2022 21st International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)

Continuous-variable measurement-device-independent quantum key distribution with passive state in oceanic turbulence

Guojun Chen[1,2], Jianmin Yi[1,3], and Ying Guo[1,2,3]
[1]Jiangsu Key Laboratory of IoT Application Technology, Wuxi Taihu University, Wuxi, 214064, China
[2]College of Computer Internet of Tings Engineering, Wuxi Taihu University, Wuxi, 214064, China
[3]School of Automation, Central South University, Changsha, 410083, China
*Corresponding Author: Ying Guo. Email: yingguo@csu.edu.cn

***Abstract*—Quantum communication, as an absolutely secure communication method, has been widely studied in recent years. While CVQKD is easier to realize and has efficient information transmission, has attracted more attention than DVQKD. And there is another kind of detection strategy which places the detector on a third party called continuous-variable measurement device independent quantum key distribution(CV-MDI), can lower the cost of implementation because it don't need such a high precision Gaussian modulator and thus can be commercialized easily. We apply a CV-MDI with passive-state preparation protocol to a oceanic turbulence model, and then we analyze the secret key rate and other performance of the protocol in the particular scenario.**

Keywords- continuous variable quantum key distribution; measurement device independent; oceanic turbulence model; application

I. INTRODUCTION

Quantum key distribution is a kind of encrypted means of communication [1], which uses the principle of quantum mechanic to enable the security for wo legitimate parties to exchange secret keys.

The first quantum key distribution protocol which is called BB84 appeared in 1984 [2], discrete-variable quantum key distribution(DV-QKD) has been a hot area of research since then. While in these years, continuous-variable quantum key distribution(CV-QKD), which is based on Gaussian-modulated coherent states, gradually replace DV-QKD in position as an optimized scheme[3].

Compared with DV-QKD, CV-QKD has many advantages. It's easy to prepare coherent quantum states and it has more means of signal modulation with more efficient and safe modulation technology.

With further study of CV-QKD, there also appear some attack strategies because of some reality factors. The actual security of CV-QKD is related to both system noise and security vulnerability. The system noise sources mainly include calibration error of homodyne detector [4] and noise attack of light source caused by non-ideal Gaussian modulation [5]. Security vulnerabilities mainly include jitter attack of local light intensity, unbalanced transmittance attack of fractional device [6], saturation effect attack of detector [7], etc. People come up with ameliorative protocol called continuous-variable measurement-device-independent (CV-MDI) [8] which adds a third party Charlie to detect the quantum states from Alice and Bob to counter the attack from practical devices.

But the cost of CV-MDI is high as it requires high precision modulators. And a group proposes a passive-state preparation scheme in CV-MDI protocol saves costs while ensuring the protocol's security and efficiency [9].

In most cases, adopt the fiber as quantum communication channel is optimal, while there are many limits for using fiber in practice such as cost and technological problems. It's also difficult to achieve in free-space and under-water condition. And building a transmission model for CV-QKD protocol application is necessary for underwater communication security[10-11].

The organization of this paper is as follows. In Sec.2, we introduce the CV-MDI protocol with passive-state as source of quantum state preparation. In Sec.3, we introduce an oceanic turbulence model and obtain the probability parameters of the distribution of transmittance. In Sec.4, we compute the secret key rate of CV-MDI protocol in oceanic scenario and analyze the performance of this model. Sec.5 shows the simulation results and Sec.6 is a conclusion of this paper.

II. CV-MDI QKD PROTOCOL WITH ACTIVE STATE PREPARATION

In this chapter, we will introduce the CV-MDI protocol with passive-state preparation in detail. This scheme uses a thermal source as the preparation source to generate passive state, it's not necessary although pure single-mode thermal can also be used for preparation. For the convenience of analysis, we assume that the thermal source is a single mode.

It's convenient and effective to establish entangle based scheme corresponding to CV-MDI for analyzing the security of protocol. In this scheme, the quantum states emitted by Alice and Bob are single-mode thermal states from the perspective of Eve and Charlie. For a given modulation variance V, the average number of photons emitted by Alice and Bob after modulation is half of the modulation variance.

In the CV-MDI QKD scheme, Alice (Bob) sends one mode of the two-mode squeezed state to Charlie through a channel and then heterodynes the remaining other mode.

Steps of CV-MDI with passive state preparation is showing in the following ways. (Refer to Figure 1)

(1) Alice and Bob prepare the thermal source respectively, and stipulate that the modulation variances is $2n_0$, and the average number of photons output by the heat source is n_0. Through a 50:50 beam splitter, Alice (Bob) divide the optical signal output by the heat source into two correlated spatial modes. (The state thermal sources output at Alice are divided into Mod_{A1}, Mod_{A2} and the state at Bod side are divided into Mod_{B1}, Mod_{B2}.)

Next, Mod_{A1} (Mod_{B1}) at Alice (Bob) modulates Mod_{A1} (Mod_{B1}) with variance of V_A (V_B) through an optical

2473-3636/22/$31.00 ©2022 IEEE
DOI 10.1109/DCABES57229.2022.00025

attenuator. The modulated signal is transmitted to a third party Charlie through a channel.

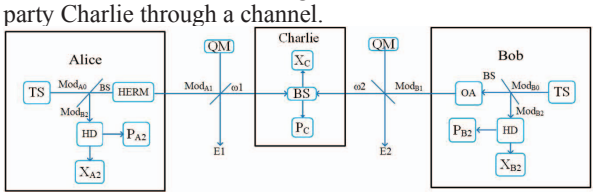


Figure 1. CV-MDI protocol with passive state preparation. ω_1, ω_2 are the variances of source noise, and E_1, E_2 are ancillary modes which mix with modes $|\alpha>$ and $|\beta>$. QM is quantum memory device which is used to store the outputs from Eve, HERM denotes high-extinction-ratio modulator and OA is optical attenuator. HD is heterodyne detector and TS is thermal source.

(2) Then Alice (Bob) performs heterodyne detection on another mode Mod_{A2} (Mod_{B2}). Alice (Bob) inputs the Mod_{A2} (Mod_{B2}) to a balanced beam splitter, to detected the X quadratures and P quadratures respectively. The quadratures of $\mathrm{Mod_{A1}}$ ($\mathrm{Mod_{B1}}$) received at Charlie have the following relation with Mod_{A2} (Mod_{B2}) as $X_{A1}=\sqrt{\frac{2\eta A}{\eta D}}X_{A2}$, $P_{A1}=\sqrt{\frac{2\eta A}{\eta D}}P_{A2}$,($X_{B1}=\sqrt{\frac{2\eta A}{\eta D}}X_{B2}$, $P_{B1}=\sqrt{\frac{2\eta A}{\eta D}}P_{B2}$), and η_A (η_B) is the transmittance of the attenuator and the efficiency of the practical homodyne detector is η_D.

(3) For received Mod_{A1} and Mod_{B1}, Charlie mixes them on a balanced beam splitter and conducts Bell State Measurement on them, and the results can be conjugated homodyne detected by its output ports. Then Charlie broadcast the quadratures (X_C, P_C) through a classical public channel to Alice and Bob. In order to ensure the security of the protocol, we assume that Eve adopts the optical attack mode, that is, using the joint two-mode attack strategy which involves the two links rather than using the single-mode attack strategy.

(4) After repeating these steps several times, Alice and Bob get a string of raw keys. And then Alice and Bob postprocess the data of (X_{A1}, P_{A1}), (X_{B1}, P_{B1}), (X_C, P_C) in a standard steps of privacy amplification and error correction, and after that, Alice and Bob get the final secret keys. By the way, this process is similar to the classical CV-MDI protocol with active state preparation, so Alice and Bob can get the secret keys if the detected total noise is less than a certain threshold value.

In summary, we describe a CV-MDI scheme that doesn't require the participation of expensive phase modulator and amplitude modulator. Because the state prepares is the passive state, and it would save lots of money in applying this protocol to practical application.

III. OCEAN QUANTUM COMMUNICATION MODEL

Oceanic quantum secret key distribution is necessary for underwater communication. Many factors in the ocean, such as seawater density, turbulence, bubble surface and so on, have important effects on the propagation of light which affects the secret key rates. We get a specific ocean quantum links model to analyze the probability of transmittance distribution [12], and then we can compute the secret key rates of CV-MDI scheme in marine circulation.

The transmittance has the following estimation form

$$\mathrm{T}=\mathrm{T}_0\mathrm{T}_{ext}/\exp\left\{\left[\frac{R}{a\Gamma\left(\frac{2}{W_{eff}(\theta-\varphi)}\right)}\right]^{\psi\left(\frac{2}{W_{eff}(\theta-\varphi)}\right)}\right\} \quad (1)$$

The deterministic losses caused by the ocean extinction has an effect on the transmittance

$$T_{ext}=e^{-zt} \quad (2)$$

T_{ext} is the extinction-induced transmittance, z denotes the transmission distance and t is the seawater extinction coefficient which is related to the wavelength λ, and it is defined by

$$\mathrm{t}=\mathrm{t_{abs}}+\mathrm{t_{sca}} \quad (3)$$

The $\mathrm{t_{abs}}$ is the ocean absorption factor which has the form

$$\mathrm{t}_{abs}=l_c^0\left[u_c(\mathrm{d})\right]^{0.602}+l_w+l_f^0u_f(\mathrm{d})\mathrm{e}^{-k_f\lambda}+l_h^0u_h(\mathrm{d})\mathrm{e}^{k_h\lambda} \quad (4)$$

u_c is the chlorophyll a content and it is defined as

$$u_c(d)=u_b+ds+\frac{h\sqrt{2\pi}}{\varsigma}\exp(-\frac{(\mathrm{d}-\mathrm{d}_{\max})^2}{2\varsigma^2}) \quad (5)$$

The standard deviation of the concentration of chlorophyll ς is given by

$$\varsigma=\frac{h}{\sqrt{2\pi(\mathrm{u}_{ch1}-\mathrm{u}_b-\mathrm{d}_{\max}\mathrm{s})}} \quad (6)$$

The content of fulvic acid is defined as

$$\mathrm{u_f(d)}=1.74098\mathrm{u_c(d)e}^{0.12327\mathrm{u_c(d)}} \quad (7)$$

The concentration of humic acid has the form

$$\mathrm{u_h(d)}=0.19334\mathrm{u_c(d)e}^{0.12343\mathrm{u_c(d)}} \quad (8)$$

The $\mathrm{t_{sca}}$ is the scattering factor which is given by

$$\mathrm{t}_{sca}=m_s^0u_s(d)+m_1^0u_t(d)+m_w \quad (9)$$

And the small particles' concentration is defined as

$$\mathrm{u_s(d)}=0.01739\mathrm{u_c(d)e}^{0.11631\mathrm{u_c(d)}} \quad (10)$$

The large particles' concentration is defined as

$$\mathrm{u_t(d)}=0.76284\mathrm{u_c(d)e}^{0.03092\mathrm{u_c(d)}} \quad (11)$$

IV. OCEAN QUANTUM COMMUNICATION MODEL IN CV-MDI WITH PASSIVE STATE PREPARATION ONCLUSION

According to part 3, we get the probability of transmittance in an oceanic communication link, and obtain the relationship between average transmittance and ocean depth and transmission distance in a specific ocean.

Compared with the CV-MDI protocol with positive state, the CV-MDI protocol with passive state will introduce redundant excessive noise, and only the eavesdropper can carry out a joint-mode attack, which is the optimal attack pattern to Eve.

A. Evaluation of secret key: Secret key rate in asymptotic scenarios

The simplified covariance matrix between Alice and Bob can be calculated as

$$\mathrm{V}_{A_1B_1|C}=\begin{bmatrix}\left(v-\frac{T_A(V^2-1)}{J}\right)I_2 & \frac{\sqrt{T_AT_B}(V^2-1)}{J}\sigma_z\\ \frac{\sqrt{T_AT_B}(V^2-1)}{J}\sigma_z & \left(v-\frac{T_B(V^2-1)}{J}\right)I_2\end{bmatrix} \quad (12)$$

With $I_2=\begin{bmatrix}1&0\\0&1\end{bmatrix}$ and $\sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$, V is the variance and $V=V_A+1(V=V_B+1)$, $\varpi_1=\varpi_2=1.01$ where

$$\vartheta = V(T_A + T_B) + \varpi(1 - T_A) + \varpi(1 - T_B) - 2g\sqrt{(1 - T_A)(1 - T_B)} \tag{13}$$

$$g = \min\left[\sqrt{(\varpi_1 - 1)(\varpi_2 + 1)}, \sqrt{(\varpi_1 + 1)(\varpi_2 - 1)}\right] \tag{14}$$

The mutual information between Alice and Bob is given by

$$I_{AB} = \log_2 \frac{V}{X_{total}} \tag{15}$$

X_{total} can be divided into two parts

$$X_{total} = X_{loss} + \varepsilon_E \tag{16}$$

The pure loss in channel from Alice to Charlie and from Bob to Charlie X_{loss}, which has the form $X_{loss} = 2\frac{T_A + T_B}{T_A T_B}$, and the total excess noise $\varepsilon_E = \varepsilon_P + \varepsilon_0$, ε_0 is the background noise, ε_P is the total excess noise in the process of passive state preparation, and it's defined as

$$\varepsilon_P = \varepsilon_A + \varepsilon_B \tag{17}$$

$$\varepsilon_A = \frac{2V_A}{\eta_D n_0}(1 + V_{el}) - \frac{V_A}{n_0} \tag{18}$$

$$\varepsilon_B = \frac{2V_B}{\eta_D n_0}(1 + V_{el}) - \frac{V_B}{n_0} \tag{19}$$

V_A and V_B are the modulation variance, and for simplicity, we set the noise of homodyne detector V_{el} is 0. η_D is the efficiency of homodyne detector and n_0 is the average number of photons output by the thermal source.

B. *Evaluation of secret key: Secret key rate in the finite-size case*

In the finite-size condition, the secret key rate is given by

$$K = \frac{n}{N}\left[K\infty\left(T_A^{low}, T_B^{low}, \varepsilon_{X_C}^{high}, \varepsilon_{P_C}^{high}\right) - \Delta(n)\right] \tag{20}$$

The signals exchanged by Alice and Bob is N. Because of the effection of finite-size, Alice and Bob should conduct the parameter estimation by using a number of m keys in practical condition, and the remain number of n, which has the correlation with m, is given by $n = N - m$, are used to generate the secret key. The correction term $\Delta(n)$ is simplified as

$$\Delta(n) = 7\sqrt{\frac{\log_2 2/\varepsilon_{P_A}}{n}} \tag{21}$$

The estimation of error in privacy amplification ε_{PA} is set to 10^{-10}. The noise of X_C and P_C generated in Charlie's detection has the form

$$\varepsilon_{X_C} = \varepsilon_{P_C} = \varepsilon_P + \frac{1}{2}\left[\varpi_1(1 - T_A) + \varpi_2(1 - T_B)\right] - g\sqrt{(1 - T_A)(1 - T_B)} \tag{22}$$

$$\delta_{\varepsilon Xc} = \delta_{\varepsilon Pc} = \sqrt{\frac{2\varepsilon_{Xc}}{m}} \tag{23}$$

The maximum noise of X_C and P_C generated in Charlie's detection is given by

$$\varepsilon_{X_C}^{high} = \varepsilon_{X_C} + 6.5\delta_{\varepsilon Xc}, \quad \varepsilon_{P_C}^{high} = \varepsilon_{P_c} + 6.5\delta_{\varepsilon Pc} \tag{24}$$

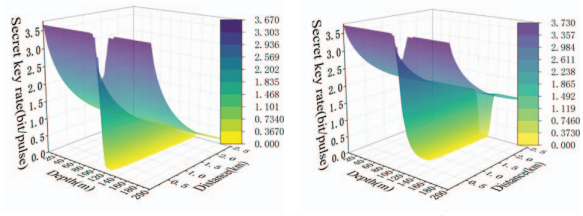
Considering the security of the protocol, we should consider the transmittance of the channel at Alice and Bob in the worst case.

V. SIMULATION RESULTS

In this part, we will give the results of system performance. As we discussed before, we consider the oceanic turbulence model in a CV-MDI scheme with passive-state quantum preparation. There are two main kinds of cases about measurement-device-independent protocol, according to the different distances between Alice and Bob and Charlie, the protocol can be divided into symmetric and asymmetric cases.

A. *Secret key rate in asymptotic scenarios*

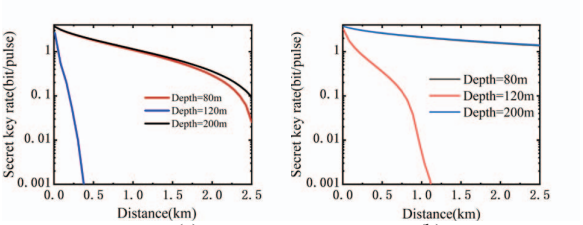
The graph of the function with transmission distance and ocean depth as independent variables and secret key rate as dependent variables is shown in Fig.2 and Fg.3.



(a) (b)

Figure 2. Distance&Depth(asymptotic scenarios): (a) sysmmetric case (b) asymmetric case.

We can see that the secret key rate decreases as the transmission distance increases, and with the depth of the ocean increases, the secret key rate first decreases and then increases until it becomes stable, which can be varified in Fig.4 and Fig.5.



(a) (b)

Figure 3. Distance(asymptotic scenarios): (a)sysmmetric case (b)asymmetric case.

The more details of Fig.4 can be seen in Fig.6.

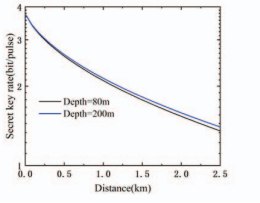


Figure 4. Distance(details): sysmmetric case

The transmission distance has a major effect on the secret key rate. And we also analyze the secret key rate relationship with ocean depth at different transmission distances in Fig.7 and Fig.8, which show that we should avoid setting up communication devices at about 100 to 140 deep in the ocean.

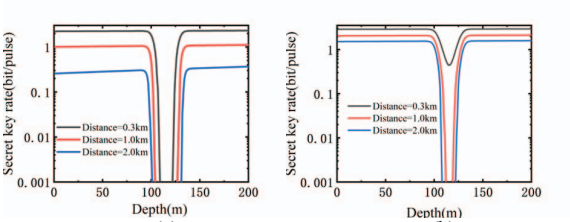


Figure 5. Depth(asymptotic scenarios): (a)sysmmetric case (b)asymmetric case

B. *Secret key rate in the finite-size case*

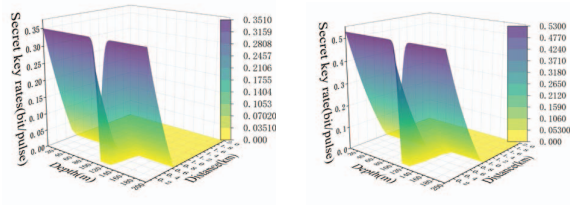


Figure 6. Distance&Depth(finite-size case): (a)sysmmetric case (b)asymmetric case

The trend of the secret key rates is the same as in the ideal case, while because of finite-size effects and other implicit factors, the secret key rates are lower than asymptotic scenarios. They can be seen clearer in at certain oceanic depths and communication distances.

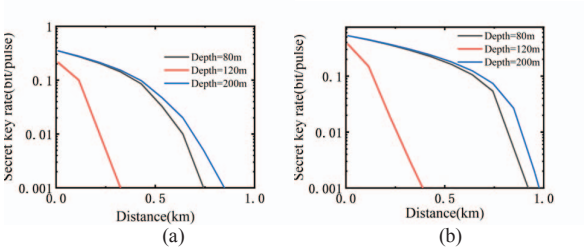


Figure 7. Distance(finite-size case): (a)sysmmetric case (b)asymmetric case

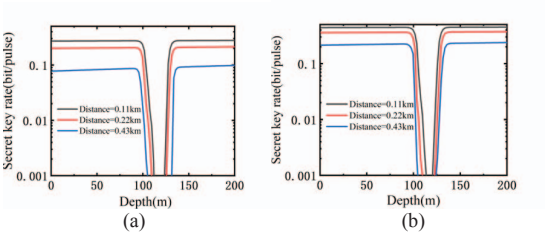


Figure 8. Depth(finite-size case): (a)sysmmetric case (b)asymmetric case

The average output photon number is set to 800 and the modulation variance is 60. For simplicity, we treat the homodyne detector as noiseless and the efficiency of it is set to 0.95. The communication block size is 10^8.

VI. CONCLUSION

In this paper, based on an oceanic turbulence model, we apply the CV-MDI protocol to a specific ocean scenario, come up with an underwater communication scheme. Then we calculated the secret key rate both in asymptotic case and in finite-size case, the results indicate that the measurement-device-independent protocol is applicative in the marine environment. By the way, there is also another construction of continuous variable measurement device independent scheme, which stipulate that the distance between Alice and Char-lie is not equal to the distance between Bob and Charlie. After analyzing the asymmetric case, we find that shorten the distance between Alice and Charlie can make the secret key rate much better than the symmetric case. Though it's generally accepted that the efficient of short-distance communication is greater than long-distance communication as the longer the communication distance the greater the signal loss and the noise. We find that in an extreme situation, i.e. the distance between Charlie and Alice is short enough to be ignored, the system performance is much better than the circumstance that Bob is close to Charlie. So to make the underwater communication more efficient, or increase underwater quantum communication distance, it's better to make Alice and Charlie close together.

REFERENCES

[1] Pirandola S, Eisert J, Weedbrook C, et al. "Advances in quantum teleportation". Nature Photonics,vol.9,no.10,pp. 641-652, 2015.

[2] BENNETT C H,BRASSARD G. "Quantum cryptography: public key distribution and coin tossing". International Conference on Computer System and Signal Processing, IEEE, pp.175-179, 1984.

[3] LI Feifan. "International Quantum Cryptography Patent Development Trend and Hot Spot Analysis". WORLD SCI-TECH R&D. vol. 44, no.1, pp.69-80, 2022.

[4] Liao S K, Yong H L, Liu C, et al. "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication". Nature Photonics, vol. 11, no.8, pp.509-513, 2017.

[5] Wang J Y, Yang B, Liao S K, et al. "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution". Nature Photonics, vol. 7, no. 5, pp.387-393, 2013.

[6] Kong M, Wang J, Chen Y, et al. "Security weaknesses of underwater wireless optical communication". Optics Express, vol. 25, no.18, pp.21509-21518, 2017.

[7] Guo Y, Xie C, Huang P, et al. "Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution". Physical Review A, vol. vol.97, no.5, pp.052326, 2018.

[8] Ruan X, Zhang H, Zhao W, et al. "Security analysis of discrete-modulated continuous-variable quantum key distribution over seawater channel". Applied Sciences, vol. 9, no.22, pp. 4956, 2019.

[9] Hao Dong, Li Bili, Yang Yi, He Fengtao. "Research on transmission characteristics of underwater wireless optical communication channel". Automation and Instrumentation, vol.9, pp.21-24, 2021.

[10] Hu C Q, Yan Z Q, Gao J, et al. "Decoy-state quantum key distribution over a long-distance high-loss air-water channel". Physical Review A, vol.15, no.2, pp.024060, 2021.

[11] J Gariano, Djordjevic I B. "Theoretical study of a submarine to submarine quantum key distribution systems". Optics express, vol.27, no.3, pp.3055, 2019.

[12] DOU Yin , ZHANG Meixiang, ZHOU Lingxia. "A Novel Reconciliation Scheme for Continuous Variable Quantum Key Distribution". Radio Engineering, vol.52, no.4, pp.685-691, 2022.