Multi-hop quantum key distribution with passive relays over underwater turbulence channels

Multi-Hop Quantum Key Distribution with Passive Relays over Underwater Turbulence Channels*

Amir Hossein Fahim Raouf, *Student Member, IEEE,*
Majid Safari, *Member, IEEE,* Murat Uysal, *Fellow, IEEE*

Abstract

Absorption, scattering, and turbulence experienced in underwater channels severely limit the range of quantum communication links. In this paper, as a potential solution to overcome range limitations, we investigate a multi-hop underwater quantum key distribution (QKD) where intermediate nodes between the source and destination nodes help the key distribution. We consider the deployment of passive relays which simply redirect the qubits to the next relay node or the receiver without any measurement. Based on the near-field analysis, we present the performance of relay-assisted QKD scheme in terms of quantum bit error rate and secret key rate in different water types and turbulence conditions. We further investigate the effect of system parameters such as aperture size and detector field-of-view on the performance. Our results demonstrate under what conditions relay-assisted QKD can be beneficial and what end-to-end transmission distances can be supported with a multi-hop underwater QKD system.

I. Introduction

Today's cryptosystems such as widely deployed RSA and elliptic curve-based schemes build upon the formulation of some intractable computational problems. They are able to offer only computational security within the limitations of conventional computing power. Recent advances in the quantum computing towards the so-called quantum supremacy have the potential to eventually break such classical cryptosystems [1], [2]. Unlike conventional counterparts, quantum

*This paper is presented in part at IEEE/IET International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) July 2020, which was held as a virtual conference.

cryptography builds upon the laws of quantum mechanics and provides a radically different solution for key distribution promising unconditional security [3].

In the current literature, most works on QKD focus on fiber optic, atmospheric and satellite links [4]. Another potential area of QKD is underwater communications. In particular, quantum-secure communication is desired for military applications such as submarine-to-submarine communication or for underwater sensor networks deployed for harbor/maritime surveillance in critical areas. There have been some recent research efforts on underwater QKD [5]–[14]. In particular, the quantum bit error rate (QBER) and secret key rate (SKR) of well-known BB84 protocol were studied in [8], [14]. The performance of other QKD protocols such as entanglement [13] and decoy state [6] were further investigated in underwater environments. In addition to these theoretical and simulation studies, experimental works were also conducted to demonstrate the feasibility of underwater QKD [7], [10]–[12].

The above experimental and theoretical studies point out that performance degradation due to absorption, scattering, and turbulence experienced in underwater channels severely limit the range of quantum communication links. In this paper, as a potential solution to overcome range limitations, we investigate relay-assisted underwater QKD where intermediate nodes between the source and destination nodes help the key distribution. The concept of relay-assisted QKD was earlier studied for atmospheric, fiber and satellite links [15]–[17], however those results are not directly applicable to underwater communications which features inherent differences. Underwater optical communication suffers from severe absorption and scattering due to the inevitable photon interactions with the water molecules and other particles in solution and suspension in water. The maximum transmission distance depends on the type of water and concentration of dissolved particles therein. Furthermore, the operation wavelength is typically in the blue and green spectrum which is distinct from those of free space and fiber optic communications. Therefore, it remains an open question to find out if relay-assisted transmission is beneficial in such a harsh propagation environment and what end-to-end transmission distances can be supported with a multi-hop underwater QKD system. To the best of our knowledge, this is the first paper which attempts to analyze the relay-assisted underwater QKD systems.

In this paper, we consider a multi-hop underwater QKD system where relay nodes are utilized along the path connecting two legitimate parties. Unlike classical optical communication systems [18], amplify-and-forward and detect-and-forward relaying cannot be used in QKD since any type of measurement modifies the quantum state [3]. To address this, we utilize passive relays

[17] which simply redirect the qubits to the next relay node or to the destination node without performing any measurement or detection process. Under the assumption of passive relays and based on a near-field analysis [19] over underwater turbulence channels, we derive an upper bound on QBER and a lower bound on SKR. Based on these bounds, we present the performance of underwater QKD in different water types and different levels of turbulence strength. We further investigate the effect of system parameters such as detector field-of-view (FOV) and aperture size on the system performance. Our results demonstrate that the multi-hop schemes with judiciously selected values of relay number, FOV size and aperture size successfully improve the end-to-end distance in water types with low turbidity.

The remainder of this paper is organized as follows. In Section II, we describe our relay-assisted system model based on BB84 QKD protocol. In Section III, we derive an upper bound on the QBER and a lower bound on the SKR of the system. In Section IV, we present numerical results and finally, we conclude in Section V.

II. System Model

We consider a relay-assisted underwater QKD system with K serial passive relay nodes over a link distance of L. As illustrated in Fig. 1, Alice (transmitter) with a diameter size of d is placed in $z = 0$ plane. Relay nodes and Bob (receiver) with the same diameter size of d are located in the $z = L_i$. The consecutive nodes in the serial scheme are placed equidistant along the path from the source to the destination. Therefore, the length of each hop is equal to $l = L/(K + 1)$.

The QKD system is built upon BB84 protocol [20] which aims to create a secret key between the authorized partners (Alice and Bob) such that eavesdropper (Eve) fails to acquire meaningful information. BB84 protocol is based on the principle of polarization encoding. In this protocol, Alice prepares a qubit by choosing randomly between two linear polarization bases namely rectilinear (denoted by $\oplus$) or diagonal (denoted by $\otimes$) for every bit she wants to send. She selects a random bit value "0" or "1" and uses polarization encoding of photons where polarization of $0°/-45°$ represents 0 and polarization of $+90°/+45°$ represents 1. At the receiver side, Bob measures the arriving photon randomly in either $\oplus$ or $\otimes$ bases. Alice and Bob determine the secure key with respect to the received qubits at the "sift" events. Sift events occurs at the bit intervals in which exactly one of the single photon detectors registers a count and both Alice and Bob have chosen the same basis. Alice and Bob can recognize the sift events by transferring information over a public classical communication channel (underwater optical

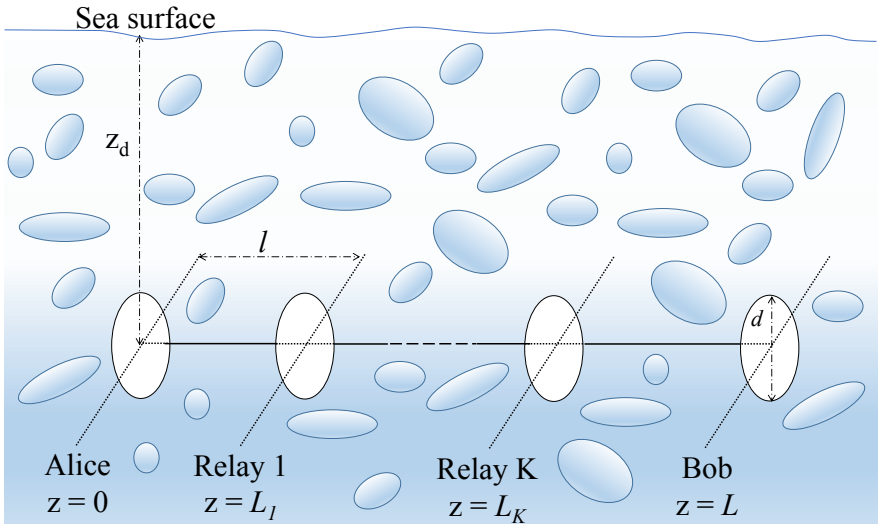


Fig. 1: Schematic diagram of the underwater relay-assisted QKD system with K relay nodes.

channel in our case). Based on the sifted qubits, a shared one-time pad key is created to use for secure communication [21].

Alice generates each qubit with an average photon number of n_S which is encoded with the corresponding polarization state of the qubit for a randomly chosen basis. As a result of underwater path loss and turbulence, the i^{th} relay ($i = 1, \ldots, K$) collects only a random fraction γ_i of the transmitted photons. Under the assumption of identical transmitter/receiver sizes and equidistant placement, we can simply write $\gamma_1 = \gamma_2 = ... = \gamma_K = \gamma$. The relay node forwards the captured photons to the next relay (or Bob) by redirecting the light beam and without any measurements. Therefore, Bob will collect an overall fraction $\gamma_{Bob} = \gamma^{K+1}$ of the originally transmitted photons from Alice.

In addition to the received photons from the source, receiver of each relay node will collect some background noise. The total average number of background photons per polarization at the i^{th} relay can be therefore expressed as

$$n_{B_i} = n_{B0} + n_{B0}\gamma + n_{B0}\gamma^2 + \ldots + n_{B0}\gamma^{i-1} \tag{1}$$

The accumulated background photons at Bob's receiver becomes [17]

$$n_B = n_{B0}\frac{1-\gamma^{K+1}}{1-\gamma} \tag{2}$$

Beside background noise, each of Bob's detectors will collect dark current noise. Let I_{dc} and Δt denote the dark current count rate and the bit period, respectively. The average number of

dark counts is given by $n_D = I_{dc}\Delta t$. Thus, the average number of noise photons reaching each Bob's detector can be obtained by $n_N = n_B/2 + n_D$. It should be noted that since the relays just redirect the photons, they do not increase the dark current.

III. Performance Analysis

In this section, we investigate the performance of the underwater QKD system through the derivation of an upper bound on QBER and a lower bound on the SKR.

A. QBER Analysis

QBER is the ratio of probabilities of sift and error which depend on the statistical characteristics of the capture fraction γ (i.e., received fraction of transmitted photons). The capture fraction can be obtained based on the extended Huygens-Fresnel principle [19]. As discussed in [19], in order to calculate the received field, we need to determine the paraxial Green's function which is a function of the complex phase perturbation of the field describing the turbulence of the path. To make the analysis mathematically tractable, Green's function can be replaced with an equivalent set of fictitious parallel channels by normal mode decomposition. Let $\hat{\mu}$ denote the largest eigenvalue. This is also called as "power transfer" in [17], [22] and defines the probability of transmitted photon being reliably received in the presence of turbulence. The statistical description of $\hat{\mu}$ is unfortunately not available in the literature. As an alternative, an upper bound on QBER was presented in [17] using an upper bound on the noise count and a lower bound on the maximum average power transfer, i.e., $\mu \triangleq \mathrm{E}\left[\hat{\mu}\right]$. Specifically, this is given by

$$\mathrm{QBER} \leq \frac{2\eta\hat{n}_N \exp\left[-\eta 4\hat{n}_N\right]\left(1-\mu^{K+1}+\exp\left[-\eta n_S h^{K+1}\left(l\right)\right]\mu^{K+1}\right)}{b\exp\left[-b\right]\left(1-c\right)+\left(a+b\right)\exp\left[-\left(a+b\right)\right]c} \tag{3}$$

In (3), η is the quantum efficiency of Geiger-mode avalanche photodiodes (APDs), $\mu \triangleq \mathrm{E}\left[\hat{\mu}\right]$ is the average power transfer and $\hat{n}_N$ is an upper bound on the noise count, i.e., $n_N \leq \hat{n}_N$, whose derivation will be elaborated later. In (3), a, b and c are respectively defined by

$$a = \eta\left[n_S h^{K+1}\left(l\right) + 2n_{B0}\left(\frac{1-h^{K+1}\left(l\right)}{1-h\left(l\right)} - 1\right)\right] \tag{4}$$

$$b = \eta\left(2n_{B0} + 4n_D\right) \tag{5}$$

$$c = \frac{n_S(\mu h\left(l\right))^{K+1} + 2n_{B0}\left(\frac{1-(\mu h(l))^{K+1}}{1-\mu h(l)} - 1\right)}{n_S h^{K+1}\left(l\right) + 2n_{B0}\left(\frac{1-h^{K+1}(l)}{1-h(l)} - 1\right)} \tag{6}$$

The calculation of $h\left(l\right)$, μ and $\hat{n}_N$ depends on the operation environment and therefore earlier results in the literature reported for other propagation environments [17] are not applicable. In the following, we elaborate on their calculations for the underwater channel under consideration.

Underwater path loss: For collimated light sources, the geometrical loss is negligible; therefore, the path loss for a laser diode transmitter only depends on the attenuation loss including the effects of absorption and scattering. Based on the modified version of Beer-Lambert formula [23], the underwater path loss can be expressed as

$$h\left(l\right)=\exp\left[-\varsigma l\left(\frac{d}{\theta l}\right)^{T}\right] \tag{7}$$

where ς is extinction coefficient, l is transmission distance, θ is the full-width transmitter beam divergence angle and T is a correction coefficient based on water type [23]. Extinction coefficient depends on the wavelength and water type. Typical values of extinction coefficients for $\lambda=532$ nm (green color) in different water types can be found in [24].

Underwater average power transfer: The average power transfer for each hop (i.e., a distance of l over turbulent path) can be expressed as [19]

$$\mu=\frac{8\sqrt{F}}{\pi}\int_{0}^{1}e^{\left(\frac{-W\left(dx,l\right)}{2}\right)}\left(\cos^{-1}\left(x\right)-x\sqrt{1-x^{2}}\right)J_{1}\left(4x\sqrt{F}\right)dx \tag{8}$$

where $J_1\left(\cdot\right)$ is the first-order Bessel function of the first kind and F is the Fresnel number product of transmit and receive diameters given by $F=\left(\pi d^2/4\lambda l\right)^2$. In (8), $W\left(\cdot,\cdot\right)$ is the underwater wave structure function. For a given transmission distance of l and given separation distance between two points on the phase front transverse to the axis of propagation (denoted by ρ), it is expressed as [14]

$$\begin{aligned}W\left(\rho,l\right)=&1.44\pi k^2 l\left(\frac{\alpha^2\chi}{\omega^2}\right)\varepsilon^{-\frac{1}{3}}\left(1.175\eta_K^{2/3}\rho+0.419\rho^{\frac{5}{3}}\right)\\&\times\left(\omega^2+d_r-\omega\left(d_r+1\right)\right)\end{aligned} \tag{9}$$

where $k=2\pi/\lambda$ is the wave number, ω is the relative strength of temperature and salinity fluctuations, ε is the dissipation rate of turbulent kinetic energy per unit mass of fluid, α is the thermal expansion coefficient, χ is the dissipation rate of mean-squared temperature and d_r is the eddy diffusivity ratio. In (9), η_K is Kolmogorov microscale length and given by $\eta_K=\left(\upsilon^3/\varepsilon\right)^{1/4}$ with υ referring to the kinematic viscosity.

Underwater noise count: In an underwater environment, the primary source of noise is the refracted sunlight from the surface of the water. Let $R_d(\lambda, z_d)$ denote the irradiance of the underwater environment as a function of wavelength and underwater depth. With respect to sea surface (i.e., $z_d = 0$), it can be written as $R_d(\lambda, z_d) = R_d(\lambda, 0)\, e^{-K_\infty z_d}$ where K_∞ is the asymptotic value of the spectral diffuse attenuation coefficient for spectral down-welling plane irradiance [25]. The background photons per polarization on average can be then given by [26]

$$n_{B0} = \frac{\pi R_d A \Delta t' \lambda \Delta\lambda \left(1 - \cos(\Omega)\right)}{2 h_p c_0} \tag{10}$$

where A is the receiver aperture area, Ω is the FOV of the detector, h_p is Planck's constant, c_0 is the speed of light, $\Delta\lambda$ is the filter spectral width, and $\Delta t'$ is the receiver gate time. Ignoring the effect of turbulence (i.e., $\hat{\mu} = 1$) on the redirected background photons coming from relays [17], an upper bound on the noise count at each of Bob's four detectors can be obtained as

$$\hat{n}_N = \frac{n_{B0}}{2} \left(\frac{1 - \exp\left[-\varsigma L^{1-T} \left(\frac{d(K+1)}{\theta} \right)^T \right]}{1 - \exp\left[-\varsigma \left(\frac{L}{K+1} \right)^{1-T} \left(\frac{d}{\theta} \right)^T \right]} \right) + n_D \tag{11}$$

Replacing (7), (8) and (11) in (3), we can obtain the upper bound on QBER for underwater environments.

Special case: As a sanity check, consider $K = 0$ (i.e., no relay). Therefore, $\hat{n}_N$, a, and c can be simplified as $\hat{n}_N = n_{B0}/2 + n_D = b/4\eta$, $a = \eta n_S h(L)$ and $c = \mu_L$. Replacing these in (3) yields

$$\text{QBER} \leq \frac{\hat{n}_N \left[1 - \mu_L + \mu_L e^{-\eta n_S h(L)} \right]}{\frac{n_S \mu_L h(L)}{2} e^{-\eta n_S h(L)} + 2\hat{n}_N [1 - \mu_L + \mu_L e^{-\eta n_S h(L)}]} \tag{12}$$

where $h(L)$ and μ_L are respectively the path loss and the average power transfer for the length of direct link connecting Alice and Bob. It can be readily checked that this result coincides with [Eq. (4), 14] which was earlier reported for underwater QKD link.

B. SKR Analysis

SKR is the difference between the amount of information shared by Alice and Bob and the amount of residual information that Eve might have [27]. In SKR analysis, the quantum channel in BB84 protocol can be modeled as a binary symmetric channel where QBER defines the crossover probability. The minimum amount of information that should be sent from Alice to Bob in order to correct his key string can be described by the entropy function

$H\left(\mathrm{QBER}\right)=-\mathrm{QBER}\log_2\left(\mathrm{QBER}\right)-\left(1-\mathrm{QBER}\right)\log_2\left(1-\mathrm{QBER}\right)$. The amount of disclosed information to Eve can be then expressed as $1-H\left(\mathrm{QBER}\right)$ [28]. In practice, the effect of error correction should be further taken into account. Therefore, we can write the SKR as

$$R=1-H(\mathrm{QBER})-f\times H(\mathrm{QBER}) \tag{13}$$

where $f>1$ is the reconciliation efficiency of the error correction scheme [28].

In this paper, we adopt low-density parity check (LDPC) codes optimized for BSCs [28] with a reconciliation efficiency of $f=\left(1-R_c\right)/H\left(\mathrm{QBER}_{th}\right)$ [29]. Here, R_c denotes the code rate and QBER_{th} is a threshold value preset in LDPC code design [30]. Replacing the definition of f and the upper bound on QBER given by (3) in (13), we obtain a lower bound for the SKR as

$$R\geq 1-\left(1+\frac{1-R_c}{H\left(\mathrm{QBER}_{th}\right)}\right)H\left(\frac{\eta\hat{n}_N\exp\left[-\eta 4\hat{n}_N\right]\left(1-\mu^{K+1}+\mu^{K+1}\exp\left[-\eta n_S h^{K+1}\left(l\right)\right]\right)}{\frac{b}{2}\exp\left[-b\right]\left(1-c\right)+\left(\frac{a+b}{2}\right)\exp\left[-\left(a+b\right)\right]c}\right) \tag{14}$$

IV. Numerical Results

In this section, we demonstrate the performance of relay-assisted underwater QKD scheme under consideration in terms of QBER and SKR. We assume the transmitter beam divergence angle of $\theta=6^\circ$, dark current count rate of $I_{dc}=60$ Hz, filter spectral width of $\Delta\lambda=30$ nm, bit period of $\Delta t=35$ ns, receiver gate time of $\Delta t'=200$ ps, average photon number of $n_S=1$, and Geiger-Mode APD quantum efficiency of $\eta=0.5$. Unless otherwise stated, we assume the transmitter and receiver aperture diameters of $d=5$ cm, FOV of $\Omega=180^\circ$, a depth of $z_d=100$ m and clear atmospheric conditions at night with a full moon. The typical total irradiances at sea level, i.e., $R_d\left(\lambda,0\right)$, in the visible wavelength band for some typical atmospheric conditions are provided in [31]. As for channel parameters, we assume $\alpha=2.56\times10^{-4}\,1/\mathrm{deg}$ and $\upsilon=1.0576\times10^{-6}\,\mathrm{m^2s^{-1}}$. We consider two representative cases for turbulence strength. Specifically, we assume $\omega=-2.2$, $\chi_T=10^{-6}\,\mathrm{K^2s^{-3}}$ and $\varepsilon=5\times10^{-7}\mathrm{m^2s^{-3}}$ for moderate turbulence and $\omega=-2.2$, $\chi_T=10^{-5}\,\mathrm{K^2s^{-3}}$ and $\varepsilon=10^{-5}\,\mathrm{m^2s^{-3}}$ [32]. For the convenience of the reader, the channel and system parameters are summarized in Table I.

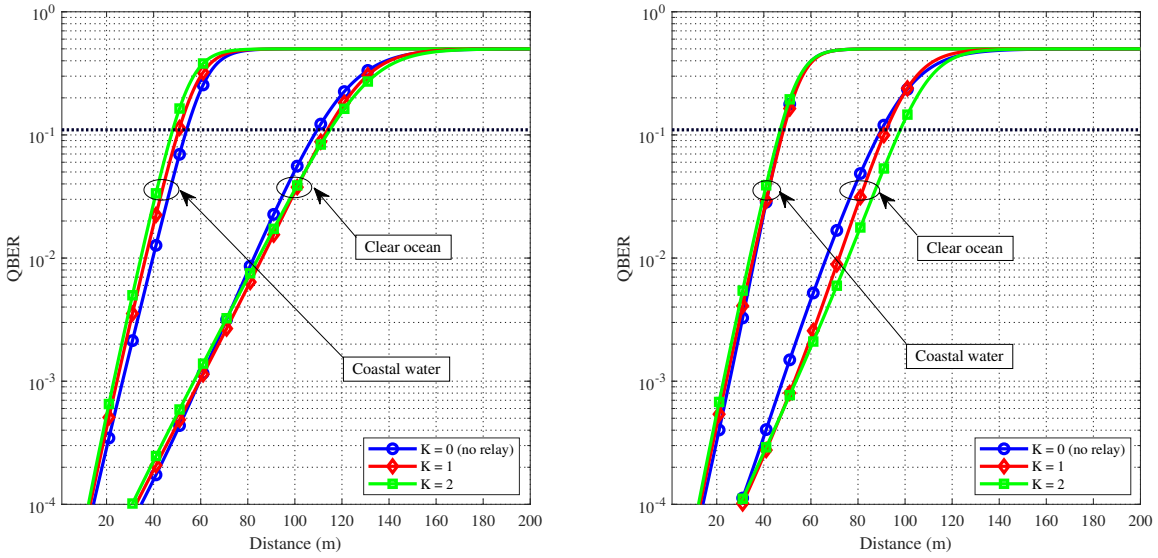
TABLE I: System and channel parameters

Parameter	Definition		Numerical Value
Ω	Field of view		180° [23]
$\Delta\lambda$	Filter spectral width		30 nm [14]
λ	Wavelength		530 nm [23]
Δt	Bit period		35 ns [26]
$\Delta t'$	Receiver gate time		200 ps [26]
d	Transmitter aperture diameter		5 cm [19]
d'	Receiver aperture diameter		5 cm [19]
η	Quantum efficiency		0.5 [19]
I_{dc}	Dark current count rate		60 Hz [26]
K_∞	Asymptotic diffuse attenuation coefficient		0.08 m^{-1} [25]
z_d	Depth		100 m [26]
θ	Transmitter beam divergence angle		6° [23]
ς	Extinction coefficient	Clear water	0.151 m^{-1} [24]
		Coastal water	0.339 m^{-1} [24]
T	Correction coefficient	$\theta = 6^\circ,\ d_1 = 5\,\mathrm{cm}$	0.13 [23]
		$\theta = 6^\circ,\ d_1 = 10\,\mathrm{cm}$	0.16 [23]
		$\theta = 6^\circ,\ d_1 = 20\,\mathrm{cm}$	0.21 [23]
		$\theta = 6^\circ,\ d_1 = 30\,\mathrm{cm}$	0.26 [23]

In Fig. 2, we illustrate the performance of QBER with respect to end-to-end link distance assuming different water types (based on turbidity level[1]) and turbulence conditions. In our simulations, we consider clear ocean and coastal water whose extinction coefficients are 0.151 m^{-1} and 0.339 m^{-1}, respectively. We consider relay-assisted systems with $K = 1$, and 2 relay nodes. The results for direct link, i.e. $K = 0$, are further included as benchmarks.

It is observed from Fig. 2 that relaying is not beneficial and even detrimental in turbid water (coastal water). To understand the reasons behind this, it should be noted that there is a fundamental trade-off between accumulated noise and the average number of collected photons coming from Alice. Adding passive relay leads to additional collected background noise redirected from relays to Bob's receiver. Although shorter hops decrease the photon loss caused by turbulence, it is not always able to mitigate the exponential loss of photons due to the path loss. Specifically, in turbid water where the value of the extinction coefficient is large, the turbulence effect on the QBER performance becomes insignificant with respect to the path loss.

[1]Turbid water results in large extinction coefficient value while the extinction coefficient in non-turbid water takes small values. Based on typical chlorophyll concentrations, pure sea and clear ocean are considered as non-turbid water and the coastal and harbor can be considered as turbid water.



(a) (b)

Fig. 2: QBER of the relay-assisted QKD system over clear ocean and coastal water for **(a)** moderate turbulence conditions **(b)** strong turbulence conditions.

On the other hand, relaying helps improve the performance for non-turbid water as seen in the plots associated with clear ocean. For instance, in moderate turbulence conditions (Fig. 2a) to achieve $\mathrm{QBER} \leq 0.11$[2], the achievable distance for direct link is 109 m. It increases to 113 m and 114 m with $K = 1$ and $K = 2$ relay nodes, respectively. The improvements are more pronounced as turbulence strength increases. In strong turbulence conditions (Fig. 2b) to achieve $\mathrm{QBER} \leq 0.11$, the achievable distance for direct link is 89 m. It increases to 91 m and 97 m with $K = 1$ and $K = 2$ relay nodes, respectively.

The aforementioned end-to-end distances are achievable under the assumption of perfect error correction, i.e., $f = 1$. In an effort to have an insight into what end-to-end distances can be achieved with a practical coding scheme, Fig. 3 depicts the SKR performance for clear ocean with strong turbulence conditions. We employ an LDPC code with a rate of $R_c = 0.5$ optimized for a BSC channel with crossover probability of $\mathrm{QBER}_{th} = 0.1071 \approx 0.11$ [28]. Although it is possible to use other LDPC codes in [28] optimized for lower QBER values to improve SKR, the maximum achievable distance will still remain the same because the highest QBER that can

[2]It is generally accepted that for BB84 protocol is secure against a sophisticated quantum attack if QBER is less than 0.11 [33].

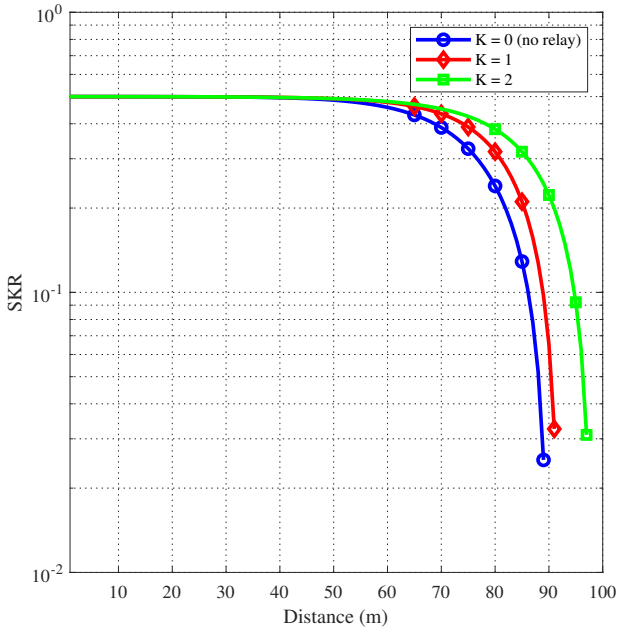


Fig. 3: SKR of the relay-assisted QKD system over clear ocean with strong turbulence conditions.

be tolerated to obtain non-zero SKR should be less than 0.11. In other words, the maximum achievable distances observed through SKR analysis remain almost the same as those obtained through QBER analysis.

In Fig. 4, we investigate the effect of atmospheric conditions on the achievable distance for different number of relay nodes. We consider clear ocean with strong turbulence and assume both hazy and heavy overcast atmosphere when sun is near the horizon at day time. As a benchmark, clear atmospheric conditions at night with a full moon (assumed in Fig. 2) is also included. It is observed that as the environment irradiance increases the optimal number of relays (in the sense of maximizing the achievable distance) decreases. Specifically, the maximum achievable distance for heavy overcast and hazy atmosphere are respectively 57 m and 42 m when we employ one relay node. These are much lower than 102 m achievable with four relay nodes at night time.

In Fig. 5, we investigate the effect of FOV on the achievable distance for different number of relay nodes. As atmospheric conditions, we assume clear weather with full moon and heavy overcast. We consider three different FOV values, i.e., $\Omega = 10°$, $60°$, and $180°$. It is observed that at night, the achievable distances are almost identical and independent of FOV values, i.e., all three plots overlap with each other. The maximum achievable distance is obtained as 102 m

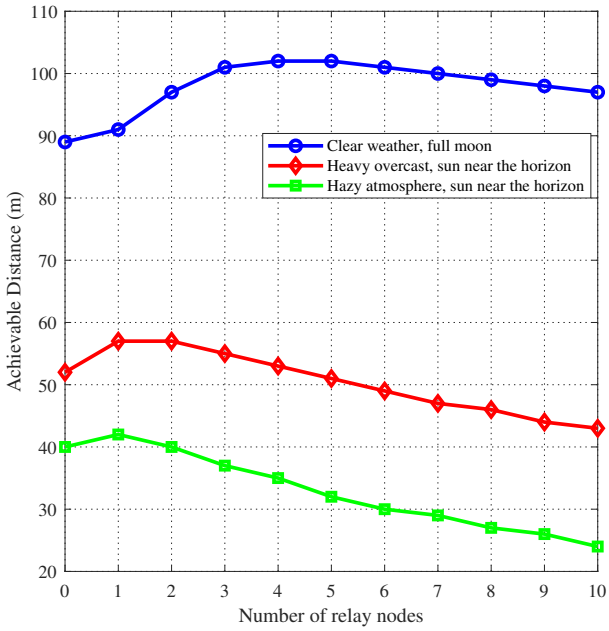


Fig. 4: Achievable distance versus the number of relay nodes for different atmospheric conditions.

when we employ four relay nodes. However, further increase in relay nodes does not improve the performance since, according to (11), increasing the number of relay nodes leads to an increase in the background noise redirected from relays to Bob's receiver.

Benefit of choosing a proper value of FOV becomes clear as the environment irradiance increases, see plots associated with day time (i.e., heavy overcast). Our results demonstrate that the optimal number of relays (in the sense of maximizing the achievable distance) increases as the FOV decreases. Specifically, maximum achievable distance for $\Omega = 180^\circ$ is 57 m which can be attained by employing one relay. On the other hand, the optimal number of relays for $\Omega = 60^\circ$ and $\Omega = 10^\circ$ to attain the maximum achievable distance is two and four relay nodes, respectively. As can be readily checked from (10), the effect of FOV on n_{B0} is more pronounced at day time due to higher value of environment irradiance. Thus, increasing FOV results in increase of the background noise at each relay node and consequently, this increases the background noise redirected from relays to Bob's receiver.

In Fig. 6, we investigate the effect of aperture size on the achievable distance for different number of relay nodes. During night time, it is observed that the direct transmission (i.e., $K = 0$) with the largest diameter size under consideration ($d = 30$ cm) achieves the largest transmission

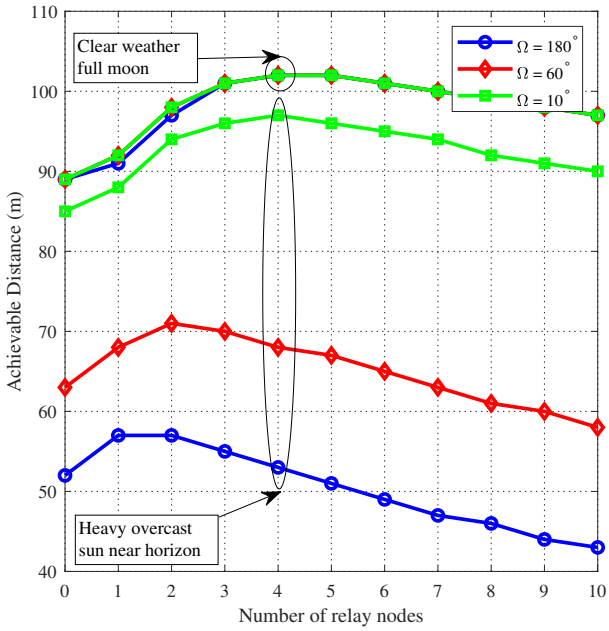


Fig. 5: Achievable distance versus the number of relay nodes for different FOV values.

distance. For $d = 30$ cm, relay-assisted scheme does not bring any improvement. Actually, its performance is even worse than direct transmission. This is as a result of the accumulation of background noise redirected from relays to Bob for such a large diameter size. On the other hand, when the background noise is limited via the selection of a smaller diameter (i.e., $d = 5$ and 10 cm), relaying can improve the achievable distance to a certain extent if the relay number is sufficiently small. For example, the maximum achievable distance for $d = 10$ cm is 111 m which is achieved by employing $K = 2$ relays. If the relay number gets larger (i.e., $K > 2$) for $d = 10$ cm, the accumulated noise becomes too large and the achievable distance decreases. During day time, it is observed that the smallest diameter size under consideration (i.e., $d = 5$ cm) yields larger achievable distances in comparison to other diameter sizes. The maximum achievable distance for $d = 5$ cm is 57 m which is achieved by employing $K = 1$ relay. On the other hand, relaying fails to improve the achievable distance for larger diameters.

As observed from the results presented in Figs. 4, 5 and 6, there is a trade-off among system parameters. To better emphasize this, we present Table II which provides the combination of "maximum achievable distance" and "required number of relay nodes to achieve that distance" for a given set of system parameters and weather conditions. For example, consider a diameter

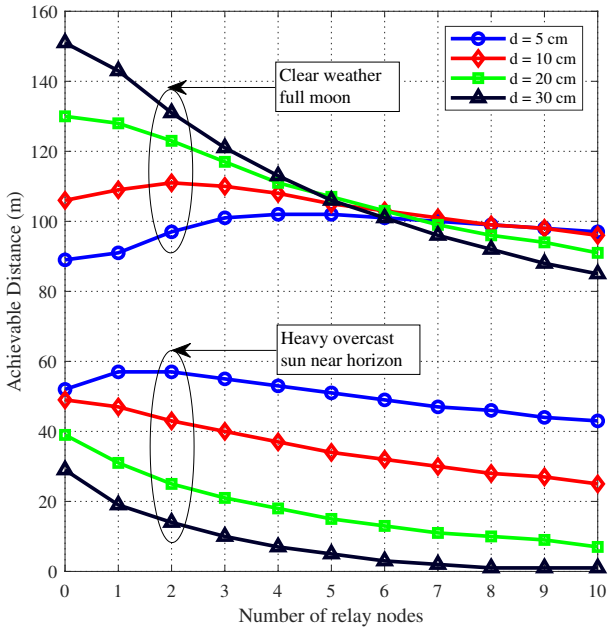


Fig. 6: Achievable distance versus the number of relay nodes for different aperture sizes.

size of $d = 5$ cm, FOV of $\Omega = 10^\circ$ and heavy overcast. For these given channel and system parameters, the maximum achievable distance is 97 m and this is possible with $K = 4$ relays. It can be readily checked from Table II that the achievable distance is 98 m for a QKD system with $d = 10$ cm, $\Omega = 10^\circ$, and $K = 2$ relays under the same weather conditions. As an another example, consider $d = 20$ cm, $\Omega = 10^\circ$ and hazy overcast. For these given parameters, the maximum achievable distance is 82 m and this is possible with direct transmission (i.e., no relay). For the same weather conditions, QKD systems with parameter sets of $\{d = 10$ cm, $\Omega = 10^\circ$, $K = 1\}$ and $\{d = 5$ cm, $\Omega = 10^\circ$, $K = 3\}$ respectively achieve 84 m and 87 m. Such observations indicate that similar achievable distances can be obtained for different combinations of system parameters. The final selection can be made by the system designer taking into account cost of related equipment, i.e., more relays or larger aperture etc.

In Fig. 7, we investigate the effect of depth on the achievable distance for different number of relay nodes. It can be observed that at night time the effect of depth is practically negligible, and the achievable distance remains almost the same for all depths under consideration. The effect of depth becomes more pronounced as the environment irradiance increases. During day time, as the depth increases the optimal number of relay nodes (in the sense of maximizing

TABLE II: The maximum achievable distance and the required number of relay nodes to achieve that distance for different combinations of system parameters

Diameter size (d)	5 cm			10 cm			20 cm			30 cm		
Field of view (Ω)	10°	60°	180°	10°	60°	180°	10°	60°	180°	10°	60°	180°
Clear weather	102 m	102 m	102 m	112 m	112 m	111 m	131 m	131 m	130 m	156 m	154 m	151 m
full moon	$K = 4$	$K = 4$	$K = 4$	$K = 2$	$K = 2$	$K = 2$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$
Heavy overcast	97 m	71 m	57 m	98 m	64 m	49 m	100 m	57 m	38 m	106 m	51 m	27 m
sun near horizon	$K = 4$	$K = 2$	$K = 1$	$K = 2$	$K = 1$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$
Hazy overcast	87 m	55 m	42 m	84 m	47 m	32 m	81 m	35 m	17 m	82 m	25 m	7 m
sun near horizon	K =3	$K = 1$	K =1	$K = 1$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$	$K = 0$

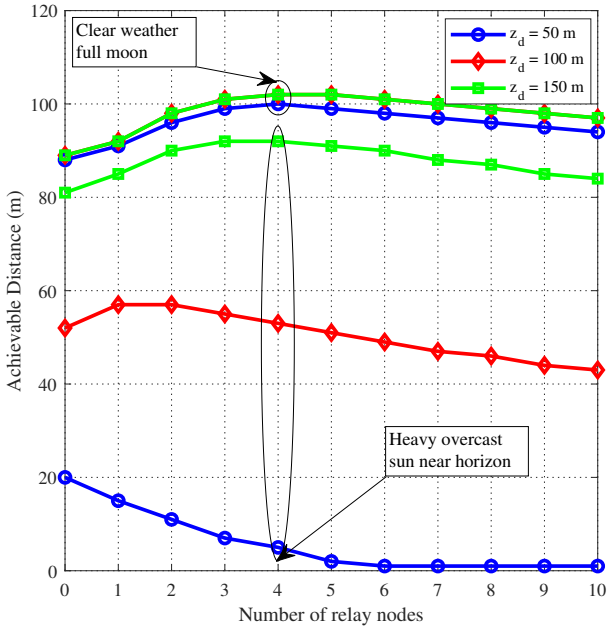


Fig. 7: Achievable distance versus the number of relay nodes for different depth.

the achievable distance) increases. Specifically, the maximum achievable distance for depth of $z_d = 50$ m is 20 m which is feasible with direct transmission ($K = 0$) and relaying is not required. However, as the depth increases, relaying might be beneficial as a result of decrease in the refracted sunlight from the surface of the water. Specifically, the maximum achievable distances for $z_d = 100$ m and $z_d = 150$ m are respectively 57 m and 92 m. These are achieved respectively by using $K = 1$ and $K = 3$ relays.

V. Conclusions

In this paper, we have investigated the performance of relay assisted underwater QKD with BB84 protocol. Based on the near-field analysis, we have obtained QBER and SKR in different water types and turbulence conditions. Our results have demonstrated that relay-assisted QKD has the potential to increase the end-to-end achievable distance if the system parameters are judiciously selected. While adding relay nodes mitigates the degrading effects of turbulence-induced fading, it also results in an increase of the average number of background photons at Bob's receiver. To investigate this trade-off, we have studied the effect of system parameters such as aperture size and FOV on the achievable distance and determined the optimal number of relays in the sense of maximizing the achievable distance. It is observed that the optimal number of relay increases as the FOV decreases and/or as the receive diameter decreases. Our results highlight that relaying brings improvements when the noise level is kept low (e.g., small receiver diameter, small FOV, and/or low environment irradiance) and the water turbidity is low (e.g., clear ocean).

References

[1] Google AI Quantum, "Quantum supremacy using a programmable superconducting processor," https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html, 2019, accessed: 2020-07-30.

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[3] D. Bruss and G. Leuchs, *Quantum Information: From Foundations to Quantum Technology Applications*. John Wiley & Sons, 2019.

[4] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.*, vol. 2, p. 16025, 2016.

[5] P. Shi, S. C. Zhao, Y. J. Gu, and W. D. Li, "Channel analysis for single photon underwater free space quantum key distribution," *J. Opt. Soc. Am. A*, vol. 32, no. 3, pp. 349–356, 2015.

[6] M. Lopes and N. Sarwade, "Optimized decoy state QKD for underwater free space communication," *Int. J. Quantum Inf.*, vol. 16, no. 02, p. 1850019, 2018.

[7] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Opt. Exp.*, vol. 26, no. 17, pp. 22 563–22 573, 2018.

[8] 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. Am. A*, vol. 36, no. 5, pp. 883–892, 2019.

[9] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE Journal of Oceanic Engineering*, vol. 45, no. 3, pp. 1138–1147, 2020.

[10] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," *Appl. Opt.*, vol. 58, no. 14, pp. 3902–3907, 2019.

[11] C. Q. Hu, Z. Q. Yan, J. Gao, Z. Q. Jiao, Z. M. Li, W. G. Shen, Y. Chen, R. J. Ren, L. F. Qiao, A. L. Yang, and H. Tang, "Transmission of photonic polarization states through 55-m water: Towards air-to-sea quantum communication," *Photonics Res.*, vol. 7, no. 8, pp. A40–A44, 2019.

[12] 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. Express*, vol. 27, no. 19, pp. 26 346–26 354, 2019.

[13] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Express*, vol. 27, no. 3, pp. 3055–3064, 2019.

[14] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *J. Opt. Soc. Am. B*, vol. 37, no. 2, pp. 564–573, 2020.

[15] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. rev. lett.*, vol. 120, no. 3, p. 030501, 2018.

[16] T. Chapuran, P. Toliver, N. Peters, J. Jackel, M. Goodman, R. Runser, S. McNown, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, no. 10, p. 105001, 2009.

[17] M. Safari and M. Uysal, "Relay-assisted quantum-key distribution over long atmospheric channels," *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, 2009.

[18] ——, "Relay-assisted free-space optical communication," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5441–5449, 2008.

[19] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A*, vol. 67, no. 2, p. 022309, 2003.

[20] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE Int. Conf. Com. Syst. Signal Processing*. IEEE, 1984, pp. 175–179.

[21] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[22] Y. Chen, S. Huang, and M. Safari, "Orbital angular momentum multiplexing for free-space quantum key distribution impaired by turbulence," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf.* IEEE, 2018, pp. 636–641.

[23] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 543–552, 2018.

[24] F. Hanson and S. Radic, "High bandwidth underwater optical communication," *Appl. Opt.*, vol. 47, no. 2, pp. 277–283, 2008.

[25] C. D. Mobley, *Light and Water: Radiative Transfer in Natural Waters*. Academic press, 1994.

[26] M. Lanzagorta, *Underwater Communications*. Morgan & Claypool Publishers, 2012.

[27] C. Kollmitzer and M. Pivk, *Applied Quantum Cryptography*. springer, 2010, vol. 797.

[28] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inform. Theory*. IEEE, 2009, pp. 1879–1883.

[29] J. Martinez Mateo, D. Elkouss Coronas, and V. Martín Ayuso, "Blind reconciliation," *Quantum Information & Computation*, vol. 12, no. 9&10, pp. 791–812, 2012.

[30] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, 2001.

[31] C. D. Mobley, E. Boss, and C. Roesler, "Ocean Optics Web Book," http://www.oceanopticsbook.info, 2010.

[32] T. Wu, X. Ji, H. Zhang, X. Li, L. Wang, and X. Fan, "Rytov variance of spherical wave and performance indicators of laser radar systems in oceanic turbulence," *Opt. Commun.*, vol. 434, pp. 36–43, 2019.

[33] V. Scarani, H. Bechmann Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.