

一种量子密钥分发网络中的资源感知路由算法

王聪, 张杰

(北京邮电大学信息光子学与光通信国家重点实验室, 北京 100876)

摘要: 随着量子信息科学的发展, 人们对量子密钥分发 (Quantum key distribution, QKD) 网络的研究方兴未艾。在量子密钥产生速率一定的情况下, 提高量子密钥的利用效率对于量子密钥网络走向实用化有着重要的意义。针对此问题, 通过对可信中继量子密钥分发网络中密钥的分发过程的分析, 本文提出了一种基于密钥资源感知的路由计算方法。并且通过仿真进行了性能验证。仿真结果表明, 与经典路由算法相比, 该算法可以显著降低密钥分发时的阻塞率, 提高密钥资源的整体利用率。

关键词: 信息与通信工程; 量子密钥分发; 信任中继; 路由计算

中图分类号: TN915.03

A Resource Awareness Routing Algorithm for Quantum Key Distribution Networks

WANG Cong, ZHANG Jie

(State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract: With the development of quantum information science, the research on Quantum key distribution (QKD) network is in the ascendant. In the case of quantum key generation rate is certain, improving the quantum key utilization efficiency is of great significance for the quantum key network to be practical. To solve this problem, through the analysis of the key distribution process in trusted relay quantum key distribution network, this paper proposes a routing algorithm based on key resource aware. The performance of the system is verified by simulation. Simulation results show that compared with the classical routing algorithm, the proposed algorithm can significantly reduce the blocking probability in key distribution and improve the overall utilization of key resources.

Keywords: Information and Communication Engineering; quantum key distribution; trusted relay; routing computation

0 引言

随着云计算与大数据的兴起, 网络中的大量数据流的传输安全问题收到了越来越多的关注。而目前通信加密的主要手段是经典的公钥加密系统。它的安全性依赖于数学上的计算复杂度。但是随着量子计算机的出现, 这种加密手段的安全保证越来越脆弱。因此人们迫切地需要一种不依赖于数学上的计算复杂性的加密手段。而随着量子信息科学的发展, 人们将量子力学的基本原理应用到经典通信中, 发展出了量子保密通信这一新技术。这一技术从物理上实现了无条件的安全性, 有着重要的研究价值^[1-2]。

经过长期的研究, 人们在点对点之间的量子密钥协商与产生技术的研究已经相当成熟。但实际的通信是网络化的, 所以量子的密钥分发 (Quantum key distribution, QKD) 也要实现组网。而事实上, 国内外都对 QKD 的组网技术做了一定的研究。国外已建成的 QKD 网络中比较著名的有美国的 DARPA 网络和欧洲的 SECOQC 网络, 我国于 2009 年也于芜湖建立

作者简介: 王聪 (1992-), 男, 硕士研究生, 主要研究方向: 通信网络

通信联系人: 张杰 (1972-), 教授, 博导, 主要研究方向: 光网络与通信系统. E-mail: lgr24@bupt.edu.cn

了世界上首个量子政务网^[3]。

虽然量子密钥分配技术为加密通信提供了很高的安全保证,但是目前量子密钥分发技术的成钥速率相对与大数据量的加密需求来说还很有限,并且还会随着链路距离的增长而急剧衰减^[4],因此提高量子密钥的利用效率对于 QKD 网络的应用前景具有十分主要的意义。而在 QKD 网络中的密钥分发路由的选择对密钥的利用率具有重大的影响,所以本文将着重研究 QKD 网络中的路由计算问题。

1 量子密钥分发网络的组网方式

按照密钥分发的原理与方式的不同,量子密钥分发网络的组网方式主要有三种。分别为量子中继,可信中继与基于经典光学的组网方式。其中量子中继基于量子纠缠交换技术,技术实现难度较高,距离实际应用还有一段距离。而基于经典光学的无源光器件网络中存在者光学器件的损耗与信道的衰减,并且单光子在传输中也不能进行放大造成接收方接受到的平均光子数目较低,不能有效地生成量子密钥。并且受限于目前量子密钥分发技术成钥速率的水平,使得它的网径跟用户数都相当有限,无法为长距离的用户提供服务,可靠性也一般。而基于可信中继的密钥分发网络是目前来说最具有应用前景的。它能够有效地实现长距离的加密通信,用户数量也没有限制,技术上容易实现,成本也适中,网络的扩展性与部署的灵活性也较高^[5]。所以本文主要研究基于可信中继量子密钥分发网络中的路由选择问题。

基于可信中继的 QKD 网络中的一条密钥分发路由由通信双方节点,可信中继节点和中继链路三部分组成。它的密钥分发的主要原理是随机密钥流通过中继节点相继加密转递直至最终到达接受方完成密钥在通信双方间的共享。下面以图例的方式来说明密钥中继的详细方式。如图一所示,主机 A 与主机 B 是通信双方,节点 1,节点 2 与节点 3 是可信中继节点。为了使主机 A 与主机 B 共享密钥,首先在主机 A 与节点 1 之间产生共享密钥 k_1 ,然后节点 1 通过它与节点 2 共享的密钥 k_2 对 k_1 加密然后传输给节点 2。后续中继节点以相似的方式在路径的各个链路上对密钥 k_1 递次进行解密和加密传输。最后,主机 B 得到 k_1 后,主机 A 与主机 B 之间的密钥分发过程就完成了最得到了一致的密钥 k_1 。

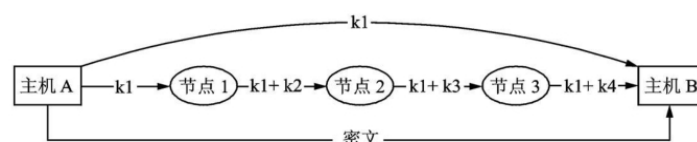


图 1 可信中继量子密钥分发网络的密钥中继方式

Fig. 1 The key relay mode in trusted relay QKD network

2 密钥分发网络中的路由算法研究

2.1 选路的参量

(1) 密钥的产生速率。QKD 网络中密钥的成钥速率随着链路的距离的增加而衰减。成钥速率与链路长度 l 的关系可以用式子 (1) 表示:

$$R(l) = R_0 e^{-l/\lambda} \quad (1)$$

其中 R_0 表示零距离下的成钥速率。 λ 是一个标度参数。可以看出成钥速率与链路长度成对数负相关关系,随着长度增长,成钥速率逐渐减少^[6]。

(2) 量子密钥池的密钥数量。因为 QKD 网络中的成钥速率相对与加密需求相对降低, 随意量子系统空闲时刻产生的密钥流要存放到量子密钥池里面去以备需要的时候使用。当量子密钥池存储的密钥数量较多时, 它就能够为更多的加密业务提供服务。

(3) 加密业务的密钥消耗速率。每一加密业务都有一个密钥更新周期。而密钥更新周期的倒数就是密钥的需求速率。它代表单位时间加密业务要消耗多少密钥。更细周期越大, 密钥的消耗率就越小, 相应的业务的安全性也就越低。

(4) 链路跳数。有 QKD 网络中的密钥分发方式可知。为用户两方分发密钥的过程中会在该分发路径上的所有链路上消耗同样的资源。一次密钥分发的分发路由上的链路数量越多, 消耗掉的 QKD 网络中的量子密钥也越多。

2.2 理论分析

假设链路的密钥消耗速率为 V_c , 并且它等于它上面承载的所有加密业务的密钥消耗速率的和。而链路的成钥率为 V_g 。量子密钥池的密钥量为 N 。我们知道, 加密业务的持续时间都是不确定的。当 $V_c < V_g$ 的时候, 所有加密业务的全生命周期中都会有稳定的密钥供给。而当 $V_c > V_g$ 时, 链路就会消耗它的邻接节点处的量子密钥池内的密钥。最差情况下我们假设直到密钥池的密钥被消耗光都没有加密业务结束。此时, 这些链路就存在一个可服务时间 T 。它是从链路开始消耗密钥池的资源到密钥池资源被消耗光的时间。而当超过这个时间后, 该链路上的部分加密业务就会因缺乏密钥而陷于中断。而 T 的计算表达式为 $T = N / (V_c - V_g)$ 。

通过以上的分析可知, 为了避免 QKD 网络中加密业务因缺乏密钥而中断, 我们应该首先选择那些 $V_c < V_g$ 的链路作为路由路径的一部分。其次对于那些 $V_c > V_g$ 的链路, 我们实现应该选择可服务时间 T 大的链路作为路由路径的一部分。而为了实现这个方式, 我们需要掌握每时刻 QKD 网络中所有链路的密钥消耗率, 量子密钥池的密钥数量等动态信息。这也是本文中所说的资源感知路由 (Resource Awareness Routing, RAR) 算法名称的由来。

路由选择方式从整体上看可以分为集中式路由方式与分布式路由方式。对于分布式路由算法来说, 它要求各个节点间相互交换大量的链路状态信息, 造成信息的收敛速度较慢, 网络的时延较大, 难以做到实时感知网络中的信息, 不适用于本文的 RAR 算法, 所以本文选择集中式的路由选择方式。这种方式包含一个中心控制节点, 它时刻收集 QKD 网络中每条链路的密钥消耗率和密钥池资源信息, 实时计算路由并下发到节点当中, 使密钥资源的消耗与密钥资源的分布相匹配。除此之外, 它还可以实现资源告警功能, 如果发现每一链路上的密钥资源紧张时会提前告警, 为该链路上的业务重新计算路由。

2.3 路由计算过程

算法的核心思想是尽量避免选择那些链路密钥消耗速率 V_c 较大并且邻接节点处的密钥池的密钥数量 N 较少的链路来避免加密业务的阻塞。尽量选择那些链路资源相对于消耗速率来说较为富裕的链路来服务与更多的加密业务请求。具体过程如下:

首先我们将 QKD 网络看成一个有权图并建立模型。为每条链路定义一个权值。对于那些密钥消耗率 V_c 小于成钥率 V_g 的链路, 定义它的值为 0。而对于密钥消耗率 V_c 大于成钥率 V_g 的链路, 它的值等于该链路的可服务持续时间 T 的倒数。链路权值整体反映了该链路此时的可承受新的加密业务的能力。权值越小, 承受的能力就越大。选择路由时, 在有权图中利用 Dijkstra 算法求解一条从起点到终点的权重最小的路径。如果没有找到, 则选路失败。

由密钥分发中继过程可知, 密钥分发路径上的链路数目越多, 网络的密钥资源消耗也越

大。同样条件下应该尽量选择链路数量小的路由路径。所以算法可以改进为使用 K 算法先计算基于权值的 K 条最小路径，再从这 K 条路径中选择链路数量最小的路径作为最优密钥分发路径。

3 路由算法性能仿真分析

3.1 仿真场景

本文仿真采用 NSFNET 的网络拓扑结构，有 14 个节点与 21 条链路。仿真以语音业务为例，业务的到达时间和业务的持续时间都符合指数分布。链路的成键率是固定的常数。另外每个业务的密钥需求率和每一节点处的密钥数量也都是给定的初始值。

3.2 结果分析

图 2 表示的是不同的路由算法在不同业务量强度下的加密业务的阻塞率。主要分为经典的最短路算法和本文提出的 RAR 算法。其中 RAR 算法又根据量子密钥池的容量的大小分为两种情况。 $RAR 1$ 的密钥池容量大于 $RAR 2$ 的。

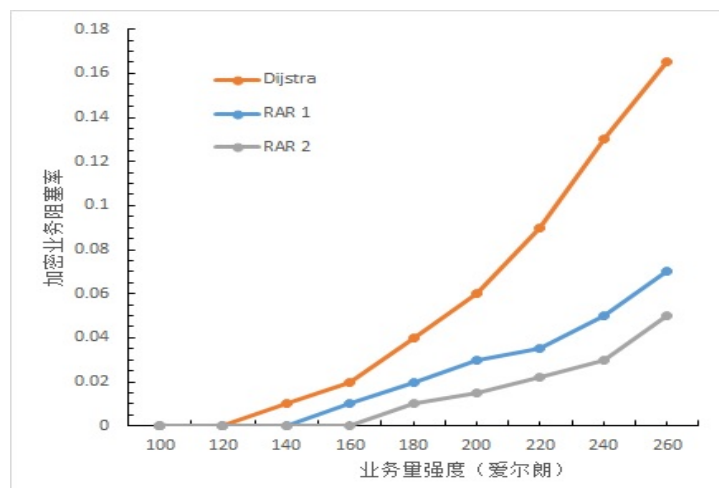


图 2 不同业务量强度下的加密业务阻塞率

Fig. 2 Blocking rate of encrypted traffic under different traffic intensities

由结果看出，当业务请求数量很小的时候，算法的阻塞率都很低。这是因为此时的密钥资源足够满足需求，网络中几乎不存在密钥资源缺乏的情况。但是当业务请求数量增加的时候， RAR 算法的阻塞率更小。这是因为 RAR 算法尽量从这个 QKD 网络的角度统筹利用密钥，引导密钥分发业务的路由选择那些较密钥资源较富裕的链路，实现了密钥资源的均衡利用。而 $RAR 1$ 与 $RAR 2$ 的差别也表明密钥池的容量越大，对密钥资源的储蓄能力越强，密钥分发业务的阻塞率也就越小。

图 3 表示不同路由算法在不同业务量强度下路由路径的平均跳数。可知， RAR 算法的路由平均跳数较 $Dijkstra$ 算法较大。这是因为 RAR 的路由选择不局限与路径跳数而是取权值和最小的路径作为选择结果的。这会使路由总是选取链路的资源情况相比于密钥的消耗而言较为充分的，实现了密钥分发业务的均衡分布，进一步提高 QKD 网络的承载能力。

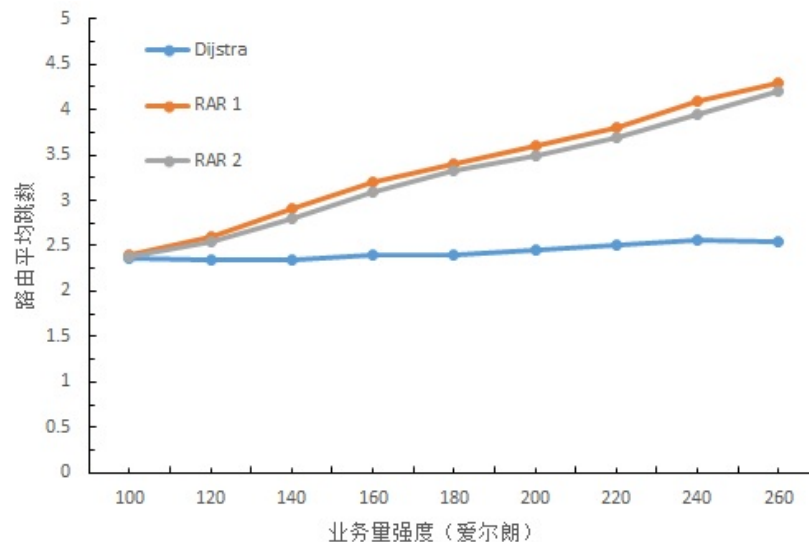


图3 不同业务量强度下的路由的平均跳数

Fig. 3 Average hops of routes under different traffic intensities

4 结论

量子保密通信是未来加密通信的重要发展方向。本文首先介绍了基于可信中继的 QKD 网络的结构和密钥中继分发的原理,在此基础上分析了 QKD 网络中的路由选择问题,研究找出了影响 QKD 网络性能的重要选路参量,进而提出了一个基于资源感知的路由算法。最后通过仿真模拟对本文提出的算法进行了验证。仿真结果表明该算法可以显著地降低 QKD 网络中加密业务的阻塞率,有效地提高密钥资源的整体利用率。

[参考文献] (References)

- [1] Bennett C H, Brassard G. "Quantum cryptography: Public key distribution and coin tossing[C]", IEEE International Conference Computers, Systems, and Signal Processing, Bangalore, India. 1984. 175-179.
- [2] 刘刚. 量子保密通信系统及组网技术研究[D].西安电子科技大学,2012.
- [3] 许方星, 陈巍, 王双等. 多层级量子密码城域网. 科学通报, 2009, 54(16):2277-2283
- [4] K. Shimizu et al., "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," in Journal of Lightwave Technology, vol. 32, no. 1, pp. 141-151, Jan.1, 2014.
- [5] Xv Fangxing , Chen Wei , Wang Shuang , et al . Field experiment on a robust hierarchical metropolitan quantum cryptogra-phy network[J]. Chinese Sci Bull, 2009, 54(17): 2991-2997
- [6] 韩伟,武欣嵘,朱勇,周星宇,徐超. 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(04):43-48+94