



(12) 发明专利

(10) 授权公告号 CN 103001875 B

(45) 授权公告日 2015.03.11

(21) 申请号 201310005105.1

(22) 申请日 2013.01.07

(73) 专利权人 山东量子科学技术研究院有限公司

地址 250101 山东省济南市高新区新泺大街1768号信息通信研究院大厦B座

专利权人 安徽量子通信技术有限公司

(72) 发明人 原磊 黄勇 赵梅生 武宏宇 赵勇

(74) 专利代理机构 济南圣达知识产权代理有限公司 37221

代理人 张勇

(51) Int. Cl.

H04L 12/733(2013.01)

H04L 9/08(2006.01)

(56) 对比文件

CN 102447584 A, 2012.05.09, 全文.

US 2012195428 A1, 2012.08.02,

CN 102291312 A, 2011.12.21,

US 7392378 B1, 2008.06.24,

韩伟等. 基于信任中继的QKD网络研究.《军事通信技术》. 2012, 第33卷(第4期), 第58-62页.

审查员 李红玲

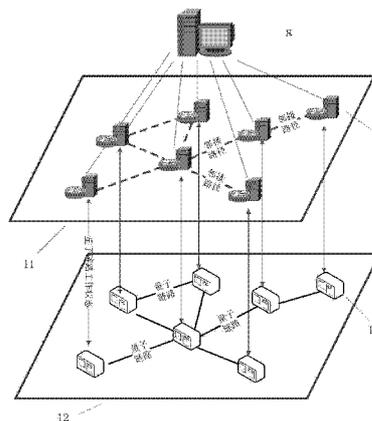
权利要求书3页 说明书12页 附图9页

(54) 发明名称

一种量子密码网络动态路由方法

(57) 摘要

本发明公开了一种量子密码网络动态路由方法,该方法根据量子密码网络的中继节点之间量子密钥量的变化,实现利用量子密码进行加密通信的动态路由选择。本方法为整个量子密码网络的中继节点设置路由服务器,设定量子密码网络的拓扑更新周期;在每个拓扑更新周期内,各个中继节点收集并处理本中继节点的状态信息,将结果上报于路由服务器。路由服务器收集各个中继节点的拓扑状态信息后,生成下一个拓扑更新周期内的量子密码网络拓扑状态信息,并将其发送给量子密码网络的所有中继节点。各个中继节点根据从路由服务器获得的量子密码网络拓扑状态信息,按照最短路径法则计算并确定目的中继节点为任意一个其他中继节点的通信数据的下一跳路由。



CN 103001875 B

1. 一种量子密码网络动态路由方法,该方法根据量子密码网络的中继节点之间量子密钥量的变化,实现利用量子密码进行加密通信的动态路由选择,其特征在于:为整个量子密码网络的中继节点设置路由服务器,设定量子密码网络的拓扑更新周期;在每个拓扑更新周期内,各个中继节点收集并处理本中继节点的状态信息,将结果上报于路由服务器;路由服务器收集各个中继节点的拓扑状态信息后,生成下一个拓扑更新周期内的量子密码网络拓扑状态信息,并将其发送给量子密码网络的所有中继节点;各个中继节点根据从路由服务器获得的量子密码网络拓扑状态信息,按照最短路径法则计算并确定目的中继节点为任意一个其他中继节点的通信数据的下一跳路由,

所述的各个中继节点收集本中继节点的状态信息包括:

- 1) 本中继节点与各个邻接节点之间的量子链路是否处于正常工作状态;
- 2) 本中继节点与各个邻近节点之间的剩余量子密钥量;
- 3) 本中继节点与各个邻近节点之间的量子密钥量的变化速度;

中继节点根据本中继节点与各个邻近节点之间的剩余量子密钥量、本中继节点与各个邻近节点之间的量子密钥量的变化速度判断在下一个拓扑更新周期内本中继节点的邻接路径是否可用。

2. 如权利要求 1 所述的一种量子密码网络动态路由方法,其特征在于,所述的中继节点与某个邻近节点之间的量子密钥量的变化速度由该中继节点与该邻近节点之间的量子密钥量的消耗速度和生成速度决定。

3. 如权利要求 1 或 2 所述的一种量子密码网络动态路由方法,其特征在于:在每个拓扑更新周期内,中继节点根据所述收集到的与某个邻近节点之间的剩余量子密钥量和量子密钥量的变化速度,计算并预测下一个拓扑更新周期内本中继节点与该邻近节点之间的剩余量子密钥量,如果所计算出的剩余量子密钥量小于预定的门限值,则认为本中继节点与该邻近节点之间的邻接路径在下一个拓扑更新周期内不可用,反之可用;各个中继节点将本中继节点信息、本中继节点的邻接量子链路是否处于正常工作状态、本中继节点的邻接路径在下一个拓扑更新周期内是否可用以及所述可用的邻接路径两端所预测的剩余量子密钥量的信息,上报于路由服务器,每个拓扑更新周期上报一次。

4. 如权利要求 3 所述的一种量子密码网络动态路由方法,其特征在于:如果所述中继节点与邻接节点之间的量子链路的工作状态发生变化,则中继节点随时将所述量子链路的工作状态上报给路由服务器。

5. 如权利要求 4 所述的一种量子密码网络动态路由方法,其特征在于,所述路由服务器收集各个中继节点的拓扑状态信息后,生成下一个拓扑更新周期内的量子密码网络拓扑状态信息,所述的量子密码网络拓扑状态信息包括网络中的中继节点信息、量子链路的状态信息、中继节点之间的邻接路径是否可用以及所述可用的邻接路径两端所预测的剩余量子密钥量的信息,路由服务器每隔一个拓扑更新周期将最新的量子密码网络拓扑状态信息发送给量子密码网络中的各个中继节点,各个中继节点收到所述的量子密码网络拓扑状态信息后,立即计算预测并上报本中继节点的拓扑状态信息,所述的本中继节点的拓扑状态信息包括本中继节点信息、本中继节点的邻接量子链路是否处于正常工作状态、本中继节点的邻接路径在下一个拓扑更新周期内是否可用以及所述可用的邻接路径两端所预测的剩余量子密钥量的信息。

6. 如权利要求 5 所述的一种量子密码网络动态路由方法,其特征在于,如果路由服务器通过量子链路一端的中继节点获知此量子链路处于异常工作状态,则路由服务器立即发送存活检测信号确认此量子链路另一端的中继节点是否继续处于工作状态,如果路由服务器在预定的延迟时间内没有收到此中继节点的反馈信息和其上报的拓扑状态信息,则认为此中继节点不可用,在所述的量子密码网络拓扑状态信息中删除此中继节点对应的相关信息。

7. 如权利要求 5 所述的一种量子密码网络动态路由方法,其特征在于:如果在量子密码网络中接入新中继节点,新中继节点主动向路由服务器上上报此新中继节点的基本信息及与此新中继节点的邻接节点之间量子链路的工作状态,同时新中继节点的邻接节点也主动上报与该新中继节点之间的量子链路的工作状态;如果在两个中继节点之间接入新量子链路,新量子链路两端的中继节点主动向路由服务器上上报该量子链路的工作状态;此外,新量子链路两端的中继节点在收到路由服务器的拓扑更新信息后,向路由服务器上上报其邻接路径在下一个拓扑更新周期内是否可用,以及所述可用的邻接路径两端所预测的剩余量子密钥量;路由服务器收到相关中继节点的上报信息后,将新中继节点信息和 / 或新路径信息添加到网络拓扑结构上。

8. 如权利要求 5 至 7 中任意一项所述的一种量子密码网络动态路由方法,其特征在于,所述的最短路径法则如下:

1) 假设整个网络的拓扑信息用图 (G, E) 表示,其中 G 表示顶点的集合, E 表示路径的集合,本中继节点对应 G 中的一个顶点,用 s 表示,构造一个以 s 为根节点的树,将根节点 s 作为树的第一层节点;

2) t 为 G 中任意一个其他顶点, $t \neq s$,如果 E 中存在有 s 到 t 的路径 (s, t) ,则将 t 作为根节点 s 的子节点,也是树的一个第二层节点,并将与路径 (s, t) 相应的边也添加到树中,搜索添加 G 中所有满足条件的第二层节点,并添加相应的边;

3) 已构造的树的层数用 L 表示,将 G 中不属于树的剩余顶点的集合表示为 \bar{G} ,对于任意顶点 $u \in \bar{G}$,考虑 u 到树的第 L 层节点的路径的数量 n :

如果 $n = 0$,则考虑下一个 \bar{G} 中的顶点;

如果 $n > 0$,如果 u 与某个第 L 层节点 r 存在路径,则将此路径相应的边添加到树中,同时将 u 添加到树中,作为树的第 $L+1$ 层节点,如果此路径对应的第 L 层节点 r 在第 L 层出现 m 次,则将此路径相应的边添加到树中 m 次,同时 u 也相应添加 m 次,使节点 u 与每一个第 L 层节点 r 一一对应;如果 u 到树的第 L 层节点的所有路径对应的边均已添加完毕,则将 u 从 \bar{G} 中删除;

4) 如果 G 中还有顶点没有添加到树中,将 $L = L+1$,重复步骤 3),直到所有 G 中的顶点均添加到树中,或重复步骤 3) 后 \bar{G} 中顶点的数量没有变化为止;

5) 对于任意一个中继节点 v ,在树中 s 到 v 的路径即对应图 (G, E) 中 s 到 v 的最短路径,即在网络中中继节点 s 到 v 的最短路径;如果存在多于一条最短路径,则将各条最短路径中每一跳路径的剩余量子密钥量各自按升序排列,首先比较剩余量子密钥量的最小值,选取最小值最大的那条路径,若最小值均相同,则比较次最小值,选取次最小值最大的那条路径,依次类推,若各条最短路径的剩余量子密钥量完全相同,则随机选取一条路径。

9. 如权利要求 8 所述的一种量子密码网络动态路由方法,其特征在于,如果按照所述最短路径法则搜索到的最短路径的下一跳路径不可用,则本中继节点在量子密码网络拓扑状态信息中删除到下一跳的路径,根据修改的量子密码网络拓扑状态信息重新按照所述的最短路径法则寻找最短路径。

一种量子密码网络动态路由方法

技术领域

[0001] 本发明涉及量子通信网络和经典通信网络构建的量子密码网络的通信领域,尤其涉及一种量子密码网络动态路由方法。

背景技术

[0002] 量子通信是近二十年发展起来的新型交叉学科,是量子论和信息论相结合的新的研究领域。近来这门学科已逐步从理论走向实验,并向实用化发展。高效安全的信息传输日益受到人们的关注。

[0003] 物理上,量子通信可以被理解为在物理极限下,利用量子效应实现的高性能通信。信息学上,我们则认为量子通信是利用量子力学的基本原理(如量子态不可克隆原理和量子态的测量塌缩性质等)或者利用量子态隐形传输等量子系统特有属性,以及量子测量的方法来完成两地之间的信息传递。

[0004] 以量子密钥分配(QKD)协议为基础的量子密码技术是现阶段量子通信最重要的实际应用之一。传统的密码学是以数学为基础的密码体制,而量子密码以量子力学为基础,它的安全性是建立在测不准原理、量子的不可克隆及量子相干性等物理特性之上的,被证明是绝对安全的,所以量子密码引起了学术界的高度重视。

[0005] 量子密码网络便是采用量子密码术的一种安全通信网络。如附图 1 所示,量子密码网络是由经典通信网络和 QKD 网络共同构建而成。QKD 网络主要由 QKD 终端设备和量子链路组成,用于密钥分发。经典通信网络使用量子密钥实现数据的加解密和加密数据的传输。一个量子密码网络节点一般是由一个连接于经典通信网络的经典通信终端和连接于量子通信网络的 QKD 设备终端组成。量子密码网络的网络节点一般分为终端节点和中继节点两种。由于量子通信最大距离的限制以及出于网络搭建成本的考虑,许多终端之间并不存在直连的量子链路,不能实现量子密钥的直接分发,它们之间的加密通信数据需要借助中继节点的转发。图 2 和图 3 分别演示了终端节点 Alice 和 Bob 通过一个中继节点和多个中继节点实现量子密钥加密通信的过程。

[0006] 规模较大的量子密码网络会具有大量的中继节点,终端节点间的加密通信数据会借助一个或几个中继节点的中转,而且在数据中转时会有不同的可选的中继节点。如何选择量子密码网络中任意两个节点的通信数据由初始节点到达目的节点所要按顺序经过的中继节点,我们称之为量子密码网络路由。

[0007] 结构简单的量子密码网络,即中继节点和终端节点的数量较少且网络结构相对固定的量子密码网络,一般是通过静态路由方式,即在中继节点中静态的写入所有终端节点之间的路由线路,实现通信数据加解密的路由选择。静态路由的缺点在于当整个网络添加或删除一个中继节点时,几乎需要重新规划网络的路由路径,并更新所有相关的中继节点的路由路径。另一缺点在于当一条路径的量子密钥量不足时,通信双方只能等待这条路径上的 QKD 设备生成足够的量子密钥才能继续通信。

[0008] 量子密码网络规模不断增加。现在量子密码网络已扩展为城域网范围,终端节点

可达上千,中继节点数量可达上百,且由于节点维护和网络规模的扩展,网络拓扑是不断变化的。在这种情况下,配置繁琐的静态路由方法已不再适合,我们需要一种适合量子密码网络的动态路由方法。

[0009] 由于量子密码网络的特殊性,量子密码网络的动态路由方法的设计必须充分考虑以下因素:

[0010] 1. 网络拓扑变化频繁。在量子密码网络中通信数据能否由一个网络节点到达另一个网络节点,即两个节点之间是否存在路由路径,取决于这两个节点之间是否存在足够用的量子密钥,即量子密钥量决定了路由路径是否可用。而量子密钥是不断地被消耗和生成的,因此路径是否可用也可能是在不断变化的。

[0011] 2. 量子密码网络路由需要充分考虑并提高量子密钥的利用率。由于通信数据每经过一跳路径都需要消耗一定量的量子密钥,而量子密钥是量子密码网络最宝贵的网络资源,具有很高的生成成本,所以量子密码网络的路由方法要尽最大可能使通信数据从初始节点到目的节点经历最少跳数路径,以达到消耗最少量子密钥的目的。

[0012] 3. 量子密码网络路由需要考虑通信数据的安全性,即要保证通信数据所要经过的路由路径的每一步具有足够的量子密钥实现数据加密,以实现量子密码网络的绝对安全性。

[0013] 由于以上因素,量子密码网络路由与经典网络的路由具有如下本质的区别:

[0014] 1. 经典网络的路由节点一般为路由器或交换机,只实现数据的转发功能,不对通讯数据进行处理,而量子密码网络路由的中继节点为带有 QKD 设备的网络节点,需要对数据进行解密和加密处理;

[0015] 2. 经典网络路由节点之间的路径是否可用取决于网络带宽或是否存在可靠物理连接,而量子密码网络路由的中继节点之间的路径是否可用(即通信数据是否可以从一个中继节点到达另一个中继节点)取决于路径两端的中继节点之间是否存在可用的量子密钥;

[0016] 3. 量子密码网络的加密机制需要消耗大量的密钥,有时密钥消耗速度远大于生成速度,量子密码网络的路径会由于路径两端的量子密钥量不足而处于不可用状态,故相对于经典网络,量子密码网络的路径状态变化往往较为频繁。

[0017] 以上特点决定了量子密码网络的路由不能直接采用经典网络路由方法。相对于经典网络路由,量子密码网络的动态路由方法必须具有以下特点:一是网络中路径两端的量子密钥量是决定网络拓扑状态的一个最重要的路由参数之一;二是中继节点必须更快更准确的收集中继节点和路径的变化信息;三是量子密码网络路由需要具有更快的网络拓扑收敛速度;四是量子密码网络路由要具有较高的量子密钥利用率。

[0018] 而迄今为止,还没有一种完善的适合量子密码网络的动态路由方法被提出。能检索到的量子密码网络路由的相关专利如下所述:

[0019] 中国专利 No. 201010144106.0 公开了“用于多用户光量子通信网络的量子路由器及其路由方法”,此专利方案应用于量子通信网络,通过控制光交叉连接器,实现两个用户之间的连接,并没有考虑通信路径上的量子密钥量是否充足。美国专利 NO. 8, 122, 242B2、NO. 7, 392, 378B1 和 NO. 7, 441, 267B1,这三篇专利是一系列相关专利,讲的是网络节点系统对将要进入通信网络的数据流在已知多条量子密码网络路由路径的前提下如何选择路由

路径的技术方案,节点系统的不同路由路径具有不同的加密能力,根据某条路径的密钥量等参数估计该条路径的加密能力,选择加密能力最强的路径作为下一跳的路径。但是,该专利方案存在两个缺点:第一,该专利方案所选择的总体路由路径可能不是最短路径;第二,该专利方案所选择的总体路由路径中加密能力最低的某一跳路径,可能比另一条可选的总体路由路径中加密能力最低的某一跳路径的加密能力更低,而一条路径的加密能力往往受制于其加密能力最低的那一跳路径的加密能力。

[0020] 以上量子密码网络路由相关专利,均没有提供量子密码网络动态路由的完整方案,即如何根据量子密码网络拓扑状态的变化,将通信数据从初始节点通过选择中继节点传送到目的节点,并能在保证通信安全性的同时消耗较少的量子密钥。

发明内容

[0021] 本发明提出一种量子密码网络动态路由方法,该方法根据量子密码网络拓扑状态的变化实现通信数据在量子密码网络节点之间加密通信的动态路由选择,可允许量子密码网络动态扩展并根据网络拓扑状态的变化实现数据安全通信。量子密码网络中,一般一个中继节点会直接连接数个终端节点和中继节点,一个终端节点通常只连接唯一的一个中继节点。

[0022] 本发明的技术方案如下所述:

[0023] 量子密码网络中的每个中继节点所获取的网络拓扑状态信息每隔固定时间更新一次,间隔的时间我们称之为拓扑更新周期。

[0024] 为整个网络的中继节点设置路由服务器,各个中继节点在每个拓扑更新周期内收集并处理本中继节点状态信息,各个中继节点收集的本中继节点的状态信息包括:

[0025] (1) 本中继节点与各个邻接节点之间的量子链路是否处于正常工作状态;

[0026] (2) 本中继节点与各个邻近节点之间的量子密钥量;

[0027] (3) 本中继节点与各个邻近节点之间的量子密钥量的变化速度。

[0028] 其中状态信息(3)取决于量子链路量子密钥的生成速度和经典信道加解密时量子密钥的消耗速度,一般根据密钥量的统计值计算得出。

[0029] 中继节点根据上述状态信息(2)、(3)判断在下一个拓扑更新周期内本中继节点的邻接路径是否可用。邻接路径是指本中继节点与邻近节点之间的最短量子密码网络路由路径。邻接路径是否可用取决于路径两端是否存在足够的量子密钥。

[0030] 中继节点的状态信息可能不仅限于上述列举的信息,其他所有与网络拓扑状态相关的信息或可能影响网络拓扑状态的信息,根据实际应用情况都可以位于被考虑之列。

[0031] 在每一个拓扑更新周期内,各中继节点将邻接路径的状态,即在下一个拓扑更新周期内是否可用,和所述可用的邻接路径两端所预测的剩余量子密钥量,以及邻接量子链路的工作状态、中继节点信息等,上报于路由服务器。路由服务器收集各个中继节点的拓扑状态信息后,生成下一个拓扑更新周期内的网络拓扑状态信息,并将其发送给网络的所有中继节点,更新各个中继节点的网络拓扑状态信息。路由服务器每隔固定时间(即一个拓扑更新周期),向各个中继节点下发一次最新的网络拓扑状态信息。此处的网络拓扑状态信息特指量子密码网络中继节点信息、量子链路的的状态信息以及各中继节点之间的邻接路径信息。各中继节点可以根据从服务器获得的网络拓扑状态信息,计算本中继节点到其他中继

节点的最短路径,即跳数最少的路径,为经过本中继节点的网络终端通信数据提供路由选择。

[0032] 上述邻接路径的状态(即在下一个拓扑更新周期内是否可用)的判断方法如下:

[0033] 根据邻接路径两端剩余的量子密钥量及其变化速度,计算并预测下一个拓扑更新周期邻接路径两端的剩余量子密钥量,如果剩余的量子密钥量小于预定的门限值,则认为此路径在下一个拓扑更新周期内不可用,反之可用。

[0034] 如果中继节点与其邻接节点的量子链路的工作状态发生变化,则随时将工作状态上报给路由服务器。如果中继节点通过 QKD 设备获知其与某邻接节点之间的量子链路处于异常状态,并将此异常状态上报给路由服务器,则路由服务器立即发送存活检测信号确认该条量子链路另一端的中继节点是否存活,如果路由服务器在预定的延迟时间内没有收到该中继节点的反馈信息及其拓扑状态上报信息,则认为此量子链路另一端的中继节点不可用,删除另一端的中继节点对应的网络拓扑状态信息。

[0035] 对于新接入网络的中继节点,新中继节点需要向路由服务器上报告其基本信息及所有的邻接量子链路的工作状态,同时新中继节点的邻接节点也需要上报与该新中继节点之间的量子链路的工作状态;对于在两个中继节点之间新接入的直连的量子链路,量子链路两端的中继节点需要上报本链路的工作状态。此外,新量子链路两端的中继节点在收到路由服务器的拓扑更新信息后,要上报邻接路径在下一个拓扑更新周期内是否可用,以及所述可用的邻接路径两端所预测的剩余量子密钥量。路由服务器收到相关中继节点的上报信息后,将新中继节点信息和 / 或新路径信息添加到网络拓扑结构上。

[0036] 上述最短路径的计算方法如下:

[0037] 1) 假设整个网络的拓扑信息用图 (G, E) 表示,其中 G 表示顶点的集合, E 表示路径的集合,本中继节点对应 G 中的一个顶点,用 s 表示,构造一个以 s 为根节点的树,将根节点 s 作为树的第一层节点;

[0038] 2) t 为 G 中任意一个其他顶点, $t \neq s$,如果 E 中存在有 s 到 t 的路径 (s, t) ,则将 t 作为根节点 s 的子节点,也是树的一个第二层节点,并将与路径 (s, t) 相应的边也添加到树中,搜索添加 G 中所有满足条件的第二层节点,并添加相应的边;

[0039] 3) 已构造的树的层数用 L 表示,将 G 中不属于树的剩余顶点的集合表示为 \bar{G} ,对于任意顶点 $u \in \bar{G}$,考虑 u 到树的第 L 层节点的路径的数量 n :

[0040] 如果 $n=0$,则考虑下一个 \bar{G} 中的顶点;

[0041] 如果 $n>0$,如果 u 与某个第 L 层节点 r 存在路径,则将此路径相应的边添加到树中,同时将 u 添加到树中,作为树的第 $L+1$ 层节点,如果此路径对应的第 L 层节点 r 在第 L 层出现 m 次,则将此路径相应的边添加到树中 m 次,同时 u 也相应添加 m 次,使节点 u 与每一个第 L 层节点 r 一一对应;如果 u 到树的第 L 层节点的所有路径对应的边均已添加完毕,则将 u 从 \bar{G} 中删除;

[0042] 4) 如果 G 中还有顶点没有添加到树中,将 $L=L+1$,重复步骤 3),直到所有 G 中的顶点均添加到树中,或重复步骤 3) 后 \bar{G} 中顶点的数量没有变化为止;

[0043] 5) 对于任意一个中继节点 v ,在树中 s 到 v 的路径即对应图 (G, E) 中 s 到 v 的最短路径,即在网络中中继节点 s 到 v 的最短路径;如果存在多于一条最短路径,则将各条最短路径中每一跳路径的剩余量子密钥量各自按升序排列,首先比较剩余量子密钥量的最小

值,选取最小值最大的那条路径,若最小值均相同,则比较次最小值,选取次最小值最大的那条路径,依次类推,若各条最短路径的剩余量子密钥量完全相同,则随机选取一条路径。

[0044] 如果搜索到的最短路径的下一跳路径不可用,则本中继节点在网络拓扑状态信息中删除到下一跳的路径,重新按照所述的方法寻找次最短路径。下列情况有可能导致最短路径的下一跳路径不可用:

[0045] i. 网络设备工作状态异常;

[0046] ii. 一个拓扑更新周期没有结束,量子密钥提前消耗殆尽。

[0047] 对本发明所采用的一些术语,解释如下:

[0048] 量子密码网络:采用量子密码术的一种安全通信网络,是由经典通信网络和 QKD 网络共同构建而成,QKD 网络主要由 QKD 终端设备和量子链路组成,用于密钥分发,可在两个 QKD 终端设备之间共享用于加解密通信的量子密钥,经典通信网络使用量子密钥实现数据的加解密和加密数据的传输。

[0049] 量子链路:QKD 网络中用于连接 QKD 终端设备、实现量子密钥分发的连接链路,一般为光纤或自由空间。

[0050] 量子密码网络中继节点:简称为中继节点,区别于终端节点,用于实现不存在直连的量子链路的终端节点之间加密通信数据的安全中转,如附图 2 和附图 3 所示。

[0051] 量子密码网络路由:量子密码网络中的通信数据按顺序经由一个或几个中继节点从初始终端节点到达目的终端节点所经过的中继节点所构成的路径。

[0052] 邻接节点:与本中继节点搭建直连的量子链路、可直接生成共享量子密钥的其他中继节点。

[0053] 邻近节点:与本中继节点存在共享量子密钥的其他中继节点,但与本中继节点之间不一定存在直连的量子链路。

[0054] 邻接路径:本中继节点与邻近节点之间的最短量子密码网络路由路径。

[0055] 本发明的工作原理如下:

[0056] 1. 集中式网络拓扑管理。为整个量子密码网络的中继节点设置路由服务器,设定量子密码网络的拓扑更新周期;在每个拓扑更新周期内,各个中继节点收集并处理本中继节点的状态信息,将结果上报于路由服务器;路由服务器收集各个中继节点的拓扑状态信息后,生成下一个拓扑更新周期内的量子密码网络拓扑状态信息,并将其发送给量子密码网络的所有中继节点;各个中继节点根据从路由服务器获得的量子密码网络拓扑状态信息,计算本中继节点到其他中继节点的最短路径,即跳数最少的路径,为经过本中继节点的网络终端通讯信息提供路由选择。

[0057] 2. 中继节点状态信息收集。在每个拓扑更新周期内,网络中的各个中继节点收集本中继节点的状态信息,包括本中继节点与各个邻接节点之间的量子链路的工作状态、本中继节点与各个邻近节点之间的剩余的量子密钥量、本中继节点与各个邻近节点之间的量子密钥量的变化速度。

[0058] 3. 中继节点预测下一个拓扑更新周期内邻接路径是否可用。在每个拓扑更新周期内,中继节点根据与邻近节点之间的剩余量子密钥量和量子密钥量的变化速度,计算并预测下一个拓扑更新周期内中继节点间的剩余量子密钥量,如果剩余量子密钥量小于预定的门限值,则认为此路径在下一个拓扑更新周期不可用,反之可用,将这一结果和所述可用的

邻接路径两端所预测的剩余量子密钥量上报于路由服务器,每个拓扑更新周期上报一次。

[0059] 4. 量子链路工作状态的上报。如果 QKD 设备故障或链路故障或其它故障导致量子链路不能正常产生量子密钥,则均认为此量子链路处于异常状态;否则,认为此量子链路处于正常状态。中继节点可以通过 QKD 设备获知其邻接量子链路是否处于异常状态,并将结果上报于路由服务器,每个拓扑更新周期上报一次。如果中继节点与邻接节点的量子链路的工作状态发生变化,则随时将工作状态上报给路由服务器。

[0060] 5. 路由服务器接收并处理拓扑状态信息。路由服务器接收各个中继节点的拓扑状态信息。所述的中继节点的拓扑状态信息主要包括本中继节点的节点信息、本中继节点的邻接路径在下一个拓扑更新周期内是否可用、所述可用的邻接路径两端所预测的剩余量子密钥量和本中继节点的邻接量子链路是否处于正常工作状态。所述的本中继节点的节点信息,主要是指本中继节点的标识信息,以及一些路由协议中可能涉及到的相关信息。

[0061] 如果一条路径两端的中继节点同时判定此路径可用,则路由服务器判定此路径可用;如果路径两端的任意一个中继节点判定此路径不可用,则路由服务器判定此路径不可用。正常情况下路径两端中继节点的判定结果应该是一致的。

[0062] 如果路由服务器获知一个中继节点的邻接量子链路工作状态异常,则立即发送信号到此量子链路的另一端的中继节点,探测其是否处于存活状态。如果路由服务器在预定的延迟时间内没有收到该中继节点的反馈信息和其上报的拓扑状态信息,则判定此量子链路两端的中继节点之间的邻接路径不可用。

[0063] 6. 路由服务器分发网络拓扑状态信息。所述的网络拓扑状态信息包括网络中的中继节点信息、量子链路的状态信息、中继节点之间的邻接路径是否可用以及所述可用的邻接路径两端所预测的剩余量子密钥量的信息。路由服务器每隔一个拓扑更新周期定期地将最新的网络拓扑状态信息分发给每个中继节点。中继节点收到最新的网络拓扑状态信息后,立即按照 3 所述的方法计算预测并上报本中继节点的邻接路径在下一个拓扑更新周期内是否可用以及所述可用的邻接路径两端所预测的剩余量子密钥量的信息,并按照 4 所述的方法上报本中继节点的邻接量子链路是否处于正常工作状态,以及将本中继节点的节点信息上报给路由服务器。

[0064] 7. 中继节点的删除。路由服务器向中继节点主动发送存活检测信息,如果路由服务器在预定的延迟时间内没有收到该中继节点的反馈信息,并且也没有收到该中继节点上报的拓扑状态信息,则认为此中继节点已死亡,删除此中继节点对应的网络拓扑状态信息。一般下列情况,路由服务器会向中继节点主动发送存活检测信息:

[0065] ▶如果中继节点对于路由服务器分发的网络拓扑状态信息在一个拓扑更新周期内,没有上报本中继节点的拓扑状态信息。

[0066] ▶如果量子链路一端的中继节点上报此链路工作状态异常,路由服务器会向此量子链路另一端的中继节点发送存活检测信息。

[0067] 8. 中继节点和量子链路的接入。对于新接入网络的中继节点,新中继节点需要向路由服务器上报其基本信息及所有的邻接量子链路的工作状态,同时新中继节点的邻接节点也需要上报与该新中继节点之间的量子链路的工作状态;对于在两个中继节点之间新接入的直连的量子链路,量子链路两端的中继节点需要上报本链路的工作状态。此外,新量子链路两端的中继节点在收到路由服务器的拓扑更新信息后,要上报邻接路径在下一个拓扑

更新周期内是否可用,以及所述可用的邻接路径两端所预测的剩余量子密钥量。路由服务器收到相关中继节点的上报信息后,将新中继节点信息和 / 或新路径信息添加到网络拓扑结构上。

[0068] 9. 最优路由路径的计算。中继节点从服务器获得整个网络的拓扑状态信息,按照下列方法计算本中继节点到其他中继节点的最短路径:

[0069] 1) 假设整个网络的拓扑信息用图 (G, E) 表示,其中 G 表示顶点的集合, E 表示路径的集合,本中继节点对应 G 中的一个顶点,用 s 表示,构造一个以 s 为根节点的树,将根节点 s 作为树的第一层节点;

[0070] 2) t 为 G 中任意一个其他顶点, $t \neq s$,如果 E 中存在有 s 到 t 的路径 (s, t) ,则将 t 作为根节点 s 的子节点,也是树的一个第二层节点,并将与路径 (s, t) 相应的边也添加到树中,搜索添加 G 中所有满足条件的第二层节点,并添加相应的边;

[0071] 3) 已构造的树的层数用 L 表示,将 G 中不属于树的剩余顶点的集合表示为 \bar{G} ,对于任意顶点 $u \in \bar{G}$,考虑 u 到树的第 L 层节点的路径的数量 n :

[0072] 如果 $n=0$,则考虑下一个 \bar{G} 中的顶点;

[0073] 如果 $n>0$,如果 u 与某个第 L 层节点 r 存在路径,则将此路径相应的边添加到树中,同时将 u 添加到树中,作为树的第 $L+1$ 层节点,如果此路径对应的第 L 层节点 r 在第 L 层出现 m 次,则将此路径相应的边添加到树中 m 次,同时 u 也相应添加 m 次,使节点 u 与每一个第 L 层节点 r 一一对应;如果 u 到树的第 L 层节点的所有路径对应的边均已添加完毕,则将 u 从 \bar{G} 中删除;

[0074] 4) 如果 G 中还有顶点没有添加到树中,将 $L=L+1$,重复步骤 3),直到所有 G 中的顶点均添加到树中,或重复步骤 3) 后 \bar{G} 中顶点的数量没有变化为止;

[0075] 5) 对于任意一个中继节点 v ,在树中 s 到 v 的路径即对应图 (G, E) 中 s 到 v 的最短路径,即在网络中中继节点 s 到 v 的最短路径;如果存在多于一条最短路径,则将各条最短路径中每一跳路径的剩余量子密钥量各自按升序排列,首先比较剩余量子密钥量的最小值,选取最小值最大的那条路径,若最小值均相同,则比较次最小值,选取次最小值最大的那条路径,依次类推,若各条最短路径的剩余量子密钥量完全相同,则随机选取一条路径。

[0076] 10. 次最优路由路径的计算。如果中继节点检测到通过 9 计算的最短路径的下一跳路径不可用,则本中继节点在网络拓扑状态信息中删除到下一跳的路径,重新按照 9 所述的方法寻找次最优路由路径。

[0077] 本发明上述技术方案的有益效果如下:

[0078] i. 本发明提出一种完善的量子密码网络动态路由方案。网络节点之间的通信数据在量子密码网络中的中继路径,不再是单一的静态路径,而是依据网络拓扑状态的变化动态选择的最短路径。

[0079] ii. 本技术方案的路由方法对于网络中继节点的删除和添加具有自适应性。这有利于网络的动态扩展。

[0080] iii. 根据量子密码网络的规模和复杂性设置路由服务器采用集中式网络拓扑管理。这种方式满足量子密码网络对网络状态具有较快收敛速度的要求。

[0081] iv. 量子密码网络最宝贵的网络资源是量子密钥,在最优路由路径的选择上采用最短路径优先法则,节约了量子密钥,提高了网络资源利用率,提高了网络性能。

[0082] v. 本路由方案充分考虑了所选路径每一跳的安全性,从而保证了通信数据的安全性。

附图说明

[0083] 图 1 :量子密码网络的一般结构,为现有技术附图 ;

[0084] 图 2 :终端节点 Alice 和 Bob 通过一个中继节点实现量子密钥加密通信,为现有技术附图 ;

[0085] 图 3 :终端节点 Alice 和 Bob 通过多个中继节点实现量子密钥加密通信,为现有技术附图 ;

[0086] 图 4 :城域量子密码网络局部 ;

[0087] 图 5 :量子密码网络路由架构图 ;

[0088] 图 6 :路由服务器主要功能模块 ;

[0089] 图 7 :路由客户端主要功能模块 ;

[0090] 图 8 :量子密码网络中继节点路径连接状态示意图 ;

[0091] 图 9 :表示网络拓扑结构的邻接矩阵 ;

[0092] 图 10 :中继节点 27 到其他中继节点的最短路径搜索树 ;

[0093] 图 11 :本动态路由方法的一般工作流程 ;

[0094] 其中,1、第一量子集控站,2、第二量子集控站,3、第三量子集控站,4、第四量子集控站,5、光交换机,6、一级用户,7、二级用户,8、路由服务器,9、经典通信设备,10、量子通信设备,11、经典通信层,12、量子通信层,13、路由客户端,14、第一网络接口模块,15、第一拓扑信息收发模块,16、中继节点存活检测模块,17、拓扑信息逻辑处理模块,18、第一中继节点信息数据库模块,19、第二网络接口模块,20、第二拓扑信息收发模块,21、存活检测反馈模块,22、路由计算模块,23、拓扑信息处理模块,24、拓扑信息收集模块,25、路由选择模块,26、第二中继节点信息数据库模块,27、第一中继节点,28、第二中继节点,29、第三中继节点,30、第四中继节点,31、第五中继节点,32、第六中继节点,33、第七中继节点,34、第八中继节点。

具体实施方式

[0095] 下面结合附图和实施例对本发明作进一步说明 :

[0096] 本实施例针对的是一个城域范围的量子密码网络,终端节点上千,中继节点少于 100 个。本城域网的中继节点为量子集控站,集控站一般直接下挂几个终端节点或通过光交换机 5 下挂数个终端节点。附图 4 为城域量子密码网络局部示意图,第一量子集控站 1、第二量子集控站 2 直接下挂终端节点,第四量子集控站 4 通过光交换机 5 下挂终端节点,第三量子集控站 3 直接下挂终端节点同时通过光交换机 5 下挂终端节点。其中,量子集控站通过光交换机 5 下挂的终端节点为一级用户 6,量子集控站直接下挂的终端节点为二级用户 7。

[0097] 城域量子密码网络终端节点之间的安全通信可分为下列三种情况 ;

[0098] 1. 同一光交换机 5 下终端节点的通信 ;

[0099] 2. 同一集控站下不同光交换机 5 下终端节点的通信,包括直接下挂终端节点的通

信；

[0100] 3. 不同集控站下终端节点的通信。

[0101] 前两种情况较为简单,本实施例只考虑第 3 种情况。第 3 种情况中由于终端节点与集控站的路径唯一,所以只考虑终端节点所属集控站之间的路由即可。

[0102] 一、路由度量和路由准则

[0103] 路由度量和路由准则是路由算法所要考虑的最重要的两个方面。我们以跳数作为路由度量,以最短跳数作为路由准则。当有多条路径到达相同的目的节点时,中继节点需要一种机制来计算最优路径。度量是指派给路由的一种变量,作为一种手段,度量可以按最好到最坏,或按最先选择到最好选择的顺序对路由进行等级划分。

[0104] 考虑到量子密码网络路由的特殊性,我们用跳数作为路由度量。由于每经过一个集控站中继节点便需要一次解密加密过程,同一通信数据路由跳数越少,其加密通信消耗的量子密钥量越少。现阶段量子密码网络通信量受限于量子密钥生成速度,以路径的最短跳数作为路由的第一准则,以增大量子密钥的使用效率。

[0105] 二、拓扑收敛

[0106] 拓扑收敛是指网络中的中继节点所获得的关于整个网络的拓扑状态信息与整个网络的真实拓扑状态信息相一致。量子密码网络中通信数据在集控站之间的每一步中继都以集控站之间存在量子密钥为先决条件,量子密钥消耗殆尽,此路径即为不可用路径,整个网络的中继节点需要立即甚至提前获知这种拓扑状态信息的变化。

[0107] 为了满足快速收敛的要求,我们采用集中式拓扑信息管理策略,所有的中继节点只需要直接与路由服务器 8 进行两点之间的交互即可获知整个网络的拓扑状态信息,这很明显优于传统经典网络路由基于洪泛的拓扑状态信息传递方法的收敛速度,后置收敛需要信息交互的次数往往与网络或网络局部的直径有关,远大于前者。

[0108] 三、基于集中式网络拓扑管理的路由算法框架

[0109] 设置路由服务器 8,设定拓扑更新周期;在每个拓扑更新周期内,位于集控站节点的路由客户端 13 收集并处理本中继节点的状态信息,将结果上报于路由服务器 8。路由服务器 8 收集各个路由客户端 13 的拓扑状态信息后,生成下一个拓扑更新周期内的整个网络的拓扑状态信息,包括网络中的中继节点信息、量子链路的状态信息、表示网络拓扑结构的邻接矩阵以及可用的邻接路径两端所预测的剩余量子密钥量,并将其发送给网络的所有路由客户端 13。路由服务器 8 每隔一个拓扑更新周期,向各个路由客户端 13 下发一次最新的网络拓扑状态信息。各个路由客户端 13 根据从路由服务器 8 获得的网络拓扑状态信息,计算本中继节点到其他集控站节点的最短路径(跳数最少的路径),为经过本中继节点的网络终端通信数据提供路由选择。

[0110] 本实施例中为了与设置的路由服务器 8 相对应,将中继节点中即集控站中负责路由信息处理的模块称之为路由客户端 13,所有路由模块均为软模块,置于高性能计算机中,其相关的路由计算具有足够好的计算速度。同时路由客户端 13 和路由服务器 8 的网络带宽环境足够好,其路由拓扑信息的传递有足够小的网络延迟。

[0111] 附图 5 为量子密码网络路由架构图。整个量子密码网络路由架构分为经典通信层 11 和量子通信层 12。量子通信层 12 由集控站中的量子通信设备 10 及量子通信设备之间的量子链路构成,用于密钥分发,可在两个量子通信设备 10 之间共享用于加解密通信的量子

密钥。经典通信层 11 由集控站中的含有路由客户端 13 的经典通信设备 9 及路由服务器 8 构成,用于实现数据的加解密和加密数据的传输。集控站中的含有路由客户端 13 的经典通信设备 9 之间存在邻接路径,与量子链路相对应。在每个拓扑更新周期内,集控站中的含有路由客户端 13 的经典通信设备 9 的路由客户端 13 根据所收集的本中继节点的状态信息,计算并预测下一个拓扑更新周期内邻接路径两端的剩余量子密钥量,如果剩余量子密钥量小于预定的门限值,则认为此邻接路径不可用,反之可用,将这一结果和所述可用的邻接路径两端所预测的剩余量子密钥量上报于路由服务器 8,每个拓扑更新周期上报一次。集控站中的含有路由客户端 13 的经典通信设备 9 的路由客户端 13 通过集控站中的量子通信设备 10 获知量子链路是否处于正常工作状态,并将结果上报于路由服务器 8,每个拓扑更新周期上报一次。如果量子链路的工作状态发生变化,则随时将工作状态上报给路由服务器 8。

[0112] 四、路由服务器功能

[0113] 路由服务器 8 的主要功能模块如附图 6 所示,包括第一网络接口模块 14、第一拓扑信息收发模块 15、中继节点存活检测模块 16、拓扑信息逻辑处理模块 17 和第一中继节点信息数据库模块 18。

[0114] ▶第一网络接口模块 14,按照网络通信协议收发网络数据,并校验数据收发的准确性,并负责网络通信的并发处理。

[0115] ▶第一拓扑信息收发模块 15,负责接收网络数据中各个路由客户端 13 的拓扑状态信息,将整个网络的拓扑状态信息发送到路由客户端 13。

[0116] ▶中继节点存活检测模块 16,向中继节点发送存活检测信息,接收中继节点的反馈信息,负责确认中继节点是否存活。

[0117] ▶拓扑信息逻辑处理模块 17,通过数据库存储、查询各个中继节点的基本配置信息和量子链路的状态信息,根据路由客户端 13 上报的拓扑状态信息和中继节点存活检测模块 16 的信息,生成表示网络拓扑结构的邻接矩阵;将第一拓扑信息收发模块 15 获得的网络各中继节点信息和量子链路的状态信息存入中继节点信息数据库。

[0118] ▶第一中继节点信息数据库模块 18,存储各个中继节点的基本配置信息和量子链路的状态信息。

[0119] 五、路由客户端功能

[0120] 路由客户端 13 的主要功能模块如附图 7 所示,包括第二网络接口模块 19、第二拓扑信息收发模块 20、存活检测反馈模块 21、路由计算模块 22、拓扑信息处理模块 23、拓扑信息收集模块 24、路由选择模块 25 和第二中继节点信息数据库模块 26。

[0121] ▶第二网络接口模块 19,按照网络通信协议收发网络数据,并校验数据收发的准确性。

[0122] ▶第二拓扑信息收发模块 20,负责接收路由服务器 8 发送的网络拓扑状态信息,将本中继节点的拓扑状态信息上报到路由服务器 8。

[0123] ▶存活检测反馈模块 21,接收路由服务器 8 发送的存活检测信息,并发送反馈信息,告知路由服务器 8 本中继节点仍存活。

[0124] ▶路由计算模块 22,按照路由服务器 8 发送的表示网络拓扑结构的邻接矩阵、可用的邻接路径两端所预测的剩余量子密钥量和数据库中的中继节点信息计算本中继节点到

其他中继节点的最短路径,并将最短路径存入数据库。

[0125] ▶拓扑信息处理模块 23,处理拓扑信息收集模块 24 收集的信息,确定上报路由服务器 8 的拓扑状态信息,包括本中继节点信息、本中继节点的邻接路径在下一个拓扑更新周期内是否可用、所述可用的邻接路径两端所预测的剩余量子密钥量和本中继节点的邻接量子链路是否处于正常工作状态;将第二拓扑信息收发模块 20 获得的网络各中继节点信息和量子链路的状态信息存入中继节点信息数据库。

[0126] ▶拓扑信息收集模块 24,收集本中继节点的状态信息,包括本中继节点与各个邻接节点之间的量子链路的工作状态、本中继节点与各个邻近节点之间的剩余的量子密钥量、本中继节点与各个邻近节点之间量子密钥的生成速度和消耗速度。

[0127] ▶路由选择模块 25,读取中继节点信息数据库中的路径信息,为通信数据提供下一跳路由。

[0128] ▶第二中继节点信息数据库模块 26,存储各个中继节点的基本配置信息、量子链路的状态信息和路由计算模块 22 计算得到的路径信息。

[0129] 六、最短路径算法

[0130] 中继节点从服务器获得整个网络的拓扑状态信息,按照下列方法计算本中继节点到其他中继节点的最短路径:

[0131] 1) 假设整个网络的拓扑信息用图 (G, E) 表示,其中 G 表示顶点的集合, E 表示路径的集合,本中继节点对应 G 中的一个顶点,用 s 表示,构造一个以 s 为根节点的树,将根节点 s 作为树的第一层节点;

[0132] 2) t 为 G 中任意一个其他顶点, $t \neq s$,如果 E 中存在有 s 到 t 的路径 (s, t) ,则将 t 作为根节点 s 的子节点,也是树的一个第二层节点,并将与路径 (s, t) 相应的边也添加到树中,搜索添加 G 中所有满足条件的第二层节点,并添加相应的边;

[0133] 3) 已构造的树的层数用 L 表示,将 G 中不属于树的剩余顶点的集合表示为 \bar{G} ,对于任意顶点 $u \in \bar{G}$,考虑 u 到树的第 L 层节点的路径的数量 n :

[0134] 如果 $n=0$,则考虑下一个 \bar{G} 中的顶点;

[0135] 如果 $n>0$,如果 u 与某个第 L 层节点 r 存在路径,则将此路径相应的边添加到树中,同时将 u 添加到树中,作为树的第 $L+1$ 层节点,如果此路径对应的第 L 层节点 r 在第 L 层出现 m 次,则将此路径相应的边添加到树中 m 次,同时 u 也相应添加 m 次,使节点 u 与每一个第 L 层节点 r 一一对应;如果 u 到树的第 L 层节点的所有路径对应的边均已添加完毕,则将 u 从 \bar{G} 中删除;

[0136] 4) 如果 G 中还有顶点没有添加到树中,将 $L=L+1$,重复步骤 3),直到所有 G 中的顶点均添加到树中,或重复步骤 3) 后 \bar{G} 中顶点的数量没有变化为止;

[0137] 5) 对于任意一个中继节点 v ,在树中 s 到 v 的路径即对应图 (G, E) 中 s 到 v 的最短路径,即在网络中中继节点 s 到 v 的最短路径;如果存在多于一条最短路径,则将各条最短路径中每一跳路径的剩余量子密钥量各自按升序排列,首先比较剩余量子密钥量的最小值,选取最小值最大的那条路径,若最小值均相同,则比较次最小值,选取次最小值最大的那条路径,依次类推,若各条最短路径的剩余量子密钥量完全相同,则随机选取一条路径。

[0138] 七、集控站节点和量子链路的接入。

[0139] 对于新接入网络的集控站节点,新中继节点需要向路由服务器 8 上报其基本配置

信息及所有的邻接量子链路的工作状态,同时新中继节点的邻接节点也需要上报与该新中继节点之间的量子链路的工作状态;对于在两个中继节点之间新接入的直连的量子链路,量子链路两端的中继节点需要上报本链路的工作状态。此外,新量子链路两端的中继节点在收到路由服务器 8 的拓扑更新信息后,要上报邻接路径在下一个拓扑更新周期内是否可用,以及所述可用的邻接路径两端所预测的剩余量子密钥量。路由服务器 8 收到相关节点的上报信息后,将新中继节点和 / 或新路径信息添加到网络拓扑结构上。

[0140] 图 8 给出了一个小型的量子密码网络中继节点在某一个拓扑更新周期内的预测连接图,其中虚线表示路径上的量子密钥不足,不能实现此路径上的量子密钥加密通信,即路径不可用;实线表示可以进行此路径上的量子密钥加密通信,即路径可用。

[0141] 图 9 给出了表示图 8 网络拓扑结构的邻接矩阵。矩阵维数为 8×8 ,表示图 8 中的第一中继节点 27 到第八中继节点 34 这 8 个中继节点之间邻接路径是否可用。矩阵元素 (i, j) (其中 $1 \leq i \leq 8, 1 \leq j \leq 8$) 表示第 i 个中继节点到第 j 个中继节点的邻接路径是否可用,其值为 1 表示可用,为 0 表示不可用或不存在邻接路径;矩阵对角元素均为 0,表示中继节点与自身不构成邻接路径。例如,图 8 中的第一中继节点 27 到第四中继节点 30 的邻接路径可用,则相应的图 9 中的矩阵元素 $(1, 4)$ 的值为 1;图 8 中的第二中继节点 28 到第六中继节点 32 的邻接路径不可用,则相应的图 9 中的矩阵元素 $(2, 6)$ 的值为 0;图 8 中的第五中继节点 31 与第七中继节点 33 之间不存在邻接路径,则相应的图 9 中的矩阵元素 $(5, 7)$ 的值为 0;图 8 中第三中继节点 29 与第八中继节点 34 点之间不存在邻接路径,则相应的图 9 中的矩阵元素 $(3, 8)$ 的值为 0。

[0142] 图 10 表示了第一中继节点 27 根据图 9 邻接矩阵所表示的网络拓扑结构构造的最短路径搜索树。特别地,第一中继节点 27 到第六中继节点 32 存在两条最短路径,而第一中继节点 27 到第八中继节点 34 存在三条最短路径,此时需要根据本发明中所述最短路径算法的步骤 5)来选取一条最短路径。例如,若第一中继节点 27 与第四中继节点 30、第七中继节点 33 之间所预测的剩余量子密钥量分别为 70kB 和 50kB,而第六中继节点 32 与第四中继节点 30、第七中继节点 33 之间所预测的剩余量子密钥量分别为 40kB 和 60kB;由于第一中继节点 27 到第六中继节点 32 的两条最短路径中,各自每一跳路径所预测的剩余量子密钥量的最小值分别为 40kB 和 50kB,且 50kB 大于 40kB,则选取第一中继节点 27 经由第七中继节点 33 到达第六中继节点 32 的这条路径,作为第一中继节点 27 到第六中继节点 32 的最短路径。

[0143] 如图 11 所示,本路由算法的一般的实现流程,分为以下具体步骤:

[0144] 步骤(1),设置路由服务器;

[0145] 步骤(2),中继节点状态信息周期性收集处理;

[0146] 步骤(3),中继节点拓扑状态信息周期性上报;

[0147] 步骤(4),路由服务器收集并处理各中继节点的拓扑状态信息;

[0148] 步骤(5),路由服务器向各个中继节点分发网络拓扑状态信息;

[0149] 步骤(6),中继节点的最优路径计算。

[0150] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,所属领域技术人员应该明白,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

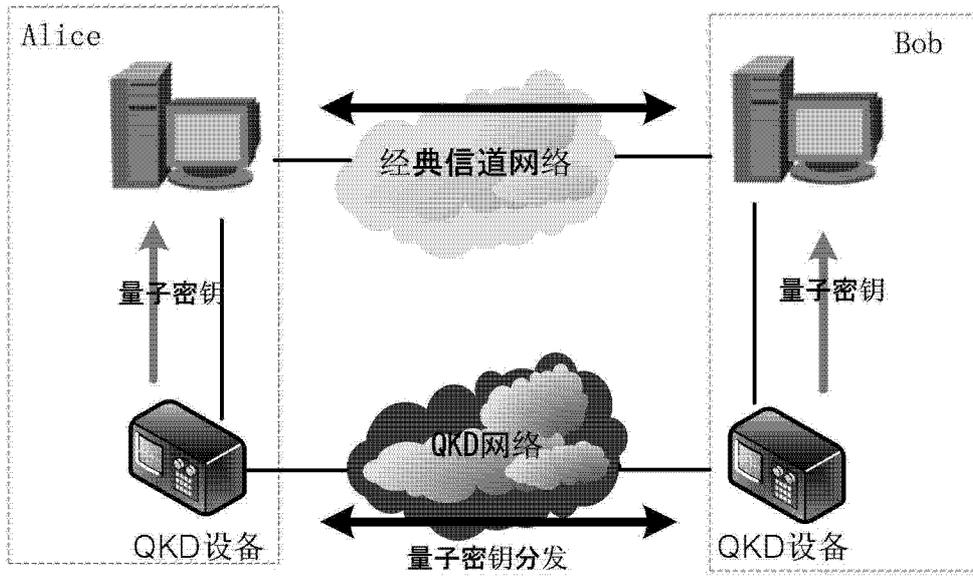


图 1

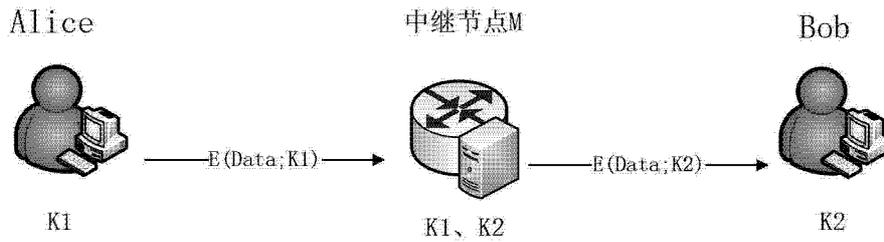


图 2

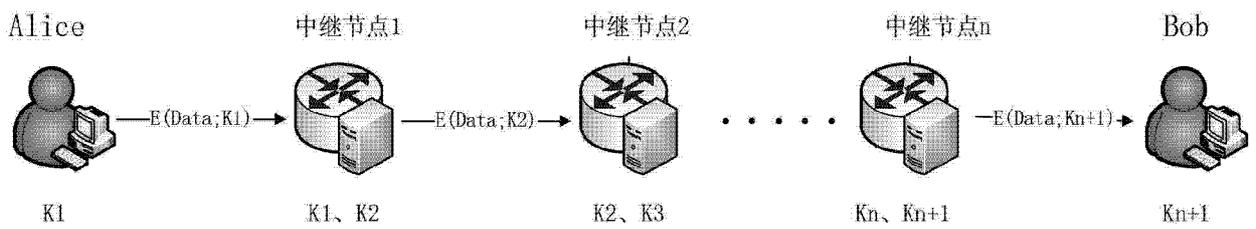


图 3

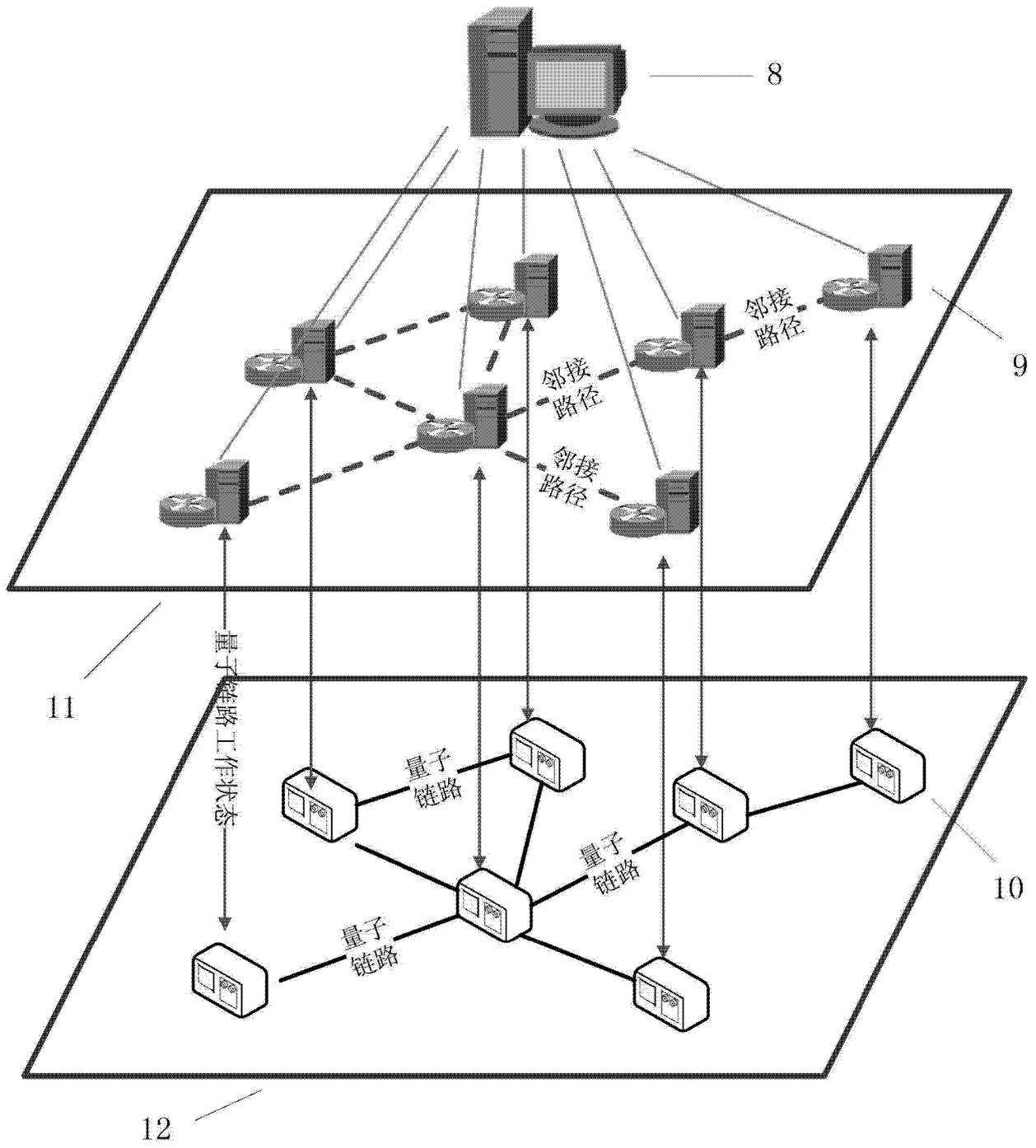


图 5

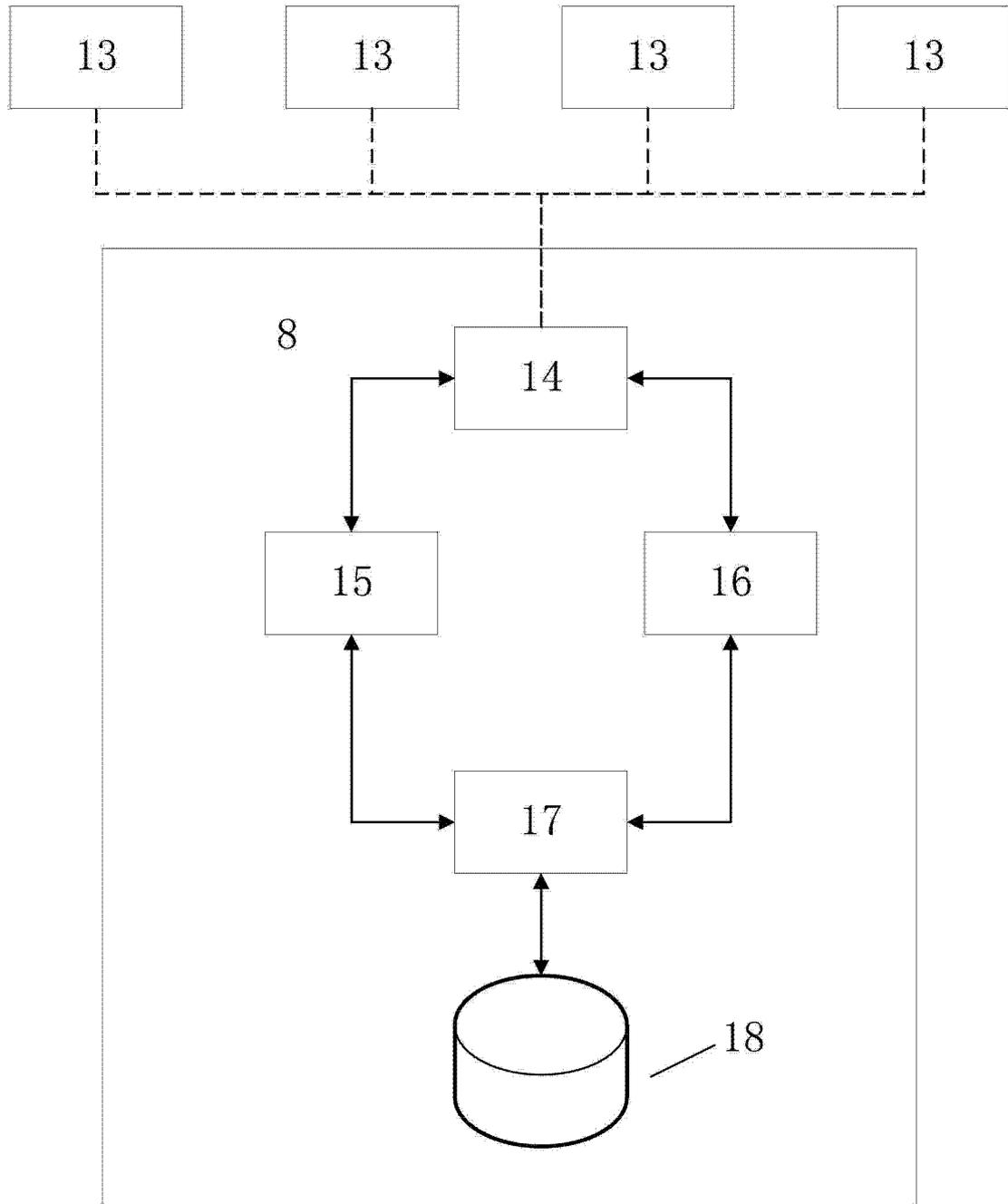


图 6

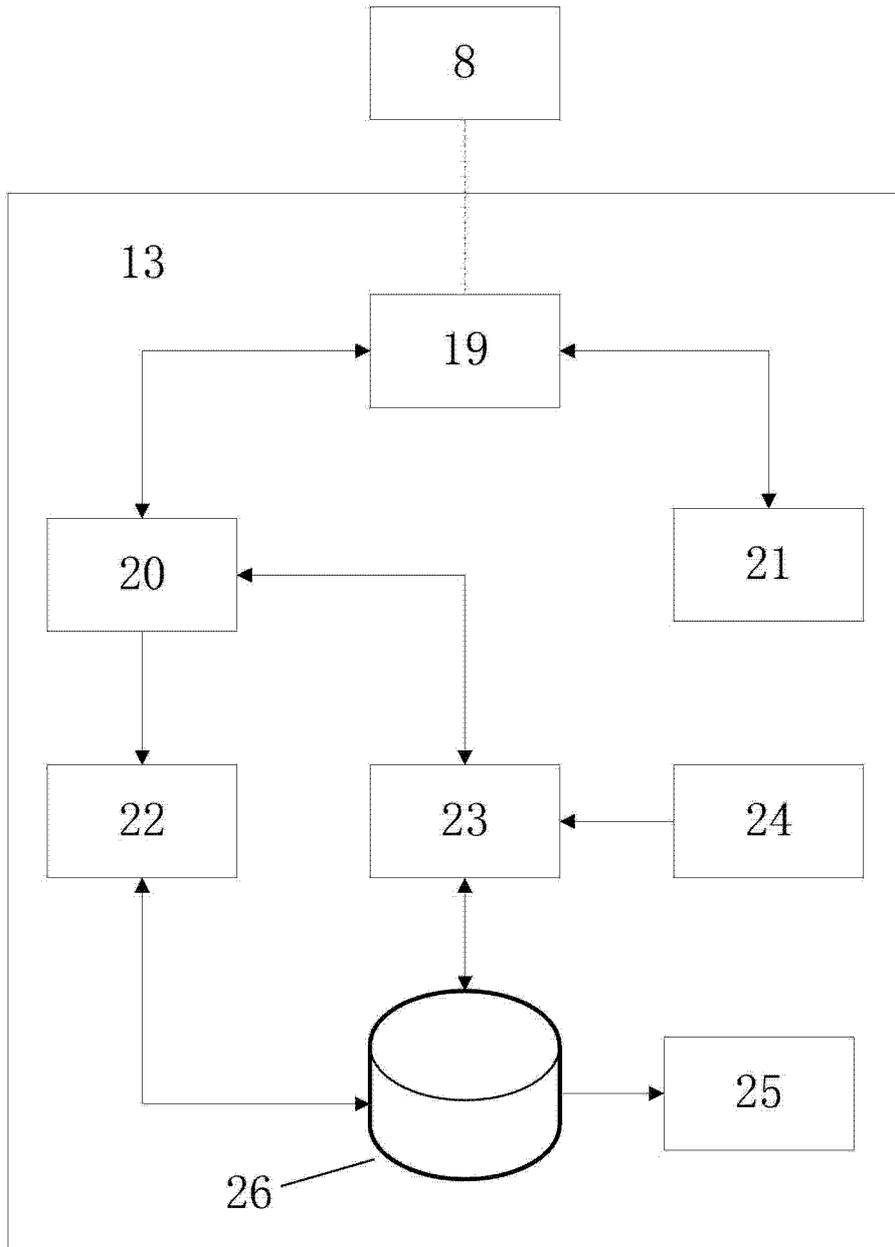


图 7

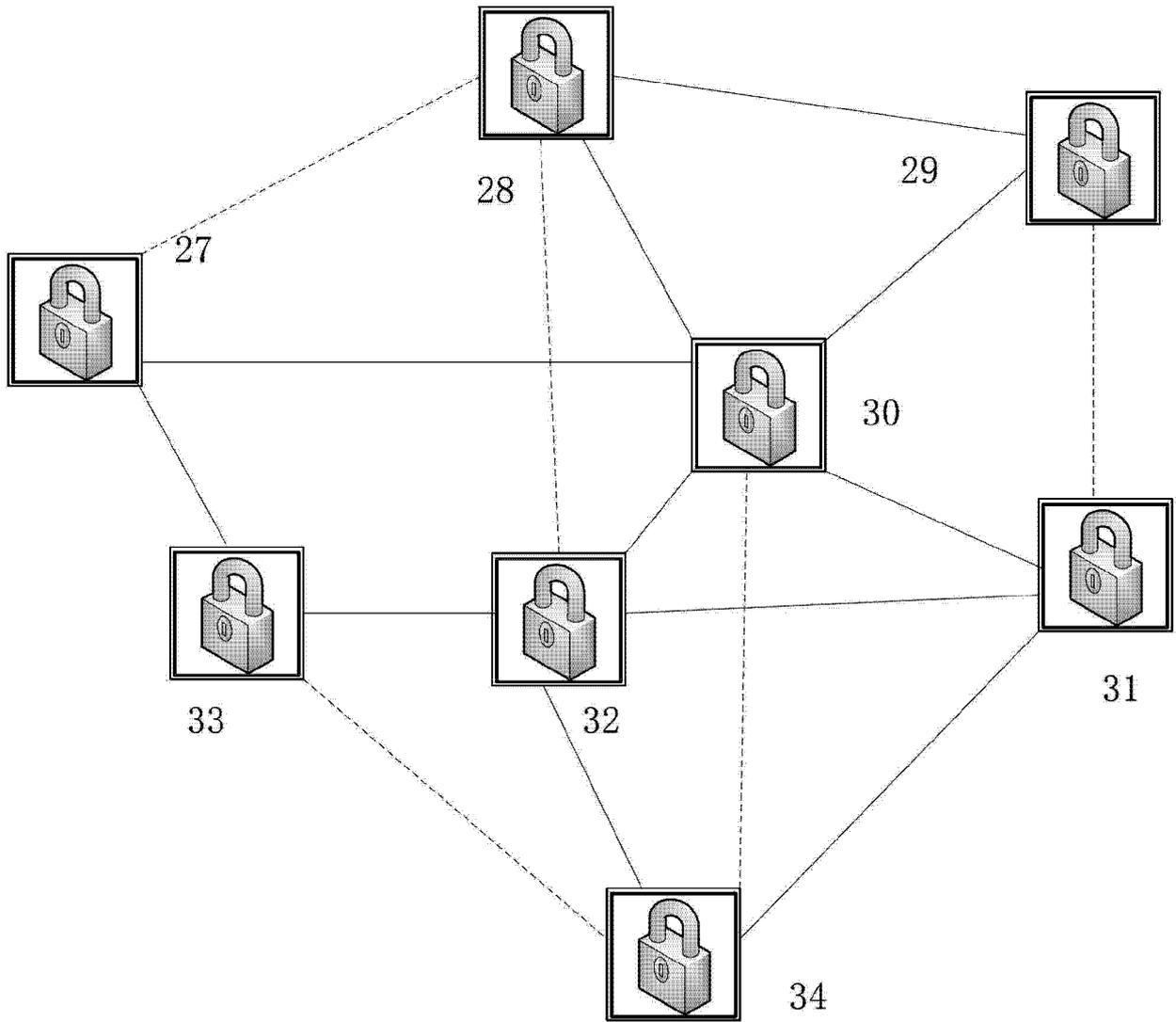


图 8

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

图9

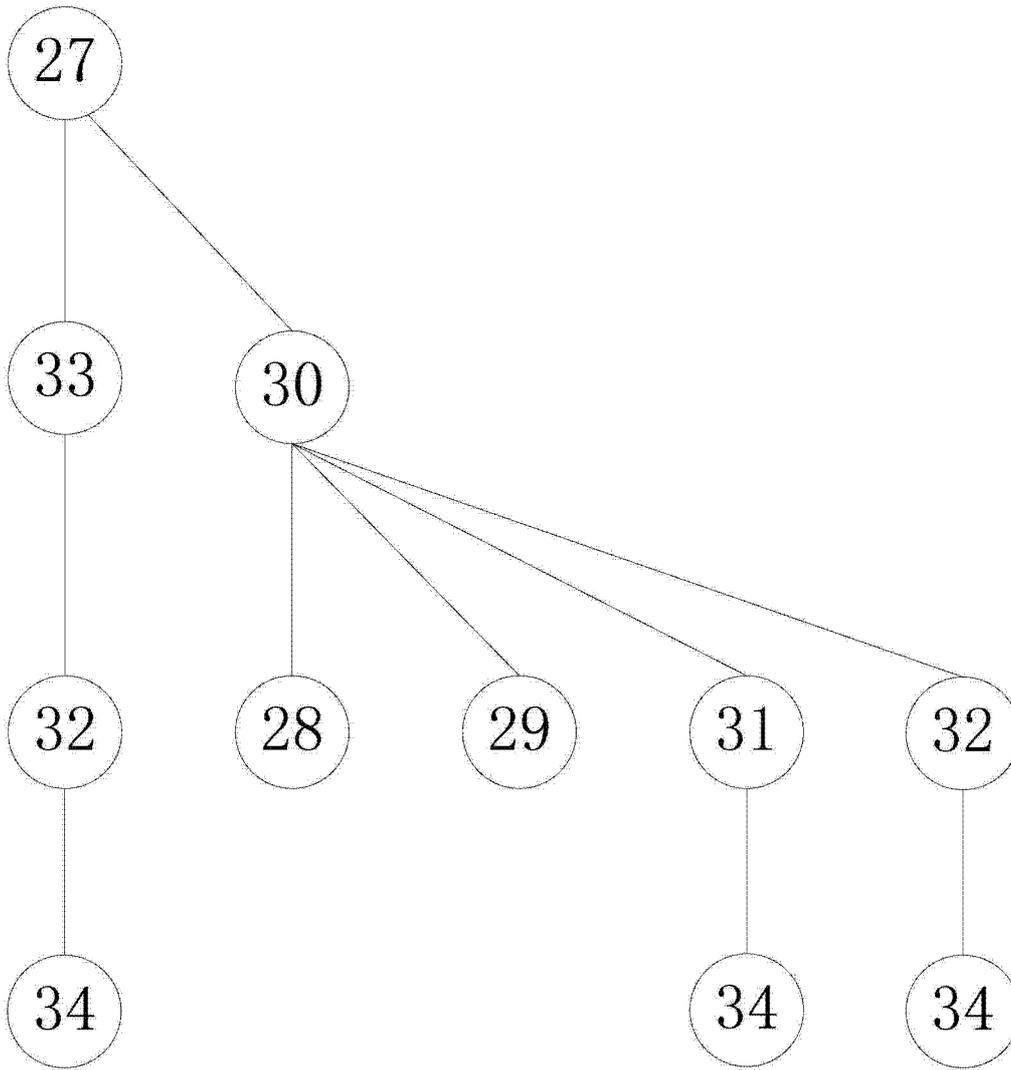


图 10

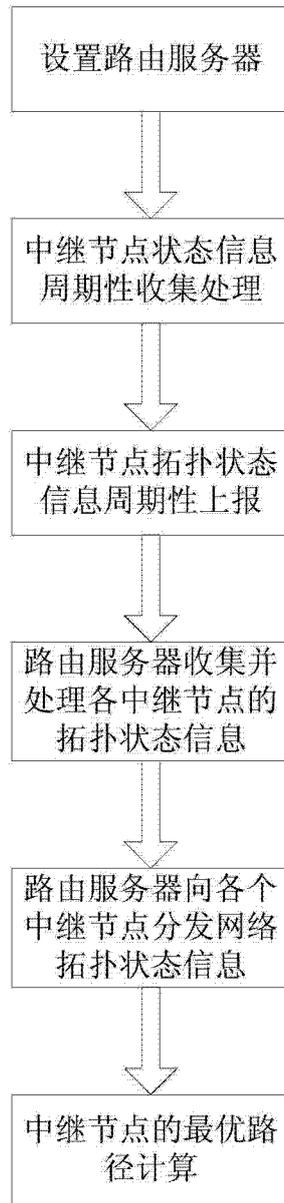


图 11