



## (12)发明专利

(10)授权公告号 CN 103385013 B

(45)授权公告日 2017.09.15

(21)申请号 201280011036.9

(22)申请日 2012.02.09

(65)同一申请的已公布的文献号

申请公布号 CN 103385013 A

(43)申请公布日 2013.11.06

(30)优先权数据

11305216.1 2011.03.01 EP

(85)PCT国际申请进入国家阶段日

2013.08.30

(86)PCT国际申请的申请数据

PCT/IB2012/050587 2012.02.09

(87)PCT国际申请的公布数据

W02012/117306 EN 2012.09.07

(73)专利权人 皇家飞利浦有限公司

地址 荷兰艾恩德霍芬

(72)发明人 J.A.C.伯恩森 M.H.J.德拉艾杰

(74)专利代理机构 中国专利代理(香港)有限公司  
72001

代理人 李舒 汪扬

(51)Int.Cl.

H04W 12/06(2006.01)

(56)对比文件

CN 101785198 A, 2010.07.21,

US 2004/0203354 A1, 2004.10.14,

US 2004/0122649 A1, 2004.06.24,

US 2009/0058635 A1, 2009.03.05,

审查员 卢志飞

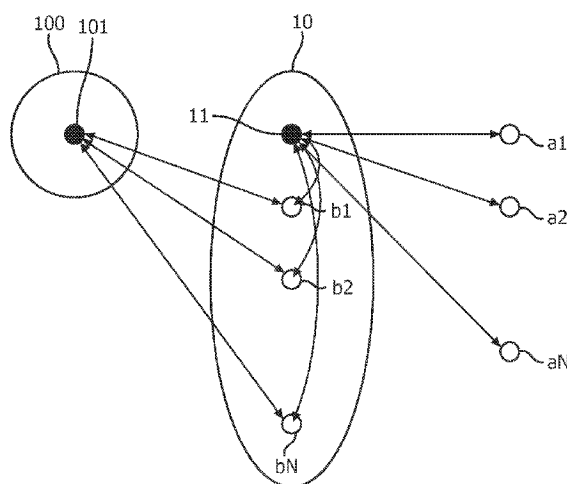
权利要求书2页 说明书6页 附图3页

### (54)发明名称

用于使能设备间的无线安全通信的方法

### (57)摘要

本发明涉及一种用于使能至少一个第一从设备(a1-aN)与第一主设备(101)之间的无线安全通信的无线对接站(10)。所述无线对接站(10)包括:-第二主设备(11),其用于使用在所述至少一个第一设备(a1-aN)上实施的配对协议与所述至少一个第一设备(a1-aN)配对;-至少一个中继从设备(b1-bN),其对应于所述至少一个第一设备(a1-aN),并且其适应于使用安全协议与所述第一主设备(101)配对;-装置,用于将关于所述至少一个中继从设备(b1-bN)的信息发送到所述第一主设备(101)。



1. 一种用于使能多个从设备 (a1-aN) 与第一主设备 (101) 之间的无线安全通信的方法, 其特征在于所述方法包括:

第一无线对接站 (10) 配置第二主设备 (11),

使用在所述多个从设备 (a1-aN) 上实施的配对协议使所述多个从设备 (a1-aN) 与所述第二主设备 (11) 配对, 以便使用第二链路密钥使能所述多个从设备 (a1-aN) 与所述第二主设备之间的第二无线安全通信;

所述第一无线对接站 (10) 配置多个中继从设备 (b1-bN), 所述多个中继从设备 (b1-bN) 与所述多个从设备 (a1-aN) 通过在具有不同的设备地址的同时功能上相同而对应, 所述多个中继从设备 (b1-bN) 适应于使用安全配对协议与第一主设备 (101) 配对;

所述第一无线对接站 (10) 将用于使用所述安全配对协议使所述多个中继从设备 (b1-bN) 与所述第一主设备 (101) 配对的关于所述多个中继从设备 (b1-bN) 的信息发送到所述第一主设备 (101), 以便使用不同于所述第二链路密钥的第一链路密钥使能所述多个中继从设备 (b1-bN) 与所述第一主设备 (101) 之间的第一无线安全通信。

2. 根据权利要求1所述的方法, 还包括:

所述第一主设备 (101) 选择要连接到的多个中继从设备 (b1-bN);

针对所述多个选择的中继从设备 (b1-bN) 仅执行所述安全配对协议所要求的交互一次。

3. 根据权利要求2所述的方法, 其中, 所述安全配对协议包括所述第一主设备 (101) 与所述第一无线对接站 (10) 之间的带外交互。

4. 根据权利要求2所述的方法, 其中, 所述第一主设备 (101) 仅与至少一个预定的中继从设备 (b1-bN) 配对。

5. 根据权利要求2所述的方法, 进一步包括记录安全配对信息以允许自动地进行所述第一主设备 (101) 的进一步配对。

6. 根据权利要求1所述的方法, 其中, 所述安全配对协议是蓝牙通信标准中的一个。

7. 根据权利要求6所述的方法, 其中, 所述安全配对协议是蓝牙V2.1的“安全简单配对-带外”协议。

8. 根据权利要求7所述的方法, 其中, 所述安全配对协议在所述第一主设备 (101) 与所述第一无线对接站 (10) 之间使用近场通信。

9. 根据权利要求1所述的方法, 所述无线安全通信包括至少一个从设备 (c1-cN) 的附加集, 所述方法进一步包括:

第二无线对接站 (20) 配置第三主设备 (22),

使用在所述附加集的所述至少一个从设备 (c1-cN) 上实施的配对协议使至少一个从设备 (c1-cN) 的所述附加集与所述第三主设备 (22) 配对;

所述第二无线对接站 (20) 配置与至少一个从设备 (c1-cN) 的所述附加集对应的至少一个中继从设备 (d1-dN) 的附加集, 至少一个中继从设备 (d1-dN) 的所述附加集适应于使用安全配对协议与所述第一主设备 (101) 配对;

在所述第一无线对接站 (10) 和所述第二无线对接站 (20) 之间配置通信信道 (30) 以用于交换关于与所述多个从设备 (a1-aN) 对应的中继从设备 (b1-bN) 以及与至少一个从设备 (c1-cN) 的所述附加集对应的至少一个中继从设备 (d1-dN) 的信息;

所述第一无线对接站(10)和所述第二无线对接站(20)中的一个将关于与所述多个从设备(a1-aN)对应的中继从设备(b1-bN)以及与至少一个从设备(c1-cN)的所述附加集对应的至少一个中继从设备(d1-dN)的信息发送到所述第一主设备(101)。

10. 根据权利要求1所述的方法,所述无线安全通信包括至少一个从设备(c1-cN)的附加集,所述方法进一步包括:

第二无线对接站(20)配置第三主设备(22),

使用在所述附加集的所述至少一个从设备(c1-cN)上实施的配对协议使至少一个从设备(c1-cN)的所述附加集与所述第三主设备(22)配对;

在所述第一无线对接站(10)和所述第二无线对接站(20)之间配置通信信道(30)以用于向所述第一无线对接站(10)提供从设备(c1-cN)的所述附加集的数据;

所述第一无线对接站(10)配置与至少一个从设备(c1-cN)的所述附加集对应的至少一个中继从设备(d1-dN)的附加集,至少一个中继从设备(d1-dN)的所述附加集适应于使用安全配对协议与所述第一主设备(101)配对;

所述第一无线对接站(10)将关于与所述多个从设备(a1-aN)对应的中继从设备(b1-bN)以及与至少一个从设备(c1-cN)的所述附加集对应的至少一个中继从设备(d1-dN)的信息发送到所述第一主设备(101)。

11. 一种用于使能多个从设备(a1-aN)与第一主设备(101)之间的无线安全通信的无线对接站(10),

其特征在于所述无线对接站(10)包括:

第二主设备(11),其用于使用在所述多个从设备(a1-aN)上实施的配对协议与所述多个从设备(a1-aN)配对,以便使用第二链路密钥使能所述多个从设备(a1-aN)与所述第二主设备之间的第二无线安全通信,

多个中继从设备(b1-bN),所述多个中继从设备(b1-bN)与所述多个从设备(a1-aN)通过在具有不同的设备地址的同时功能上相同而对应,并且所述多个中继从设备适应于使用安全配对协议与所述第一主设备(101)配对,

装置,用于将用于使用所述安全配对协议使所述多个中继从设备(b1-bN)与所述第一主设备(101)配对的关于所述多个中继从设备(b1-bN)的信息发送到所述第一主设备(101),以便使用不同于所述第二链路密钥的第一链路密钥使能所述多个中继从设备(b1-bN)与所述第一主设备(101)之间的第一无线安全通信。

12. 根据权利要求11所述的无线对接站,

所述第一主设备(101)被布置用于选择要连接到的多个中继从设备(b1-bN);

所述无线对接站被布置用于针对所述多个选择的中继从设备(b1-bN)仅执行所述安全配对协议所要求的交互一次。

## 用于使能设备间的无线安全通信的方法

### 技术领域

[0001] 本发明涉及无线家庭网络,并且更特别地,涉及用于使能至少一个从设备与主设备之间的无线安全通信的方法。这个发明例如与蓝牙无线网络相关。

### 背景技术

[0002] 文档W003/053048A1公开了一种包括被无线互连的设备的系统。这个系统可以形成适应于与诸如个人数字助理PDA、智能电话、膝上型电脑等之类的便携式设备进行通信的对接(docking)环境。用于所有这种设备之间的无线通信的适当技术例如是Wi-Fi或蓝牙等等。尽管通信是无线的,但是所述设备不能够直接地通信,并且他们需要被配对。一旦两个设备之间的初始配对已被执行,这两个设备之间的进一步配对就可以以自动的方式发生。

[0003] 存在用于使设备配对的各种可能性。例如,在V2.1以前的蓝牙版本的常规蓝牙核心规范中,如果用户想要蓝牙设备之间的安全配对,则蓝牙设备的配对可能要求用户输入个人识别号码PIN码。

[0004] 在蓝牙V2.1中,称作安全简单配对的另一配对方案被添加。存在安全简单配对的四个基本变体。前两个要求用户动作(“万能钥匙比较(Passkey Compare)”和“万能钥匙输入(Passkey Entry)”)。下一个变体“简单工作”不要求用户交互,但它不提供针对所谓的中间人攻击的保护。剩下一个“带外(Out of Band)”可能牵涉一些用户交互,诸如在近场通信(NFC)被使用的情况下移动一个设备靠近另一个设备。

[0005] 现有配对协议的缺点是设备必须能够执行可用于它们中两者的配对协议。另一缺点是便携式设备必须一次并用适当的配对协议配对到单个设备。

[0006] US2004/0122649描述了一种用于计算机外围设备的无线电缆更换。用于模拟物理连接的方法使用无线连接并且包括使用主机控制器根据通信协议来建立与外围设备的通信连接。所述方法进一步包括:接收携带具有由所述通信协议所规定的格式的数据的无线信号;从所述无线信号中提取所述数据;以及使用所述通信连接将所述数据传送到所述外围设备。

[0007] US2009/0058635描述了在无线网络上的数据传输。患者可植入医疗设备(PIMD)与便携式患者发信机(PPC)之间的通信经由PPC的第一无线电依照第一协议被提供,而PPC的第二无线电与无线网络之间的通信依照第二协议被实现。来自PIMD的数据经由第一无线电被接收,PIMD数据经由第二无线电使用选择的传输机制而被传送到无线网络。

### 发明内容

[0008] 本发明的目的是解决上面提到的缺点中的至少一个。

[0009] 本发明的目标是提供一种用于使能至少一个从设备与主设备之间的无线安全通信的方法。

[0010] 这个目标被用这样的方法实现,所述方法包括:

[0011] 一 无线对接站配置第二主设备,

[0012] — 使用在多个从设备上实施的配对协议使所述多个从设备与所述第二主设备配对,以便使用第二链路密钥使能所述多个从设备与所述第二主设备之间的第二无线安全通信;

[0013] — 所述无线对接站配置对应于所述多个从设备的多个中继从设备,其通过在具有不同的设备地址的同时功能上相同来实现,所述多个中继从设备适应于使用安全配对协议与第一主设备配对;

[0014] — 所述无线对接站将用于使用所述安全配对协议使所述多个中继从设备与所述第一主设备配对的关于所述多个中继从设备的信息发送到所述第一主设备,以便使用不同于所述第二链路密钥的第一链路密钥使能所述多个中继从设备与所述第一主设备之间的第一无线安全通信。

[0015] 所述方法具有优点:使第一从设备可用于经由安全配对协议配对到第一主设备而无论可用于每个第一从设备的配对协议如何。

[0016] 根据本发明的实施例,所述方法还包括:

[0017] — 所述第一主设备选择要连接到的多个中继从设备;

[0018] — 针对所述多个选择的设备仅执行所述安全配对协议所要求的交互一次。

[0019] 这具有简化用户交互的优点。代替重复第一主设备到每个中继从设备的配对,用户仅仅被要求针对所有所选中继从设备进行一次。因此,所要求保护的发明使能了无线设备之间的方便且安全的配对,而无论第一从设备的数目如何以及无论可用于第一从设备的配对协议如何。

[0020] 根据本发明的其它实施例:

[0021] — 安全配对协议可以包括所述第一主设备与所述无线对接站之间的带外交互;

[0022] — 所述第一主设备可以仅与至少一个预定的中继从设备配对;

[0023] — 安全配对信息可以被记录以允许自动地进行所述第一主设备的进一步配对;

[0024] — 安全配对协议可能是蓝牙通信标准中的安全配对协议;

[0025] — 安全配对协议可能是蓝牙V2.1的“安全简单配对-带外”协议;

[0026] — 安全协议可以在所述第一主设备与所述无线对接站之间使用近场通信。

[0027] 根据其中无线安全通信包括至少一个从设备的附加集的本发明的另一实施例,所述方法进一步包括:

[0028] — 附加的无线对接站配置第三主设备,

[0029] — 使用在所述附加集的至少一个从设备上实施的配对协议使至少一个从设备的所述附加集与所述第三主设备配对;

[0030] — 所述附加的无线对接站配置与至少一个从设备的附加集对应的至少一个中继从设备的附加集,至少一个中继从设备的所述附加集适应于使用安全配对协议与所述第一主设备配对;

[0031] — 在所述无线对接站之间配置通信信道以用于交换关于中继从设备的信息;

[0032] — 所述无线对接站中的一个将关于所述中继从设备的信息发送到所述第一主设备。

[0033] 根据其中无线安全通信还包括至少一个从设备的附加集的本发明的另一实施例,所述方法进一步包括:

- [0034] — 附加的无线对接站配置第三主设备，
- [0035] — 使用在所述附加集的至少一个从设备上实施的配对协议使至少一个从设备的所述附加集与所述第三主设备配对；
- [0036] — 在所述无线对接站之间配置通信信道以用于向所述中间系统提供从设备的附加集的数据；
- [0037] — 所述无线对接站配置与至少一个从设备的附加集对应的至少一个中继从设备的附加集，至少一个中继从设备的所述附加集适应于使用安全配对协议与所述第一主设备配对；
- [0038] — 所述无线对接站将关于所述中继从设备的信息发送到所述第一主设备。
- [0039] 本发明的这些和其它方面从在下文中所描述的实施例中将是明显的，并且将参考在下文中所描述的实施例而被阐明。

## 附图说明

- [0040] 现将参考附图通过例子对本发明进行更详细的描述，其中
- [0041] 图1是具有从设备、中间系统、第一中继从设备以及第一主设备的无线网络的示意图；
- [0042] 图2是具有两个从设备集群、两个中间系统、中继设备以及第一主设备的无线网络的示意图；
- [0043] 图3是图2的另一实施例的示意图。

## 具体实施方式

- [0044] 本发明涉及用于使能无线设备之间的无线安全通信的方法。
- [0045] 第一无线设备能够创建与至少一个其它无线设备的连接，在这种情况下第一无线设备成为新连接的主设备，而所述其它的无线设备成为从设备。
- [0046] 在图1中，从设备在参考a1、a2至aN下被描绘。至少一个从设备可以包括像鼠标、键盘、电视机、DVD播放机、扬声器等这样的设备。根据本发明的一个实施例，所有这些从设备都可以优选地使用蓝牙协议的现有版本用于无线通信。从设备所使用的蓝牙配对协议对于必须执行配对的用户来说未必是方便的。
- [0047] 在图中的参考100下所描绘的第一设备可能是像移动电话、平板计算机、数字视频或静物相机、便携式音频设备等这样的设备（无论便携与否）中的一个。第一设备100包括第一主设备101，并且实施用于配对的安全无线通信协议。根据本发明的一个实施例，所述安全协议是蓝牙V2.1的“安全简单配对-带外”协议；以及它被实施在蓝牙主机101中。作为附加的特征，所述安全协议还可以包括NFC以用于配对。
- [0048] 根据本发明，中间系统10担任无线对接站的角色。无线对接站10可能是特定和专用的站，或者可以作为应用或软件而被合并在任何其它设备中，所述任何其它设备例如PC、接入点、媒体播放机、TV、PC监视器等。
- [0049] 对接站10包括第一无线电模块（未示出），例如具有单个发射机/接收机部分的基于软件无线电的系统。第一无线电模块包括第二主设备11（例如蓝牙主设备）以用于与在这个例子中为蓝牙从设备的从设备a1-aN配对。对接站10优选地支持所有已知的配对机制。例

如,对接站10的蓝牙主设备11优选地包括直到V4.0为止的所有蓝牙版本的现有配对协议以用于与对应从设备a1-aN配对。

[0050] 对接站10和从设备a1-aN形成针对第一设备100的对接环境。在这个环境中,对接站10使从设备a1-aN可用来以更安全和方便的方式连接到主设备。为了做到这个,在根据本发明的方法的预备步骤中,例如经由用户交互,从设备a1-aN与对接站10的第二主设备11进行配对,其针对每个从设备a1-aN使用适当的配对协议。在蓝牙配对的情况下,通过使用第二蓝牙主设备11,全部N个蓝牙从设备都使用每个设备支持的蓝牙配对协议与对接站10配对。

[0051] 在这个初始配对之后,在本发明的下一个步骤中,对接站10创建并配置在参考b1、b2至bN下所描绘的虚拟或中继从设备。这些设备能够使用安全协议被配对。它们具有不同的设备地址(‘BD\_ADDR’),可能具有不同的名称,并且使用不同的链路密钥,但否则看起来功能上与已经配对的第一设备a1-aN相同。在一个实施例中,对接站10的第一无线电模块可以不仅实施蓝牙主机11,而且实施中继设备b1-bN,使得中继设备b1-bN将消息传送到其它蓝牙主机(例如第一设备100的蓝牙主机)以及对其作出反应。这可以通过在第二蓝牙主机及其配对的从设备不使用的时隙中对第一蓝牙无线电模块和从端a1-aN的传送时间进行调度来完成。在另一实施例中,对接站10可以包括实施中继设备b1-bN的一个附加的蓝牙无线电模块,或一个以上的附加的蓝牙无线电模块。

[0052] 中继设备b1-bN具有名称,所述名称可以指对应从设备a1-aN的名称,并且其可以包括指示与对接站10的链路的附加信息。例如,如果从设备的名称是“家用键盘(Family Keyboard)”,则中继设备的名称可能是“家用键盘槽形对接站”。这些虚拟从设备b1-bN被配置成使用安全协议与第一设备100配对,所述安全协议例如上面所提到的蓝牙V2.1的安全简单配对-带外。这个协议有利地简化了用户交互,特别是在NFC被使用时。无线对接站10和第一设备100两者都支持安全配对协议。

[0053] 然后,对接站10发送信息以便通告对接环境中的中继从设备b1-bN。当第一设备100进入对接环境并碰巧能达到和正在侦听时,它从对接站10接收它可以配对到中继从设备b1-bN的信息(诸如存在、能力、连接细节等之类的连接信息)。此外,第一设备100可以接收这些中继从设备b1-bN是什么(例如家用键盘槽形对接站)以及它们支持的配对协议的描述。必须指出,并非所有的从设备a1-aN都可能需要被中继。对接站10可以识别是否需要经由虚拟设备复制的从设备a1-aN。例如,对接站10可以包括从设备的预定列表,对于所述从设备对接站10必须创建并配置对应的虚拟设备,并且必须通告对接环境中的所述虚拟设备。用于通告的信息的发送可以用不同的方式执行。根据一个实施例,它可以通过蓝牙在对接站10的蓝牙主机11、从设备a1-aN以及中继从设备b1-bN不需要传送任何消息时的时间上被执行。根据另一实施例,对接站10可以包括专用于虚拟设备通告的另一蓝牙无线电模块(未示出)。在另一实施例中,单独的通信信道可以被用于信息的传输。Wi-Fi、具有DNLA(用于数字生活网络联盟)的Wi-Fi或Wi-Fi Direct(Wi-Fi对等P2P)也可以被使用。

[0054] 附加地,为了帮助第一设备100与正确的中继从设备b1-bN配对,对接站10还可以发送消息通知存在于网络中的哪些从设备a1-aN应该被忽略以便直接地配对,因为对接站10提供了通过虚拟从设备b1-bN连接到它们的另一更安全而且方便的方式。

[0055] 然后,当用户想要在对接环境中使第一设备100配对时,他选择中继从设备b1-bN

中的全部或部分。第一设备100还可以选择或者建议选择对于其来说是方便的预定中继从设备。例如,预定设备可以被列举在第一设备100的存储器中。然后,第一设备100创建与对接站10已配置的所选虚拟从设备b1-bN的连接,例如在蓝牙简单安全配对协议的情况下为蓝牙连接。然后,通过例如将NFC使用于认证,用户可能仅必须使第一设备100和对接站10接触,以便提供与它接触所选虚拟从设备b1-bN中的每一个相同的效果。所以用户的动作是更简单的,因为他仅需要交互一次,而无论选择的虚拟从设备b1-bN的数目如何。第一设备100成为新连接的主机。

[0056] 在另一实施例中,对接站10可以选择第一设备100必须接触到其以便经由NFC执行认证的从设备并且将对应的信息发送到第一设备100的注意(attention)。

[0057] 在建立新连接之后,对接站10中继它配对的从设备a1-aN与它假装成的对应虚拟从设备b1-bN之间的所有通信,以便第一设备100正通过对接站10与作为对接环境的部分的蓝牙从设备a1-aN进行通信。

[0058] 一旦第一设备100的初始配对已完成,对接站10和第一设备100就可以在存储器中记录第一设备100的安全配对信息以允许自动地进一步配对。

[0059] 图2和3示出了其它实施例,其中对接环境可以包括至少两个从设备集群以及用于每个集群的一个中间系统。

[0060] 如上面所描述的那样,用户针对每个从设备a1-aN使用适当的配对协议将从设备a1-aN的第一集群与对接站10的第二主设备11配对。用户还针对每个从设备c1-cN使用适当的配对协议将从设备c1-cN的第二集群与对接站20的第三主设备22配对。

[0061] 在图2的实施例中,在这个初始配对之后,在下一个步骤中,每个对接站10、20创建并配置虚拟或中继从设备b1-bN、d1-dN。这些中继从设备能够使用安全协议被配对,但否则与已经配对的从设备相同。如上面所描述的相同过程适用。

[0062] 为了使能所有中继从设备b1-bN、d1-dN与第一设备100之间的方便配对,对接站10和20在它们之间配置通信信道30以用于交换中继从设备b1-bN、d1-dN的信息(诸如存在、能力、连接细节等之类的连接信息),并且对接站10将关于中继从设备b1-bN、d1-dN的信息(诸如存在、能力、连接细节等之类的连接信息)发送到第一主设备101。为了配置这样的通信信道,每个对接站10、20包括发射机/接收机无线电模块(未示出),其优选地适应于实施Wi-Fi通信。软件模块也在对接站10、20中被实施来控制发射机/接收机。可以使用其它通信信道,诸如例如有线通信信道。

[0063] 在图3的实施例中,对接站10和20也配置至少一个通信信道30,例如Wi-Fi或有线通信信道,以用于向对接站10提供从设备c1-cN的第二集群的数据,并且以用于一方面在对接站10与c1-cN之间中继消息,以及另一方面在对接站20与d1-dN之间中继消息。在从设备a1-aN、c1-cN的初始配对之后,对接站20发送所有必要的信息以使得对接站10能够配置对应于从设备a1-aN、c1-cN的所有中继从设备b1-bN、d1-dN。中继从设备b1-bN、d1-dN适应于使用如上面所描述的安全配对协议与第一主设备101配对。以及,然后对接站10将关于中继从设备b1-bN、d1-dN的连接信息发送到第一主设备101。

[0064] 图2和图3的实施例的优点是从设备的数目不限于中间系统10的容量。另外的优点是每个中间系统10、20都可以具有不同的专业化并且能够与适当的蓝牙设备配对。例如,一个中间系统可能是能够与蓝牙键盘和鼠标配对但不能与蓝牙耳机配对的显示器,然而另一

中间系统可能是能够被与蓝牙耳机配对但不能与鼠标或键盘配对的音频系统。

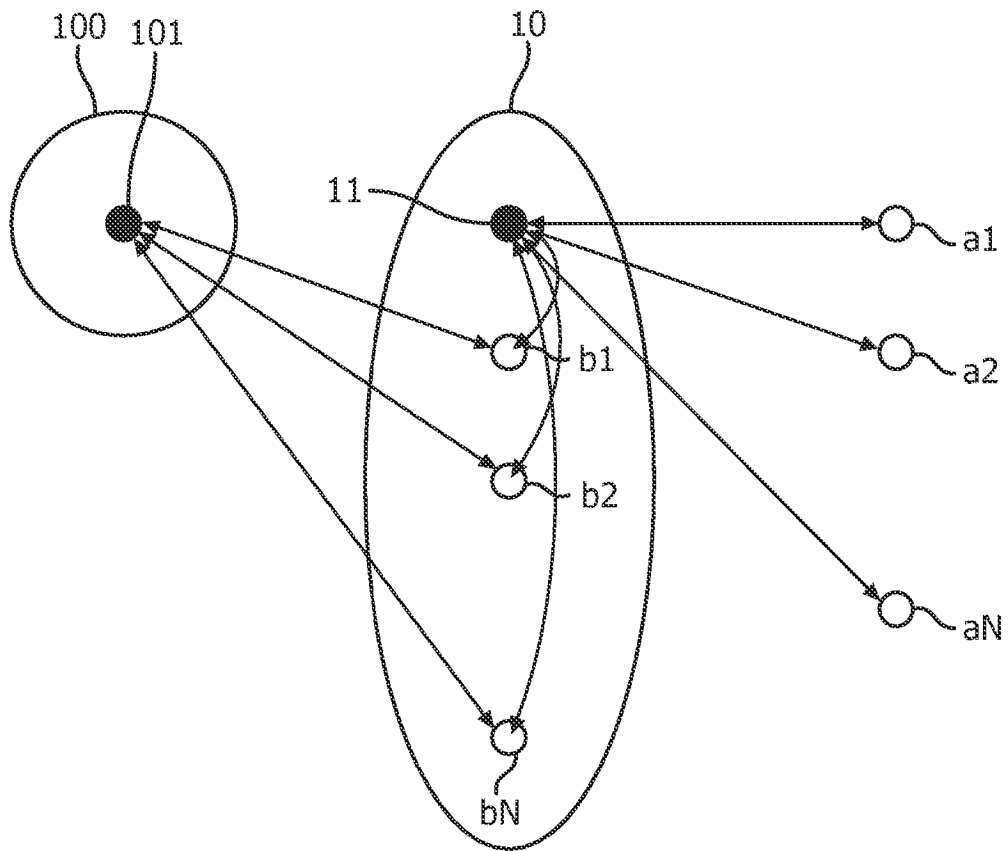


图 1

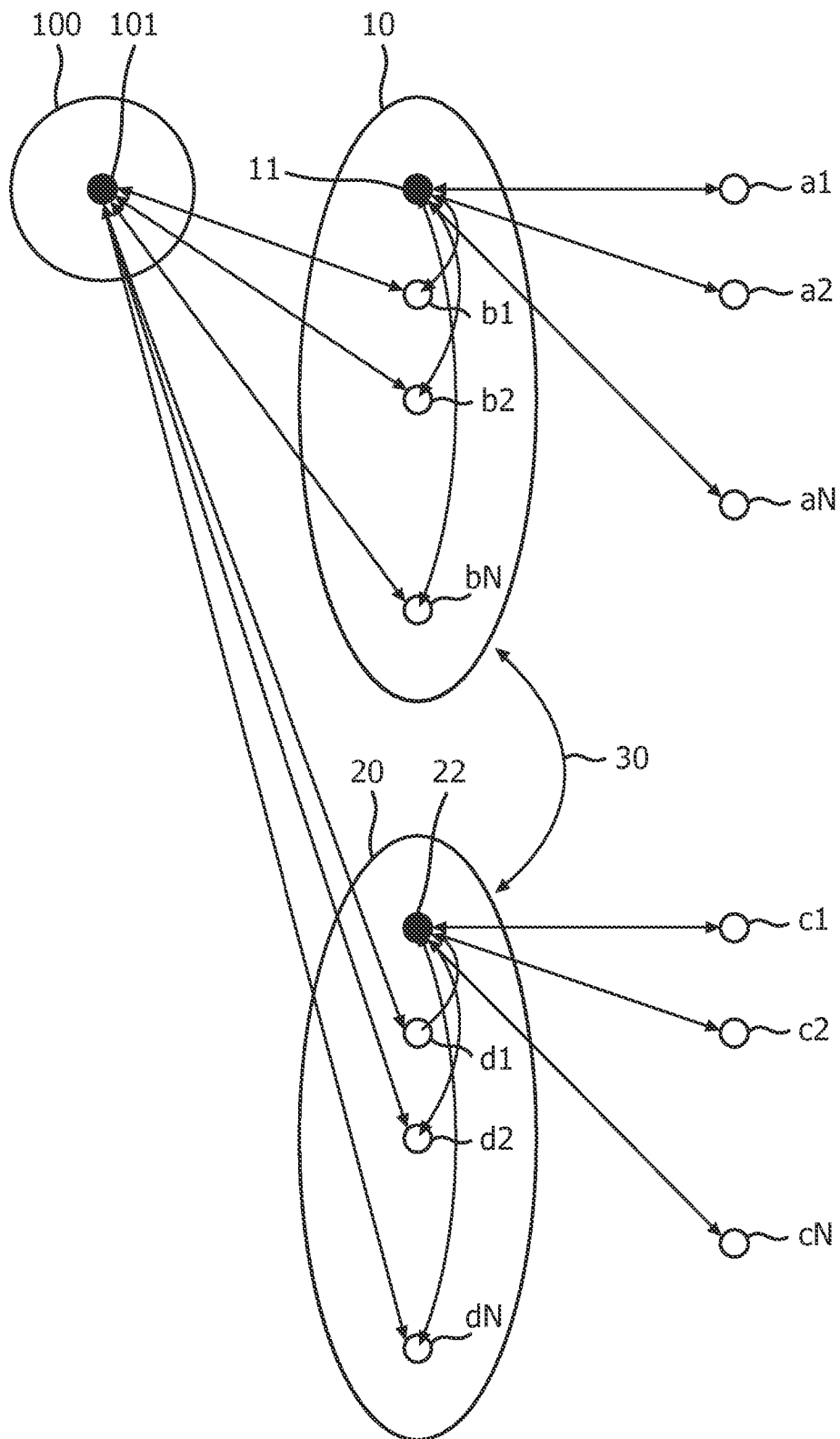


图 2

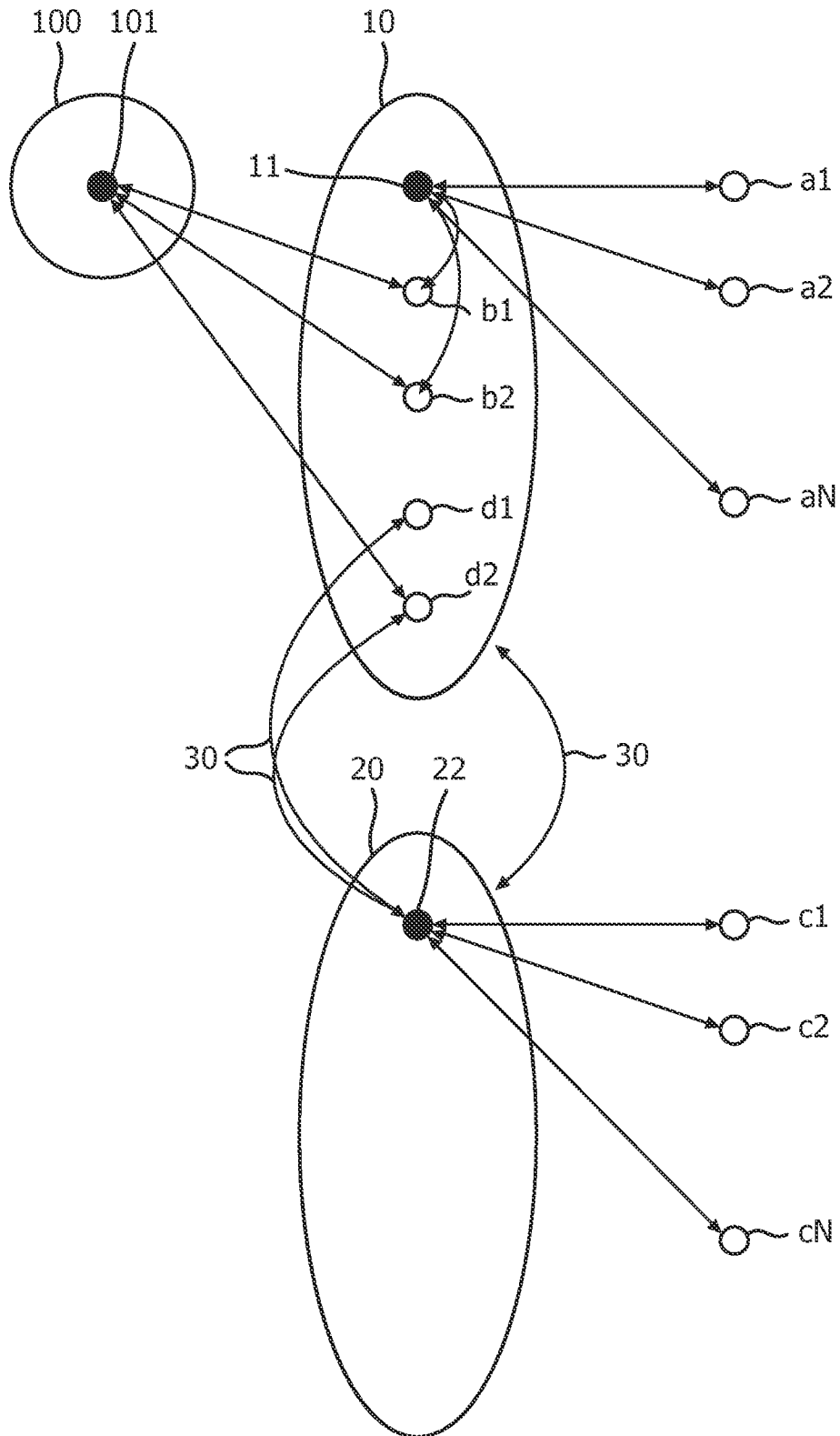


图 3