实用化量子密钥分发光网络中的资源优化配置*

朱佳莉[1)2)3)] 曹原[1)2)3)] 张春辉[1)2)3)] 王琴[1)2)3)†]

1) (南京邮电大学, 量子信息技术研究所, 南京 210003)

2) (南京邮电大学, 宽带无线通信与传感网教育部重点实验室, 南京 210003)

3) (南京邮电大学, 通信与网络国家工程研究中心, 南京 210003)

(2022 年 8 月 21 日收到; 2022 年 10 月 12 日收到修改稿)

在大规模量子通信网络应用研究中, 人们一般通过构建虚拟业务网络并将其映射到实际物理空间来实现资源的分配. 在该映射过程中, 为简化模型常常做一些假设, 比如假定物理拓扑中的密钥资源为某一固定值, 即忽略实际物理条件以及不同协议对密钥供给带来的性能差异. 这种忽略实际物理条件的假设可能导致该网络在实际应用中无法正常运行. 为解决以上问题, 本文从链路映射的角度出发, 以量子密钥分发光网络为底层网络, 提出了改进的虚拟业务映射模型和虚拟业务映射算法, 使其更加接近于实际应用场景. 一方面通过增加地理位置的约束, 对虚拟节点到可映射的物理节点范围做合理限制; 另一方面, 从硬件成本和实际密钥生成速率角度出发, 提出了性价比的评估指标对资源进行分配管理. 此外, 我们通过结合 3 种主流的量子密钥分发协议 (BB84、测量设备无关、双场), 构建了普适的虚拟业务在量子密钥分发光网络中的映射模型, 实现了最优协议的推荐和资源的优化配置管理.

关键词: 资源优化配置, 量子密钥分发, 虚拟业务映射, 性价比

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.72.20221661

1 引 言

不论是在传统光网络中, 还是在量子密钥分发光网络中, 都是通过将所构建的虚拟网络映射到实际的物理空间来实现资源的分配[1–3]. 在进行网络拓扑的表征时, 网络通常由点和线构成, 点代表骨干中继站, 线代表路径, 因此映射分为节点 (点) 映射和链路 (线) 映射. 虚拟业务由虚拟节点和虚拟链路组成[4], 在资源分配中, 需要将虚拟节点与物理节点一一对应起来, 虚拟链路与实际物理链路一一对应起来[5], 这两个映射顺序可以颠倒, 但必须要互洽, 从而满足虚拟业务的资源需求, 实现数据的加密传输. 在虚拟业务的映射过程中, 如何降低业务阻塞率并提高资源利用率是研究重点.

在之前的研究中, 许多假设都是过于理想化而不符合实际, 例如, 假定每条物理链路上的密钥产生速率相同而不考虑具体使用哪一种量子密钥分发 (quantum key distribution, QKD) 协议[6]. 因为 QKD 协议不同, 其密钥产生速率不同[7,8], 而且由于每条物理链路的长度不尽相同, 即使采取同一种量子密钥分发协议, 不同物理链路上的密钥产生速率也应该有所区别. 因此在本文中, 我们结合具体的 QKD 协议, 研究了不同长度的物理链路的密钥产生速率以及之间的关联和相似性. 为了对不同 QKD 协议的性能进行评价与比较, 考虑了各类

* 国家重点研究发展计划 (批准号: 2018YFA0306400)、国家自然科学基金 (批准号: 12074194, 12104240, 62201276)、江苏省重点研发计划产业前瞻与关键核心技术项目 (批准号: BE2022071)、江苏省自然科学基金 (批准号: BK20192001, BK20210582)、江苏省高等学校自然科学研究项目 (批准号: 22KJB510007) 和南京邮电大学自然科学基金 (批准号: NY220123) 资助的课题.

† 通信作者. E-mail: qinw@njupt.edu.cn

QKD 协议可信中继的成本及其传输效率, 设计了基于不同 QKD 协议确定不同长度物理链路上密钥产生速率的算法, 然后通过编程对实际情况进行仿真计算, 同时引入“性价比”这个性能指标, 考察了不同 QKD 协议“性价比-链路长度”函数曲线. 通过以性价比最高为目的, 结合实际物理条件限制, 可以对每个链路选取合适的 QKD 协议以及中继数量. 在选择了合适的 QKD 协议之后, 还需要结合实际物理条件, 建立虚拟业务映射模型. 在映射模型中, 实际物理链路是量子与经典的融合通道, 除了要考虑所选的 QKD 协议带来密钥资源, 还要考虑经典信息传输占据的带宽资源[9]. 在本文的映射模型中, 考虑到实际物理空间的限制, 对于随机生成的一个虚拟业务, 其可映射到的物理节点是有限制的, 我们通过距离算法求出其最近距离内的可映射节点. 每条链路选定 QKD 协议以及中继数后, 就确定了密钥产生速率, 继而基于我们建立的映射模型, 通过随机生成大量虚拟业务, 对实际网络进行业务映射以及性能考察. 并指出可以根据编程计算的结果对原模型中 QKD 协议的选取以及中继数进行反馈改进.

2 QKD 协议的评价指标——性价比

在关于量子密钥分发光网络虚拟业务映射的研究中, 为了评估算法的网络虚拟, 可采用 USNET 和 NSFNET 这样不同规模的网络拓扑[10]. 本文基于 USNET 网络拓扑进行仿真, 如图 1 所示, 共有 24 个物理节点和 43 条物理链路.

在 USNET 拓扑中, 所有节点都是骨干节点, 每对骨干节点之间的距离为几百到几千千米. 受距离长度的限制, 在一对骨干节点之间无法直接完成量子密钥分发, 因此无法产生所需的密钥量. 通过使用可信中继可以实现两个骨干节点之间的长距离量子密钥分发. 可信中继主要是通过逐跳加密和解密的方式, 将密钥沿着量子密钥分发路径进行传输, 从而将密钥从源节点转发到宿节点. 可信中继基本原理如图 2 所示. 本文假设骨干节点之间采取等距离间隔放置可信中继的方式. 可信中继放置的间隔距离不同, 密钥生成率也会随之不同.

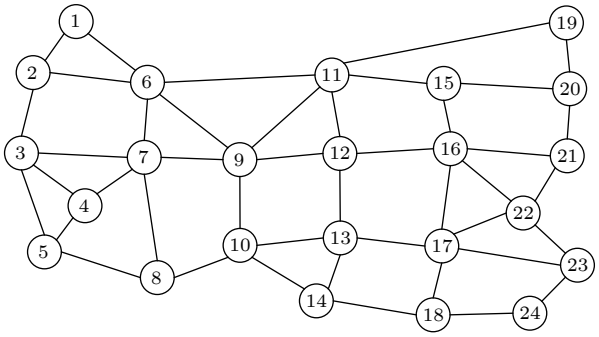

图 1 USNET 拓扑图

Fig. 1. USNET topological graph.

2.1 性价比

为了确定链路上使用什么协议, 不同长度的物理链路上如何合理地放置可信中继, 定义“性价比”这个评估指标. 通过比较同一协议下同一长度的物理链路放置不同个数可信中继的性价比大小, 可确定不同长度的物理链路应该如何放置可信中继. 通过比较不同协议中同一长度的物理链路放置最佳个数可信中继的性价比大小, 可确定不同长度的物理链路应该采用哪一种量子密钥分发协议.

性价比 CP 的公式为

$$\mathrm{CP}=\frac{R}{C}=\frac{R}{c\times n},\quad n\geqslant 1, \tag{1}$$

式中, R 表示密钥产生率, C 表示放置设备的总成本, c 为 QKD 发送机和 QKD 接收机的成本, n 为物理链路上需要放置可信中继的数量.

如果已知链路总长度为 L_{s}, 中继间距为 L, 则

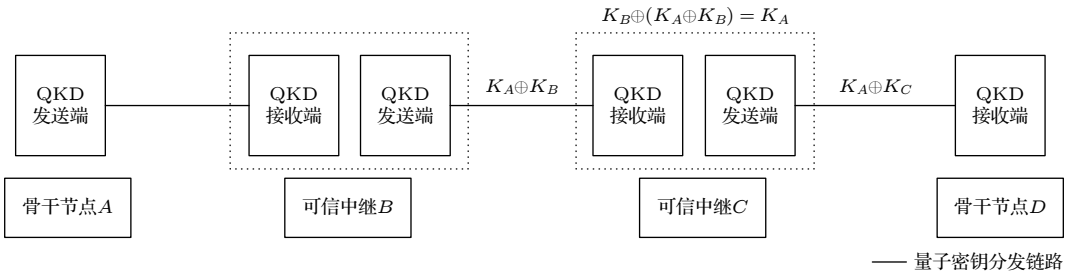

图 2 可信中继原理图

Fig. 2. Schematic diagram of trusted relay.

中继数 $n = L_{\rm s}/L - 1$, 代入 (1) 式, 得到性价比 CP 与 L 的函数关系:

$$\mathrm{CP} = \frac{R}{c \times n} = \frac{R}{c} \cdot \frac{L}{L_{\rm s} - L}. \tag{2}$$

从 (2) 式可以看出, 在链路总长度和中继间距不变的情况下, 当可信中继之间使用不同的协议时, 密钥率会发生改变, 性价比也会随之改变; 在中继间距和可信中继之间使用的协议都不变的情况下, 当链路总长度发生改变时, 性价比也会随之发生改变; 在链路总长度和可信中继之间使用的协议都不变的情况下, 中继间距发生变化将会导致中继数量改变, 性价比也会随之而改变. 因此, 本文定义的性价比公式从整体上讨论了包含可信中继之间采用不同协议、链路总长度不同和中继数量发生变化的情况.

(2) 式是性价比评估指标的一个简单表达, 具有普适性, 适用于包括 BB84、测量设备无关 (measurement-device-independent, MDI)、双场 (twin-field, TF) 等不同类型的 QKD 协议. 其中 BB84 是双方协议, 而 MDI 和 TF 是三方协议. 在 BB84 协议中, 可信中继包含一个 QKD 接收机和一个 QKD 发送机; 在 MDI, TF 协议中, 可信中继包含两个 QKD 发送机, 可信中继之间放置一个 QKD 接收机. 据此, 给出使用 3 种协议时 c 的表达式:

$$c_{kl} = \begin{cases} c_{\mathrm{BB84_{QR}}} + c_{\mathrm{BB84_{QT}}}, \\ c_{\mathrm{MDI_{QR}}} + 2c_{\mathrm{MDI_{QT}}}, \\ c_{\mathrm{TF_{QR}}} + 2c_{\mathrm{TF_{QT}}}, \end{cases}$$

其中, $c_{kl}(k \in \{\mathrm{BB84, MDI, TF}\},\ l \in \{\mathrm{QR、QT}\})$ 表示中继之间使用 k 协议时, 一个量子密钥分发发送机 (QT) 或量子密钥分发接收机 (QR) 的成本. 后文为了便于说明, 以 BB84 协议为例来解释说明模型构建过程.

2.2 BB84 协议的性价比

对三强度诱骗态条件下 BB84 协议的性价比公式展开具体的推导. BB84 协议的安全密钥产生率表达式为 [11]

$$R = q\left\{ -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L \left[1 - H_2(e_1^{\rm U})\right]\right\}. \tag{3}$$

其中 q 代表对基概率, 一般取值为 0.5, f 为纠错效率, $H_2(x)$ 是香农熵函数, 表达式如下:

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \tag{4}$$

密钥产生率主要与系统的总增益 Q_μ、误码率 E_μ、单光子脉冲的增益 Q_1 的下界 Q_1^L 和单光子脉冲的误码率 e_1 的上界 e_1^U 有关, 相关表达式为 [12]

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}, \tag{5}$$

$$\begin{aligned} E_\mu Q_\mu &= \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \\ &= e_0 Y_0 + e_{\rm detector}\left(1 - e^{-\eta\mu}\right), \end{aligned} \tag{6}$$

$$\begin{aligned} Q_1 \geqslant Q_1^{\rm L} &= \frac{\mu^2 e^{-\mu}}{\mu v_1 - v_1^2} \\ &\times \left(Q_{v_1} e^{v_1} - Q_\mu e^{\mu} \frac{v_1^2}{\mu^2} - \frac{\mu^2 - v_1^2}{\mu^2} Y_0\right), \end{aligned} \tag{7}$$

$$e_1 \leqslant e_1^U = \frac{E_{v_1} Q_{v_1} e^{v_1} - e_0 Y_0}{v_2 Y_1^L}, \tag{8}$$

式中, v_1 和 v_2 是诱骗态的强度, μ 为信号态的强度. 诱骗态的强度需要满足: $v_1 + v_2 < \mu$, $0 \leqslant v_2 \leqslant v_1$. $e_{\rm detector}$ 表示光子触发错误探测器的概率. e_0 代表真空态的误码率, 一般取值 0.5. Y_0 代表真空态的增益. 系统的整体效率可表示为 $\eta = \eta_{\rm Bob} 10^{-\alpha L/10}$, 其中 $\eta_{\rm Bob}$ 代表接收端 Bob 端的单侧效率, α 代表信道损耗系数以及 L 是信道长度.

在得到 BB84 协议的安全密钥产生率后, 就可将其代入 (1) 式中, 然后就可以得到 BB84 协议性价比公式的具体表达:

$$\begin{aligned} &\mathrm{CP} = R/C = \\ &\frac{q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1^L\left[1 - H_2\left(e_1^U\right)\right]\right\}}{c \times n}. \end{aligned} \tag{9}$$

根据 MDI 协议 [13] 和 TF 协议的密钥产生速率 [14], MDI 协议和 TF 协议的性价比公式可做同样推导.

3 虚拟业务映射模型以及映射范围求解算法

3.1 虚拟业务映射模型

介绍完 QKD 协议的评价指标, 来考虑虚拟业务的映射模型. 虚拟业务映射模型如图 3 所示, 该虚拟业务映射模型包含虚拟业务层和量子密钥分发光网络层两部分.

1) 虚拟业务层主要是由虚拟节点和虚拟链路组成. 虚拟业务具有两类网络资源需求, 包括量子密钥资源 (用于安全性) 和带宽资源. 虚拟业务层

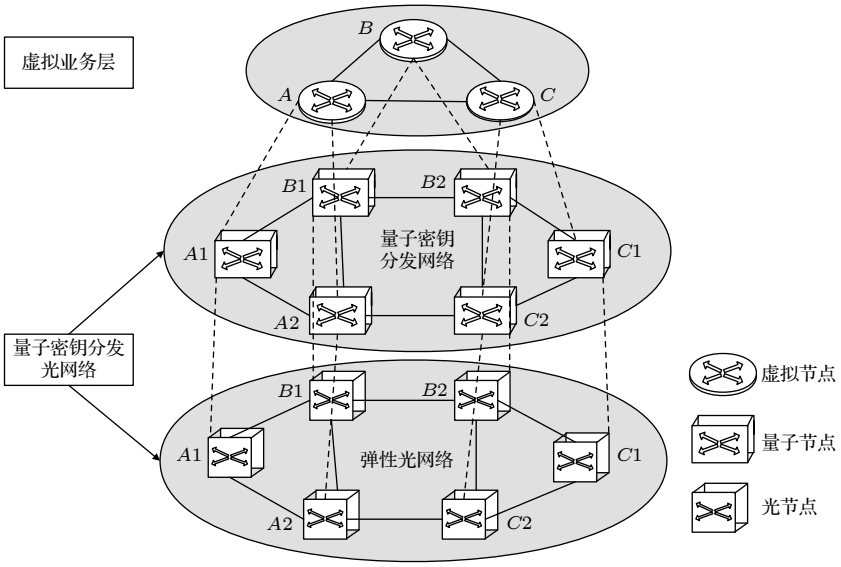

图 3 虚拟业务映射模型

Fig. 3. Virtual service mapping model.

通过一定的映射规则映射到实际物理层, 以实现业务的安全运行. 映射规则需要实现虚拟节点映射到实际物理节点, 虚拟链路映射到实际物理链路.

2) 量子密钥分发光网络层 (实际物理层) 主要由量子的“QKD 网络层”和经典的“弹性光网络层”组成. QKD 网络层产生密钥, 并存储在量子密钥池[15]中, 即每个可信中继将密钥生成并存储在量子密钥池中, 当进行密钥中继时可以直接调用, 避免时延等因素影响而造成密钥率不足的情况, 从而实现对数据的加密; 弹性光网络层用于提供带宽资源, 完成数据的传输. 在本文的虚拟业务映射模型中, 量子信道和数据传输信道共享弹性光网络的光纤资源, 其中量子信道由独立的光纤实现, 或者可以与完成 QKD 所需的同步信道和协商信道等通过波分复用的方式共享光纤中的频谱带宽资源, 该同传方式对密钥率损耗的影响较小. 然而, 当量子信道与数据传输信道在单根光纤中同传时, 受高速数据传输的影响, 不同协议的密钥率损耗可能不同. 本工作主要基于前一种同传方式开展, 不对密钥与数据同传的相互影响进行具体讨论. 虚拟业务的数据传输信道需要占用大量的带宽资源, 而其安全需求需要通过密钥资源来满足, 量子信道的主要功能是实现 QKD 以提供密钥资源. 量子信道和数据传输信道共享弹性光网络的光纤资源, 其中量子信道由独立的光纤实现. 本文中所有的量子节点均设为可信节点, 并且在量子节点之间等距放置可信中继, 进而实现密钥的远程传输.

考虑到地域的关系, 虚拟节点无法随意地映射到任意一个物理节点上, 可映射到的物理节点范围受地理位置限制, 必须对每个虚拟节点可以映射到的物理节点进行划分. 例如, 在图 3 中, 令虚拟节点 A 随机出现在一个位置, 譬如出现在物理节点 $A1$ 附近, 通过计算距离发现, $A1$, $A2$ 这两个物理节点最靠近虚拟节点 A, 其他物理节点距离虚拟节点 A 的空间位置太远, 不适合作为映射对象, 那么, A 的可映射范围即集合$\{A1, A2\}$.

3.2 考虑实际物理条件的可映射范围求解算法

根据 3.1 节中介绍的虚拟业务映射模型, 可以知道主要的映射就是将虚拟业务层映射到量子密钥分发光网络层, 即 $F\left(G^{\mathrm{v}}\right): G^{\mathrm{v}} \rightarrow G^{\mathrm{p}}$. 在虚拟业务中, 每条虚拟链路都有一对源宿节点. 在现有的虚拟节点可映射范围求解过程中, 都是随机的[6]. 这是不合理的, 因此考虑到地理位置这一限制条件, 对每个虚拟节点的可映射范围进行合理的限制, 具体的算法在表 1 列出.

在得到每个虚拟节点 v_i^{v} 对应的可以映射的物理节点的范围 D_i^{v} 之后, 将源宿节点可映射物理节点范围进行两两组合. 这样就可得到源宿虚拟节点映射的源宿物理节点集合 CMPNPS_{ij} (candidate mapping physical node pair set, CMPNPS). 这个集合中的元素 (一对源宿物理节点), 代表一种可能的映射.

表 1 虚拟节点可映射范围求解算法

Table 1. Mapping range solving algorithm for the virtual nodes.

输入	虚拟节点 v_i^{v}, 物理节点 v_i^{p}, 物理网络 $G^{\mathrm{p}}(V^{\mathrm{p}}, L^{\mathrm{p}}, BW^{\mathrm{p}}, K^{\mathrm{p}})$
输出	虚拟节点 v_i^{v} 可映射的物理节点范围 D_i^{v}
1	For 每个虚拟节点 v_i^{v} do
2	随机生成一个相应的物理节点 v_i^{p}
3	End for
4	For 每个物理节点 v_i^{p} do
5	根据USNET网络拓扑图得出与每个物理节点直接相连的节点
6	将物理节点 v_i^{p} 和与其直接相连的节点, 记为 D_i^{v}
7	End for
8	每个虚拟节点 v_i^{v} 可映射的物理节点范围为 D_i^{v}

3.3 虚拟业务映射算法

基于第 3.2 节给出的基于距离的可映射范围求解算法, 构建了符合实际物理条件的映射模型, 并将所构建的 QKD 模型融入在其中. 我们构建的虚拟业务映射算法可以分为 4 个部分: 虚拟链路排序, 映射范围求解, 节点映射+密钥中继路径, 数据传输路径.

1) 虚拟链路排序

为了满足一些对密钥和带宽高需求的虚拟业务, 给虚拟链路引入评估值:

$$\mathrm{VLSE}_{ij}=\frac{bw_{ij}^{v}}{\sum_{i=1}^{m}\sum_{j=1}^{n}bw_{ij}^{v}}+\frac{k_{ij}^{v}}{\sum_{i=1}^{m}\sum_{j=1}^{n}k_{ij}^{v}}. \tag{10}$$

(10) 式中, VLSE_{ij} (virtual link sequence evaluation, VLSE) 用于表示对虚拟链路 l_{ij}^{v} 的评估值, 等号右边第一项表示虚拟链路 l_{ij}^{v} 的带宽需求除以所有虚拟链路的总带宽需求, 第二项表示虚拟链路 l_{ij}^{v} 的密钥需求除以所有虚拟链路的总密钥需求, 也就是对每条虚拟链路上的带宽需求和密钥需求做了归一化处理.

2) 映射范围求解

考虑到地理位置的约束, 对每个虚拟节点可映射范围进行一定的限制. 通过表 1 中所介绍的虚拟节点可映射范围求解算法, 可以求得每个虚拟节点到可映射的物理节点范围, 该范围为随机对应的一个物理节点以及与其直接相连的其他物理节点.

3) 节点映射+密钥中继路径

对可映射物理节点集合 CMPNPS_{ij} 中的每个源宿物理节点组合采用 KSP 算法得到 k 条路径, N 个组合就得到 $N{\cdot}k$ 条路径. 然后以链路密钥评估 PKE (path key evaluation, PKE) 为评估标准对 $N{\cdot}k$ 条路径进行评估, 选取 PKE 最大的那条路径为密钥中继路径, 并将该路径两端的物理节点与虚拟节点确定映射关系. 评估指标 PKE 的定义为

$$\mathrm{PKE}=\frac{\mathrm{key}_{\min}-\mathrm{key}_{\mathrm{demand}}}{\mathrm{hops}}. \tag{11}$$

在两个物理节点之间通常包含多条物理链路, 每条物理链路上包含了多个密钥池, 链路的密钥提供能力有链路上最小的密钥池来决定. 将链路上最小密钥池的密钥量记为 $\mathrm{key}_{\min}$, 虚拟链路的密钥需求记为 $\mathrm{key}_{\mathrm{demand}}$. 通过计算出大于 $\mathrm{key}_{\mathrm{demand}}$ 路径的 PKE 进行排序, 将 PKE 最大的那条路径设置为密钥中继路径. 如果不存在密钥量大于密钥需求路径, 则业务阻塞. 确定了密钥中继路径之后, 该路径两端的物理节点就被选为虚拟链路两端源宿虚拟节点所映射到的物理节点.

4) 数据传输路径

对于整个业务, 虚拟节点和密钥中继路径映射都完成之后, 就剩下数据中继路径的映射. 数据中继路径的映射流程是: 首先在以确定的源宿物理节点之间采用 k 条最短路径算法 (k-shortest pathes, KSP) 选出前 k 条路径[16], 然后运用首次命中算法 (first fit, FF) 依次为 k 条路径分配频谱. 一旦有一条路径上的频谱资源满足虚拟业务的频谱需求, 就将那条路径确定为数据中继路径. 如果不存在这样的路径使频谱资源满足虚拟业务的频谱需求, 那么整个业务阻塞.

以上就是一个完整的虚拟链路映射过程, 只有当所有的虚拟链路都映射成功之后, 整个虚拟业务才算映射成功.

4 仿真结果与分析

4.1 虚拟节点可映射范围

根据表 1 所描述的虚拟节点可映射范围求解算法, 对图 1 的 USNET 拓扑图进行求解, 通过软件 MATLAB 求解后能得出每个虚拟节点可映射的物理节点范围, 每个虚拟节点可映射的物理节点范围集合由随机产生的一个物理节点以及与该物理节点直接相连的物理节点组成, 具体见表 2.

表 2 每个虚拟节点可映射的物理节点范围

Table 2. The range of physical nodes that can be mapped to each virtual node.

随机生成物理节点	可映射物理节点范围	随机生成物理节点	可映射物理节点范围	随机生成物理节点	可映射物理节点范围
1	1, 2, 6	9	9, 6, 7, 10, 11, 12	17	17, 13, 16, 18, 22, 23
2	2, 1, 3, 6	10	10, 8, 9, 13, 14	18	18, 14, 17, 24
3	3, 2, 4, 5, 7	11	11, 6, 9, 12, 15, 19	19	19, 11, 20
4	4, 3, 5, 7	12	12, 9, 11, 13, 16	20	20, 15, 19, 21
5	5, 3, 4, 8	13	13, 10, 12, 14, 17	21	21, 16, 20, 22
6	6, 1, 2, 7, 9, 11	14	14, 10, 13, 18	22	22, 16, 17, 21, 23
7	7, 3, 4, 6, 8, 9	15	15, 11, 16, 20	23	23, 17, 22, 24
8	8, 5, 7, 10	16	16, 12, 15, 17, 21, 22	24	24, 18, 23

随机产生的物理节点即虚拟业务所在的空间位置, 这样设定, 相当于让虚拟业务在物理空间上接近随机均匀分布. 对于实际的情况, 可以根据人口密集程度以及繁荣程度, 合理设定分布函数.

使用表 1 中所描述的算法求解虚拟节点可映射范围, 假设有 100000 条虚拟业务动态到达, 虚拟节点在一个虚拟业务中只能映射到一个物理节点上. 本模型设定虚拟业务为均匀分布, 即对于 24 个物理节点来说, 虚拟节点映射到每个物理节点上的概率一致. 通过软件仿真, 可以发现虚拟节点映射到每个物理节点上的次数基本一致, 基本呈现均匀分布的状态, 如图 4 所示.

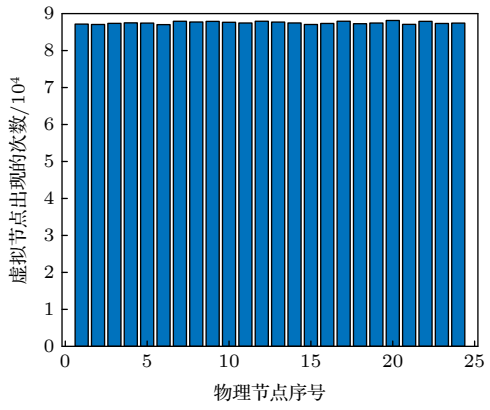

图 4 虚拟节点映射到每个物理节点上的次数

Fig. 4. The number of times the virtual nodes are mapped to each physical node.

均匀分布是模型设定的, 然而在具体的实际应用中, 由于人口密集程度以及繁荣程度等因素, 分布情况不一定接近均匀分布, 这时候就可以通过改变分布函数来趋近于实际情况, 在代码中, 虚拟业务映射到 24 个物理节点的概率是可调的, 只需要在代码中改变权重因子即可实现对 24 个物理节点被映射到的概率进行调节.

4.2 采用不同协议的性价比对比

本文采用三强度诱骗态条件下的 BB84 协议、MDI 协议和 TF 协议, 根据 BB84 协议 [12]、MDI 协议 [13] 和 TF 协议 [14] 的密钥产生速率, 并对诱骗态以及信号态的强度进行了全局优化, 通过全局优化, 可以得到在不同距离下信号态强度和诱骗态强度的最优参数. 例如, 当采用 BB84 协议时, 在传输距离为 100 km 的情况下, 通过全局优化后密钥生成速率的条件是信号态强度为 0.70、诱骗态强度为 0.05. 仿真中使用的是局部搜索算法 [17], 仿真参数见表 3, 其中考虑到 TF 协议的实际系统稳定性比较差, 据目前已报道实验数据水平 [18,19], 合理设定 TF 系统的本底误码均为 BB84 和 MDI 同等情况下的 4 倍.

表 3 仿真参数

Table 3. Simulation parameters.

$\alpha/(\mathrm{dB\cdot km^{-1}})$	e_{detector}	Y_0	η_{Bob}	f/MHz
0.2	0.015	10^{-8}	0.5	2

通过仿真得到 3 种协议密钥产生速率随距离变化曲线图, 如图 5 所示. 在得到 3 种协议密钥产生速率随距离的变化曲线后, 将其代入性价比 CP 公式 ((1) 式) 中进行求解. 为简单起见, 不考虑不同协议的安全性等级和有限长效应, 仅将密钥率作为主要评价指标. 其次, 考虑到搭建实际 QKD 系统时不同协议所需要消耗的资源大小不同, 将 BB84 协议、MDI 协议和 TF 协议接收机 (发送机) 的成本设为 1:2:4. 然后仿真出采用 3 种不同协议时, 不同长度物理链路长度下放置可信中继的最佳数量, 并得到合理放置中继时的密钥量, 具体仿真结果图如图 6 所示 (为简化计算, 此处忽略了有限长效应).

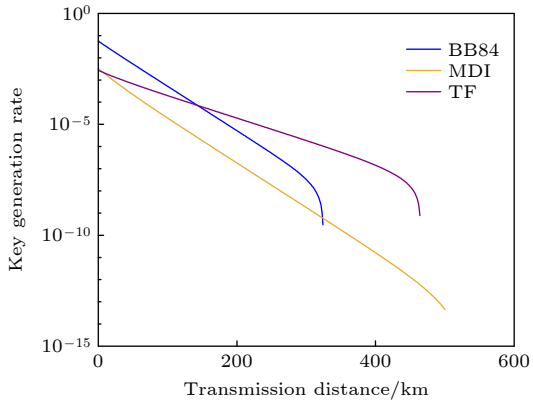

图 5 3 种协议密钥产生速率随距离变化曲线图

Fig. 5. Plot of key generation rate of three protocols versus distance.

图 6 展现了不同长度的物理链路采用不同协议时, 物理链路上放置中继数量与性价比关系图. 由图 6 可知, BB84 协议的优势十分明显, 性价比是其他两个协议的几十倍, 然后 MDI 协议比 TF 协议略好一些. 最开始定义性价比公式时, 是预期 BB84 协议在短距离时性价比最高, MDI 协议在较长距离下性价比最高, TF 协议在最长距离下性价比最高. 但是只从图 6 来看, 无法准确分辨出在不同中继距离下的最佳协议. 然后根据性价比 (2) 式仿真得出了 3 种协议在相同长度链路上放置中继间隔距离和性价比的对比图, 具体见图 7.

如图 7 所示, 链路长度 $L_{\rm s}$ 取 1000 km, 中继间距在 34 km 以内时, BB84 协议性价比最高, MDI 协议次之, TF 协议最低; 中继间距在 34—205 km 时, BB84 协议性价比最高, TF 协议次之, MDI 协议最低; 结合图 7(b), 在中继间隔大于 205 km 之后, TF 协议的性价比超越了其他两个协议. 中继距离越短, 放置中继个数越多, 那么链路上的安全性也会随之降低. 因此, 如果不考虑链路安全性等级划分的话, 在较短的中继间隔上 BB84协议最好. 不过, 如果实际网络中限需要较高的安全性, 设置中继间隔大于 200 km 时, 采取 TF 协议的性价比大于其他两种协议.

结合图 5 所示 3 种协议的“密钥产生速率随传输距离变化”曲线图, 可知 BB84 协议在 100 km 以内的密钥量比另外两种协议要高至少 1 个数量级; 在传输距离只有几千米时, MDI 协议与 TF 协议有一个交点, 由于两者成本不同, 故性价比曲线的交点发生了移动; 超过 200 km 之后, TF 协议一直处在优势地位. 该结果对于今后开展大规模量子通信网络实际应用具有重要的指导价值.

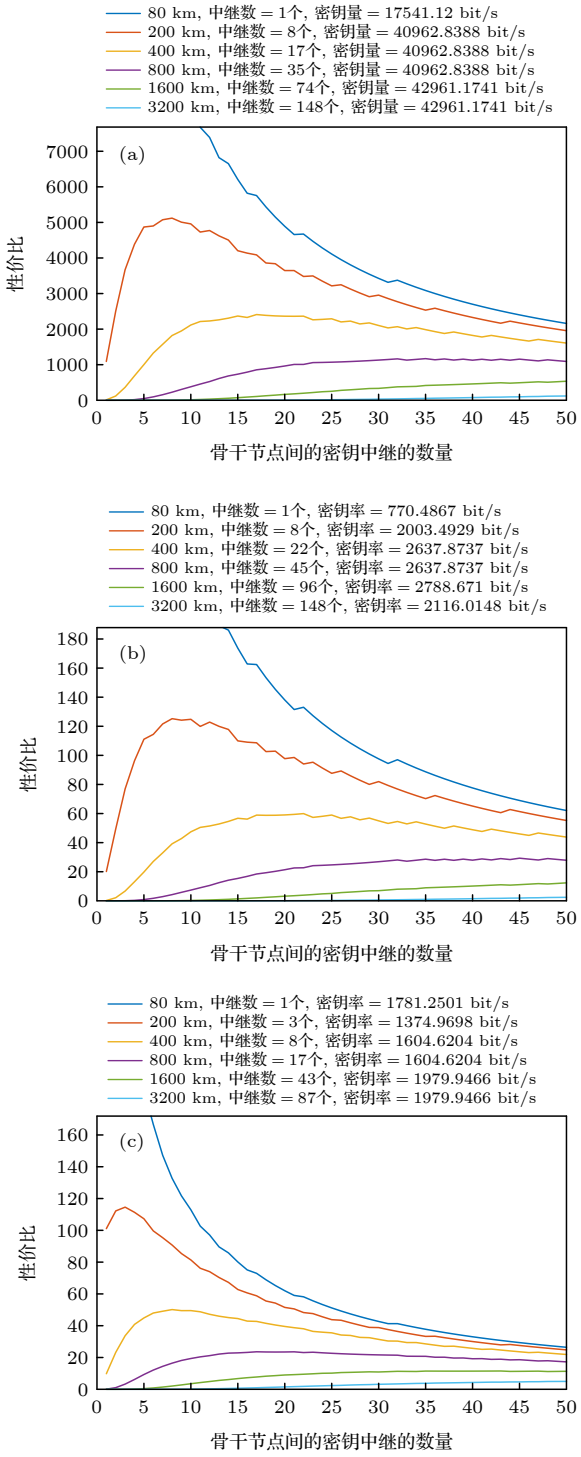

图 6 (a) 采用 BB84 协议时不同距离下中继数量与性价比关系图; (b) 采用 MDI 协议时不同距离下中继数量与性价比关系图; (c) 采用 TF 协议时不同距离下中继数量与性价比关系图

Fig. 6. (a) Plot of relay number and cost performance at different distances with BB84 protocol; (b) plot of relay number and cost performance at different distances with measurement-device-independent protocol; (c) plot of relay number and cost performance at different distances with two-field protocol.

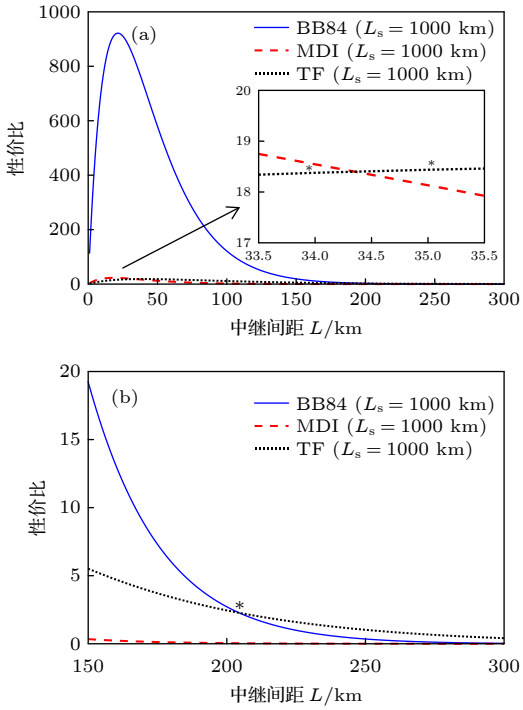

图 7 (a) 中继距离 (0—300 km) 时性价比关系对比图; (b) 中继距离 (150—300 km) 时性价比关系对比图

Fig. 7. (a) Cost performance-price ratio for relay distance (0–300 km); (b) cost performance-price ratio for relay distance (150–300 km).

本文中, 不考虑链路安全性等级划分, 以性价比最高为目标放置中继, 最终发现对于 USNET 拓扑中任何链路长度 L_s, BB84 协议性价比的最高值在 3 个协议中始终独占鳌头, 相应的最佳中继间距也都在 20—30 km, 而相近的传输距离导致密钥产生速率也相近, 从而使得每条链路上的密钥量大小相近, 这对于业务需求均匀分布的网络来说是一大裨益. 但是在实际应用时, 可以根据具体网络的需求分布调节密钥产生速率, 即减少密钥需求低的链路上的中继数, 从而减少不必要的资源浪费.

综上, 本文中物理节点之间采用 BB84 协议效果最佳. 后文物理节点之间也都是采用 BB84 协议进行计算.

4.3 阻塞率和密钥利用率

结合 4.1 节的可映射范围求解和 4.2 节的 QKD 协议选取, 采用 3.3 节的映射思路来评估本文映射模型, 仍然采用图 1 所示的 24 节点的 USNET 拓扑进行软件仿真. 仿真参数如表 4 所示, 对于经典信道 (数据传输信道), 每条链路的最大频谱数量都设定为 386 个频谱, 带宽需求设为随机均匀分布; 对于量子信道, 密钥资源的生成率与所采用的协议以及中继数量相关, 密钥需求也是采用随机均匀分布. 100000 条虚拟业务动态到达, KSP 算法中的 k 值设为 3.

对虚拟业务映射算法的评估指标主要有阻塞率和密钥利用率. 阻塞率 BP(blocking probability, BP) 为被阻塞的虚拟业务的数量除以虚拟业务的总量; 密钥利用率 KRU(key resource utilization, KRU) 为所有没有被阻塞的虚拟业务密钥需求总量除以物理网络中生成的密钥总量.

图 8 展示了物理节点之间分别使用 3 种协议时业务阻塞率随业务到达速率变化曲线. 从图 8 来看, 随着业务到达速率加快, 阻塞率 BP 会逐渐增大. 当业务到达速率增大时, 一定时间内的虚拟业务的密钥需求总量增大, 而密钥产生速率是固定的. 所以当业务到达速率增大到某个值之后, 就会导致密钥供不应求, 阻塞率明显增大.

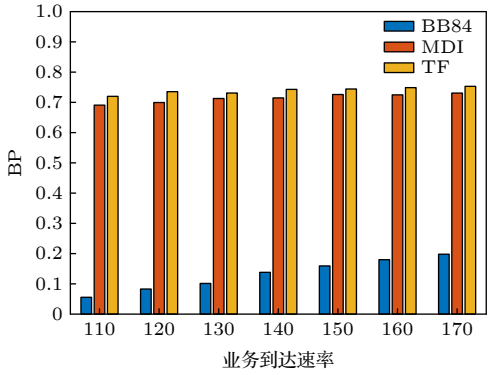

图 8 业务阻塞率随业务到达速率变化曲线

Fig. 8. Curve of traffic blocking probability versus traffic arrival rate.

图 9 展示了密钥利用率随业务到达速率的变化曲线. 从图中可以发现, 当业务到达速率增大时, 密钥利用率 KRU 也会有一定的增大. 业务到达速

表 4 仿真参数

Table 4. Simulation parameters.

名称	值	名称	值
物理节点数量	24个	物理链路数量	43条
链路频谱数量	386个	每条虚拟链路带宽需求	{5, 6, 7, 8, 9}个
虚拟节点数量	{2, 3, 4}个	每条虚拟链路密钥需求	{2000, 2400, 2800, 3200, 3600}bit

率即单位时间内到达的虚拟业务的密钥需求量. 当业务到达率增大时, 密钥的利用率缓慢增大, 而密钥产生速率是固定的, 说明密钥利用量增大缓慢, 说明有更多的阻塞, 与图 8 相吻合.

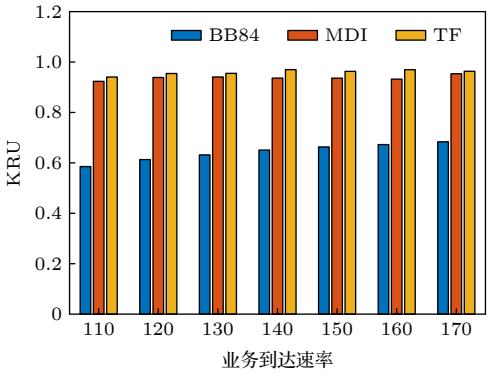

图 9 密钥利用率随业务到达速率变化曲线

Fig. 9. Curve of the key resource utilization versus traffic arrival rate.

从图 8 和图 9 中可以看出, BB84 协议的阻塞率最低, 同时密钥利用率也最低; MDI 和 TF 协议的密钥利用率虽然很高, 但是阻塞率也非常高. 结合 3 种协议的性价比曲线图 6, 可以看到 BB84协议的密钥生成量很高, 而其他两种协议密钥量生成量较少. 在相同的密钥需求情况下, 密钥生成越多, 那么就能满足业务的需求, 阻塞率会降低, 同时密钥量会有些许剩余.

从理论上预估, 当业务到达速率足够大时, 本映射方案应该会让密钥利用率 KRU 趋向于理想值 1. 但是从图 9 中发现, 物理节点之间采用 BB84 协议时, KRU 的发展趋势距离 1 还很遥远. 于是, 为了寻找 KRU 的临界值, 设置业务到达率大小为 600 w/s (w 为单位业务量) 时, KRU≈0.8; 业务到达率为 5000 w/s 时, KRU≈0.95. 但此时的 BP 已经超过 0.5, 没有太大意义. 为了搞清楚 KRU 受限制的原因, 对一定的业务到达速率下物理链路上每条虚拟链路的密钥利用率进行了考察. 在图 10 中, 业务到达率设为 170 w/s, 也就是 1 s 内有 170 个业务同时到达.

观察图 10 可以发现, 物理节点 1, 2, 23, 24 等节点所在路径的密钥利用率非常低. 结合网络拓扑图 (图 1) 可以发现, 物理节点 1, 2, 23, 24 等节点处在网络的边缘位置, 所以有些虚拟业务的通信路径几乎不会经过它们. 而处在网络中心位置 (或者说分支多的) 的物理点, 它们的密钥利用率则非常高, 因为大多数虚拟业务的通信需要经过它们. 相同地, 阻塞主要也是由中间部分这些节点导致. 从图 10 得出网络边缘的节点是不活跃区域, 密钥利用率较低, 因而提高网络主干处的密钥产生速率, 降低网络边缘处的密钥产生速率, 对于提高 KRU 并降低阻塞率 BP 有指导性作用.

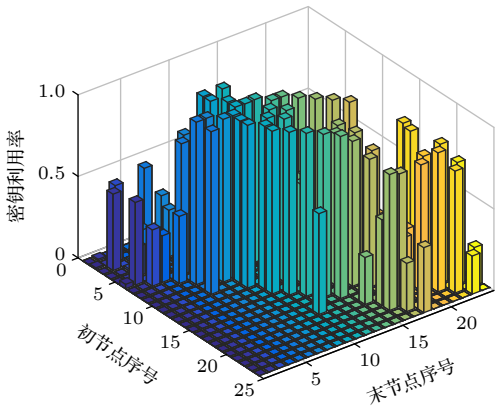

图 10 每条物理链路的密钥利用率

Fig. 10. Key utilization for each physical link.

总而言之, 对于一个具体的网络, 查看每条链路的密钥利用率, 密钥利用率较低的物理节点可以降低其密钥产生速率, 例如减少中继数以减少资金损耗, 来减少不必要的浪费, 从而提高资源利用率.

5 结 论

本文主要结合实际物理条件, 研究了动态虚拟业务在量子密钥分发光网络中的映射问题. 首先给出本模型中 QKD 协议的性能评估指标——性价比, 并通过理论分析以及数值模拟对 BB84, MDI, TF 这三类协议的性价比进行了比较以及原因分析, 得出当中继距离在 100 km 以内时, BB84协议具有最佳性价比, 于是基于此类协议进一步研究, 给出网络中密钥的产生速率; 接着综合考虑带宽和密钥资源, 建立了虚拟业务在量子密钥分发光网络中的映射模型, 并结合地理条件限制, 给出了虚拟节点映射范围求解算法, 此外, 让虚拟业务出现的位置遵循概率分布, 对实际应用具有很好的启示作用; 最后, 对本文的映射算法进行软件仿真, 通过整个网络的阻塞率和密钥资源利用率对网络性能进行评估, 接着通过三维图直观展示每条链路的性能, 进而分析得出利用率有限的主要原因, 并提出了改进的方案, 对实际网络的应用具有很好的指导

性意义.

在实用化量子密钥分发光网络的实际应用中, 对网络运行实时性造成影响的因素主要包含物理层时延和网络层时延. 物理层时延主要是由 QKD 密钥的生成、数据后处理等产生. 网络层时延涉及资源优化算法运行和实施的时延、控制时延等. 在本文构建的虚拟业务映射模型中, 每条物理链路上的密钥生成速率由每对相邻可信中继之间密钥生成速率的最低值决定. 当部分中继之间受时延影响导致密钥不足时, 容易造成密钥率损失. 而当网络层时延对虚拟业务映射产生较大影响时, 容易造成业务阻塞.

为了减少密钥率损失, 在本文的模型中采用了量子密钥池[15]的思想, 即每个可信中继将密钥生成并存储在量子密钥池中, 当进行密钥中继时可以直接调用, 避免时延等因素影响而造成密钥率不足的情况. 同时, 本文假设网络层时延较低, 从而对虚拟业务映射的影响很小. 此外, 本文重点关注基于性价比对资源进行分配管理以及虚拟业务在量子密钥分发光网络中的映射模型和相关算法, 在后续的工作中将对时延等因素造成的密钥率损失以及各种时延对资源优化配置的影响开展进一步研究.

参考文献

[1] Lin R P, Luo S, Zhou J W, Wang S, Cai A L, Zhong W D, Moshe Z 2018 *J. Lightwave Technol.* **36** 3551

[2] Jiang H H, Wang Y X, Gong L, Zhu Z Q 2015 *J. Opt. Commun. Netw.* **7** 1160

[3] Gong L, Zhu Z 2013 *J. Lightwave Technol.* **32** 450

[4] Jarray A, Karmouch A 2014 *IEEE/ACM Trans. Netw.* **23** 1012

[5] Botero J F, Hesselbach X, Fischer A, Hermann D M 2012 *Telecommun. Syst.* **51** 273

[6] Wang Y 2020 *M. S. Dessertation* (Beijing: Beijing University of Posts and Telecommunications) (in Chinese) [王妍 2020 硕士学位论文(北京: 北京邮电大学)]

[7] Zeng P, Zhou H Y, Wu W J, Ma X F 2022 *Nat. Commun.* **13** 1

[8] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2019 *Phys. Rev. A* **99** 062316

[9] Mao Y Q, Wang B X, Zhao C X, Wang G Q, Wang R C, Wang H H, Zhou F, Nie J M, Chen Q, Zhao Y, Zhang Q, Zhang J, Chen T Y, Pan J W 2018 *Opt. Express* **26** 6010

[10] Wang P H, Zhang N, Xiao M M 2019 *Comput. Eng. Appl.* **55** 106 (in Chinese) [王鹏辉, 张宁, 肖明明 2019 计算机工程与应用 **55** 106]

[11] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325

[12] Zhu F D 2016 *M. S. Thesis* (Nanjing: Nanjing University of Posts and Telecommunications) (in Chinese) [朱凤丹 2016 硕士学位论文 (南京: 南京邮电大学)]

[13] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324

[14] Xu H, Yu Z W, Jiang C, Hu X L, Wang X B 2020 *Phys. Rev. A* **101** 042330

[15] Cao Y, Zhao Y L, Wang Q, Zhang J, Ng S X, Hanzo L 2022 *IEEE Commun. Surv. Tut.* **24** 839

[16] Zhao L F, Huang Y W 2017 *Comput. Technol. Dev.* **27** 98 (in Chinese) [赵礼峰, 黄奕雯 2017 计算机技术与发展 **27** 98]

[17] Xu F, Xu H, Lo H K 2014 *Phys. Rev. A.* **89** 052333

[18] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao M Q, Huang M Q, Zhang W J, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X B, Pan J W 2016 *Phys. Rev. Lett.* **117** 190501

[19] Liu Y, Yu Z W, Zhang W J, Guan J Y, Chen J P, Zhang C, Hu X L, Li H, Jiang C, Lin J, Chen T Y, You L X, Wang Z, Wang X B, Zhang Q, Pan J W 2019 *Phys. Rev. Lett.* **123** 100505

Optimal resource allocation in practical quantum key distribution optical networks*

Zhu Jia-Li [1)2)3)] Cao Yuan [1)2)3)] Zhang Chun-Hui [1)2)3)] Wang Qin [1)2)3)†]

1) (*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

2) (*Key Laboratory of Broadband Wireless Communication and Sensor Network of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

3) (*The National Engineering Research Center for Communications and Networks, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 21 August 2022; revised manuscript received 12 October 2022)

Abstract

In the application research of large-scale quantum communication network, one generally realizes resource allocation by constructing virtual service network and mapping it to actual physical space. In this mapping process, some assumptions are often made to simplify the model. For example, the key resource in the physical topology is assumed to be a fixed value, that is, the actual physical conditions and the performance differences of key supply caused by different protocols are ignored. This assumption may lead the network to fail to run appropriately in practical applications. In order to solve the above problems, from the perspective of link mapping, this paper proposes an improved virtual service mapping model and virtual service mapping algorithm with the quantum key distribution optical network as the underlying network, which makes it closer to the actual application scenario. On the one hand, by increasing the constraints of geographical location, the range from virtual nodes to the mappable physical nodes is reasonably restricted. On the other hand, from the perspective of hardware cost and actual key generation rate, the cost performance evaluation index is proposed to allocate and manage resources. In addition, by combining three mainstream quantum key distribution protocols (BB84, measurement-device-independent, and twin-field), we construct a universal virtual service mapping model in the quantum key distribution optical network, and realize the recommendation of the optimal protocol and the optimal allocation and management of resources.

Keywords: optimal allocation of resources, quantum key distribution, virtual service embedding, cost performance

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.72.20221661

* Project supported by the National Key R&D Program of China (Grant No. 2018 YFA0306400), the National Natural Science Foundation of China (Grant Nos. 12074194, 12104240, 62201276), the Industry Foresight and Key Core Technology Project of Key R&D Plan of Jiangsu Province, China (Grant No. BE2022071), the Jiangsu Natural Science Foundation, China (Grant Nos. BK20192001, BK20210582), the Natural Science Research Project of Jiangsu Higher Education Institutions, China (Grant No. 22KJB510007), and the Natural Science Foundation of Nanjing University of Posts and Telecommunications, China (Grant No. NY220123).

† Corresponding author. E-mail: qinw@njupt.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

实用化量子密钥分发光网络中的资源优化配置

朱佳莉　曹原　张春辉　王琴

Optimal resource allocation in practical quantum key distribution optical networks

Zhu Jia-Li　Cao Yuan　Zhang Chun-Hui　Wang Qin

引用信息 Citation: Acta Physica Sinica, 72, 020301 (2023)　DOI: 10.7498/aps.72.20221661
在线阅读 View online: https://doi.org/10.7498/aps.72.20221661
当期内容 View table of contents: http://wulixb.iphy.ac.cn
