

doi:10.3969/j.issn.1001-893x.2015.09.003

引用格式:李铁飞,杨峰,李伟,等.单光子卫星量子通信噪声和干扰分析[J].电讯技术,2015,55(9):959-963.[LI Tiefei,YANG Feng,LI Wei,et al. Analysis of Noise and Interference to Single Photon Satellite Quantum Communication[J].Telecommunication Engineering,2015,55(9):959-963.]

单光子卫星量子通信噪声和干扰分析*

李铁飞**,杨 峰,李 伟,崔树民

(空军工程大学 信息与导航学院,西安 710077)

摘 要:卫星量子通信是建立全球量子通信网络的最佳选择之一。针对采用偏振编码的卫星量子通信中的偏振保持问题,研究了大气散射和卫星与地面站间相对运动等因素对量子偏振态相位和对准的影响以及相位延迟和对准误差对系统量子误码率的影响,分析了背景噪声和系统硬件噪声对通信产生的影响以及单光子通信过程中可能受到的光子分离攻击干扰,为量子信号认知设计提供借鉴意义。

关键词:量子通信;卫星通信;偏振误差;相位延迟;背景噪声;分离攻击干扰

中图分类号:TN918 文献标志码:A 文章编号:1001-893X(2015)09-0959-05

Analysis of Noise and Interference to Single Photon
Satellite Quantum Communication

LI Tiefei,YANG Feng,LI Wei,CUI Shumin

(Information and Navigation College,Air Force Engineering University,Xi'an 710077,China)

Abstract:Satellite quantum communication is one of the best choices for building a global quantum network. In view of the polarization maintaining problem in satellite quantum communication which uses polarization encoding, the impact of atmospheric scattering and relative movement between satellite and ground station on the photon polarization states' phase and alignment and the influence of alignment error and phase delay on quantum bit error rate of the system is researched. The influence of background noise and hardware on the quantum communication and the photon-number-splitting attacks to the single photon in quantum communication are analyzed. Research in this paper has important significance to quantum signal's cognitive design.

Key words:quantum communication;satellite communication;polarization error;phase delay;background noise;photon-number-splitting attacks

1 引 言

近年来,基于量子力学不确定性原理和不可克隆原理的量子密码技术受到人们极大关注,因其采用量子密钥分发和一次一密的方式进行信息加密和解密,具有很强的安全性^[1-2]。为克服光子与周围环境之间的消相干效应,光纤量子通信得到了迅猛发展,已实现超过100 km的光纤量子密钥分发^[3]。与光纤量子通信相对应的卫星量子通信可通过空间平台中转的方式在地球上任意两点之间建立量子信道,是建立全球量子安全通信网络的最佳选择之一^[4]。然而,在开放自由空间信道进行信息传递的光量子将不可避免地受到各种环境噪声和人为干扰

* 收稿日期:2015-01-06;修回日期:2015-05-26 Received date:2015-01-06;Revised date:2015-05-26
基金项目:国家自然科学基金资助项目(61302153);航空基金资助项目(20140196003);航天科技创新基金项目(CASC040203)
Foundation Item:The National Natural Science Foundation of China(No.621302153);The Aeronautical Science Fund(204196003);The Aerospace Science and Technology Innovation Fund(CASC040203)

** 通讯作者:lrf_anian@foxmail.com Corresponding author:lrf_anian@foxmail.com

的影响^[5-6]。

单光子信号,即光子数态中的单光子态,是光辐射场的最小能量单位。单光子信号的产生是实现量子保密通信协议的核心技术,是量子通信领域研究的重点,且目前应用最广泛的密码协议是 Bennett 和 Brassard 提出的采用偏振编码进行信息传递的 BB84 协议^[7]。若单光子卫星量子通信采用偏振编码,为实现信息准确传递,要求光子在经过大气信道传输后仍保持最初偏振态。光子在大气信道中传输时,其偏振态将受到大气体分子、气溶胶粒子和浑浊介质散射、大气湍流、地磁场法拉第效应、卫星与地面站之间相对运动等因素影响^[8],我们将其统称为噪声。

为实现安全可靠的卫星量子通信,本文系统地研究了整个单光子通信过程中可能受到的噪声和干扰。

2 噪声假设和噪声类型

目前,涉及噪声的量子通信方案中都包含一个重要假设——联合噪声假设。不同物理实体在不同环境条件下,受噪声影响形式不同,且会随时间改变。为研究方便,一般假设噪声随时间缓变,即同时或时间间隔很短的几个光子或波包在同一噪声信道中传输时受到的影响相同^[9]。

联合噪声类型包含联合退相位噪声和联合旋转噪声。偏振粒子态 $|H\rangle$ 和 $|V\rangle$ 穿过联合退相位噪声信道时有^[10-11]

$$|H\rangle \rightarrow |H\rangle, |V\rangle \rightarrow e^{i\phi} |V\rangle; \tag{1}$$

穿过联合旋转噪声信道时有

$$\begin{aligned} |H\rangle &\rightarrow \cos\theta |H\rangle + \sin\theta |V\rangle, \\ |V\rangle &\rightarrow -\sin\theta |H\rangle + \cos\theta |V\rangle. \end{aligned} \tag{2}$$

式中, θ 和 ϕ 为噪声参数。可以看出,无论是联合退相位噪声还是联合旋转噪声都是对量子偏振态产生影响。其他一些常见噪声还包括比特翻转噪声、相位翻转噪声、幅值阻尼噪声和退极化噪声等^[12-13]。除了信道噪声外,系统噪声还包括发射端激光噪声、接收端背景噪声和系统硬件噪声等。

3 噪声分析

3.1 联合退相位噪声

由公式(1)得,偏振粒子穿过联合退相位噪声信道时会产生相位延迟。相位延迟主要由光学因素(错误的光学涂膜和不合适的材料均会造成严重的相位延迟)和大气条件决定。相位延迟会导致偏振圆极化进而降低信号的偏振消光比(ER),如图1所示。

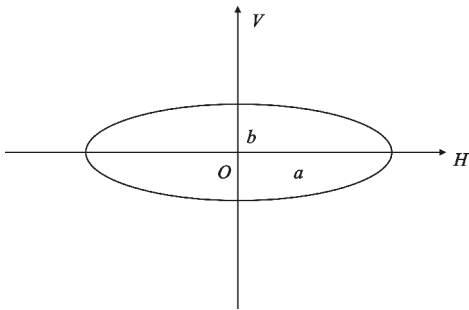


图1 以H、V为基的圆极化光轮廓
Fig.1 The profile of elliptic-polarized light detected by the H/V base

相位延迟导致的圆极化光使用椭圆率角 α 表示,则偏振消光比 ER 为

$$ER = \left(\frac{a}{b}\right)^2 = \frac{1}{\tan^2 \alpha}. \tag{3}$$

由公式(3)得,偏振消光比随相位延迟的增大而减小。在存在相位延迟情况下,接收端使用基H/V对圆极化光检测将得到两种测量结果:水平偏振光子和竖直偏振光子,探测比率为ER:1。因此,由相位延迟引起的量子误码率(QBER)为

$$N = \frac{1}{ER+1} \tag{4}$$

3.2 联合旋转噪声

偏振粒子穿过联合旋转噪声信道时,会使偏振粒子的偏振态产生随机性波动,不再与入射光保持相同偏振特性。影响因素包括大气湍流、卫星与地面站间相对运动、大气散射等。因大气湍流对光子偏振态的影响十分微弱可忽略不计,在此不作分析。

3.2.1 卫星与地面站间的相对运动

卫星量子通信使用量子偏振态来传递信息,发射端(Alice)和接收端(Bob)通过共享相同参考系来比对量子偏振态。由于卫星一直处于运动状态,在通信过程中 Alice 和 Bob 的望远镜需不断调整来进行链路保持,将产生一定偏差和倾斜,对终端参考系产生影响,Alice 和 Bob 的参考系在未进行补偿情况下存在对准误差。此时,若 Alice 根据自己的参考系发射信号而 Bob 根据自己的参考系检测量子偏振态,因两个共享参考系间存在 β 的误差角,测量结果将导致量子误码率急剧增大。

3.2.2 大气散射

散射主要包括大气分子 Rayleigh 散射和气溶胶粒子 Mie 散射,因光量子尺度微小性,大气分子 Rayleigh 散射影响很小,因此主要散射影响为气溶胶粒子 Mie 散射,通常表现为散射光偏离入射光传

播方向,且散射光偏振特性不再与入射光保持一致,即产生了退偏振效应^[8]。

沿 Z 方向传播的偏振光可用 Stokes 矢量法描述为

$$S = \begin{pmatrix} I \\ P \\ U \\ V \end{pmatrix} = \begin{pmatrix} a_x^2 + a_y^2 \\ a_x^2 - a_y^2 \\ 2a_x a_y \cos(\delta) \\ 2a_x a_y \sin(\delta) \end{pmatrix} \quad (5)$$

式中, a_x 和 a_y 分别表示电场 E 在 x 和 y 两个方向振幅, δ 为 x 和 y 两个方向电场分量相位差。根据 Mie 散射理论^[14], 可用 Muller 矩阵表示光与大气粒子的交互作用^[15]:

$$M = \begin{pmatrix} m_{11}(\theta) & m_{12}(\theta) & 0 & 0 \\ m_{21}(\theta) & m_{22}(\theta) & 0 & 0 \\ 0 & 0 & m_{33}(\theta) & m_{34}(\theta) \\ 0 & 0 & m_{43}(\theta) & m_{44}(\theta) \end{pmatrix} \quad (6)$$

传播中光子与粒子发生单次散射后,其偏振态 Stokes 矢量为

$$S_1 = R(-\varphi) M(\theta) R(\varphi) S_0 \quad (7)$$

式中, $R(\varphi)$ 为坐标系旋转矩阵,作用是将入射光 Stokes 矢量从参考面旋转至散射面, φ 为旋转角; $R(-\varphi)$ 的作用相反。 $R(\varphi)$ 表达式为

$$R(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos 2\varphi & -\sin 2\varphi & 0 \\ 0 & \sin 2\varphi & \cos 2\varphi & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (8)$$

光子在经过 n 次散射后 Stokes 矢量为

$$S_n = M_n(\theta_n) R_n(\varphi_n) \times \cdots \times M(\theta) R_1(\varphi) S_0 \quad (9)$$

其他大气散射对光子偏振态的研究还存在“虚粒子”概念,将大气层对光子偏振态的影响进行分层步长处理,最后将多层大气散射进行叠加,并通过 Monte Carlo 仿真方法揭示偏振态变化规律^[16]。

假设 Bob 接收到的水平偏振光偏离原来坐标系角度为 $\theta(\theta = \beta + \varphi)$, 如图 2 所示。当 Bob 采用基 H/V 对入射光进行探测时,水平和竖直方向能量比为

$$R = \frac{(PP')^2}{(QQ')^2} = \frac{ER \cos^2 \theta + \sin^2 \theta}{\cos^2 \theta + ER \sin^2 \theta} \quad (10)$$

根据公式(4)和式(10)可以计算得出由相位延迟和相对运动引起的 QBER 为

$$N' = \frac{1}{R+1} = \frac{(ER+1) - (ER-1) \cos 2\theta}{2(ER+1)} = N + \frac{ER-1}{ER+1} \sin^2 \theta, \quad (11)$$

由相对运动引起的 QBER 为

$$\Delta N = N' - N = \frac{ER-1}{ER+1} \sin^2 \theta \quad (12)$$

由公式(11)和式(12)可见, N' 和 ΔN 均与 ER 和 θ 有关。在对准误差为 0.52 rad 时 QBER 将高达 24.8% 。Shor 和 Preskill 在 2000 年给出了 BB84 协议单向通信的 QBER 上限为 11% ^[17], 其后, Lo 等人又利用双向通信技术将上限推进到了 18.9% ^[18], 因此,在对偏振信号进行设计时需考虑偏振消光比 ER 对系统的影响和接收端对准误差的补偿问题。

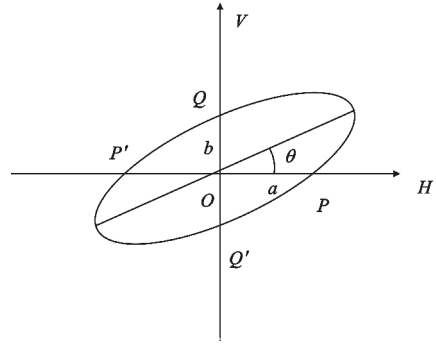


图 2 偏离原来坐标系 θ 的偏振光轮廓
Fig. 2 The profile of elliptic-polarized light with a basis deviation of θ detected by the H/V base

3.3 背景噪声

处在一个亮背景下的卫星量子通信接收系统除光源信号外,还将接收到落在探测器空间和频率范围内的较强背景噪声^[19]。

背景光对接收机的影响主要包括以下两个方面:强背景光引起探测器饱和,即探测器接收的光功率超过其正常工作范围;背景光电流引起的散弹噪声使探测器灵敏度降低。

太阳光是主要背景光干扰源,太阳光在地球大气层外辐照度在平均日-地距离上为 1390 W/m^2 ,且太阳光的主要能量聚集在可见光和红外区。对于接收视场不大的量子通信系统,背景光辐射功率为^[20]

$$P_b = E_\lambda \Omega_\lambda A_r \eta_\alpha \quad (13)$$

式中, E_λ 为光谱辐照度, Ω_λ 为接收天线接收立体角, A_r 为接收天线面积, η_α 为效率。

目前常采用滤波器技术来消除背景噪声,滤波器主要有频率滤波器、时域门滤波器和空间滤波器^[21]。若频率滤波器带宽为 B_{opt} ,则背景光辐射功率为

$$P_b = E_\lambda \Omega_\lambda A_r \eta_\alpha B_{\text{opt}} \quad (14)$$

3.4 系统硬件噪声

激光器量子噪声表现为输出光的相位和幅度存在随机起伏,分束器涂膜效率不佳,间接导致能量透过率降低,光子计数装置雪崩二极管 (APD) 随机噪

声。APD 雪崩倍增过程本质为一个复杂随机过程,在此随机过程中将引入随机噪声,将其定义为过剩噪声。过剩噪声系数可近似表示为^[22]

$$F=M^x. \quad (15)$$

式中, x 是与材料有关的指数。对于 Si, x 为 0.3 ~ 0.5;对于 Ge, x 为 0.6 ~ 1。

APD 的线性工作范围较窄易出现线性饱和。令 APD 量子效率为 η ,时间 t 内探测到 n 个光子的概率为

$$P(n,t)=(\eta R_t)^n \cdot e^{-\eta R_t}/n!. \quad (16)$$

式中, ηR_t 为时间 t 内探测器产生的平均光电子数, R 为光子速率。

4 干扰分析

量子通信过程中涉及的单光子源可以分为两类:单光子枪和基于弱相干脉冲产生的准单光子源。弱相干光源在实用性、普及性等方面都已有长足发展。激光光源的粒子数分布服从 Poisson 分布,令 μ 为平均光子数,则在单个脉冲中含 n 个光子的几率为^[2]

$$p(n,\mu)=\frac{\mu^n}{n!}e^{-\mu}, \quad (17)$$

在非空脉冲中每个脉冲含多个光子的几率为

$$p(n>1|n>0,\mu)=\frac{1-p(0,\mu)-p(1,\mu)}{1-p(0,\mu)}=\frac{1-e^{-\mu(1+\mu)}}{1-e^{-\mu}}\approx\frac{\mu}{2}, \quad (18)$$

空脉冲概率为

$$p(n=0,\mu)=e^{-\mu}\approx 1-\mu. \quad (19)$$

由公式(18)可知,多光子产生概率随 μ 值的增大而增加,降低 μ 可以降低多光子脉冲产生概率,但是, μ 会一直大于零,不能完全避免多光子脉冲产生,且当 μ 值过低时会产生过多的空脉冲。当且仅当 μ 值在一个较低水平时才会认为是单光子源。在普通量子通信实验中,一般采用 $\mu=0.1$,以此来获得准单光子源。因为此时仍有 5% 的脉冲含多个光子,所以并非真正意义上的单光子源。因这些多光子脉冲不再具备单量子态特征,易受攻击者的干扰。

窃听者采用光子数分离攻击的方法^[23-24]截取部分光子进行窃听,具体过程为^[25]:在量子信道中把所有光子脉冲截断,在多光子脉冲中分离出部分光子,提取并存储其量子态,然后将剩余光子无损地发送给接收方,当通信双方通过公共信道公布测量基时,窃听者使用相同测量基进行测量,就可得到跟合法用户相同的密码本。

对抗此类人为干扰的有效方法是制备真正意义

上的单光子源或采用纠缠光子通信,或采用诱骗态协议弥补。

5 结束语

卫星量子通信采用偏振编码方式进行信息传递,需保证光子在经过传输后仍保持原来偏振态。本文研究了卫星与地面站相对运动和大气散射对量子偏振态相位和对准的影响以及相位延迟和对准误差对量子误码率的影响,并对背景噪声、系统硬件噪声和人为干扰等对通信的影响进行了分析。在下一步认知量子信号设计时会将这些干扰和影响因素考虑进来,以实现更好的偏振保持。

参考文献:

- [1] Gisin N, Ribordy G, Tittel W, et al. Quantum Cryptography [J]. Reviews of Modern Physics, 2002, 74(1): 145-195.
- [2] Gisin N, Ribordy G. Quantum cryptography [EB/OL]. 2009-05-05 [2014-12-25]. <http://arxiv.org/abs/quant-ph/0101098v2>.
- [3] Song S Y, Wang C. Recent development in quantum communication [J]. Bulletin of the Chinese Academy of Science, 2012, 57(36): 4694-4700.
- [4] Wang J Y, Yang B, Liao S K, et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution [J]. Nature Photonics, 2013, 7(5): 387-393.
- [5] Brassard G, Nayak A, Tapp A, et al. Noisy Interactive Quantum Communication [C]//Proceedings of 2014 IEEE 55th Annual Symposium on Foundations of Computer Science. Philadelphia, PA: IEEE, 2014: 296-305.
- [6] Takeoka M, Guha S. Capacity of optical communication in loss and noise with general quantum Gaussian receivers [C]//Proceedings of 2014 IEEE International Symposium on Information Theory. Honolulu, HI: IEEE, 2014: 2799-2803.
- [7] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]//Proceedings of 1984 IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore, India: IEEE, 1984: 175-180.
- [8] 俞重远, 李明, 芦鹏飞. 自由空间量子通信的光子偏振研究[J]. 北京邮电大学学报, 2013, 36(2): 1-9.
YU Zhongyuan, LI Ming, LU Pengfei. Photon Polarizations in Free-Space Quantum Communication [J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(2): 1-9. (in Chinese)
- [9] 程巍. 联合噪声中得量子通信[D]. 锦州: 渤海大学, 2013.

- CHENG Wei. The Quantum communication in Collective Noise Channel [D]. Jinzhou: Bohai University, 2013. (in Chinese)
- [10] Li C Y, Li Y S. Fault-tolerate quantum key distribution over a collective noise channel[J]. International Journal of Quantum Information, 2010, 8(7): 1-9.
- [11] Li C Y, Li Y S. Fault-tolerate quantum secret sharing over a collective noise channel[J]. China Physical Letters, 2011, 28(2): 020304.
- [12] 李宁. 有噪信道中的量子安全通信技术研究[D]. 武汉: 华中科技大学, 2006.
- LI Ning. A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering [D]. Wuhan: Huazhong University of Science and Technology, 2006. (in Chinese)
- [13] Bash B A, Guha S, Goeckel D, et al. Quantum noise limited optical communication with low probability of detection[C]//Proceedings of 2013 IEEE International Symposium on Information Theory. Istanbul: IEEE, 2013: 1715-1719.
- [14] Wu Jian, Yang Chunping, Liu Jianbin. Theory of Light-Transmission in the Atmosphere [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2005: 11-20.
- [15] de Haan J F, Bosma P B, Hovenier J W. The adding method for multiple scattering calculations of polarized light [J]. Astronomy and Astrophysics, 1987, 183: 371-391.
- [16] 史鹏, 张闻钊, 马丽珍, 等. 偏振光子的多层大气散射模型及其应用[J]. 大气与环境光学学报, 2010, 5(5): 334-341.
- SHI Peng, ZHANG Wenzhao, MA Lizhen. A Model for Polarized Photons Scattering in Multilayered Atmosphere and Its Application [J]. Journal of Atmospheric and Environmental Optics, 2010, 5(5): 334-341. (in Chinese)
- [17] Shor P W, Preskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol [J]. Physical Review Letters, 2000, 85(2): 441-444.
- [18] Gottesman D, Lo H K. Proof of Security of Quantum Key Distribution with Two-Way Classical Communications [J]. IEEE Transactions on Information Theory, 2003, 49(2): 457-475.
- [19] Tomaello A, Bonato C, Deppo V A, et al. Link budget and background noise for satellite quantum key distribution [J]. Advances in Space Research, 2011, 47(5): 802-810.
- [20] 柯熙政, 席晓莉. 无线激光通信理论[M]. 北京: 北京邮电大学出版社, 2004.
- KE Xizheng, XI Xiaoli. Wireless laser communication theory [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004. (in Chinese)
- [21] Bonato C, Tomaello A, Deppo V D, et al. Feasibility of satellite quantum key distribution [J]. New Journal of Physics, 2009, 11(4): 045017.
- [22] 王佳. 光纤通信与空间光通信技术[M]. 北京: 电子工业出版社, 2013.
- WANG Jia. The Technology of Fiber Optical Communication and Free-Space Optical Communication [M]. Beijing: Electronics Industry Press, 2013. (in Chinese)
- [23] Huttner B, Imoto N, Gisin N, et al. Quantum Cryptography with Coherent States [J]. Physical Review A, 1995, 51(3): 1863-1869.
- [24] Lukenhaus N, Jahma M. Quantum key distribution with realistic states: photo-number statistics in the photo-number splitting attack [J]. New Journal of Physics, 2002(4): 44-53.
- [25] 陈杰. 实用化量子通信系统及其关键技术的研究[D]. 上海: 华东师范大学, 2010.
- CHEN Jie. The Research of Practical Quantum Communication System and Its Key Technology [D]. Shanghai: East China Normal University, 2010. (in Chinese)

作者简介:



李铁飞(1991—),男,河北人,硕士研究生,主要研究方向为卫星量子通信;

LI Tiefei was born in Hebei Province, in 1991. He is now a graduate student. His research concerns satellite quantum communication.

Email: ltf_anian@foxmail.com

杨峰(1975—),男,陕西人,教授、硕士生导师,主要研究方向为卫星量子通信;

YANG Feng was born in Shaanxi Province, in 1975. He is now a professor and also the instructor of graduate students. His research concerns satellite quantum communication.

李伟(1978—),男,山东人,副教授、硕士生导师,主要研究方向为通信与雷达新技术新体制;

LI Wei was born in Shangdong Province, in 1978. He is now an associate professor and also the instructor of graduate students. His research concerns new technology and new system of communication and radar.

崔树民(1990—),男,山东人,硕士研究生,主要研究方向为光纤量子通信。

CUI Shumin was born in Shangdong Province, in 1990. He is now a graduate student. His research concerns fiber quantum communication.