广域量子密钥网络分层路由方案

杨 超[1],张红旗[2],苏锦海[2],胡 浩[2],赵 丹[1],王 昉[1]
(1. 中国空气动力研究与发展中心计算空气动力研究所,四川绵阳 621000; 2. 信息工程大学,河南郑州 450004)

摘 要: 针对现有可信中继QKD(Quantum Key Distribution)网络路由方案应用于广域环境时存在着密钥交换效率低、密钥资源无意义消耗大的问题,分析了影响密钥交换效率的因素,设计了适应广域QKD网络的分层路由方案.该方案将QKD网络划分为若干路由域,并通过拓扑聚合构建分层QKD网络,设计了基于最低层网络匹配的跨域密钥路由算法,使得高层路由域内一跳便可跨过多个低层路由域,极大地降低了密钥中继跳数,提高了密钥交换效率及密钥资源利用率.仿真结果表明分层路由方案相对于现有单层逐跳式路由方案能够提高大约77.6%密钥资源利用率,同时缩短一半密钥服务延时.

关键词: QKD网络; 量子密钥分发; 路由机制; 分层网络
中图分类号: TP393.2 **文献标识码:** A **文章编号:** 0372-2112 (2021)05-0975-09
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20170960

Hierarchical Routing Scheme for Wide-Area Quantum Key Distribution Network

YANG Chao[1], ZHANG Hong-qi[2], SU Jin-hai[2], HU hao[2], ZHAO Dan[1], WANG Fang[1]
(1. *Computational Aerodynamics Institute, China Aerodynamics Research and Development Center, Mianyang, Sichuan* 621000, *China*; 2. *Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: Aimed at the problems, such as low key exchange efficiency and large meaningless consumption of secret key materials, when the existing routing schemes for trust relaying QKD (quantum key distribution) network used in the wide-area environment, a hierarchical routing scheme which is suitable for wide-area QKD network was designed. This routing scheme divided the QKD network into multiple routing areas, built a hierarchical network by topological aggregation and designed a cross-domain routing algorithm based on the principle of the lowest layer matching. Then the hop number in the routing path is decreased, and the efficiency of key exchange and the utilization rate of secret key materials ware increased. At last, the simulation results shows that our hierarchical routing scheme can increase about 77.6% utilization rate of secret key materials and reduce service delay by half compared with the existing routing schemes which just relaying secret key hop by hop in a single layer.

Key words: QKD (quantum key distribution) network; quantum key distribution; routing scheme; hierarchical network

1 引言

量子密钥分配(Quantum Key Distribution, QKD)技术[1]利用量子态对信息(即密钥)进行编码并传递,可以为通信双方提供理论上无条件安全的共享密钥.它的安全性依赖于量子力学基本原理[2],一旦有人窃取密钥,就必然会被使用者发现.通过将多个点到点QKD系统连接起来组成的量子密钥分发网络,可以为多用户提供远距离、网络化的密钥服务.凭借QKD技术独特的安全性,QKD网络必然会在国防、军事、金融等众多信息安全领域发挥重要作用[3,4].

国内外已经提出的QKD网络组网方式可分为三类[5]:光学节点QKD网络、信任节点QKD网络以及量子节点QKD网络.其中,由信任节点构成的QKD网络(也被称为可信中继QKD网络),理论上可以实现全球范围的密钥分发,被认为是目前技术条件下实际可行

收稿日期:2017-08-26; 修回日期:2020-11-05; 责任编辑:孙瑶

的广域量子密钥网络组网方式[6,7],因此,本文主要针对由信任节点构成的 QKD 网络展开相关研究. 目前国内外已有多个国家建立了可信节点 QKD 网络[8~12],这些可信中继 QKD 网络规模相对较小节点数目有限,主要在于验证 QKD 技术组网的可行性. 然而,在广域 QKD 网络环境中必然还有许多需要解决的问题. 比如,广域 QKD 网络的系统参数优化配置[13]、系统稳定控制优化[14],以及广域 QKD 网络路由方案选择等. 其中,路由作为网络建设过程中与生俱来的问题,在 QKD 网络建设中无法回避,但是目前在 QKD 网络相关研究中路由问题并没有得到足够的重视[15],研究成果较少.

在 SECOQC 网络中采用了经典网络中的 OSPF 协议进行中继路径选择[16],文献[15]在 OSPF(Open Shortest Path First)协议基础上进一步考虑各链路的有效密钥量来进行路径计算. 韩伟等人[17]根据可信中继 QKD 网络中各链路的量子密钥会先存入两端密钥池的特点,在路由计算中综合考虑密钥池中现有密钥量及链路的密钥生成速率来确定各链路的权重. 石磊等人[18]针对可信中继 QKD 网络中瓶颈链路上密钥容易耗尽的特点,设计了包含若干备选路径的多路径路由选择算法. 上述这些路由方案内的密钥中继都是在 QKD 网络物理拓扑相邻的节点之间进行逐跳式密钥中继,本文将这些路由方案统称为单层逐跳式路由方案,其主要适合于小规模的 QKD 网络,然而,广域 QKD 网络规模大、节点数量多,如果采用单层逐跳式路由方案,可能需要经过很多跳才能到达目的节点,通过分析发现中继跳数过多会降低密钥交换效率. 因此,本文针对基于可信中继的广域 QKD 网络(后文中 QKD 网络均指可信中继广域 QKD 网络)路由问题,从提高密钥交换效率的角度出发,设计了适应广域 QKD 网络的分层路由算法.

2 问题分析

本节从密钥交换原理出发,通过建立密钥交换效率模型给出影响密钥交换效率的主要参数,然后通过对各参数进一步分析找出核心影响因素,最后从提高密钥交换效率角度出发,提出在广域 QKD 网络路由方案中需要解决的问题.

2.1 密钥交换原理介绍

在 QKD 网络中,不同节点根据应用需求通过密钥共享关系联系在一起. 本文将这种密钥共享关系称为密钥链路,相邻节点间通过量子信道建立的密钥链路称为实链路,而远距离节点通过密钥中继建立的密钥链路称为虚链路. 密钥中继过程则可以理解为通过若干实链路构建一条虚链路的过程,这个过程本文称之为密钥交换,其基本原理如图 1 所示.

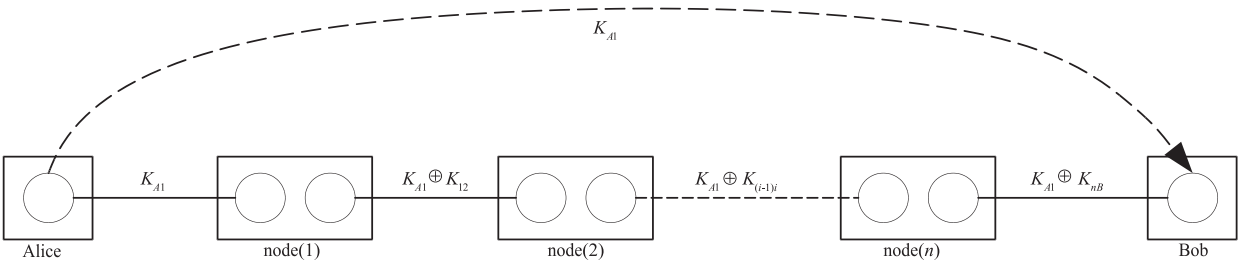

图1 密钥交换原理

假设两个邻近节点 QKD 系统生成的共享密钥为 K_{ij},远距离节点 Alice 和 Bob 密钥分发路径为 Alice→node(1)→node(2)→…→node(i)→…→Bob,则中继步骤如下[19].

步骤 1 Alice 与 node(1)生成共享密钥 K_{A1}.

步骤 2 node(1)利用 OTP(One-Time Password)算法将 K_{A1} 用 K_{12} 加密并传输给 node(2).

步骤 3 node(2)解密并获得 K_{A1},然后重复 node(1)的步骤将 K_{A1} 传递给下一个节点.

步骤 4 直到 Bob 得到 K_{A1} 后整个过程结束. 至此 Alice 和 Bob 获得了密钥 K_{A1}.

在上述步骤中,为了完成密钥交换,沿途密钥链路都需要消耗一定的密钥资源. 而且,Alice 与 Bob 之间虚链路的质量参数,如共享密钥生成速率、生成速率的稳定性等,直接体现了 QKD 网络对外提供密钥服务的能力,而虚链路的质量好坏完全取决于密钥交换的效率. 因此,可以说密钥交换的效率是影响 QKD 网络服务能力的关键因素.

2.2 密钥交换效率分析

2.2.1 密钥交换效率模型

密钥交换效率受多种因素影响. 一方面,从如何影响密钥链路质量的角度来看,单次交换的密钥量、密钥交换耗时等因素直接反应了虚链路的密钥生成速率,密钥交换成功率则会影响虚链路密钥生成速率的稳定性,因此,这些因素必然是分析密钥交换效率不可忽略的对象. 另一方面,从网络密钥资源有效利用来看,成功交换一定密钥量所需要消耗的密钥资源同样是影响密钥交换效率的因素. 综上分析,本文提出如下密钥交

换效率模型:

$$EP(n,L,T,C,p) \tag{1}$$

相关参数含义如下.

(1)密钥交换的中继跳数 n:密钥交换所经过实链路的数量.

(2)密钥交换的密钥量 L:单次密钥交换的最小密钥量. 为了方便讨论,本文假设每次密钥交换只处理一个基本密钥块,其密钥的长度为 L.

(3)密钥交换耗时 T:主要由密钥资源生成时间及密钥块传输处理时间两部分构成. 密钥资源生成时间指每条实链路为完成密钥交换生成足够密钥资源所需要的时间;密钥块传输处理时间指经过的所有实链路传输处理密钥块的时间之和. 为了方便讨论,本文假设各实链路的密钥资源生成时间相同,用 t_g 表示;同时,假设传输处理时间也相同,用 t_r 表示,则成功完成密钥交换的耗时为 $T=t_g+nt_r$.

(4)密钥资源消耗 C:为了完成密钥交换,所有实链路消耗的密钥资源之和. 假设所有实链路处理一个基本密钥块需要消耗的密钥资源为 L,则成功完成密钥交换所消耗的密钥资源为 $C=nL$.

(5)单跳中继成功概率 p:密钥交换成功通过某一条实链路的概率. 密钥交换经过的每一条实链路可能由于单点故障或者密钥资源不足而导致密钥交换失败. 本文假设所有实链路的单跳中继成功概率相同,记失败概率为 $q=1-p$,则密钥交换成功的概率为 $P=p^n$.

最佳密钥交换效率的条件可形式化表示如下:

$$\begin{cases}\max(v),v=L/T\\ \min(C)\\ \max(P),P=p^n\end{cases} \tag{2}$$

2.2.2　密钥交换效率影响因素

由于只有一段时间内密钥交换的累积情况才能真实反应密钥交换的效率,而式(2)中需要考虑累积特性的参数总共有两个:密钥交换耗时 T 及密钥资源消耗 C,下面分别对这两个参数进行详细分析.

(1)密钥交换耗时 T

考虑到单跳中继成功概率 p,单次密钥交换到第 i 跳失败而结束的耗时为 $T'_i=t_g+it_r$,单次密钥交换成功时的耗时为 $T''=t_g+nt_r$,结合第 i 跳失败而结束的概率 $P_i=p^{i-1}q$ 及密钥交换成功的概率 $P=p^n$,可得任意单次密钥交换的平均耗时为

$$\bar{T}=\sum_{i=1}^{n}T'_iP_i+T''P=\sum_{i=1}^{n}(t_g+it_r)p^{i-1}q+(t_g+nt_r)p^n \tag{3}$$

对式(3)进一步求和化简可得

$$\bar{T}=t_g+\frac{1-p^n}{q}t_r \tag{4}$$

由于每一次密钥交换可以看作一个相互独立的随机事件,则直到密钥交换成功时所进行的密钥交换次数属于单次成功概率为 $P=p^n$ 的几何分布,因此,直到密钥交换成功时平均需要进行的密钥交换次数 m 为

$$m=\frac{1}{p^n} \tag{5}$$

则直到密钥交换成功时的平均耗时为

$$T=\bar{T}\times m=\left(t_g+\frac{1-p^n}{q}t_r\right)\times\frac{1}{p^n} \tag{6}$$

(2)密钥资源消耗 C

假设实链路处理一个基本密钥块需要消耗的密钥资源也为 L,则单次密钥交换到第 i 跳失败而结束时需要消耗的密钥资源为 $C'_i=iL$,单次密钥交换成功时需要消耗的密钥资源为 $C''=nL$,考虑到相关的概率因素,可得任意单次密钥交换的平均密钥资源消耗为

$$\bar{C}=\sum_{i=1}^{n}C'_iP_i+C''P=\sum_{i=1}^{n}iLp^{i-1}q+nL \tag{7}$$

进一步化简可得

$$\bar{C}=\frac{1-p^n}{q}\times L \tag{8}$$

结合式(5)可得直到密钥交换成功时的平均密钥资源消耗为

$$C=\bar{C}\times m=\frac{1-p^n}{p^nq}\times L \tag{9}$$

从式(6)(9)中可以看出密钥交换耗时及密钥资源消耗均与多个参数有关,但是,由于 t_g、t_r、L 这三个参数主要与 QKD 网络中所采用的量子密钥生成设备及量子信道的性能、密钥中继使用的 OTP 算法等因素密切相关,因此,对于一个确定的 QKD 网络真正影响密钥交换效率的核心参数主要是密钥中继跳数 n 及单跳中继成功概率 p.

2.3　需要解决的问题

假设 $t_g=10\text{s}$、$t_r=1\text{s}$,则根据式(6)可得密钥交换耗时 T 随 n 和 p 的变化如图 2 所示.

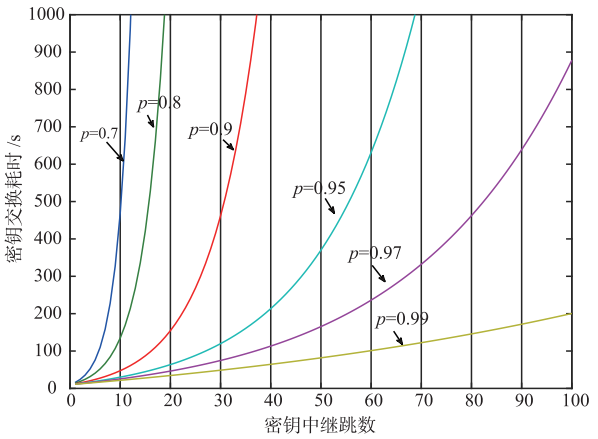

图2　密钥交换耗时

从图 2 可以看出 T 随 n 单调递增,随 p 单调递减. 同样的,可以发现密钥资源消耗 C 与 n 和 p 的关系类似. 因此,为了提高密钥交换效率可以从两个方面入手:①提高单跳中继成功率,②尽可能减少中继跳数.

单跳中继成功概率受 QKD 网络的多方面因素影响,如节点软硬件故障率、经典网络吞吐量等;中继跳数主要与由所选择的中继路径决定,可以通过路由机制来优化. 因此,本文从减少中继跳数角度出发,设计了 QKD 网络分层路由方案,提高密钥交换的效率.

3 分层路由方案设计

考虑到分层的目的是减少中继跳数,因此,本文按照物理位置将各路由节点划分为多个独立区域,便构成分层路由网络的最底层 Level 0 拓扑,然后通过拓扑聚合逐步构建上层网络拓扑,最后设计了分层路由算法.

3.1 基本概念

首先给出一些有关分层网络结构的基本概念方便后文详细描述分层路由方案,相关概念如下所述.

密钥路由节点(Key Routing Node,KRN):在 QKD 网络中完成路由计算、路由信息维护、密钥中继等功能的实体. 在分层 QKD 网络结构中,同一个物理节点可能映射成为不同层的路由节点,从而在多层网络中发挥作用.

密钥路由域(Key Routing Area,KRA):按照物理位置将一些邻近的 KRN 及密钥链路组成相对独立的 QKD 网络子集. 在分层 QKD 网络中,只有处于同一层的路由节点及密钥链路才能组成 KRA.

路由边界节点(Routing Border Node,RBN):每个 KRA 内与同层其他 KRA 相连的 KRN 被称为边界节点. 在分层路由网络结构中,边界节点通常会被抽象为上层 KRA 中的 KRN,不同层之间交互通常在 RBN 内部完成.

路由管理节点(Routing Control Node,RCN):负责对 KRA 内所有 KRN 及 RBN 管理的实体. 在分层路由网络中,除 Level 0 层外其他层 KRA 内的管理节点均从所属下层 KRA 的管理节点中选举产生. 管理节点在分层网络中有着非常重要的作用,其功能包括 KRA 内节点及密钥链路管理、域间路由信息发送及接收、KRA 拓扑抽象管理、协助构建上层 KRA 等.

3.2 分层 QKD 网络结构

在分层路由网络中,每一层均由若干密钥路由域构成,每一个路由域由若干个密钥路由节点及密钥链路构成. 在最底层 Level 0 中,密钥路由节点及密钥链路均是由实际的物理设备及量子信道构成,其拓扑结构反应的是物理设备之间通过量子信道构成的连通关系;在其他 Level i ($i\neq0$)层中,密钥路由节点及密钥链路通过下层网络的密钥路由域抽象而来,一个上层网络路由域中的密钥路由节点可能代表了下层网络中的一个密钥路由域,其拓扑结构反应的是下层网络路由域之间的连通关系. 一个上层网络路由域能够覆盖多个下层网络路由域. 图 3 为一个三层路由 QKD 网络结构示例.

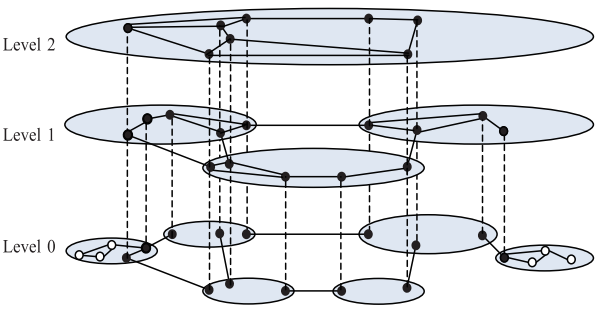

图3 三层路由QKD网络结构示例

图 3 的 QKD 网络是一个由 6 个 Level 0 层路由域构成的复杂 QKD 网络,在 Level 1 层被抽象为三个路由域,最后抽象成一个 Level 2 层的路由域. 对比 Level 0 层与 Level 2 层,节点总数及密钥链路总数大幅减少,远距离节点通过 Level 2 层进行密钥交换时中继跳数远远少于通过 Level 0 层直接进行密钥中继,有利于提高密钥交换效率.

3.3 基于拓扑聚合的分层 QKD 网络构建

3.3.1 拓扑聚合原理

拓扑聚合的目的是将 KRA 内复杂的 QKD 网络拓扑抽象为少量 KRN 及密钥链路构成的简单网络用于上层 KRA 的构建. 拓扑聚合的基本原理是在 RCN 的控制下通过 KRA 内的密钥交换在 RBN 之间建立虚链路,从而将整个 KRA 抽象为由 RBN 及这些虚链路构成的简单网络,最终这个简单网络将成为上层 KRA 拓扑的一部分. 根据上述基本原理,在 RBN 之间虚链路上生成共享密钥时必然会消耗 KRA 内的密钥资源. 此时,RCN 的作用尤为重要,它必须时刻维持 RBN 之间虚链路的密钥生成速率与整个 KRA 网络资源之间的平衡:既不能为了提高 RBN 之间密钥链路的生成速率而过度消耗 KRA 内密钥资源,也不能为了保留 KRA 内密钥资源使得 RBN 之间密钥链路的生成速率过低而影响上层网络的密钥中继. 下面以图 4 所示的 KRA 为例介绍拓扑聚合过程.

图 4(a)为拓扑聚合前 KRA 的网络结构,图 4(b)为拓扑聚合后的网络结构. 拓扑聚合的详细步骤如下.

步骤 1 所有 KRN 必须向 RCN 注册并上报邻近密钥链路信息,方便 RCN 及时掌握整个 KRA 的网络拓扑,确认哪些 KRN 是边界密钥路由节点.

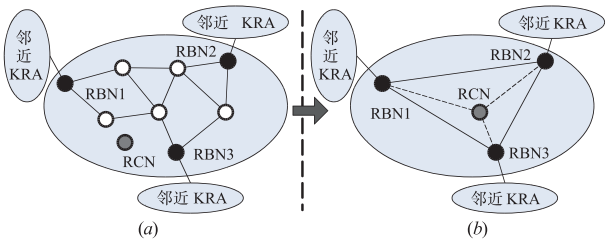

图4　拓扑聚合示例

步骤 2　所有 KRN 周期性地向 RCN 上报邻近密钥链路的状态信息,包括链路的密钥生成速率、剩余有效密钥资源等,从而方便 RCN 确定 RBN 之间虚链路的密钥生成速率,例如可以将 KRA 内密钥链路的平均密钥生成速率的 50% 作为 RBN 之间密钥链路的密钥生成速率.

步骤 3　RCN 根据确定的密钥生成速率,向所有 RBN 周期性发出密钥交换指令,包含密钥交换的目的节点及需要交换的密钥量大小等信息,RBN 根据指令与其他 RBN 建立虚链路. 例如在图 4(*b*)中 RBN1 根据指令分别与 RBN2、RBN3 建立虚链路.

步骤 4　RBN 向 RCN 返回密钥交换的结果,方便 RCN 准确掌握 RBN 之间虚链路的状态.

在上述拓扑聚合过程中还需要配合相应的身份认证措施,确保各节点的真实性、合法性,但由于身份认证并非本文研究重点,上述过程中省略了对相关认证过程的描述. 拓扑聚合后:①在高层 KRA 中密钥中继可以实现一跳跨跃整个下层 KRA,极大减少中继跳数,并且所处的层次越高对应跨跃的 Level 0 范围越广;②各 KRN 只需要存储所处网络分层 KRA 内的路由信息,可以减少节点中的路由项.

3.3.2　分层 QKD 网络的拓扑构建

对于已有的 QKD 网络,采用自底向上逐层聚合的思路从 Level 0 层开始逐层向上构建. 随着网络拓扑聚合层级越来越高,其中 KRA 覆盖的下层网络范围会越来越广,最终聚合到某个高层网络后,只需要一个 KRA 就能覆盖所有下层网络,至止,拓扑聚合结束,整个 QKD 网络的分层网络拓扑构建完成. 其中,通过 Level n 层构建 Level $n+1$ 层的过程如图 5 所示.

下面以图 6 所示的 Level n 层网络拓扑为例详细介绍如何构建 Level $n+1$ 层网络拓扑. 图中所示的 Level n 层网络由三个 KRA 构成,记为 KRA1、KRA2、KRA3,相应的 RCN 记为 RCN1、RCN2、RCN3,这三个 KRA 在 Level $n+1$ 层属于一个 KRA,记为 KRA4.

首先,KRA1、KRA2、KRA3 各自完成拓扑聚合如图 7 所示.

然后,RCN1、RCN2 及 RCN3 根据邻接关系通过经典网络建立连接,假设选举 RCN2 作为 KRA4 的 RCN,

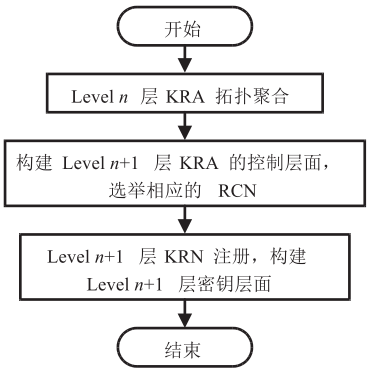

图5　通过Level n层构建Level $n+1$层过程

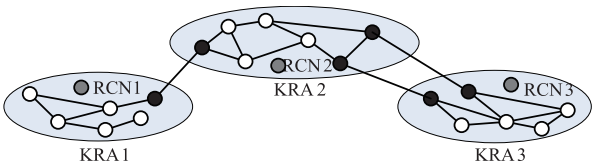

图6　Level n层网络拓扑示例

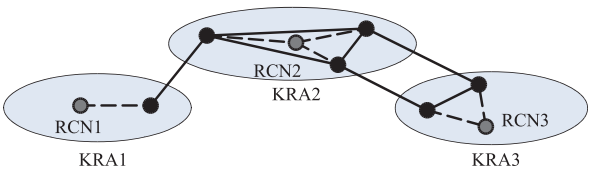

图7　Level n层各KRA聚合后的拓扑结构

记为 RCN4,完成构建控制层面. 最后,RCN4 通过 Level $n+1$ 层控制层面将 Level n 层各 KRA 聚合后的 KRN 注册为 Level $n+1$ 层 KRA4 的 KRN,随后 RCN4 通过 RCN1、RCN2、RCN3 向这些 KRN 下发相应的网络拓扑信息,从而完成构建 Level $n+1$ 层的密钥层面. 如图 8 所示.

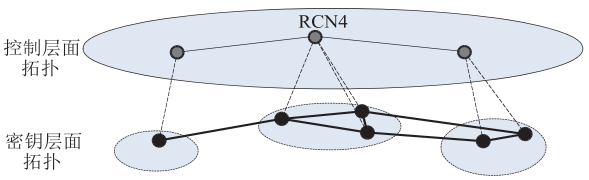

图8　Level $n+1$层的控制层面及密钥层面结构

至此,整个 Level $n+1$ 层便构建完成. Level $n+1$ 层构建好之后的两层网络结构如图 9 所示.

3.4　分层路由方案描述

3.4.1　方案基本思想

分层路由方案分为域内交换及跨域交换两部分,对于域内密钥交换,各路由域可以根据各自情况独立地灵活选择路由协议及算法,获得域内中继路径;对于跨域密钥交换,采用类似于邮件递送的方式. 方案基本思想如图 10 所示.

在分层路由方案中,源节点 SRC 与目的节点 DST

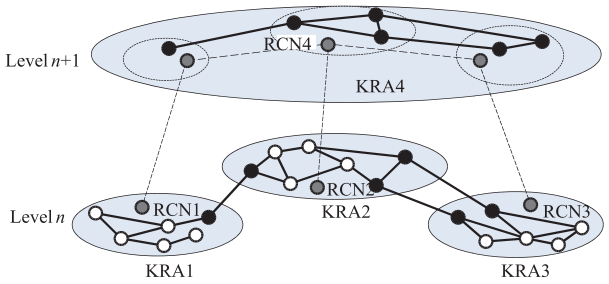

图9 两层网络拓扑示例

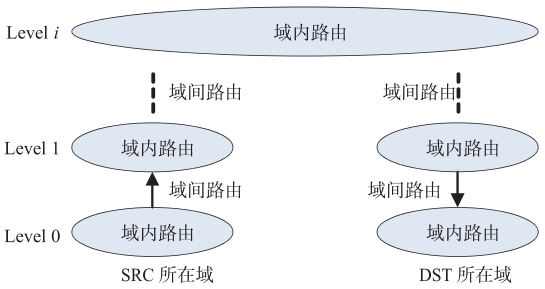

图10 分层路由方案基本思想

不在同一个路由域时,不需要计算到 DST 的完整中继路径,SRC 只需要将密钥交换申请通过 RBN(即上层的 KRN)提交给上层,直到某个上层覆盖了 DST 所在路由域,从而能够完成密钥交换为止,随后将共享密钥向下中继给 DST 所在的下层网络路由域,最终到达 DST 节点. 对于域内路由算法,由于各 KRA 相对独立且范围较小,不同 KRA 可以自由设计或者直接采用现有的一些路由算法(如文献[15~18]的路由算法),在此不作详细研究. 本文主要针对跨多层多域的域间路由问题,设计了相应算法.

3.4.2 基于最低层网络匹配的跨域密钥路由算法

假设各 KRA 内已经定义了各自的域内路由算法,设计了基于最低层网络匹配的跨域路由算法,假设目的节点为 DST,则任意 KRN 计算到 DST 的下一跳路径的基本流程如 11 图所示.

由于每个 KRN 可能会映射到多个分层,因此,当前 KRN 首先从最底层(即 Level 0 层)开始逐层计算当前层 KRA 是否能够覆盖目的节点 DST(如图分支①所示);如果直到当前 KRN 工作的最高层 KRA_{ll}都不能覆盖 DST 时,便将 KRA_{ll}内最近的边界节点 RBN 作为目的节点来计算下一跳节点(如图分支②所示);如果当前 KRN 在某一层(Level i 层)的 KRA 能够覆盖 DST,便在该 KRA 内其他节点中从 Level 0 层开始寻找能够在 Level $j(j\leqslant i)$层 KRA 覆盖 DST 的路由节点,记为集合 A,随后当前 KRN 将 A 集合中最近的节点作为目的节点来计算下一跳(如图分支③所示). 其中几点需要说明:

(1)算法的目标是计算到目的节点的下一跳 KRN

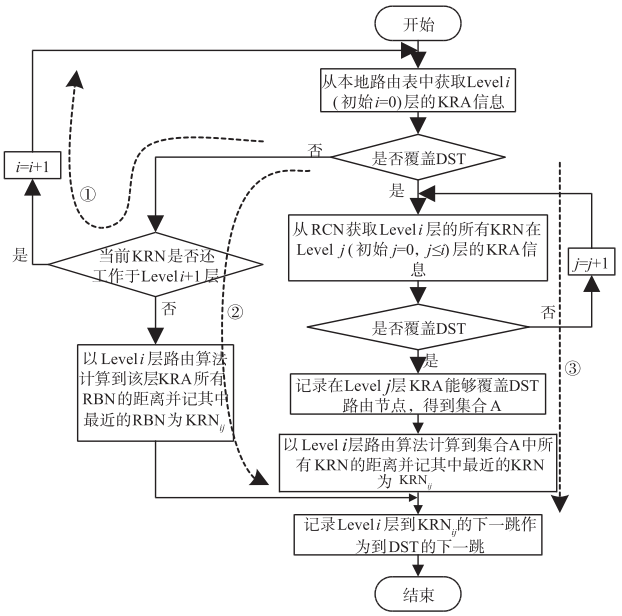

图11 跨域路由算法流程图

而不是完整的中继路径.

(2)由于上层 KRA 内密钥链路上的密钥资源是通过下层网络密钥交换而来,因此越靠上的分层网络内密钥链路上的密钥资源越珍贵. 算法采用自 Level 0 层逐层向上匹配覆盖目的节点的 KRA,能够在一定程度上节省上层网络的密钥资源.

3.4.3 分层路由应用举例

下面通过图 12 的三层 QKD 网络实例详细介绍分层路由方案.

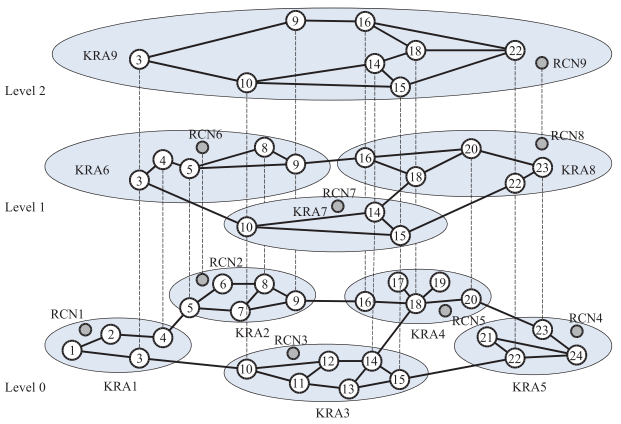

图12 分层路由应用示例网络

在示例网络中,Level 0 层 QKD 网络被划分为 5 个密钥路由域 KRA1~5,其中 KRA1~2、KRA3、KRA4~5 通过拓扑聚合分别被聚合为 Level 1 层的 KRA6、KRA7 与 KRA8,而 KRA6~8 又被聚合为 Level 2 层的路由域 KRA9.

假设源节点 KRN1 与目的 KRN24 之间需要进行密钥交换,则密钥中断路径上各节点计算下一跳的过程

如下.

(1) KRN1 在 Level 0 层通过本地路由表发现 KRN24 与自身并不在同一个 KRA,且 KRN1 只工作于 Level 0 层,因此 KRN1 计算到 KRA1 内最近边界路由节点 KRN3 的路径,可得 KRN1→KRN3.

(2)KRN3 作为工作在多层的密钥路由节点,其计算下一跳的过程可分为两步:

第一步是自底向上确定下一跳 KRN 所在的网络分层. 首先 KRN3 在 Level 0 层计算发现其与 KRN24 并不在同一密钥路由域,说明需要在更高层计算下一跳;最终 KRN3 在 Level 2 层发现所在的路由域能够覆盖 KRN24,因此下一跳应该是 Level 2 层 KRA9 中的密钥路由节点.

第二步是在对应网络分层中计算下一跳 KRN. 首先,KRN3 在 CRN9 的帮助下,从 Level 0 层开始逐层获得 KRA9 中其他密钥路由节点所在低层 KRA 与 KRN24 的关系. 可以发现 KRN22 与 KRN24 在 Level 0 层属于同一密钥路由域 KRA5. 本文采用最低层网络匹配原则,因此不再向上层寻找,则选择 KRN22 作为 KRA9 内的目标节点. 然后,KRN3 在 KRA9 内计算到 KRN22 的密钥中继路径,可得 KRN3→KRN9→KRN16→KRN22,则下一跳为 KRN9.

(3)其他工作在多层的密钥路由节点计算下一跳的过程与 KRN3 类似. 但是,不同节点计算出的中继路径以可能存在差异. 例如 KRN16 在计算下一跳时,发现自身 Level 1 层所在的 KRA 便能覆盖 KRN24,因此会直接在 Level 1 层计算下一跳. 由于 Level 1 层的 KRN22、KRN23 在 Level 0 层与 KRN24 在同一个路由域,因此首先将 KRN22、KRN23 都添加到集合 A 中,接着 KRN16 在 Level 1 层 KRA 中计算发现与距 KRN23 更近,因此计算到 KRN23 的路径,可得 KRN16→KRN20→KRN23,下一跳为 KRN16.

各密钥路由节点按照上述算法计算路径,可得完整密钥交换的路径为:

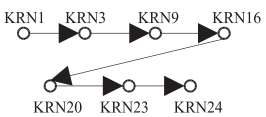

图13　密钥交换的最终路径

原本直接在物理拓扑(即 Level 0 层)中需要跨跃多个路由域(KRA2、KRA3 及 KRA4)才能完成的密钥交换,在分层网络中只需要 7 跳就可以完成. 可以看出,分层路由方案可以极大的减少密钥交换的中继跳数,有利于提高密钥交换效率.

4　仿真分析对比

考虑到广域 QKD 网络的网络规模较大,受实验环境限制并不能搭建真实的网络进行测试,因此,本文采用 OPNET 网络仿真软件进行仿真测试.

4.1　仿真环境及参数设置

本文仿真测试网络由 18 个 Level 0 层密钥路由域 KRA0 ~ 17 组成三层 QKD 网络. 在 Level 0 层,各密钥路由域之间按照格形网方式连接. 其中,KRA0 ~ 8 这 9 个密钥路由域通过拓扑聚合构成 Level 1 层的 KRA18;KRA9 ~ 17 这 9 个密钥路由域通过拓扑聚合构成 Level 1 层的 KRA19. 随后,KRA18 及 KRA19 这两个密钥路由域通过拓扑聚合构成 Level 2 层的 KRA20. QKD 网络结构及各密钥路由域之间的拓扑关系如图 14 所示.

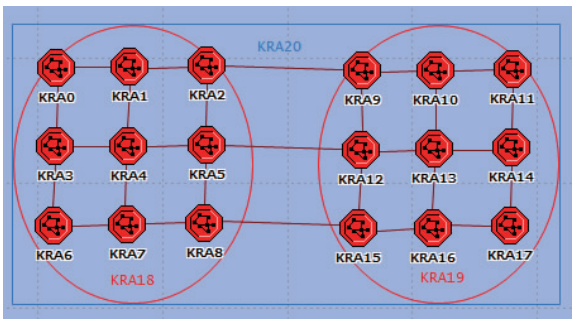

图14　仿真网络路由域划分

图 14 上每个 Level 0 层密钥路由域均由 16 个密钥路由节点 KRN0 ~ 15 及一个管理节点 RCN 构成. 这些节点通过一个网络路由“classical router”连接到同一个经典网络中. 各密钥路由节点 KRN0 ~ 15 通过量子信道同样按照格形网结构连接,例如 KRA0 的网络拓扑如图 15 所示. 因为 QKD 网络中通过量子信道生成量子密钥的过程并不属于本文探讨的重点,因此,本文在仿真过程中每个 KRN 的进程模型为每个邻接的密钥链路维护一个整型变量来模拟密钥池,并通过变量值的增减来模拟密钥生成及消耗过程,例如,周期性地根据密钥链路的生成速率增加该变量值可以模拟密钥生成,根据密钥交换的密钥量来减少该变量值可以模拟中继过程的密钥资源消耗.

在仿真过程,每个 KRN 都连接一个密钥用户并且随机的向其他任意用户发出密钥交换,各量子信道的密钥生成速率为 10 ~ 20kbps 之间的随机整数值. 另外,每个密钥路由域内采用改进的 OSPF 路由协议,即在 OSPF 协议基础上进一步考虑各链路的有效密钥量来进行路径计算.

4.2　仿真结果分析

为了检验本文路由方案的有效性及可行性,展现其优越性,同时考虑到密钥交换效率的主要影响因素,仿真实验主要针对网络整体性能进行测试,分别对密钥资源利用率及密钥服务延时两个参数进行了检测,并与单层逐跳式路由方案(如文献[15 ~ 18]中所使用

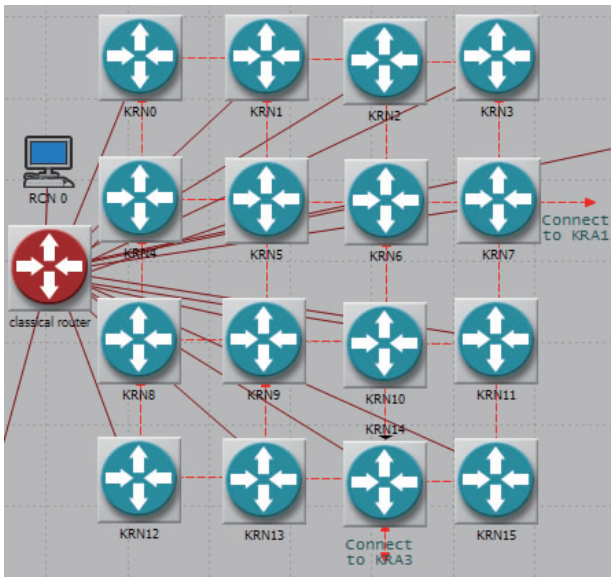

图15 路由域KRA0内详细拓扑

的方案)进行了相关对比分析.

4.2.1 密钥资源利用率

密钥资源利用率是一定时间内 QKD 网络向用户输出的总密钥量与这段时间内整个网络所消耗的密钥资源总和的比值,该指标反应了整个 QKD 网络有效输出密钥的效率. 仿真过程中取时间间隔为 1 分钟,并且统计在这段时间内 QKD 网络所有实链路生成的密钥资源总和及所有用户节点成功完成密钥中继的总密钥量,最后计算两者比值. 仿真时长 10 小时的测试结果如图 16 所示.

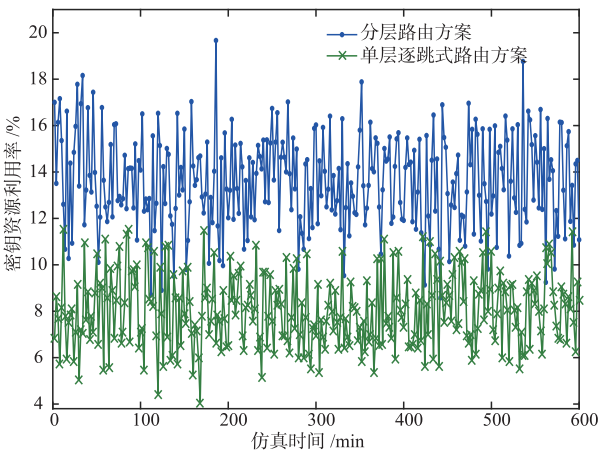

图16 密钥利用率仿真结果

从图 16 可以看出,在实验网络中密钥资源利用率整体都比较低,不到 20%,也就是说成功中继一定量的密钥,需要消耗的密钥资源相对比较大. 但是,从仿真结果可以看出,本文方案密钥资源利用率平均为 13.5%,相对于而单层逐跳式路由方案 7.6% 的利用率,提高 77.6%. 其主要原因可能是通过分层路由大大降低了由于密钥交换失败导致的无意义密钥资源消耗量,提高了密钥资源利用率.

4.2.2 密钥服务延时

密钥服务延时指从用户发出密钥交换申请到最终与远端用户成功完成密钥交换为止所需要的时间,它从时效性方面反应了 QKD 网络对外提供密钥服务的性能. 本文仿真实验在其他节点工作过程不变的情况下,通过选取并测试两个固定节点间的密钥服务延时来获得需要的实验数据. 数据采集过程如下:选择距离最远的两个密钥路由节点 KRA0 中的 KRN0 与 KRA17 中的 KRN15,然后这两个密钥路由节点的用户在随机时间间隔的情况下相互申请密钥交换,最后采集 100 次成功密钥交换的服务延时,测试结果如图 17 所示.

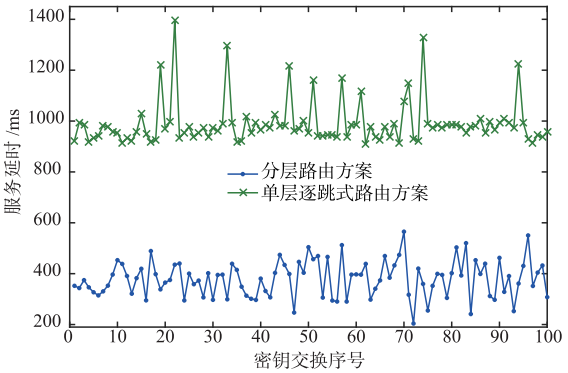

图17 密钥服务延时仿真结果

从图 17 中可以看出,单层逐跳式路由方案密钥服务延时相对平稳,平均延时大约为 950ms,而本文的分层路由方案密钥服务时间虽然波动范围稍大,但是平均延时大约为 400ms,服务延时缩短了一半.

5 结束语

本文对基于可信中继的广域 QKD 网络路由问题进行了研究,针对现有相关路由方案存在的密钥交换效率低、密钥资源无意义消耗大的问题提出了一种基于拓扑聚合的分层路由方案. 该方案根据节点物理位置将广域 QKD 网络划分为不同路由域,并且通过拓扑聚合构建分层 QKD 网络,设计了分层 QKD 网络路由算法,极大的降低了远距离节点间密钥中继的路径长度,提高了密钥交换效率. 仿真实验表明,与单层逐跳式路由方案相比,分层路由方案能够显著提高 QKD 网络密钥资源利用率,降低密钥服务延时.

参考文献

[1] Bennett C H, Brassard, G. Quantum cryptography: Public key distribution and coin tossing[A]. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing[C]. Bangalore, India: IEEE Press, 2014.

175 – 179.
[2] 马瑞霖. 量子密码通信[M]. 北京:科学出版社,2006.
[3] Zhang S B,Xie Z H,Li L L,et al. Study on quantum trust model based on node trust evaluation[J]. Chinese Journal of Electronics,2017,26(3):608 – 613.
[4] Wan X J,Chen Y Z,Jiang L,et al. UnionPay payment scheme based on controlled quantum teleportation[J]. Chinese Journal of Electronics,2020,29(3):533 – 539.
[5] 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,(2):22 – 24,60.
Wu Z B,Chen G,Yang B J. Analysis of quantum key distribution networks[J]. Study on Optical Communications,2009,(2):22 – 24,60. (in Chinese)
[6] Nicol'o L P,et al. Long-distance trust-free quantum key distribution[J]. IEEE Journal of Selected Topics in Quantum Electronics,2015,21(3):6600508.
[7] 王华,赵永利. 量子密钥分发城域光组网技术前瞻[J]. 通信学报,2019,40(9):168 – 174.
Wang H,Zhao Y L. Overview of quantum key distribution metropolitan optical networking technology[J]. Journal on Communications. 2019,40(9):168 – 174. (in Chinese)
[8] Peev M,Pacher C,Alléaume R,et al. The SECOQC quantum keydistribution network in Vienna[J]. New Journal of Physics,2009,11(7):075001.
[9] Ghernaouti-Helie S,Tashi I,Laenger T,et al. SECOQC Business White Paper[R]. Paris,France:SECOQC,2008.
[10] 许华醒. 量子通信网络发展概述[J]. 中国电子科学研究院学报,2014,9(3):259 – 271.
Xu H X. Overview of the development of quantum communication networks[J]. Journal of China Academy of Electronics and Information Technology,2014,9(3):259 – 271. (in Chinese)
[11] Sasaki M,Fujiwara M,Ishizuka H,et al. Field test of quantum key distribution in the Tokyo QKD network [J]. Optics Express,2011,19(11):10387 – 10409.
[12] 高芳,徐峰. 全球量子信息技术最新进展及对中国的启示[J]. 中国科技论坛,2017,5(6):164 – 170.
Gao F,Xu F. The latest development of global quantum information technology and its implications to China[J]. Forum on Science and Technology in China,2017,5(6):164 – 170. (in Chinese)
[13] Ding H J,Liu J Y,Zhang C M,et al. Predicting optimal parameters with random forest for quantum key distribution [J]. Quantum Information Processing,2020,19(2):1 – 8.
[14] Liu J Y,Ding H J,Zhang C M,et al. Practical phase-modulation stabilization in quantum key distribution via machine learning [EB/OL]. https://arxiv. org/abs/1906.06681. 2020-11-05.
[15] Tanizawa Y,Takahashi R,Dixon A R. A routing method designed for a Quantum Key Distribution network[A]. Proceedings of Eighth International Conference on Ubiquitous and Future Networks[C]. Vienna,Austria:IEEE,2016. DOI:10.1109/ICUFN.2016.7537018.
[16] Dianati M,Alléaume R,Gagnaire M,et al. Architecture and protocols of the future European quantum key distribution network[J]. Security & Communication Networks,2007,1(1):57 – 74.
[17] 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 – 48,94.
Han W,Wu X R,Zhu Y,et al. QKD network routing research based on trust relay[J]. Journal of Military Communications Technology,2013,34(4):43 – 48,94. (in Chinese)
[18] 石磊,苏锦海,郭义喜. 量子密钥分发网络端端密钥协商最优路径选择算法[J]. 计算机应用,2015,35(12):3336 – 3340,3397.
Shi L,Su J H,Guo Y X. Optimal routing selection algorithm of end-to-end key agreement in quantum key distribution network[J]. Journal of Computer Applications,2015,35(12):3336 – 3340,3397. (in Chinese)
[19] Yan S L,Wang J D,Fang J B,et al. An improved polar codes-based key reconciliation for practical quantum key distribution[J]. Chinese Journal of Electronics,2018,27(2):250 – 255.

作者简介

杨　超　男,1988 年 4 月出生,四川巴中人. 2018 年毕业于战略支援部队信息工程大学,获博士学位,主要研究方向为信息安全、量子密钥分发、科学可视化.
E-mail:ych8988@163.com

张红旗　男,1962 年 10 月出生,河北唐山人. 教授,博士生导师,主要研究方向为可信计算、网络安全、安全管理.