(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112235318 A
(43)申请公布日 2021.01.15

(21)申请号 202011288381.X

(22)申请日 2020.11.17

(71)申请人 国科量子通信网络有限公司
地址 201203 上海市浦东新区自由贸易试验区芳春路400号1幢3层

(72)发明人 聂勋坦 韩圣龙

(74)专利代理机构 北京汉鼎理利专利代理事务所(特殊普通合伙) 11618
代理人 潘满根

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 12/715(2013.01)
H04L 12/721(2013.01)
H04L 12/723(2013.01)

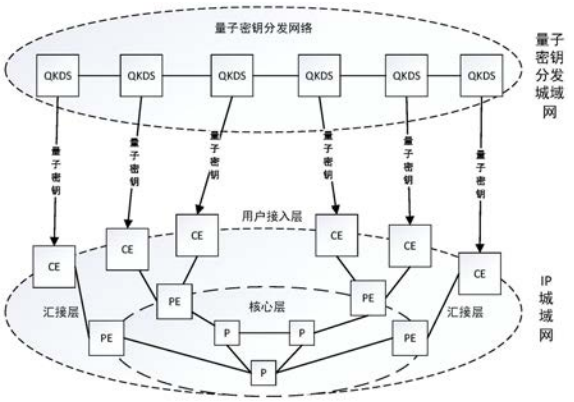
权利要求书1页 说明书5页 附图4页

(54)发明名称

实现量子安全加密的城域网系统

(57)摘要

本发明提供一种实现量子安全加密的城域网系统,所述城域网系统包括IP城域网和量子密钥分发城域网,所述IP城域网是通过MPLS技术组建的数据传输网,为企业用户提供VPN组网;所述量子密钥分发城域网为企业用户的通信提供加密所需的量子密钥。本发明的城域网系统使得在城域网中传输数据得到保护,防止对网络资源的非法访问,对网络传输的窃听和破坏,保护网络使用者的合法利益。



CN 112235318 A

1.实现量子安全加密的城域网系统,其特征在于,所述城域网系统包括IP城域网和量子密钥分发城域网,所述IP城域网是通过MPLS技术组建的数据传输网,为企业用户提供VPN组网;所述量子密钥分发城域网为企业用户的通信提供加密所需的量子密钥。

2.根据权利要求1所述的城域网系统,其特征在于,在所述IP城域网中部署具有量子密钥加密功能的用户网络边缘设备,该设备支持扩展使用量子密钥,采用IPsec的加密通信机制,实现接入用户的量子安全通信;和

所述用户网络边缘设备通过量子密钥分发系统安全接口接入所述量子密钥分发城域网,获取对称量子密钥对,用于IPsec VPN的协商及会话加密过程。

3.根据权利要求2所述的城域网系统,其特征在于,所述IP城域网包括核心层、汇接层和接入层,所述核心层包括运营商核心路由器,用于核心网络路由及数据的转发;所述汇接层包括运营商边界路由器,用于提供用户边缘设备的接入,为VPN用户建立虚拟路由转发;所述接入层包括所述用户边缘设备,该设备支持IPsec扩展使用量子密钥,在该设备上实现量子加密功能。

4.根据权利要求3所述的城域网系统,其特征在于,所述核心层包括多台核心路由器,核心路由器支持MPLS、OSPF和/或BGP协议。

5.根据权利要求4所述的城域网系统,其特征在于,多台核心路由器进行环形组网。

6.根据权利要求5所述的城域网系统,其特征在于,所述核心路由器与骨干网连接。

7.根据权利要求3所述的城域网系统,其特征在于,所述量子密钥分发城域网包括核心控制层、汇接层和所述接入层;所述核心控制层包括量子密钥管理系统,用于城域网内的量子密钥分发系统的路由调度、密钥生成控制和密钥管理;所述汇接层包括量子密钥分发系统的接收端,用于对接所述接入层的量子密钥分发系统的发送端,实现点到点的量子密钥生成;所述接入层包括量子密钥分发系统的发送端,用于接收用户边缘设备的量子密钥请求,并经过量子密钥协商与生成后响应密钥请求,为用户边缘设备建立IPsec VPN提供量子密钥。

8.根据权利要求7所述的城域网系统,其特征在于,在VPN用户节点,部署支持IPSec扩展使用量子密钥的用户边缘设备和量子密钥分发系统的发送端。

9.根据权利要求8所述的城域网系统,其特征在于,所述VPN用户节点的量子密钥分发系统的发送端接入所述量子密钥分发城域网的量子密钥分发系统的接收端,全网量子密钥分发系统接入所述量子密钥管理系统。

10.根据权利要求7所述的城域网系统,其特征在于,在所述用户边缘设备中配置需要加密的访问控制策略,加密感兴趣流被触发后,用户边缘设备向与其相连的量子密钥分发系统的发送端请求量子密钥,响应的量子密钥可用于IPSec VPN的会话密钥。

实现量子安全加密的城域网系统

技术领域

[0001] 本发明涉及通信安全领域,具体涉及一种实现量子安全加密的城域网系统。

背景技术

[0002] 上世纪九十年代以来,科学家开始了量子密码的研究。量子密钥分发(QKD)技术基于“海森堡测不准原理”和“量子不可复制原理”,使用每比特单光子传输随机数,由此发送端和接收端能够产生相同随机数密钥。量子密钥分发不依赖于计算的复杂性来保证通信安全,而是基于量子力学基本原理,量子密码系统的安全性不会受到计算能力和数学水平的不断提高的威胁。近几年,国内量子密钥分发技术已经得到全国范围的广泛应用。

[0003] 近年来,随着城域网组网技术的不断发展,在城域网上开展的业务逐渐多样化。同时,越来越多的新型互联网业务对城域网的安全性也有了更高的要求,如:电子政务、电子商务、企业分支互联、远程办公等业务对数据传输提出了很高的加密要求。

[0004] MPLS(Multi-Protocol Label Switching)技术已成为目前主流的城域网方案,其组建的逻辑隔离网络为多样化的应用开展提供了平台。MPLS(Multi-Protocol Label Switching)VPN(Virtual Private Network)技术利用了开放的MPLS网络建立专用的数据传输通道,为企业的远程分支机构互联提供虚拟专用网络。MPLS通过路由的控制来实现了网络的隔离,相对于传统的IP网络有了较高的安全性,但是MPLS VPN在路由信息交换及数据传输时仍然存在被攻击的可能。数据在MPLS网络传输过程中,没有经过加密处理,无法保证数据的安全性。

[0005] 目前,互联网中主流的数据加密通信方案是IPsec(Internet Protocol Security)。IPSec是IETF制定的为保证在Internet上传送数据的安全保密性能的三层隧道加密协议。IPSec在IP层对IP报文提供安全服务。IPSec协议本身定义了如何在IP数据包中增加字段来保证IP包的完整性、私有性和真实性,以及如何加密数据包。使用IPsec,数据就可以安全地在公网上传输。IPsec提供了两个主机之间、两个安全网关之间或主机和安全网关之间的保护。IPsec对传输中数据加密所获取的密钥主要通过IKE(Internet Key Exchange)生成,IKE协议通常采用SHA-1和MD5作为消息完整性算法,采用预共享密钥、RSA加密nonce或RSA签名作为对等体的鉴别方法,采用Diffie-Hellman算法作为会话密钥协商算法,采用DES、3DES或AES作为数据加密算法。从数学层面来看,只要掌握了合适的方法,任何密码都可以破译,无非就是所需时间的问题。随着高性能计算技术的发展,尤其是在量子计算环境下,RSA、ECC等非对称加密算法都将可能在短时间内被破译。

发明内容

[0006] 目前通过MPLS技术组建的IP城域网并不具备数据加密机制和用户的认证功能,所以它无法提供数据安全服务,无法满足结构复杂、安全性要求高的企业商用需求。为了解决上述问题,本发明提供一种实现量子安全加密的城域网系统,所述城域网系统包括IP城域网和量子密钥分发城域网,所述IP城域网是通过MPLS技术组建的数据传输网,为企业用户

提供VPN组网;所述量子密钥分发城域网为企业用户的通信提供加密所需的量子密钥。

[0007] 在一种实施方式中,在所述IP城域网中部署具有量子密钥加密功能的用户网络边缘设备,该设备支持扩展使用量子密钥,采用IPsec的加密通信机制,实现接入用户的量子安全通信;和,所述用户网络边缘设备通过量子密钥分发系统安全接口接入所述量子密钥分发城域网,获取对称量子密钥对,用于IPsec VPN的协商及会话加密过程。

[0008] 在一种实施方式中,所述IP城域网包括核心层、汇接层和接入层,所述核心层包括运营商核心路由器,用于核心网络路由及数据的转发;所述汇接层包括运营商边界路由器,用于提供用户边缘设备的接入,为VPN用户建立虚拟路由转发;所述接入层包括所述用户网络边缘设备,该设备支持IPsec扩展使用量子密钥,在该设备上实现量子加密功能。

[0009] 在一种实施方式中,所述核心层包括多台核心路由器,核心路由器支持MPLS、OSPF和/或BGP协议。

[0010] 在一种实施方式中,多台核心路由器进行环形组网。

[0011] 在一种实施方式中,所述核心路由器可与骨干网连接。

[0012] 在一种实施方式中,所述量子密钥分发城域网包括核心控制层、汇接层和所述接入层;所述核心控制层包括量子密钥管理系统,用于城域网内的量子密钥分发系统的路由调度、密钥生成控制和密钥管理;所述汇接层包括量子密钥分发系统的接收端,用于对接所述接入层的量子密钥分发系统的发送端,实现点到点的量子密钥生成;所述接入层包括量子密钥分发系统的发送端,用于接收用户边缘设备的量子密钥请求,并经过量子密钥协商与生成后响应密钥请求,为用户边缘设备建立IPsec VPN提供量子密钥。

[0013] 在一种实施方式中,在VPN用户节点,部署支持IPSec扩展使用量子密钥的用户边缘设备和量子密钥分发系统的发送端。

[0014] 在一种实施方式中,所述VPN用户节点的量子密钥分发系统的发送端接入所述量子密钥分发城域网中的量子密钥分发系统的接收端,全网量子密钥分发系统接入所述量子密钥管理系统。

[0015] 在一种实施方式中,在所述用户边缘设备中配置需要加密的访问控制策略,加密感兴趣流被触发后,用户边缘设备向与其相连的量子密钥分发系统发送端请求量子密钥,响应的量子密钥可用于IPSec VPN的会话密钥。本发明利用用户边缘设备可实现IPSec扩展使用量子密钥的特性,不同用户的边缘设备之间通过IP城域网互通,在隧道模式下实现不同用户通信数据的高安全保密传输。

[0016] 在本发明中,缩略语、英文和关键术语定义如下:

[0017] MPLS(Multi-Protocol Label Switching):多协议标签交换;

[0018] VPN(Virtual Private Network):虚拟专用网络;

[0019] IPSec(Internet Protocol Security):互联网安全协议

[0020] IKE(Internet Key Exchange):互联网密钥交换;

[0021] P(Provider Core Router):运营商核心路由器;

[0022] PE(Provider Edge Router):运营商边缘路由器;

[0023] CE(Customer Edge):用户边缘设备;

[0024] QKD(Quantum Key Distribution):量子密钥分发;

[0025] QKDS(Quantum Key Distribution System):量子密钥分发系统;

[0026] VRF(Virtual Routing and Forwarding):虚拟路由转发;

[0027] BGP(Border Gateway Protocol):边界网关协议;

[0028] MBGP(Multiprotocol BGP):多协议边界网关协议;

[0029] VPN设备:利用VPN技术实现网络中安全通信服务的设备。

[0030] IPsec VPN:指采用IPSec协议来实现远程接入的一种VPN技术,在公网上为两个私有网络提供安全通信通道,通过加密通道保证连接的安全。

[0031] 密钥:控制密码算法运算的关键信息或参数。

[0032] 对称加密:采用单钥密码系统的加密方法,同一个密钥可以同时用作信息的加密和解密。

[0033] 非对称密码体制:非对称密码体制又称为双密钥密码体制或公开密钥密码体制,是指加密和解密操作分别使用两个不同的密钥,并且不可能由加密密钥推导出解密密钥。

[0034] 本发明提供实现量子安全加密的城域网系统,该系统在MPLS VPN城域网中叠加量子密钥分发城域网,使用量子密钥为城域网中用户间的通信提供量子安全加密。

[0035] 本发明将量子加密技术应用于MPLS VPN组网中,可使网络的安全得到质的提高。确保了企业分支间互联通信数据的私有性、完整性及真实性。在城域网中传输数据得到保护,防止对网络资源的非法访问,对网络传输的窃听和破坏,保护网络使用者的合法利益。

附图说明

[0036] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请中记载的一些实施例,对于本领域普通技术人员来说,在不付出创造性劳动的前提下,还可以根据这些附图获得其它的附图。

[0037] 图1是本发明实现量子安全加密的城域网系统的总体架构图;

[0038] 图2是本发明IP城域网的组网架构图;

[0039] 图3是本发明量子密钥分发城域网的组网架构图;

[0040] 图4是本发明的量子密钥加密通道建立流程图;和

[0041] 图5是本发明的MPLS VPN的组网架构图。

具体实施方式

[0042] 为了使本领域技术领域人员更好地理解本申请中的技术方案,下面将结合实施例对本发明作进一步说明,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都应当属于本申请保护的范围。下面结合附图及实施例对本发明作进一步描述。

[0043] 如图1所示,本发明的一种实现量子安全加密的城域网系统,该系统包括IP城域网和量子密钥分发城域网。

[0044] 如图2所示,IP城域网的架构示意图,IP城域网分为三层:核心层、汇接层和接入层。核心层主要由运营商核心路由器(P)组成,负责核心网络路由及数据的转发,以及MPLS包的转发,设置多台P设备以保证核心网络的高可用和可靠性;汇接层主要由运营商边界路

由器(PE)组成,提供用户边缘设备(CE)的接入,为VPN用户建立虚拟路由转发(VRF),并通过MBGP路由协议分发VPN用户的路由表,分配MPLS标签并负责MPLS包的封装、解封装及转发。接入层主要由用户边缘路由器(CE)组成,该设备需支持IPsec扩展使用量子密钥,本发明中的量子加密功能在该设备上实现。

[0045] 如图3所示,量子密钥分发城域网的架构示意图,该组网架构分为三层:核心控制层、汇接层及接入层。核心控制层包括量子密钥管理系统,用于城域网内的量子密钥分发系统的路由调度、密钥生成控制和密钥管理;汇接层包括量子密钥分发系统接收端,用于对接接入层的量子密钥分发系统发送端,实现点到点的量子密钥生成;接入层包括量子密钥分发系统发送端,用于接收用户边缘设备的量子密钥请求,并经过量子密钥协商与生成后响应密钥请求,为用户边缘设备建立IPsec VPN提供量子密钥。本发明实施步骤如下:

[0046] 1.根据业务量需要,选择一到多台P路由器构建核心层,P路由器支持MPLS、OSPF、BGP等协议,多台P路由器组网的情形下,P路由器环形组网,如有业务需要,P路由器可与骨干网对接;

[0047] 2.根据城域网地域特性和具体地理分布的情况,在各城区或业务聚集点设置多个汇聚节点PE路由器,负责汇聚本地流量或者下级的汇聚节点流量;

[0048] 3.在MPLS VPN用户节点,部署支持IPSec扩展使用量子密钥的用户边缘设备(CE)和量子密钥分发系统发送端;

[0049] 4.各用户节点的量子密钥分发系统接入量子密钥分发城域网,全网量子密钥分发系统接入量子密钥管理系统;

[0050] 5.用户边缘设备(CE)接入本地量子密钥分发系统发送端,获取量子密钥;

[0051] 6.根据用户业务加密需要,在用户边缘设备(CE)中配置需要加密的访问控制策略(感兴趣流),IPSec VPN设置为从量子密钥分发系统中获取加密所需的对称密钥。

[0052] 在本发明中,量子密钥分发城域网采用量子密钥分发技术制备量子密钥,发起端用户边缘设备(CE)使用量子密钥对通信数据进行加密,加密数据到达对端CE后,响应端用户边缘设备使用相同的量子密钥对数据进行解密,从而实现两端通信数据受量子安全加密保护。如图4所示,其加密建立过程如下:

[0053] (1)站点A向站点B发送通信请求,首先将数据包发送至同一局域网内的用户网络边缘设备(CE),触发站点A侧CE和站点B侧CE建立IPsec;

[0054] (2)站点A侧CE和站点B侧CE分别向各自侧量子密钥分发系统发送量子密钥分发请求;

[0055] (3)量子密钥分发系统进行量子密钥协商,并将协商到的量子密钥分发给站点A侧CE和站点B侧CE;

[0056] (4)站点A侧CE和站点B侧CE使用获取的量子密钥进行IKE SA协商和IPsec SA协商,量子密钥作为协商过程中的预共享密钥和会话密钥;

[0057] (5)至此,站点A侧CE和站点B侧CE完成了基于量子加密的IPsec隧道,站点A和站点B实现通过基于量子加密的MPLS VPN互联。

[0058] 如图5所示,本发明提供的城域网组网方案主要为企业多分支互联提供量子保密通信服务,企业的多个分支站点接入网MPLS VPN,实现多个站点的网状组网。各站点之间的通信连接在CE设备上配置为IPsec感兴趣流,每当有跨站点通信数据触发时,双方建立基于

量子安全加密的IPsec隧道，确保数据经过量子安全加密传输。以企业三个分支机构通过MPLS VPN互连组网举例：

[0059] 1.企业三个分支机构分别为站点1、站点2和站点3；

[0060] 2.三个站点各配置一台支持扩展使用量子密钥的用户边缘设备(CE)；

[0061] 3.用户站点CE设备接入IP城域网，并通过配置MPLS VPN的方式实现三各站点间的网络互通；

[0062] 4.用户站点CE设备同时接入量子密钥分发城域网，可实时获取量子密钥；

[0063] 5.两两站点间需要加密通信的数据流，在各自站点CE设备上配置相应的访问控制列表；

[0064] 6.两两站点间配置IPSec VPN，并把需要加密通信的数据流对应的访问控制列表引入IPSec VPN，同时，配置IPSec VPN使用量子密钥进行IKE SA协商和IPsec SA协商，量子密钥作为协商过程中的预共享密钥和会话密钥；

[0065] 7.每两个站点间需要量子加密通信时，通信请求匹配访问控制列表，感兴趣流触发IPSec VPN建立，两站点CE使用量子密钥进行IKE SA和IPSec SA协商，协商完成后建立基于量子加密的安全通道，从而保证两站点间的通信具备量子安全加密保护。

[0066] 本领域的技术人员容易理解的是，在不冲突的前提下，上述各有利方式可以自由地组合、叠加。

[0067] 以上仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。以上仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明技术原理的前提下，还可以做出若干改进和变型，这些改进和变型也应视为本发明的保护范围。

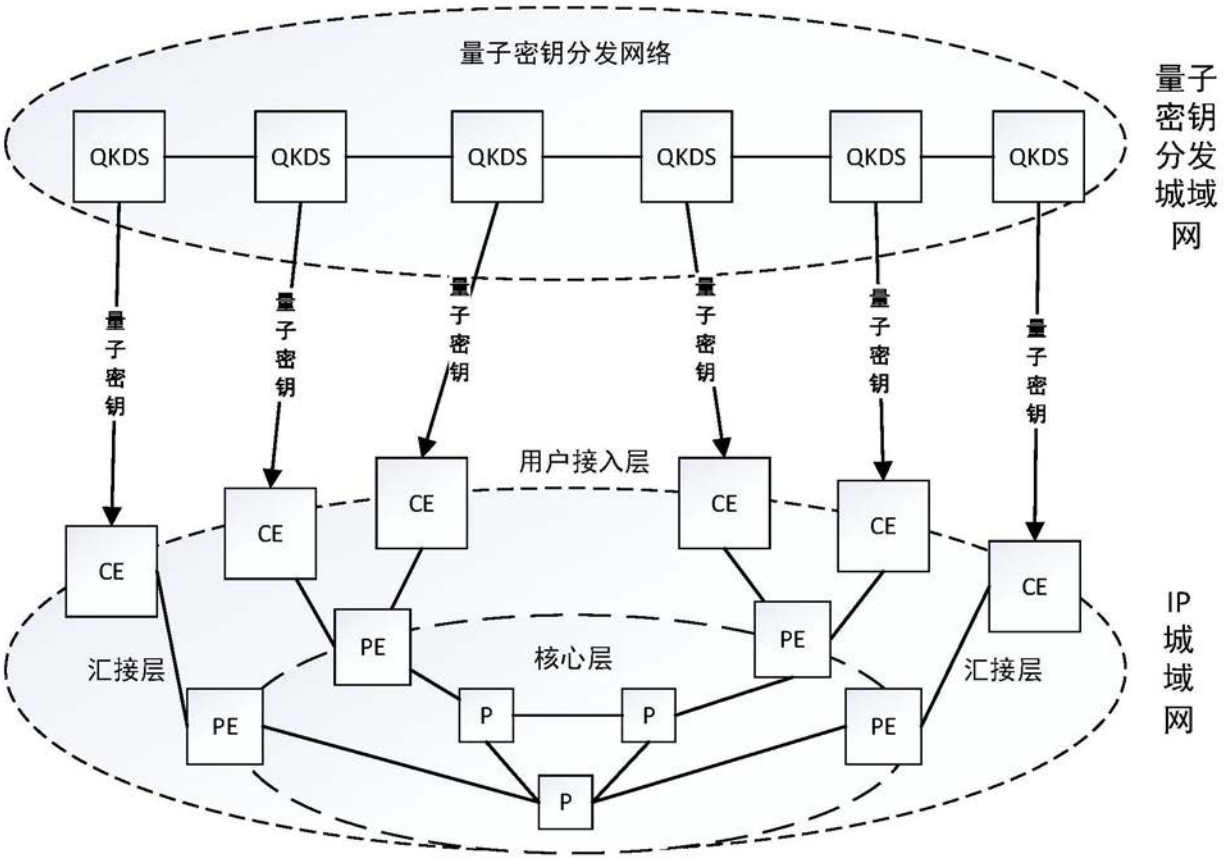

量子密钥分发网络
QKDS
QKDS
QKDS
QKDS
QKDS
QKDS
量子密钥分发域网
量子密钥
量子密钥
量子密钥
量子密钥
量子密钥
量子密钥
用户接入层
CE
CE
CE
CE
CE
CE
PE
PE
汇接层
核心层
汇接层
PE
PE
P
P
P
IP城域网

图1

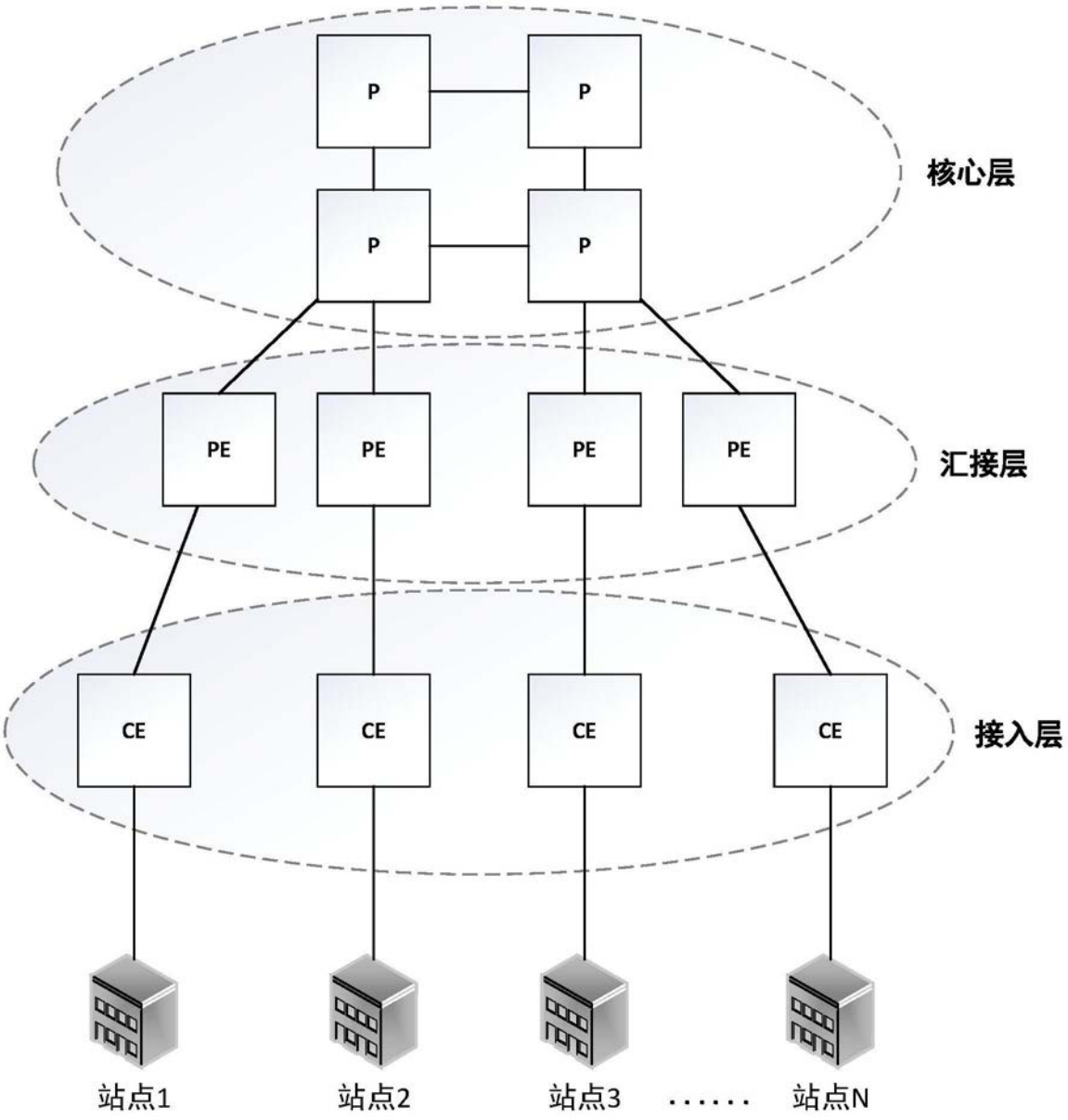


图2

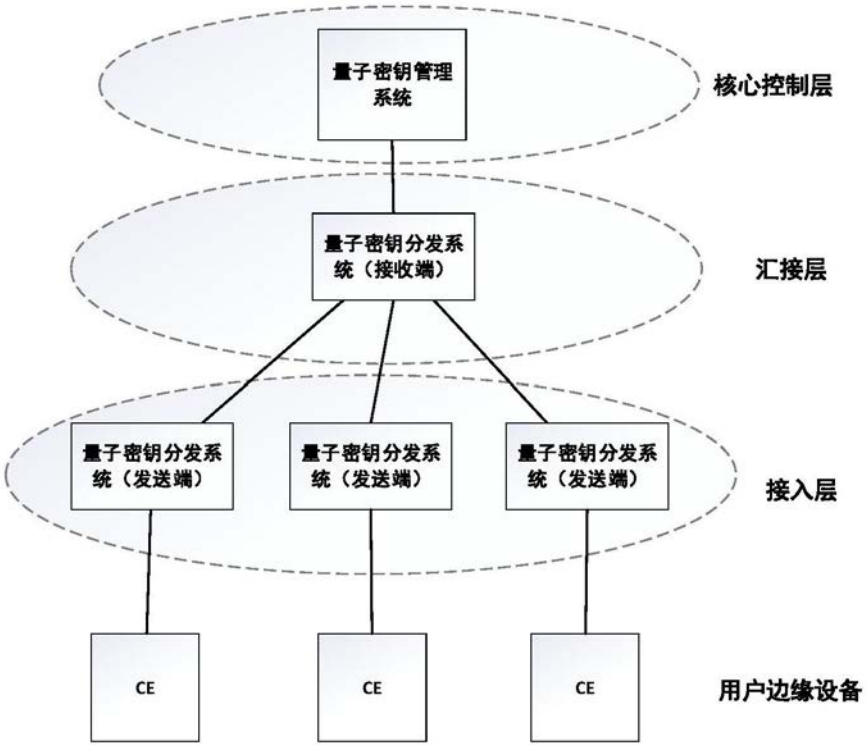

量子密钥管理系统
核心控制层
量子密钥分发系统（接收端）
汇接层
量子密钥分发系统（发送端）
量子密钥分发系统（发送端）
量子密钥分发系统（发送端）
接入层
CE
CE
CE
用户边缘设备

图3

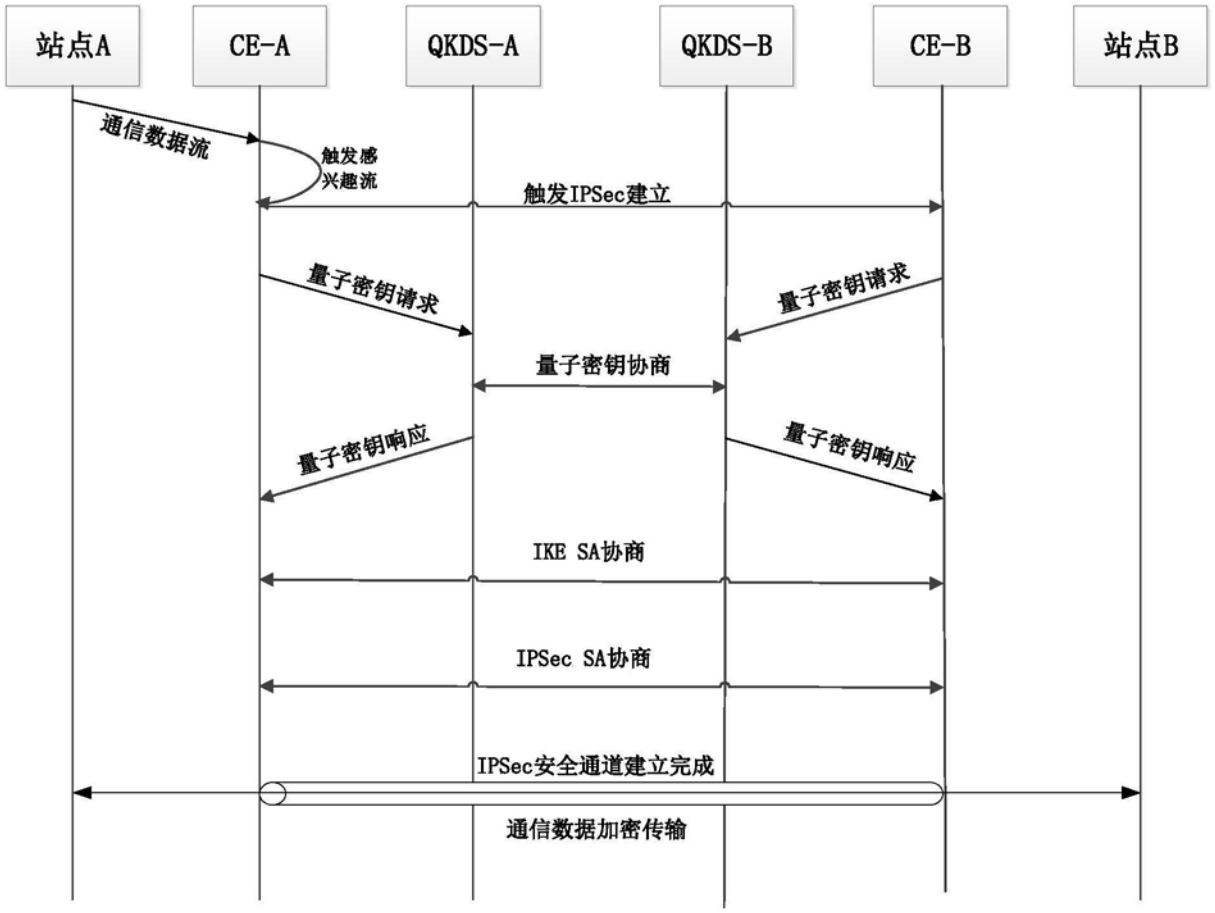

站点A
CE-A
QKDS-A
QKDS-B
CE-B
站点B
通信数据流
触发感兴趣流
触发IPSec建立
量子密钥请求
量子密钥请求
量子密钥协商
量子密钥响应
量子密钥响应
IKE SA协商
IPSec SA协商
IPSec安全通道建立完成
通信数据加密传输

图4

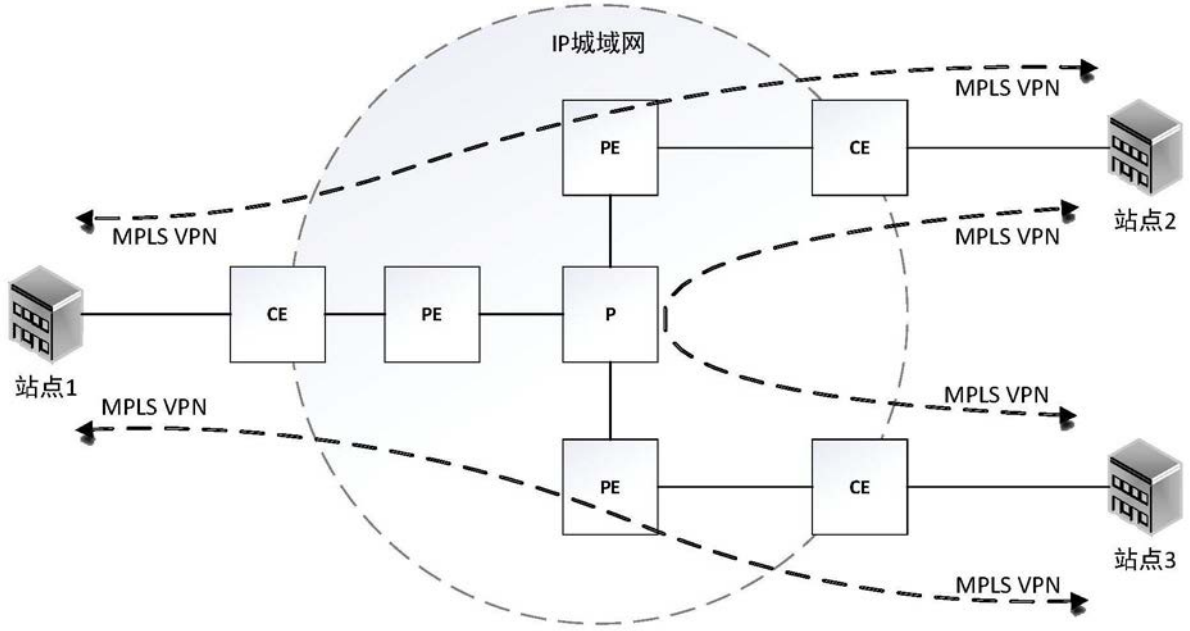

IP城域网
MPLS VPN
PE
CE
站点2
MPLS VPN
MPLS VPN
CE
PE
P
站点1
MPLS VPN
MPLS VPN
PE
CE
站点3
MPLS VPN

图5