

降雨背景下诱骗态协议最优平均光子数的变色龙自适应策略

聂敏 王允 杨光 张美玲 裴昌幸

Optimal mean photon number of decoy state protocol based on chameleon self-adaptive strategy under the background of rainfall

Nie Min Wang Yun Yang Guang Zhang Mei-Ling Pei Chang-Xing

引用信息 Citation: *Acta Physica Sinica*, 65, 020303 (2016) DOI: 10.7498/aps.65.020303

在线阅读 View online: <http://dx.doi.org/10.7498/aps.65.020303>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn/CN/Y2016/V65/I2>

您可能感兴趣的其他文章

Articles you may be interested in

多跳噪声量子纠缠信道特性及最佳中继协议

Characteristics of multi-hop noisy quantum entanglement channel and optimal relay protocol

物理学报.2015, 64(24): 240304 <http://dx.doi.org/10.7498/aps.64.240304>

基于分组交换的量子通信网络传输协议及性能分析

Transmission protocol and its performance analysis of quantum communication network based on packet switching

物理学报.2015, 64(21): 210303 <http://dx.doi.org/10.7498/aps.64.210303>

利用信息流方法优化多激发自旋链中的量子态传输

Optimizing quantum state transfer in multi-excitation spin chains via information flux

物理学报.2015, 64(16): 160305 <http://dx.doi.org/10.7498/aps.64.160305>

噪声情况下的量子网络直接通信

Quantum network direct communication protocol over noisy channel

物理学报.2015, 64(16): 160306 <http://dx.doi.org/10.7498/aps.64.160306>

量子直接通信

Quantum secure direct communication

物理学报.2015, 64(16): 160307 <http://dx.doi.org/10.7498/aps.64.160307>

降雨背景下诱骗态协议最优平均光子数的变色龙自适应策略*

聂敏¹⁾ 王允^{1)†} 杨光¹⁾²⁾ 张美玲¹⁾ 裴昌幸³⁾

1)(西安邮电大学通信与信息工程学院, 西安 710121)

2)(西北工业大学电子信息学院, 西安 710072)

3)(西安电子科技大学, 综合业务网国家重点实验室, 西安 710071)

(2015年8月16日收到; 2015年10月29日收到修改稿)

为了应对降雨给采用诱骗态协议的量子通信系统带来的突发性干扰, 根据降雨分布模型和退极化信道的特性, 本文提出了基于变色龙算法的每脉冲最优平均光子数自适应策略; 建立了降雨强度、链路距离与最优平均光子数之间的自适应关系; 并对采用变色龙算法前后, 系统的性能参数进行了比较. 仿真结果表明, 当降雨强度 J 为 30 mm/24 h、链路距离 L 为 30 km 时, 通过采用变色龙算法, 系统的安全密钥生成率由 2×10^{-4} 提高到 3.5×10^{-4} ; 当 J 为 60 mm/24 h, L 为 20 km 时, 系统的信道生存函数值由 0.52 提高到 0.63; 当要求生存函数不低于 0.5 时, 系统能够应对的最大雨强由 62 mm/24 h 提高到 74 mm/24 h. 因此, 根据降雨强度和链路距离, 通过变色龙算法自适应地调整系统发送端信号脉冲所含的平均光子数, 可以提高量子通信系统在降雨背景下的有效性和可靠性.

关键词: 诱骗态协议, 降雨, 平均光子数, 变色龙自适应算法

PACS: 03.67.Hk, 92.60.Wc, 42.50.Md, 03.67.Ac

DOI: 10.7498/aps.65.020303

1 引言

近年来, 国际上频频发生的通信窃听事件, 让人们人们对通信的安全性提出了更新、更高的要求. 基于量子不可克隆及量子态叠加原理的自由空间量子通信, 不仅能够保证理论上的绝对安全, 而且在实现更远距离、更广覆盖方面具有天然优势, 因此成为了目前量子通信领域的研究热点. 2003年, Hwang 首次提出了利用诱骗态进行自由空间量子通信的思想^[1], 克服了无理想单光子源制备技术的缺陷, 并能有效抵御 PNS 攻击, 真正将自由空间量子通信推向了实际应用; 2010年, 由清华大学和中国科技大学组成的研究团队, 在河北和北京之间搭建了长度为 16 km 的自由空间量子信道, 成功地完

成了世界上最远距离的量子隐形传态实验^[2]; 2012年, 中国科技大学潘建伟、彭承志团队, 在青海湖完成了国际上第一个百公里量级自由空间量子隐形传态和纠缠分发实验^[3], 为在自由空间中构建广域量子通信网打下了坚实的基础; 2013年, 潘建伟科研小组又利用百公里地面自由空间来模拟星地之间高度衰减链路信道, 完成了星地量子通信地基验证试验^[4], 成功地验证了星地之间进行量子卫星通信的可行性; 2015年, 中国科技大学又成功实现了多自由度量子体系隐形传态^[5], 为进一步提高自由空间量子通信的保密性和有效性提供了理论和实验基础.

然而, 在自由空间中进行量子通信也有其局限性. 当量子态在大气中传输时, 不可避免地会受到环境及自然因素的影响. 文献^[6]研究了中尺度沙

* 国家自然科学基金(批准号: 61172071, 61201194)、陕西省自然科学基金(批准号: 2014JQ8318)和陕西省国际科技合作与交流计划项目(批准号: 2015KW-013)资助的课题.

† 通信作者. E-mail: 285025572@qq.com

尘暴对自由空间量子信道的影响, 为沙尘条件下量子通信的进行提供了理论基础; 文献[7]讨论了大气湍流环境对携带轨道角动量的量子纠缠态传输的影响, 给出了湍流强度与信道容量之间的关系; 文献[8]研究了在大气噪声环境下, 如何有效地实现广域的量子无线通信和量子卫星通信; 文献[9]讨论了PM2.5大气污染对自由空间量子通信的影响, 为雾霾背景下自由空间量子通信系统的有序运行提供了参照依据。

自由空间量子通信系统所受到的干扰分为平稳干扰和突发干扰。当天气状况发生突变时, 由于大气成分的迅速变化, 给光子传输带来的额外干扰为突发干扰。降雨会使大气湿度和粒子成分在短时间内迅速发生变化, 对自由空间光子的传输造成突发干扰, 导致系统的误码率上升, 安全密钥生成率骤降, 严重时甚至迫使通信中断。因此, 研究降雨对量子通信造成的突发干扰具有重大意义。

与BB84协议要求系统必须拥有理想单光子源不同, 诱骗态量子通信安全协议[10]采用更容易实现的弱相干光源代替理想单光子源, 其有效性和安全性已被证明[11], 因此成为了目前最接近实用化, 也是应用最为广泛的量子保密协议。

为了应对降雨给采用诱骗态协议的自由空间量子通信系统带来的突发干扰, 改善降雨环境中系统的性能参数, 本文提出了变色龙自适应算法(chameleon self-adaptive algorithm, CSA)。针对降雨天气中的退化信道, 分析了CSA算法中每脉冲所含平均光子数对系统安全密钥生成率和生存函数的影响, 并作了仿真验证, 为降雨天气下量子通信系统的可靠运行提供了理论依据。

2 降雨对自由空间量子通信的影响分析

作为日常生活中最常见的天气之一, 降雨给自由空间量子通信带来了严重的突发干扰。为方便研究降雨特性, 假设雨粒子为球形形状, 用雨强 J (mm/24 h) 作为描述降雨量大小的参数, 雨滴的平均尺度分布一般满足Marshall-Palmer指数分布[12]:

$$\frac{dN(r)}{dr} = n(r) = k e^{-2hrJ^{-0.214}}, \quad (1)$$

式中 r 为雨滴半径(mm), 其他参数取典型值: $k = 1.6 \times 10^3 \text{ m}^{-3} \cdot \text{mm}^{-1}$, $h = 8.23$ 。 $n(r)$ 为雨

粒子尺度谱分布:

$$n(r) = \begin{cases} 60000 e^{-11.4J^{-0.21}} r, & 0 < J \leq 10, \\ 2800 e^{-6J^{-0.21}} r, & 25 \leq J \leq 50, \end{cases} \quad (2)$$

其中, $0 < J \leq 10$ 表示小雨, $25 \leq J \leq 50$ 为大雨。结合适用于中国亚热带气候特征的Weibull分布模型[13], 以及Mie散射理论[14], 可得出雨滴粒子的衰减截面

$$Q_{t,j}(r) = \frac{2\pi}{k^2} \sum_{n=1}^{\infty} (2n+1) \text{Re}(a_n + b_n), \quad (3)$$

式中 k 为波数; a_n 和 b_n 是Mie散射系数, 其取值与波长和雨滴粒子半径有关。结合(1)式和(3)式, 可得出降雨环境中光子所受到的突发衰减系数为

$$\begin{aligned} a_{\text{rain}} &= 1.41\pi \cdot 10^3 \int_0^{2r_{\text{max}}} Q_{t,j}(r) N(r) dr \\ &= 0.29 + \frac{J}{2.53} - \left(\frac{J}{20.3} \right)^2 \text{ (dB/km)}, \end{aligned} \quad (4)$$

式中 r_{max} 为雨滴的最大半径。

此外, 由于发射端的信号光存在一定的发散角 θ , 随着传输距离 L 的增加, 信号光斑也逐渐增大, 而接收望远镜的光学孔径 D_R 有限, 这就导致了系统会受到几何衰减, 根据文献[15],

$$A_{\text{geo}} = \left(\frac{D_R}{D_T + \theta \cdot L} \right)^2, \quad (5)$$

式中, D_T 为发送端望远镜的光学孔径。本文仿真中, 设定脉冲激光器的频率为10 MHz, $D_R = 300 \text{ mm}$, $D_T = 100 \text{ mm}$, 发射装置的发散角 $\theta = 40 \text{ } \mu\text{rad}$, 发送端望远镜的接收效率为80%。综上, 系统受到来自雨水的总衰减为

$$A_{\text{rain}} = e^{a_{\text{rain}} \cdot L} + \left(\frac{D_R}{D_T + \theta \cdot L} \right)^2, \quad (6)$$

L 为链路长度, 即通信距离。本文分别仿真了无降雨、小雨($J = 5 \text{ mm/24 h}$)和大雨($J = 30 \text{ mm/24 h}$)的天气下, 系统受到的雨水衰减与 L 的关系, 如图1所示。

从仿真结果可以看出, 在降雨强度一定的情况下, 通信距离 L 越大, 系统受到的雨水衰减越大; 在 L 一定时, 这种衰减随着降雨量的增大而加剧。例如, $L = 80 \text{ km}$ 时, 在无降雨、小雨和大雨的天气下, 系统受到的衰减分别为21 dB, 49 dB和74 dB。因此, 为了应对降雨给系统带来的这种突发干扰, 本文提出了平均光子数的变色龙算法。

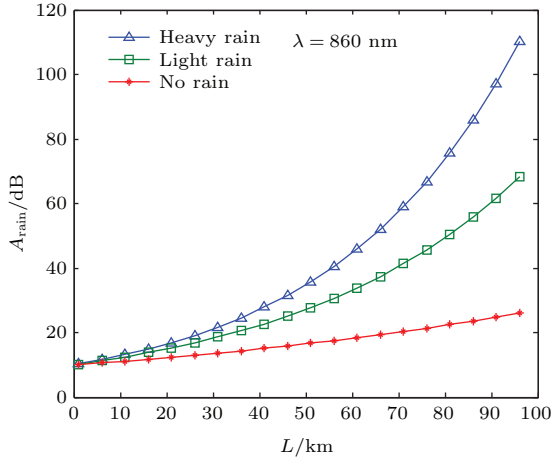


图1 系统所受雨水衰减与通信距离的关系

Fig. 1. Relationship between system attenuation and link length in rain.

3 诱骗态量子协议和变色龙算法

3.1 基于BB84的诱骗态量子协议

诱骗态量子协议系统使用高度衰减的弱相干光源进行量子通信, 假设光源的弱相干态为

$$|\varphi\rangle = e^{-\frac{|\varphi|^2}{2}} \sum_{n=0}^{\infty} \frac{\varphi^n}{\sqrt{n!}} |n\rangle, \quad (7)$$

且光脉冲的相位随机, 则 $|\varphi\rangle$ 的密度矩阵可以表示为

$$\begin{aligned} \rho &= \frac{1}{2\pi} \int_0^{2\pi} d\theta |\varphi| e^{i\theta} \langle \varphi | e^{i\theta} | \\ &= \frac{1}{2\pi} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{|\varphi|^{m+n}}{\sqrt{m!n!}} e^{-|\varphi|^2} |n\rangle \langle m| \\ &\quad \times \int_0^{2\pi} d\theta e^{i(m-n)\theta} \\ &= \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n\rangle \langle n|, \end{aligned} \quad (8)$$

其中, θ 为相干态 $|\varphi\rangle$ 的相位, μ 为每脉冲所含平均光子数. 从上式可以看出, 在弱相干光源中, 每脉冲所含的光子数 n 服从Poisson分布, 即

$$p(n; \mu) = \frac{\mu^n}{n!} e^{-\mu}. \quad (9)$$

计算可得, 空脉冲的概率为 $p(n=0) = e^{-\mu} \approx 1 - \mu$; 在一个非空脉冲中, 含有一个以上光子的概率为

$$\begin{aligned} p(n > 1; \mu) &= \frac{1 - p(0; \mu) - p(1; \mu)}{1 - p(0; \mu)} \\ &= \frac{1 - (1 + \mu)e^{-\mu}}{1 - e^{-\mu}} \approx \frac{\mu}{2}. \end{aligned} \quad (10)$$

脉冲通过率为

$$\begin{aligned} Q_\mu &= \sum_n Y_n p(n; \mu) \\ &= Y_{\text{dark}} e^{-\mu} + \sum_{n=1}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu}, \end{aligned} \quad (11)$$

上式中 Y_n 为发送 n 光子脉冲时, 被接收端检测到的概率, Y_{dark} 为接收端探测器的暗记数率. 令降雨背景下信道的总传输率 η_{rain} 为

$$\eta_{\text{rain}} = 10^{-\frac{\alpha_{\text{rain}} \cdot L}{10}} \cdot \eta_{\text{det}}, \quad (12)$$

η_{det} 为接收端探测器的探测效率, 则发送端发送含有 n 个光子脉冲的通过率可以表示为 $\eta_n = 1 - (1 - \eta_{\text{rain}})^n$, 则

$$Y_n = \eta_n + Y_0(1 - \eta_n). \quad (13)$$

代入到(11)式中, 得到所含平均光子数为 μ 的脉冲通过率为

$$Q_\mu = 1 + Y_{\text{dark}} - \exp(-\mu \cdot \eta_{\text{det}} 10^{-\frac{\alpha_{\text{rain}} \cdot L}{10}}). \quad (14)$$

可以看出, μ 值越大, 脉冲在降雨环境中的通过率越高, 通信效率也越高, 但是, 系统受到光子数分裂攻击而不被发现的可能性越大; 如果降低 μ 值, 可以有效地提高通信的安全性, 但此时多数是空脉冲, 大部分时间链路处于闲置状态, 导致信道的利用率下降, 系统的比特率也会降低. 因此, 如何确定发送端信号脉冲的最佳 μ 值, 对于改善在降雨环境中采用诱骗态协议的量子通信系统的性能有很大意义.

3.2 变色龙算法

为了确定采用诱骗态协议的自由空间量子通信系统发送端脉冲的最佳 μ 值, 本文提出了变色龙自适应算法.

首先, 结合退极化信道^[16], 研究光子与降雨环境之间的消相干现象. 在自由空间传输的光子态的密度算子 ρ 可以由其自旋极化矢量 $\mathbf{P}$ 来描述, 即 $\rho = \frac{1}{2}(\mathbf{I} + \mathbf{P} \cdot \mathbf{v})$, $\mathbf{I}$ 为恒等算子. 假设已发送出来但未经传输的量子态为叠加态: $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, 其中 α, β 为复数, 且 $|\alpha|^2 + |\beta|^2 = 1$. 设其密度矩阵为

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}. \quad (15)$$

在降雨退极化信道的作用下, 演化为

$$\rho = \begin{pmatrix} (1 - 2p/3)\rho_{00} + 2p/3\rho_{11} & (1 - 4p/3)\rho_{01} \\ (1 - 4p/3)\rho_{10} & (1 - 2p/3)\rho_{11} + 2p/3\rho_{00} \end{pmatrix}. \quad (16)$$

由于雨滴粒子对光子的吸收和散射, 导致极化矢量 $\mathbf{P}$ 退极化. 以 $|e\rangle$ 表示降雨环境的量子态, 量子位与降雨环境构成的系统联合演化后可以表示为

$$|\varphi\rangle|e\rangle = (\alpha|0\rangle + \beta|1\rangle)|e\rangle \rightarrow |0\rangle(\alpha|e_0\rangle + \beta|e'_1\rangle) + |1\rangle(\alpha|e'_0\rangle + \beta|e_1\rangle). \quad (17)$$

降雨环境态可以表示为

$$|e_{\pm}\rangle = \frac{1}{2}(|e_0\rangle + |e_1\rangle), \\ |e'_{\pm}\rangle = \frac{1}{2}(|e'_0\rangle + |e'_1\rangle). \quad (18)$$

则上式可以化简为

$$(\alpha|0\rangle + \beta|1\rangle)|e\rangle \\ \rightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes [|e'_+\rangle X + |e'_-\rangle Y \\ + |e_-\rangle Z + |e_+\rangle I], \quad (19)$$

令 $|e_+\rangle = |e_I\rangle$, $|e'_+\rangle = |e_X\rangle$, $|e'_-\rangle = |e_Y\rangle$, $|e_-\rangle = |e_Z\rangle$, 系统的么正演化如下:

$$U : |\varphi\rangle|e_I\rangle \\ \rightarrow \sqrt{1-p}I|\varphi\rangle \otimes |e_I\rangle + \sqrt{\frac{p}{3}}X|\varphi\rangle \otimes |e_X\rangle \\ + \sqrt{\frac{p}{3}}[Y|\varphi\rangle \otimes |e_Y\rangle + Z|\varphi\rangle \otimes |e_Z\rangle], \quad (20)$$

式中 p 为量子位受降雨突发干扰后翻转的概率. 对环境初态演化而来的正交基 $\{|e_I\rangle, |e_X\rangle, |e_Y\rangle, |e_Z\rangle\}$ 求偏迹后, 可以得到降雨环境中的四个 Kraus 算子元素:

$$K_0 = \sqrt{1-p}I, \quad K_1 = \sqrt{\frac{p}{3}}X, \\ K_2 = \sqrt{\frac{p}{3}}Y, \quad K_3 = \sqrt{\frac{p}{3}}Z. \quad (21)$$

由上式可以得到量子态在 t 时刻传输的密度算子为

$$\rho_A(t) = \sum_{p=0}^1 A_p \rho_A(t_0) A_p^\dagger \\ = [I + (1 - 4p/3) \cdot P(0) \cdot v]/2. \quad (22)$$

由此可知, 自旋极化矢量的大小减小到初始值的 $1 - 4p/3$ 倍, 假设四个 Kraus 密度算子等概率出现, 则整个量子位出错的概率为 $P_{\text{error}} = 75\%$.

通过在发送端随机发送信号态、诱骗态和真空态的组合信号, 三态协议已被证明可以达到诱骗态

理论的极限值, 所以是目前最为成熟的协议之一. 因此, 本文的分析基于三态协议, 并利用发送端的随机数产生器, 使信号态、诱骗态和真空态之间的脉冲比例固定为 $2:1:1$, 在此基础上, 研究信号态脉冲平均光子数对系统参数的影响. 令信号态每脉冲所含的平均光子数为 μ , 其相干态的密度算符可以表示为

$$\rho_u = e^{-u}|0\rangle\langle 0| + u e^{-u}|1\rangle\langle 1| + c\rho_c, \quad (23)$$

其中 c 为密度算符系数, $c = 1 - e^{-u} - u e^{-u}$, ρ_c 为诱骗态中多光子成分的密度算符.

根据 GLLP 公式^[17], 在使用弱相干光源进行量子密钥分发时, 诱骗态协议系统的安全密钥生成率为

$$R_{\text{key}} \geq \eta_{\text{sys}} \{-Q_u f(E_u) H_2(E_u) \\ + Q_1 [1 - H_2(E_1)]\}, \quad (24)$$

式中 η_{sys} 为系统效率; $f(E_u)$ 为双边误码纠错效率; $H_2(x)$ 是二元熵函数, $H_2(x) = -x \log(x) - (1-x) \log(1-x)$; E_u 为接收到光子态的误码率; Q_1 为单光子到达接收端的概率; E_1 为单光子导致的误码率. 含有 i 个光子的脉冲误码率为

$$E_i = \frac{1/2 Y_{\text{bac}} + e_{\text{det}} P_n}{Y_n}, \quad (25)$$

Y_{bac} 为背景噪声的通过率, e_{det} 为探测器噪声带来的误码率. 系统总的误码率可以表示如下:

$$E_u Q_u = \sum_{i=0}^{\infty} Q_i e_i = \sum_{i=0}^{\infty} Y_i e_i \frac{\mu^i}{i!} \exp(-\mu) \\ = e_0 Y_0 + e_{\text{det}} (1 - e^{-u \eta_{\text{rain}}}). \quad (26)$$

代入到 (24) 式中, 得到系统的安全密钥生成率为

$$R_{\text{key}} \geq -\eta_{\text{rain}} \mu f(e_{\text{det}}) H_2(e_{\text{det}}) \\ + \eta_{\text{rain}} \mu e^{-\mu} [1 - H_2(e_{\text{det}})]. \quad (27)$$

最终得到系统发送端信号态的最优平均光子数 μ_{opt} 满足

$$(1 - \mu_{\text{opt}}) e^{-\mu_{\text{opt}}} \\ = \frac{10^{[-0.29 + \frac{J}{2.53} - (\frac{J}{20.3})^2 \cdot L]/10} \cdot \eta_{\text{det}} f(e_{\text{det}})}{1 - H_2(e_{\text{det}})}. \quad (28)$$

该公式就是针对降雨环境下, 采用诱骗态协议的自由空间量子通信系统的信号态最优平均光子数变

色龙自适应算法, 它是降雨强度 J 与通信距离 L 的函数, 对该公式进行仿真, 结果如图 2 所示.

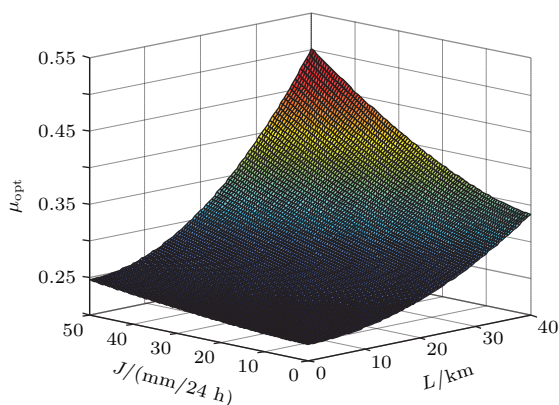


图 2 (网刊彩色) CSA 算法下最优平均光子数与雨强、通信距离的关系

Fig. 2. (color online) Relationship among μ_{opt} , rainfall intensity and link length by CSA.

从仿真结果可以看出, 当降雨强度和链路长度为 0 时, 采用诱骗态协议的自由空间量子通信系统的信号态最优平均光子数 μ_{opt} 为 0.23; 随着通信距离 L 和降雨强度 J 的增大, μ_{opt} 也逐渐增大; 在降雨强度 J 超过 35 mm/24 h 时, 由于系统受到雨水的突发性衰减迅速增加, μ_{opt} 的值也迅速升高; 当 $J = 50$ mm/24 h, $L = 40$ km 时, μ_{opt} 的值大约为 0.5.

采用诱骗态协议的自由空间量子通信系统在降雨天气下受到突发干扰时, 可以根据降雨强度和通信距离, 通过 CSA 算法实时地调整信号态最优平均光子数的大小. 仿真结果表明, 该算法能够有效地应对降雨带来的突发干扰.

4 CSA 算法对系统安全密钥生成率的影响

安全密钥生成率指量子通信系统在单位时间内生成安全密钥的个数与所收到密钥总个数的比值, 是衡量系统有效性能的重要参数.

设发送端光子脉冲的产生频率为 f_s , 发送端和接收端的平稳干扰损耗为 L_d (dB), 光子被接收的概率为 Y_n , 大气透射率为 T_r :

$$T_r = e^{-\frac{2}{3}} \cdot J^{0.6}. \quad (29)$$

结合 GLLP 公式, 最终得到系统的安全密钥生成率与每脉冲平均光子数的关系式为

$$R_{\text{key}} = e^{-\frac{2}{3}} J^{0.6} f_s \mu_{\text{opt}} 10^{-L_d} \eta_{\text{det}} Y_n. \quad (30)$$

本文分别仿真了在小雨和大雨的天气下, 采用变色龙自适应算法前后系统的安全密钥生成率, 如图 3 所示.

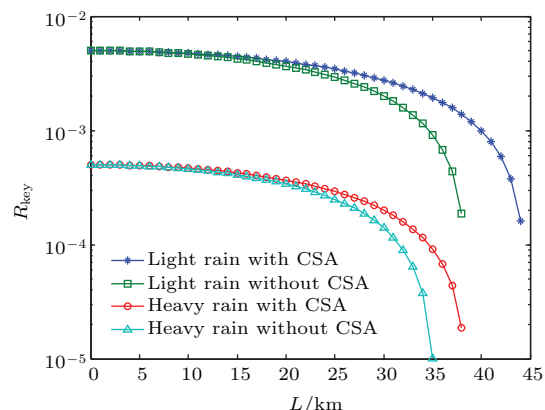


图 3 (网刊彩色) 不同雨强下采用 CSA 前后系统的安全密钥生成率与通信距离的关系

Fig. 3. (color online) Relationship between secure key rate and link length with/without CSA in light/heavy rain.

从仿真结果可以看出, 系统的安全密钥生成率随着通信距离的增大逐渐减小, 当距离超过 30 km 时, R_{key} 的值迅速下降; 采用变色龙自适应算法后, 系统的密钥生成率有了明显提高, 大雨天气下, 当通信距离为 35 km 时, R_{key} 由 10^{-5} 提高到 10^{-4} 左右; 系统的安全通信距离也有所提高, 小雨天气下从 35 km 提高到 38 km. 可见, 通过采用 CSA 算法, 系统能够在单位时间内生成更多的安全密钥, 这对于提高系统的有效性具有很大意义.

5 CSA 算法对系统生存函数的影响

为了评估量子通信系统在自由空间中的抗干扰能力和生存性能, 文献 [18] 提出了生存函数的概念. 降雨环境的量子退极化信道中, 生存函数可以表示为

$$S = \xi_{\text{rain}} \cdot F_{\text{rain}}, \quad (31)$$

式中 ξ_{rain} 为降雨信道生存系数, 是衡量信道传输量子信号难易程度的标准, 其大小与量子系统所处的具体环境及降雨强度有关, 且 $0 < \xi_{\text{rain}} \leq 1$. 对于自由空间大气信道而言, 生存系数的表达式为

$$\xi_{\text{rain}} = \frac{5809}{5810} - \frac{9A_{\text{rain}}}{2905}. \quad (32)$$

可以看出, 量子信号在信道中受到的衰减 A_{rain} 越小, 该信道的生存系数越大. F_{rain} 为系统的量子态

传输保真度, 是用来衡量量子输入态和输出态之间的相近程度. 其定义^[19]为

$$F_{\text{rain}} = F(\rho, \rho') = \left(\text{tr} \sqrt{\rho^{1/2} \rho' \rho^{1/2}} \right)^2, \quad (33)$$

式中, ρ' 为输出量子态的密度矩阵. 自由空间量子信令系统 S 与降雨环境系统 R 的演化过程为

$$\begin{aligned} & |\varphi\rangle_S \otimes |0\rangle_R \xrightarrow{U_{\text{SR}}} \sqrt{1-p} |\varphi\rangle_S \otimes |0\rangle_R \\ & + \sqrt{p/3} [\sigma_1 |\varphi\rangle_S \otimes |1\rangle_R + \sigma_2 |\varphi\rangle_S \otimes |2\rangle_R \\ & + \sigma_3 |\varphi\rangle_S \otimes |3\rangle_R], \end{aligned} \quad (34)$$

其中

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

量子态在降雨环境中的通过率为 Q_μ , 结合(33)式与经过退极化信道的量子态密度算子 ρ (16)式), 可以得到系统的保真度为

$$F_{\text{rain}} = \exp((\mu_{\text{opt}} Q_\mu - \bar{Y}_n)^{4/3} A_{\text{rain}}). \quad (35)$$

最终得出降雨环境下量子态的生存函数为

$$\begin{aligned} S_{\text{rain}} = & \left[\frac{5809}{5810} - \frac{9 e^{0.29 + \frac{J}{2.53} - (\frac{J}{20.3})^2 \cdot L}}{2905} \right] \\ & \times \exp[(\mu_{\text{opt}} Q_\mu - \bar{Y}_n)^{4/3} A_{\text{rain}}]. \end{aligned} \quad (36)$$

图4为在通信距离一定($L = 20$ km)的条件下, 系统在采用CSA算法前后, 信道生存函数随着降雨强度的变化关系.

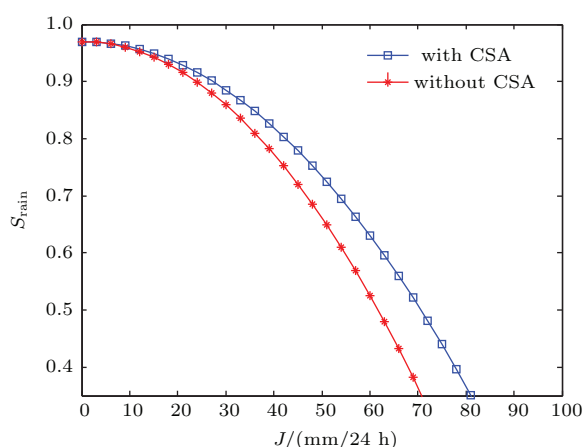


图4 采用CSA前后系统的信道生存函数与雨强的关系

Fig. 4. Relationship between channel survival function and rainfall intensity with/without CSA.

从仿真图可以看出, 降雨强度 J 越大, 系统的信道生存函数 S_{rain} 越小; 采用CSA算法后, 系统的 S_{rain} 值有了明显的提高, 系统也能够应对强度更大的降雨. 例如, 当降雨强度 60 mm/24 h 时, 系统

的 S_{rain} 值由 0.52 提高到 0.63 ; 当要求生存函数大于 0.5 时, 系统能够应对的降雨强度由 62 mm/24 h 提高到 74 mm/24 h. 可见, CSA算法的引入能够有效提高量子通信系统在降雨天气下的可靠性和生存性能.

6 结 论

本文研究了降雨天气下量子通信系统所受到的突发干扰问题, 提出了诱骗态协议最优平均光子数的概念, 并结合降雨衰减模型和退极化信道的特性, 构建了变色龙自适应算法. 依据该算法以及降雨强度和链路距离, 系统可以实时地对每脉冲平均光子数进行调整. 仿真结果表明, 降雨带来的突发干扰, 会对系统造成很大衰减, 而通过调节信号脉冲的平均光子数, 系统的安全密钥生成率和生存函数有了明显的改善. 因此, CSA算法为在降雨环境中更可靠、更安全地进行量子通信提供了一种理论依据, 对确保自由空间量子通信系统的鲁棒性具有重要意义.

参考文献

- [1] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 508
- [2] Jin X M, Ren J G, Yang B, Yi Z H, Zhou F, Xu X F, Peng C Z, Wang S K, Yang D, Pan J W, Hu Y F, Jiang S 2010 *Nat. Photon.* **4** 376
- [3] Yin J, Ren J G, Lu H, Cao Y, Yong H L, Wu Y P, Liu C, Liao S K, Zhou F, Jiang Y, Cai X D, Xu P, Pan G S, Jia J J, Huang Y M, Yin H, Wang J Y, Chen Y A, Peng C Z, Pan J W 2012 *Nature* **488** 185
- [4] Wang J Y, Yang B, Liao S K, Zhang L, Shen Q, Hu X F, Wu J C, Yang S J, Jiang H, Tang Y L, Zhong B, Liang H, Liu W Y, Hu Y H, Huang Y M, Qi B, Ren J G, Pan G S, Yin J, Jia J J, Chen Y A, Chen K, Peng C Z, Pan J W 2013 *Nat. Photon.* **7** 387
- [5] Wang X L, Cai X D, Su Z E, Chen M C, Wu D, Li L, Liu N L, Lu C Y, Pan J W 2015 *Nature* **518** 516
- [6] Nie M, Shang P G, Yang G, Zhang M L, Pei C X 2014 *Acta Phys. Sin.* **63** 240303 (in Chinese) [聂敏, 尚鹏钢, 杨光, 张美玲, 裴昌幸 2014 物理学报 **63** 240303]
- [7] Tyler GA, Boyd R W 2009 *Opt. Lett.* **34** 142
- [8] Chen N, Quan D X, Pei C X, Yang H 2015 *Chin. Phys. B* **24** 020304
- [9] Nie M, Ren J, Yang G, Zhang M L, Pei C X 2015 *Acta Phys. Sin.* **64** 150301 (in Chinese) [聂敏, 任杰, 杨光, 张美玲, 裴昌幸 2015 物理学报 **64** 150301]
- [10] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 508
- [11] Elliott C, Pearson D, Troxel G 2003 *Acm Sigcomm Computer Communication Review* **33** 227

- [12] Marshall J S, Langile R C, Palmer W M 1947 *Journal of the Atmospheric Science* **4** 186
- [13] Weibull W, Mech A J 1951 *Journal of Applied Micro-electron* **28** 613
- [14] Mie G 1908 *Ann. Phys.* **25** 377
- [15] Liu M, Liu X G, Mou Y J 2012 *Infrared and Laser Engineering* **41** 2136 (in Chinese) [刘敏, 刘锡国, 牟京燕 2012 红外与激光工程 **41** 2136]
- [16] Bruss D, Faoro L, Macchiavello C 2000 *Journal of Modern Optics* **47** 325
- [17] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quant. Inf. Comput* **5** 325
- [18] Zhang L, Nie M, Liu X H 2013 *Acta Phys. Sin.* **62** 150301 [张琳, 聂敏, 刘晓慧 2013 物理学报 **62** 150301]
- [19] Liu T K, Wang J S, Liu X J, Zhan M S 2000 *Acta Optica Sinica* **20** 1449 (in Chinese) [刘堂昆, 王继锁, 柳晓军, 詹明生 2000 光学学报 **20** 1449]

Optimal mean photon number of decoy state protocol based on chameleon self-adaptive strategy under the background of rainfall*

Nie Min¹⁾ Wang Yun^{1)†} Yang Guang¹⁾²⁾ Zhang Mei-Ling¹⁾ Pei Chang-Xing³⁾

1) (School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

2) (School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China)

3) (State Key Laboratory of Integrated Service Networks, Xi'an University of Electronic Science and Technology, Xi'an 710071, China)

(Received 16 August 2015; revised manuscript received 29 October 2015)

Abstract

As one of the most common weathers in daily life, the rain can change the atmospheric compositions and humidity in a short time, which may cause non-ignorable attenuation in free-space quantum communication system. Besides, the absorption and scattering effects caused by raindrops can also bring huge attenuation to photon's propagation. In order to solve this burst interference caused by rain weather, optimal mean photon number per pulse and chameleon self-adaptive algorithm (CSA) are proposed based on the rainfall distribution model and decoy-state quantum key distribution. Due to the lack of producing mature ideal single photon source technology, the decoy-state protocol with highly attenuated laser becomes the most practical and most widely used quantum secure communication protocol currently. Among all the different kinds of decoy-state protocols, the vacuum+weak decoy state quantum communication secure protocol is chosen to be the basis of our research. Besides, in order to study the influence of mean photon number per signal pulse, we set the pulse ratio between signal state, decoy state and vacuum state to be fixed at 2 : 2 : 1. Since the performance of the vacuum+weak decoy state quantum communication system is closely related to the mean photon number per pulse, it is very necessary to confirm the optimal value. Combining the Weibull rainfall distribution model and Mie scattering theory, we first analyze the attenuation caused by rainfall in a free-space quantum communication system. Then the functional relationship among μ_{opt} , rainfall intensity (J) and link distance (L) is built by studying the propagation of highly attenuated laser in depolarizing channel. Finally, two parameters, secure key rate and channel survival function, are chosen to evaluate the system's performance of reliability and validity. These two parameters are respectively compared between the system with and without CSA. Simulation results show that, as $J = 30$ mm/24 h, $L = 30$ km, the secure key generation rate rises from 2×10^{-4} up to 3.5×10^{-4} when using the CSA in the quantum communication system; as $J = 60$ mm/24 h, $L = 20$ km, the quantum channel survival function value increases from 0.52 to 0.63; as the quantum channel survival function value is required no lower than 0.5, the rainfall intensity in which quantum communication system can survive rises from 62 mm/24 h up to 74 mm/24 h. These results prove that there is a close relationship between μ_{opt} and the channel parameters of the quantum communication system under the background of rainfall. Therefore, it is necessary for us to self-adapt the μ_{opt} value by combining rainfall intensity with the CSA strategy if the reliability and survivability of free space quantum communication system are required to be improved.

Keywords: decoystate protocol, rainfall, mean photon number, chameleon self-adaptive algorithm

PACS: 03.67.Hk, 92.60.Wc, 42.50.Md, 03.67.Ac

DOI: 10.7498/aps.65.020303

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61172071, 61201194), the Natural Science Research Foundation of Shaanxi Province, China (Grant No. 2014JQ8318), and the International Scientific and Technological Cooperation and Exchange Program in Shaanxi Province, China (Grant No. 2015KW-013).

† Corresponding author. E-mail: 285025572@qq.com