# QKD 网络量子信道管理关键技术研究

郑祎能

(华中科技大学电子信息与通信学院 武汉 430074)

**摘 要** 随着网络的发展,网络传播的信息日益增多,其中某些信息需要较高的安全性,因此信息加密手段的研究具有重大意义。量子密钥分发(Quantum Key Distribution,QKD)技术基于量子力学中的不可克隆定理,即不可能复制一个未知的量子态而不对其造成扰动,保证了其无条件的安全性,能够实现安全的密钥分发。但目前 QKD 网络规模较小,不能满足大规模组网的需求。同时,经典网络的路由技术已经不能适应 QKD 网络,量子信道寻径成为了一个需要解决的问题。鉴于以上问题,提出了一种能够满足较大规模 QKD 通信的基于光开关切换的 QKD 网络模型,并重点设计了其网络结构和信令体系,在此基础上设计了一个用于量子信道寻径的先导信号协议,并提出了量子信道管理机制。经实验验证,该模型的性能良好。

**关键词** 量子通信,量子密钥分发网络,量子信道管理

**中图法分类号** TP393 **文献标识码** A

## Research on Key Technologies of Quantum Channel Management in QKD Network

ZHENG Yi-neng

(School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China)

**Abstract** With the development of the Internet, the information dissemination is increasing and the information security is more and more important. As some information requires higher security, researches on information encryption methods are of great significance. Quantum key distribution (QKD) technology is based on the no-cloning theorem, which states that it is impossible to create an identical copy of an arbitrary unknown quantum state. That is why QKD is unconditionally secure and it enables keys distribution to be safe. However, the current QKD network is small in size and cannot meet the needs of large-scale network. At the same time, the routing techniques on the classical networks can not apply to the QKD network. Finding out feasible quantum paths becomes a problem to be solved. In view of the above issues, a QKD network model which can meet the large-scale QKD communication was put forward according to optical switch, and its network structure and signaling systems were designed. Based on this, the pilot signal protocol and the quantum channel management mechanism were proposed. The results show that the model works well.

**Keywords** Quantum communication, Quantum key distribution network, Quantum channel management

## 1 引言

量子通信是一种新的保密通信机制[1],它的密码思想通过量子物理学的方法实现,即在量子通信中,窃听者窥测通信信息时会破坏量子态而被通信双方及时发现。因此,量子通信具有很高的安全性。

量子通信由于其安全性上的优势[2],越来越被人们所重视,并成为研究热点。目前很多国家的研究机构都在积极研究量子保密通信技术,并取得了一定的研究成果,例如:量子密钥分发技术、量子安全直接通信技术、量子身份认证技术、量子秘密共享技术以及量子签名技术等[3]。

在量子密钥分配(Quantum Key Distribution,QKD)方面,1982 年,量子力学中著名的不可克隆原理由 *Nature* 上的一篇文章引出,文章的作者 Wootters 等指出了非正交未知量子态的不可复制性。1984 年,Bennet 等提出了著名的量子密码学协议——BB84 协议[4]。1991 年,Ekert 提出了基于 Einsein-Podolsky-Rosen 的 E91 协议。1992 年,Bennett 提出了 B92 协议。BB84,E91 和 B92 是 QKD 中非常重要的三大协议,其他的三态协议[5]和六态协议[6]等基本上都是对 BB84,E91 以及 B92 的改进。

早在 QKD 技术出现之初,Biham 等就在理论[7]和实践[8-9]方面对 QKD 的网络化分别进行了研究和尝试。构建量子网络的核心问题之一是量子网络的路由技术。尽管关于量子中继器和量子存储的研究已经取得了很大进展[10-13],但量子存储时间、量子纠缠态的产生速率和可靠性等都远未达到实际应用的要求,因此经典网络的路由机制无法应用到量子网络中。目前量子网络中的路由主要借助经典网络辅助及光学器件控制来建立通信两端之间的直接量子信道。

目前已经有人研究和探讨了光开关对 QKD 的影响[14],验证了光开关可比较好地应用于 QKD 网络中。因此,本文提出了一种基于光开关和 ASON 分层管理思想的 QKD 网络模型 ASQN(Automatically Switched Quantum Network)。在 ASQN 中,重点设计了 ASQN 信令体系和量子信道管理。经实验验证,该网络模型能够高效地利用网络资源完成一对或

郑祎能(1997—),女,主要研究方向为网络通信与多媒体信息处理,E-mail:915230866@qq.com。

多对并行的 QKD 通信,能在多条可行的量子信道路径中选出最优路径,同时当量子信道发生故障时,可以在较短的时间内对故障进行恢复。

## 2　ASQN 网络模型与信令体系

### 2.1　ASQN 网络架构

ASQN 网络模型的网络架构如图 1 所示。ASQN 网络包括 3 个平面:控制平面、管理平面和传送平面,这 3 个平面之间通过数据通信网进行信息交互传输。

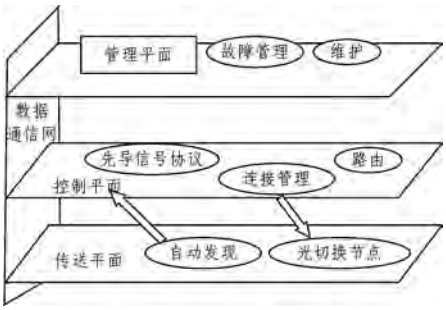


图 1　ASQN 网络架构示意图

#### 2.1.1　ASQN 控制平面

ASQN 控制平面的每个控制网元主要有以下几种核心组件:

1)协议控制器(Protocol Controller,PC)

对光切换节点收到的数据包进行解析,并将其传送给相应的协议处理模块。

2)连接控制器(Connection Controller,CC)

实现连接建立与释放,以及对连接参数的配置等功能。

3)路由控制器(Routing Controller,RC)

主要有 3 个功能:①响应 CC 建立连接时对路由信息的查询和更新;②运行 ASQN 路由协议发现网络拓扑;③在用户呼叫连接时通过先导信号协议发现可用的量子信道路径。

4)链路资源管理器(Link Resource Manager,LRM)

实现光开关和链路资源的配置和管理。

5)呼叫控制器(CallController,CallC)

呼叫控制器负责管理呼叫请求,对呼叫进行一系列的处理。

图 2 为控制平面的核心组件关系示意图。

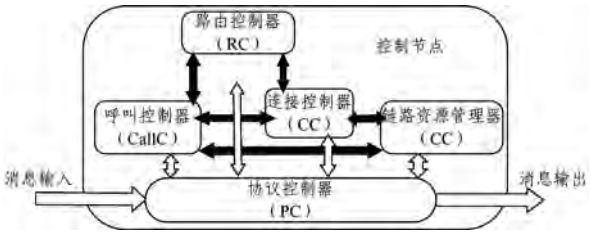


图 2　控制平面核心组件关系示意图

#### 2.1.2　ASQN 传送平面

在 ASQN 中,传送平面由 QKD 终端和一系列传送网元构成。QKD 终端指有能力进行 QKD 密钥交换的通信终端;传送网元主要包括光切换节点、光纤链路和经典链路。

光切换节点是 ASQN 中主要的网络节点。其主要功能是经典信息的路由和转发、光通路的连接以及光开关和链路属性的配置等。为实现经典信息路由和光路交换,每个光切换节点中都设置了一个光路切换装置。光路切换装置的设计如图 3 所示。

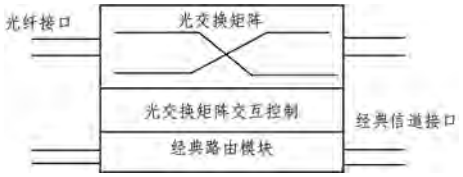


图 3　光路切换装置设计示意图

光路切换装置的结构从上往下依次为光开关矩阵、光交换矩阵交互控制模块、经典路由模块以及输入输出端口。光路切换装置的上层通过光开关矩阵来连接光纤从而形成光交换网络,底层通过具有经典路由功能的经典路由模块来连接经典链路从而形成经典信息网络。经典路由模块通过光交换矩阵交互控制模块查询光交换矩阵的状态。

### 2.2　ASQN 信令体系

ASQN 中,信令信道建立在经典信道之上,采用灵活的多径方式。信令信道和信令协议一起构成了信令系统,其功能包括:处理呼叫请求、管理量子信道、传递网络协议信息和管理信令通道。

#### 2.2.1　ASQN 信令的呼叫处理

ASQN 信令体系中,呼叫处理主要包括呼叫建立和呼叫释放两个过程。

ASQN 呼叫请求的建立步骤如下:

1)QKD 终端发起呼叫建立请求。

2)相关控制网元呼叫控制器(CallC)收到请求后,对其进行验证。若验证通过,则执行步骤 3),否则执行步骤 7)。

3)启动量子信道寻径过程,通过先导信号协议找到可用的量子信道路径。呼叫请求信息搭载先导信号协议包传输到被叫方的 CallC。

4)被叫方的 PC 对收到的先导信号协议包进行解析,将先导信号协议信息传送给先导信号协议模块,并将提取的呼叫请求信息传送给被叫方的 CallC。

5)被叫方的先导信号协议模块进行路径计算,确定量子信道路径。被叫方的 CallC 对呼叫建立请求信息进行验证处理,若拒绝接受呼叫请求,则执行步骤 7);若接受呼叫请求,则构建先导信号协议确认包,将选定的路径信息和呼叫请求确认信息一起封装到该确认包中,向通信发起端发送该确认包。然后执行步骤 6)。

6)主叫方的 PC 收到先导信号协议确认包后进行解析,提取出量子信道路径信息和呼叫建立请求确认信息。主叫方的 CallC 对请求确认信息验证成功则说明呼叫建立请求成功,然后向 CC 发送量子信道连接建立请求,启动量子信道连接建立过程。若验证失败,则执行步骤 7)。

7)向管理平面发送呼叫建立请求失败消息,管理平面首先对失败原因进行分析。对于主叫方的 CallC 和被叫方的 Call 拒绝的呼叫请求失败,执行步骤 8);对于步骤 6)对应的呼叫请求失败,执行步骤 9)。

8)通知主叫方呼叫建立请求失败。

9)通知主叫方呼叫建立请求失败,并对选定量子信道路径的节点预留资源进行释放。

呼叫建立过程的流程如图 4 所示。

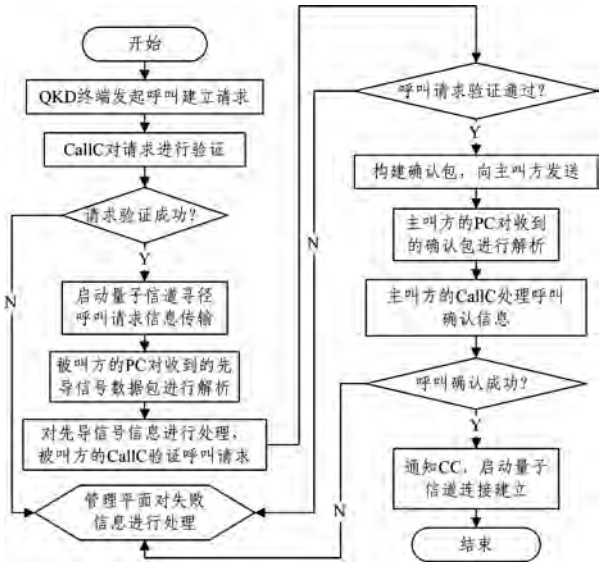


图 4 呼叫建立过程流程图

ASQN 呼叫释放请求的步骤如下：

1)通信结束或者故障时，发出呼叫释放请求。

2)相关 CallC 对呼叫释放请求进行验证。

3)若呼叫释放请求验证成功，则向连接控制器 CC 发出连接释放请求，CC 启动连接释放的过程，对链路资源进行回收。若验证失败，则执行步骤 4)。

4)将呼叫释放请求失败消息发送给管理平面进行相应处理。

呼叫释放过程的流程如图 5 所示。

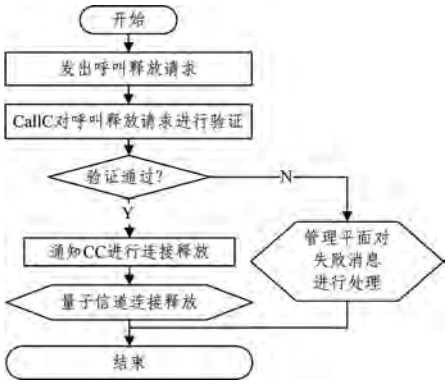


图 5 呼叫释放过程的流程图

### 2.2.2 量子信道建立和释放

量子信道建立过程通过对信令的处理来分配网络资源，其信令流程如图 6 所示。图中 USN 为主叫方节点，UDN 为被叫方节点，OSN-$i$ 为量子信道路径上的第 $i$ 个光切换节点，CC-$i$ 为节点 $i$ 的连接控制器。

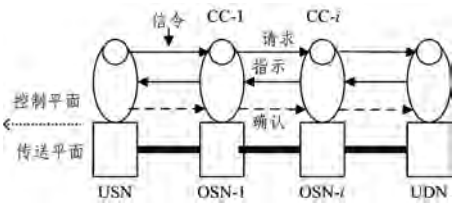


图 6 连接建立过程示意图

以图 6 为例，量子信道建立过程的具体步骤如下：

1)S 端用户连接控制器 CC 和路由控制器 RC 交互，获得构建光通路所需的下一个光切换节点 OTN-$i$。

2)S 端用户 CC 和 LRM 交互，查看现有网络资源是否满足建立 USN(QKD 终端)和 OTN-$i$(光切换节点)链路所需，若满足则执行步骤 3)，否则执行步骤 4)。

3)LRM 分配资源，建立 USN 到 OTN-$i$ 的光通路，$i$ 为下一个节点，执行步骤 5)。

4)链路建立失败，反馈失败信息给管理模块，管理模块对失败信息进行相应处理。

5)判断节点 $i$ 是否是目的节点，若不是，则转到步骤 7)；若是，则执行步骤 6)。

6)节点 $i$ 的 CC 处理连接请求，完成量子信道光通路的建立，然后向主叫方节点发出响应消息，告知量子信道连接建立成功。

7)节点 $i$ 的连接控制器 CC 和路由控制器 RC 交互获得构建光通路需要的下一个节点 $j$。

8)节点 $i$ 的 CC 和 LRM 交互，查看现有网络资源是否满足建立 OTN-$i$ 和 OTN-$j$ 光通路所需，若满足，则执行步骤 9)；若不满足，则执行步骤 4)。

9)LRM 分配资源，建立 OTN-$i$ 到 OTN-$j$ 的光通路，$i=j$，转到步骤 5)。

量子信道光通路的建立过程如图 7 所示。

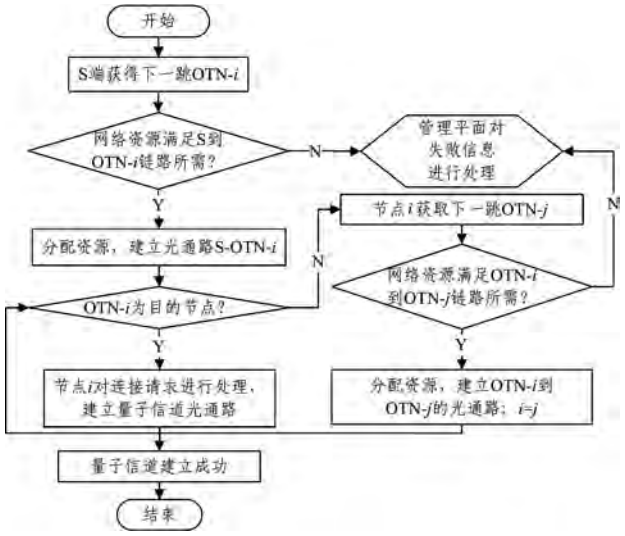


图 7 量子信道连接建立的流程图

量子信道连接释放过程是量子信道连接建立的逆过程，具体步骤如下：

1)呼叫释放请求已经验证通过。

2)在 S 端，CC 和 LRM 协作，释放 S 节点的相关链路资源，若释放成功转到步骤 3)，否则转到步骤 7)。

3)获取 S 端在量子信道路径上的下一跳光切换节点 OTN-$i$，执行步骤 4)。

4)OTN-$i$ 的 CC 和 LRM 协作，释放相关链路资源，释放成功则转到步骤 5)，否则转到步骤 7)。

5)判断 OTN-$i$ 是否为目的节点，若是，则对连接进行处理，完成量子信道路径资源的全部释放；若不是，则执行步骤 6)。

6)获取 OTN-$i$ 在量子信道路径上的下一跳节点 OTN-$j$，$i=j$，执行步骤 4)。

7)将与释放失败有关的故障报告给管理模块做相应处理。

量子信道连接释放过程的流程如图 8 所示。

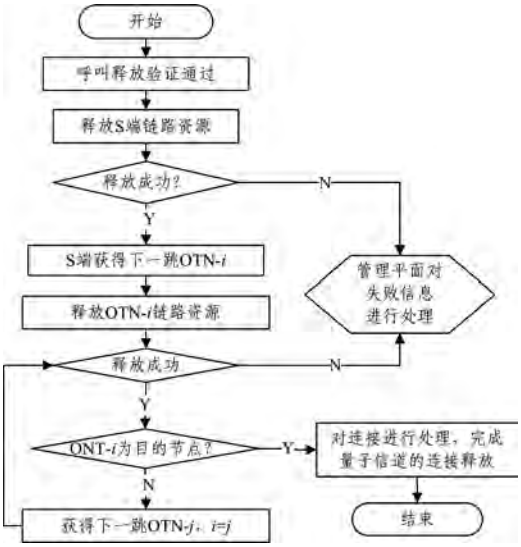


图 8　量子信道连接释放的流程图

## 3　ASQN 先导信号协议及量子信道管理

量子信道建立的前提是发现可用的量子信道路径，由于经典网络的路由机制不能满足这一需求，因此设计了一种先导信号协议(Pilot Signal Protocol，PSP)，通过此协议可以找到多条可行的端到端量子信道路径，并选择最优的路径作为量子信道，其余路径作为备用路径。

### 3.1　ASQN 先导信号协议

先导信号协议主要完成量子信道路径的寻找和选择，包括 3 个阶段：路径探测阶段、路径选择阶段、路径确认阶段。

#### 3.1.1　路径探测阶段

1)通信源端 S 的路由控制器 RC 查询网络拓扑中到达目的节点的所有可能路由。对于每一条路由，RC 和 LRM 交互，查询当前的资源是否满足建立 S 到路由下一跳节点的光通路所需，若满足，则计算路径 ID、损耗和时延，并将其和本地节点 IP 一起写入 PSP 协议信息包中，向路由下一跳节点转发 PSP 请求包，转向步骤 2)；若不满足，则放弃该路由。若所有的路由均不满足要求，则转向步骤 5)。

2)节点协议控制器对 PSP 协议进行解析并将信息发送给 RC。若该节点为 PSP 请求的目的节点，则进入路径选择阶段，否则转向步骤 3)。

3)根据 PSP 协议信息包的地址记录计算是否有回路产生，若有，则路径探测失败，放弃路径探测；若没有，则转向步骤 4)。

4)RC 查询通往目的节点所有可能的路由，然后 RC 和 LRM 交互，查询当前的资源是否满足建立本节点到上一跳节点和下一跳节点的两条光通路所需。若均满足，则计算路径 ID、损耗、时延，并将其和本地 IP 一起写入 PSP 协议包，然后向下一跳节点转发 PSP 请求包，转向步骤 2)；若资源不能满足两条光通路所需，则该条路径发现失败；

5)先导信号路径探测过程失败，则表明呼叫请求失败，将失败信息通知管理平面。

在路径探测开始时，路径探测发起端维护一个时钟，若在时钟有效期内未收到目的端的路由确认的信息，则认为先导信号路径探测失败。此时采用与步骤 5)相同的操作。

#### 3.1.2　路径选择阶段

路径探测后，携带路径信息的 PSP 协议请求包到达目的端，目的端提取 PSP 请求包携带的路径信息，并维护一个路径信息表，不同的路径通过路径 ID 来标示。路径信息表的结构如图 9 所示。

| PathID | SrcAddr | DsAddr | Weight | PathDelay | OpticalNum | 总耗损 | 节点序列 |
|---|---|---|---|---|---|---|---|

图 9　路径信息表

路径选择是对路径信息表中的路径进行排序。因为在 ASQN 中，影响 QKD 通信的主要因素是损耗(Loss)和时延(Delay)，所以将路径总损耗和总时延作为排序标准，其中损耗对 QKD 通信的影响比时延要大，因此设定路径总权重的计算公式为 $W=Loss\times 0.75+Delay\times 0.25$。其中参数 0.75 和 0.25 的设定是通过实验获得的。

#### 3.1.3　路径确认阶段

路径确认阶段主要完成路径各个节点路由信息的更新和设置。具体步骤如下：

1)目的节点选择最优路径作为光通路路径，并将其路径的节点序列封装到 PSP 确认包中。目的节点向路径序列中目的节点的上一跳节点(设置为 $i$)发送 PSP 确认包。

2)收到 PSP 确认包后，节点 $i$ 的协议控制器 PC 对 PSP 确认包进行解析，并将解析后的信息发送给 RC。若节点 $i$ 为 PSP 确认包的目的节点(QKD 通信发起的源端)，则路径确认阶段结束，呼叫请求阶段成功。否则，执行步骤 3)。

3)节点 $i$ 的 RC 和 LRM 交互，判断目前链路资源是否满足建立光通路路径的需求。若满足，则为光通路路径预留资源，RC 和 RDB 交互，更新量子信道路由表(为连接请求阶段提供支持)，并且将 $i$ 置为 $i-1$，向节点 $i$ 转发 PSP 确认包，执行步骤 3)。若不满足，则执行步骤 4)。

4)构建 PSP 反馈包，将失败信息反馈给目的节点。目的节点将次优路径替换成最优路径，并将最优路径从路径信息表中剔除。执行步骤 1)。

RDB 中更新的量子信道路由表结构如图 10 所示。

| PathID | DsAddr | SrcAddr | NextHop | PreHop |
|---|---|---|---|---|

图 10　量子信道路由表

路径确认阶段的流程如图 11 所示。

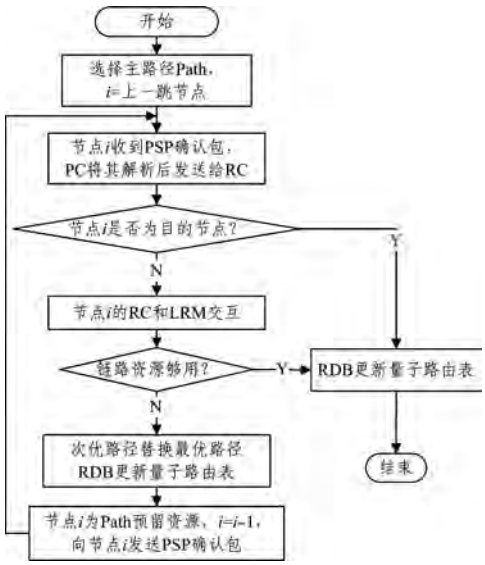


图 11　先导信号协议的路径确认阶段

### 3.2 量子信道的管理技术

量子信道的管理技术主要包括量子信道维护、量子故障恢复以及链路资源管理等相关技术。

#### 3.2.1 量子信道维护

量子信道维护主要包括建立量子维护信道及通过 KeepAlive 协议对量子信道进行维护。

1)信令维护信道的建立

建立信令维护信道首先须进行参数协商,主要通过配置消息 Config 和配置确认消息 ConfigAck 来完成。这些消息包含建立信令信道所需的各项参数(如 KeepAlive 间隔、KeepAlive 死亡间隔等)。当信令维护信道建立过程启动后,信令维护信道进入初始配置(Config)阶段,同时设置死亡间隔(ConfigDeadInterval)。在收到配置确认消息(ConfigAck)之前,Config 消息进行周期性发送。若死亡配置间隔内未收到配置确认消息(ConfigAck),则认为信令维护信道建立失败。

2)KeepAlive 协议

ASQN 中,将 KeepAlive 协议分为两个过程:配置过程和保持过程。配置过程在信令维护信道建立时完成,协商两个参数 KeepAlive 间隔和 KeepAlive 死亡间隔。

KeepAlive 消息沿信令维护信道传输,每到达一个节点都会与该节点的链路资源控制器进行交互,查询量子通道上光开关和光纤链路的状态,若出现故障,则把故障信息传送给 QKD 终端。

#### 3.2.2 量子信道故障管理

链路故障管理涉及故障检测、故障定位和保护转换等过程。故障定位主要通过 KeepAlive 完成,随后故障位置的 LRM 对故障进行分析,判断能否通过配置链路资源对故障进行恢复。若无法定位或无法对已定位的故障进行恢复,则该量子信道失效,管理平面释放该路径上的链路资源,并通知目的节点选择次优路径作为光通路路径。

#### 3.2.3 链路资源管理技术

ASQN 中,QKD 通信具有资源独占性,因此对链路资源进行有效的利用至关重要。

光切换节点主要管理光开关矩阵,包括资源预留、资源分配和资源回收。为实现光开关的预留操作,本文设置了一个光开关状态表,其结构如图 12 所示。

| 光开关ID | 相连接点 | 光开关状态 | 延迟 | 耗损 |
|---|---|---|---|---|

图 12 光开关状态信息表

当对光开关资源预留时,将光开关状态预留标志位设置为 1。同时设定预留死亡间隔,若在预留死亡间隔内,LRM 未对光开关进行实际的物理设置,则将光开关预留标志位重新设置为 0。

在连接建立请求阶段,当有连接对光开关提出申请时,CC 和 LRM 交互,LRM 首先查询光开关资源是否可用,若可用,则对光开关资源进行实际的物理设置,并将其分配给发起请求的连接,同时更新光开关状态表,将光开关状态设置为 1。

在连接释放阶段,CC 和 LRM 交互,LRM 释放相应的光开关资源,将光开关状态设置为 0。

由于 QKD 通信对损耗和时延有较严格的要求,在光切换节点,LRM 对光开关和光纤通路的一些性能指标进行记录,有连接请求时,LRM 首先计算光开关和相应的光纤链路引入的损耗和时延,若这些性能不符合通信要求,则该通信连接在建立的过程中就被筛除。

## 4 仿真及仿真结果

通过网络仿真软件 NS2(Network Simulator Version 2)对 ASQN 网络模型及其关键技术进行仿真实验,以验证 ASQN 网络模型的合理性和各项关键技术对 QKD 网络的适应性。

### 4.1 ASQN 网络模型的仿真

相对于经典网络,ASQN 的不同之处主要在于光切换节点的结构和功能。每个光切换节点都包括光开关矩阵、连接控制器、协议控制器、链路资源管理器、路由控制器以及呼叫控制器等功能组件。

在 NS2 仿真实现时,这些功能组件用具有相关功能的类进行模拟。具体实现如下。

#### 4.1.1 光切换节点

在 NS2 中,通过对节点 node 类的扩展来模拟光切换节点,主要有以下几种:

opt_switch:模拟光开关矩阵;

ASQN_C:模拟连接控制器;

ASQN_PC:模拟协议控制器;

ASQN_LRM:模拟链路资源管理器;

ASQN_RC:模拟路由控制器;

ASQN_CallC:模拟呼叫控制器。

#### 4.1.2 光开关矩阵

设计 optical_switch 类来模拟光开关。设置 3 个属性 keyID,bind_node 和 is_op_open,分别代表光开关的唯一标识、与光开关相连的节点 ID、光开关的状态。

#### 4.1.3 连接控制器

创建 ASQN_CC 类来模拟连接控制器的功能,其中包含两个重要属性:link_map_,用于记录当前连接控制器所维护的连接信息;status_cc,用于记录连接控制器的当前状态。

#### 4.1.4 协议控制器

设计类 ASQN_PC 模拟协议控制器。ASQN_PC 类的主要属性有:status_pc_,用于记录当前 ASQN_PC 类的状态;R_Cache[SIZE],用于记录 ASQN_PC 收到但是还没有来得及处理的数据包;S_Cache[SIZE],用于记录经过 ASQN_PC 处理但是还没发出的数据包。

协议控制器包含两个功能函数:RecvPacket(),用来接收数据包,并对其协议类型进行分析;CalPacket(),用于对不同协议的数据包进行相应的处理。

#### 4.1.5 链路资源管理器

ASQN_LRM 类用来对链路资源管理器进行模拟。主要属性有:switch_map_,表示链路资源管理器的光开关状态表;channel_map_,表示链路资源管理器的信道资源信息表。

ASQN_LRM 具有以下几个主要功能函数:StatusOpticalSwitch(),为光开关状态查询函数;SetOpticalSwitch(),为光开关状态设置函数;SetOSTable(),是对光开关状态信息表设置的函数;IsLinkResourceOK(),用来查询链路资源的状态;SetParam(),用来对链路资源参数进行设置。

#### 4.1.6 路由控制器

路由控制器用 ASQN_RC 类模拟。通过设置一个

m_path_路由表来记录量子信道路径。具体的数据结构采用 map 类型。ASQN_RC 的功能函数如下:

1)receivePSP(),用来接收 PSP 协议包;

2)computeRoutes(),用来 PSP 计算量子信道路径;

3)sendPSP(),用来发送 PSP 包;

4)set_m_path_(),用来对 m_path_进行操作;

5)sendHelloPacket()和 receiveAck(),用来发送和接收 Hello 包,主要用于量子信道维护阶段。

#### 4.1.7　呼叫控制器

呼叫控制器用类 ASQN_CallC 模拟。其属性和函数主要有:status_pc_,用来记录 CallC 当前的状态;R_Cache[ ]和 S_Cache[ ],分别用来缓存待处理和已处理的呼叫信息。

### 4.2　ASQN 先导信号协议仿真

随机选择 4 个网络拓扑对先导信号协议进行模拟。4 个网络拓扑的规模分别为 6 个节点、11 个节点、20 个节点以及 30 个节点。其网络拓扑图分别如图 13－图 16 所示。

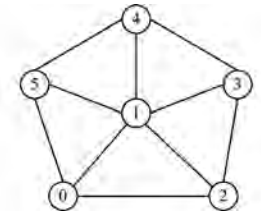

图 13　6 节点网络拓扑

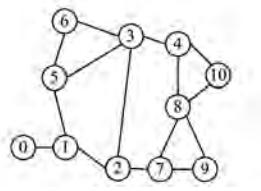

图 14　11 节点网络拓扑

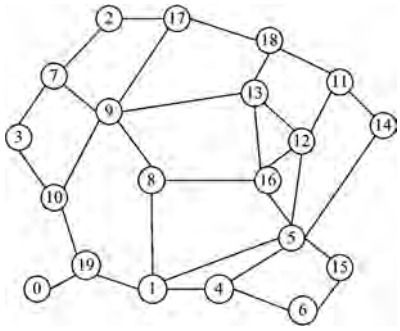

图 15　20 节点网络拓扑

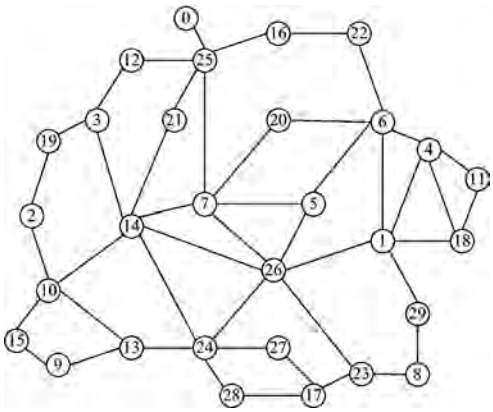

图 16　30 节点网络拓扑

6 节点、20 节点以及 30 节点的网络拓扑中,链路带宽均设为 10 MB,链路长度设在 5～15 km,相邻节点的链路延迟均设为 2 ms。11 节点的网络拓扑中,各条链路的属性如表 1 所列。

表 1　网络链路属性

| 链路起始节点 ID | 链路终端节点 ID | 带宽/Mb | 延迟/ms |
|---|---|---|---|
| 0 | 1 | 10 | 3 |
| 1 | 2 | 10 | 2 |
| 2 | 3 | 10 | 3 |
| 3 | 4 | 10 | 1 |
| 1 | 5 | 10 | 3 |
| 5 | 3 | 10 | 2 |
| 5 | 6 | 10 | 2 |
| 6 | 3 | 10 | 2 |
| 2 | 7 | 10 | 1 |
| 7 | 9 | 10 | 3 |
| 8 | 9 | 10 | 2 |
| 4 | 8 | 10 | 3 |
| 4 | 10 | 10 | 2 |
| 8 | 10 | 10 | 3 |
| 7 | 8 | 10 | 1 |

#### 4.2.1　连通性测试

该测试方案的主要目的是验证先导信号过程能建立量子信道。在 4 个网络拓扑中随机选择一对 QKD 通信进行测试,测试结果如表 2 所列。

表 2　连通性测试

| 网络拓扑 | 发起端 ID | 接收端 ID | 所选量子信道路径序列 | 光损耗/dB | 建立延迟/ms | 光开关个数 | 结果 |
|---|---|---|---|---|---|---|---|
| 6 节点 | 0 | 4 | 0-1-4 | 6.4 | 27.4 | 3 | 成功 |
| 6 节点 | 3 | 5 | 3-1-5 | 6.5 | 27.3 | 3 | 成功 |
| 6 节点 | 0 | 1 | 0-1 | 4.0 | 16.3 | 2 | 成功 |
| 11 节点 | 2 | 8 | 2-7-8 | 6.2 | 22.2 | 3 | 成功 |
| 11 节点 | 3 | 10 | 3-4-10 | 6.3 | 25.1 | 3 | 成功 |
| 11 节点 | 1 | 8 | 1-2-7-8 | 9.0 | 33.7 | 4 | 成功 |
| 10 节点 | 0 | 4 | 0-1-4-3-4 | 10.9 | 54.3 | 5 | 成功 |
| 20 节点 | 1 | 3 | 1-19-10-3 | 11.3 | 38.6 | 4 | 成功 |
| 20 节点 | 8 | 18 | 8-9-13-18 | 8.9 | 39.5 | 4 | 成功 |
| 20 节点 | 4 | 18 | 4-5-12-11-18 | 11.7 | 51.1 | 5 | 成功 |
| 20 节点 | 6 | 7 | 6-4-1-8-9-7 | 13.9 | 63.1 | 6 | 成功 |
| 30 节点 | 0 | 29 | 0-25-7-26-1-29 | 14.1 | 63.6 | 6 | 成功 |
| 30 节点 | 0 | 17 | 0-25-7-26-23-17 | 14.0 | 63.3 | 6 | 成功 |
| 30 节点 | 11 | 10 | 11-4-1-26-14-10 | 13.8 | 63.1 | 6 | 成功 |
| 30 节点 | 9 | 6 | 9-13-24-26-1-6 | 14.2 | 63.2 | 6 | 成功 |

分析表 2 可知,无论是较小的 6 节点还是较大的 30 节点的网络规模,先导信号协议都能找到一条有效的量子信道路径。

目前互联网的链路延迟在几十毫米到几百毫秒的范围内,而在实验中量子信道的建立延迟在几十毫秒左右,是可以接受的。

光损耗是影响 QKD 通信的效率的一个主要因素。根据对国内 QKD 通信现状的调研,设定量子信道总损耗的阈值为 15 dB。在量子信道总损耗小于 15 dB 的情况时,QKD 通信是可行的。该实验中,总损耗均小于 15 dB,达到了预期的目标。

综上，ASQN 中用于量子信道寻径的先导信号协议是可行的。

4.2.2 量子信道建立延迟和光损耗

由于光开关产生的光损耗较大，因此初步判定影响光损耗的主要因素是光开关的个数，为验证此猜想，对表 2 的实验结果进行分析，如图 17 所示。

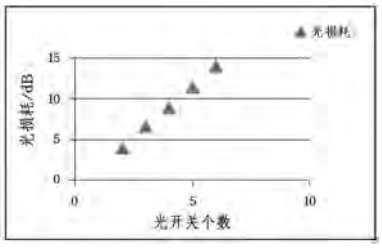


图 17 光开关个数和光损耗的关系

由图 17 结果可以看出，随着光开关个数的增加，光损耗有线性增长的趋势，由此可判定，光开关个数是影响量子通信光损耗的主要因素。

对图 17 中光损耗与光开关个数的关系进行分析，如图 18 所示。由图 18 可以得出结论：在目前光开关的技术条件下，光开关个数越多，引入的光损耗越大。在 ASQN 先导信号协议中，可以通过先导信号协议数据包的 TTL 设置量子信道所能承载的最大光开关个数，避免光损耗超过阈值的路径。

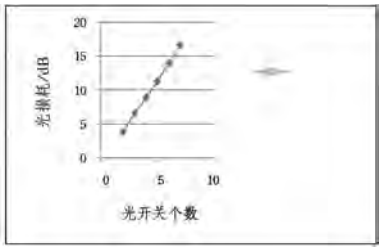


图 18 光损耗变化趋势

为了分析光开关个数对量子信道建立总延迟的影响，对表 2 中的数据进行分析，结果如图 19 所示。

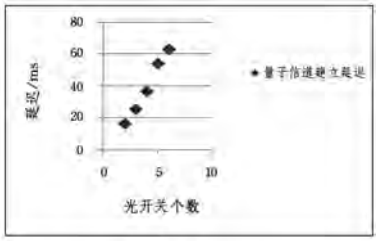


图 19 量子信道建立延迟变化趋势

由图 19 可知，随着光开关个数的增加，量子信道建立总延时有着近似线性的增长。可见，光开关的个数对量子信道总延迟的影响很大。

4.2.3 多路径策略及最优路径选择

先导信号协议是基于多路径策略的，因此能够探测到通信双方之间的多条可行量子信道路径。以 11 个节点的网络拓扑为例，对多路径策略进行测试，以节点 2 为 QKD 发起端，以节点 8 为 QKD 接收端。若先导信号协议多路径策略有效，则会在节点 8 生成一个记录多条路径的路径信息表。测试完成后，打印输出节点 8 的路径信息表，如图 20 所示。

```
root@ubuntu:/home/ict/ns/ns-allinone-2.34/ns-2.34# ns 7.tcl
1 pkts send
PathNodSequence:  2  7  8
PathNodSequence:  2  3  4  8
PathNodSequence:  2  7  9  8
PathNodSequence:  2  3  4  10  8
PathNodSequence:  2  1  5  3  4  8
PathNodSequence:  2  1  5  3  4  10  8
PathNodSequence:  2  1  5  6  3  4  8
PathNodSequence:  2  1  5  6  3  4  10  8
```

图 20 6 节点多路径测试

对图 20－图 22 的分析可知，先导信号协议的多路径策略是有效的。同时，从表 2 可知，对应图 20－图 22 的 QKD 通信，选择的路径均为最优路径。

```
root@ubuntu:/home/ict/ns/ns-allinone-2.34/ns-2.34# ns test20.tcl
1 pkts send
PathNodSequence:  6  4  1  8  9  7
PathNodSequence:  6  4  1  19  10  3  7
PathNodSequence:  6  4  1  19  10  9  7
PathNodSequence:  6  4  5  1  8  9  7
PathNodSequence:  6  4  5  12  13  9  7
PathNodSequence:  6  15  5  1  8  9  7
PathNodSequence:  6  15  5  12  13  9  7
PathNodSequence:  6  4  1  8  9  17  2  7
PathNodSequence:  6  4  1  8  9  10  3  7
PathNodSequence:  6  4  5  1  19  10  3  7
PathNodSequence:  6  15  5  1  19  10  3  7
PathNodSequence:  6  4  1  19  10  9  17  2  7
PathNodSequence:  6  4  5  1  8  9  10  3  7
PathNodSequence:  6  4  5  12  13  18  17  2  7
PathNodSequence:  6  15  5  4  1  19  10  3  7
PathNodSequence:  6  4  5  1  8  9  17  2  7
PathNodSequence:  6  4  5  12  13  9  10  3  7
PathNodSequence:  6  4  5  12  11  18  17  2  7
```

图 21 20 节点网络多路径测试

```
root@ubuntu:/home/ict/ns/ns-allinone-2.34/ns-2.34# ns test30.tcl
1 pkts send
PathNodSequence:  9  13  24  26  1  6  22
PathNodSequence:  9  13  24  26  5  6  22
PathNodSequence:  9  13  24  26  1  4  6  22
PathNodSequence:  9  13  24  26  7  25  16  22
PathNodSequence:  9  13  24  26  7  5  6  22
PathNodSequence:  9  13  24  14  21  25  16  22
PathNodSequence:  9  13  24  26  7  20  6  22
PathNodSequence:  9  13  24  14  7  25  16  22
PathNodSequence:  9  13  24  14  26  1  6  22
PathNodSequence:  9  13  10  14  7  25  16  22
PathNodSequence:  9  13  24  14  26  5  6  22
PathNodSequence:  9  15  10  14  7  25  16  22
PathNodSequence:  9  13  24  14  7  20  6  22
PathNodSequence:  9  13  10  14  26  1  6  22
PathNodSequence:  9  13  24  14  7  5  6  22
PathNodSequence:  9  13  10  14  7  20  6  22
PathNodSequence:  9  15  10  14  26  1  6  22
PathNodSequence:  9  13  10  14  26  5  6  22
PathNodSequence:  9  15  10  14  7  20  6  22
PathNodSequence:  9  13  10  14  7  5  6  22
PathNodSequence:  9  15  10  14  26  5  6  22
PathNodSequence:  9  15  10  14  7  5  6  22
PathNodSequence:  9  13  24  26  5  7  25  16  22
```

图 22 30 节点网络多路径测试

由此可见，先导信号协议的最优路径选择是可靠的，通过 $W=Loss\times 0.75+Delay\times 0.25$ 来对路径进行选择是合理的。

4.2.4　多路并行传输

在实际的网络通信中,应允许网络中多对节点之间并行通信。

以 11 个节点的网络拓扑为例进行测试,选择两对节点(节点 1 和节点 3、节点 7 和节点 10)和 3 对节点(节点 0 和节点 7、节点 4 和节点 6 以及节点 8 和节点 10)进行并发通信,实验结果如图 23 所示。

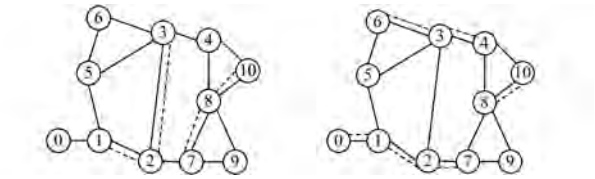

图 23　多对节点并行通信

另外,分别对 6 节点、20 节点以及 30 节点的网络拓扑中的多对并行通信进行测试,通信节点对的选择是随机的。通信节点对的选择和实验结果如表 3 所列。

表 3　并行通信测试表

| 网络拓扑 | 并行通信节点对 | 运行结果 |
|---|---|---|
| 6 节点 | 0 到 3 | 成功 |
| | 4 到 5 | 成功 |
| 6 节点 | 0 到 4 | 成功 |
| | 3 到 5 | 成功 |
| 20 节点 | 1 到 7 | 成功 |
| | 6 到 13 | 成功 |
| | 11 到 17 | 成功 |
| 20 节点 | 0 到 6 | 成功 |
| | 8 到 12 | 成功 |
| | 1 到 6 | 成功 |
| 30 节点 | 10 到 17 | 成功 |
| | 7 到 11 | 成功 |
| | 0 到 7 | 成功 |
| 30 节点 | 1 到 16 | 成功 |
| | 13 到 17 | 成功 |
| | 2 到 9 | 成功 |

通过对表 3 的分析可知,在不同规模的网络拓扑中,先导信号协议均支持并行多路 QKD 通信。

4.2.5　故障恢复测试

故障恢复是 ASQN 中重要的组成部分,以上文 11 个节点的网络拓扑进行仿真实验。首先选取节点 0 到节点 6 的通信进行测试,用 CBR 产生数据流来模拟量子信息的传输。仿真过程如下:

1)在 0.4 s 时运行先导信号协议进行量子信道寻径,寻径结果为 0-1-5-6。

2)在 0.6 s 时开始在路径 0-1-5-6 上传输模拟量子信息的 CBR 数据流,如图 24 所示。

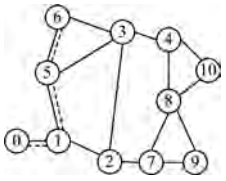

图 24　CBR 数据流模拟量子信息

3)在 0.755 s 时将节点 5 与节点 6 相连的光开关设为故障状态,0-1-5-6 路径上 5-6 阶段开始不可用,量子信道断开,进入故障处理阶段,如图 25 所示。

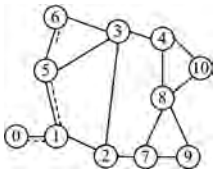

图 25　量子信道断开

图 25 中节点 5 向节点 1 发送的数据包为信道故障探测包(KeepAlive 包),该包将故障信息发送给通信终端节点,通信终端节点根据探测包携带的故障信息对故障进行处理。

图 26 中,在量子信道路径 0-1-5-6 故障后,选择次优路径 0-1-2-3-6 作为量子信道路径,与前述设计相吻合。这说明故障恢复时选择次优路径做为量子信道是可行的。在实验中,随机进行了多条通信的故障恢复过程,并整理其恢复时间如表 4 所列。

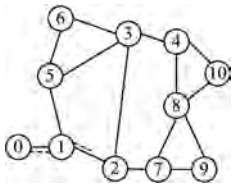

图 26　恢复的量子信道

表 4　量子信道恢复测试

| 量子信道路径 | 故障位置 | 发生故障时间/s | 恢复完成时间/s | 恢复路径 | 恢复耗时/ms |
|---|---|---|---|---|---|
| 0-1-5-6 | 节点 5 | 0.7550 | 0.7988 | 0-1-2-3-6 | 43.8 |
| 2-3-4-10 | 节点 4 | 0.7550 | 0.7905 | 2-7-8-10 | 35.5 |
| 1-2-7-8 | 节点 7 | 0.7550 | 0.8023 | 1-2-3-4-10 | 47.3 |
| 1-2-3 | 节点 2 | 0.7550 | 0.7729 | 1-4-3 | 17.9 |
| 2-3-4 | 节点 3 | 0.7550 | 0.7932 | 2-7-8-4 | 32.2 |
| 0-1-2-7-8-10 | 节点 8 | 0.7550 | 0.8147 | 0-1-2-7-3-4-10 | 59.7 |

对表 4 进行分析可知,当量子信道路径发生故障时,可以在较短的时间内对信道故障进行恢复。

在光开关个数相同的情况下,路径的恢复耗时与建立新的量子信道路径延迟的大小关系如图 27 所示。其中,每个节点对应两个条状矩形,左侧表示量子信道恢复延迟,右侧表示量子信道建立延迟。由图 27 可知,对于相同的光开关个数,量子信道恢复时间比建立新的量子信道的时间要短,最重要的是减少了量子信道寻径过程对网络资源的浪费。

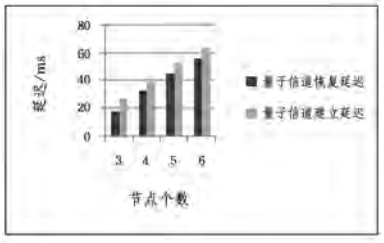


图 27　光开关个数和延迟的关系

(下转第 391 页)

[5] CHENG X，LIU J，GUO L，et al. Identity-based multi-signature and aggregate signature schemes from m-torsion groups [J]. Journal of Electronics (China)，2006，23(4)：569-573.

[6] XU J，ZHANG Z，FENG D. ID-Based Aggregate Signatures from Bilinear Pairings [M]// Cryptology and Network Security. Springer Berlin Heidelberg，2005：110-119.

[7] GENTRY C，RAMZAN Z. Identity-Based aggregate signatures [C]// International Conference on Theory and Practice of Public-Key Cryptography. Springer-Verlag，2006：257-273.

[8] SHIM K. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems & Software，2010，83(10)：1873-1880.

[9] 杜红珍，温巧燕. 高效的基于身份的聚合签名方案[J]. 四川大学学报(工程科学版)，2011，43(1)：87-90.

[10] REDDY P，GOPAL P. Identity-based key-insulated aggregate signature scheme[J]. Journal of King Saud University Computer and Information Sciences，2015，29(3)：303-310.

[11] 寻甜甜，于佳，杨光洋，等. 密钥隔离的无证书聚合签名[J]. 电子学报，2016，44(5)：1111-1116.

[12] 许芷岩，吴黎兵，李莉，何德彪. 无线漫游认证中可证安全的无证书聚合签名方案[J]. 通信学报，2017，38(7)：123-130.

[13] 杜红珍，温巧燕. 无证书聚合签名方案的攻击与改进[J]. 中山大学学报(自然科学版)，2017，56(1)：77-84.

[14] ANDERSON R. Two remarks on public-key cryptology[C]// ACM Conference on Computer and Communications Security. 1997.

[15] BELLARE M，MINER S. A Forward-Secure Digital Signature Scheme[C] // International Cryptology Conference. Springer Berlin Heidelberg，1999：431-448.

[16] BELLARE M，YEE B. Forward security in private key cryptography[J]. Lecture Notes in Computer Science，Springer-Verlag，Berlin，2003：1-18.

[17] ITKIS G，REYZIN L. Forward-Secure Signatures with Optimal Signing and Verifying [M]// Advances in Cryptology - CRYPTO 2001. Springer Berlin Heidelberg，2001：332-354.

[18] KOZLOV A，REYZIN L. Forward-Secure Signatures with Fast Key Update [M] // Security in Communication Networks. Springer Berlin Heidelberg，2003：241-256.

[19] 王彩芬，刘国军，贾爱库，等. 具有前向安全性质的秘密共享方案. [J]电子与信息学报，2006，28(9)：1974-1976.

[20] 汪保友，胡运发. 基于强 RSA 假设的签名方案[J]. 软件学报，2002，13(8)：1729-1734.

[21] 徐文华，贺前华，李韬. 基于强 RSA 假设的数字签名方案[J]. 华中科技大学学报(自然科学版)，2008，36(12)：24-26.

(上接第 363 页)

综上，ASQN 中的量子信道恢复机制所需时间短，占用的网络资源也更少，因此 ASQN 中量子信道故障恢复机制是有效的。

**结束语**　本文分析了现有量子密钥分发网络存在的问题，提出了一种基于光开关切换的 QKD 网络模型 ASQN，同时提出了一种基于多路径策略和源路由技术的先导信号协议。同时，量子密钥分发通信过程需要进行大量信息的交互，而这些 QKD 交互信息是通过经典网络信道传输的，经典网络信道的能力有限，很容易造成网络局部的负载压力过大，因此下一步将研究对经典信息传输的优化。

## 参 考 文 献

[1] 王剑，王振国. 量子密码协议理论研究[M]. 长沙：国防科技大学出版社，2011：79-100.

[2] ID-Quantique (Geneva，Switzerland) [OL]. http://www.idquantique.com.

[3] 万骏. 浅谈量子通信理论及其应用[J]. 科技传播，2018(6)：1674-6708.

[4] BENNET C H，BRASSARD G. Quantum cryptography：Public key distribution andcointossing[C]// IEEE International Conference on Computers Systems and Signal Processing Bangalore. 1984：175-179.

[5] BECHMANN-PASQUINUCCI H，PERES A. Quantum cryptography with 3-state systems[J]. Physical Review Letters，2000，85(15)：3313-3316.

[6] BRUSS D. Optimal eavesdropping in quantum cryptography with six states[J]. Physical Review Letters，1998，81(14)：3018-3021.

[7] BIHAM E，HUNTTER B，MOR T. Quantum cryptographic network based on quantum memories[J]. Physical Review A，1996，54(4)：2651.

[8] TOWNSEND P. Quantum cryptography on optical fibernetworks in European 98 Parallel Processing[J]. Springer，1998，1470：35-46.

[9] TOWNSEND P. Quantum cryptography on multiuser optical fiber network[J]. Nature，1997，385(6611)：47-49.

[10] LONGDELL，FRAVEL J J，SELLARS E，et al. Stopped light with storage times Greater than one second using electrom agentically induced transparency in a solid[J]. Physical Review Letters，2005，95：63-601.

[11] CHEN Z，BCHE N，ZHAO B. Experimental demonstration of a BDCZ quantum repeater node[J]. Nature，2008，454(28)：1098-1101.

[12] YUAN Z S，CHEN Y A. Fault-tolerent quantum repeater with atomic ensembles and linear optical[J]. Physical Review A，2007，76(2)：22-29.

[13] CLAUSEN C，USMANI I，BUSSIERES F. Quatum storage of photonic entanglement in a crystal[J]. Nature，2011，469：508-511.

[14] TOLIVER P，CHAPURAN T E，RUNSEP R J，et al. Experimental investigation of quantum key distribution through transparent optical switch elements[J]. IEEE Photonics Technology Letters，2003，15(11)：1669-1671.

[15] BEIGE A，ENGLERT B G，KURTSIEFER C，et al. Secure communication with single-photon two-qubit states[J]. Physical Review A，2002，35(28)：407-413.

[16] CAI Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping[J]. Physical Review Letters，2003，91(10)：109801.

[17] CAI Q Y，LI B W. Deterministic secure communication without using entanglement[J]. China Physical Letters，2004，21(4)：601-603.

[18] MAN Z X，ZHANG Z J，LI Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations[J]. China Physical Letters，2005，22(1)：18-21.

[19] WANG J，ZHANG Q，TANG C J. Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state[J]. Optics Communications，2006，266(2)：732-737.