Research on measurement-device-independent quantum key distribution based on an air-water channel*

ZHOU Yuan-yuan (周媛媛), ZHOU Xue-jun (周学军), XU Hua-bin (徐华彬), and CHENG Kang (程康)**
Electronic Engineering College, Naval University of Engineering, Wuhan 430033, China

(Received 12 September 2016; Revised 11 October 2016)

A measurement-device-independent quantum key distribution (MDI-QKD) method with an air-water channel is researched. In this method, the underwater vehicle and satellite are the legitimate parties, and the third party is at the air-water interface in order to simplify the unilateral quantum channel to water or air. Considering the condition that both unilateral transmission distance and transmission loss coefficient are unequal, a perfect model of the asymmetric channel is built. The influence of asymmetric channel on system loss tolerance and secure transmission distance is analyzed. The simulation results show that with the increase of the channel's asymmetric degree, the system loss tolerance will descend, one transmission distance will be reduced while the other will be increased. When the asymmetric coefficient of channel is between 0.068 and 0.171, MDI-QKD can satisfy the demand of QKD with an air-water channel, namely the underwater transmission distance and atmospheric transmission distance are not less than 60 m and 12 km, respectively.

Document code: A **Article ID:** 1673-1905(2016)06-0469-4
DOI 10.1007/s11801-016-6198-8

In recent years, the research of quantum key distribution (QKD)[1] has made a breakthrough in the improvement of system security and performance[2-9]. In particular, the combination of measurement-device-independent quantum key distribution (MDI-QKD)[10] and decoy-state idea[4] makes the security and performance of QKD to a new level[11-14] in the existing technical condition. But the current research of QKD is mainly based on homogeneous or similar homogeneous medium, such as optical fiber or free space. However, people hope that QKD can adapt to more complex transmission media and meet more communication needs. Since 2011, some scholars have proposed using an optical channel to facilitate a two-way communication link between the satellite and underwater vehicle via perfectly secure ciphers enabled by a QKD protocol[15,16]. In this scheme, the quantum signal needs to go through the free space, the air-water interface and the sea water, which is an unprecedented challenge[16,17].

This paper will discuss the MDI-QKD method with an air-water channel. The method sets the third party at the air-water interface to simplify the unilateral quantum channel to sea water or air, exert the superiority of MDI-QKD, and satisfy the transmission requirement of QKD with an air-water channel.

As shown in Fig.1, the satellite and underwater vehicle are two legitimate users in our method. They don't make any measurement, just prepare quantum states, encode bit information and send them to an untrusted third party, Charlie or Eve. The third party is a sea platform at the air-water interface, such as a ship or a communication buoy. Charlie performs the Bell state measurement (BSM) and tells her results to Alice and Bob, then Alice and Bob can use this information to distill a secret key. In this method, there is no need for quantum signal to go through different media. The quantum signal in channel A only needs to pass through about 10—12 km troposphere and then can easily reach the satellite. The quantum signal in

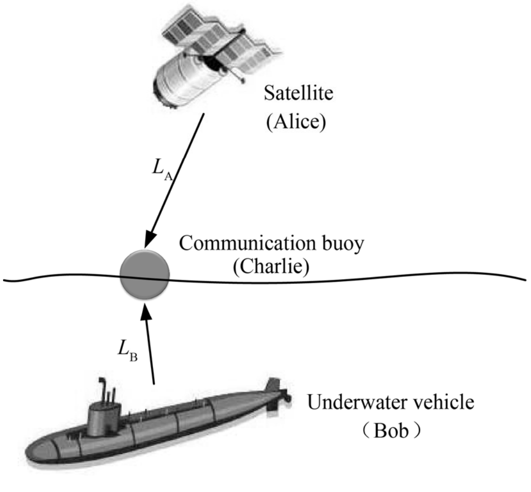


Fig.1 The system diagram of MDI-QKD with an air-water channel

* This work has been supported by the National Natural Science Foundation of China (No.61302099).

** E-mail: zyy_hjgc@aliyun.com

channel B only needs to go through the sea water. Compared with the standard QKD with an air-water channel, this method simplifies the channel. It is important to notice that channel B needs to be operational at depths greater than the mixed layer (60—100 m)[16], so the underwater vehicle will not reveal its location to an active surface sonar.

In this method, both the distances and the transmission attenuation coefficients from Alice (Bob) to Charlie are different. Ref.[18] analyzed the performance of MDI-QKD with unequal unilateral distance. This paper will improve the model of asymmetric channel, considering asymmetric transmission distance and asymmetric transmission attenuation coefficient.

We define L_A, L_B, α_A and α_B to be the transmission distances and transmission attenuation coefficients from Alice and Bob to Charlie, respectively. Let η_D denote the detection efficiency, and we assume that all detectors' efficiencies are the same in this paper. β_A and β_B mean the unilateral transmission attenuations in Alice side and Bob side, respectively, $\beta_A=\alpha_A L_A$ and $\beta_B=\alpha_B L_B$. Let $\beta=(\beta_A+\beta_B)/2$. The channels with equal unilateral transmission attenuation are defined as symmetric channels, i.e., $\beta_A=\beta_B=\beta$. Then, the channel transmittance can be expressed as

$$t=t_A=t_B=10^{-\beta/10} \quad . \tag{1}$$

Then, we can obtain the local transmittance as following expression

$$\eta=\eta_A=\eta_B=t\eta_D \quad . \tag{2}$$

The channels are asymmetric when $\beta_A \neq \beta_B$. One side local channel transmittance must be reconsidered as

$$t_{\mathrm{A}}=10^{-\beta_{\mathrm{A}}/10} \quad , \tag{3}$$

$$t_{\mathrm{B}}=10^{-\beta_{\mathrm{B}}/10} \quad . \tag{4}$$

Define $\kappa=\beta_A/\beta_B$ as the ratio of channel transmission loss. We call it channel asymmetry coefficient which indicates the asymmetric degree of channel. Here we assume $0 \leq\kappa \leq 1$. When $\kappa=0$, the Bell state measurement occurs at Alice's private space, and when $\kappa=1$, the asymmetric MDI-QKD degenerates to a symmetric MDI-QKD.

The unilateral channel transmittance of an asymmetric MDI-QKD can be deduced by Eqs.(1), (2), (3) and (4) as

$$t_{\mathrm{A}}=t^{2\kappa/(1+\kappa)} , \tag{5}$$

$$t_{\mathrm{B}}=t^{2/(1+\kappa)} . \tag{6}$$

In this method, Alice and Bob respectively prepare three kinds of pulses with different intensities, denoted as u_0, u_1, u_2 and v_0, v_1, v_2. The intensities u_i and v_j correspond to vacuum state, decay state and signal state, respectively. Without loss of generality, we assume that $u_2>u_1>u_0=0$, $v_2>v_1>v_0=0$. When Alice's pulse intensity is u and Bob's pulse intensity is v, Q_{uv} and E_{uv} are used to denote the overall gain and quantum bit error rate ($QBER$), respectively.

$$Q_{uv}^{\omega}=\sum_{n,m=0}^{\infty}\frac{u^n v^m}{n!m!}\mathrm{e}^{-u-v}Y_{nm}^{\omega} , \tag{7}$$

$$E_{uv}^{\omega}Q_{uv}^{\omega}=\sum_{n,m=0}^{\infty}\frac{u^n v^m}{n!m!}\mathrm{e}^{-u-v}Y_{nm}^{\omega}e_{nm}^{\omega} , \tag{8}$$

where the basis is $\omega=x, z$. Y_{nm}^{ω} (e_{nm}^{ω}) is the yield (error rate) when Alice sends n-photon pulse, Bob sends m-photon pulse, and the basis ω is used by them.

Alice and Bob can estimate the secret key rate using the following formula

$$R \geq u_2 v_2 \mathrm{e}^{-u_2-v_2} Y_{11}^{z}\left[1-H_2\left(e_{11}^{x}\right)\right]-$$

$$Q_{u_2 v_2}^{z} f H_2\left(E_{u_2 v_2}^{z}\right) , \tag{9}$$

where $f(x)$ is the bidirectional error correction efficiency, $H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$.

The parameters in Eq.(9) are given by[19]

$$Q_{uv}^{x}=2y^2\left[1+2y^2-4yI_0\left(s\right)+I_0\left(2s\right)\right], \tag{10}$$

$$E_{uv}^{x}Q_{uv}^{x}=e_0 Q_{uv}^{x}-2\left(e_0-e_{\mathrm{d}}\right)y^2\left[I_0\left(2s\right)-1\right], \tag{11}$$

where $I_0(s)$ is the modified Bessel function of the first kind,

$$Q_{uv}^{z}=Q_{\mathrm{C}}+Q_{\mathrm{E}} , \tag{12}$$

$$E_{uv}^{z}Q_{uv}^{z}=e_{\mathrm{d}}Q_{\mathrm{C}}+\left(1-e_{\mathrm{d}}\right)Q_{\mathrm{E}} , \tag{13}$$

where

$$Q_{\mathrm{C}}=2\left(1-P_{\mathrm{d}}\right)^2 \mathrm{e}^{-u'/2}\left[1-\left(1-P_{\mathrm{d}}\right)\mathrm{e}^{-\eta_{\mathrm{A}}u/2}\right]\times$$

$$\left[1-\left(1-P_{\mathrm{d}}\right)\mathrm{e}^{-\eta_{\mathrm{B}}v/2}\right], \tag{14}$$

$$Q_{\mathrm{E}}=2P_{\mathrm{d}}\left(1-P_{\mathrm{d}}\right)^2 \mathrm{e}^{-u'/2}\times$$

$$\left[I_0\left(2s\right)-\left(1-P_{\mathrm{d}}\right)\mathrm{e}^{-u'/2}\right]. \tag{15}$$

The expression of u' must be modified for the asymmetric channel. According to Eqs.(5) and (6), we can obtain

$$u'=t^{(2\kappa/1+\kappa)}\eta_{\mathrm{D}}u+t^{(2/1+\kappa)}\eta_{\mathrm{D}}v , \tag{16}$$

$$s=\sqrt{\eta_{\mathrm{A}}u\eta_{\mathrm{B}}v}/2 , \tag{17}$$

$$y=\left(1-P_{\mathrm{d}}\right)\mathrm{e}^{-u'/4} . \tag{18}$$

Y_{11} and e_{11} are given by[11]

$$Y_{11}^x = Y_{11}^z = \left(1-P_d\right)^2\left[\frac{\eta_A\eta_B}{2} + \right.$$

$$\left.\left(2\eta_A + 2\eta_B - 3\eta_A\eta_B\right)P_d + 4\left(1-\eta_A\right)\left(1-\eta_B\right)P_d^2\right], \quad (19)$$

$$e_{11}^x Y_{11}^x = e_0 Y_{11}^x - \left(e_0 - e_d\right)\left(1-P_d\right)^2 \frac{\eta_A\eta_B}{2}, \quad (20)$$

$$e_{11}^z Y_{11}^z = e_0 Y_{11}^z - \left(e_0 - e_d\right)\left(1-P_d\right)^2 \left(1-2P_d\right)\frac{\eta_A\eta_B}{2}. \quad (21)$$

In the simulation, the optical sources of the satellite and underwater vehicle by strong attenuation produce the optical pulses with a wavelength of 550 nm. The typical values of the attenuation coefficients in the troposphere and sea water are α_A=0.2 dB/km, α_B=230 dB/km[16]. After quantum signal goes through the troposphere for about 10—12 km, the loss caused by atmosphere can be negligible. We assume u_1=v_1=0.1 and u_2=v_2=0.5. Other parameters are from Ref.[20]: P_d=3×10^{-6}, e_d=1.5%, η_D=0.3, f=1.16. Now, by substituting the bounds of Y_{11} and e_{11} into Eq.(9), the final key rate of MDI-QKD can be calculated.

As shown in Fig.2, with the decrease of the channel asymmetry coefficient κ, the channel transmittance of Alice side increases while that of Bob side descends. Therefore, we can choose an appropriate value of κ for an optimal distribution of the transmission performance in the sea water and atmosphere.

In Fig.3, the tolerated channel loss increases with the rising of κ. When κ=0, the maximal tolerated channel loss is 36 dB, and when κ=1, the maximal tolerated channel loss can reach 62 dB.

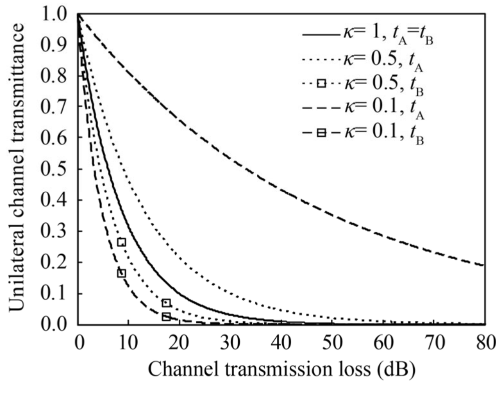


Fig.2 The unilateral channel transmittance as a function of the channel transmission loss

But κ=1 is not the optimal choice for the MDI-QKD with an air-water channel. Fig.4 shows that the transmission distances of Alice side (L_A) and Bob side (L_B) change oppositely. With the increase of κ, L_A increases while L_B descends.

As shown in Fig.5(a), when L_A=12 km which is the troposphere thickness weakening the quantum signals, the channel asymmetry coefficient κ must be less than 0.171 for underwater vehicle's secure communication at a least depth of 60 m. In Fig.5(b), when κ<0.068, the factual channel transmission loss exceeds the maximal tolerated channel loss of MID-QKD system. Therefore, when 0.068<κ<0.17, 60 m<L_B<152 m and the distance fully meets the requirement of underwater vehicle's covert communication.

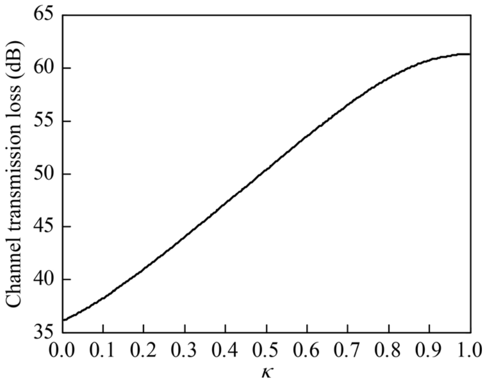
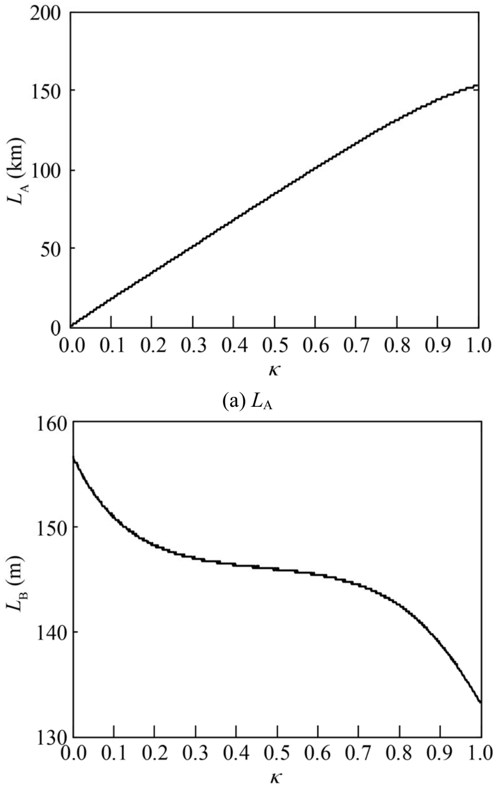


Fig.3 The channel transmission loss as a function of the channel asymmetry coefficient *κ*



(a) L_A

(b) L_B

Fig.4 The unilateral transmission distance as a function of the channel asymmetry coefficient *κ*

In summary, this paper investigates an MDI-QKD method with an air-water channel. In this method, the underwater vehicle and satellite are the legitimate users, and the third party is set at the air-water interface to sim-

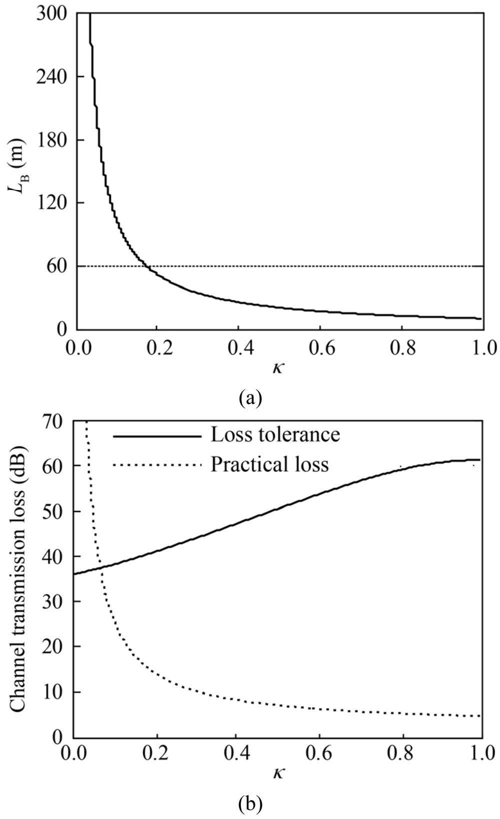


Fig.5 (a) L_B and (b) the channel transmission loss as a function of the channel asymmetry coefficient κ with L_A=12 km

plify the unilateral quantum channel to sea water or air. A perfect model of the asymmetric channel is built. The influence of asymmetric channel on system loss tolerance and secure transmission distance is analyzed. The simulation results show that with the increase of the channel's asymmetric degree, the system loss tolerance will descend from 62 dB to 36 dB, one transmission distance will be reduced and the other will be increased. For the air-water channel, symmetrical channel (κ=1) is not the optimal choice. When the asymmetric coefficient of channel is between 0.068 and 0.171, MDI-QKD can satisfy the demand of underwater vehicle's covert communication. When the transmission distance in the aerosphere is 12 km, the underwater transmission distance is not less than 60 m and the farthest distance can reach 152 m.

References

[1] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in Proceedings of IEEE International Conference on Computers, Syetems and Signal Processing **175**, 1984.

[2] W Y Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[3] Y. Y. Zhou, X. J. Zhou, P. G. Tian and Y. J. Wang, Chin. Phys. B **22**, 010305 (2013).

[4] F H Xu, Phys. Rev. A **92**, 012333 (2015).

[5] Y. Y. Zhou and X. J. Zhou, Optoelectron. Lett. **11**, 0149 (2015).

[6] R Rahaman, M G Parker, P Mironowicz and M Pawlowski, Phys. Rev. A. **92**, 062304 (2015).

[7] E A Aguilar, R Ramanathan, J Kofler and M Pawlowski, Phys. Rev. A **94**, 022305 (2016).

[8] Y H Zhou, Z W Yu and X B Wang, Phys. Rev. A **93**, 042324 (2016).

[9] M Schiavon, G Vallone, F Ticozzi and P Villoresi, Phys. Rev. A **93**, 012331 (2016).

[10] H. K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[11] X F Ma, C-H F Fung and M Razavi, Phys. Rev. A **86**, 052305 (2012).

[12] Z Y Tang, K J Wei, O Bedroya, L Qian and H L Lo, Phys. Rev. A **93**, 042308 (2016).

[13] Y. Y. Zhou, X. J. Zhou and B B Su, Optoelectron. Lett. **12**, 0149 (2016).

[14] D Chen, S H Zhao, L Shi and Y Liu, Phys. Rev. A **93**, 032320 (2016).

[15] J ARON, New Scientist **212**, 23 (2011).

[16] L MARCO, Underwater Communications, Morgan: Claypool Publishers, 82 (2012).

[17] F Zhou, H L Yong, D D Li, J Yin, J G Ren and C Z Peng, Acta Phys. Sin. **63**, 140303 (2014). (in Chinese)

[18] C Dong, S H Zhao, W H Zhao, L Shi and G H Zhao, Acta Phys. Sin. **63**, 030302 (2014). (in Chinese)

[19] X F Ma and M Razavi, Phys. Rev. A **86**, 062319 (2012).

[20] S H Sun, M Gao, C Y Li and L M Liang, Phys. Rev. A **87**, 052329 (2013).