calculated as $n_B = 9 \times 10^{-11}$, 9.1×10^{-11}, 9.1×10^{-11}, and 4.85×10^{-11}, respectively, for $L =$ 10, 20, 30, and 40 meters. In comparison, the utilized bit times in [20] are Δt =0.8, 3.5, 7.5, and 10.5 ns for the corresponding link lengths. The dark current noise levels for $I_{dc} = 60$ Hz are measured as $n_D = 4.8 \times 10^{-8}$, 2.1×10^{-7}, 4.5×10^{-7}, and 6.3×10^{-7} in [20] while the irradiance background noise are $n_B = 3.3 \times 10^{-9}$, 2.2×10^{-8}, 7.3×10^{-8}, and 1.3×10^{-7}. In comparison to [20], it is observed that our judiciously selected values of bit time result in significant reductions of the dark current noise and irradiance background noise values eventually leading to a better QBER performance.

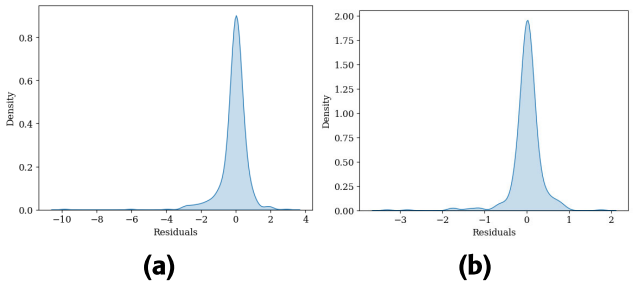


FIGURE 9. Density of residuals for a) bit time, b) FoV.

The optimization process described up to here is applied for each of the samples in the dataset and corresponding values of bit time and FoV are recorded for the training process of DNN. The optimization resolution for the bit time is set at 1 ps, and for the FoV, it is $\frac{\pi}{720}$. In the training process, in addition to the necessity of including samples from all water types without skewing towards any particular type, ensuring that the link length samples are nearly uniformly distributed across their range, without high bias towards excluding any segment of the range, helps maintain consistent model performance, with no significant changes across different folds in k-fold cross-validation. In Fig.7a and Fig.7b, we depict MSE with respect to epochs for bit time and FoV, respectively. Furthermore, the R-squared criterion reaches above 0.99 for both bit time and FoV. Our model achieves an average MSE value of less than 1.5 for bit time, and 0.5 for FoV on the test data. The overall behavior of MSE curve illustrates the efficiency of the deep learning model without experiencing overfitting or high bias. The slight fluctuations in the curves are as a result of utilizing mini-batch gradient descent. This indicates that the model is estimated to capture 99% of variation in the dependent variables and is therefore able to effectively explain the underlying relationship between variables. Fig.8a and Fig.8b illustrate the associated residual plots. These demonstrate that the variance of residuals from the fitted model is around 0.77 ps for the bit time and $0.15 \times \frac{\pi}{720}$ for the FoV. Finally, Fig.9a and Fig.9b present the PDF of residuals. They demonstrate that the density of residuals around zero is high and the residuals approximate the normal distribution in both cases.

VI. CONCLUSION

In this paper, we have investigated the impact of bit time, FoV, and gate time on the QBER performance of an underwater QKD system in the presence of ISI. The optimal bit time and FoV were selected with the goal of minimizing QBER based on the propagation delay and angle of arrival, respectively. For the optimization, we take into account the interdependency between bit time and FoV, and struck a balance between the number of photon arrivals and background noise, aiming to reduce the QBER. Finally for the selected values of bit time and FoV and a given propagation environment, we optimized the SPAD gate time in terms of minimizing the QBER. For optimization purposes, we built a dataset to leverage on-board deep learning techniques to instantly predict optimal bit time and FoV for a given set of system parameters and propagation environment. Our simulation results indicate that conducting interdependency analysis between parameters and considering background photons during the optimization process leads to significant improvements in QBER.

ACKNOWLEDGMENT

The author Mostafa Nozari would like to extend his sincere appreciation to Amir Hossein Fahim Raouf with his help in the initial simulations.

REFERENCES

[1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.
[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.
[3] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.
[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.
[5] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over FSO: Current development and future perspectives," in *Proc. Prog. Electromagn. Res. Symp.*, 2018, pp. 1672–1679.
[6] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 58–69, Feb. 2022.
[7] S.-C. Zhao, X.-H. Han, Y. Xiao, Y. Shen, Y.-J. Gu, and W.-D. Li, "Performance of underwater quantum key distribution with polarization encoding," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 36, no. 5, p. 883, 2019.
[8] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE J. Ocean. Eng.*, vol. 45, no. 3, pp. 1138–1147, Jul. 2020.
[9] Y. Guo, C. Xie, P. Huang, J. Li, L. Zhang, D. Huang, and G. Zeng, "Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 97, no. 5, May 2018, Art. no. 052326.

[10] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Exp.*, vol. 27, no. 3, p. 3055, 2019.
[11] A. H. Fahim Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 37, no. 2, p. 564, 2020.
[12] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Opt. Exp.*, vol. 26, no. 17, p. 22563, 2018.
[13] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, and E. Karimi, "Characterization of an underwater channel for quantum communications in the Ottawa river," *Opt. Exp.*, vol. 27, no. 19, p. 26346, 2019.
[14] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of decoy state quantum key distribution over underwater turbulence channels," *J. Opt. Soc. Amer. B*, vol. 39, no. 6, p. 1470, 2022.
[15] J. Gariano, I. B. Djordjecvic, and Y. Xiang, "Simulation of a submarine to submarine QKD system," in *Quantum Information Science and Technology IV*, vol. 10803. Bellingham, WA, USA: SPIE, 2018, pp. 14–21.
[16] W. Zhao, R. Shi, X. Ruan, Y. Guo, Y. Mao, and Y. Feng, "Monte Carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel," *Quantum Inf. Process.*, vol. 21, no. 5, p. 186, May 2022.
[17] A. H. Fahim Raouf, M. Safari, and M. Uysal, "Multi-hop quantum key distribution with passive relays over underwater turbulence channels," *J. Opt. Soc. Amer. B*, vol. 37, no. 12, p. 3614, 2020.
[18] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Sci. Appl.*, vol. 4, no. 5, pp. e286–e286, May 2015.
[19] S. Jiang, W. O. Popoola, and M. Safari, "Quantum key distribution using time-gated spads over turbid underwater channels," in *CLEO: Applications and Technology*. Washington, DC, USA: Optica Publishing Group, 2021.
[20] A. H. Fahim Raouf and M. Uysal, "On the optimization of underwater quantum key distribution systems with time-gated SPADs," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 39, no. 8, p. 2013, 2022.
[21] H. V. Nguyen, P. V. Trinh, A. T. Pham, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "Network coding aided cooperative quantum key distribution over free-space optical channels," *IEEE Access*, vol. 5, pp. 12301–12317, 2017.
[22] M. Lanzagorta, *Underwater Communications*. San Rafael, CA, USA: Morgan & Claypool, 2012.
[23] B. Liu and B. Liu, "Supervised learning," in *Web Data Mining: Exploring Hyperlinks, Contents, Usage Data*. Cham, Switzerland: Springer, 2011, pp. 63–132.
[24] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533–536, Oct. 1986.
[25] E. Akleman, "Deep learning," *Computer*, vol. 53, no. 9, pp. 1–17, Sep. 2020.
[26] Z. Lee, K. Du, and R. Arnone, "A model for the diffuse attenuation coefficient of downwelling irradiance," *J. Geophys. Res., Oceans*, vol. 110, no. 2, pp. 1–26, Feb. 2005.
[27] C. Gabriel, M.-A. Khalighi, S. Bourennane, P. Leon, and V. Rigaud, "Monte-Carlo-based channel characterization for underwater optical communication systems," *J. Opt. Commun. Netw.*, vol. 5, no. 1, pp. 1–12, Jan. 2013.
[28] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.
[29] L. Prechelt, "Early stopping–but when?" in *Neural Networks: Tricks of the Trade*. Cham, Switzerland: Springer, 1998, pp. 55–69.
[30] A. Gulli and S. Pal, *Deep Learning With Keras*. Maharashtra, India: Packt Publishing, 2017.
[31] R. Christensen, *Log-Linear Models and Logistic Regression*. Cham, Switzerland: Springer, 2006.



MOSTAFA NOZARI (Student Member, IEEE) received the degree in telecommunication engineering from Isfahan University of Technology (IUT). In 2021, he joined the Communication Theory and Technologies (CT&T) Research Group, Özyeğin University, Istanbul, Türkiye. His research interests include wireless communication/networks and machine learning (ML).



MURAT UYSAL (Fellow, IEEE) received the B.Sc. and M.Sc. degrees in electronics and communication engineering from Istanbul Technical University, Istanbul, Türkiye, in 1995 and 1998, respectively, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2001.

He began his academic career as an Assistant Professor with the University of Waterloo, Canada, in 2002, and was promoted to an Associate Professor with tenure, in 2007. In 2011, he joined Özyeğin University, Türkiye, where he served as the Department Chair of the Electrical and Electronics Engineering and the Founding Director of the Center of Excellence, Optical Wireless Communication Technologies (OKATEM). Since 2023, he has been with New York University Abu Dhabi as a Professor of electrical engineering. His research interests include communication theory with a particular emphasis on the physical layer aspects of wireless communication systems in radio and optical frequency bands. On these topics, he has authored some 400 journal articles and conference papers and received more than 20,000 citations with an H-index of 65.

Dr. Uysal's major distinctions, including the NSERC Discovery Accelerator Award, in 2008; the University of Waterloo Engineering Research Excellence Award, in 2010; Turkish Academy of Sciences Distinguished Young Scientist Award, in 2011; Özyeğin University Outstanding Researcher Award, in 2014; the National Instruments Engineering Impact Award, in 2017; the Elginkan Foundation Technology Award, in 2018; the IEEE Communications Society Best Survey Paper Award, in 2019; the IEEE Turkey Section Outstanding Service Award, in 2021; and the Mustafa Prize and Tubitak Science Award, in 2023. He is the former Chair of the IEEE Turkey Section. He was involved in the organization of several IEEE conferences at various levels. In particular, he served as the Technical Program Committee Chair for major IEEE conferences, including WCNC 2014, PIMRC 2019, and VTC-Fall 2019. From 2011 to 2015, he was the Chair of the EU COST Action OPTICWISE, a high-profile consolidated European scientific platform which brought together more than 150 researchers in the research area of optical wireless communication. He serves as an Area Editor for IEEE TRANSACTIONS ON COMMUNICATIONS. In past, he served as an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE COMMUNICATIONS LETTERS.