



专题：量子保密通信技术与应用

量子保密通信网络骨干链路流量规划

原磊, 赵梅生

(山东量子科学技术研究院有限公司, 山东 济南 250101)

摘要: 量子保密通信网络是一种新兴的安全网络。如何通过合理的流量规划方法提升量子保密通信网络骨干链路的带宽利用率、提升网络性价比是一个新问题。分析了量子保密通信网络流量规划的特殊性, 给出了一种流量规划模型, 可以实现下列 3 个方面的目标: 在确定网络骨干链路密钥分发带宽的情况下, 可以实现用户广域加密通信带宽的规划; 借助路由规划可以提升用户广域加密通信带宽和量子链路密钥分发带宽的利用率; 可以实现对网络瓶颈量子链路密钥分发带宽的合理调整。最后, 通过数值模拟示例演示了本文所提出的流量规划方法的应用。

关键词: 量子保密通信网络; 流量规划; 骨干链路

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018255

Traffic planning of backbone link of quantum secure communication network

YUAN Lei, ZHAO Meisheng

Shandong Quantum Science and Technology Research Institute Co., Ltd., Jinan 250101, China

Abstract: Quantum secure communication network is a new kind of security network. It is a new problem that how to improve the bandwidth utilization ratio of the backbone link of quantum secure communication network and the network performance-price ratio by reasonable traffic planning method. The particularity of traffic planning in the quantum secure communication network was analyzed, and a traffic planning model was given. Based on this model, the user wide area encrypted communication bandwidth could be planned in the case of determining the key distribution bandwidth of the backbone link. At the same time, the model could be used to adjust the bandwidth of key distribution in network bottleneck links and improve the network performance. Finally, the application of the proposed flow planning method was demonstrated by numerical simulation.

Key words: quantum secure communication network, traffic planning, backbone link

1 引言

量子保密通信网络是一种新兴的安全网络。2017 年全球首个远距离量子保密通信骨干网“京

沪干线”正式开通^[1], 量子保密通信网络的实用规模由城域网扩展为广域网。在今后的很长一段时期内会不断出现新的广域网络, 现有的广域网也会不断扩展, 覆盖更多的经典互联网区

收稿日期: 2018-08-06; 修回日期: 2018-09-10

域和用户,直到扩展为全球互联的量子保密通信广域网络^[2]。

量子保密通信网络骨干链路是指广域量子保密通信网络中所有连接相邻城域网的量子链路,用于生成相邻城域网之间的共享量子密钥数据。量子保密通信网络骨干链路流量规划是指如何根据当前网络骨干链路的量子密钥生成带宽合理规划用户节点的量子密钥加密通信带宽,以提升骨干链路的带宽利用率。量子保密通信网络骨干链路流量规划是新的广域网络和扩展广域网络在网络规划阶段所必须要考虑的问题。

在网络规划阶段,网络设计需要确定用户节点的加密通信带宽。经典互联网络的用户平均带宽主要是根据用户的入户网线的频宽确定的。而量子保密通信网络的用户平均加密通信带宽由整个网络能够为用户提供的共享量子密钥量和量子密钥重复使用的次数(或密钥扩展的倍数)决定。前者主要取决于广域骨干链路的密钥生成带宽,而后者(量子密钥重复使用的次数或密钥扩展的倍数)取决于通信数据所要求的安全等级。如何根据广域量子链路的密钥分发带宽通过流量规划获得用户的广域加密通信带宽,这是一个新的问题。

通过密钥中继获得共享密钥,然后使用共享密钥进行加密通信,是当前用户节点之间进行量子密钥加密通信的主要方式^[3]。城域网之间距离相对较远,为增加用户节点广域加密通信的实时性,需要在相互通信的城域网之间预置共享密钥。相邻城域网之间的骨干链路生成的共享密钥,一部分用于相邻城域网之间加密通信的密钥中继,另一部分用于城域网之间的密钥中继,如何确定两者之间的比例也是量子保密通信网络骨干链路流量规划所必须考虑的问题。

经典网络中,瓶颈路径的存在一直是影响网络性能的一个重要问题^[4],发现和调整瓶颈路径能够提升网络性能。广域量子保密通信网络中同

样存在瓶颈量子链路,其密钥分发速度较低,限制了用户节点广域加密通信带宽的提升。发现和合理调整瓶颈骨干量子链路密钥分发带宽,也是流量规划的任务之一。

2 流量规划模型

流量规划用于网络搭建和使用之前,属于前期网络规划的一个方面,主要解决网络应用初期每条量子链路的密钥使用比例规划和用户节点广域加密通信带宽规划两个问题。基于下述模型假设进行流量规划。

模型假设:用户节点为加密通信无差别节点,即任意两个不同城域网的用户节点进行广域通信的概率相等。

2.1 量子链路的密钥使用比例规划

引理 1 假设所有广域网络用户节点为加密通信无差别节点。 G 表示所有广域网中城域网的集合, L 为任意一条量子链路,其两端的相邻城域网为 U_L 和 V_L ,其用户数量分别为 u_L 和 v_L ,如果 G 中任意两个城域网 U 和 V 进行广域通信密钥中继时使用量子链路 L 生成的共享密钥,则表示为 $L(U, V)=1$ 。如果量子链路 L 的带宽利用率为 100%,则城域网 U_L 和 V_L 之间进行广域通信所消耗的量子链路 L 生成的共享密钥与其他城域网之间(包括 U_L 与其他城域网之间和 V_L 与其他城域网之间)进行广域通信所消耗的量子链路 L 生成的共享密钥的比例为: $u_L v_L / \sum_{U \in G, V \in G}^{L(U, V)=1} uv$,其中 u 、 v 分别为城域网 U 和 V 的用户数量。

证明:假设当量子链路 L 的带宽利用率为 100%时,单位时间(每秒)任意两个不同城域网的用户节点进行广域通信的平均概率为 p ,任意两个不同城域网的用户节点之间广域通信消耗的平均密钥量为 q ,则城域网 U 和 V 在单位时间平均消耗的密钥量为 $q \times u \times v \times p$ 。所有使用量子链路 L 生成的共享量子密钥进行加密通信的城域网在单位时间消耗的平均密钥量 W 为:



$$W = \sum_{U \in G, V \in G}^{L(U, V)=1} (quvp) = pq \sum_{U \in G, V \in G}^{L(U, V)=1} uv \quad (1)$$

根据密钥中继的特性，密钥中继在经过每段量子链路时，密钥消耗速度均相等，所以当量子链路 L 的带宽利用率为 100% 时， W 即量子链路 L 的密钥分发带宽。

城域网 U_L 和 V_L 在单位时间平均消耗的密钥量为 qu_Lv_Lp 。根据密钥中继的特性，故城域网 U_L 和 V_L 之间进行广域通信所消耗的量子链路 L 生成的共享密钥与其他城域网之间（包括 U_L 与其他城域网之间和 V_L 与其他城域网之间）进行广域通信所消耗的量子链路 L 生成的共享密钥的比例为 $qu_Lv_Lp / (pq \sum_{U \in G, V \in G}^{L(U, V)=1} uv) = u_Lv_L / \sum_{U \in G, V \in G}^{L(U, V)=1} uv$ 。

将城域网 U 和 V 的用户数量乘积 uv 称为城域网 U 和 V 的线路数量。同时将每条线路上用于用户广域加密通信在单位时间消耗的平均量子密钥量，称为线路平均带宽。任意一条量子链路 L ，假设其带宽利用率为 100%，将 L 的密钥生成带宽除以经过 L 的总的线路数量所得的值称为量子链路 L 的线路平均带宽。由式 (1) 可知，任意两个不同城域网的用户节点进行广域通信的平均概率 p 和两个不同城域网的用户节点之间广域通信消耗的平均密钥量 q 的乘积 pq 为量子链路 L 的线路平均带宽。

将任意两个不同城域网的用户节点之间广域通信消耗的平均密钥量 q ，称为用户平均带宽，表示网络用户在单位时间消耗的密钥量的均值。

在下述用户广域加密通信流量规划流程中，首先计算每条量子链路的线路平均带宽和用户平均带宽，然后根据量子密钥重复使用的次数（或密钥扩展的倍数）和用户每天平均广域加密通信时间，计算用户广域加密通信带宽。

根据引理 1，每条量子链路均可以在假设本链路量子密钥生成带宽利用率为 100% 的情况下，分配量子链路的使用比例，即用于本链路的相邻城域网之间密钥中继的量子密钥量与用于其他城域网之间密钥中继量子密钥量的比例。

2.2 用户广域加密通信流量规划

用户广域加密通信流量规划的目的是在网络规划期间预估用户节点的加密通信的平均带宽，首先需要考虑下述几个关键方面。

(1) 路由规划

最初的广域量子保密通信网络通常是一条单连通的骨干线路，上面接入若干城域网络，然后基于最初的骨干线路不断扩展为多连通的复杂广域网络。由于技术的发展和产品的进步，新扩张网络的量子链路密钥生成带宽会远远大于原有网络的量子链路密钥生成带宽。原有网络中处于网络中心位置的量子密钥分发带宽较小的量子链路往往会成为加密通信的瓶颈链路。这样就需要对城域网密钥中继的广域路由进行合理规划，在考虑路由成本的情况下，城域网之间密钥中继的广域路由需要尽量避开瓶颈量子链路（线路平均带宽较小的量子链路），以提升用户节点的全局广域加密通信带宽。

(2) 密钥扩展

量子加密技术要求采用一次一密的加密方式以达到无条件安全的安全级别。由于当前的量子密钥分发技术所限，量子密钥分发速度满足不了一个一次一密的加密需求。但考虑到当前密码学的进展，许多对称加密算法，比如 AES 算法，现在仍然是安全的加密算法，破解者只有在获得足够的数据后才能够获得一定的破解概率。按照密钥分析的结果，使用 AES 算法加密，量子密钥重复使用次数（或密钥扩展倍数）小于门限值，加密数据依然是相对安全的。

(3) 密钥缓存机制

为了增加密钥中继的实时性，广域量子密钥中继需要在城域网两两之间缓存共享密钥，由于当前密钥分发速度不大，这种缓存过程会一直存在，不论用户节点是否在进行广域加密通信，相对于用户的广域加密通信时间，密钥缓存机制相当于增加了量子链路的量子密钥分发的可用带

宽。因此这就需要预估用户节点每天的广域通信时间。

考虑到当前广域量子保密通信网络的发展进程,即广域量子保密通信网络还处于不断扩张阶段,给出适合当前广域量子保密通信网络的流量规划方法,用户广域加密通信带宽规划如图1所示,详述如下。

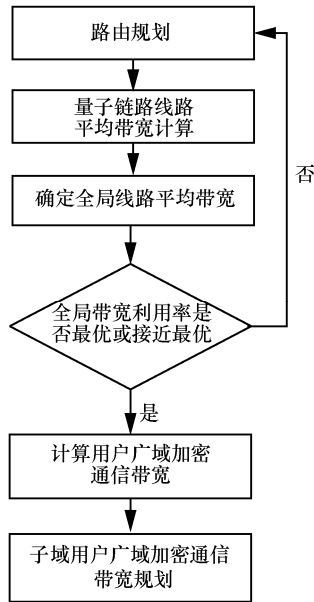


图1 用户广域加密通信带宽规划

步骤1 路由规划

本方法中只考虑单路径路由密钥中继。在广域路由中,瓶颈量子链路的线路平均带宽决定全局线路平均带宽。为了减少瓶颈链路的加密通信线路数量,增加瓶颈量子链路的线路平均带宽,在密钥中继成本差别不是太大的情况下,需要尽量选择不经瓶颈量子链路的密钥中继路由路径。

如图2所示,A、B、C、D、E为5个城域网节点,城域网节点D和E之间的量子链路为瓶颈量子链路,A到D密钥中继路径有两条:AED和ABCD。路径AED较短,密钥中继成本较低,但为了降低量子链路DE的负担,将A到D密钥中继路径规定为ABCD。

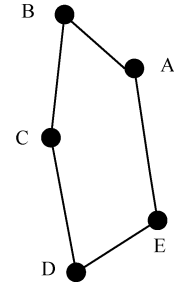


图2 路由规划

步骤2 计算量子链路的线路平均带宽

通过路由规划可以确定任意两个城域网之间的密钥中继路由路径,任意一条量子链路 L 可以根据其密钥生成带宽 W 和加密通信密钥中继线路数量 T_L 计算本量子链路的线路平均带宽 w_L ,计算式为:

$$w_L = W_L / \sum_{U \in G, V \in G}^{L(U,V)=1} uv = W_L / T_L \quad (2)$$

其中, $T_L = \sum_{U \in G, V \in G}^{L(U,V)=1} uv$ 为经过量子链路 L 的加密通信密钥中继线路数量,见式(1)的相关定义。

步骤3 确定全局线路平均带宽

将线路平均带宽最小的量子链路的线路平均带宽作为全局线路平均带宽。判断全局量子链路密钥生成带宽利用率是否最优或接近最优,如果不是,则转到步骤1,重新进行路由规划;如果是,则继续步骤4。

步骤4 计算用户节点广域加密通信带宽

首先计算用户平均带宽。预估用户节点每天的平均广域通信时长为 t_0 h。

整个网络所有的用户广域通信线路数量 L_n ,用户数量为 Q_u ,则每条线路平均每天的使用时间 t 为 $t=t_0/(2 \times L_n/Q_u)=Q_u \times t_0/L_n$ 。则:

$$p=t/t_d=Q_u \times t_0/(2 \times L_n \times t_d) \quad (4)$$

其中, t_d 为24h。

由式(1)和式(2)可得全局线路平均带宽 $w=pq$,故用户平均带宽计算式为:

$$q=w/p \quad (5)$$

同时考虑密钥缓存与密钥扩展倍数,可获得



用户节点广域加密通信带宽。密钥扩展倍数（或密钥重复使用次数）为 M_x ，则用户节点的平均加密通信带宽 w_e 为：

$$w_e = q \times (t_d/t_0) \times M_x \quad (6)$$

步骤 5 子域用户广域加密通信带宽规划

对于扩展网络，由于原有骨干量子链路密钥生成带宽的限制，新搭建的量子链路的全局加密通信的带宽利用率往往会非常低。为了增加带宽利用率，将位置相近的新建骨干链路划分为子网，在子网内利用量子链路的剩余带宽，按照步骤 1~步骤 4，规划子网的线路平均带宽。如果利用剩余带宽规划的子网线路的平均带宽为 w_{ss} ，全局线路平均带宽为 w ，则子网内总的线路平均带宽为 $w_s = w_{ss} + w$ ，子网内的加密通信带宽为 $w_{se} = (w_s/p) \times (t/t_d) \times M_x$ 。

3 数据模拟示例

通过一个具体网络的用户广域加密通信流量规划，说明应用流量规划模型实现用户广域加密通信流量规划的具体方法，然后根据流量规划，给出网络量子链路密钥分发带宽的调整建议。

整个量子保密通信广域网络结构如图 3 所示：每一个节点代表一个城域网络，相邻两个节点间的连线代表一段广域量子链路。各量子链路的密钥分发速率为：A1C2 线路的密钥分发速率为 2 kbit/s；

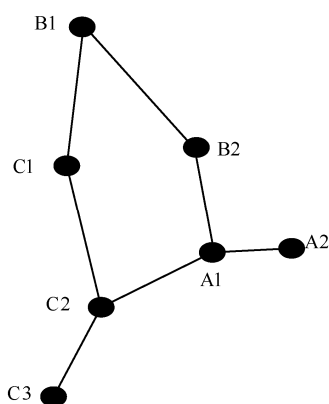


图 3 广域网络结构

线路 B1B2A1A2 上的各段量子链路的密钥分发速率为 4 kbit/s；线路 B1C1C2C3 上的各段量子链路为扩展骨干链路，其密钥分发速率较高，为 10 kbit/s。

整个网络用户数量规划为 2 400（总共 12 单位，每单位用户代表 200 个用户），具体占比为：

B1—3（表示城域网 B1 的用户数量为 3 单位，下同）、B2—1、A1—1、A2—2、C1—1、C2—2、C3—2。

按照下列步骤进行流量规划。

步骤 1 路由规划与线路平均带宽计算

给出以下 3 种路由规划方案。

- 方案 A：严格按照最短路径原则路由，不进行路由规划；
- 方案 B：C1 与 A1、A2 两点之间的路由经过 B1 点，其他路径路由严格遵循最短路径原则；
- 方案 C：C1 与 A1、A2 两点之间的路由经过 B1 点，B2 与 C1、C2 两点之间的路由经过 B1 点，其他路径路由严格遵循最短路径原则。

方案 B 和方案 C 是考虑到量子链路 A1C2 密钥分发带宽相对较小，而且处于网络的中心位置，为了降低 A1C2 线路的密钥消耗。

在每一种路由规划方案下，分别计算每条量子链路的广域加密通信线路数量，并按照式（2）分别计算每条量子链路的线路平均带宽，计算结果分别见表 1~表 3。

表 1 路由方案 A 时的线路平均带宽计算

量子链路	密钥分发带宽/ (kbit·s ⁻¹)	加密通信线路 数量 (×40 000)	线路平均带宽/ (kbit·s ⁻¹)
B1C1	10	16	1.56×10 ⁻⁵
C1C2	10	19	1.32×10 ⁻⁵
C2C3	10	20	1.25×10 ⁻⁵
B1B2	4	13	7.69×10 ⁻⁶
B2A1	4	16	6.25×10 ⁻⁶
A1A2	4	20	5.00×10 ⁻⁶
A1C2	2	20	2.50×10 ⁻⁶

表2 路由方案B时的链路平均带宽计算

量子链路	密钥分发带宽/ (kbit·s ⁻¹)	加密通信线路 数量 (×40 000)	线路平均带宽/ (kbit·s ⁻¹)
B1C1	10	19	1.32×10^{-5}
C1C2	10	16	1.56×10^{-5}
C2C3	10	20	1.25×10^{-5}
B182	4	16	6.25×10^{-6}
B2A1	4	19	5.26×10^{-6}
A1A2	4	20	5.00×10^{-6}
A1C2	2	16	3.13×10^{-6}

表3 路由方案C时的链路平均带宽计算

量子链路	密钥分发带宽/ (kbit·s ⁻¹)	加密通信线路 数量 (×40 000)	线路平均带宽/ (kbit·s ⁻¹)
B1C1	10	23	1.09×10^{-5}
C1C2	10	20	1.25×10^{-5}
C2C3	10	20	1.25×10^{-5}
B182	4	20	5.00×10^{-6}
B2A1	4	15	6.67×10^{-6}
A1A2	4	20	5.00×10^{-6}
A1C2	2	12	4.17×10^{-6}

通过表1~表3中的计算结果可知,量子链路A1C2的线路平均带宽均为最小,选其线路平均带宽作为全局线路平均带宽。路由方案A、路由方案B和路由方案C的全局线路平均带宽分别为 2.5×10^{-6} kbit/s、 3.13×10^{-6} kbit/s和 4.17×10^{-6} kbit/s。路由方案C的全局线路平均带宽最大,网络的带宽利用率最高,综合考虑路由成本的差距(还有其他能够增大全局线路平均带宽的路由规划,但通信成本会增大),选择路由规划方案C作为最优方案。

步骤2 计算每条量子链路的剩余带宽

在选择路由规划方案C时,全局线路平均带宽为 4.17×10^{-6} kbit/s,计算每条量子链路的密钥分发剩余带宽及带宽利用率,结果见表4。

由表4所知量子链路B1C1、C1C2和C2C3的剩余带宽较大,带宽利用率不足40%,将线路B1C1C2C3划分为一个子域,通过增加子域线路平均带宽来增加带宽利用率。

表4 剩余带宽计算

量子链路	剩余带宽/(kbit·s ⁻¹)	带宽利用率
B1C1	6.1636	38.46%
C1C2	6.664	33.33%
C2C3	6.664	33.33%
B182	0.664	83.40%
B2A1	1.498	62.55%
A1A2	0.664	83.40%
A1C2	0	100%

步骤3 子域线路平均带宽计算

子域B1C1C2C3为单通网络,不需要路由规划。按照最短路径原则路由,首先计算子域内每条量子链路剩余带宽所产生的线路平均带宽,计算结果见表5。

表5 子域线路平均带宽计算

量子链路	剩余带宽/ (kbit·s ⁻¹)	子域内加密通信线路 数量 (×40 000)	线路平均带宽/ (kbit·s ⁻¹)
B1C1	6.163 6	15	1.03×10^{-5}
C1C2	6.664	16	1.04×10^{-5}
C2C3	6.664	12	1.39×10^{-5}

由表5可知,子域B1C1C2C3由剩余带宽所产生的子域线路平均带宽为 1.03×10^{-5} kbit/s,加上广域网络的全局线路平均带宽 4.17×10^{-6} kbit/s,得到子域内的子域线路平均带宽为 1.45×10^{-5} kbit/s。

步骤4 计算用户节点广域加密通信带宽

预估计用户节点每天广域通信时间为8 h。根据网络结构计算网络线路数量 $L_n=2.4 \times 10^6$,用户数量为2 400,根据式(4)可得单位时间任意两个不同城域网的用户节点进行广域通信的平均概率 p 为:

$$p = Q_u \times t_0 / (2 \times L_n \times t_d) = 2\,400 \times 8 / (2 \times 2\,400\,000 \times 24) = 1/6\,000 \quad (7)$$

密钥扩展的倍数为 10^5 (在密码分析的安全范围之内),即 $M_x=10^6$ 。按照式(5)和式(6)计算用户节点的加密通信带宽,结果见表6。



表 6 广域加密通信带宽计算

示例网络	线路平均带宽/ (kbit·s ⁻¹)	用户加密通信带 宽/(Mbit·s ⁻¹)
整个广域网络	4.17×10^{-6}	7.5
子域网络 B1C1C2C3	1.44×10^{-5}	25.92

由表 7 可知,本示例网络的流量规划结果为:广域网络用户广域加密通信的带宽规划为 7.5 Mbit/s,子域 B1C1C2C3 内用户广域加密通信的带宽规划为 25.92 Mbit/s。

根据上述流量规划过程和相关计算结果,给出如下网络量子链路密钥分发带宽调整建议。

按照表 1 的计算结果,可以将量子链路的密钥分发带宽提高到 4 kbit/s,这样全局线路平均带宽可以达到 5×10^{-6} kbit/s (即 A1A2 的线路平均带宽),用户的广域加密通信带宽可以达到 9 Mbit/s。在不需要进行路由规划的情况下,各量子链路的密钥分发带宽利用率见表 7。

表 7 各量子链路的使用带宽和密钥分发带宽利用率

量子链路	使用带宽/(kbit·s ⁻¹)	带宽利用率
B1C1	3.2	32%
C1C2	3.8	38%
C2C3	4	40%
B182	2.6	65%
B2A1	3.2	80%
A1A2	4	100%
A1C2	4	100%

如果将全局线路平均带宽提高到 7.69×10^{-6} kbit/s (表 1 中线路 B1B2 的线路平均带宽),量子链路 B2A1、A1A2 和 A1C2 密钥分发带宽应该提升为表 8 中所示的需求带宽,其他量子链路的使用带宽和带宽利用率见表 9。

表 8 量子链路 B2A1、A1A2 和 A1C2 密钥分发带宽

量子链路	需求带宽/(kbit·s ⁻¹)
B2A1	4.921 6
A1A2	6.152
A1C2	6.152

表 9 其他量子链路的使用带宽和带宽利用率

量子链路	使用带宽/(kbit·s ⁻¹)	带宽利用率
B1C1	4.921 6	49%
C1C2	5.844 4	58%
C2C3	6.152	62%
B182	4	100%

如果将全局线路平均带宽提高到 1.25×10^{-5} kbit/s (表 1 中线路 B1C1 的线路平均带宽),量子链路 B1B2、B2A1、A1A2 和 A1C2 密钥分发带宽应该提升为表 10 中所示的需求带宽,其他量子链路的使用带宽和带宽利用率见表 11。

表 10 量子链路 B1B2、B2A1、A1A2 和 A1C2 密钥分发带宽

量子链路	需求带宽/(kbit·s ⁻¹)
B1C1	8
C1C2	9.5
C2C3	10
B182	6.5
B2A1	8
A1A2	10
A1C2	10

表 11 其他量子链路的使用带宽和带宽利用率

量子链路	使用带宽/(kbit·s ⁻¹)	带宽利用率
B1C1	8	80%
C1C2	9.5	95%
C2C3	10	100%

数值模拟示例分析如下。

- 在不增加网络搭建成本,即在网络量子链路密钥分发带宽固定不变的情况下,本文方法通过合理的路由规划能够增加量子链路密钥分发带宽的利用率,提升用户的广域加密通信带宽,提高网络性价比。
- 通过子域网络的流量规划,提升了子域用户的广域加密通信带宽,合理利用了量子链路的闲置带宽。
- 本文所述的流量规划方法,可以为不同规模的量子链路密钥分发带宽扩展提供数据

参考,使其扩展带宽更加合理。

4 结束语

广域量子保密通信网络骨干链路流量规划是量子保密通信网络发展过程中的一个新问题。本文根据目前广域量子保密通信网络的发展现状,提出了一种适合当前广域量子保密通信网络骨干链路流量规划方案。通过数值模拟示例,具体演示了如何通过路由规划提升用户节点的全局广域加密通信带宽以及如何参照流量规划,调整瓶颈量子链路的密钥分发带宽。数值模拟示例说明了本文方法的有效性和可用性。本方法较为适合目前阶段处于扩展中的较为简单的广域量子保密通信网络,对于复杂网络的流量规划方法,还需要进一步的研究和探索。

参考文献:

- [1] 费城, 沈仲良. 小量量子光通信[J]. 中国新通信, 2018(2): 1-4.
FEI C, SHEN Z L. On quantum optical communications [J]. China New Communications, 2018(2): 1-4.
- [2] 赖俊森, 吴冰冰, 汤瑞, 等. 量子保密通信标准化现状与发展分析[J]. 电信科学, 2018, 34(1): 1-7.
LAI J S, WU B B, TANG R, et al. Analysis on the status quo

and development of standardization of quantum secure communication [J]. Telecommunications Science, 2018, 34(1): 1-7.

- [3] 杨超, 张红旗, 苏锦海, 等. 基于密钥中继的广域量子密钥网络路由方案[J]. 网络与信息安全学报, 2017(11): 12-21.
YANG C, ZHANG H Q, SU J H, et al. Wide area quantum key network routing scheme based on key relay [J]. Journal of Network and Information Security, 2017(11): 12-21.
- [4] 焦利, 林宇, 金跃辉, 等. 随机路由网络中瓶颈链路推测新算法[J]. 高技术通讯, 2005(8): 6-10.
JIAO L, LIN Y, JIN Y H, et al. New algorithm for bottleneck link inference in random routing networks [J]. High-Tech Communications, 2005(8): 6-10.

[作者简介]



原磊 (1975—), 男, 山东量子科学技术研究院有限公司研究员, 主要研究方向为量子保密通信网络架构、路由、应用扩展等。



赵梅生 (1980—), 男, 博士, 山东量子科学技术研究院有限公司副总工程师, 主要研究方向为量子信息理论、量子保密通信网络、量子加密技术等。