IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MISSION CRITICAL SENSORS AND SENSOR NETWORKS (MC-SSN)

Received December 18, 2019, accepted February 5, 2020, date of publication February 19, 2020, date of current version March 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2975155

Continuous-Variable Quantum Key Distribution Over Air Quantum Channel With Phase Shift

MING LI[1] AND TIANYI WANG[2]

[1]Tianjin Key Laboratory of Wireless Mobile Communications and Power Transmission, Tianjin Normal University, Tianjin 300387, China
[2]College of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China

Corresponding authors: Ming Li (mliece@163.com) and Tianyi Wang (tywang@gzu.edu.cn)

This work was supported in part by the Natural Science Youth Foundation of Tianjin under Grant 17JCQNJC01800 and Grant 18JCQNJC01900, in part by the Doctoral Funding at Tianjin Normal University under Grant 52XB1506, in part by the National Natural Science Foundation of China under Grant 61805176, and in part by the State Key Laboratory of Advanced Optical Communication Systems and Networks, China, under Grant 2019GZKF8.

ABSTRACT Continuous-variable quantum key distribution (CV-QKD) over air quantum channel enables to provide unconditional information security, which is the one of most promising techniques for information wireless transfer. Since the air channel is of fluctuation in nature due to the presence of air turbulence, the random variations have to be taken into account when the security of CV-QKD is analyzed. We study the secret key rate of CV-QKD over the air quantum channel in this paper. The fluctuation of air channel is characterized by beam wandering and phase distortion under weak air turbulence conditions. The impact of fluctuation on the CV quantum signals is reflected by transmittance perturbation and phase shift. Our numerical results show that the secret key rate may keep relatively high level as the air quantum link increases at the outset. However, when the air link distance further increases beyond certain range, the secret key rate decreases strikingly since the both transmittance perturbation and the phase shift simultaneously deteriorate the performance of CV-QKD. Nevertheless, operating the CV-QKD under weak air turbulence conditions is available.

INDEX TERMS Quantum key distribution, quantum cryptography, continuous variable, air channel.

I. INTRODUCTION

The machine possessing powerful-computational capacity, like the quantum computer [1], poses huge threat to the current classical cryptosystem which relies on computational complexity. Quantum key distribution (QKD) [2], [3], unlike the classical cryptography, launches non-orthogonal quantum states to share the secret key between distant parties. Its security is based on the quantum physics laws. Thus, QKD combing with one-time pad strategy enables to provide unconditional information security, which is expected to address the security issue inherently in communications [3].

QKD can be mainly sorted into two categories. One is called discrete-variable QKD (DV-QKD), where the information is encoded to the discrete variables, like polarizations of single photon [4], [5]. The other is referred to as continuous-variable QKD (CV-QKD) since the information is encoded to the continuous variable of electromagnetic field, like conjugate quadratures [6], [7]. Compared to the DV-QKD that requires dedicated single photon source and counter, the CV-QKD employs the mature infrastructure of coherent optical communication. As a result, the CV-QKD may have much simpler operation, and have the potential of offering higher rate and longer transmission [8]–[10]. On the other side, the quantum channel includes air and fiber. The transmission range of fiber-based CV-QKD is limited unless the quantum repeater is ready to use. Instead, the air-based CV-QKD allows large range transmission since the attenuation of air within the transmission window is extremely low and satellite is used as the repeater [11]. Moreover, air CV-QKD also can be deployed in special communication scenarios that the fiber CV-QKD fails to be implemented, for instance, the security communications with handheld devices, over rivers, and among buildings, etc. Therefore, the CV-QKD over air quantum channel is the one of most promising techniques for information wireless transfer [12]. Further, global quantum communication networks may be established by satellites [11], [13].

When CV-QKD over air quantum channel is concerned, the impact of air turbulence has to be taken in account. Due to the presence of air turbulence, the air medium will change randomly as well as the air refractive index [14]. Accordingly, after the optical quantum signals travel through the air channel, the turbulence effects will be induced and significantly degrade performance of CV-QKD. Among them, beam wandering is the most involved effect. In the continuous variable

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

regime, the beam wandering impact is characterized by transmittance perturbation. Reference [15] firstly modelled the transmittance following a specific probability density function (PDF) with expression of the log-negative Weibull distribution. This model is appropriate under weak air turbulence only, and assumed that the beam wandering is the dominant turbulence effect. Based on this model, numerous literatures studied the quantum character of continuous variable when the transmittance perturbation is present. Reference [16] has analyzed entanglement characters of quantum signal in the case of random transmittance. Also, a specific experiment has been demonstrated over a 1600 m air optical channel [17], where the beam wandering was considered only. Reference [18] comprehensively evaluated the influence of air attenuation, beam wandering and fiber coupling efficiency on the CV-QKD. Besides the beam wandering, however, phase distortion will be also induced by the air turbulence, which has to be considered. The objectives of this paper are summarized as follows. (1) The CV-QKD employs intradyne detector to measure the quadratures. Obviously, the phase distortion will lead to phase mismatch, which would bring phase noise thus degrading the performance of CV-QKD. However, the study related to the impact of phase distortion has been extremely limited. This point is concerned specifically. (2) We comprehensively analyze the secret key rate of CV-QKD by taking the transmittance perturbation caused by beam wandering and the phase noise resulting from phase distortion into account in this paper. To the best of our knowledge, it is the first time to evaluate the performance of CV-QKD over air quantum channel by simultaneously considering the both deleterious aspects above.

The remainder of this paper is organized as follows. In Section II, the transmittance perturbation caused by beam wandering and phase shift resulting from the phase distortion is analyzed. Subsequently, the secret key rate of CV-QKD is evaluated by taking the both aspects into account. The numerical simulations are performed, and the results are presented in Section III. Lastly, the conclusions are given in Section IV.

II. SECRET KEY RATE OVER AIR QUANTUM CHANNEL

The CV-QKD over the air quantum channel is demonstrated in Fig. 1. Here, the transmitter named Alice and the receiver called Bob. The eavesdropper Eve possesses the capability of launching the most powerful attack, namely the collective attack in the air quantum channel. That means we assume that Eve can not access any equipment of Alice and Bob [19].

Alice firstly prepares the quantum signals. More concretely, she generates laser pulses, which subsequently are introduced into the intensity/quadrature (I/Q) modulator. We assume that the Gaussian modulation is adopted, which aims to achieve the Shannon-approaching information capacity [20]. After the attenuator, Gaussian modulated coherent states are produced, and are injected into the air quantum channel. Along the air channel, the eavesdropper Eve may launch the collective attack to try to achieve the secret key information. The coherent states arrive at the receiving (Bob) side. Bob measures them with intradyne detector. Once the measurement of quadratures is completed, reverse reconciliation will be performed to correct and correlate the data that Alice and Bob hold. Lastly, Alice and Bob operate parameter estimation and private amplification, which aims to eliminate the information that may have leaked to Eve. Note that, the air channel is actually random in nature due to the presence of air turbulence. The impact of beam wandering and phase distortion resulting from the air turbulence has to be taken into account when the secret key rate of CV-QKD is analyzed.

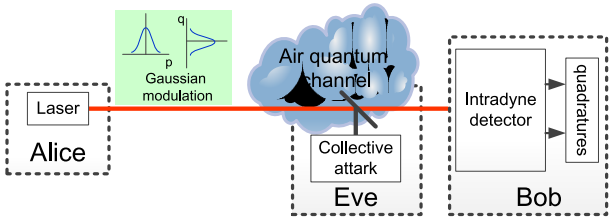

FIGURE 1. CV-QKD over air quantum channel. Symbols *p* and *q* denote the conjugate quadratures of Gaussian modulated coherent state.

A. TRANSMITTANCE PERTURBATION CAUSED BY BEAM WANDERING

The prepare-measure scheme that has been demonstrated in Fig. 1 has always its entanglement-based version. That is, Alice produces an entangled state. She keeps one, and sends the other one. Although the prepare-measure scheme has much easier operation, the entanglement version is more tractable in handling the theoretical security proof. Therefore, we adopt the entanglement-based scheme to analyze the secret key rate. It has been concluded that the secret key rate depends on the covariance matrix of the bipartite entanglement state only, providing that the transmittance of channel does not randomly fluctuate [8], [21]. In such case, the covariance matrix has the form below

$$\mathrm{M} = \begin{pmatrix} (V_A+1)\,\mathbf{I}_2 & \sqrt{T\left(V_A^2+2V_A\right)}\sigma_z \\ \sqrt{T\left(V_A^2+2V_A\right)}\sigma_z & T\eta\left(V_A+1+\chi\right)\mathbf{I}_2 \end{pmatrix}, \quad (1)$$

where T is the transmittance of quantum channel; V_A is modulation variance; $\mathbf{I}_2$ denotes a unit matrix with size of 2×2; σ_z is the Pauli matrix of $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$; χ is noise; η is quantum efficiency of intradyne detector. Referring to Alice, χ can be written as $\chi = \chi_{\text{line}} + \chi_{\text{D}}/T$, where $\chi_{\text{line}} = 1/T - 1 + \xi_{\text{phase}} + \xi'$ denotes the excess noise with ξ_{phase} being phase noise and ξ' being the noise caused by attack from Eve, etc. χ_{D} represents the noise resulting from coherent detection. For the heterodyne detection, $\chi_{\text{D}} = (1+(1-\eta)+2V_{\text{el}})/\eta$, where V_{el} is the electrical noise of photon detector.

When the air quantum channel is involved, the air turbulence effects will cause the transmittance perturbation. Now the covariance matrix is characterized by the convex sum of the moments in the Eq. (1), namely, the ensemble average of

transmittance [16]. Eq. (1) becomes

$$\tilde{\mathrm{M}} = \begin{pmatrix} (V_A+1)\,\mathbf{I}_2 & \sqrt{\langle T\rangle\left(V_A^2+2V_A\right)}\sigma_z \\ \sqrt{\langle T\rangle\left(V_A^2+2V_A\right)}\sigma_z & \langle T\rangle\,\eta\,(V_A+1+\chi)\,\mathbf{I}_2 \end{pmatrix}, \quad (2)$$

where the operator $\langle\cdot\rangle$ indicates ensemble average.

Given that the beam wandering is dominant under weak turbulence conditions, a specific model has been proposed in [15] to describe the transmittance perturbation. This model is also employed in this paper; while, as we mentioned previously, we further incorporate the impact of phase distortion resulting from the air turbulence for the first time, which will be presented concretely in next section. The beam wandering leads to beam-center position varying randomly. Providing that the coordinates of beam-center position follow a two-dimensional Gaussian distribution, it can be easily concluded that the beam-deflection distance r away from the center position is a random variable which follows the Rice distribution. Also, the transmittance is a function of r with $T^2(r) = T_0^2 \exp\left[-\left(r/R\right)^2\right]$. Therefore, we can derive that the transmittance follows the log-negative Weibull distribution, and the PDF has expression of

$$p(T) = \begin{cases} \dfrac{2R^2}{\sigma^2\Gamma T}\left(2\ln\dfrac{T_0}{T}\right)^{\frac{2}{\Gamma}-1} \\ \exp\left[-\dfrac{R^2}{2\sigma^2}\left(2\ln\dfrac{T_0}{T}\right)^{\frac{2}{\Gamma}}\right], & \text{if} \quad T\in[0,T_0] \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

with parameters T_0, Γ and R being calculated by the incomplete Weber integral,

$$T_0^2 = 1-\exp\left(-2a^2/w^2\right), \quad (4)$$

$$\Gamma = 8\frac{a^2}{w^2}\frac{\exp\left(-4a^2/w^2\right)I_1\left(4a^2/w^2\right)}{1-\exp\left(-4a^2/w^2\right)I_0\left(4a^2/w^2\right)} \times\left[\ln\frac{2T_0^2}{1-\exp\left(-4a^2/w^2\right)I_0\left(4a^2/w^2\right)}\right]^{-1}, \quad (5)$$

$$R = a\left[\ln\frac{2T_0^2}{1-\exp\left(-4a^2/w^2\right)I_0\left(4a^2/w^2\right)}\right]^{-1/\Gamma}, \quad (6)$$

where a and w denotes beam spot radius at the receiving side and receiving aperture, respectively; $I_n(\cdot)$ is the Bessel function of n-th order; σ^2 represents the variance of optical beam center position around the receiving aperture center. Under weak air turbulence conditions, we have

$$\sigma^2 = 1.919C_n^2z^3\left(2w_0\right)^{-1/3}, \quad (7)$$

where C_n^2 is the air refractive index structure parameter in unit of $\mathrm{m}^{-2/3}$; z is the distance from Alice to Bob; w_0 indicates the spot size at source. w can be calculated by w_0 with [22]

$$w = \sqrt{w_0^2+\frac{\lambda^2z^2}{\pi^2w_0^2}}. \quad (8)$$

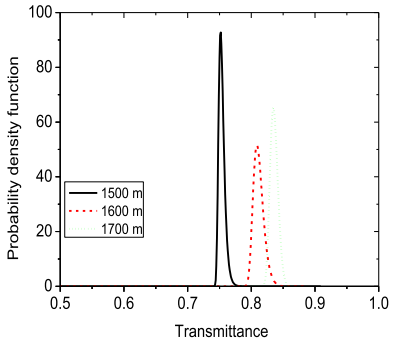

FIGURE 2. Transmittance perturbation caused by the beam wandering effect. The curves are created by assuming the parameters as follows. $w_0 = 0.01\mathrm{m}$; a=0.07m; $C_n^2 = 10^{-17}\ \mathrm{m}^{-2/3}$.

where λ is the wavelength of laser. As an example, the transmittance model with the PDF of log-negative Weibull distribution is demonstrated in Fig. 2. As the air link increases from 1500 m to 1700 m, the air turbulence clearly becomes stronger. Nevertheless, the beam size becomes larger, which is the dominant factor to the Eqs. (3)-(6). Accordingly, the PDF curve of transmittance moves towards the right side. It is worth to note that the perturbation level increases firstly, and it decreases subsequently in terms of the width of curves.

B. PHASE SHIFT RESULTING FROM PHASE DISTORTION

Due to the presence of air turbulence, the air refractive index fluctuates randomly in both space and time domains [14]. Accordingly, after the optical quantum signals propagate through the air channel, phase distortion will be induced. In the CV-QKD, the intradyne detector requires that the phase of coming signal matches that of local oscillator (LO). Obviously, the phase distortion will result in phase shift between signal and LO, thus leading to phase noise.

The phase noise can be described by the variance of phase distortion. Now let us proceed to the phase distortion resulting from the air turbulence. The phase distortion can be generated by employing the Monte-Carlo phase screen method [23]–[25]. Here we briefly outline this scheme. Providing that the Fourier series is adopted to express the phase distortion caused by air turbulence, we have

$$\theta(x,y) = \sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty} c_{mn}\exp\left[i2\pi\left(f_{x_m}x+f_{y_n}y\right)\right], \quad (9)$$

where f_x and f_y are the spatial frequencies in x and y axis, respectively, and c_{mn} denotes the coefficients of Fourier series. According to the Parseval's theorem, the power of phase equals in both space and frequency domains,

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left|\theta(x,y)\right|^2dxdy = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left|\Theta\left(f_x,f_y\right)\right|^2df_xdf_y. \quad (10)$$

where $\Theta\left(f_x,f_y\right)$ is the power spectrum density (PSD) function of turbulence-induced phase. Since c_{mn} follows the Gaussian distribution with mean of zero, then its variance can be

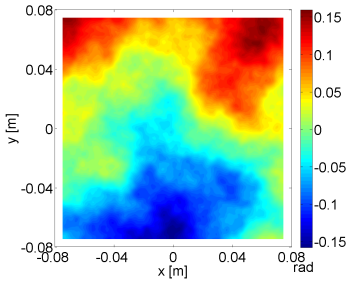

FIGURE 3. Phase distortion resulting from the air turbulence. The parameters are adopted as follows. $C_n^2 = 10^{-17}$ $m^{-2/3}$; $w_0 = 0.01$ m; $a = 0.07$ m; $z = 1500$ m; sampling array size is 512 × 512; in order to match the beam spot radius at the receiver w=0.0747 m, the sampling spacing requires 2.92×10^{-4} m.

calculated readily in terms of Eq. (10). With the calculated c_{mn}, the turbulence-induced phase can be produced by merely using the Inverse Fast Fourier Transform (IFFT).

To summarize, the phase screen scheme is to numerically generate the computer-sampling point array that matches the phase PSD function. There exist several models that reflect the phase distortion. Among them, the pump spectrum model is the most realistic one since it includes the turbulent cell factors and agrees with the pump behavior when the turbulent cell falls into small size. The pump spectrum model gives the analytical expression of PSD function [14]

$$\Phi_\phi(\kappa) = 0.49 r_0^{-5/3} \left[1 + 1.802\left(\frac{\kappa}{\kappa_l}\right) - 0.254\left(\frac{\kappa}{\kappa_l}\right)^{7/6}\right] \times \frac{\exp\left(-\kappa^2/\kappa_l^2\right)}{\left(\kappa^2 + \kappa_0^2\right)^{11/6}}, \quad \text{for } 0 \le \kappa < \infty, \tag{11}$$

where κ represents the spatial frequency; $\kappa_l = 3.3/l_0$ and $\kappa_0 = 2\pi/L_0$ with l_0 and L_0 being the inner and outer scale of turbulence, respectively; $r_0 = (0.423k^2 C_n^2 z)^{-3/5}$ denotes the atmospheric coherent diameter.

We have produced the phase distortion by the use of Monte-Carlo phase screen method, which is presented in Fig.3. As one can see, even air turbulence is in the weak region, it results in certain phase distortion within the range of $[-0.158, 0.159]$ rad and having variance of 0.0031 rad^2.

With the knowledge of phase distortion above, we are able to calculate the phase noise. Given that the variance of phase distortion is τ^2, the phase noise can be derived with the form [8]

$$\xi_{phase} = V_A\left[\tau^2 + \frac{1}{4}\tau^4\right]. \tag{12}$$

C. SECRET KEY RATE UNDER WEAK AIR TURBULENCE CONDITIONS

Under the collective attack, the secret key rate of CV-QKD can be given by the following expression

$$K = \beta I(a;b) - \left[S(\rho_{AB}) - S\left(\rho_{A|b}\right)\right], \tag{13}$$

where β denotes the reverse reconciliation efficiency; $I(a;b)$ represents the classical Shannon mutual information between Alice and Bob; $S(\rho)$ denoting the quantum von Neumann entropy of the quantum state ρ and $\chi_{\text{Holevo}} = S(\rho_{AB}) - S\left(\rho_{A|b}\right)$ is the Holevo bound with ρ_{AB} and $\rho_{A|b}$ being the Alice-Bob bipartite state and the quantum state held by Alice under the condition of measured information by Bob. As we mentioned, the secret key rate depends on the covariance matrix of Alice-Bob bipartite state only. When the air quantum channel is concerned, we have to substitute the transmittance with its ensemble average, as shown in Eq. (1). Therefore, for the CV-QKD over air quantum channel, Eq. (11) now becomes [26]

$$K = \int p(T)\left\{\beta I(a;b) - \left[S(\rho_{AB}) - S\left(\rho_{A|b}\right)\right]\right\} dT, \tag{14}$$

Firstly, the Shannon mutual information can be evaluated in the case of Gaussian modulation [27], [28].

$$I(a;b) = \log\left(\frac{V+\chi}{1+\chi}\right), \tag{15}$$

where $V = V_A + 1$. Next let us proceed to the Holevo bound. It is calculated in accordance with the von Neumann entropy. Mathematically, the von Neumann entropy $S(\cdot)$ is directly associated with the symplectic eigenvalues of the covariance matrices of quantum state ρ_{AB} and $\rho_{A|b}$. Accordingly, we can calculate $S(\cdot)$ with the formula

$$S(\rho) = \sum_i G(\varepsilon_i), \tag{16}$$

where ε_i is the i-th symplectic eigenvalue of the variance matrix of quantum state ρ, and $G(x) = \frac{x+1}{2}\log\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log\left(\frac{x-1}{2}\right)$. As a result, achieving the symplectic eigenvalues becomes the principal issue which requires to be addressed.

To calculate $S(\rho_{AB})$, we need to simplify its covariance matrix based on the preceding assumption. Since Eve can not access Alice and Bob's equipment, the noises from Bob's intradyne detector can be calibrated. By doing so, the covariance matrix of ρ_{AB}(i.e. Eq. (2)) reduces to [21]

$$\tilde{\mathrm{M}} = \begin{pmatrix} V\mathbf{I}_2 & \sqrt{\langle T\rangle\left(V^2-1\right)}\sigma_z \\ \sqrt{\langle T\rangle\left(V^2-1\right)}\sigma_z & \langle T\rangle\left(V+\chi_{line}\right)\mathbf{I}_2 \end{pmatrix} = \begin{pmatrix} a\mathbf{I}_2 & c\sigma_z \\ c\sigma_z & b\mathbf{I}_2 \end{pmatrix}. \tag{17}$$

When a matrix is the symmetric form as the Eq. (17), the symplectic eigenvalues can be calculated by

$$\varepsilon_{1,2}^2 = \left(A \pm \sqrt{A^2 - 4B}\right)\Big/2, \tag{18}$$

where A and B hold [27]

$$A = a^2 + b^2 - 2c^2 = V^2(1-2T) + 2T + T^2(V+\chi_{line})^2,$$
$$B = \left(ab - c^2\right)^2 = T^2\left(V\chi_{line} + 1\right)^2. \tag{19}$$

As to the entropy $S(\rho_{A|b})$, we also have to know the covariance matrix of quantum state $\rho_{A|b}$. Fortunately, given that Bob measures the entanglement state with the heterodyne detection, covariance matrix of $\rho_{A|b}$ is similar as that of $\rho_{A|B}$.

In such case, the symplectic eigenvalues of covariance matrix of state $\rho_{A|b}$ can be calculated by

$$\varepsilon_{3,4}^2 = \left(C \pm \sqrt{C^2 - 4D}\right)\Big/2, \quad \varepsilon_5 = 1 \tag{20}$$

with symbols C, D denotes [27]

$$C_{\text{hete}} = \frac{\left[A\chi_D^2 + B + 1 + 2\chi_D\left(V\sqrt{B} + T(V + \chi_{\text{line}})\right) + 2T\left(V^2 - 1\right)\right]}{[T(V+\chi)]^2};$$
$$D_{\text{hete}} = \left(\frac{V + \sqrt{B}\chi_D}{T(V+\chi)}\right)^2. \tag{21}$$

III. RESULTS AND DISCUSSIONS

Based on the analysis and derivation above, now we are able to perform the concrete numerical simulations to evaluate the secret key rate of CV-QKD over air quantum channel.

The parameters associated with air quantum channel are adopted as follows. Since the air link is assumed to be horizontal, the air refractive index structure parameter C_n^2 is a constant. Here we set $C_n^2 = 10^{-17}$ m$^{-2/3}$. The wavelength of laser λ =1550 nm, the waist of laser at the source (Alice) w_0 =0.005 m. the aperture of receiver (at Bob site) a = 0.15 m. The strength of air turbulence is measured by the Rytov variance $\Omega^2 = 1.23C_n^2 k^{7/6} z^{11/6}$. Based on this expression, the air turbulence becomes stronger as the propagation link increases. However, note that the air turbulence must be limited within weak region so that the log-negative Weibull model of transmittance is appropriate. $\Omega^2 < 1$ means weak air turbulence conditions. Therefore, the air quantum link does not allow beyond 10^5 m. By dint of those air parameters above, we evaluate the ensemble average of transmittance $< T >$ and variance of phase distortion τ^2 as the air link increases up to 2200 m, respectively, which is presented in Fig. 4.

Due to the random nature of air turbulence in time of $\sim$ ms in reality, we performed 1000 simulations of Monte-Carlo phase screen method for a given air link distance. The ensemble average of phase distortion variance can be obtained over those 1000 phase screens. From the Fig. 4, one can clearly see that as the air quantum link increases, the phase distortion becomes severer and its variance increases significantly. With respect to the ensemble average of transmittance, it becomes larger as the air link distance increases firstly. After the transmission distance exceeds 1700 m, the ensemble average of transmittance starts to go down gradually. Further, it decreases remarkably after distance of 1900 m.

With the results in hand, now we can analyze the secret key rate of CV-QKD over air quantum channel. Before specific calculations, we have to set the parameters related to CV-QKD. The Gaussian modulation variance $V_A = 2$. The reconciliation efficiency $\beta = 0.95$. The quantum efficiency of coherent detector $\eta = 0.7$. The remainder excess noise $\xi' = 0.001$. The electrical noise of detector $V_{\text{el}} = 0.01$. All variances are normalized to shot-noise-unit.

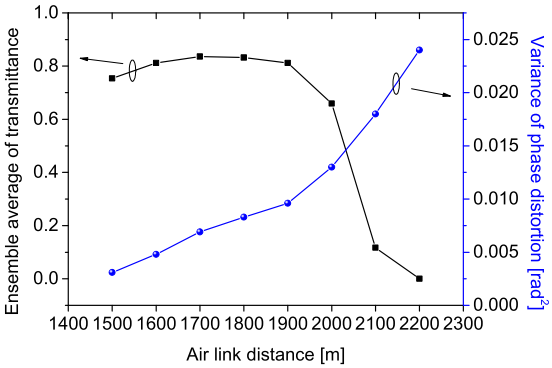

FIGURE 4. Ensemble average of transmittance and phase distortion variance under weak air turbulence conditions.

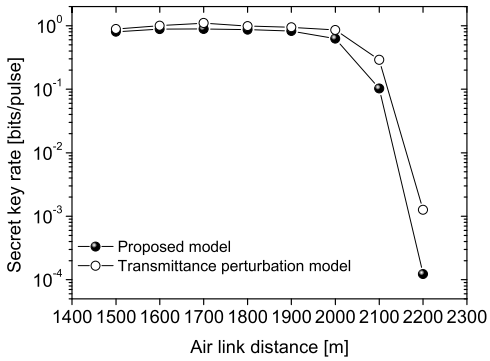

FIGURE 5. Secret key rate of CV-QKD over the air quantum channel in the presence of weak air turbulence.

By taking the achieved transmittance perturbation and phase shift into account, we are able to calculate the secret key rate of CV-QKD under weak air turbulence conditions. The concrete results are presented in Fig.5 below. As a comparison, we also plot the curve with respect to the existing model involving transmittance perturbation only.

As one can see, the phase shift resulting from the phase distortion obviously degrades the secret key rate further compared to the case that involves transmittance perturbation only. As a result, the existing model may overestimate the performance of CV-QKD. Our proposed model enables to offer a more realistic evaluation since it simultaneously takes the transmittance perturbation and phase distortion are simultaneously into account. Moreover, the secret key rate keeps unchanged approximately as the air quantum link increases at the outset. This is attributed to that the gain from ensemble average of transmittance and the degradation from phase shift reach a trade-off. However, when the air link distance increases over 1900 m, the secret key rate decreases strikingly since the both transmittance perturbation and the phase shift simultaneously deteriorate the performance of CV-QKD. Nevertheless, within the range of weak air turbulence level, the secret key is available. We should mention that it is of interest when the air turbulence enhances into medium/strong regime. In such case, the transmittance perturbation model in [15] is inappropriate, and other deleterious effects have to be considered as well [29]–[32], which we plan to study at our next step.

IV. CONCLUSION

We have analyzed the secret key rate of CV-QKD over air quantum channel by taking beam wandering and phase distortion into account. Under weak air turbulence conditions, the beam wandering is assumed to be the dominant factor causing the transmittance perturbation. The transmittance is modelled following the log-negative Weibull distribution. On the other hand, the phase distortion resulting from the air turbulence leads to the phase shift in the CV-QKD, thus impacts the secret key rate. The variance of phase distortion can be used to measure the phase noise. We have employed the Monte-Carlo phase screen method to evaluate the phase distortion variance. The numerical results revealed that the air turbulence effects including the beam wandering and phase distortion impact the performance of CV-QKD remarkably. Nevertheless, the CV-QKD can be executed under the weak air turbulence conditions. Since the CV-QKD could offer unconditional information security, we believe our results may offer potential applications for secure communications over the air channel.

ACKNOWLEDGMENT

The authors would like to thank Dr. J. Han at the Tianjin Key Laboratory of Wireless Mobile Communications and Power Transmission, Tianjin Normal University for his helpful suggestions.

REFERENCES

[1] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Rev. Mod. Phys.*, vol. 68, no. 3, pp. 733–753, Jul. 1996.
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. New York, NY, USA: Cambridge Univ. Press, 2010.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.
[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bengaluru, India, Dec. 1984, pp. 175–179.
[5] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010504.
[6] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002, Art. no. 057902.
[7] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, Jan. 2003.
[8] M. Li and M. Cvijetic, "Continuous-variable quantum key distribution with self-reference detection and discrete modulation," *IEEE J. Quantum Electron.*, vol. 54, no. 5, pp. 1–8, Oct. 2018.
[9] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, no. 12, pp. 6072–6092, Aug. 2015.
[10] M. Li and T. Wang, "Optimized coherent state based quantum cryptography with high robust for networks deployment," *IEEE Access*, vol. 7, pp. 109628–109634, 2019.
[11] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions [invited]," *Opt. Express*, vol. 26, no. 18, p. 24260, Aug. 2018.
[12] M. Li, "Orbital-angular-momentum multiplexing optical wireless communications with adaptive modes adjustment in Internet-of-Things networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6134–6139, Aug. 2019.
[13] R. J. Hughes and J. E. Nordholt, "Quantum space race heats up," *Nature Photon.*, vol. 11, no. 8, pp. 456–458, Aug. 2017.
[14] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. Bellingham, WA, USA: SPIE, 2005.
[15] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, no. 22, Jun. 2012, Art. no. 220501.
[16] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, "Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels," *New J. Phys.*, vol. 14, no. 9, Sep. 2012, Art. no. 093048.
[17] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, "Atmospheric continuous-variable quantum communication," *New J. Phys.*, vol. 16, no. 11, Nov. 2014, Art. no. 113018.
[18] S. Wang, P. Huang, T. Wang, and G. Zeng, "Atmospheric effects on continuous-variable quantum key distribution," *New J. Phys.*, vol. 20, no. 8, Aug. 2018, Art. no. 083037.
[19] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, no. 19, Nov. 2006, Art. no. 190502.
[20] M. Cvijetic and I. Djordjevic, *Advanced Optical Communication Systems and Networks*. Norwood, MA, USA: Artech House, 2013.
[21] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, May 2012.
[22] R. L. Phillips and L. C. Andrews, "Spot size and divergence for Laguerre Gaussian beams of any order," *Appl. Opt.*, vol. 22, no. 5, pp. 643–644, Mar. 1983.
[23] J. D. Schmidt, *Numerical Simulation of Optical Wave Propagation With Examples in MATLAB*. Bellingham, WA, USA: SPIE, 2010.
[24] M. Li and M. Cvijetic, "Coherent free space optics communications over the maritime atmosphere with use of adaptive optics for beam wavefront correction," *Appl. Opt.*, vol. 54, no. 6, pp. 1453–1462, Feb. 2015.
[25] M. Li, M. Cvijetic, Y. Takashima, and Z. Yu, "Evaluation of channel capacities of OAM-based FSO link with real-time wavefront correction by adaptive optics," *Opt. Express*, vol. 22, no. 25, pp. 31337–31346, Dec. 2014.
[26] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 3, Mar. 2018, Art. no. 032311.
[27] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers," *J. Phys. B, At. Mol. Opt. Phys.*, vol. 42, no. 11, May 2009, Art. no. 114014.
[28] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, no. 4, Oct. 2015, Art. no. 041009.
[29] X. Zhu and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1293–1300, Aug. 2002.
[30] V. W. S. Chan, "Free-space optical communications," *J. Lightw. Technol.*, vol. 24, no. 12, pp. 4750–4762, Dec. 1, 2006.
[31] M. Li, "Phase corrections with adaptive optics and gerchberg-saxton iteration: A comparison," *IEEE Access*, vol. 7, pp. 147534–147541, 2019.
[32] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, Jun. 2014.

MING LI received the Ph.D. degree in electronic science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015.

Since 2015, he has been an Assistant Professor with the College of Electronic and Communication Engineering, Tianjin Normal University, Tianjin, China. His research interests include optical quantum communications and optical wireless communications.

TIANYI WANG received the Ph.D. degree in communication and information systems from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015.

Since 2015, he has been an Assistant Professor with the College of Big Data and Information Engineering, Guizhou University, Guiyang, China. His research interests include continuous variable quantum key distribution and quantum information processing.