Free-space measurement-device-independent quantum key distribution under strong atmospheric turbulence

Dong Chen[1,2], Ding De-Qiang[1], Li Wei[1], Zhao Wei-Hu[1]

[1]Information and Communication College, National University of Defense and Technology, Xi'an 710006, China

[2]State Key Laboratory of Cryptology, P.O.Box5159, Beijing, 100878, China

Abstract:

The atmospheric turbulence, which causes local refractive index fluctuations, has specific effect for fluctuations of channel transmittance in free-space quantum key distribution. In this paper, a free space measurement-device-independent quantum key distribution (MDI-QKD)scheme is analyzed under strong atmospheric turbulence, where the gamma-gamma distribution is used to model the strong atmospheric turbulence. Compared with the original MDI-QKD protocols with weak atmospheric turbulence described by log-normal distribution, the numerical simulations show that our modified scheme has apparent improvements both in transmission distance and key generation rate.

Free-space QKD based on satellite has become an attractive and feasible proposition to over the problem[1]. However, Atmospheric turbulence is the major loss factor, which influences QKD performance by causing fluctuations in channel transmittance. The log-normal distribution is widely applied to simulate weak turbulence, but it can not be directly used to estimate the channel transmission rate correctly in the case of strong turbulence. The gamma-gamma distribution can be used to mimic real atmospheric turbulence, since it is suitable for the entire range of turbulent conditions.

In this paper, a free space measurement-device-independent quantum key distribution (MDI-QKD) scheme is analyzed under strong atmospheric turbulence, where the gamma-gamma distribution is used to model the strong atmospheric turbulence. And we adopt the threshold real-time selection method[2] to improve the performance of our modified MDI-QKD protocol. The simulation results emerge that the performance of our scheme is greatly improved in the key generation rate and robustness.

Alice and Bob independently prepare weak coherent pulses in the rectilinear (Z) or diagonal (X) basis with decoy states, while the measurement process is performed by an untrusted third party. In asymptotic case, the secure key rate R can be derived as follows:

$$R \geq \mu_2 \nu_2 e^{-\mu_2-\nu_2} Y_{11}^{Z}[1-H(e_{11}^{X})]-Q_{\mu_2\nu_2}^{Z} f(E_{\mu_2\nu_2}^{Z}) H(E_{\mu_2\nu_2}^{Z}) \tag{1}$$

we adopt the gamma-gamma distribution which is a first choice to satisfy the significant requirement[4]. The probability distribution of transmission rate can be represented:

$$P_{\sigma_0,\eta_0}(\eta)=\frac{2(\alpha\beta)^{(\alpha+\beta)}\eta^{(\alpha+\beta)/2-1}}{\Gamma(\alpha)\Gamma(\beta)\eta_0^{(\alpha+\beta)/2}} K_{\alpha-\beta}(2\sqrt{\alpha\beta\frac{\eta}{\eta_0}}) \tag{2}$$

In conclusion, we proposed a free-space MDI-QKD scheme with the gamma distribution to model the strong atmospheric turbulence. Compared with the original MDI-QKD protocols with weak atmospheric turbulence described by log-normal distribution, the numerical simulations show that our modified scheme has apparent improvements both in transmission distance and key generation rate.

ACKNOWLEGEMENTS

We gratefully acknowledge support from National natural science youth fund(11704412) and National university of defense technology(project zk17-02-09)

[1] Stucki D, Walenta N, Vannel F, et al. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres[J]. New Journal of Physics, 2009, 11(7):075003.

[2] Wang W , Xu F , Lo H K . Prefixed-threshold real-time selection method in free-space quantum key distribution[J]. Physical Review A, 2018, 97(3):032337.

[3] J-P Bourgoin Experimental and theoretical demonstration of the feasibility of global quantum cryptography using satellites, University of Waterloo (2014).

[4] WO Popoola, Z Ghassemlooy. Performance of sub-carrier modulated Free-Space Optica communication link in negative exponential atmospheric turbulence environment[J]. International Journal of Autonomous and Adaptive Communications Systems， 2008, 1 (3): 342-355