# 飞行中继平台的 MDI-QKD 应用性能

李天秀，石　磊，李佳豪，王俊辉

(空军工程大学 信息与导航学院，陕西 西安 710077)

**摘　要：**量子密钥分发 (Quantum Key Distribution, QKD) 技术的应用领域不断拓宽，其良好的安全保密性能可以有效应对通信安全威胁，在航空通信领域，基于航空飞行平台应用量子密钥分发技术有望大幅提升航空通信系统安全性级别，为局部地区保密通信提供可靠保障，进一步提高区域安全通信保障能力。针对非对称传输效率测量设备无关量子密钥分发 (Measurement Device Independent QKD, MDI-QKD) 协议在机载条件下的应用问题，在以飞行平台作为测量节点的测量设备无关量子密钥分发技术应用场景下，应用诱骗态协议建立了仿真分析模型，分析了气象条件、飞行高度对系统仿真性能的影响。仿真实验结果表明，在 15 km 能见度的晴朗天气下，在无人机常用高度飞行的空中移动平台应用诱骗态测量设备无关量子密钥分发协议可以提供作战通信保障，在较远距离通信中存在通信盲区和飞行平台运动限制。同时证明了优化选择信号光源光脉冲强度方案可以有效提高通信能力。实验及分析为量子密钥分发技术在飞行平台上的后续研究和实际应用提供了理论分析基础和优化方法。

**关键词：**量子通信；　量子密钥分发；　航空通信；　测量设备无关

**中图分类号：**TN918　　**文献标志码：**A　　**DOI：**10.3788/IRLA20210124

# Performance of Measurement Device Independent Quantum Key Distribution on flight repeater platform

Li Tianxiu, Shi Lei, Li Jiahao, Wang Junhui

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

**Abstract:** Quantum Key Distribution (QKD) technology now is used in more fields with its good security and confidentiality performance can effectively deal with communication security threats. The application of QKD technology based on aviation flight platform is expected to greatly improve the security level of aviation communication system and provide reliable guarantee for local area secure communication. To analyze airborne application of Measurement Device Independent QKD(MDI-QKD) with asymmetric transmission efficiency, the simulation analysis model combined with the decoy state method was established. The effect of meteorological conditions, flight height on the performance of the system simulation were analyzed. The results show that the application of MDI-QKD protocol in the air mobile platform at the common flight altitude of early-warning aircraft can provide combat communication guarantee under the fine weather with the visibility of about 15 km, but there are communication blind areas and movement restrictions of the flight platform in the long-distance communication. Further experiment indicates the adjustment of signal pulse intensity is an effective method to improve the performance. Above all, the experiment provides theoretical basis and optimization method for the further research and practical application of QKD on flight repeater platform.

**收稿日期:**2021−02−26；　**修订日期:**2021−04−14

**基金项目:**国家自然科学基金 (61971436)

**作者简介:**李天秀，女，硕士生，主要从事量子通信方面的研究。

**导师简介:**石磊，男，教授，博士生导师，博士，主要从事量子通信方面的研究。

**Key words:** quantum communication; Quantum Key Distribution; aeronautical communication; Measurement Device Independent

## 0 引 言

量子密钥分发 (Quantum Key Distribution, QKD) 作为目前量子信息技术领域最成熟的分支之一, 其迅猛发展推动了保密通信技术的革新。

QKD 是基于不确定性原理、不可克隆定理等量子力学特性传输安全密钥的通信保密手段, 并在结合“一次一密”模式条件下, 可以提供无条件安全性 [1−3]。其安全性不再依赖于计算复杂度, 而是仅取决于量子力学原理的正确性 [4]。基于 QKD 的量子保密通信有望在高度网络化、智能化军事变革背景下为破解传统射频通信手段安全隐患带来新的解决思路。在军事通信保障行动中, 飞行平台可以作为重要的区域通信中继节点[5], 将量子通信手段加装在机载平台可以有效解决通信安全问题, 提供更具安全性和可靠性的区域通信保障。

近年来, 国内外多个团队在机载量子通信实验和理论方面进行了广泛研究, 取得了一定成果。Nauerth 等人实现了相距 20 km 的飞机与地面接收站之间的 QKD 实验, 获得筛选密钥率 145 bit/s[6]。加拿大 Waterloo 大学的 Bourgoin 等人使用运动速度为 33 km/s 的卡车模拟机载平台相对运动场景, 在解决了光束指向纠正、光子偏振选择等问题的基础上, 实现了最终误码率小于 7% 的 QKD 实验[7]。该团队随后以飞行平台作为接收端, 在高度约为 1.6 km、距离 3~10 km 不等的链路中进行了机载 QKD 实验, 标志着机载 QKD 应用的又一进步[8]。

但上述实验均采用只包含一个发送者和一个接收者的 BB84 协议, Lo 等人于 2012 年提出的测量设备无关量子密钥分发 (Measurement-Device-Independent QKD, MDI-QKD)[9] 协议中则采用由两个发送者同时将制备的量子态发送到非可信第三方进行 Bell 测量, 不仅能有效免疫探测器单元的侧信道漏洞, 还能大大拓展密钥分发距离[10−12], 为机载量子通信提供了又一选择。2020 年, 曹原等进行了远距离自由空间诱骗态 MDI-QKD 验证性实验, 在总距离约为 19.2 km 的大气信道中实现了密钥分发, MDI-QKD 在固定对称信道中的可行性得到实际检验[13]。同时, 针对 MDI-QKD 协议的研究和改进也在进一步深入, 基于纠缠粒子、双光场干涉等形式的改进型协议从理论上表现出了良好的性能, 使得 MDI-QKD 协议具有更大的应用潜力[14−16]。

文中结合作战区域通信保障的实际情况, 在以飞行平台为通信中继节点的应用模式下, 建立诱骗态 MDI-QKD 协议的通信保障能力的理论模型, 分析了不同天气条件、飞行平台高度、通信终端运动等因素对通信能力的影响, 结合链路非对称性对信号光强度选择进行了优化, 并提出提高密钥生成率的一种方案。

## 1 应用场景

通信保障始终是现代化军事斗争的重要基础, 随着冲突形式的发展变化, 在规模化的固定通信网络外, 针对任务区域的临时性通信保障成为了完善战场信息传输网络体系的重要一环。以美军为例, 大量使用无人机通信中继是目前美军解决其作战部队在执行战术任务时的超视距通信问题的主要方法之一。美军战术分队在伊拉克和阿富汗山区和城区, 面对所处环境的复杂地形和超短波通信电台避障能力相对较差导致的通信障碍, 选择采用全球鹰 Block20 等型号无人机搭载战场机载通信节点为地面战术单元提供实时信息交换、话音中继服务。此种方式可以有效规避复杂地面环境对通信的影响, 同时又提供了更具灵活性、机动性的通信保障[17−18]。文中所提出的应用场景正是基于这一思路, 将量子保密通信纳入区域临时通信保障范畴, 利用机载平台实现安全密钥传输, 提高通信系统整体的安全性和可靠性。

基于图 1 所示的应用场景, 模型将两地面站点作为通信收发双方, 采用 MDI-QKD 协议, 以无人机、预警机等飞行平台作为通信测量方。这样既可以有效解决地面两临时通信站点的保密通信需求, 又充分利用 MDI-QKD 协议隔离通信第三方的优点, 解决飞行平台不可信对通信安全性的威胁, 提供更好的反劫持能力。

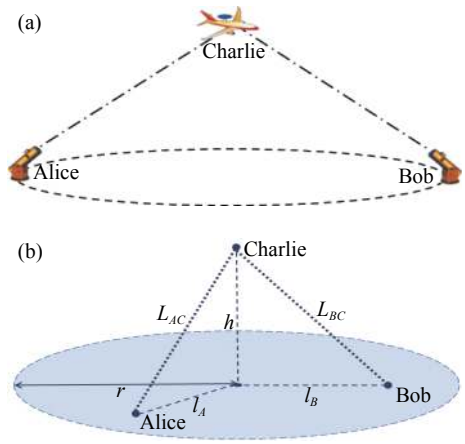


图 1 飞行通信中继平台应用模型。(a) 应用结构; (b) 几何结构

Fig.1 Application model of communication via flight repeater platform. (a) Application structure; (b) Geometry structure

## 2 理论模型

在 MDI-QKD 协议中, 通信双方 Alice 和 Bob 不在己端进行 Bell 态测量, 而将光脉冲发送至第三方 Charlie 进行 Bell 态测量, 这一方案具有更高的安全性, 通信距离也得到拓展。此外, 在实际应用的 QKD 系统中, 通常选择使用弱相干光源 (Weak coherent source) 代替单光子光源, 光源选择引入的安全威胁可通过采用诱骗态方案予以改善, 常见的诱骗态方案包括单诱骗态、双诱骗态等[19−20], 诱骗态方案可结合不同量子密钥分发协议进行应用。

文中仿真分析采用三强度诱骗态 MDI-QKD 协议, 三强度诱骗态是指 Alice 和 Bob 发送的相关光脉冲在经过偏振编码后, 经过强度调制器调制为三强度, 分别对应真空态、诱骗态、信号态, 发送至第三方。第三方通过分束器、偏振分束器和探测器对接收到的光脉冲信号进行贝尔态测量。这一方案能够以较低的复杂度获得诱骗态协议的安全性, 且有效表征诱骗态 MDI-QKD 协议的应用性能。对这一协议的进一步介绍见参考文献 [20]。

在上述诱骗态 MDI-QKD 协议中, Alice 和 Bob 最终提取出的安全密钥率为[20]:

$$R \geqslant \mu_2\nu_2\exp(-\mu_2-\nu_2)\,Y_{11}^{Z}\left[1-H\left(e_{11}^{x}\right)\right]-Q_{\mu_2\nu_2}^{z} f H\left(E_{\mu_2\nu_2}^{z}\right) \tag{1}$$

式中: $Y_{11}^{z}$为单光子增益; $e_{11}^{x}$为单光子误码率。单光子增益的下界和单光子误码率的上界可表示为:

$$Y_{11}^{\omega} \geqslant \frac{g_1^{\omega}+g_2^{\omega}+g_3^{\omega}-\exp(\mu_2+\nu_2)\,Q_{\mu_2\nu_2}^{\omega}}{\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1\alpha\mu_1\nu_2}+\frac{\exp(\mu_1+\nu_1)\,Q_{\mu_1\nu_1}^{\omega}}{\mu_1\nu_1-\mu_2\nu_2+\alpha\mu_2\nu_1+\alpha\mu_1\nu_2} \tag{2}$$

$$e_{11}^{\omega} \leqslant \frac{\exp(\mu_1+\nu_1)\,Q_{\mu_1\nu_1}^{\omega}E_{\mu_1\nu_1}^{\omega}-g_4^{\omega}}{\mu_1\nu_1 Y_{11}^{\omega}} \tag{3}$$

式中: $Q_{\mu_i\nu_j}^{\omega}$和$E_{\mu_i\nu_j}^{\omega}$分别为给定光脉冲强度时指定基的增益和误码率, 通常可由实验数据给出。在仿真实验中可使用以下公式进行计算[19]:

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

$$Q_{\mu_i\nu_j}^{x}E_{\mu_i\nu_j}^{x}=e_0Q_{\mu_i\nu_j}^{x}-2(e_0-e_d)y^2\left[I_0(2s)-1\right] \tag{5}$$

$$Q_{\mu_i\nu_j}^{z}=Q_c+Q_E \tag{6}$$

$$Q_{\mu_i\nu_j}^{z}E_{\mu_i\nu_j}^{z}=e_dQ_c+(1-e_d)Q_E \tag{7}$$

在前述计算过程中出现的参数组$g_n^{\omega}$、$Q_c$、$Q_E$、$\alpha$等的具体计算方式见参考文献 [21]。这里需要注意的是以上公式中出现的如下参量:

$$s=\frac{\sqrt{\eta_a\mu_i\eta_b\nu_j}}{2} \tag{8}$$

$$y=(1-P_d)\exp\left(-\frac{\mu'}{4}\right) \tag{9}$$

$$\mu'=\eta_a\mu_i+\eta_b\nu_j \tag{10}$$

这一组参量包括信号态、诱骗态光源的脉冲强度、两侧传输效率等, 是密钥率估算函数的自变量, 这一系列的参数从根本上决定了误码率、增益及最终的生成密钥率。其中$\eta_a$、$\eta_b$为系统传输效率, 在机载平台应用条件下, 系统传输效率可表示为大气信道传输效率、单光子探测器探测效率与光束衍射衰减的乘积[22]:

$$\eta=\eta_{\rm atm}\times\eta_D\times\eta_{diff} \tag{11}$$

大气信道传输效率包含吸收散射损耗和湍流损耗。其中, 大气吸收与散射损耗$\eta_{\rm abs}$由实时大气信道衰减系数$\alpha$与通信链路长度$L$共同决定, 湍流损耗系数$\eta_{\rm turb}$与信号光波长、发射机半径等有关。

$$\eta_{\rm atm}=\eta_{\rm abs}\eta_{\rm turb} \tag{12}$$

$$\eta_{\rm abs}=\exp(-\alpha L) \tag{13}$$

$$\eta_{\rm turb}=\frac{\left(\frac{\lambda}{R_t}\right)^2}{\left(\frac{\lambda}{R_t}\right)^2+\theta_{\rm turb}^2} \tag{14}$$

式中：$R_t$为发射机望远镜主镜半径；$\theta_{\text{turb}}^2$为湍流造成的附加散度，与湍流性质有关。

在前文所述的应用背景下，根据图 1(b) 给出的几何模型，利用链路两端及测量端投影点间三角函数关系，两侧通信链路长度$L_{AC}$，$L_{BC}$可以表示为：

$$\begin{aligned} L_{AC} &= \frac{h}{\cos\left[\arctan\left(\frac{l_A}{h}\right)\right]} \\ L_{BC} &= \frac{h}{\cos\left[\arctan\left(\frac{l_B}{h}\right)\right]} \end{aligned} \tag{15}$$

式中：$h$为平台飞行高度；$l_A$、$l_B$为飞行平台垂直投影点距离通信站点的水平距离。

实时大气信道衰减系数$\alpha$通常用于表征大气环境对量子信号的影响，量子光信号在大气中的传输受到包括大气分子吸收、悬浮微粒吸收、瑞利散射、米氏散射在内的多种因素影响[23−25]，通过对系数$\alpha$的描述，可以有效反映大气信道对量子信号的影响。为了便于进一步估测大气中量子信号的实际衰减情况，参考文献 [26] 根据实验结果，给出了大气衰减系数$\alpha$与能见度$V_v$之间的经验公式：

$$\alpha(\lambda)=\left(\frac{3.91}{V_v}\right)\left(\frac{0.55}{\gamma}\right)^q \tag{16}$$

其中，参数$q$的取值与能见度$V_v$的关系为：

$$q=\begin{cases} 1.6, & V_v>50\ \text{km} \\ 1.3, & 6\ \text{km}<V_v<50\ \text{km} \\ 0.16V_v+0.34, & 1\ \text{km}<V_v<6\ \text{km} \\ V_v-0.5, & 0.5\ \text{km}<V_v<1\ \text{km} \\ 0, & V_v<0.5\ \text{km} \end{cases} \tag{17}$$

目前，在量子密钥分发实验系统中普遍采用波长为 850 nm的信号光，在这一条件下计算公式 (14)、(15)，其结果在图 2(a) 中给出，并结合图 2(b) 所示的某日我国境内气象实况，在能见度等级 5~10 km、10~20 km 范围内，选择图 2(a) 中标注数据作为后续仿真实验参数。

光束衍射损耗的计算方法如下：

$$\eta_{diff}=\left(\mathrm{e}^{-2\gamma_t^2\alpha_t^2}-\mathrm{e}^{-2\alpha_t^2}\right)\left(\mathrm{e}^{-2\gamma_r^2\alpha_r^2}-\mathrm{e}^{-2\alpha_r^2}\right) \tag{18}$$

$$\gamma_{t,r}=\frac{b_{t,r}}{R_{t,r}},\alpha_{t,r}=\frac{R_{t,r}}{\omega_{t,r}},\omega_t=R_t,\omega_r=\frac{\sqrt{2}\lambda L}{\pi R_t} \tag{19}$$

式中：下标$t$为发射端；$r$为接收端；$R$、$b$为主、副镜半径；$\omega$为波束半径。仿真使用的具体参数取值参考文献 [27]，详见表 1。

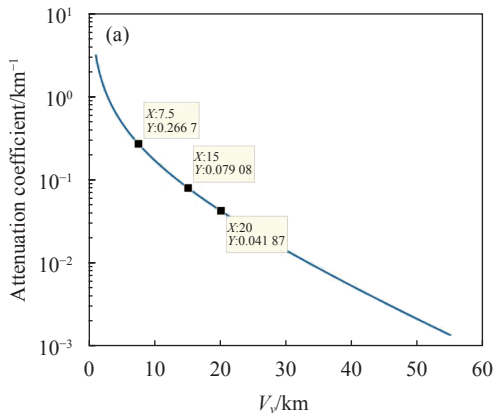


图 2 大气衰减系数与能见度关系及取值。(a) 大气衰减系数与能见度关系；(b) 能见度情况图

Fig.2 Visibility and attenuation coefficient relationship and values. (a) Relationship between visibility and attenuation coefficient; (b) Visibility map

在实际通信系统中仍存在诸多因素对通信系统整体性能产生影响，如背景光、有限码长效应等，在此作以补充分析。

背景杂散光问题与 ATP 等系统精度均是影响空间量子通信系统性能的主要因素，但是包括“三域”滤波，即时域、空域、频域滤波等在内的多种抑制手段能够有效减弱背景光的影响，同时元器件性能的改善也提高了系统对背景光的抑制能力，背景杂散光干扰的影响程度在不断减弱。量化表示背景光干扰涉及到大气条件下背景辐射率及实际通信系统的发射器脉冲重复率、探测器时间窗口大小、发射机跟瞄误差、光源光束远场发散角、接收机天线孔径等诸多因素，需要对实际通信系统器件等进行详尽的分析和描述。但是实验系统之间存在较大的性能差异，包括 ATP 系统在内的各组成部分所使用的补偿算法也会对整体性能产生影响[28]，上述问题需结合实际实验环

**表 1 仿真参数设置**

**Tab.1 Simulation parameter**

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| $\mu_0$ | 0 | $P_d$ | $3\times10^{-6}$ |
| $\mu_1$ | 0.01 | $f$ | 1.16 |
| $\mu_2$ | 0.36 | $R_t$ | 50 cm |
| $\nu_0$ | 0 | $R_r$ | 15 cm |
| $\nu_1$ | 0.01 | $b_t$ | 5 cm |
| $\nu_2$ | 0.36 | $b_r$ | 1 cm |
| $e_d$ | 1.5% | | |
| $e_0$ | 0.5 | | |

境及数据进行分析讨论。因此文中模型在有效表征通信性能的同时，简化了通信系统差异带来的影响，弱化了背景光、ATP 系统等因素的影响，着重分析空间时变信道，突出了链路长度变化、大气环境变化对飞行平台量子通信性能的影响及运动情况下通信覆盖区域的变化情况。

有限码长效应是指由于密钥长度的有限，引起参数估计的统计波动，从而影响最终的密钥估计。在考虑有限码长效应时，$Q^{\omega}_{\mu_i\nu_j}$、$E^{\omega}_{\mu_i\nu_j}$的计算方式可修正为：

$$\begin{aligned} &Q^{\omega}_{\mu_i\nu_j}(1-\beta_q)\leqslant\overline{Q}^{\omega}_{\mu_i\nu_j}\leqslant Q^{\omega}_{\mu_i\nu_j}(1+\beta_q)\\ &Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}(1-\beta_{eq})\leqslant\overline{Q}^{\omega}_{\mu_i\nu_j}\overline{E}^{\omega}_{\mu_i\nu_j}\leqslant Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}(1+\beta_{eq}) \end{aligned} \tag{20}$$

波动率定义为：

$$\beta_q=\frac{n_a}{\sqrt{N^{\omega}_{\mu_i\nu_j}Q^{\omega}_{\mu_i\nu_j}}}\qquad \beta_{eq}=\frac{n_a}{\sqrt{N^{\omega}_{\mu_i\nu_j}Q^{\omega}_{\mu_i\nu_j}E^{\omega}_{\mu_i\nu_j}}} \tag{21}$$

式中：$n_a$为用于统计波动分析的标准偏差的参数值；$N^{\omega}_{\mu_i\nu_j}$为数据长度[29−30]。同时，对密钥率的估计需增加协议因子$f_q$，即在公式 (1) 右侧乘以$f_q$。对于有限集而言，该因数定义为：

$$f_q=P_{\mu_a}P_{z|\mu_a}P_{\mu_b}P_{z|\mu_b} \tag{22}$$

式中：$P_{\mu_a}$、$P_{z|\mu_a}$、$P_{\mu_b}$、$P_{z|\mu_b}$分别为 Alice 和 Bob 发送信号态的概率及其该态下选 $Z$ 基编码的条件概率[31]。

根据参考文献 [29] 的仿真结果，在$n_a=5$、$N^{\omega}_{\mu_i\nu_j}=10^{10}$条件下，相较于无限码长情况，系统可容忍的最大传输损耗下降约 15 dB，会进一步降低通信性能。但这一效应与飞行平台运动及大气环境改变关系并不密切，因此在后续分析中仍使用无限码长条件，但是仍然必须认识到有限码长效应在实际应用中对通信距离的限制。

## 3 仿真结果与分析

根据公式 (2)、(3) 及参考文献 [16] 可以计算得到单光子计数率的下限和单光子误码率上限，进而最终计算出密钥生成率的数值。计算过程中所使用到的仿真参数设置参考文献 [20]，详见表 1。

在仿真实验过程中，首先假定飞行中继平台位于通信双方的正中央，即两侧通信链路等长。在此条件下，设定飞行高度为 8 km，在改变大气衰减系数也就是在不同天气情况下，可以得到如图 3(a) 所示结果。由此可以发现，在天气晴朗条件下，机载诱骗态 MDI-QKD 通信覆盖半径可到达 30 km 以上，但在天气条件较为恶劣的情况下，通信覆盖半径将显著减少至不足 20 km。表明 MDI-QKD 在大气中应用能力受到天气条件的限制，在天气条件较差时，通信距离的下降十分显著，需要采取适当的补偿方法提高实际通信能力。图 3(b) 所示为在天气情况给定条件下、改变飞行平台飞行高度情况下所能提供的通信覆盖范围的变化情况。根据仿真结果，飞行平台高度对通信能力的影响很小，在实际应用过程中可以调节适宜的飞行高度以适应实际需要，并且这种改变不会很大程度地影响通信性能，也有利于飞行平台选择范围的进一步拓展。

在实际应用过程中很难保证上述仿真情况下两链路绝对对称，由于飞行平台的运动，实际系统中的通信链路为时变链路，单侧链路衰减会实时改变，因此需进一步分析平台运动情况下的通信能力。在仿真实验中，首先假定飞行平台运动而地面站 Alice 固定，自飞行平台从 Alice 端过顶时起算，以生成密钥率大于$10^{-9}$ bit/pulse 为通信限制，即千兆频率光源生成密钥 1 bit/s，得到此时最远通信距离。

表 2 中$l_B$表示在飞行平台投影点与 Alice 端距离$l_A$改变情况下，Bob 所处的位置范围的极限。从结果来看，在飞行平台与 Alice 端距离达到 20 km 时出现了通信盲区情况，也就是$l_B$存在下限，出现了环状覆盖区域，空间结构见图 4(a)。这一现象的产生是由于链路不对称性的显著加剧使得通信系统整体能够容忍的信道损耗急剧减少。此时虽然总距离远小于可通信范围的最大值，但是由于性能劣化严重，仍然无法进行通信。

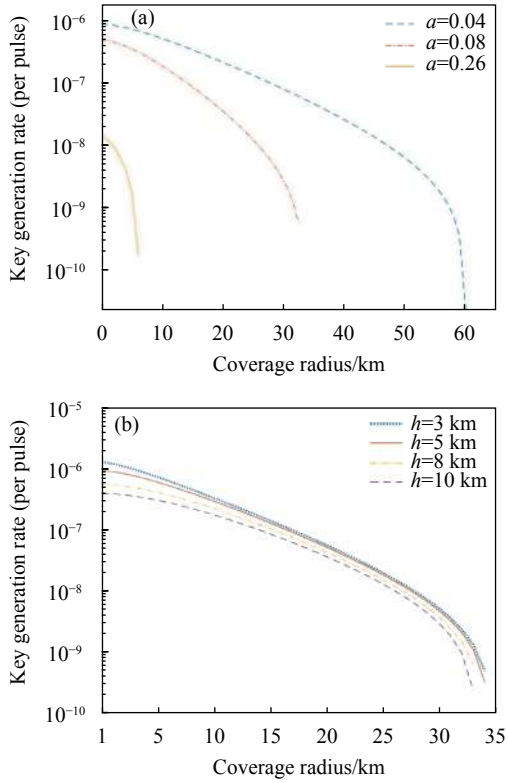


图 3 不同情况下通信覆盖范围。(a) 不同大气衰减下通信覆盖范围; (b) 不同飞行高度通信覆盖范围

Fig.3 Coverage radius in different situation. (a) Coverage radius with different atmospheric attenuation; (b) Coverage radius with different height

**表 2 移动情况下 Bob 通信距离限制 (单位：km)**

**Tab.2 Communication distance limits of Bob with moving platform (Unit: km)**

| $l_A$ | $l_B$ |
|---|---|
| 0 | 25 |
| 5 | 28 |
| 10 | 31 |
| 20 | 3, 35 |
| 30 | 12, 33 |

从另一角度分析，在 Alice 和 Bob 相对位置关系确定时，自飞行平台从 Alice 端过顶时起算其运动距离，可以得到飞行平台运动情况与密钥率之间的关系，结果如图 5 所示。

在总通信距离为 20 km 时，飞行平台的运动会随链路对称性的改善而提高，而在通信距离达到 30 km 时出现部分区域无法通信的情况。说明当总距离达到一定程度时，中心节点过于靠近两地面站则无法通

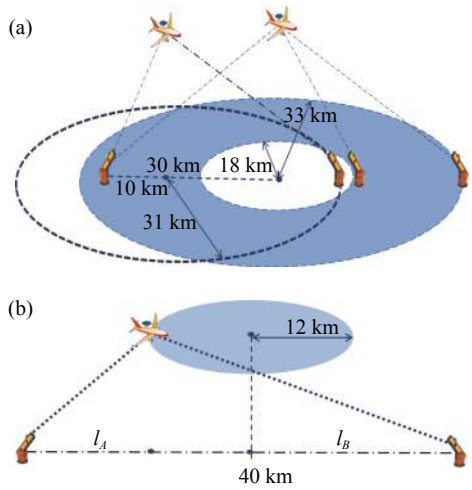


图 4 通信平台运动限制。(a) 飞行平台运动时 Bob 端距离限制; (b) 给定总距离下飞行平台运动限制

Fig.4 Moving limits of communication platform. (a) Distance limits of Bob with moving aerial platform; (b) Moving limits of aerial platform with given total distance

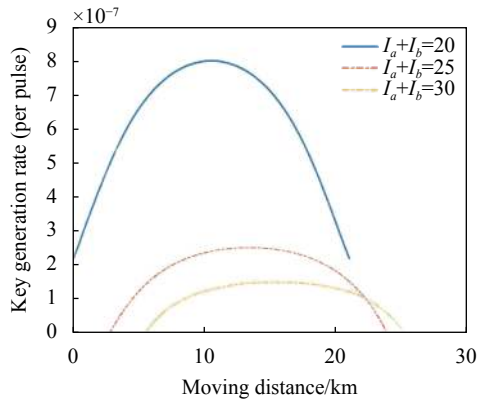


图 5 给定总长度情况下移动距离与密钥生成率关系

Fig.5 Relationship between key generation rate and distance of moving platform with given total length

信。也就是在总通信距离确定时，飞行平台在其中空域进行一定范围移动，其移动区域存在一定限制，采用同上的通信限制条件可得如表 3 所示数据，其空间结构如图 4(b) 所示。表 3 中 $l_A+l_B$ 表示地面通信双方之间的直线距离即给定总距离，$l_A-l_B$ 表示飞行平台运动范围的直径，在两地面站距离 40 km 范围内，以地面站连线中点为圆心，飞行平台的运动直径仅为 10 km，表明在远距离通信中要尽可能保证中继平台位于地面站的中心位置，中继平台的过度偏移将会导致通信性能下降。

上述通信限制的出现，除由于通信系统所能容

**表 3 给定距离下移动范围限制 (单位：km)**

**Tab.3 Moving diameter with given total distance (Unit: km)**

| $l_A+l_B$ | $l_A-l_B$ |
|---|---|
| 20 | 20 |
| 25 | 21 |
| 30 | 18 |
| 35 | 16 |
| 40 | 12 |

忍的总链路衰耗有限外，链路非对称性带来的性能劣化是另一重要原因。图 6 所示为在不同链路长度比值$\sigma$条件下密钥生成率与信道衰减之间的关系。在$\sigma=0.1$情况下，相较于链路等长，即$\sigma=1$时系统所能容忍的信道损耗急剧下降，在相同密钥率限制情况下，$\sigma=1$能够容忍的信道损耗可达到$\sigma=0.1$情况下的 2 倍，这就解释了前述运动情况下出现的环状通信覆盖范围和飞行平台的运动限制。

针对链路不对称带来的性能劣化，可以采用调节信号光强度的方式进行补偿。这一方式是在给定某一链路情况的条件下匹配可以获得实时最大密钥率的最佳光强组合。通过应用前文给出的计算方法，对信号光强度在一定范围内进行遍历搜索，可以得到理论上最大密钥率对应的光强选择。在文中的优化过程中仅针对 Alice 和 Bob 信号光强两参数进行优化，其他参数仍采用原仿真实验参数，示例结果在表 4 中给出，其中$(l_A,l_B)$为两侧通信链路长度，$R_0$为按原光源参数得到的生成密钥率计算结果，$R_{\max}$表示在最佳信号光强组合$(\mu_2,\nu_2)$情况下的生成密钥率。

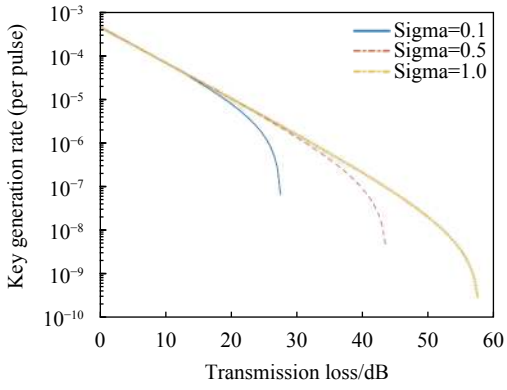


图 6 不对称链路件下密钥生成率与信道衰减关系

Fig.6 Relationship between key generation rate and transmission loss in asymmetric link

根据优化结果，在有效调整信号光强的情况下，最终密钥率提高可以达到一个数量级。在工程实践中，根据通信情况对光源进行预先调整是有效应对链路非对称性导致通信性能劣化的有效方式。同时，可以进一步对弱诱骗态光强、矢基选择概率等参数进行同步优化，以进一步提高通信性能，但多参数最优值搜索过程的时间复杂度较高，文中仅以两参数优化举例，在后续研究中应考虑使用改进的搜索算法、人工智能方法[32] 实现全局参数优化，最终达到根据通信现实条件的光源参数的自适应调整方式。

**表 4 不对称链路下最佳信号光强选择**

**Tab.4 Optimal signal intensity selection in asymmetric link**

| $(l_A,l_B)$ | $(\mu_2,\nu_2)$ | $R_0$ | $R_{\max}$ |
|---|---|---|---|
| (20, 20) | (0.42,0.42) | $8.35\times10^{-8}$ | $2.23\times10^{-7}$ |
| (20, 25) | (0.43,0.45) | $6.28\times10^{-8}$ | $1.02\times10^{-7}$ |
| (20, 30) | (0.42,0.46) | $4.55\times10^{-8}$ | $8.59\times10^{-7}$ |

## 4 结 论

在以飞行平台作为通信中继节点的应用条件下，应用诱骗态 MDI-QKD 量子通信协议具有理论上的可行性。在天气晴朗、平台处于无人机常用飞行高度条件下，可实现数十千米的安全通信服务保障，但其通信能力受天气影响显著。在飞行平台实时运动情况下，链路非对称性带来的通信性能劣化会对通信节点运动范围产生限制，存在通信盲区、环状通信覆盖等情况。为解决这一问题可采用调整包括信号光强度在内的光源参数的方式，匹配不同链路情况，以获得最大密钥生成。在下一步的研究工作中将就智能化的参数优化进行探索，并尝试开展机载实验。

**参考文献：**

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984, 560: 175–179.

[2] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography [J]. ***Review of Modern Physics***, 2002, 74: 145.

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution [J]. ***Review of Modern Physics***, 2009, 81(3): 1301.

[4] Guo G C. Research status and future of quantum information technology [J]. ***Sci Sin Inform***, 2020, 50(9): 121-132. (in Chinese)

[5] Wu Zhongbo, Yi Jianqiang. Cooperative communication relay selection method for UVA formation support networks [J]. ***Acta Aeronautica et Astronautica Sinica***, 2020, 41(S2): 187-194. (in Chinese)

[6] Nauerth S, Moll F, Rau M, et al. Air to ground quantum key distribution [C]//Proceedings of SPIE, 2012, 8518: 85180D.

[7] Bourgoin J P, Higgins B L, Gibov N, et al. Free-space quantum key distribution to a moving receiver [J]. ***Optics Express***, 2015, 23(26): 33437-33447.

[8] Pugh C J, Kaiser S, Bourgoin J P, et al. Airborne demonstration of a quantum key distribution receiver payload [J]. ***Quantum Science and Technology***, 2017, 2(2): 024009.

[9] Lo H K, Curty M, Qi B. Measurement device independent quantum key distribution [J]. ***Physical Review Letters***, 2012, 108(13): 130503.

[10] Huang J Z, Yin Z Q, Chen W, et al. A survey on device-independent quantum communications [J]. ***China Communications***, 2013(2): 1-10.

[11] Yin H L, Chen T Y, Yu Z W, et al. Measurement device independent quantum key distribution over 404 km optical fiber [J]. ***Physical Review Letters***, 2016, 117(19): 190501.

[12] Ma X F, Razav M. Alternative schemes for measurement-device-independent quantum key distribution [J]. ***Physical Review A***, 2012, 86(6): 3818-3821.

[13] Cao Y, Li Y H, Yang K X, et al. Long-distance free-space measurement-device-independent quantum key distribution [J]. ***Physical Review Letter***, 2020, 125(26): 260503-260509.

[14] Ke Z J, Wang Y T, Yu S, et al. Detection and quantification of entanglement with measurement-device-independent and universal entanglement witness [J]. ***Chin Phys B***, 2020, 8(14): 080301.

[15] Wang C, Yin Z Q, Wang S, et al. Measurement-device-independent quantum key distribution robust against environmental disturbances [J]. ***Optica***, 2017, 9(4): 1016-1023.

[16] Rubenok A, Slater J A, Chan P, et al. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks [J]. ***Physical Review Letters***, 2013, 9(27): 130501.

[17] Liu H J. Current situation and trend of USA communication relay [J]. ***Airborne Missile***, 2017(2): 39-44. (in Chinese)

[18] Guan Z F. Current status and trend of US military UA communication system [J]. ***Communications Technology***, 2014, 47(10): 1109-1113. (in Chinese)

[19] Ma X F, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution [J]. ***Physical Review A***, 2005, 72(1): 012326-012341.

[20] Yu Z W, Zhou Y H, Wang X B. Three-intensity decoy state method for device independent quantum key distribution [J]. ***Physical Review A***, 2013, 88(1): 019901.

[21] Dong C, Zhao S H, Zhao W H, et al . Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficiency [J]. ***Acta Physical Sinica***, 2014, 63(3): 030302. (in Chinese)

[22] Yang R, Li Y X, Meng W, et al. Channel characteristics of continuous variable quantum communication system on aviation platform [J]. ***Acta Optica Sinica***, 2018, 38(9): 0927002. (in Chinese)

[23] Han L Q, Wang Q, Katsunori S. Performance of free space optical communication over gamma-gamma atmosphere turbulence [J]. ***Infrared and Laser Engineering***, 2011, 40(7): 1318-1322. (in Chinese)

[24] Liu T, Zhu C, Sun C Y, et al. Influences of different weather conditions on performance of free-space quantum communication system [J]. ***Acta Optica Sinica***, 2020, 14(2): 0227001. (in Chinese)

[25] Cao Minghua, Hu Qiu, Wang Huiqin, et al. Atmospheric optical communications channel estimation employing superimposed training sequence under sand-dust weather conditions [J]. ***Infrared and Laser Engineering***, 2019, S2(48): S218002. (in Chinese)

[26] Kim I I, McArthur B, Korevaar E J. Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications [C]//Proceedings of SPIE, 2001, 4214: 26-37.

[27] Khaleel A I, Tawfeeq S K. Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links [J]. ***International Journal of Quantum Information***, 2018, 16(3): 1850027.

[28] Zhang Guangyu, Yu Siyuan, Ma Jing, et al. Influence of

background light on quantum bit error rate in satellite-to-ground quantum key distribution [J]. ***Opto-Electronic Engineering***, 2018, 34(2): 126-129. (in Chinese)

[29] Zhang Peng. Research on the performance of practical quantum key distribution system [D]. Beijing: Beijing University of Posts and Telecommunications, 2019. (in Chinese)

[30] Song Tingting. Finite key security analysis of quantum key distribution protocols [D]. Beijing: Beijing University of Posts and Telecommunications, 2014. (in Chinese)

[31] Xu F H, Xu H, Lo H K. Protocol choice and parameter optimization in decoy-state measurement-device- independent quantum key distribution [J]. ***Physical Review A***, 2014, 89(5): 3846-3855.

[32] Wang Qin, Chen Yipeng. Application and research of machine learning in quantum secure communication [J]. ***Journal of Nanjing University of Posts and Telecommunications***, 2020, 40(5): 141-157. (in Chinese)