基于回溯的 QKD 网络随机路由选择算法研究

徐雅斌[1,2*]，张梅舒[2]，李艳平[2]

(1. 北京信息科技大学网络文化与数字传播北京市重点实验室 北京 朝阳区 100101；2. 北京信息科技大学计算机学院 北京 朝阳区 100101)

【摘要】为了解决已有的基于信任中继的 QKD 网络路由方案存在的密钥浪费、传输效率低下等问题，该文针对已有的路由算法进行改进，提出了一种基于回溯的随机路由算法。该算法在选路过程中对每个分支添加回溯点，针对已选路径传输过程中遇到某条链路密钥量不足的情况，通过查找最近的回溯点，从回溯点开始沿着随机选择的新路径重新进行密钥传递。对比实验及分析结果表明，该算法在选路时间、密钥消耗量及密钥传输效率方面都有一定的优势。

关 键 词 回溯； 量子密钥分发； QKD 网络； 随机路由； 信任中继

中图分类号 TN393 **文献标志码** A doi:10.12178/1001-0548.2019175

Research and Design of QKD Network Random Routing Algorithm Based on Backtracking

XU Ya-bin[1,2*], ZHANG Mei-shu[2], and LI Yan-ping[2]

(1. Beijing Key Laboratory of Internet Culture and Digital Dissemination Research, Beijing Information Science &Technology University Chaoyang Beijing 100101; 2. School of Computer, Beijing Information Science &Technology University Chaoyang Beijing 100101)

Abstract In order to solve the problems of key waste and low transmission efficiency in the existing routing scheme of quantum key distribution (QKD) network based on trust relay, a random routing algorithm based on backtracking is proposed to improve the existing routing algorithm. In the process of routing, the algorithm adds backtracking points to each branch, in the transmission process along the selected path, when the key quantity of a certain link is insufficient, by looking for the nearest backtracking point, the key can be transferred along the randomly selected new path again from the backtracking point. The comparison experiment and analysis results show that the algorithm has certain advantages in routing time, key consumption and key transmission efficiency.

Key words backtracking; quantum key distribution; QKD network; random routing; trust relay

量子密钥分发 (quantum key distribution, QKD) 技术利用量子密钥进行量子编码并传递，可以为通信双方提供理论上无条件安全的共享密钥[1]。将多个点到点 QKD 网络连接起来组成的量子密钥分发网络可以提供多用户、长距离的密钥服务。

目前，国内外提出的 QKD 网络主要有 3 种[2-3]：光学中继 QKD 网络、量子中继 QKD 网络及信任中继 QKD 网络。其中，基于信任中继的 QKD 网络技术由于不受覆盖范围和用户数量的限制，是目前建设大规模、实用化保密通信网络的首选方案。但是，基于信任中继的 QKD 网络在进行端到端密钥协商时，可能存在多条传输密钥的路径，这就需要进行选路。

在当前密钥生成量难以满足需求的情况下，相对最近路径的选择，网络中密钥的消耗量和密钥传输的安全性显得更为重要。即在信任中继 QKD 网络中，路由选择的关注点发生了根本变化，需要与之相适应的路由选择算法。因此，研究和设计适合大规模 QKD 网路的高效路由算法对于促进量子通信网络的发展具有重要意义。

当前，针对信任中继 QKD 网络路由问题的研究主要有单路径和多路径两种设计方式[4-5]。对于现有的单路径路由方案[3-6]，密文转发总是在同一条路径上进行，在网络拓扑等信息已知的情况下，各中间节点是可预测的，易受到窃听而威胁通信安全。多路径路由方案[7-10]通过提供多条不同路径同时传输信息，提高了网络服务质量，增强了网络安全性，但消耗的本地密钥量较多，传输效率较低。

收稿日期：2019－09－29；修回日期：2021－03－15

基金项目：中央引导地方科技发展专项 (Z171100004717002)

作者简介：徐雅斌 (1962－)，男，教授，主要从事网络安全、大数据、社交网络及量子加密通信等方面的研究. E-mail：xyb@bistu.edu.cn

为了解决单路径路由安全性不足的问题和多路径路由的密钥浪费问题，文献 [11] 提出一种将当前节点的所有邻居节点作为下一跳的候选，以一定概率随机选择下一跳的自适应路由算法。文献 [12] 在此基础上通过添加一种带标签的随机路径策略，以减少公共节点的数量，避免产生环路。文献 [13] 基于宽带利用率分别提出了针对单路径和多路径的路由算法，其中单路径路由算法主要考虑网络的服务质量和密钥管理，而多路径路由算法则着重考虑提高网络的安全性，从而减少量子密钥分配网络的密钥消耗，提高密钥服务效率。

针对多路径解决方案，文献 [14] 设计了基于格型拓扑结构的量子密钥分发网络方案，提出了一种适合量子密钥分发网络的冗余路由算法，并对其呼损性能进行分析。文献 [15] 提出了多随机路径方案，有效解决了部分受信任的中继网络的致命安全性问题。文献 [16] 在选路中考虑到了密钥量，提出了一种基于 RIP 协议的随机路由算法。具体做法是：首先根据改进的 RIP 协议找到所有最短路径，然后选路时在多个密钥充足的下一跳中随机选择一个，直至到达目的节点。

为了进一步提高多路径解决方案的质量和效率，文献 [17] 提出了基于光交换机的量子保密通信网络路由算法，保证了较高的安全成码率，提高了通信质量，然后在考虑链路剩余密钥量和最短路径的基础上提出了基于可信中继的量子保密通信网络随机路由算法。文献 [18] 提出了一种基于距离矢量和剩余密钥的随机路由算法，在获得所有最短路径后，通信密钥位可以在剩余密钥位足够多的任意路径上随机传输，提供更高的安全性。

通过分析发现，在已提出的针对信任中继的 QKD 网络随机路由算法中，有些忽略了密钥量对信任中继网络路由的影响，有些虽然在一定程度上解决了单路径路由的安全性低和多路径路由的密钥浪费问题，但在遇到密钥量不足的情况下，就要中断通信，重新开始进行密钥传递，从而造成密钥的浪费和成功率的降低。因而，在选路失败后，应考虑如何充分利用已经进行的密钥传递过程，以提高传输效率和密钥传递成功率，节约密钥。

因此，本文提出一种改进的多路径随机路由算法。该算法找到源节点到目的节点的 3 条最短路径，在选路时随机选择其中 1 条，使窃听者无从获知确切的密钥传输路径，从而提高密钥传输的安全性。此外，在选路过程中加入回溯策略，当选路出现密钥量不足而无法推进时，通过最短路径的回溯，找到新的可用路径，从而提高选路的成功率，并最大程度地减少选路时间和密钥消耗量。

1 基于信任中继的 QKD 网络

1.1 信任中继 QKD 网络结构

图 1 是基于信任中继的 QKD 网络结构[5]，网络由用户、信任中继节点和链路 3 部分组成，信任中继节点之间通过链路连接在一起。由用户发起通信请求，各信任中继节点负责转发密文和密钥，在网络中起中继交换的作用。

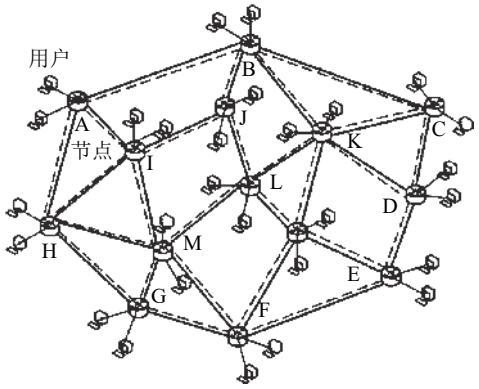

图 1 信任中继 QKD 网络结构

信任中继 QKD 网络中有两条信道，一条是用于传输密钥的量子信道，另一条是用于传输路由信息和加密信息的经典信道。在图 1 中，实线表示量子信道，是两节点间的直通信道；虚线表示经典信道，可以是两节点间的直连信道，也可以是经由其他节点转接的信道。由于两个信道的传输内容和传输方式都不同，因此量子信道的路由方式不能直接使用经典网络中成熟的路由技术。本文所提及的 QKD 网络特指由量子信道组成的网络。

1.2 信任中继密钥传输原理

信任中继密钥传输原理如图 2，假定用户 A 要和用户 B 进行密钥传递，中继节点 1 和中继节点 2 共享密钥 $K1$，中继节点 2 和中继节点 3 共享密钥 $K2$，中继节点 3 与用户 B 共享密钥 $K3$。用户 A 和中继节点 1 协商出全局密钥 K 后 (通信密钥)，通过中继节点 1、2 和 3 传递给用户 B。传递过程中，中继节点先解密后加密，如中继节点 2 从中继节点 1 接收到 $K\oplus K1$，先用与中继节点 1 共享的 $K1$ 解密得到 K，再用与中继节点 3 共享的密钥 $K2$ 加密得到 $K\oplus K2$，然后发送给中继节点 3。

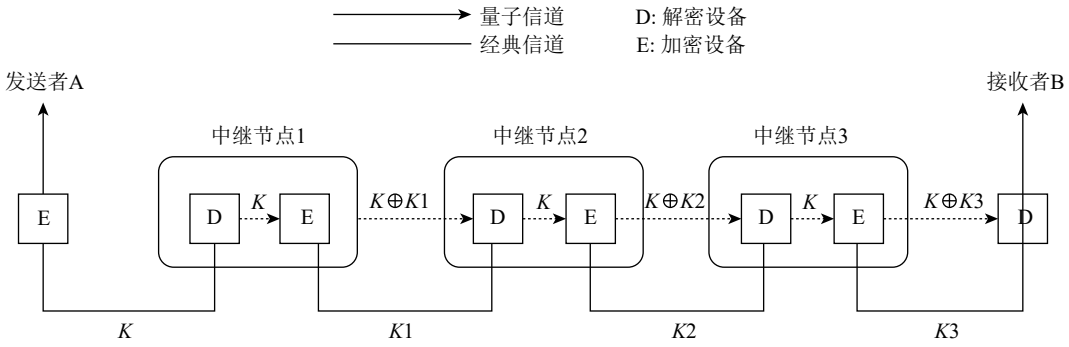

图 2　信任中继密钥传输原理

由于相邻中继节点共享的密钥是通过密钥分发产生的，具有无条件安全性，因而节点之间进行密钥传输时，可以保证密钥不被泄露；又由于中继节点是可以信任的，所以基于信任中继的密钥传递在理论上是安全的。

2　随机路由算法

2.1　问题分析

文献 [16] 提出一种基于 RIP 协议的随机路由算法，该算法通过改进基于距离矢量的路由算法扩展路由表，为到达某一目的地址的中继节点添加多个下一跳，进而得到源中继节点到目的中继节点的多条最短路径；在选路时，将链路上的剩余密钥量考虑在内，在存在多个密钥量充足的下一跳中继节点的情况下，在其中随机地选择一个，然后逐跳转发，直到转发至目的中继节点。

虽然该方法路径最短且安全性较高，但仍然存在以下不足：1) 只适用于源节点和目的节点之间有多条最短路径的情况，如果源、目的节点之间只有一条最短路径，该算法就会失效；2) 在选中密钥量不足的下一跳节点时就将中断传输，按新的最短路径从头开始密钥协商，浪费资源且成功率较低。

针对该随机路由算法的不足，本文将路由算法进行改进，并提出一种基于回溯的 QKD 网络随机路由选择方案。

2.2　改进的随机路由算法

针对文献 [16] 不适用于源、目的节点之间只有一条最短路径的问题，本文提出一种寻找两个节点之间多条路径的方法：1) 采用文献 [6] 改进的 Dijkstra 算法找到源节点到目的节点的所有最短路径；2) 判断最短路径的条数：如果路径条数少于 3，就在网络中删除当前的最短路径，继续找最短路径，直到找到 3 条最短路径；如果路径条数不少于 3，就从中随机选择 3 条最短路径；3) 将选出的 3 条路径加入路由表中。

本文提出的随机路由算法的思想是：从源节点开始进行寻路，在当前节点与目的节点存在多条传输路径时，查看链路上的剩余密钥量，在剩余密钥量足够的所有链路中随机选择一条，逐跳选择中继节点来转发密钥。当选择的节点不存在密钥量足够的链路时，判断该节点是否存在可回溯的中继节点。如果存在，就回溯；如果不存在，结束通信，重新开始协商密钥。

为了找到可回溯的中继节点，本文设计一种标记回溯点的方法。在路由表中添加一个新项——回溯点，用于标记该节点的回溯点。即，如果所选路径中某节点的链路密钥量不足，此节点就查找其回溯点。如果存在，就回溯到该点；如果不存在，就结束此次密钥协商。标记回溯点的算法步骤如下：

1) 初始情况下，路由表中每一项的回溯点均为空；2) 从源中继节点开始，判断当前节点到目的节点的下一跳个数：如果个数为 1，将下一跳的回溯点标记为当前节点的回溯点的值；如果个数大于 1，将多个下一跳的回溯点标记为当前节点。

图 3 是一个简单的例子，如果 Alice 要与 Bob 通信，计算得到 3 条最短路径：P1：1→2→3→4；P2：1→2→5→4；P3：1→8→6→4。所以，节点 2,8 的回溯点为 1；节点 3,5 的回溯点为 2。

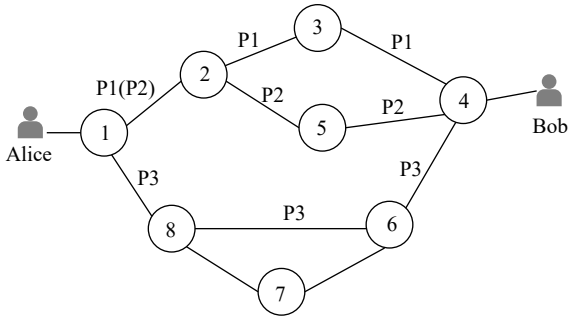

图 3　标记回溯点的例子

各节点的路由表如表 1～表 6 所示。

表 1 节点 1 的路由表

目的地址	下一跳	跳数	回溯点
4	2	3	
4	8	3	

表 2 节点 2 的路由表

目的地址	下一跳	跳数	回溯点
4	3	2	1
4	5	2	1

表 3 节点 3 的路由表

目的地址	下一跳	跳数	回溯点
4	4	1	2

表 4 节点 5 的路由表

目的地址	下一跳	跳数	回溯点
4	4	1	2

表 5 节点 8 的路由表

目的地址	下一跳	跳数	回溯点
4	6	2	1

表 6 节点 6 的路由表

目的地址	下一跳	跳数	回溯点
4	4	1	8

本文提出的随机路由选择的算法步骤为：

1) 找到源中继节点到目的中继节点的 3 条最短路径，并将下一跳信息添加到路由表；

2) 相邻中继节点利用量子密钥分发协议协商出量子密钥 K，并存储；

3) 源量子通信终端与其相连的中继节点 (源节点) 协商出本次通信的通信密钥 Kc；

4) 从源节点出发，首先对收到的密文进行解密，然后根据目的地址查找路由表，判断路由表中到此次协商的目的地址的下一跳个数 N(如果是回溯到此节点，则去掉选路失败的下一跳)：

① 如果 N=1，执行步骤②；如果 N>1，执行步骤③；

② 判断下一跳相邻中继节点中存储的量子密钥的比特数是否大于通信密钥的比特数。若是，将通信密钥加密后转发至下一跳相邻中继节点，执行步骤④，否则，执行步骤 5)；

③ 将收到的密钥存储，然后在 N 个下一跳相邻中继节点中选出量子密钥的比特数大于通信密钥的比特数的中继节点，并在其中随机地选取一个，然后将通信密钥加密后转发至该相邻中继节点，执行步骤④；对于多个下一跳相邻中继节点中存储的量子密钥的比特数均小于通信密钥的比特数的情况，执行步骤 5)；

④ 对选取的相邻节点标记回溯点，该节点收到加密后的通信密钥，利用存储的量子密钥对其进行解密，并判断当前中继节点是否为目的中继节点。若是，则源中继节点与目的中继节点端到端的通信密钥建立成功，源中继节点利用该通信密钥 Kc 对数据加密进行传输；否则，根据目的地址查找路由表，返回步骤①；

5) 查找该节点的回溯点，判断回溯点是否存在：

① 如果存在，通知回溯点本路径通信失败，回溯点执行步骤 4)；② 如果不存在，此次密钥协商失败，执行步骤 6)；

6) 释放源量子通信终端与目的量子通信终端间的连接。

2.3 实例分析

以图 4 为例，假设此次通信所需密钥为 10，图中链路上的数字代表路径上剩余密钥量。首先，寻找节点 1 到节点 5 之间的所有最短路径，找到 1 条最短为：1-2-6-5。由于当前路径条数少于 3，继续寻找节点 1 到节点 5 之间的所有最短路径，找到的结果为：1-10-3-4-5，1-2-3-4-5 和 1-9-8-7-5，至此，获得 3 条最短路径。随机选择其中的 2 条，假定选择的结果为：1-2-3-4-5，1-9-8-7-5。再加上之前选择的 1 条最短路径：1-2-6-5，则获得 3 条最短路径：1-2-6-5，1-2-3-4-5，1-9-8-7-5。

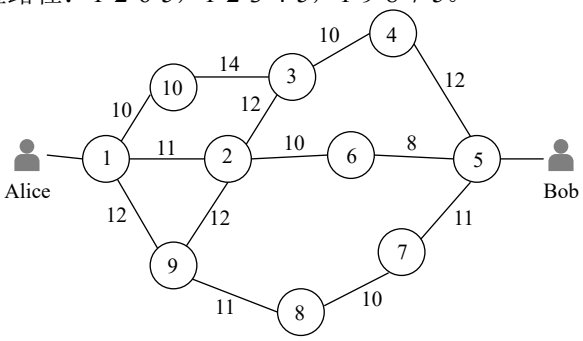

图 4 路由选择实例

路由选择过程如下：

1) 从源节点 1 开始，查找路由表，得到的到达节点 5 的路径有两条，由于两条链路的密钥量都充足，因而随机选择下一跳，假设选择节点 2；

2) 由于从节点 1 经节点 2 到节点 5 有多条路径，因而将节点 2 的回溯点标记为 1；

3) 从节点 2 开始，进一步查找路由表，得到的

到达节点 5 的路径有两条，分别为节点 3 和节点 6，由于两条链路的密钥量都充足，因而随机选择下一跳节点，假定选择节点 6；

4) 由于从节点 2 经节点 6 到节点 5 有多条路径，因而将节点 6 的回溯点标记为节点 2；

5) 从节点 6 开始进一步查找路由表，得到的到达节点 5 的下一跳节点即为节点 5。但链路 6-5 的密钥量不足，因而回到它的回溯点，即节点 2；

6) 从节点 2 开始，去掉选路失败的下一跳节点 6，进一步查找路由表，得到到达节点 5 的唯一一个下一跳节点为节点 3，且密钥量充足，因此确定下一跳节点为节点 3；

7) 由于从节点 2 经节点 3 到节点 5 有多条路径，因而将节点 3 的回溯点标记为节点 2；

8) 从节点 3 开始，进一步查找路由表，得到到达节点 5 的唯一的下一跳节点为节点 4，且密钥量充足，因此确定下一跳节点为节点 4；

9) 但由于从节点 3 经节点 4 到节点 5 只有一条路径，因此将节点 4 的回溯点仍然标记为节点 2；

10) 从节点 4 开始，进一步查找路由表，发现可直接到达节点 5，且链路的密钥量充足，因而可直接将密钥转发给节点 5。

至此，算法结束。

由此算法可以看出，当发现密钥量不足的链路后，本算法就回溯到存在其他最短路径的节点，由此以最小的代价沿着新的最短路径进行路由选择。

3　实验及分析

本文对图 3 的网络拓扑做进一步的扩展，采用图 5 所示的网络拓扑图，对使用单路径路由算法、多路径路由算法、文献 [16] 提出的随机单路径路由算法以及本文提出的算法来实现 Alice 和 Bob 之间的密钥传递情况进行仿真实验。

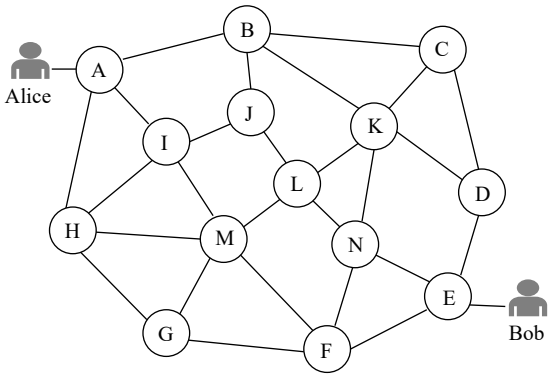

图 5　实验的网络拓扑结构

3.1　实验环境及性能指标

本实验的硬件环境是 Intel(R) Core(TM) i7-4790 CPU @ 3.60 GHz，8.0 GB RAM，Windows 7 专业版操作系统，Visual Studio 2015，算法的实现语言为 C++。

本文采用以下 3 个性能指标进行评价和分析：1) 选路成功率。选择路径成功与否是路由算法可行与否的关键，该指标用来评价路由算法的可行性。2) 密钥消耗量。充足的密钥量是信任中继量子网络密钥传递的必要条件，密钥消耗的多少直接影响到接下来的密钥通信，该指标用来评价路由算法的效率。3) 选路时间。一次密钥传递的时间对路由的效率影响很大，该指标用来评价路由算法的效率。

3.2　选路成功率比较

针对图 5 所示的网络拓扑结构，Alice 到 Bob 之间的路径有很多条，通过路由算法选择 3 条最短路径：A-B-C-D-E；A-I-M-F-E；A-H-G-F-E。

针对密钥量充足的情况，4 种方法的选路成功率均为 100%。因此，本实验只考虑存在密钥量不足链路的情况。本网络中可选择的链路有 11 条。本实验仿真一条链路密钥量不足时的选路成功率，分别用 4 种路由算法做了 11 组实验来仿真 11 条链路在密钥量不足情况下的选路情况，每组 20 次，统计其选路成功次数和选路成功率 (选路成功率=选路成功次数/实验次数)。

4 种不同算法的选路成功率情况如图 6 所示。可以看出，本算法在一条链路密钥量不足的时候，选路成功率都是 100%，选路效果最好；而文献 [16] 提出的随机单路径路由算法，当存在链路密钥量不足时，成功率很难达到 100%；对于单路径路由算法，当链路 A-B、B-C、C-D 和 D-E 密钥量不足时，选路成功率为 0，其他情况选路成功率为 100%；对于多路径路由算法，存在密钥量不足链路时，选路成功率为 0。

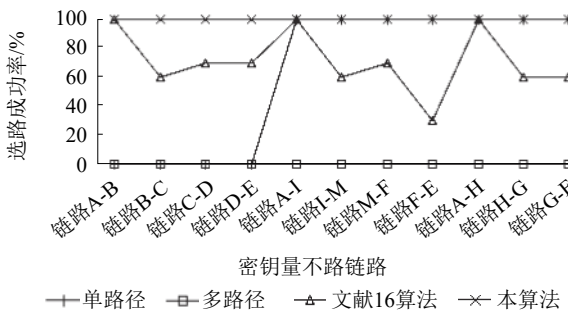

图 6　4 种不同算法的选路成功率对比图

分析原因如下：单路径路由算法在选路时选择一条路径，当选中的路径的链路密钥量不足时，就会宣告选路失败；多路径路由算法在选路时，虽然可选择多条路径 (这里为 3 条路径)，但无论哪条路径的链路密钥量不足，都会宣告选路失败；文献 [16] 提出的随机单路径路由算法在选路时随机选择一条，可能会选中密钥量不足的链路，进而导致选路失败；而本文提出的算法，选路时会从 3 条最短路径中随机选择一条，当选中的最短链路密钥量不足时，就会回溯到有具有多条路径的节点，继续进行路由选择，而不是宣告选路失败，因而选路代价较低，成功率较高。因此，相对于已存在的针对 QKD 网络的路由算法来说，本文提出的路由选择算法的选路成功率更高，效果更好。

3.3 密钥消耗量比较

假设本次密钥传递需要的密钥量为 10。用 $K1$、$K2$、$K3$ 和 $K4$ 分别代表 4 种算法的密钥消耗量，其中，$K1$ 表示单路径路由的密钥消耗量，$K2$ 表示多路径路由的密钥消耗量，$K3$ 表示文献 [16] 的随机单路径路由的密钥消耗量，$K4$ 表示本文算法的密钥消耗量。

密钥消耗量比较分以下 4 种情况：

1) 链路密钥量充足：4 种算法都选路成功，密钥消耗量为：$K1=K3=K4=40$，$K2=120$。

2) 第二跳密钥量不足：单路径路由算法选路失败后从起点重新开始进行密钥传递，则 $K1=10+40n$ ($n\geqslant 1$)；多路径路由算法其中一条路径选路失败后该路径重新开始进行密钥传递，则 $K2=80+10+40n=90+40n$($n\geqslant 1$)；文献 [16] 的随机路由算法的密钥消耗量等同于单路径路由算法，则 $K3=10+40n$($n\geqslant 1$)；而当选中的链路密钥量不足时，本算法将回溯到回溯点继续进行密钥传递，直至选路成功，则 $K4=10+40=50$。

3) 第三跳密钥量不足：$K1=20+40n$($n\geqslant 1$)；$K2=80+20+40n=100+40n$($n\geqslant 1$)；$K3=20+40n$($n\geqslant 1$)；$K4=20+40=60$。

4) 第四跳密钥量不足：$K1=30+40n$($n\geqslant 1$)；$K2=80+30+40n=110+40n$($n\geqslant 1$)；$K3=30+40n$($n\geqslant 1$)；$K4=30+40=70$。

密钥消耗量结果如表 7 所示：由表 7 可知，当存在链路密钥量不足的情况时，本算法的密钥消耗量明显小于或等于其他 3 种算法，效率更高。

表 7　4 种算法的密钥消耗量的对比

4种情况	$K1$	$K2$	$K3$	$K4$
链路密钥量充足	40	120	40	40
第二跳密钥量不足	$10+40n$($n\geqslant 1$)	$90+40n$($n\geqslant 1$)	$10+40n$($n\geqslant 1$)	50
第三跳密钥量不足	$20+40n$($n\geqslant 1$)	$100+40n$($n\geqslant 1$)	$20+40n$($n\geqslant 1$)	60
第四跳密钥量不足	$30+40n$($n\geqslant 1$)	$110+40n$($n\geqslant 1$)	$30+40n$($n\geqslant 1$)	70

3.4 选路时间比较

由单路径路由、多路径路由和文献 [16] 提出的随机路由算法的选路原理可知，3 种方法的选路时间相差无几。本实验只比较文献 [16] 算法与本算法的选路时间。

对于文献 [16] 的路由算法，当选择的路径密钥量不足时，就中断通信，重新开始进行密钥传递。为了比较两个算法的选路时间，本实验设定密钥产生速率为 100 单位/s，当文献 [16] 的算法失败后，更新密钥量，重新开始密钥传递，直到密钥传递成功。将每次的时间相加，即可得到选路时间。

本实验利用图 5 所示的网络，采用本文提出的算法进行多次实验，记录 20 次有回溯的选路时间；采用文献 [16] 的算法进行多次实验，记录 20 次选择路径失败后重新进行选路的选路时间。对比结果如图 7 所示。

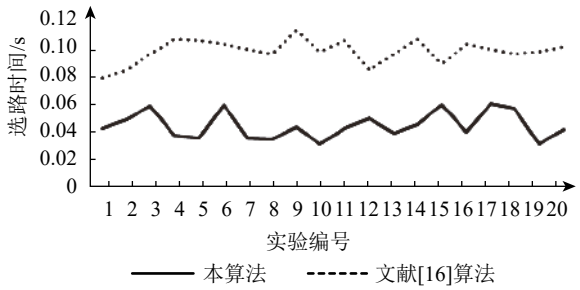

图 7　选路时间的对比

由图 7 可知，本算法的选路时间为 0.03～0.06 s，而算法 [16] 的选路时间为 0.08～0.12 s。显而易见，本算法的选路时间较短，效率较高。

上述实验及分析结果表明：相对于已有的单路径路由算法、多路径路由算法和随机单路径路由算法，本算法在密钥量不足的网络中有更好的选路成功率、更少的密钥消耗量和更短的选路时间。

4 结束语

本文主要针对基于信任中继的量子密钥网络的路由问题展开研究，分析了现有路由方案存在的问题，提出了一种随机路由方案。该方案通过改进的路由算法找到两点之间的 3 条最短路径，从而保证有多条较短路径；在选路过程中，随机选择其中的一条，安全性较高；遇到密钥量不足的链路时，回溯到有其他路径的节点，节省密钥量并提高了密钥传输效率。实验及分析结果表明，本算法不仅适用范围广，并且在选路时间、密钥消耗量以及密钥传输效率方面有一定的优势。

本文工作得到网络文化与数字传播北京市重点实验室 (ICDDXN004) 的资助，在此表示感谢。

参 考 文 献

[1] 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, 3(11): 12-21.
YANG Chao, ZHANG Hong-qi, SU Jin-hai. Routing scheme for key-relaying-based quantum key distribution network in wide-area[J]. Chinese Journal of Network and Information Security, 2017, 3(11): 12-21.

[2] 吴张斌, 陈光, 杨伯君. 量子密钥分配网络分析[J]. 光通信研究, 2009, 35(2): 22-24.
WU Zhang-bin, CHEN Guang, YANG Bo-jun. Analysis of quantum key distribution networks[J]. Study on Optical Communications, 2009, 35(2): 22-24.

[3] 曹原, 赵永利. 量子通信网络研究进展[J]. 激光杂志, 2019, 4(9): 1-7.
CAO Yuan, ZHAO Yong-li. Research progress of quantum communication networks[J]. Laser Journal, 2019, 4(9): 1-7.

[4] ZHANG Shi-bin, CHANG Yan, YAN Li-li, et al. Quantum communication networks and trust management: A survey[J]. CMC: Computers, Materials & Continua, 2019, 61(3): 1145-1174.

[5] 袁小虎, 李春文. 光纤量子通信网络路由选择协议[J]. 控制理论与应用, 2019, 4(9): 1-7.
YUAN Xiao-hu, LI Chun-wen. Routing protocol of fiber quantum communication network[J]. Control Theory & Applications, 2019, 4(9): 1-7.

[6] WANG Xin-liang, HUANG Qing-gai, LIU Zhi-huai, et al. Routing protocol research for wireless quantum networks based on resource reservation[J]. International Journal of Performability Engineering, 2019, 15(4): 1112-1121.

[7] DIANATI M, ALLÉAUME R, GAGNAIRE M, et al. Architecture and protocols of the future European quantum key distribution network[J]. Security & Communication Networks, 2010, 1(1): 57-74.

[8] TANIZAWA Y, TAKAHASHI R, DIXON A R. A routing method designed for a quantum key distribution network[C]//The 8th International Conference on Ubiquitous and Future Networks. [S.l]: IEEE, 2016: 208-214.

[9] 韩伟, 武欣嵘, 朱勇, 等. 基于信任中继的 QKD 网络路由选择研究[J]. 军事通信技术, 2013, 34(4): 43-48.
HAN Wei, WU Xin-rong, ZHU Yong, et al. QKD network routing research based on trust relay[J]. Journal of Military Communications Technology, 2013, 34(4): 43-48.

[10] 石磊, 苏锦海, 郭义喜. 量子密钥分发网络端密钥协商最优路径选择算法[J]. 计算机应用, 2013, 34(4): 3336-3341.
SHI Lei, SU Jin-hai, GUO Yi-xi. Optimal routing selection algorithm of end-to-end key agreement in quantum key distribution network[J]. Journal of Computer Applications, 2013, 34(4): 3336-3341.

[11] QUOC C L, BELLOT P, DEMAILLE A. Stochastic routing in large grid-shaped quantum networks[C]//IEEE International Conference on Research, Innovation and Vision for the Future. [S.l.]: IEEE, 2007: 166-174.

[12] MA C, GUO Y, SU J. A multiple paths scheme with labels for key distribution on quantum key distribution network[C]//Advanced Information Technology, Electronic and Automation Control Conference. [S.l.]: IEEE, 2017: 2513-2517.

[13] 杨灏. 基于信任中继的量子密钥分配网络的路由算法研究[D]. 北京: 北京邮电大学, 2017.
YANG Hao. Research on routing selection algorithm in trusted relay quantum key distribution networks[D]. Beijing: Beijing University of Posts and Telecommunications, 2017.

[14] 侯保刚. 量子密钥分发网络拓扑结构及路由算法研究[D]. 西安: 西安电子科技大学, 2013.
HOU Bao-gang. Research on topology and routing algorithm of quantum key distribution network[D]. Xi'an: Xidian University, 2013.

[15] WEN Hao, HAN Zheng-fu, ZHAO Yi-bo, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network[J]. Science in China, 2009, 52(1): 18-22.

[16] 李敏. 量子保密通信网络路由算法研究[D]. 西安: 西安电子科技大学, 2017.
LI Min. Research on the routing algorithm in quantum cryptography communication network[D]. Xi'an: Xidian University, 2017.

[17] 权东晓, 李敏, 朱畅华, 等. 量子保密通信网络中的随机路由方法: CN106230582A[P]. 2016-12-14.
QUAN Dong-xiao, LI Min, ZHU Chang-hua, et al. Random routing methods in quantum secure communication networks: CN106230582A[P]. 2016-12-14.

[18] LI Min, QUAN Dong-xiao, ZHU Chang-hua. Stochastic routing in quantum cryptography communication network based on cognitive resources[C]//International Conference on Wireless Communications & Signal Processing. [S.l.]: IEEE, 2016: 1-4.

编　辑　蒋　晓