Satellite-based measurement-device-independent quantum key distribution

Wentao Liang\textsuperscript{1} and Rongzhen Jiao\textsuperscript{1,2,3}

1 School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, People’s Republic of China
2 State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, People’s Republic of China
3 Author to whom any correspondence should be addressed.
E-mail: rzjiao@bupt.edu.cn

Keywords: measurement-device-independent quantum key distribution, satellite links, free space

Abstract

A satellite-based measurement-device-independent quantum key distribution model is proposed and its performance is analyzed through numerical simulations. The simulation result shows that the key rate increases almost linearly as transmittance increases and the higher the key rate is, the lower its probability may be. More significantly, as the transmission distance increases, the optimal intensities of the signal states decrease while those of the decoy states increase. The optimal values in the daytime are slightly larger than those at night. This work may provide some important parameters for the relevant experiment on satellite-based quantum communication network.

1. Introduction

Quantum key distribution (QKD) allows two distant parties (Alice and Bob) to share confidential information securely [1–3]. QKD theoretically guarantees unconditional security but real-world devices can not meet the assumed requirements, so it may be attacked by the eavesdropper (Charles) [4–7]. Many techniques have been proposed to address the vulnerabilities caused by imperfected devices such as the decoy-state technique [8–10] and measurement-device-independent quantum key distribution (MDI–QKD) [11]. In recent years, MDI–QKD combined with the decoy-state technique has become the mainstream and has been widely studied both theoretically [12–14] and experimentally [15–17].

In fiber-based networks, the high loss of fiber has become the main reason for limiting the transmission distance. Fortunately, schemes utilizing satellite links have been proposed to achieve longer distance quantum communication in recent years. For example, Oi et al. used the micro satellite SOCRATES to demonstrate a QKD experiment with an average quantum error rate of less than 5% [18] and Liao et al. used the quantum satellite Micius to complete a number of experiments on satellite-ground quantum communication [19–22]. Since fiber-based networks have been well developed, in order to establish worldwide quantum communication networks at lower cost, satellite-based quantum channels and fiber-based networks should be effectively integrated. Hence, the performance of satellite-based QKD protocols combined with fiber-based networks needs to be studied. Satellite-based MDI–QKD proposed in this paper can easily solve detector vulnerabilities caused by imperfect devices in real life and prolong the transmission distance. In previous demonstration, the longest transmission distance of MDI–QKD in optical fiber is only 404 km [16], while satellite-based MDI–QKD combined with fiber-based networks can easily reach more than 500 km. Satellite-based MDI–QKD can make full use of fiber-based networks and satellite channels, thus promoting the establishment of global quantum communication networks.

This work is organized as follows. In section 2, the theory of the satellite-based MDI-QKD is briefly introduced. In section 3, the main simulation and optimization results are shown and discussed. Finally, the conclusion is given in section 4.
2. Theory

In satellite-based MDI–QKD, Alice and Bob randomly prepare their quantum states and send them to Charles, who will perform the Bell state measurement. Inside the measurement device, the photons from Alice and Bob interfere at a 50:50 beam splitter and then are projected into either horizontal or vertical polarization states through a polarizing beam splitter and finally are being detected by the signal-photon detector. Note that the photons from Alice are at 1550 nm while the photons from Bob are in the visible range, so the optical transponder unit (OTU) is needed to convert the wavelength of Bob’s photons to the same as Alice’s before measurement [23, 24]. After the Bell state measurement, the detection results are announced in the public channel. Based on the announcement, Alice and Bob can decide whether to flip their bits or not and then distill the secure key. Unlike the original MDI–QKD protocol, Alice and Charles are on the ground, while Bob is in the outer space, as seen in figure 1. Hence, Alice uses the fiber channels in which transmittance ratio can be described as:

\[ t = 10^{-\alpha L/10} \]

(\( \alpha \) and \( L \) denotes the channel loss coefficient and the transmission distance respectively) to send her states to Charles, while Bob utilizes the satellite links whose transmittance can be modeled by the probability distribution of the transmittance (PDT) [25]. In real life application, the case that Alice inside the city and Charles outside the city is better because it can make full use of fiber-based networks and avoid extra light pollution at the receiver.

The final key rate in satellite-based MDI–QKD is averaged over the PDT and is given by [25]

\[ \bar{R} = \int_0^1 R(\eta)P(\eta) d\eta = \sum_{i=1}^{N_{\text{bins}}} R(\eta_i)P(\eta_i). \]  

(1)

Where \( \bar{R} \) is the average (final) key rate, \( R(\eta) \) is the key rate at the specific value of the transmittance, \( P(\eta) \) is the PDT. The integral average is approximated dividing the range [0, 1] in \( N \) bins and taking the weighted sum of the key rate. When using weak coherent pulses source with decoy states, \( R(\eta) \) can be calculated by [11]

\[ R(\eta) \geq P_{\bar{Z}}^+ Y_{\bar{Z}}^+ \left[ 1 - H_{\bar{Z}} \left( e_{\bar{X}}^+ \right) \right] - Q_{\bar{Z}} f_\epsilon \left( E_{\bar{Z}} \right) H_{\bar{Z}} \left( E_{\bar{Z}} \right). \]  

(2)

Where \( P_{\bar{Z}}^+ \) is the probability that both Alice and Bob send single-photon in the rectilinear (Z) basis; \( Y_{\bar{Z}}^+ \) and \( e_{\bar{X}}^+ \) is the single-photon yield in the Z basis and the single-photon error rate in the diagonal (X) basis respectively; \( H_{\bar{Z}}(x) \) is the binary entropy function given by \( H_{\bar{Z}}(x) = -x \log_2(x) - (1-x) \log_2(1-x) \); \( Q_{\bar{Z}} \) and \( E_{\bar{Z}} \) is the gain and quantum bit error rate (QBER) in the Z basis respectively; \( f_\epsilon \geq 1 \) is the error correction
inefficiency function. Generally, $Q_{Z}$ and $E_{Z}$ can be measured directly, while $Y_{Z}^{11}$ and $e_{X}^{11}$ need to be estimated.

3. Simulation results

In this section, the distance between Bob and Charles is fixed at 500 km because the case of Low-Earth-Orbit satellites such as the Chinese satellite Micius is focused on. Numerical simulation results of satellite-based MDI–QKD using the vacuum + weak decoy states scheme in the asymptotic case are given. The experimental parameters used in simulations are listed in table 1 [25–27].

Firstly, the intensities of Alice’s (Bob’s) signal states $μ_{a}$ ($μ_{b}$) and decoy states $ν_{a}$ ($ν_{b}$) are set to 0.3 (0.5) and 0.003 (0.005) respectively. When the distance between Bob and Charles is fixed at 500 km, the transmittance of down-link ranges from 0 to 0.12 [25]. When the distance between Alice and Charles ($L_{A}$) is fixed at 0 km, the key rate increases almost linearly with the increase of transmittance, as shown in figure 2. The key rate equals to zero at the beginning because the transmittance is too low to transmit information. Next, the probability distribution of the key rate (PDR) is obtained through the key rate and PDT, as illustrated in figure 3. The simulation result shows that the higher the key rate is, the lower its probability may be.
With PDR, the final key rate of different $L_A$ can be easily calculated (only need to take the weighted sum of the key rate according to its probability) and is shown in figure 4. The maximum value of the key rate is $1.5988 \times 10^{-5}$ per pulse and the longest transmission distance is 120 km. Note that the results are not optimal since the intensities of Alice’s (Bob’s) signal and decoy states are set to the fixed values. In addition, a further discussion about PDR of different $L_A$ is given. As can be seen from figure 5, with the increase of $L_A$, the key rate decreases on the whole while the shape of PDR remains the same due to the unchanged PDT.

Since the above results are not optimal, parameter optimization should be taken into account to improve the performance of the protocol. As shown in figure 6, the key rate is higher and the transmission distance is longer after using the optimal intensities of the signal and decoy states. Compared with the key rate using $\mu_a = 0.3, \nu_a = 0.003, \mu_b = 0.5, \nu_b = 0.005$, the maximum key rate using the optimal intensities is $2.3098 \times 10^{-5}$ per pulse, increasing by 44.47% and the longest transmission distance is 145 km, increasing by 20.83%. The optimal intensities of different $L_A$ under different atmospheric conditions (see [25] for more details) are shown in figure 7. As can be seen, with the increase of the transmission distance, the optimal intensities of the signal states decrease while those of the decoy states increase no matter what atmospheric condition is. The optimal values during the day are slightly larger than those at night.
4. Conclusion

In this paper, the performance of satellite-based MDI–QKD combined with fiber-based networks is analyzed. When the distance between Bob and Charles is fixed at 500 km and the distance between Alice and Charles is fixed at 0 km, the key rate increases almost linearly as transmittance increases and the higher the key rate is, the lower its probability may be. With PDR, the final key rate of different $L_A$ has been calculated and displayed. After parameter optimization, the key rate and the transmission distance increased by 44.47% and 20.83% respectively. It is also found that with the increase of $L_A$, the key rate decreases as a whole while the shape of PDR remains unchanged. More significantly, the optimal intensities of different $L_A$ under different atmospheric conditions are given. These simulation results may provide some important parameters for the relevant experiment on satellite-based quantum communication network.

Acknowledgments

This work is supported by the Fundamental Research Funds for the Central Universities (No.2019XD-A02), Ministry of Science and Technology of China (No.2016YFA0301300) and National Natural Science Foundation of China (No. 61571060).
References

[1] Bennett C H and Brassard G 2014 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. Comput. Syst. Signal Process 560 7
[2] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661
[3] Gisin N et al 2002 Quantum cryptography Rev. Mod. Phys. 74 145
[4] Huttner B et al 1995 Quantum cryptography with coherent states Phys. Rev. A 51 1863
[5] Scarani V et al 2009 The security of practical quantum key distribution Rev. Mod. Phys. 81 1301
[6] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution Nat. Photon. 8 595
[7] Diamanti E et al 2016 Practical challenges in quantum key distribution npj Quantum Inf. 2 16025
[8] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication Phys. Rev. Lett. 91 5
[9] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution Phys. Rev. Lett. 94 230504
[10] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography Phys. Rev. Lett. 94 230503
[11] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution Phys. Rev. Lett. 108 130503
[12] Wang Y-H, Yu Z-W and Wang X-B 2016 Making the decoy-state measurement-device-independent quantum key distribution practically useful Phys. Rev. A 93 042324
[13] Wang Q, Zhou X-Y and Guo G-C 2016 Realizing the measure-device-independent quantum-key-distribution with passive heralded-single photon sources Sci. Rep. 6 35394
[14] Jiang C, Yu Z-W and Wang X-B 2016 Measurement-device-independent quantum key distribution with source state errors in photon number space Phys. Rev. A 94 062323
[15] Comandar L C et al 2016 Quantum key distribution without detector vulnerabilities using optically seeded lasers Nat. Photon. 10 312
[16] Yin H-L et al Measurement-device-independent quantum key distribution over a 404 km optical fiber Phys. Rev. Lett. 117 190501
[17] Wang C et al Measurement-device-independent quantum key distribution robust against environmental disturbances Optica 4 1016
[18] Oi D K L et al 2017 Cubesat quantum communications mission EPJ Quantum Technol. 4 6
[19] Liao S-K et al 2017 Satellite-to-ground quantum key distribution Nature 549 43
[20] Ren J-G et al 2017 Ground-to-satellite quantum teleportation Nature 549 70
[21] Yin J et al 2017 Satellite-based entanglement distribution over 1200 kilometers Science 356 1140–4
[22] Yin J et al 2017 Satellite-to-satellite entanglement-based quantum key distribution Phys. Rev. Lett. 119 200501
[23] Zaske S et al 2012 Visible-to-telecom quantum frequency conversion of light from a single quantum emitter Phys. Rev. Lett. 109 147403
[24] De Greve K et al 2012 Quantum-dot spin–photon entanglement via frequency downconversion to telecom wavelength Nature 491 421
[25] Liorini C, Kampermann H and Brub D 2019 Satellite-based links for quantum key distribution: beam effects and weather dependence New J. Phys. 21 093055
[26] Ma X, Fung C-H F and Razavi M 2012 Statistical fluctuation analysis for measurement-device-independent quantum key distribution Phys. Rev. A 86 052305
[27] Xu F, Xu H and Lo H-K 2014 Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution Phys. Rev. A 89 052333