

基于密钥中继的广域量子密钥网络路由方案

杨超¹, 张红旗¹, 苏锦海¹, 陈华城²

(1. 信息工程大学, 河南 郑州 450004;

2. 解放军 73503 部队, 福建 福州 350001)

摘要: 针对现有基于密钥中继的 QKD 网络路由方案存在适用范围有限、不能满足广域环境路由需求的问题, 分析了广域 QKD 网络路由特点并提出了相应的路由需求, 进而设计了基于虚链路的分域量子密钥网络路由方案。将广域 QKD 网络划分为多个小规模密钥路由域, 降低了域内密钥路由的复杂度, 通过建立跨越密钥路由域的虚链路缩短了域间路由长度, 从而提高了广域环境下密钥路由效率。理论分析表明, 该方案具有路由更新收敛快、路由时延小、密钥资源消耗少的优点。

关键词: 量子密钥分发; 广域 QKD 网络; 密钥中继; 路由方案

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00215

Routing scheme for key-relaying-based quantum key distribution network in wide-area

YANG Chao¹, ZHANG Hong-qi¹, SU Jin-hai¹, CHEN Hua-cheng²

(1. Information Engineering University, Zhengzhou 450004, China;

2. 73503 PLA Troops, Fuzhou 350001, China)

Abstract: The existing routing schemes for key relaying QKD network had a limited scope of application and could not satisfy the requirements of the routing issue of wide-area QKD network. A multi-domain routing scheme based on visual link was proposed for QKD network after the analyzing of the characteristics of QKD network and the proposing of the design requirements of routing issue. In this routing scheme, the QKD network was divided into multiple routing areas to reduce the complexity of intra-domain routing, and a visual QKD link striding over the whole key routing area was built to shorten the routing path. Therefore, the routing efficiency can be increased by this scheme. After theoretical analysis, the proposed routing scheme has advantages of fast convergence of routing update, little time delay and low key material cost.

Key words: quantum key distribution, wide-area QKD network, key relaying, routing scheme

1 引言

量子密钥分发 (QKD, quantum key distribution) 技术^[1]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。其安全性依赖于量子力学基本原理^[2,3], 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

收稿日期: 2017-09-16; 修回日期: 2017-11-02。通信作者: 杨超, ych8988@163.com

基金项目: 国家高技术研究发展计划基金资助项目 (No.2014AA7116082, No.2015AA7116040)

Foundation Item: The National High Technology Research and Development Program of China (No.2014AA7116082, No.2015AA7116040)

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^[4]。

国内外已经提出的 QKD 网络组网方式可分为 3 类^[5]：光学节点 QKD 网络、量子节点 QKD 网络以及信任节点 QKD 网络。其中，由光学节点和量子节点构成的 QKD 网络均是在量子密钥生成层根据用户需要，通过灵活地在不同节点构建临时量子信道并直接生成点对点的量子密钥，可以实现多用户、远距离量子密钥分发，然而受量子信号衰减的影响，光学节点 QKD 网络主要适用于构建局域网的 QKD 网络，另外，由于量子存储等关键技术还不成熟，使量子节点 QKD 网络目前还处于实验阶段；由信任节点构成的 QKD 网络则是在量子密钥生成层之上通过密钥数据的逐跳中继实现多用户、远距离密钥分发，因此它本质上属于一种密钥中继 QKD 网络，这种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的广域量子密钥网络组网方式^[6]。因此，本文主要以基于密钥中继的 QKD 网络为对象展开相关研究，下文的量子密钥网络均指基于密钥中继的 QKD 网络。

路由选择作为伴随网络建设过程的一个与生俱来问题，在 QKD 网络建设中同样无法回避，但目前在 QKD 网络相关研究中路由问题并没有得到足够的重视^[7]，研究成果较少。当前，在有关密钥中继 QKD 网络路由问题的研究成果中，既有希望最大限度利用经典网络中成熟路由技术的路由方案，也有根据密钥中继 QKD 网络特点设计路由算法、协议的路由方案。例如，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^[8]；文献[7]在 OSPF 协议基础上进一步考虑各链路的有效密钥量进行路径计算；韩伟等^[9]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^[10]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。上述路由方案都是直接在点到点量子密

钥分发系统上进行的逐跳式密钥中继（本文将其称为全网直接路由方案），在路径计算过程中对网络的链路状态（如链路有效密钥量）掌握的准备性要求较高。然而，在广域 QKD 网络中，网络规模大、节点数量多，网络状态更新收敛较慢，因此上述方案主要适用于小范围的 QKD 网络路由。因此，研究高适用于广域 QKD 网络路由技术具有重要的现实意义。

本文在深入分析广域 QKD 网络路由面临的问题基础上设计了基于虚链路的分域量子密钥网络路由方案。通过划分路由域、构建虚链路，避免在复杂的整个广域 QKD 网络范围内直接计算路由，降低了实际路由计算的 QKD 网络规模，能够更好地解决广域环境下 QKD 网络路由问题。

2 量子密钥网络介绍

当前，在基于密钥中继的量子密钥网络相关技术研究中，对很多基本概念、原理的理解还不完善，描述比较模糊。因此，本节对一些主要技术基础进行了重新描述与界定，以方便后续工作的展开。

2.1 密钥中继

通过量子信道为通信双方生成共享密钥的方式可以称为一种直接量子密钥分发，光学节点及量子节点 QKD 网络即属于直接量子密钥分发网络；密钥中继则可以称为一种间接量子密钥分发，它利用多个量子信道上已经生成的量子密钥，并采用一次一密的方式保护用户的通信密钥，经过逐跳接力传递的方式为通信双方生成共享密钥。直接量子密钥分发过程中需要一条完整的量子信道，但由于信道物理特征及当前技术条件的限制，在构建 QKD 网络过程中也受到诸多制约。然而，密钥中继需要的不是完整量子信道，而是多段相对独立的量子信道，在当前技术条件下更容易实现，构建 QKD 网络更加方便、灵活。密钥中继的基本原理可由图 1 表示。

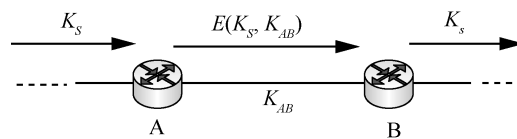


图 1 密钥中继基本原理

假设最终分发给通信双方的共享密钥为 K_s (用户密钥), 该密钥可以由中继路径上的某一段链路生成; AB 段链路生成的量子密钥分别为 K_{AB} (链路密钥), 则将 K_s 通过密钥中继从节点 A 传递到节点 B 的过程为: 节点 A 采用 AB 段的链路密钥对 K_s 进行加密 $E(K_s, K_{AB})$, 其中 E 为一次一密加密算法, 然后将密文传递给节点 B; 节点 B 用 K_{AB} 解密便可以得到 K_s , 根据需要, 节点 B 还可以按同样的方法将 K_s 传递给下一个节点。

从上述原理可以看出: 1) K_s 受到链路密钥 K_{AB} 的保护, 并且采用一次一密的加密算法 E , 在传输过程中可以保证 K_s 的安全性, 防止第三方外部窃听、破译; 2) 密钥中继经过的每一段链路都会消耗一定密钥量, 并且消耗的密钥量与加密算法及传输的用户密钥量有关; 3) 应该有相应的措施防止第三方从系统内部窃取用户密钥, 如通过节点 A 或 B 直接窃取 K_s , 最简单的方法是确保节点 A、B 的绝对可信 (这种方式也被称为可信中继), 但这并不是唯一的方法, 目前比特传输^[11]、异或存储、随机路由^[12]、多路径路由^[13]等相关方案已经能够部分或者完全解决系统内部泄露用户密钥的问题。

2.2 量子密钥网络

BB84^[1]、B92^[14]、基于诱骗态方案^[15]等现有量子密钥分发协议^[16,17]在通过量子信道生成密钥的过程中无一不依靠经典网络完成, 因此, 量子密钥网络的运行也必然依靠经典网络支撑, 甚至可以把它看作经典网络上的一种服务于其他应用系统的网络系统。图 2 详细描述了量子密钥网络基本结构, 展示了量子密钥网络与经典网络的关系。

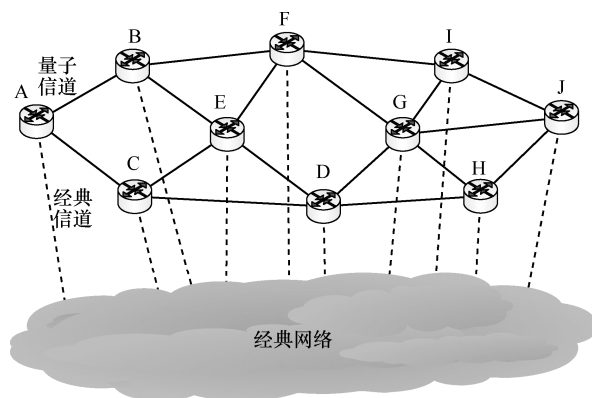


图2 量子密钥网络基本结构

量子密钥网络由2种信道构成: 经典信道、量子信道。其中, 经典信道将各节点连接到同一经典网络, 用于传输量子密钥分发过程中的各种控制、协商、检验报文及密钥中继中的密文; 量子信道连接相邻节点并构成“量子信道网”, 主要用于传输量子信号及生成量子密钥。从经典信道的角度来看, 所有节点都能够与任何其他节点进行通信, 属于全连通网络; 但从量子信道的角度来看, 只有具备量子信道的邻节点间才能传输量子信号, 整个网络拓扑唯一确定。正是这个唯一确定的“量子信道网”决定了密钥中继必须沿着量子信道传输用户密钥, 不能随意传输给其他节点, 因此, 本文所研究的量子密钥网络主要指“量子信道网”。

3 量子密钥网络路由特点分析

经过数十年的研究与发展, 经典网络路由技术已经非常成熟。本节通过对比量子密钥网络路由与经典网络路由, 分析量子密钥网络路由的特征及面临的问题, 进而提出量子密钥网络路由的设计需求, 为下文广域量子密钥网络路由方案的提出奠定基础。

3.1 与经典网络路由对比

经典网络以存储转发原理为基础, 量子密钥网络以密钥中继为基础。存储转发与密钥中继的不同使经典网络路由与量子密钥网络路由之间有很大的区别。下面分别从传输内容、传输能力、传输速率等方面对经典网络路由与量子密钥网络路由进行对比分析。

1) 传输内容。存储转发过程中以分组报文作为传输对象, 转发报文时主要关注报文头部的相关字段便可以查找下一跳, 对于报文的数据部分并不需要做太多处理。然而, 密钥中继时还需要对报文数据进行相关的密码运算, 必然会增加节点传输数据的处理开销。

2) 传输能力。在经典网络中, 带宽用来表示网络传输数据的能力, 虽然存储转发数据时会占用一定的带宽, 但是网络的总带宽主要与网络的物理性能有关, 因此带宽可以当作一个固定值。相应地, 链路密钥生成速率可以看作是量子密钥网络中的带宽 (可以称为密钥带宽), 然而由于量子信道受物理环境影响较大, 密钥带宽并不稳定, 甚至波动

较大。另外, 由于链路密钥池的影响, 池中的有效密钥能够随时使用, 从而转变为密钥带宽, 使量子密钥网络的密钥带宽随时变化且通常变化很大。

3) 传输速率。在存储转发过程中, 数据的传输速率主要与光/电信号在介质中的传送速率及采用的信息编码方法有关, 同样可以当作固定值。在密钥中继过程中, 数据传输速率不仅与经典网络中传送的耗时有关, 还与链路密钥池中的有效密钥量有关, 特别是当池中有效密钥量不足时, 需要等待量子信道生成足够的链路密钥, 极大影响了传输速率。

4) 传输成功率。密钥中继及存储转发的成功率均受网络拥塞状态、误码率等因素影响, 但由于量子密钥网络的密钥带宽、传输速率波动较大, 必然会影响网络的拥塞状态, 使密钥中继成功率变得不稳定, 波动性较大。

经过上述分析可以发现, 经典网络路由与量子密钥网络路由虽然在某些方面有一定的相似之处, 但量子密钥网络路由受到的影响因素更复杂。

3.2 量子密钥网络路由问题分析

3.2.1 路由时延

路由时延由链路密钥生成时间及传输处理时间 2 部分构成。链路密钥生成时间指链路为完成密钥中继生成一定密钥资源所需要的时间, 因为各链路独立并行工作, 所以其取值为各段链路中生成密钥资源的最大耗时, 用 t_g 表示; 传输处理时间指用户密钥从源节点逐跳传输到目的节点所需的时间, 由于传输过程依靠经典网络完成, 传输处理时间受经典网络性能影响较大, 假设单跳的传输处理最大时间为 t_r , 则完成 i 跳路由的时延为

$$T_i = t_g + it_r \quad (1)$$

假设路径长度为 n , 单跳中继成功概率 p , 则中继到第 i 跳失败而结束的概率 $P_i = p^{i-1}q$, 密钥路由成功的概率 $P = p^n$, 可得任意单次路由的平均耗时为

$$\bar{T} = \sum_{i=1}^{n-1} T_i P_i + T_n P = \sum_{i=1}^{n-1} (t_g + it_r) p^{i-1} q + (t_g + nt_r) p^n \quad (2)$$

对式(2)进一步求和化简可得

$$\bar{T} = t_g + \frac{1-p^n}{q} t_r \quad (3)$$

由于每一次密钥中继可以看作一个相互独立

的随机事件, 则直到密钥路由成功时所需要的密钥中继次数服从单次成功概率 $P = p^n$ 的几何分布, 因此, 直到密钥路由成功时, 平均需要进行的密钥中继次数 m 为

$$m = \frac{1}{p^n} \quad (4)$$

则直到密钥路由成功时的平均耗时为

$$T = \bar{T}m = \left(t_g + \frac{1-p^n}{q} t_r \right) \frac{1}{p^n} \quad (5)$$

从式(5)可以看出, 路由时延与路径长度 n 及单跳中继成功概率 p 关系非常密切。

3.2.2 密钥资源开销

假设密钥中继 L 长度的密钥量时, 每经过一段链路消耗 l 长度的密钥资源, 则密钥中继到第 i 跳时需要消耗的密钥资源为

$$C_i = il \quad (6)$$

与路由时延类似, 考虑到相关的概率因素, 可得任意单次路由的平均密钥资源消耗为

$$\bar{C} = \sum_{i=1}^{n-1} C_i P_i + C_n P = \sum_{i=1}^{n-1} il p^{i-1} q + nlp^n \quad (7)$$

进一步化简可得

$$\bar{C} = \frac{1-p^n}{q} l \quad (8)$$

结合式(4)平均密钥中继次数 m 可得直到密钥路由成功时的平均密钥资源消耗为

$$C = \bar{C}m = \frac{1-p^n}{p^n q} l \quad (9)$$

从式(9)可以看出, 密钥资源开销同样与路径长度 n 及单跳中继成功概率 p 关系非常密切。

3.2.3 广域量子密钥网络路由特点

由于量子密钥网络路由的目的是为传输密钥这种不确定性信息选择合适的路径, 而密钥中继过程又必须沿着量子信道传输, 使量子密钥网络路由虽然根据量子信道构成的网络选择路径, 但却需要依靠经典网络完成报文转发、传输。这种路径选择与数据传输分离的现象以及广域量子密钥网络规模大、节点多、用户多的特点使广域量子密钥网络路由具有许多自身的特点。

1) 网络状态变化快。通过前文与经典网络路由对比可以发现, 很多与量子密钥网络路由密切

相关的重要网络状态参数处于时刻变化之中，特别是链路密钥带宽随着量子信道生成及密钥中继消耗变化得更快，并且毫无规律。

2) 路由延迟变化大。从式(1)中可以看出，路由延迟随着路径长度呈线性增加，而 t_r 本身就受经典网络的拥塞状态影响。另外加上路由成功的概率因素，使时延变化范围更大。

3) 密钥资源消耗大。当前，由于通过量子信道生成密钥的速率相对较低，链路可用密钥变得非常珍贵。因此，相对于计算、存储等网络资源来说，链路密钥消耗问题在量子密钥网络路由开销中更加重要。从式(6)中可以看出，密钥资源消耗同样与路径长度呈线性增加。广域环境下，通常需要经过很多跳才能到达目的节点，需要消耗的密钥资源必然很大，再加上路由成功概率因素的存在，造成密钥资源无意义消耗，使密钥资源消耗更大。

3.3 广域量子密钥网络路由设计需求

通过上述对量子密钥网络路由特别是广域环境下路由特点的分析，笔者认为广域量子密钥网络路由主要应该满足以下需求。

1) 具有较高的更新频率，能够实现网络拓扑、状态变化等信息快速更新，使路由更新过程能够快速收敛。

2) 能够减少密钥资源无意义消耗，提高链路密钥资源利用率。

3) 能够实现网络负载均衡，充分利用链路密钥资源，提高量子密钥网络整体性能。

4 广域量子密钥网络路由方案

广域环境下网络规模大、路由距离较远等特征使广域量子密钥网络路由出现上述特点。经典网络中通常采用划分自治系统（路由域）的方法解决大规模网络中的路由问题。然而，受光量子传输衰减的影响，单条量子信道的物理距离有限，使量子密钥网络中的路由跳数与实际物理距离密

切相关，因此单纯采用划分路由域的方法并不能减少量子密钥路由跳数，无法满足广域量子密钥网络路由设计需求。本节提出基于虚链路的分域量子密钥网络路由方案，通过划分路由域、构建虚链路减少路由跳数。

4.1 方案基本思想

从密钥中继原理可知，量子密钥网络路由过程可分为2个阶段：第一阶段为各量子信道为邻近节点生成链路密钥，第二阶段为通过密钥中继完成源节点及目的节点密钥传输。本文设计的路由方案在上述2个阶段中增加1个阶段，该阶段将较长的路径划分为多段，每段内部通过密钥中继为首尾节点建立一条虚链路，源节点与目的节点间通过这些虚链路进行密钥传输，其基本思想描述如图3所示。

假设源节点 S 与目的节点 D 之间需要经过若干中间节点 $V1, V2, V3, V4, \dots$ ，相邻节点间均存在量子信道，阶段2可以描述如下。当 S 向 D 传输用户密钥时，首先将路径 $p = (S, V1, V2, V3, \dots, D)$ 划分为若干短距离的路由段，如图3中 $p1 = (S, V1, V2, V3, V4)$ ， $p2 = (V4, V5, V6, V7, V8)$ 等，然后各路由段内部通过密钥中继建立虚链路，获得量子密钥（同样称为链路密钥），如 K_{s4} 、 K_{48} 等，从而将路径转变为 $p' = (S, V4, V8, \dots, D)$ ，最终从 S 向 D 的用户密钥传输在 p' 上完成。通过增加阶段2缩短了密钥路由跳数，可以提高密钥路由的效率。

4.2 基于虚链路的分域量子密钥网络路由方案

4.2.1 方案描述

根据方案基本原理，将整个广域量子密钥网络分为多个相对独立的密钥路由域（KRA, key routing area），如图4的量子密钥网络被划分为7个密钥路由域 KRA1~KRA7。因此该方案也由2部分组成：1) 域内密钥路由，如图4中 KRA1 内的 $S1$ 与 $D1$ 之间的用户密钥传输；2) 域间密钥路由，如图4中 KRA3 内的 $S2$ 与 KRA7 内的 $D2$ 之间的用户密钥传输。

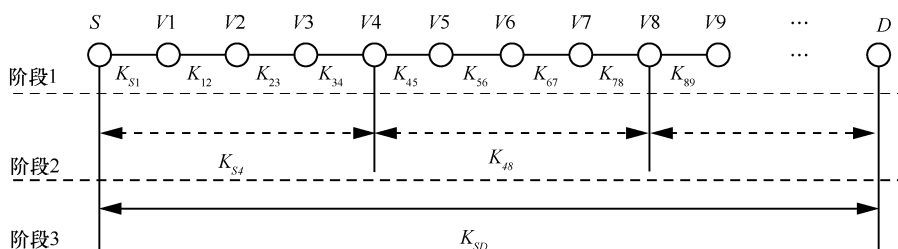


图3 广域量子密钥网络路由方案基本原理

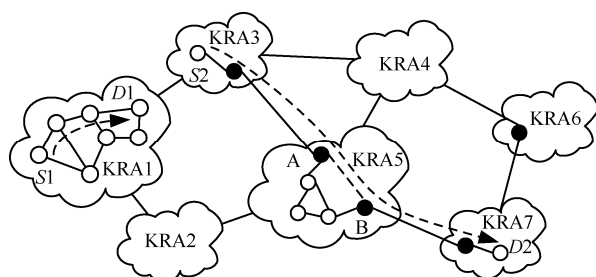


图 4 量子密钥网络分域拓扑示例

1) 域内密钥路由

源节点及目的节点属于同一个 KRA 的密钥路由过程称为域内密钥路由。不同的 KRA 可以根据自身情况选择不同的路由协议及算法，但是不管采用哪种路由协议及算法，所选择的传输路径中所有节点必须同样属于该 KRA，并且路径中的每一条链路也必须由真实的量子信道构成。域内密钥路由属于小范围网络路由，其路由延迟、密钥资源消耗都不大，路由收敛速度也比较快。

2) 域间密钥路由

源节点及目的节点属于不同 KRA，密钥传输需要跨过多个 KRA 的密钥路由过程称为域间密钥路由。在域间密钥路由中，每个 KRA 的边界节点之间通过密钥中继建立一条虚链路，从而通过一条链路便可以跨过整个密钥路由域。例如，图 4 中 KRA5 内的节点 A 与节点 B 之间建立虚链路之后，原本 KRA3 内的 S2 与 KRA7 内的 D2 之间传输用户密钥需要通过 KRA5 中的很多链路，现在只需要通过 AB 这一条虚链路就行。需要说明的是，虚链路的构建需要采用域内密钥路由生成虚链路的密钥资源。

4.2.2 密钥路由域划分

经典网络根据路由器采取的路由选择协议划分自治系统（路由域），与路由器所处的物理位置无关。在广域量子密钥网络中，划分密钥路由域的目的是减少密钥路由跳数，因而本文按照节点所处的物理位置划分密钥路由域。在广域量子密钥网络建设之前，各密钥路由域可以提前规划好，节点之间通过标识判定是否属于同一个路由域。节点标识定义如下。

$$NID ::= \{ < KRAID >, < HID > \} \quad (10)$$

其中，NID 为一个 32 bit 的无符号整型数，由 2 部分构成：节点所在的路由域的标识 KRAID 及节点的主机号 HID。

除了节点标识，还会为每个节点设置一个密钥路由域掩码 KRAMASK，用于指示 NID 的前多少位表示密钥路由域标识。值得说明的是，整个量子密钥网络中所有节点的 KRAMASK 是相同的，当节点之间进行路由信息交换时，可以方便节点识别其他节点的 KRAID。

4.2.3 节点路由模块组成

节点的路由模块如图 5 所示，主要由以下几部分组成：路由信息数据库、路由表查询、路由计算、网络状态更新。

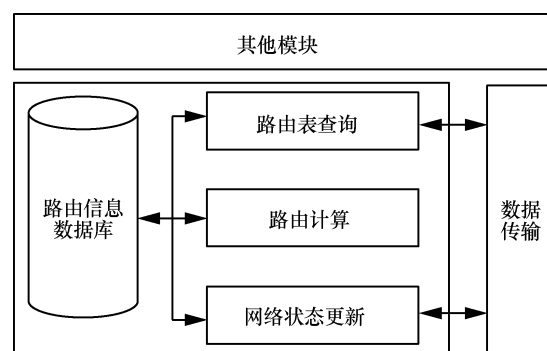


图 5 路由模块组成

整个路由模块主要围绕路由信息数据库进行工作，首先通过网络状态更新组件收集所属 KRA 内详细拓扑并定期更新各链路的状态，边界节点还需要收集各 KRA 之间的连接状态信息及对应虚链路的状态；然后由路由计算组件实时计算并更新路由表；当需要传输数据时则通过路由表查询组件获得下一跳节点信息。

4.2.4 路由信息数据库

节点需要存储的路由信息主要包括本地配置、网络拓扑、链路状态和路由表。本文设计的数据库结构如图 6 所示。

其中，网络拓扑信息按节点信息 (Node_Info)、链路信息 (Link_Info) 分别存储在 2 个不同表中。边界节点既要存储所属 KRA 内的拓扑信息，也要存储各 KRA 之间的连通关系，因此边界节点的 Node_Info 表中也包含了其他 KRA 内的边界节点信息，而各 KRA 内的虚链路则存储在 VLink_Info 信息表中。Routing_Info 由路由计算组件负责更新与维护。

4.2.5 路由信息交换内容

为了寻找最优路径，保证密钥路由的效率，各节点之间需要定期相互交换有关网络拓扑、链

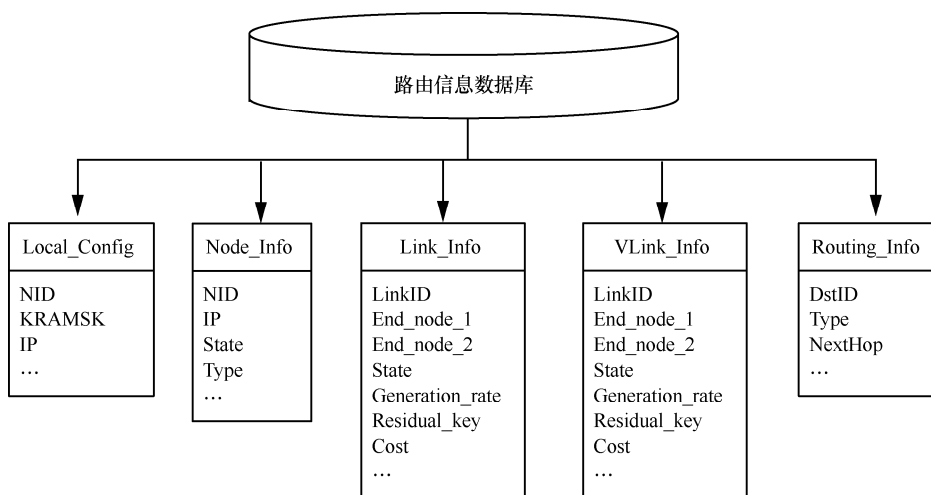


图6 路由信息数据库结构示例

路状态等信息。在分域量子密钥网络中，路由信息交换分为域内路由信息交换与域间路由信息交换2类情况。

1) 域内路由信息交换

域内路由信息交换是同一个 KRA 内节点间进行的路由信息交换，其目的是让所有节点能够及时掌握 KRA 内的网络拓扑及链路状态信息变化情况，同时确保 KRA 内所有节点的路由信息一致性。需要交换的信息内容与 KRA 内使用的路由协议有关，可能包括链路代价、链路密钥生成速率、链路的可用密钥量等。

2) 域间路由信息交换

域间路由信息交换是不同 KRA 的边界节点之间进行的信息交换，其目的是确保边界节点准确掌握所有 KRA 之间的连接关系及各虚链路的状态。需要交换的信息内容同样与采用的域间路由协议有关，一般包括各 KRA 的边界节点信息、各 KRA 内虚链路的可用密钥量等。域间路由信息交换时需要跨越的网络规模比较大，因此要求协议具备较快的收敛速度以应对快速变化的链路状态。

4.2.6 路由算法要求

通过密钥路由域划分，使单个密钥路由域规模大大缩小，现有的路由算法^[7~10]也可以用于各个密钥路由域内，当然也可以根据量子密钥网络特点设计更合适的路由协议及算法。为了确保域间路由计算的一致性，整个网络的域间路由算法只能采用一种协议及算法。不管采用哪种路由协议及算法，都应该满足以下要求。

1) 计算得出的路径上各链路的有效密钥量充足。

2) 能够减少密钥资源消耗，特别是无意义的消耗。

3) 能够实现网络中的负载均衡，合理利用网络中的所有密钥资源。

4) 由于域间路由信息交换延迟可能比较大，因此要求域间路由协议及算法在计算路由时能够考虑当前网络状态可能存在误差的因素。

4.3 方案分析

本节分别从路由更新的收敛性、路由延时、密钥资源消耗3个方面针对基于虚链路的分域量子密钥网络路由方案进行理论分析，并与全网直接路由方案进行对比，展示了本文方案的优越性。

4.3.1 路由更新收敛性分析

路由更新收敛速度与网络的规模及网络结构的复杂性密切相关，规模越小、网络结构越简单，路由更新收敛越快。在分域路由方案中，各密钥路由域的域内路由更新互不影响，可以同时、并行更新路由信息；域间路由更新虽然涉及网络中的每个密钥路由域，覆盖的物理范围很广，但只需各密钥路由域的边界节点之间进行路由信息交换，因此分域路由方案中路由更新收敛速度比较快。然而，在全网直接路由方案中，整个量子密钥网络中的所有节点之间都要进行路由信息交换，由于广域环境下网络规模较大，节点数量较多，极大地影响了全网直接路由方案的路由更新收敛速度。综上分析可得，广域量子密钥网络通过划分密钥路由域，可以缩小路由更新规模，减

少路由更新节点数，与全网直接路由方案相比，路由更新收敛速度更快速。

4.3.2 路由时延分析

3.2.1 节专门分析了量子密钥网络路由时延，并得出了直到密钥路由成功时的平均时延，如式(5)所示，这也是全网直接路由方案中的路由时延。在分域路由方案中，域内密钥路由直接通过量子信道构成的链路进行密钥中继，路由时延与全网直接路由方案一样。域间密钥路由通过各虚链路完成用户密钥传输，因此，式(5)中的密钥生成时间为各条虚链路的链路密钥生成时间。由于虚链路覆盖的范围较大，单跳的传输时间可能会增加，并且因为虚链路的链路密钥是通过密钥中继获得，使虚链路的单中继成功概率也可能降低。下面对域间密钥路由时延进行详细分析。

假设以 10 跳为每个密钥路由域的最长路径，则虚链路的密钥生成时间为

$$t'_g = \left(t_g + \frac{1-p^{10}}{q} t_r \right) \frac{1}{p^{10}} \quad (11)$$

假设虚链路的单跳中继成功概率降低为 $p' = p^2$ ，单跳传输时延增加为 $t'_r = 2t_r$ ，则域间密钥路由直到成功的时延为

$$T_{\text{outer}} = \left(t'_g + \frac{1-p'^{\lceil n/10 \rceil}}{(1-p')} t'_r \right) \frac{1}{p'^{\lceil n/10 \rceil}} \quad (12)$$

其中， $\lceil n/10 \rceil$ 为经过的密钥路由域个数。进一步可得分域路由方案的时延为

$$T = \begin{cases} \left(t_g + \frac{1-p^n}{(1-p)} t_r \right) \frac{1}{p^n}, & n \leq 10 \\ \left(t'_g + \frac{1-(p^2)^{\lceil n/10 \rceil}}{(1-p^2)} t'_r \right) \frac{1}{(p^2)^{\lceil n/10 \rceil}}, & n > 10 \end{cases} \quad (13)$$

假设 $t_g = 10$ ， $t_r = 1$ ， $p = 0.99$ ，可得全网直接路由方案与分域路由方案的时延，如图 7 所示。

从图 7 中可以看出分域路由方案时延远低于全网直接路由时延，并且量子密钥网络规模越大，时延差别越大。

4.3.3 密钥资源消耗分析

与路由时延类似，3.2.2 节分析了量子密钥网络路由的密钥资源开销，得出了直到密钥路由成功时平均密钥资源消耗，如式(9)所示，同样也是

全网直接路由方案中的密钥资源消耗。在分域路由方案中，域内密钥路由的密钥资源消耗与全网直接路由方案类似。然而，对于域间密钥路由，不仅各虚链路生成链路密钥需要消耗密钥资源，通过虚链路生成用户密钥也需要消耗虚链路的密钥资源，下面对域间密钥路由的密钥资源消耗进行详细分析。

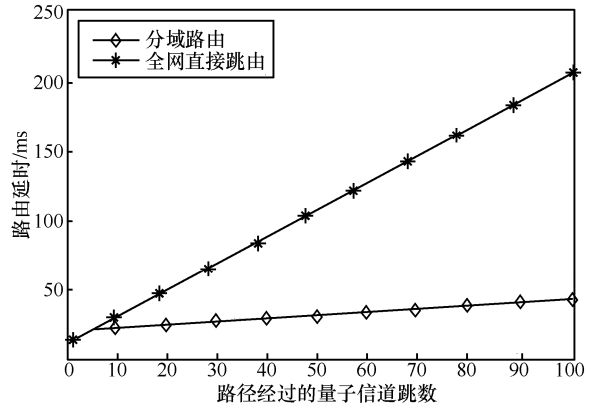


图 7 路由时延分析

同样假设以 10 跳为每个密钥路由域的最长路径，则虚链路生成链路密钥的密钥消耗为

$$C' = \frac{1-p^{10}}{p^{10}q} l \quad (14)$$

在密钥路由时，源节点与目的节点在各自密钥路由域内与边界节点之间需要通过域内路由完成，因此假设对于经过 n 条量子信道的路径包含 $n' = \lfloor n/10 \rfloor$ 个密钥路由域，余下的部分 $n'' = n \% 10$ 为域内路由跳数，假设虚链路的单跳中继成功概率降低为 $p' = p^2$ ，则域间密钥路由的密钥资源消耗为

$$C_{\text{outer}} = n' C' + \frac{1-(p^2)^{n'}}{(p^2)^{n'}(1-p^2)} l + \frac{1-p^{n''}}{p^{n''}q} l \quad (15)$$

假设传输 L 长度的密钥量同样也消耗 $l = L$ 长度的密钥资源，则分域路由方案的密钥资源消耗比为

$$C = \begin{cases} \frac{1-p^n}{p^n q}, & n \leq 10 \\ n' \frac{1-p^{10}}{p^{10}q} + \frac{1-(p^2)^{n'}}{(p^2)^{n'}(1-p^2)} + \frac{1-p^{n''}}{p^{n''}q}, & n > 10 \end{cases} \quad (16)$$

假设 $p = 0.99$ ，可得全网直接路由方案与分域路由方案的密钥资源消耗比，如图 8 所示。

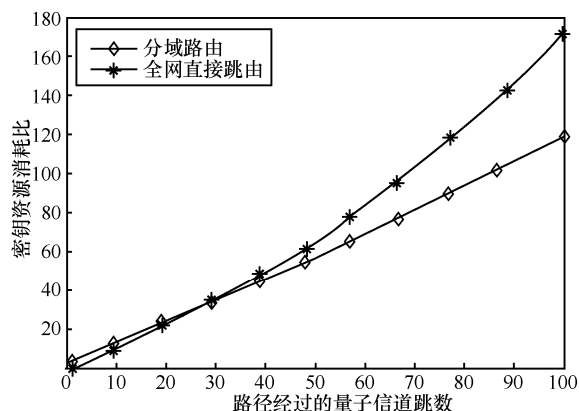


图8 密钥资源消耗分析

从图8中可以知,当量子密钥网络规模不大时,2种方案密钥资源消耗比基本相同,这是因为在密钥中继过程中每经过一跳必然会消耗一定量的密钥资源。随着量子密钥网络规模逐渐增大,2种方案的密钥资源消耗比均会增加,但是分域路由方案的密钥资源消耗比明显低于全网直接路由方案。

5 结束语

本文主要针对基于密钥中继的广域量子密钥网络的路由问题展开研究,分析了广域量子密钥网络路由的特点,进而提出了广域量子密钥网络路由的设计需求,最后设计了基于虚链路的分域路由方案。该方案将广域量子密钥网络划分为多个规模较小的密钥路由域,极大降低了域内密钥路由的复杂度。同时,该方案为每个密钥路由的边界节点间建立虚链路,仅需要传输一跳就可以跨过整个路由域,极大地缩短了域间路由路径长度。通过上述方法很好地满足了广域量子密钥网络的路由需求。理论分析表明,在网络规模大、节点数量多的广域环境下,该方案具有路由更新收敛快、路由时延短、密钥资源消耗少的优点。然而,由于本文旨在探索一种广域量子密钥网络路由的解决方案,因此并未对方案中涉及的技术细节进行深入研究。下一步将逐步深入研究方案中的各项技术,如相关路由协议、路由信息交换协议、路由算法等,并进行实验验证。

参考文献:

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public

key distribution and coin tossing[C]//IEEE International Conference on Computers, Systems, and Signal Processing. 1984: 175-1984.

[2] 马瑞霖. 量子密码通信[M]. 北京: 科学出版社. 2006.

MA R L. Quantum cryptography communication[M]. Beijing: China Science Publishing. 2006.

[3] 尹浩, 马怀新. 军事量子通信概论[M]. 北京: 军事科学出版社. 2006.6

YIN H, MA H X. The outline of military quantum communication[M]. Beijing: Military Science Publishing House. 2006.6.

[4] 李泽霞, 边文越. 未来10年中国可能发生的19个重大科技突破[J]. 中国科学院院刊, 2013, 28(5): 601-604.

LI Z X, BIAN W Y. The 19 Chinese possible major technological breakthroughs in the next 10 Years[J]. Bulletin of Chinese Academy of Sciences. 2013, 28(5):601-604.

[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.

WU ZH B, CHEN G, YANG B J. Analysis of quantum key distribution networks[J]. Study on Optical Communications, 2009, 2: 22-24.

[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] TANIZAWA Y, TAKAHASHI R, DIXON A R. A routing method designed for a Quantum Key Distribution network[C]//The Eighth International Conference on Ubiquitous and Future Networks, IEEE. 2016:208-214.

[8] DIANATI M, ALLÉAUME R, GAGNAIRE M, et al. Architecture and protocols of the future European quantum key distribution network[J]. Security & Communication Networks, 2008, 1(1):57-74.

[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 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.

[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 L, SU J H, et al. 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] PHOENIX S J D, BARNETT S M. Relay QKD networks & bit transport[J]. arXiv: 1502.06319v1[quant-ph] 23 Feb 2015.

[12] WEN H, HAN Z F, ZHAO Y B, et al. Multiple stochastic paths scheme on partially trusted relay quantum key distribution network[J]. Science in China, 2009, 52(1):18-22.

[13] BARNETT S M, PHOENIX S J D. Securing a quantum key distribution relay network using secret sharing[C]//2011 IEEE GCC Conference and Exhibition(GCC). 2011:19-22.

[14] BENNETT C H. Quantum cryptography using any two nonorthogonal[J]. Physical Review Letters, 1992, 68(21):3121.

- [15] LO H K, MA X F, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(3): 230-504
- [16] 陈晖, 张文政. 量子密钥分发技术的机遇与挑战[J]. 中国电子科学研究院学报, 2014, 9(1): 27-31.
- CHEN H, ZHANG W Z. The opportunity and challenge on quantum key distribution[J]. Journal of CAEIT, 2014, 9(1): 27-31.
- [17] 吴华, 王向斌, 潘建伟. 量子通信现状与展望[J]. 中国科学, 2014, 44(3): 296-311.
- WU H, WANG X B, PAN J W. Quantum communication: status and prospects[J]. Science China, 2014, 44(3): 296-311.

作者简介:



杨超 (1988-), 男, 四川巴中人, 信息工程大学博士生, 主要研究方向为信息安全、量子密钥分发。



张红旗 (1962-), 男, 河北唐山人, 博士, 信息工程大学教授, 主要研究方向为可信计算、网络安全、安全管理。



苏锦海 (1968-), 男, 河北张家口人, 博士, 信息工程大学教授, 主要研究方向为信息安全、密钥服务与管理、量子密钥分发。

陈华城 (1986-), 男, 福建漳州人, 解放军 73503 部队助理工程师, 主要研究方向为网络与信息安全。