(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110505606 B
(45)授权公告日 2022.12.02

(21)申请号 201810480458.X
(22)申请日 2018.05.18
(65)同一申请的已公布的文献号
申请公布号 CN 110505606 A
(43)申请公布日 2019.11.26
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱
(72)发明人 胡俊锋
(74)专利代理机构 北京太合九思知识产权代理有限公司 11610
专利代理师 刘戈
(51)Int.Cl.
H04W 4/80(2018.01)
H04W 12/06(2021.01)
H04W 84/18(2009.01)

(56)对比文件
CN 101068196 A,2007.11.07
US 2015245204 A1,2015.08.27
WO 2017087903 A1,2017.05.26
CN 101112039 A,2008.01.23
US 2018132102 A1,2018.05.10

审查员 段巍

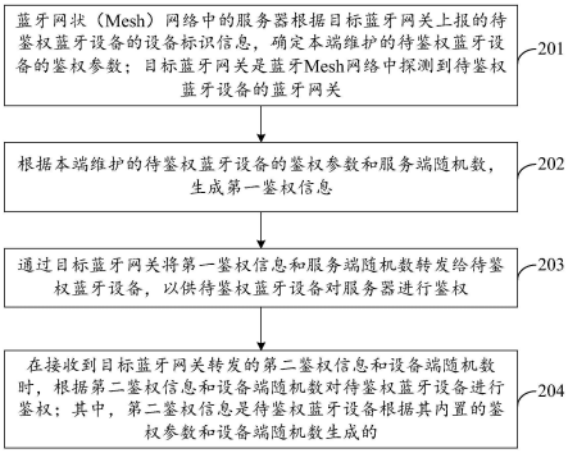
权利要求书3页 说明书19页 附图7页

(54)发明名称

蓝牙Mesh网络及其配网鉴权方法、设备和存储介质

(57)摘要

本申请实施例提供一种蓝牙Mesh网络及其配网鉴权方法、设备和存储介质。在本申请实施例中，提供一种包括蓝牙网关和服务器的蓝牙Mesh网络，该网络中的蓝牙网关负责探测请求接入蓝牙Mesh网络的蓝牙设备，并在服务器与该蓝牙设备之间进行信息传递，使得服务器可通过探测到蓝牙设备的蓝牙网关与蓝牙设备进行鉴权，为蓝牙设备安全接入蓝牙Mesh网络提供基础。其中，由服务器统一与各请求接入蓝牙Mesh网络的蓝牙设备进行鉴权，实现配网鉴权的全局化，将网关设备从配网鉴权过程中解放出来，降低了对蓝牙网关的要求，简化了蓝牙Mesh网络的部署实施，有利于促进蓝牙Mesh技术的发展。



CN 110505606 B

1.一种蓝牙网状网络,其特征在于,包括:至少一个蓝牙网关和与所述至少一个蓝牙网关通信连接的服务器;

所述至少一个蓝牙网关,用于探测请求接入所述蓝牙网状网络的待鉴权蓝牙设备,并在所述待鉴权蓝牙设备与所述服务器之间进行信息传递;

所述服务器,用于根据目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息,确定所述服务器维护的所述待鉴权蓝牙设备的鉴权参数,所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关;根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数,生成第一鉴权信息;通过所述目标蓝牙网关将所述第一鉴权信息和所述服务端随机数转发给所述待鉴权蓝牙设备;在接收到所述目标蓝牙网关转发的第二鉴权信息和设备端随机数时,根据所述第二鉴权信息和所述设备端随机数对所述待鉴权蓝牙设备进行鉴权;

所述待鉴权蓝牙设备,用于接收所述目标蓝牙网关转发的第一鉴权信息和服务端随机数,并根据所述第一鉴权信息和所述服务端随机数对所述服务器进行鉴权;以及根据所述待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息,并通过所述目标蓝牙网关将所述第二鉴权信息和所述设备端随机数转发给所述服务器。

2.根据权利要求1所述的蓝牙网状网络,其特征在于,所述鉴权参数包括设备标识信息和鉴权密钥,所述鉴权密钥与所述设备标识信息具有一一对应关系。

3.根据权利要求2所述的蓝牙网状网络,其特征在于,所述设备标识信息包括产品标识和MAC地址,所述产品标识代表设备能力。

4.根据权利要求1所述的蓝牙网状网络,其特征在于,所述服务器在生成所述第一鉴权信息时,具体用于:

根据约定的加密算法对所述服务器维护的所述待鉴权蓝牙设备的鉴权参数进行加密处理,以生成第一认证值;

根据所述第一认证值和所述服务端随机数,生成所述第一鉴权信息。

5.根据权利要求1所述的蓝牙网状网络,其特征在于,所述服务器还用于:

预先为所述待鉴权蓝牙设备分配鉴权参数,并在所述服务器端维护所述待鉴权蓝牙设备的鉴权参数;以及

将为所述待鉴权蓝牙设备分配的鉴权参数提供给所述待鉴权蓝牙设备的制造商,以供所述制造商将所述鉴权参数内置于所述待鉴权蓝牙设备中。

6.根据权利要求1-5任一项所述的蓝牙网状网络,其特征在于,所述服务器还用于:

在双向鉴权成功通过后,为所述待鉴权蓝牙设备分配配网数据,并将所述配网数据下发给所述目标蓝牙网关,以供所述目标蓝牙网关对所述待鉴权蓝牙设备进行配网操作。

7.一种蓝牙网状网络的配网鉴权方法,适用于蓝牙网状网络中的服务器,其特征在于,所述方法包括:

根据目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息,确定所述服务器维护的所述待鉴权蓝牙设备的鉴权参数;所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关;

根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数,生成第一鉴权信息;

通过所述目标蓝牙网关将所述第一鉴权信息和所述服务端随机数转发给所述待鉴权蓝牙设备，以供所述待鉴权蓝牙设备对所述服务器进行鉴权；以及

在接收到所述目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据所述第二鉴权信息和所述设备端随机数对所述待鉴权蓝牙设备进行鉴权；其中，所述第二鉴权信息是所述待鉴权蓝牙设备根据其内置的鉴权参数和所述设备端随机数生成的。

8.根据权利要求7所述的方法，其特征在于，所述根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息，包括：

根据约定的加密算法对所述服务器维护的所述待鉴权蓝牙设备的鉴权参数进行加密处理，以生成第一认证值；

根据所述第一认证值和所述服务端随机数，生成所述第一鉴权信息。

9.根据权利要求7或8所述的方法，其特征在于，在接收目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息之前，所述方法还包括：

预先为所述待鉴权蓝牙设备分配鉴权参数，并在所述服务器端维护所述待鉴权蓝牙设备的鉴权参数；以及

将为所述待鉴权蓝牙设备分配的鉴权参数提供给所述待鉴权蓝牙设备的制造商，以供所述制造商将所述鉴权参数内置于所述待鉴权蓝牙设备中。

10.一种蓝牙网状网络的配网鉴权方法，适用于请求接入蓝牙网状网络的待鉴权蓝牙设备，其特征在于，所述方法包括：

广播所述待鉴权蓝牙设备的设备标识信息，以供目标蓝牙网关将所述设备标识信息转发给所述蓝牙网状网络中的服务器，所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

接收所述目标蓝牙网关转发的第一鉴权信息和服务端随机数，并根据所述第一鉴权信息和所述服务端随机数对所述服务器进行鉴权；所述第一鉴权信息是所述服务器根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和所述服务端随机数生成的；以及

根据所述待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息，并通过所述目标蓝牙网关将所述第二鉴权信息和所述设备端随机数转发给所述服务器，以供所述服务器对所述待鉴权蓝牙设备进行鉴权。

11.根据权利要求10所述的方法，其特征在于，所述根据所述待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息，包括：

根据约定的加密算法对所述待鉴权蓝牙设备内置的鉴权参数进行加密处理，以生成第二认证值；

根据所述第二认证值和所述设备端随机数，生成所述第二鉴权信息。

12.一种服务器，适用于蓝牙网状网络，其特征在于，所述服务器包括：存储器、处理器和通信组件；

所述通信组件，用于接收目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息；其中所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

所述存储器，用于存储计算机程序以及包括所述待鉴权蓝牙设备在内的已注册蓝牙设备的鉴权参数；

所述处理器，用于执行所述计算机程序，以用于：

根据所述待鉴权蓝牙设备的设备标识信息，确定所述服务器维护的所述待鉴权蓝牙设备的鉴权参数；

根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息；

通过所述目标蓝牙网关将所述第一鉴权信息和所述服务端随机数转发给所述待鉴权蓝牙设备，以供所述待鉴权蓝牙设备对所述服务器进行鉴权；以及

在所述通信组件接收到所述目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据所述第二鉴权信息和所述设备端随机数对对所述待鉴权蓝牙设备进行鉴权；其中，所述第二鉴权信息是所述待鉴权蓝牙设备根据其内置的鉴权参数和所述设备端随机数生成的。

13.一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被执行时能够实现权利要求7-9任一项所述方法中的步骤。

14.一种蓝牙设备，适用于蓝牙网状网络，其特征在于，蓝牙设备包括：存储器、处理器和通信组件；

所述通信组件，用于广播所述蓝牙设备的设备标识信息，以供目标蓝牙网关将所述设备标识信息转发给所述蓝牙网状网络中的服务器，以及接收所述目标蓝牙网关转发的第一鉴权信息和服务端随机数；所述第一鉴权信息是所述服务器根据所述服务器维护的待鉴权蓝牙设备的鉴权参数和所述服务端随机数生成的，所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

所述存储器，用于存储计算机程序以及所述蓝牙设备的鉴权参数；

所述处理器，用于执行所述计算机程序，以用于：

根据所述第一鉴权信息和所述服务端随机数对所述服务器进行鉴权；以及

根据所述存储器中的鉴权参数和设备端随机数生成第二鉴权信息，并通过所述目标蓝牙网关将所述第二鉴权信息和所述设备端随机数转发给所述服务器，以供所述服务器对所述待鉴权蓝牙设备进行鉴权。

15.一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被执行时能够实现权利要求10或11所述方法中的步骤。

蓝牙Mesh网络及其配网鉴权方法、设备和存储介质

技术领域

[0001] 本申请涉及无线通信技术领域，尤其涉及一种蓝牙Mesh网络及其配网鉴权方法、设备和存储介质。

背景技术

[0002] 网状(Mesh)网络是一种与传统无线网络完全不同的新型无线网络，在Mesh网络中，每个节点都可以发送和接收信号，每个节点都可以与一个或者多个对等节点进行直接通信。为了突破蓝牙设备在通信范围上的限制，蓝牙技术联盟发布了蓝牙Mesh协议，它是建立在蓝牙低功耗(Bluetooth Low Energy，BLE)标准上的蓝牙协议(Profile)。

[0003] 在现有蓝牙Mesh网络中，主要包含两种角色：启动配置设备(Provisioner)和蓝牙设备(Device)。为了保证蓝牙Mesh网络的安全性，蓝牙设备需要由启动配置设备通过启动配置流程(Provisioning)将其加入蓝牙Mesh网络。在启动配置过程中，启动配置设备需要使用所选的带外信息(Out-Of-Band，OOB)对蓝牙设备进行鉴权，以保证入网安全。但是，现有鉴权方法对启动配置设备的处理能力要求较高，可能限制蓝牙Mesh网络的部署实施。

发明内容

[0004] 本申请的多个方面提供一种蓝牙Mesh网络及其配网鉴权方法、设备和存储介质，用以提供一种新的蓝牙Mesh网络及其配网鉴权方法，简化蓝牙Mesh网络的部署实施。

[0005] 本申请实施例提供一种蓝牙Mesh网络，包括：

[0006] 至少一个蓝牙网关和与所述至少一个蓝牙网关通信连接的服务器；

[0007] 所述至少一个蓝牙网关，用于探测请求接入所述蓝牙网状网络的待鉴权蓝牙设备，并在所述待鉴权蓝牙设备与所述服务器之间进行信息传递；

[0008] 所述服务器，用于通过探测到所述待鉴权蓝牙设备的目标蓝牙网关与所述待鉴权蓝牙设备进行鉴权，以供所述待鉴权蓝牙设备安全接入所述蓝牙网状网络。

[0009] 本申请实施例还提供一种蓝牙Mesh网络的配网鉴权方法，适用于蓝牙网状网络中的服务器，所述方法包括：

[0010] 根据目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息，确定所述服务器维护的所述待鉴权蓝牙设备的鉴权参数；所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

[0011] 根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息；

[0012] 通过所述目标蓝牙网关将所述第一鉴权信息和所述服务端随机数转发给所述待鉴权蓝牙设备，以供所述待鉴权蓝牙设备对所述服务器进行鉴权；以及

[0013] 在接收到所述目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据所述第二鉴权信息和所述设备端随机数对所述待鉴权蓝牙设备进行鉴权；其中，所述第二鉴权信息是所述待鉴权蓝牙设备根据其内置的鉴权参数和所述设备端随机数生成的。

[0014] 本申请实施例还提供另一种蓝牙Mesh网络的配网鉴权方法，适用于请求接入蓝牙网状网络的待鉴权蓝牙设备，所述方法包括：

[0015] 广播所述待鉴权蓝牙设备的设备标识信息，以供目标蓝牙网关将所述设备标识信息转发给所述蓝牙网状网络中的服务器，所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

[0016] 接收所述目标蓝牙网关转发的第一鉴权信息和服务端随机数，并根据所述第一鉴权信息和所述服务端随机数对所述服务器进行鉴权；所述第一鉴权信息是所述服务器根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和所述服务端随机数生成的；以及

[0017] 根据所述待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息，并通过所述目标蓝牙网关将所述第二鉴权信息和所述设备端随机数转发给所述服务器，以供所述服务器对所述待鉴权蓝牙设备进行鉴权。

[0018] 本申请实施例还提供一种服务器，适用于蓝牙Mesh网络，该服务器包括：

[0019] 存储器、处理器和通信组件；

[0020] 所述通信组件，用于接收目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息；其中所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

[0021] 所述存储器，用于存储计算机程序以及包括所述待鉴权蓝牙设备在内的已注册蓝牙设备的鉴权参数；

[0022] 所述处理器，用于执行所述计算机程序，以用于：

[0023] 根据所述待鉴权蓝牙设备的设备标识信息，确定所述服务器维护的所述待鉴权蓝牙设备的鉴权参数；

[0024] 根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息；

[0025] 通过所述目标蓝牙网关将所述第一鉴权信息和所述服务端随机数转发给所述待鉴权蓝牙设备，以供所述待鉴权蓝牙设备对所述服务器进行鉴权；以及

[0026] 在所述通信组件接收到所述目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据所述第二鉴权信息和所述设备端随机数对对所述待鉴权蓝牙设备进行鉴权；其中，所述第二鉴权信息是所述待鉴权蓝牙设备根据其内置的鉴权参数和所述设备端随机数生成的。

[0027] 本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被执行时能够实现由服务器所执行的方法实施例中的步骤。

[0028] 本申请实施例还提供一种蓝牙设备，适用于蓝牙Mesh网络，该蓝牙设备包括：

[0029] 存储器、处理器和通信组件；

[0030] 所述通信组件，用于广播所述蓝牙设备的设备标识信息，以供目标蓝牙网关将所述设备标识信息转发给所述蓝牙网状网络中的服务器，以及接收所述目标蓝牙网关转发的第一鉴权信息和服务端随机数；所述第一鉴权信息是所述服务器根据所述服务器维护的所述待鉴权蓝牙设备的鉴权参数和所述服务端随机数生成的，所述目标蓝牙网关是所述蓝牙网状网络中探测到所述待鉴权蓝牙设备的蓝牙网关；

[0031] 所述存储器，用于存储计算机程序以及所述蓝牙设备的鉴权参数；

[0032] 所述处理器，用于执行所述计算机程序，以用于：

[0033] 根据所述第一鉴权信息和所述服务端随机数对所述服务器进行鉴权;以及

[0034] 根据所述存储器中的鉴权参数和设备端随机数生成第二鉴权信息,并通过所述目标蓝牙网关将所述第二鉴权信息和所述设备端随机数转发给所述服务器,以供所述服务器对所述待鉴权蓝牙设备进行鉴权。

[0035] 本申请实施例还提供一种存储有计算机程序的计算机可读存储介质,其特征在于,所述计算机程序被执行时能够实现由蓝牙设备所执行的方法实施例中的步骤。

[0036] 在本申请实施例中,提供一种包括蓝牙网关和服务器的蓝牙Mesh网络,该网络中的蓝牙网关负责探测请求接入蓝牙Mesh网络的蓝牙设备,并在服务器与该蓝牙设备之间进行信息传递,使得服务器可通过探测到蓝牙设备的蓝牙网关与蓝牙设备进行鉴权,为蓝牙设备安全接入蓝牙Mesh网络提供基础。在本申请实施例中,增设服务器,并由服务器统一与各请求接入蓝牙Mesh网络的蓝牙设备进行鉴权,实现配网鉴权的全局化,将网关设备从配网鉴权过程中解放出来,降低了对蓝牙网关的要求,简化了蓝牙Mesh网络的部署实施,有利于促进蓝牙Mesh技术的发展。

[0037] 进一步,在本申请各实施例中,服务器可以结合本端维护的蓝牙设备的鉴权参数和蓝牙设备内置的鉴权参数,采用静态OOB鉴权方式与蓝牙设备进行双向鉴权。在整个静态OOB鉴权过程中,无需用户介入,实现了配网鉴权的自动化,有利于改善用户体验,提高了配网鉴权的效率;另外,不同蓝牙设备对应不同静态OOB信息,这有利于保证配网鉴权过程的安全性。

附图说明

[0038] 此处所说明的附图用来提供对本申请的进一步理解,构成本申请的一部分,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0039] 图1为本申请一示例性实施例提供的一种蓝牙Mesh网络的结构示意图;

[0040] 图2为本申请另一示例性实施例提供的从服务器角度描述的蓝牙Mesh网络的配网鉴权方法的流程示意图;

[0041] 图3为本申请另一示例性实施例提供的从目标蓝牙网关角度描述的蓝牙Mesh网络的配网鉴权方法的流程示意图;

[0042] 图4为本申请另一示例性实施例提供的从待鉴权蓝牙设备角度描述的蓝牙Mesh网络的配网鉴权方法的流程示意图;

[0043] 图5为本申请又一示例性实施例提供的蓝牙Mesh网络基于三元组的配网鉴权方法的流程示意图;

[0044] 图6a为本申请又一示例性实施例提供的一种配网鉴权装置的结构示意图;

[0045] 图6b为本申请又一示例性实施例提供的一种服务器的结构示意图;

[0046] 图7a为本申请又一示例性实施例提供的另一种配网鉴权装置的结构示意图;

[0047] 图7b为本申请又一示例性实施例提供的一种蓝牙设备的结构示意图。

具体实施方式

[0048] 为使本申请的目的、技术方案和优点更加清楚,下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然,所描述的实施例仅是本申请一

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他实施例，都属于本申请保护的范围。

[0049] 针对现有OOB鉴权方法对启动配置设备的处理能力要求较高，可能限制蓝牙Mesh网络的部署实施的技术问题，在本申请一些实施例中，提供一种新的包括蓝牙网关和服务器的蓝牙Mesh网络，该网络中的蓝牙网关负责探测请求接入蓝牙Mesh网络的蓝牙设备，并负责在服务器与该蓝牙设备之间进行信息传递，而服务器可通过探测到蓝牙设备的蓝牙网关与蓝牙设备进行鉴权，实现配网鉴权的全局化，将网关设备从配网鉴权过程中解放出来，降低对蓝牙网关的要求，简化了蓝牙Mesh网络的部署实施，有利于促进蓝牙Mesh技术的发展。

[0050] 以下结合附图，详细说明本申请各实施例提供的技术方案。

[0051] 图1为本申请一示例性实施例提供的一种蓝牙Mesh网络的结构示意图。如图1所示，该蓝牙Mesh网络10包括：至少一个蓝牙网关10a和服务器10b。其中，至少一个蓝牙网关10a与服务器10b通信连接，该通信连接可以是有线连接，也可以是无线连接。

[0052] 在一可选实施方式中，服务器10b部署在云端，则蓝牙网关10a可以通过WIFI、以太网、光纤、2/3/4G/5G等移动网络接入互联网(例如广域网或城域网)，通过互联网与服务器10b建立通信连接，实现与服务器10b的双向通信，如图1所示。

[0053] 在本实施例中，至少一个蓝牙网关10a可以是同时支持蓝牙通信技术，具有蓝牙探测功能以及一定通信能力的计算机设备，例如可以是支持蓝牙通信技术的无线路由器，智能手机、平板电脑、个人电脑、蓝牙探针等等。值得说明的是，图1中所呈现的蓝牙网关10a的实现形态只是示例性说明，并不对其实现形态做限定。

[0054] 不论蓝牙网关10a的实现形态如何，蓝牙网关10a一般会包括至少一个处理单元、至少一个存储器以及蓝牙通信模块。处理单元和存储器的数量取决于蓝牙网关10a的配置和类型。存储器可以包括易失性的，例如RAM，也可以包括非易失性的，例如只读存储器(Read-Only Memory，ROM)、闪存等，或者也可以同时包括两种类型的。存储器内通常存储有操作系统(Operating System，OS)、一个或多个应用程序，也可以存储有程序数据等。除了处理单元、存储器和蓝牙通信模块之外，蓝牙网关10a还包括一些基本配置，例如其它类型的网卡芯片、IO总线、音视频组件等。可选地，蓝牙网关10a还可以包括一些外围设备，例如键盘、鼠标、输入笔、打印机、显示器、电子屏幕等。这些外围设备在本领域中是众所周知的，在此不做赘述。

[0055] 在本实施例中，还包括服务器10b。服务器10b可以是常规服务器、云服务器、云主机、虚拟中心等服务器设备。其中，服务器设备的构成主要包括处理器、硬盘、内存、系统总线等，和通用的计算机架构类似。

[0056] 在本实施例中，服务器10b与至少一个蓝牙网关10a相互配合，可实现蓝牙Mesh协议中规定的启动配置流程(Provisioning)，即通过相互配合可授权未配网的蓝牙设备接入蓝牙Mesh网络10中。其中，蓝牙Mesh协议中规定的Provisioning是一种能够使未配网的蓝牙设备成为给定蓝牙Mesh网络中的成员节点的配置流程，主要包括为未配网的蓝牙设备提供成功接入Mesh网络所需的配网数据的过程。除了为未配网的蓝牙设备提供配网数据之外，该Provisioning还包括与未配网的蓝牙设备进行鉴权的过程。其中，在鉴权成功通过的情况下，再为未配网的蓝牙设备分配配网数据，可保证蓝牙Mesh网络的安全性，提高整个入

网过程的安全性。在本实施例中，重点关注与未配网的蓝牙设备进行双向鉴权的过程。

[0057] 在本实施例中，蓝牙Mesh网络10中的蓝牙网关10a一方面用于探测请求接入蓝牙Mesh网络10的未配网的蓝牙设备。由于本实施例主要关注与探测到的未配网的蓝牙设备进行鉴权的过程，故为便于描述，将蓝牙网关10a探测到的请求接入蓝牙Mesh网络10的未配网的蓝牙设备称为待鉴权蓝牙设备。除了探测待鉴权蓝牙设备之外，蓝牙网关10a还负责在待鉴权蓝牙设备与服务器10b之间进行信息传递，为服务器10b与待鉴权蓝牙设备进行鉴权提供通信基础。这里的信息传递主要包括在待鉴权蓝牙设备与服务器10b之间转发鉴权所需的各种信息。当然，该信息传递也包括在待鉴权蓝牙设备与服务器10b之间转发启动配网流程中的其它信息。

[0058] 在本实施例中，待鉴权蓝牙设备可以是任何支持蓝牙通信技术，且可以接入蓝牙Mesh网络10中的设备，例如可以是蓝牙灯、蓝牙开关，蓝牙插座、蓝牙电视、蓝牙耳机、蓝牙音响、蓝牙键盘、蓝牙手环、蓝牙报警器、蓝牙跟踪器、蓝牙耳温枪、蓝牙心率计、蓝牙传感器等等。在本实施例中，待鉴权蓝牙设备是指尚未接入蓝牙Mesh网络10且需要与服务器10b进行鉴权的蓝牙设备。

[0059] 在本实施例的蓝牙Mesh网络10中，增设服务器10b，该服务器10b可通过探测到待鉴权蓝牙设备的蓝牙网关与待鉴权蓝牙设备进行鉴权，实现了配网鉴权的全局化。另外，由服务器10b与待鉴权蓝牙设备进行鉴权，将蓝牙网关从配网鉴权中解放了出来，有利于降低对蓝牙网关的要求，有利于降低蓝牙Mesh网络的部署难度，便于促进蓝牙Mesh技术的发展。

[0060] 值得说明的是，本申请实施例提供的蓝牙Mesh网络10，允许用户根据网络覆盖范围的需求灵活布设合理数量的蓝牙网关10a。例如，在一些网络覆盖范围不大的应用场景中，可以布设少量蓝牙网关10a，例如可以布设一个蓝牙网关10a；在一些网络覆盖范围较大的应用场景中，可以布设大量蓝牙网关10a。

[0061] 下面重点描述与蓝牙网关10a探测相关的内容：

[0062] 在本申请实施例提供的蓝牙Mesh网络10中，未配网的蓝牙设备在做好入网准备时，可以以广播的方式通知其附近的蓝牙网关10a。可选地，如果未配网的蓝牙设备支持PB-ADV承载层，则可以对外广播信标(Beacon)信号；如果未配网的蓝牙设备使用的是PB-GATT承载层，则可以发送可连接的广播数据包。蓝牙网关10a接收到信标信号或广播数据包时，可以确定探测到发送该信标信号或广播数据包的蓝牙设备，并可确定该蓝牙设备已经做好准备，于是将其作为待鉴权蓝牙设备。

[0063] 在上述或下述实施例中，用户可以向蓝牙网关10a发出探测指令。对蓝牙网关10a来说，可响应于用户发出的探测指令，探测其信号覆盖范围内请求接入蓝牙Mesh网络的待鉴权蓝牙设备。

[0064] 在一些应用场景中，用户可以向蓝牙Mesh网络10中的所有蓝牙网关10a分别发出探测指令，以控制所有蓝牙网关10a探测其信号覆盖范围内的待鉴权蓝牙设备。例如，在蓝牙Mesh网络10部署完成后刚启动时，可能需要所有蓝牙网关10a分别探测其信号覆盖范围内的待鉴权蓝牙设备，此时用户可以向蓝牙Mesh网络10中的所有蓝牙网关10a分别发出探测指令。

[0065] 在另一些应用场景中，用户也可以向蓝牙Mesh网络10中的部分蓝牙网关10a发出探测指令，以控制这部分蓝牙网关10a探测其信号覆盖范围内的待鉴权蓝牙设备。例如，在

家庭住宅环境中，用户在某个位置增加了新的蓝牙灯，而其它位置的蓝牙设备并未发生变化，在这种情况下，用户可以只向与该新增的蓝牙灯相距最近的一个蓝牙网关10a发出探测指令，触发该蓝牙网关10a对其信号覆盖范围内的待鉴权蓝牙设备即可，可以节约蓝牙网关的资源。

[0066] 在本实施例中，蓝牙网关10a可以具有触控屏幕，则用户可以采用触发方式或手写方式向蓝牙网关10a发出探测指令。或者，蓝牙网关10a支持语音输入，则用户可以采用语音方式向蓝牙网关10a发出探测指令。例如，用户可以说“请开始探测”。

[0067] 除用户触发之外，蓝牙网关10a也可以按照预先配置的探测方案自动探测其信号覆盖范围内的待鉴权蓝牙设备。例如，蓝牙网关10a可以周期性探测其信号覆盖范围内的待鉴权蓝牙设备。或者，蓝牙网关10a可以在设定的探测时间到达时，开始探测其信号覆盖范围内的待鉴权蓝牙设备。或者，蓝牙网关10a也可以在探测到设定的触发事件时，开始探测其信号覆盖范围内的待鉴权蓝牙设备。所述触发事件可以是开机事件，激活事件，或者用户事件等。

[0068] 对每个蓝牙网关10a来说，在其信号覆盖范围内可能探测到一个待鉴权蓝牙设备，也可能探测到多个待鉴权蓝牙设备，也有可能未探测到任何待鉴权蓝牙设备。另外，因为应用场景的不同，在一些蓝牙Mesh网络10中，各蓝牙网关10a的信号覆盖范围不会重叠；而在另一些蓝牙Mesh网络10中，部分蓝牙网关10a的信号覆盖范围可能存在重叠。对于部分蓝牙网关10a的信号覆盖范围存在重叠的情况，处于重叠区域内的待鉴权蓝牙设备可能会被两个甚至更多的蓝牙网关10a探测到，这样同一待鉴权蓝牙设备的设备标识信息会被两个甚至更多的蓝牙网关10a上报给服务器10b。相应地，服务器10b可能会先后接收到两个甚至更多蓝牙网关10a上报的同一待鉴权蓝牙设备的设备标识信息。其中，待鉴权蓝牙设备的设备标识信息主要是一些能够标识待鉴权蓝牙设备的信息，例如通用唯一识别码(Universally Unique Identifier,UUID)，该UUID包括产品标识(Product ID)，MAC地址等。其中，Product ID可代表待鉴权蓝牙设备的能力等信息。

[0069] 由上述分析可知，在一些情况下，探测到待鉴权蓝牙设备的蓝牙网关可能是一个，则服务器10b可以基于该蓝牙网关与待鉴权蓝牙设备进行鉴权。在另一些情况下，探测到待鉴权蓝牙设备的蓝牙网关可能是多个，则服务器10b可以从探测到待鉴权蓝牙设备的多个蓝牙网关中选择其中一个蓝牙网关，并基于所选择的蓝牙网关与待鉴权蓝牙设备进行鉴权。为便于描述，将最终负责在服务器10b与待鉴权蓝牙设备进行鉴权过程中进行信息传递的蓝牙网关称为目标蓝牙网关。该目标蓝牙网关是蓝牙Mesh网络10中探测到待鉴权蓝牙设备的某个蓝牙网关。

[0070] 下面重点描述确定目标蓝牙网关的内容：

[0071] 在探测到待鉴权蓝牙设备的蓝牙网关为多个的情况下，服务器10b可以按照多个蓝牙网关上报待鉴权蓝牙设备的设备标识信息的先后顺序、多个蓝牙网关探测到的待鉴权蓝牙设备的信号强度和/或多个蓝牙网关之间的优先级等信息，从多个蓝牙网关中选择目标蓝牙网关。下面给出几种实施方式进行示例性说明，但不限于此。

[0072] 在一种实施方式中，探测到待鉴权蓝牙设备的多个蓝牙网关除了向服务器10b上报待鉴权蓝牙设备的设备标识信息之外，还可以向服务器10b上报各自探测到的该待鉴权蓝牙设备的接收信号的强度指示(Received Signal Strength Indicator,RSSI)。基于此，

服务器10b可以根据各蓝牙网关探测到的待鉴权蓝牙设备的RSSI，从中选择信号强度符合信号强度要求的蓝牙网关作为目标蓝牙网关。例如，服务器10b可以从中选择RSSI最大的蓝牙网关作为目标蓝牙网关。又例如，服务器10b可以从中选择RSSI位于预设RSSI范围内的蓝牙网关作为目标蓝牙网关。又例如，可以从中选择RSSI大于设定的RSSI阈值的蓝牙网关作为目标蓝牙网关。

[0073] 在另一种实施方式中，可以预先为蓝牙Mesh网络10中各蓝牙网关10a配置优先级，不同蓝牙网关10a具有不同的优先级。例如，可以将蓝牙Mesh网络10中的蓝牙网关10a划分为主网关、一级从网关、二级从网关等。基于此，服务器10b可以根据探测到待鉴权蓝牙设备的多个蓝牙网关之间的优先级，从中选择优先级符合优先级要求的蓝牙网关作为目标蓝牙网关。例如，服务器10b可以选择优先级最高的蓝牙网关作为目标蓝牙网关。

[0074] 在又一种实施方式中，考虑到各蓝牙网关10a与待鉴权蓝牙设备之间的距离可能不同，故在多个蓝牙网关探测到待鉴权蓝牙设备的情况下，各蓝牙网关探测到待鉴权蓝牙设备的时间会有所不同，相应地，各蓝牙网关向服务器10b上报待鉴权蓝牙设备的设备标识信息的先后顺序会不同。基于此，服务器10b可以根据多个蓝牙网关上报待鉴权蓝牙设备的设备标识信息的先后顺序，从中选择目标蓝牙网关。例如，服务器10b可以选择最先上报待鉴权蓝牙设备的设备标识信息的蓝牙网关作为目标蓝牙网关。又例如，服务器10b可以选择最后上报待鉴权蓝牙设备的设备标识信息的蓝牙网关作为目标蓝牙网关。

[0075] 进一步，在服务器10b与待鉴权蓝牙设备之间的双向鉴权成功通过后，服务器10b还可以为待鉴权蓝牙设备分配配网数据，并将待鉴权蓝牙设备的配网数据下发给目标蓝牙网关，以供目标蓝牙网关对待鉴权蓝牙设备进行配网操作。

[0076] 其中，配网数据是指待鉴权蓝牙设备成功接入蓝牙Mesh网络10所需的数据，例如包括网络密钥(Netkey)、应用密钥(AppKey)、单播地址(UnicastAddress)等。Netkey确保网络层(network layer)通信的安全，并在网络中所有成员节点(node)之间共享。是否拥有给定的Netkey定义了给定蓝牙Mesh网络10的成员资格，为蓝牙设备赋予网络的Netkey是配网操作的主要结果之一。其中，成员节点是指成功接入蓝牙Mesh网络10中的蓝牙设备。AppKey是蓝牙Mesh网络应用密钥，比如蓝牙网关和某个接入蓝牙Mesh网络的蓝牙设备在某个具体应用场景(比如门锁应用场景)中沟通的密钥。单播地址是待鉴权蓝牙设备成功接入蓝牙Mesh网络10之后与其它成员节点通信时所使用的地址。

[0077] 其中，蓝牙网关10a根据配网数据为待鉴权蓝牙设备进行配网操作，主要是指将配网数据转发给待鉴权蓝牙设备，以供该待鉴权蓝牙设备接入蓝牙Mesh网络10。这里的配网操作是蓝牙Mesh协议中规定的Provisioning中的部分功能，例如在配网操作之前，还包括服务器10b与待鉴权蓝牙设备进行双向鉴权的操作。

[0078] 下面重点描述服务器10b与待鉴权蓝牙设备进行双向鉴权的内容：

[0079] 在已有蓝牙Mesh协议中规定了几种OOB鉴权方式，包括：输入OOB(InputOOB)，输出(Output OOB)，静态OOB(Static OOB)或无OOB(No OOB)。在本申请各实施例中，服务器10b可以选择使用任何一种OOB鉴权方式与待鉴权蓝牙设备进行鉴权。无论采用哪一种OOB鉴权方式，在本申请实施例提供的网络架构中，鉴权方法中的鉴权功能主要由服务器10b和待鉴权蓝牙设备实现，而蓝牙网关10a主要负责信息转发，可选地，蓝牙网关10a还可以辅助性地向用户显示或输出一些与鉴权相关的信息。

[0080] 在本申请一些实施例中，服务器10b可以采用静态OOB鉴权方式与待鉴权蓝牙设备进行双向鉴权，这样服务器10b可以对待鉴权蓝牙设备进行鉴权，便于保证蓝牙Mesh网络的安全性，待鉴权蓝牙设备也可以对服务器10b进行鉴权，便于保证待鉴权蓝牙设备的安全。

[0081] 进一步，为了提高双向鉴权的效率，实现双向鉴权的自动化，服务器10b可以预先在本端维护各个已注册蓝牙设备的鉴权参数，并在各个已注册蓝牙设备中内置自己的鉴权参数。已注册蓝牙设备是指预先向服务器10b注册过的蓝牙设备，属于合法的蓝牙设备。上述鉴权参数包括生成静态OOB信息所需的一些信息，以便于进行静态OOB鉴权。另外，对每个蓝牙设备来说，鉴权参数具有唯一性，即不同蓝牙设备，其鉴权参数不同，基于此所计算出来的静态OOB信息也不同。

[0082] 可选地，鉴权参数可以包括设备标识信息和鉴权密钥(Secret)，设备标识信息是指可唯一标识蓝牙设备的一些信息。其中，鉴权参数中的鉴权密钥与设备标识信息具有一一对应关系，这样可以做到一机一密，可防篡改，防逆向，防仿冒，有利于提高鉴权的安全性。

[0083] 在一些示例性实施例中，鉴权参数中的设备标识信息可以包括蓝牙设备的产品标识(Product ID)和MAC地址。Product ID代表着蓝牙设备的设备能力。不同类型或型号的蓝牙设备，其Product ID不同。同一类型或型号的蓝牙设备，其Product ID相同。基于此，鉴权参数可以表示为三元组信息(Product ID,MAC,Secret)。值得说明的是，鉴权参数并不限于这里的三元组信息。

[0084] 在一可选实施方式中，服务器10b可以向各蓝牙设备制造商开放注册功能，并可为蓝牙设备分配上述鉴权参数。这样，蓝牙设备制造商可以向服务器10b发送注册请求，以请求服务器10b为其生产、制造的蓝牙设备分配具有唯一性的鉴权参数，然后可以将服务器10b分配的鉴权参数内置到相应蓝牙设备中。以待鉴权蓝牙设备为例，待鉴权蓝牙设备对应的制造商在生产或制造出该待鉴权蓝牙设备之前，可以向服务器10b发送注册请求，以请求服务器10b为该蓝牙设备分配鉴权参数。对服务器10b来说，可接收待鉴权蓝牙设备对应的制造商发送的注册请求，根据该注册请求预先为待鉴权蓝牙设备分配鉴权参数，例如分配三元组信息(Product ID,MAC,Secret)，并将分配的鉴权参数发送给制造商，以供制造商在待鉴权蓝牙设备出厂前将分配到的鉴权参数内置到该待鉴权蓝牙设备中。另外，服务器10b为已注册蓝牙设备分配鉴权参数之后，也会在本端维护已注册蓝牙设备的鉴权参数。

[0085] 可选地，制造商可以通过其终端设备与服务器10b进行通信，但不限于终端设备。

[0086] 基于上述鉴权参数，服务器10b可以基于本端维护的待鉴权蓝牙设备的鉴权参数和待鉴权蓝牙设备内置的鉴权参数，采用静态OOB鉴权方式通过目标蓝牙网关与待鉴权蓝牙设备进行双向鉴权，以供待鉴权蓝牙设备安全接入蓝牙Mesh网络10。

[0087] 其中，服务器10b采用静态OOB鉴权方式，通过目标蓝牙网关与待鉴权蓝牙设备进行双向鉴权的过程如下：

[0088] 待鉴权蓝牙设备广播自己的设备标识信息，以便于蓝牙Mesh网络中的蓝牙网关探测到自己。目标蓝牙网关探测到待鉴权蓝牙设备后，将待鉴权蓝牙设备的设备标识信息上报给服务器10b。

[0089] 服务器10b接收目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息；然后，根据待鉴权蓝牙设备的设备标识信息，从本端维护的各个已注册蓝牙设备的鉴权参数中，确定

出待鉴权蓝牙设备的鉴权参数，例如三元组信息(Product ID,MAC,Secret)；然后，根据待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息；通过目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权。其中，服务端随机数是指服务器10b生成第一鉴权信息所使用的随机数。在生成第一鉴权信息的过程中，采用随机数，可以防止暴力破解，有利于提高配网鉴权的安全性。

[0090] 对待鉴权蓝牙设备来说，也可以根据其内置的鉴权参数，例如三元组信息(Product ID,MAC,Secret)和设备随机数生成第二鉴权信息，并可通过目标蓝牙网关将第二鉴权信息和设备随机数转发给服务器10b，以供服务器对待鉴权蓝牙设备进行鉴权。其中，设备随机数是待鉴权蓝牙设备生成第二鉴权信息使用的随机数。同理，在生成第二鉴权信息的过程中，采用随机数，可以防止暴力破解，有利于提高配网鉴权的安全性。

[0091] 可选地，待鉴权蓝牙设备可以先行根据第一鉴权信息和服务端随机数对服务器10b进行鉴权；若服务器10b通过鉴权，则通过目标蓝牙网关将第二鉴权信息和设备随机数转发给服务器10b；若服务器10b未通过鉴权，则可以不向服务器10b发送第二鉴权信息和设备随机数，有利于节约网络资源。

[0092] 对服务器10b来说，可能接收到目标蓝牙网关转发的第二鉴权信息和设备随机数，也有可能不会接收到目标蓝牙网关转发的第二鉴权信息和设备随机数。当接收到目标蓝牙网关转发的第二鉴权信息和设备随机数时，服务器10b可以根据第二鉴权信息和设备随机数对待鉴权蓝牙设备进行鉴权。

[0093] 进一步可选地，服务器10b在生成第一鉴权信息时，可以采用约定的加密算法对本端维护的待鉴权蓝牙设备的鉴权参数进行加密，以生成第一认证值；然后，根据第一认证值和服务端随机数生成第一鉴权信息。其中，服务器10b约定采用的加密算法包括但不限于：SHA256、MD5等。以SHA256加密算法和三元组信息(Product ID,MAC,Secret)为例，第一认证值AuthValue1＝(SHA256(Product ID+MAC+Secret)的高128位。在该公式中，Product ID表示服务器10b本端维护的待鉴权蓝牙设备的产品标识，Secret表示服务器10b本端维护的待鉴权蓝牙设备的鉴权密钥，MAC表示服务器10b本端维护的待鉴权蓝牙设备的MAC地址，AuthValue1表示第一认证值。另外，公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。可选地，第一鉴权信息可以采用公式AES-CMAC(Random1||AuthValue1)计算获得。其中，AES-CMAC表示基于高级加密标准(Advanced Encryption Standard,AES)算法实现的保障信息完整性和认证的密码学方法(Cypher-Based Message Authentication Code)，但并不限于采用AES-CMAC；Random1表示服务端随机数。

[0094] 相应地，待鉴权蓝牙设备在生成第二鉴权信息时，可以采用约定的加密算法对待鉴权蓝牙设备内置的鉴权参数进行加密处理，以生成第二认证值；然后，根据第二认证值和设备随机数生成第二鉴权信息。其中，待鉴权蓝牙设备约定采用的加密算法包括但不限于：SHA256、MD5等。以SHA256和三元组信息(Product ID,MAC,Secret)为例，第二认证值AuthValue2＝(SHA256(ProductID+MAC+Secret)的高128位。在该公式中，Product ID表示待鉴权蓝牙设备内置的产品标识，Secret表示待鉴权蓝牙设备内置的鉴权密钥，MAC表示待鉴权蓝牙设备内置的MAC地址，AuthValue2表示第二认证值。可选地，第二鉴权信息可以采用公式AES-CMAC(Random2||AuthValue1)计算获得。其中，Random2表示设备端随机数。

[0095] 在上述双向鉴权过程中，待鉴权蓝牙设备在收到第一鉴权信息和服务端随机数之后，可以同时结合第一鉴权信息、服务端随机数以及待鉴权蓝牙设备中内置的鉴权参数对服务器10b进行鉴权。以三元组信息(Product ID,MAC,Secret)为例，待鉴权蓝牙设备可以利用同样的加密算法对其内置的三元组信息进行加密处理以生成临时认证值，例如AuthValue0＝(SHA256(Product ID+MAC+Secret)的高128位；然后，利用服务端随机数和该临时认证值AuthValue0计算出临时鉴权信息，例如AES-CMAC(Random1||AuthValue0)；将第一鉴权信息AES-CMAC(Random1||AuthValue1)与临时鉴权信息AES-CMAC(Random1||AuthValue0)进行比较；若临时鉴权信息与第一鉴权信息相同，确定服务器10b通过鉴权；反之，若临时鉴权信息与第一鉴权信息不相同，确定服务器10b未通过鉴权。

[0096] 同理，服务器10b在接收到第二鉴权信息和设备端随机数之后，可以同时结合第二鉴权信息、设备端随机数以及本端维护的待鉴权蓝牙设备的鉴权参数对待鉴权蓝牙设备进行鉴权。以三元组信息(Product ID,MAC,Secret)为例，服务器10b可以利用同样的加密算法对本端维护的待鉴权蓝牙设备的三元组信息进行加密处理以生成临时认证值，例如AuthValue0＝(SHA256(Product ID+MAC+Secret)的高128位；然后，利用设备端随机数和该临时认证值AuthValue0计算出临时鉴权信息，例如AES-CMAC(Random2||AuthValue0)；将第二鉴权信息AES-CMAC(Random2||AuthValue1)与临时鉴权信息AES-CMAC(Random2||AuthValue0)进行比较；若临时鉴权信息与第二鉴权信息相同，确定待鉴权蓝牙设备通过鉴权；反之，若临时鉴权信息与第二鉴权信息不相同，确定待鉴权蓝牙设备未通过鉴权。

[0097] 值得说明的是，上述目标蓝牙网关在服务器10b与待鉴权蓝牙设备之间转发信息的先后顺序可按照蓝牙Mesh协议中约束的顺序。当蓝牙Mesh协议中规定的信息交互顺序发生变化或改变时，上述示例性实施例中目标蓝牙网关转发信息的先后顺序也可以适应性变化。

[0098] 在上述示例性实施例中，服务器可以结合本端维护的待鉴权蓝牙设备的鉴权参数和待鉴权蓝牙设备内置的鉴权参数，采用静态OOB鉴权方式与待鉴权蓝牙设备进行双向鉴权。在整个静态OOB鉴权过程中，无需用户介入，实现了配网鉴权的自动化，有利于改善用户体验，提高了配网鉴权的效率；另外，不同蓝牙设备对应不同静态OOB信息，这有利于保证配网鉴权过程的安全性。

[0099] 本申请实施例除了提供蓝牙Mesh网络之外，还提供了一些方法，这些方法主要从蓝牙Mesh网络中的服务器、目标蓝牙网关以及待鉴权蓝牙设备的角度对配网鉴权过程进行了详细描述。

[0100] 如图2所示，从服务器角度描述的蓝牙Mesh网络的配网鉴权方法包括以下步骤：

[0101] 201、蓝牙Mesh网络中的服务器根据目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息，确定本端维护的待鉴权蓝牙设备的鉴权参数；目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0102] 202、根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息。

[0103] 203、通过目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权。

[0104] 204、在接收到目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据第二鉴

权信息和设备端随机数对待鉴权蓝牙设备进行鉴权;其中,第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的。

[0105] 进一步可选地,在步骤202中,可以根据约定的加密算法对本端维护的待鉴权蓝牙设备的鉴权参数进行加密处理,以生成第一认证值;根据第一认证值和服务端随机数,生成第一鉴权信息。

[0106] 在一些可选实施方式,鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0107] 以三元组信息(Product ID,MAC,Secret)为例,生成第一认证值的一种可选方式包括:采用约定的加密算法,例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理,例如SHA256(Product ID+MAC+Secret),然后取加密结果的高128位作为第一认证值。公式中的“+”表示几种信息之间的组合,但并不限定具体组合方式,例如可以是“拼接”、“与”或“或”等组合方式。

[0108] 可选地,可以采用下述公式AES-CMAC(Random1||AuthValue1)计算出第一鉴权信息。在该公式中,Random1表示服务端随机数;AuthValue1表示第一认证值。

[0109] 可选地,在步骤203中,服务器可以在同一通信过程中将第一鉴权信息和服务端随机数发送给目标蓝牙网关;对目标蓝牙网关来说,可以先将第一鉴权信息转发给待鉴权蓝牙设备,并在接收到待鉴权蓝牙设备发送的第二鉴权信息之后,再将服务端随机数转发给待鉴权蓝牙设备。相应地,在步骤204中,目标蓝牙网关可以在接收到待鉴权蓝牙设备发送的设备端随机数之后,通过同一通信过程将第二鉴权信息和设备端随机数转发服务器。

[0110] 进一步可选地,在步骤201之前,该方法还包括:预先为待鉴权蓝牙设备分配鉴权参数,并在本地维护待鉴权蓝牙设备的鉴权参数;以及将为待鉴权蓝牙设备分配的鉴权参数提供给待鉴权蓝牙设备的制造商,以供该制造商将该鉴权参数内置于待鉴权蓝牙设备中。可选地,可以接收待鉴权蓝牙设备对应的制造商发送的注册请求;根据注册请求为待鉴权蓝牙设备分配鉴权参数。

[0111] 在本实施例中,服务器结合本端维护的蓝牙设备的鉴权参数和蓝牙设备内置的鉴权参数,采用静态OOB鉴权方式与蓝牙设备完成相互鉴权,为蓝牙设备安全接入蓝牙Mesh网络提供了基础。在整个静态OOB鉴权过程中,无需用户介入,实现了自动化,有利于改善用户体验,提高了配网鉴权的效率;另外,不同蓝牙设备对应不同静态OOB信息,这有利于保证配网鉴权过程的安全性。

[0112] 如图3所示,从目标蓝牙网关角度描述的蓝牙Mesh网络的配网鉴权方法包括以下步骤:

[0113] 301、目标蓝牙网关探测到请求接入蓝牙网状(Mesh)网络的待鉴权蓝牙设备的设备标识信息,目标蓝牙网关是蓝牙Mesh网络中的蓝牙网关。

[0114] 302、目标蓝牙网关将待鉴权蓝牙设备的设备标识信息上报给蓝牙Mesh网络中的服务器。

[0115] 303、目标蓝牙网关接收服务器发送的第一鉴权信息和服务端随机数,第一鉴权信息是服务器根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的。

[0116] 304、目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备,以供待鉴权蓝牙设备对服务器进行鉴权。

[0117] 305、目标蓝牙网关在接收到待鉴权蓝牙设备发送的第二鉴权信息和设备端随机

数时，将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权；第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的。

[0118] 可选地，在步骤304和步骤305中，目标蓝牙网关可以先将第一鉴权信息转发给待鉴权蓝牙设备；然后接收待鉴权蓝牙设备发送的第二鉴权信息，在接收到第二鉴权信息之后将服务端随机数转发给待鉴权蓝牙设备。对待鉴权蓝牙设备来说，可以先行根据第一鉴权信息和服务端随机数对服务器进行鉴权；当服务器通过鉴权后，将设备端随机数发送给目标蓝牙网关。基于此，在步骤305中，目标蓝牙网关可以在接收到设备端随机数之后，通过同一通信过程将第二鉴权信息和设备端随机数转发给服务器。

[0119] 在本实施例中，蓝牙网关在服务器与待鉴权蓝牙设备之间进行信息传递，为服务器结合本端维护的待鉴权蓝牙设备的鉴权参数和待鉴权蓝牙设备内置的鉴权参数，采用静态OOB鉴权方式与蓝牙设备完成相互鉴权提供了通信基础。

[0120] 如图4所示，从待鉴权蓝牙设备角度描述的蓝牙Mesh网络的配网鉴权方法包括以下步骤：

[0121] 401、待鉴权蓝牙设备广播其设备标识信息，以供目标蓝牙网关将设备标识信息转发给蓝牙网状(Mesh)网络中的服务器，目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0122] 402、接收目标蓝牙网关转发的第一鉴权信息和服务端随机数，并根据第一鉴权信息和服务端随机数对服务器进行鉴权；第一鉴权信息是服务器根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的。

[0123] 403、根据待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息。

[0124] 404、通过目标蓝牙网关将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权。

[0125] 进一步可选地，在步骤403中，可以根据约定的加密算法对待鉴权蓝牙设备内置的鉴权参数进行加密处理，以生成第二认证值；根据第二认证值和设备端随机数，生成第二鉴权信息。

[0126] 在一些可选实施方式，鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0127] 以三元组信息(Product ID,MAC,Secret)为例，生成第二认证值的一种可选方式包括：采用约定的加密算法，例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理，例如SHA256(Product ID+MAC+Secret)，然后取加密结果的高128位作为第二认证值。公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。

[0128] 可选地，可以采用下述公式AES-CMAC(Random2||AuthValue2)计算出第二鉴权信息。在该公式中，Random2表示设备端随机数；AuthValue2表示第二认证值。

[0129] 在本实施例中，待鉴权蓝牙设备基于内置的鉴权参数，采用静态OOB鉴权方式与服务器完成相互鉴权，使得自己可以安全接入蓝牙Mesh网络。在整个静态OOB鉴权过程中，无需用户介入，实现了自动化，有利于改善用户体验，提高了配网鉴权的效率。

[0130] 其中，图5所示是采用交互方式描述的蓝牙Mesh网络基于三元组的配网鉴权方法的流程示意图。在图5所示实施例中，服务器部署在云端，故简称为云端。如图5所示，该方法包括以下步骤：

[0131] 51、蓝牙设备制造商向云端发送注册请求，以注册蓝牙设备的信息，例如蓝牙灯。

[0132] 52、云端根据注册请求为蓝牙设备分配三元组信息：产品ID(Product ID)(一型一号)，MAC地址以及和MAC地址一一对应的鉴权密钥(Secret)，并将三元组信息返回给制造商。其中，三元组信息用于后续鉴权使用。

[0133] 53、制造商在蓝牙设备出厂前将三元组信息内置到蓝牙设备中，例如可以烧录到蓝牙设备中。

[0134] 54、蓝牙设备上电后广播数据包，该数据包包括蓝牙设备内置的产品ID(Product ID)和MAC地址。

[0135] 55、蓝牙网关探测到蓝牙设备的广播数据包后，向云端上报Product ID和MAC地址。

[0136] 56、云端根据蓝牙网关上报的Product ID和MAC地址，确定本端维护的该蓝牙设备的三元组信息(Product ID1，MAC1，Secret1)，并结合服务端随机数Random1生成第一鉴权信息：AES-CMAC(Random1||AuthValue1)，AuthValue1是SHA256(Product ID1+MAC1+Secret1)的高128位。

[0137] 57、云端向蓝牙网关发送第一鉴权信息和服务端随机数。

[0138] 58、蓝牙网关转发第一鉴权信息给蓝牙设备。

[0139] 59、蓝牙设备根据其内置的三元组信息(Product ID2，MAC2，Secret2)和设备端随机数Random2生成第二鉴权信息：AES-CMAC(Random2||AuthValue2)，AuthValue2是SHA256(Product ID2+MAC2+Secret2)的高128位。

[0140] 60、蓝牙设备发送第二鉴权信息给蓝牙网关。

[0141] 61、蓝牙网关转发服务端随机数给蓝牙设备。62、蓝牙设备根据服务端随机数、第一鉴权信息以及蓝牙设备内置的三元组信息(Product ID2，MAC2，Secret2)对云端进行鉴权。

[0142] 63、当云端通过鉴权时，蓝牙网关发送设备端随机数给蓝牙网关。

[0143] 64、蓝牙网关向云端转发第二鉴权信息和设备端随机数。

[0144] 65、云端根据设备端随机数、第二鉴权信息以及本端维护的三元组信息(Product ID2，MAC2，Secret2)对蓝牙设备进行鉴权。

[0145] 值得说明的是，在本实施例中，采用标号1和2对云端维护的蓝牙设备的三元组信息和蓝牙设备内置的三元组信息进行区分；在正常情况下，两个三元组信息是相同的。

[0146] 在本实施例中，云端可以结合本端维护的蓝牙设备的三元组信息和蓝牙设备内置的三元组信息，采用静态OOB鉴权方式与蓝牙设备进行双向鉴权。在整个静态OOB鉴权过程中，无需用户介入，实现了配网鉴权的自动化，有利于改善用户体验，提高了配网鉴权的效率；另外，不同蓝牙设备对应不同静态OOB信息，这有利于保证配网鉴权过程的安全性。

[0147] 需要说明的是，上述实施例所提供方法的各步骤的执行主体均可以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤401至步骤403的执行主体可以为设备A；又比如，步骤401和402的执行主体可以为设备A，步骤403的执行主体可以为设备B；等等。

[0148] 另外，在上述实施例及附图中的描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的序号如401、402等，仅仅是用于区分开各个不同的操作，序号本身不代表任何

的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。需要说明的是，本文中的“第一”、“第二”等描述，是用于区分不同的消息、设备、模块等，不代表先后顺序，也不限定“第一”和“第二”是不同的类型。

[0149] 图6a为本申请又一示例性实施例提供的一种配网鉴权装置的结构示意图。该配网鉴权装置可位于蓝牙Mesh网络中的服务器内实现，或者独立于服务器但与服务器通信连接。如图6a所示，该装置包括：接收模块60a、确定模块60e、生成模块60b、发送模块60c以及鉴权模块60d。

[0150] 接收模块60a，用于接收目标蓝牙网关上报的请求接入蓝牙Mesh网络的待鉴权蓝牙设备的设备标识信息；目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0151] 确定模块60e，用于根据接收模块60a接收到的待鉴权蓝牙设备的设备标识信息，确定服务器维护的所述待鉴权蓝牙设备的鉴权参数。

[0152] 生成模块60b，用于根据服务器维护的待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息。

[0153] 发送模块60c，用于通过目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权。

[0154] 接收模块60a还用于：接收目标蓝牙网关转发的第二鉴权信息和设备端随机数；其中，第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的。

[0155] 鉴权模块60d，用于在接收模块60a接收到第二鉴权信息和设备端随机数时，根据第二鉴权信息和设备端随机数对待鉴权蓝牙设备进行鉴权。

[0156] 在一可选实施方式中，生成模块60b具体用于：根据约定的加密算法对服务器维护的待鉴权蓝牙设备的鉴权参数进行加密处理，以生成第一认证值；根据第一认证值和服务端随机数，生成第一鉴权信息。

[0157] 在一些可选实施方式，鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0158] 以三元组信息(Product ID,MAC,Secret)为例，生成模块60b在生成第一认证值时，具体用于：采用约定的加密算法，例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理，例如SHA256(Product ID+MAC+Secret)，然后取加密结果的高128位作为第一认证值。公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。

[0159] 可选地，生成模块60b在生成第一鉴权信息时，具体用于：采用下述公式AES-CMAC(Random1||AuthValue1)计算出第一鉴权信息。在该公式中，Random1表示服务端随机数；AuthValue1表示第一认证值。

[0160] 在一可选实施方式中，该配网鉴权装置还包括：分配模块，用于预先为待鉴权蓝牙设备分配鉴权参数，并在服务器端维护待鉴权蓝牙设备的鉴权参数。相应地，发送模块60c还用于：将分配模块为待鉴权蓝牙设备分配的鉴权参数提供给待鉴权蓝牙设备的制造商，以供该制造商将所述鉴权参数内置于待鉴权蓝牙设备中。

[0161] 可选地，接收模块60a还用于：接收待鉴权蓝牙设备对应的制造商发送的注册请求。相应地，分配模块具体可用于：根据注册请求预先为待鉴权蓝牙设备分配鉴权参数。

[0162] 以上描述了配网鉴权装置的内部功能和结构，实际中，该配网鉴权装置可实现为

蓝牙Mesh网络中的服务器，如图6b所示，该服务器包括：存储器601、处理器602以及通信组件603。

[0163] 通信组件603，用于接收目标蓝牙网关上报的请求接入蓝牙Mesh网络的待鉴权蓝牙设备的设备标识信息；其中目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0164] 存储器601，用于存储计算机程序，并可被配置为存储其它各种数据以支持在服务器上的操作。这些数据的示例包括用于在服务器上操作的任何应用程序或方法的指令，例如，各个已注册蓝牙设备的鉴权参数，联系人数据，电话簿数据，消息，图片，视频等。

[0165] 处理器602，与存储器601耦合，用于执行存储器601中的计算机程序，以用于：

[0166] 根据待鉴权蓝牙设备的设备标识信息，确定服务器维护的待鉴权蓝牙设备的鉴权参数；

[0167] 根据服务器维护的待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息；

[0168] 通过目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权；以及

[0169] 通过通信组件603接收目标蓝牙网关转发的第二鉴权信息和设备端随机数，并在通信组件603接收到第二鉴权信息和设备端随机数时，根据第二鉴权信息和设备端随机数对待鉴权蓝牙设备进行鉴权。其中，第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的。

[0170] 在一可选实施方式中，处理器602具体用于：根据约定的加密算法对服务器维护的待鉴权蓝牙设备的鉴权参数进行加密处理，以生成第一认证值；根据第一认证值和服务端随机数，生成第一鉴权信息。

[0171] 在一些可选实施方式，鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0172] 以三元组信息(Product ID,MAC,Secret)为例，处理器602在生成第一认证值时，具体用于：采用约定的加密算法，例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理，例如SHA256(Product ID+MAC+Secret)，然后取加密结果的高128位作为第一认证值。公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。

[0173] 可选地，处理器602在生成第一鉴权信息时，具体用于：采用下述公式AES-CMAC(Random1||AuthValue1)计算出第一鉴权信息。在该公式中，Random1表示服务端随机数；AuthValue1表示第一认证值。

[0174] 在一可选实施方式中，处理器602还用于：预先为待鉴权蓝牙设备分配鉴权参数，并在服务器端维护待鉴权蓝牙设备的鉴权参数。通信组件603还用于：将分配模块为待鉴权蓝牙设备分配的鉴权参数提供给待鉴权蓝牙设备的制造商，以供该制造商将所述鉴权参数内置于待鉴权蓝牙设备中。

[0175] 可选地，通信组件603还用于：接收待鉴权蓝牙设备对应的制造商发送的注册请求。相应地，处理器602具体可用于：根据注册请求预先为待鉴权蓝牙设备分配鉴权参数。

[0176] 进一步，如图6b所示，该服务器还包括：电源组件604等其它组件。图6b中仅示意性给出部分组件，并不意味着服务器只包括图6b所示组件。

[0177] 相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，计算机程序被执行时能够实现上述方法实施例中可由服务器执行的各步骤。

[0178] 图7a为本申请又一示例性实施例提供的另一种配网鉴权装置的结构示意图。该配网鉴权装置可位于待鉴权蓝牙设备内实现，或者独立于待鉴权蓝牙设备但与待鉴权蓝牙设备通信连接。如图7a所示，该装置包括：广播模块70a、接收模块70b、生成模块70c、发送模块70d以及鉴权模块70e。

[0179] 广播模块70a，用于广播待鉴权蓝牙设备的设备标识信息，以供目标蓝牙网关将该设备标识信息转发给蓝牙Mesh网络中的服务器，目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0180] 接收模块70b，用于接收目标蓝牙网关转发的第一鉴权信息和服务端随机数，第一鉴权信息是服务器根据服务器维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的。

[0181] 鉴权模块70e，用于根据第一鉴权信息和服务端随机数对服务器进行鉴权。

[0182] 生成模块70c，用于根据待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息。

[0183] 发送模块70d，用于通过目标蓝牙网关将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权。

[0184] 在一可选实施方式中，生成模块70c具体用于：根据约定的加密算法对待鉴权蓝牙设备内置的鉴权参数进行加密处理，以生成第二认证值；根据第二认证值和设备端随机数，生成第二鉴权信息。

[0185] 在一些可选实施方式，鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0186] 以三元组信息(Product ID,MAC,Secret)为例，生成模块70c在生成第二认证值时，具体用于：采用约定的加密算法，例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理，例如SHA256(Product ID+MAC+Secret)，然后取加密结果的高128位作为第二认证值。公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。

[0187] 可选地，生成模块70c在生成第二鉴权信息时，具体用于：可以采用下述公式AES-CMAC(Random2||AuthValue2)计算出第二鉴权信息。在该公式中，Random2表示设备端随机数；AuthValue2表示第二认证值。

[0188] 以上描述了配网鉴权装置的内部功能和结构，实际中，该配网鉴权装置可实现为蓝牙设备，如图7b所示，该蓝牙设备包括：存储器701、处理器702以及通信组件703。

[0189] 通信组件703，用于广播蓝牙设备的设备标识信息，以供目标蓝牙网关将设备标识信息转发给蓝牙Mesh网络中的服务器；以及接收目标蓝牙网关转发的第一鉴权信息和服务端随机数，第一鉴权信息是服务器根据服务器维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的，目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关。

[0190] 存储器701，用于存储计算机程序，并可被配置为存储其它各种数据以支持在服务器上的操作。这些数据的示例包括用于在服务器上操作的任何应用程序或方法的指令，例如，待鉴权蓝牙设备的鉴权参数，联系人数据，电话簿数据，消息，图片，视频等。

[0191] 处理器702，与存储器701耦合，用于执行存储器701中的计算机程序，以用于：

[0192] 根据第一鉴权信息和服务端随机数对服务器进行鉴权，根据待鉴权蓝牙设备内置

的鉴权参数和设备端随机数生成第二鉴权信息，并通过目标蓝牙网关将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权。

[0193] 在一可选实施方式中，处理器702具体用于：根据约定的加密算法对待鉴权蓝牙设备内置的鉴权参数进行加密处理，以生成第二认证值；根据第二认证值和设备端随机数，生成第二鉴权信息。

[0194] 在一些可选实施方式，鉴权参可以数是三元组信息(Product ID,MAC,Secret)。

[0195] 以三元组信息(Product ID,MAC,Secret)为例，处理器702在生成第二认证值时，具体用于：采用约定的加密算法，例如SHA256、MD5等对三元组信息(Product ID,MAC,Secret)进行加密处理，例如SHA256(Product ID+MAC+Secret)，然后取加密结果的高128位作为第二认证值。公式中的“+”表示几种信息之间的组合，但并不限定具体组合方式，例如可以是“拼接”、“与”或“或”等组合方式。

[0196] 可选地，处理器702在生成第二鉴权信息时，具体用于：可以采用下述公式AES-CMAC(Random2||AuthValue2)计算出第二鉴权信息。在该公式中，Random2表示设备端随机数；AuthValue2表示第二认证值。

[0197] 进一步，如图7b所示，该蓝牙设备还包括：显示器704、电源组件705、音频组件706等其它组件。图7b中仅示意性给出部分组件，并不意味着蓝牙设备只包括图7b所示组件。

[0198] 相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，计算机程序被执行时能够实现上述方法实施例中可由蓝牙设备执行的各步骤。

[0199] 上述图6b和图7b中的存储器，可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0200] 上述图7b和图7b中的通信组件被配置为便于通信组件所在设备和其他设备之间有线或无线方式的通信。通信组件所在设备可以接入基于通信标准的无线网络，如WiFi，2G或3G，或它们的组合。在一个示例性实施例中，通信组件经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件还包括近场通信(NFC)模块，以促进短程通信。例如，在NFC模块可基于射频识别(RFID)技术，红外数据协会(IrDA)技术，超宽带(UWB)技术，蓝牙(BT)技术和其他技术来实现。

[0201] 上述图7b中的显示器包括屏幕，其屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。

[0202] 上述图6b和图7b中的电源组件，为电源组件所在设备的各种组件提供电力。电源组件可以包括电源管理系统，一个或多个电源，及其他与为电源组件所在设备生成、管理和分配电力相关联的组件。

[0203] 上述图7b中的音频组件，可被配置为输出和/或输入音频信号。例如，音频组件包括一个麦克风(MIC)，当音频组件所在设备处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存

储器或经由通信组件发送。在一些实施例中，音频组件还包括一个扬声器，用于输出音频信号。

[0204] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0205] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0206] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0207] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0208] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0209] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0210] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitorymedia)，如调制的数据信号和载波。

[0211] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0212] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

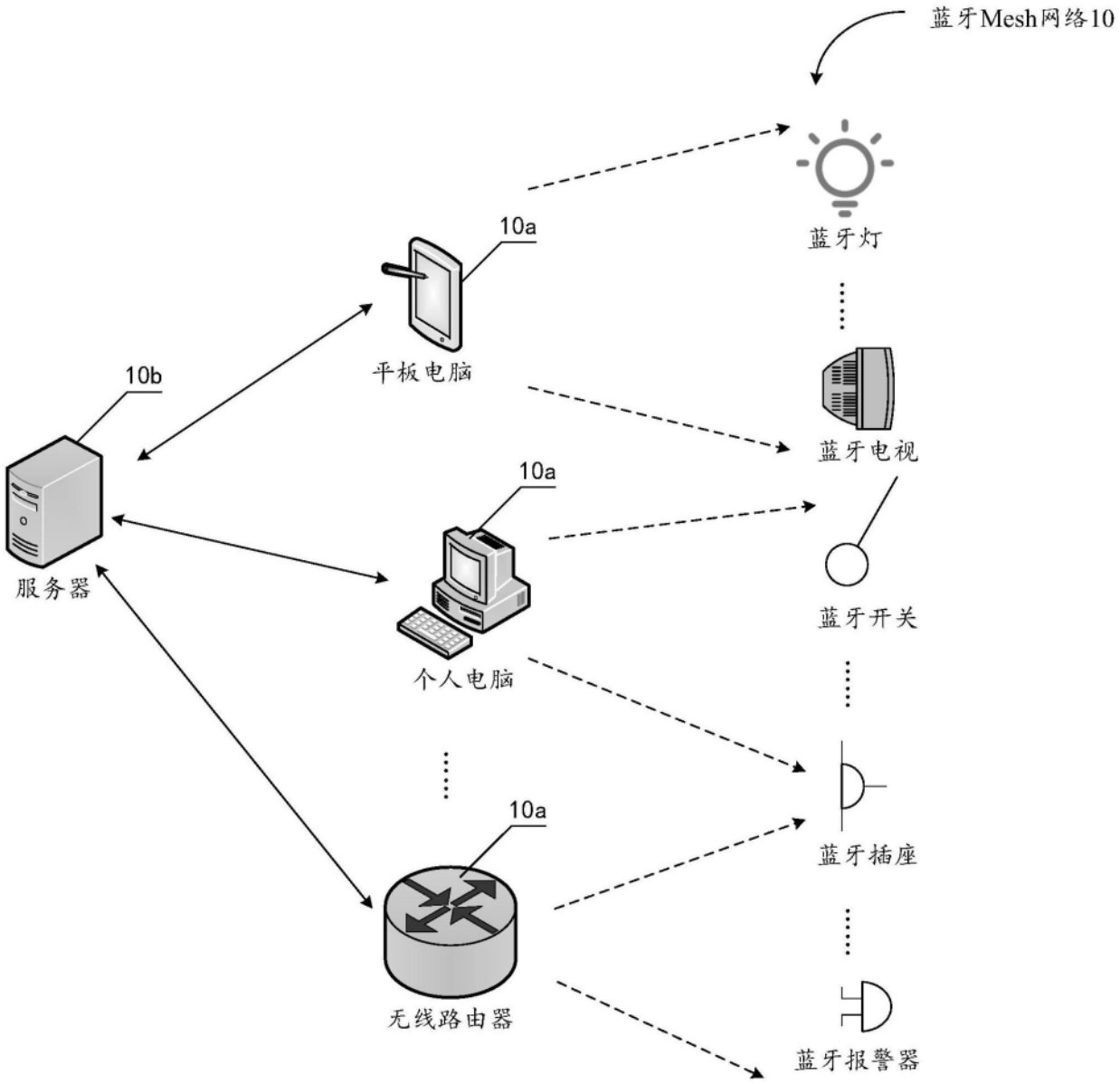

蓝牙Mesh网络10
蓝牙灯
10a
平板电脑
10b
服务器
蓝牙电视
10a
蓝牙开关
个人电脑
10a
蓝牙插座
无线路由器
蓝牙报警器

图1

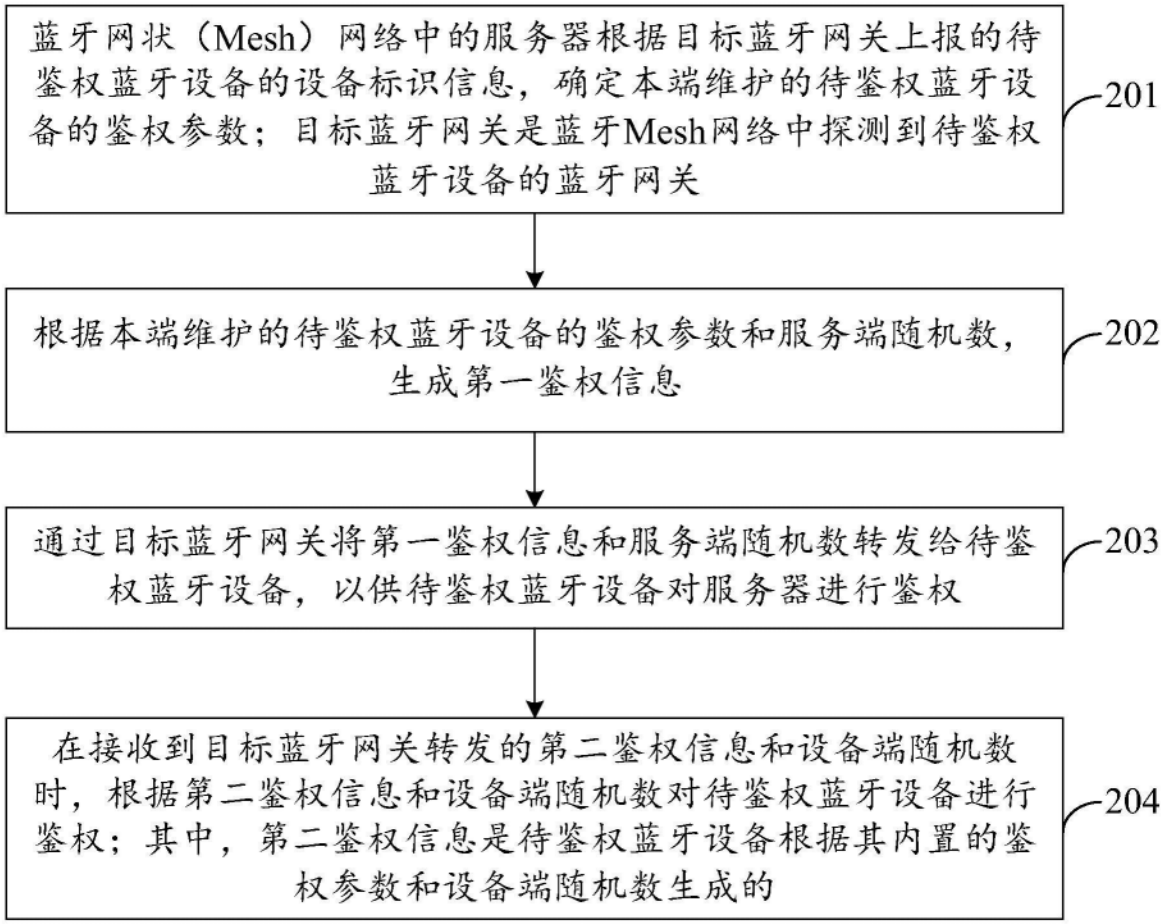

蓝牙网状（Mesh）网络中的服务器根据目标蓝牙网关上报的待鉴权蓝牙设备的设备标识信息，确定本端维护的待鉴权蓝牙设备的鉴权参数；目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关
201
根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数，生成第一鉴权信息
202
通过目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权
203
在接收到目标蓝牙网关转发的第二鉴权信息和设备端随机数时，根据第二鉴权信息和设备端随机数对待鉴权蓝牙设备进行鉴权；其中，第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的
204

图2

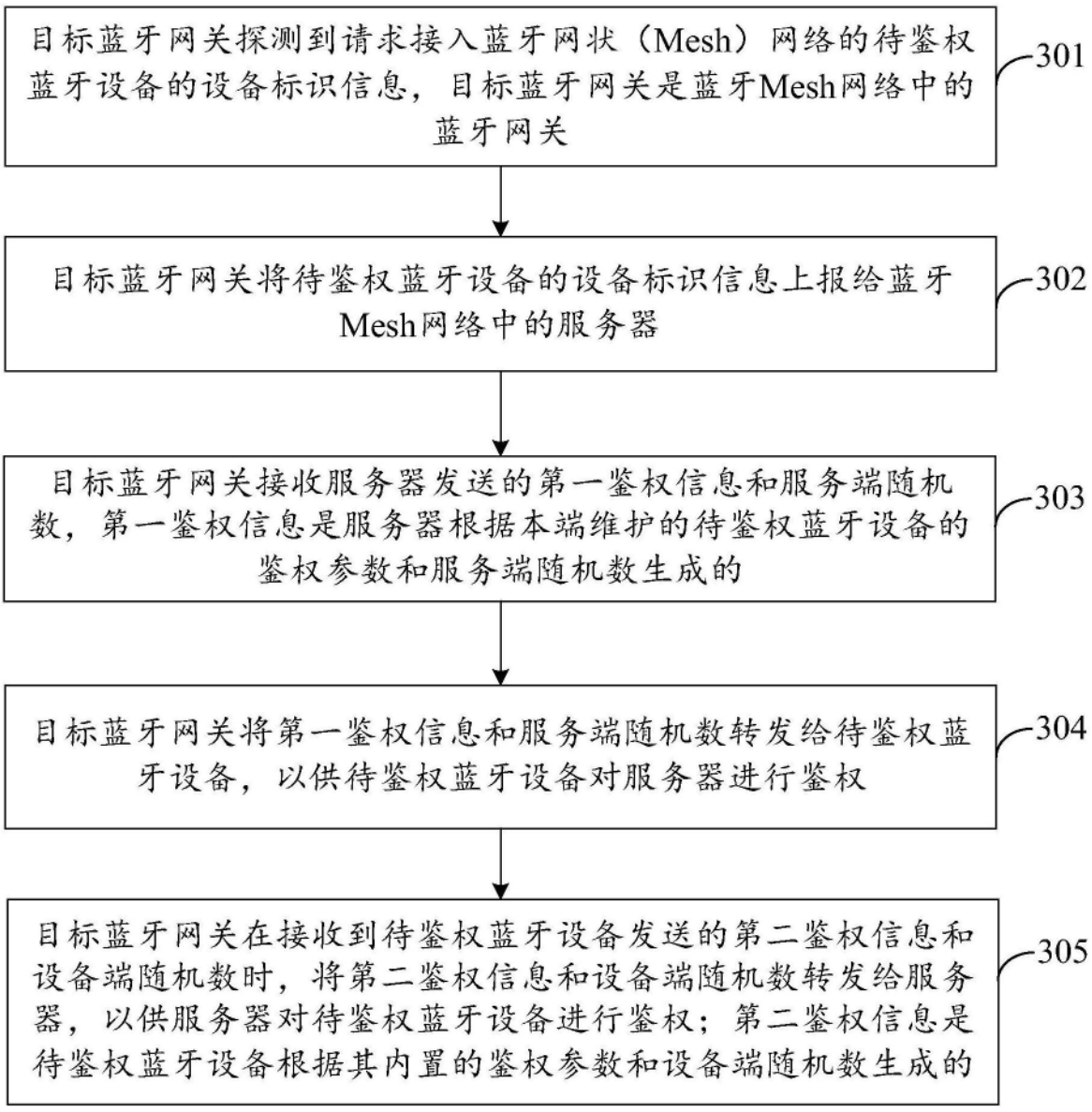

目标蓝牙网关探测到请求接入蓝牙网状（Mesh）网络的待鉴权蓝牙设备的设备标识信息，目标蓝牙网关是蓝牙Mesh网络中的蓝牙网关
301
目标蓝牙网关将待鉴权蓝牙设备的设备标识信息上报给蓝牙Mesh网络中的服务器
302
目标蓝牙网关接收服务器发送的第一鉴权信息和服务端随机数，第一鉴权信息是服务器根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的
303
目标蓝牙网关将第一鉴权信息和服务端随机数转发给待鉴权蓝牙设备，以供待鉴权蓝牙设备对服务器进行鉴权
304
目标蓝牙网关在接收到待鉴权蓝牙设备发送的第二鉴权信息和设备端随机数时，将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权；第二鉴权信息是待鉴权蓝牙设备根据其内置的鉴权参数和设备端随机数生成的
305

图3

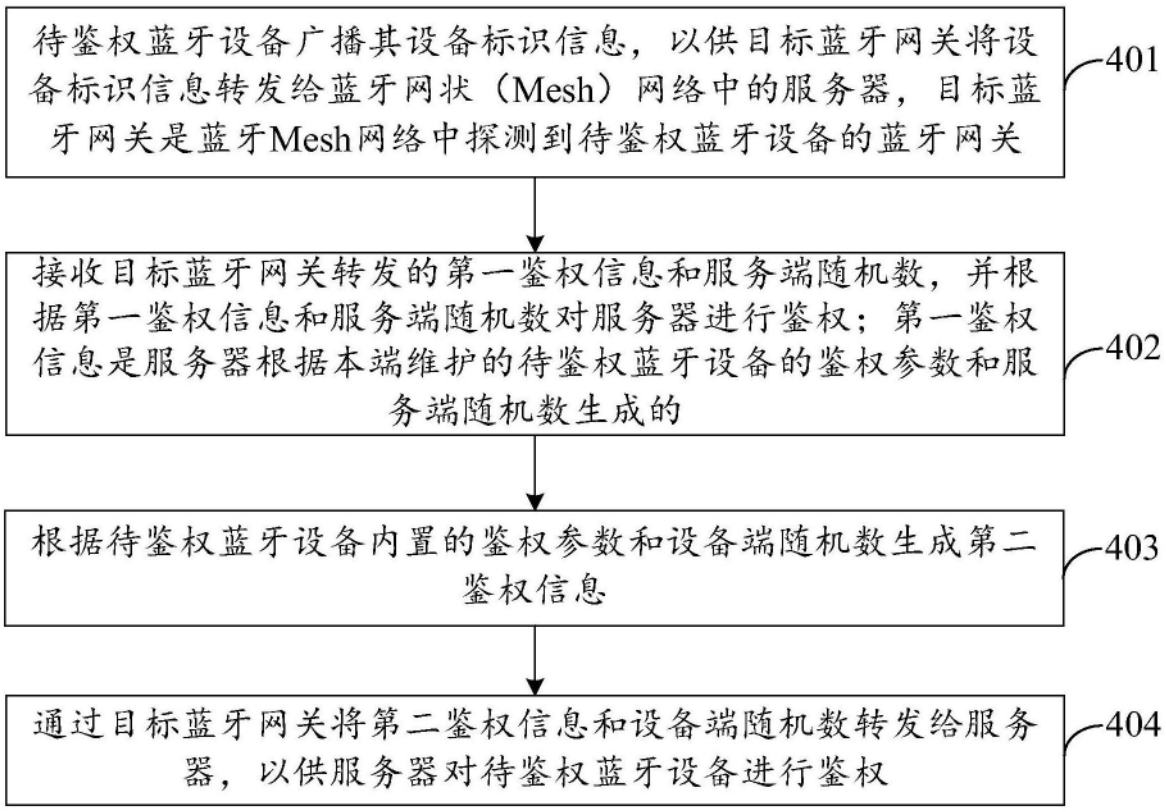

待鉴权蓝牙设备广播其设备标识信息，以供目标蓝牙网关将设备标识信息转发给蓝牙网状（Mesh）网络中的服务器，目标蓝牙网关是蓝牙Mesh网络中探测到待鉴权蓝牙设备的蓝牙网关
401
接收目标蓝牙网关转发的第一鉴权信息和服务端随机数，并根据第一鉴权信息和服务端随机数对服务器进行鉴权；第一鉴权信息是服务器根据本端维护的待鉴权蓝牙设备的鉴权参数和服务端随机数生成的
402
根据待鉴权蓝牙设备内置的鉴权参数和设备端随机数生成第二鉴权信息
403
通过目标蓝牙网关将第二鉴权信息和设备端随机数转发给服务器，以供服务器对待鉴权蓝牙设备进行鉴权
404

图4

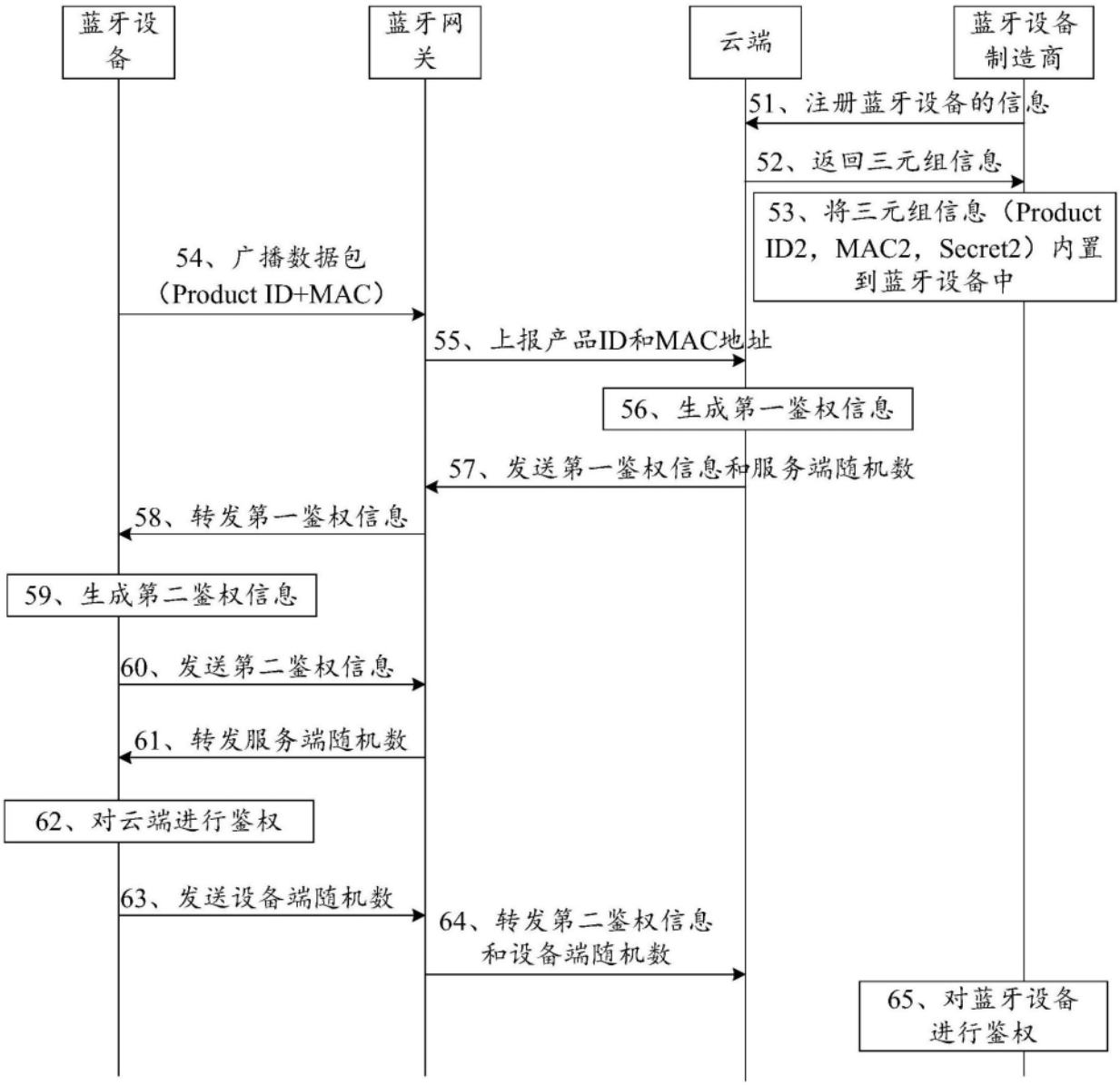

蓝牙设备
蓝牙网关
云端
蓝牙设备制造商
51、注册蓝牙设备的信息
52、返回三元组信息
53、将三元组信息（Product ID2，MAC2，Secret2）内置到蓝牙设备中
54、广播数据包（Product ID+MAC）
55、上报产品ID和MAC地址
56、生成第一鉴权信息
57、发送第一鉴权信息和服务端随机数
58、转发第一鉴权信息
59、生成第二鉴权信息
60、发送第二鉴权信息
61、转发服务端随机数
62、对云端进行鉴权
63、发送设备端随机数
64、转发第二鉴权信息和设备端随机数
65、对蓝牙设备进行鉴权

图5

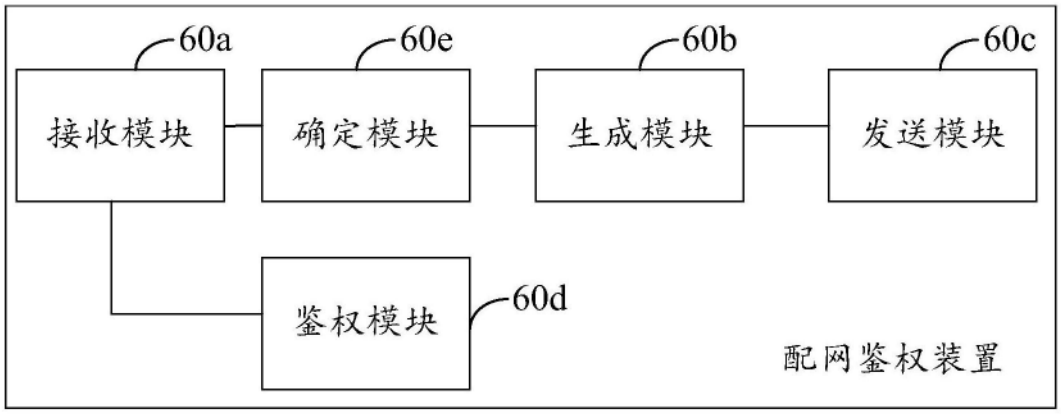

60a
60e
60b
60c
接收模块
确定模块
生成模块
发送模块
鉴权模块
60d
配网鉴权装置

图6a

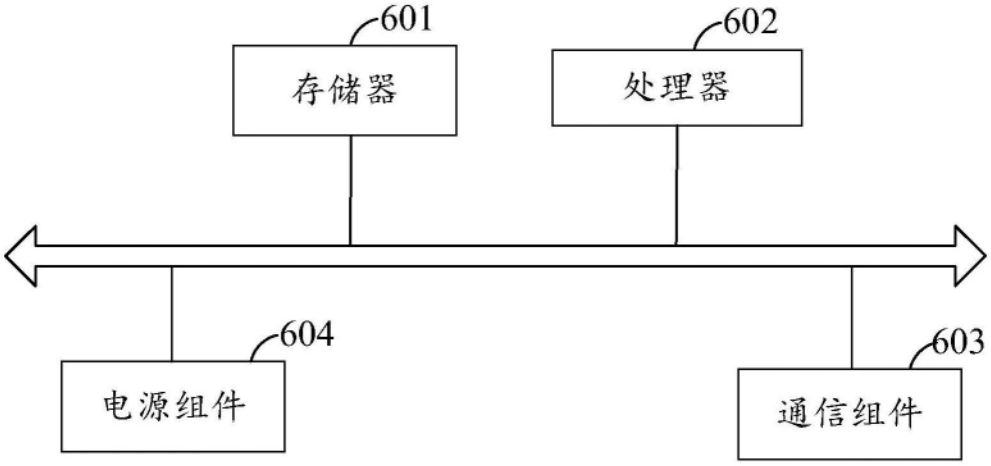

601
602
存储器
处理器
604
603
电源组件
通信组件

图6b

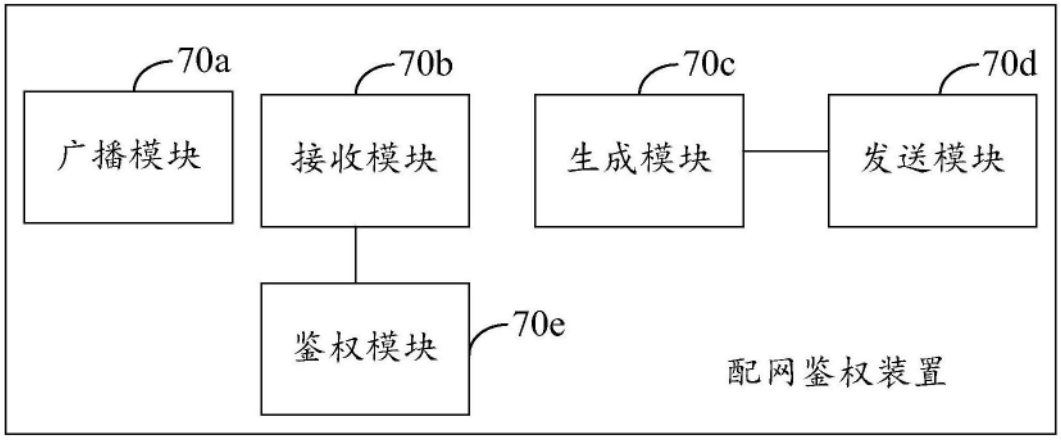

70a
70b
70c
70d
广播模块
接收模块
生成模块
发送模块
鉴权模块
70e
配网鉴权装置

图7a

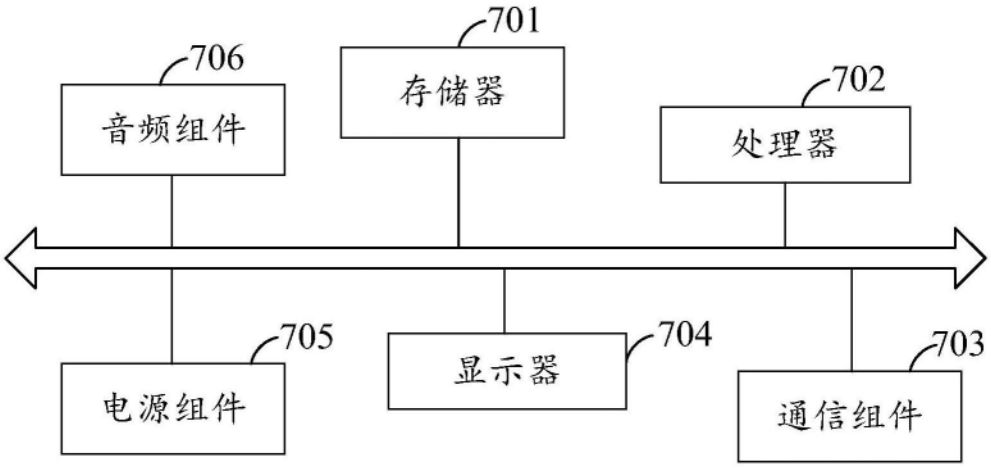


图7b