文章编号：2095-2163(2021)06-0214-04 中图分类号：TP391;TN911.73 文献标志码：A

基于两层架构的量子密钥分发网络仿真系统

王亚星，李 琼
（哈尔滨工业大学 计算学部，哈尔滨 150001）

摘 要：量子密钥分发(Quantum Key Distribution，QKD)与一次一密加密机制的结合，可以为远程通信方提供信息安全的保密通信服务。由于 QKD 设备固有的点对点特性，研究和发展 QKD 设备组网技术，是为更大范围、更大规模的用户群体提供保密通信服务的必须途径。针对 QKD 网络的仿真需求，本文设计了一种基于两层架构的 QKD 网络仿真系统，并利用 NS3 平台进行了实现。实验结果及性能分析，验证了仿真系统的可行性，该系统能够为 QKD 网络的高效构建提供有力的支撑和保障。

关键词：量子密钥分发；网络仿真；NS3；信息论安全

NS3-based simulation system for quantum key distribution networks

WANG Yaxing，LI Qiong
（Faculty of Computing，Harbin Institute of Technology，Harbin 150001，China）

【Abstract】 Quantum Key Distribution (QKD)，combined with the encryption mechanism of one-time-pad，can provide information-theoretical secure communication service for remote communication parties. Due to the inherent point-to-point characteristics of QKD device，the research and development of QKD network technology is critical for providing secure communication services for large-scale of users over a large area. Aiming at the QKD network simulation requirements，a QKD network simulation system based on two-layer architecture is designed in this paper，with the implementation on NS3 platform. Experimental results and performance analysis validate the feasibility of the proposed simulation system，which can provide strong support and guarantee for the efficient construction of QKD network.

【Key words】 quantum key distribution；network simulation；ns3；information-theoretical secure

0 引 言

由于 QKD 设备具有点对点模式的固有特性[1]，利用多套 QKD 设备的连接来构建 QKD 网络[2-4]，是突破节点规模和通信距离限制的一种主流解决方案。目前，单套 QKD 设备已能够在点对点模式下支持数百公里的保密通信服务，为构建 QKD 网络提供了物质保障。例如，单套 QKD 设备在 10 km 和 50 km 的传输距离下，密钥分发速率分别可达 10 Mbps[5]和1 Mbps[5-6]；单套 QKD 设备在光纤和自由空间环境中的传输距离分别可达 509 km 和 1200 km[7-8]。搭建的实验性 QKD 网络也已经能够为数十用户提供千公里范围内的保密通信服务，验证了建设大规模 QKD 网络的物理可行性。经过三十多年的发展，实验性 QKD 网络的节点规模已经从 6 个扩展到了 56 个，覆盖范围从 19.6 km 扩展到了 7 600 km[9-11]。随着实验性 QKD 网络用户规模和覆盖范围的不断扩大，预先进行方案设计与仿真验证在性能保障、设备优化、成本控制等方面都发挥着至关重要的作用。

与经典网络领域不同，QKD 网络的仿真验证还没有引起足够的重视，相关的研究文献较少。为了对通信过程中的量子密钥消耗量进行统计，Yang 等人[12]在 2017 年搭建了一个简单的 QKD 网络仿真系统 。然而，该系统将一套 QKD 设备的密钥生成能力设置为无穷大，仅对密钥消耗进行了统计，这与 QKD 设备密钥生成能力十分受限于光纤长度的特性是不相符的。此外，Mehic 等人[13]在 2017 年设计了一套相对完善的 QKD 网络仿真系统，可支持对密钥生成过程和流量生成过程的仿真模拟。然而，该系统将所有链路上的密钥生成能力都假定为同一常数，这不仅与 QKD 设备密钥生成能力十分受限于光纤长度的特性是不相符的，与 QKD 网络需要满足的波动性通信流量需求特性也是不相符的。

为了对受限性密钥生成能力、波动性通信流量需求及两者之间的博弈关系进行详细分析，本文通

基金项目：面向复杂通信需求的量子密钥分发网络建模与优化(62071151)。

作者简介：王亚星(1994-)，女，博士研究生，主要研究方向：量子密钥分发、量子密钥分发网络；李 琼(1976-)：女，博士，教授，主要研究方向：量子密钥分发、信息安全技术。

收稿日期：2021-02-27

过设计以全网密钥生成模块和多方并发流量生成模块为核心的两层架构，提出了一种基于两层架构的 QKD 网络仿真系统，并基于 NS3 平台进行实现。此外，使用单向时延、吞吐量、数据包投递率及路由代价 4 项指标，对传统目的节点序列距离矢量协议（Destination Sequenced Distance Vector routing，DSDV）、路由协议应用于 QKD 网络的通信性能进行了仿真与分析，验证本文所提仿真系统的可行性。

1　仿真系统的提出

QKD 网络与经典网络的最大不同之处在于，QKD 网络的通信过程需要消耗 QKD 设备生成的量子密钥，导致了 QKD 网络的通信性能十分受限于密钥生成能力与通信流量需求之间的匹配程度。由于密钥生成能力取决于网络中点对点连接的通信链路，而通信流量需求取决于网络中端到端的通信用户。为了对两者之间的联系进行准确描述，本文提出了一种基于两层架构的 QKD 网络仿真系统。该系统主要包含全网密钥生成、多方并发流量生成、通信数据生成、通信数据接收、数据加密、数据解密、数据包封装、数据包解析、密钥管理及路由协议等多个关键模块，QKD 网络仿真系统如图 1 所示。

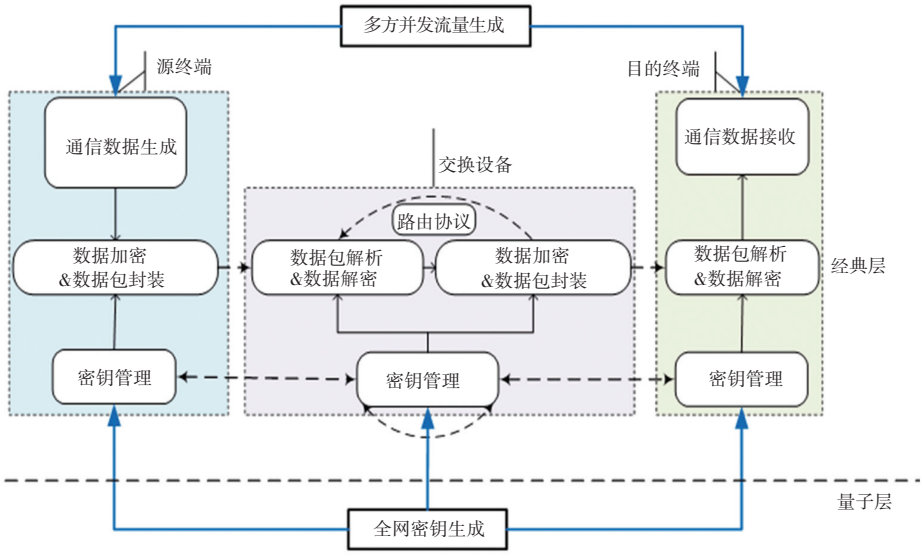


图 1　QKD 网络仿真系统

Fig. 1　The simulation system of QKD network

该仿真系统中，全网密钥生成模块属于量子层，用于模拟全网所有链路上的密钥生成过程；其它模块均属于经典层，用于模拟全网所有通信用户之间的保密通信过程。为了最大限度地兼容传统通信设施，除了全网密钥生成模块和多方并发流量生成模块，需要针对 QKD 网络特点进行特殊设计外，其它模块均可借鉴经典网络中的技术方案。

1.1　全网密钥生成模块

全网密钥生成模块的主要功能，是对 QKD 网络受限性的密钥生成能力进行刻画。2004 年，Gottesman、Lo、Lutkenhaus 与 Preskill 4 位学者联合提出了 GLLP 理论，对单套 QKD 设备的实际密钥生成速率进行计算[14]，并在其后被广泛采用。据此，本文设计的全网密钥生成模块，通过将 QKD 设备看成黑盒，使用 GLLP 理论对其外在特性，即密钥生成速率，进行了精确描述。

单套 QKD 设备密钥生成能力的计算公式为：

$$R_k = f_{req}q\{-Q_\mu f_{ec}H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}. \quad (1)$$

其中，f_{req} 表示光路重复频率；q 表示基选择效率；Q_μ 表示信号态脉冲的响应率，计算公式为：$Q_\mu = 1 - e^{-\mu 10^{-\frac{\alpha d}{10}}\eta_{Bob}} + Y_0$；$\mu$ 表示信号态的平均光子数；α 表示每公里光纤的衰减系数；d 表示光纤长度；η_{Bob} 表示光路系统的透过率；Y_0 表示暗计数的响应率；f_{ec} 表示误码协商算法的纠错效率；$H_2(x)$ 表示二进制熵函数；E_μ 表示信号态脉冲的误码率（计算公式为：$E_\mu = [(1 - e^{-\mu 10^{-\frac{\alpha d}{10}}\eta_{Bob}})e_{detector} + e_0 Y_0]/Q_\mu$，其中，$e_{detector}$ 表示探测器的探测效率；e_0 表示暗计数的误码率）；Q_1 表示单光子脉冲的响应率（计算公式为：$Q_1 = \mu e^{-\mu} 10^{-\frac{\alpha d}{10}\eta_{Bob}}$）；$e_1$ 表示单光子脉冲的误码率（计算公式为：$e_1 = \frac{Q_v E_v e^v}{v Y_1}$，$v$ 表示诱骗态的平均光子数；Q_v 表示诱骗态脉冲的响应率，计算公式为：$Q_v = 1 - e^{-v10^{-\frac{\alpha d}{10}}\eta_{Bob}} + Y_0$；$E_v$ 表示诱骗态脉冲的误码率，计算公

式为：$E_v=[(1-e^{-v10^{-\frac{\alpha d}{10}}\eta_{Bob}})e_{detector}+e_0Y_0]/Q_v$；$Y_1$ 表示单光子脉冲的计数率，计算公式为：$Y_1=\frac{\mu}{\mu v-v^2}[Q_v e^v-Q_\mu e^\mu\frac{v^2}{\mu^2}]$）。

根据公式（1）可计算出网络中每套 QKD 设备的密钥生成能力。将各个密钥生成能力进行累加，即可得到全网总的密钥生成能力。

1.2 多方并发流量生成模块

多方并发流量生成模块的主要功能，是对 QKD 网络波动性的通信流量需求进行刻画。数据包的发送过程可认为满足以下假设：

（1）在任意两个互斥的时间段内，发送的数据包数目是互相独立的随机变量；

（2）在一个任意小的时间段内，发送一个数据包的概率与起始时间无关，只与时间长度有关；

（3）在一个任意小的时间段内，发送一个数据包的概率为 1 或者为 0。数据包的发送过程可被证明是一种泊松随机过程，可用基于指数分布的发包间隔来模拟。

用 λ 表示单位时间内平均数据包发送个数；η 表示多个数据包发送间隔组成的随机数序列；ξ 表示满足 [0,1] 区间上均匀分布的随机数序列。则 η 服从均值为 $1/\lambda$ 的指数分布，计算公式为：

$$\eta=\frac{1}{\lambda}\ln(1-\xi). \tag{2}$$

根据公式（2），可计算出每个通信对进行流量生成的发包间隔。令网络中所有通信根据各自的发包间隔同时进行，即可得到多方并发的流量生成过程。

2 仿真实验

为了验证本文所设计 QKD 网络仿真系统的有效性，本节使用单向时延、吞吐量、数据包投递率及路由代价 4 项指标，对传统 DSDV 路由协议应用于 QKD 网络的通信性能进行了仿真与分析。

实验选用欧盟在 2008 年搭建的实验性 QKD 网络—SECOQC 网络的拓扑结构，共包含 6 个通信用户和 8 条通信链路，如图 2 所示。

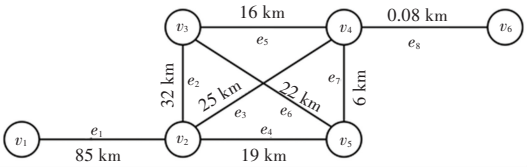


图 2 SECOQC 网络的拓扑结构

Fig. 2 Topology of the SECOQC network

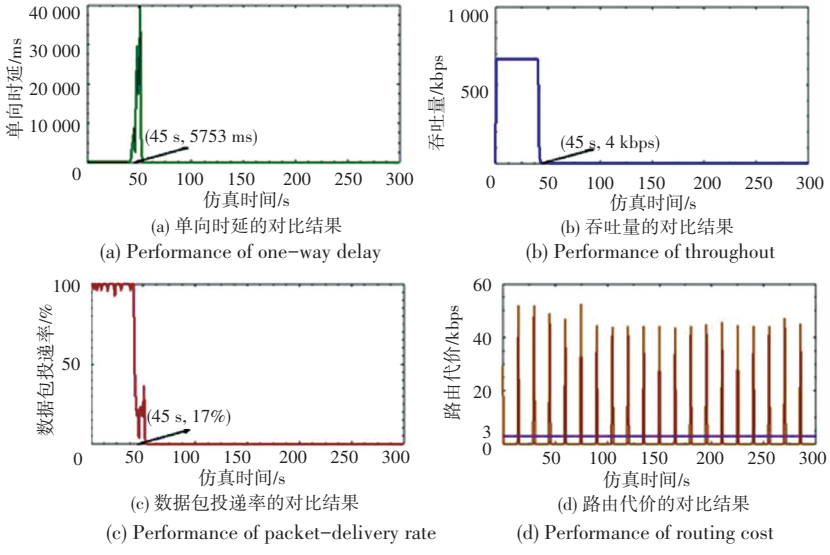
假定图 2 中每条链路上布置一套 QKD 设备，每套 QKD 设备的光学参数相同，见表 1。将其带入公式（1），可得到每套 QKD 设备的密钥生成能力。由于每条链路的光纤距离不同，每套 QKD 设备的密钥生成能力也不相同。

表 1 QKD 设备的参数设计

Tab. 1 Parameters of QKD devices

参数	f_{req}	q	α	η_{Bob}	$e_{detector}$	μ	v	Y_0	e_0	E_c
取值	1 GHz	0.9	0.2	0.1	0.01	0.4	0.1	2.1E-5	0.5	1.15

令用户 v_1 为发送方，v_6 为接收方，进行性能仿真。将数据包大小设置为 500 字节，平均通信流量需求设置为 100 kbps，采用 DSDV 路由协议得到的实验结果如图 3 所示。



(a) 单向时延的对比结果 (a) Performance of one-way delay

(b) 吞吐量的对比结果 (b) Performance of throughout

(c) 数据包投递率的对比结果 (c) Performance of packet-delivery rate

(d) 路由代价的对比结果 (d) Performance of routing cost

图 3 100 kbps 流量需求下的通信性能

Fig. 3 Network performance with 100 kbps communication rate