



(12)发明专利申请

(10)申请公布号 CN 105794244 A

(43)申请公布日 2016.07.20

(21)申请号 201480064919.5

(74)专利代理机构 上海专利商标事务所有限公
司 31100

(22)申请日 2014.12.22

代理人 黄嵩泉

(30)优先权数据

14/142,795 2013.12.28 US

(51)Int.Cl.

H04W 12/06(2006.01)

(85)PCT国际申请进入国家阶段日

H04W 88/02(2006.01)

2016.05.27

(86)PCT国际申请的申请数据

PCT/US2014/071817 2014.12.22

(87)PCT国际申请的公布数据

W02015/100210 EN 2015.07.02

(71)申请人 英特尔公司

地址 美国加利福尼亚州

(72)发明人 F·M·萨拉贝尔 S·S·沙哈

L·克里希纳默西 S·达杜

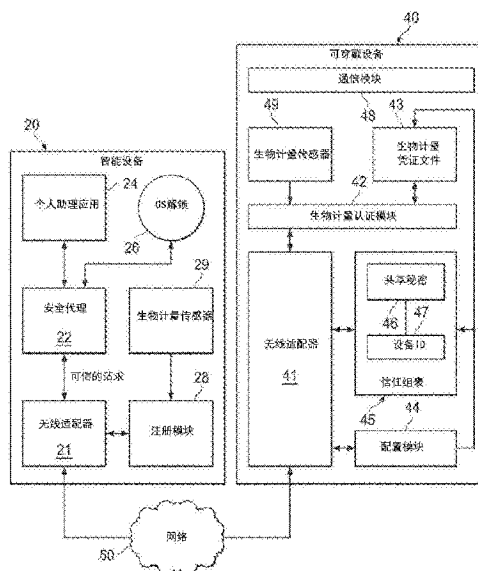
权利要求书3页 说明书23页 附图10页

(54)发明名称

跨智能设备的信任组扩展用户认证

(57)摘要

本文中描述的特定实施例提供具有生物计量传感器和逻辑的可穿戴电子设备。在硬件中实现所述逻辑的至少部分。所述逻辑配置成用于：接收指示生物计量输入的输入数据；以及至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据。所述逻辑配置成用于：建立到智能设备的无线连接；判定所述智能设备是否被包括在一个或多个智能设备的信任组中；以及当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时，发送用于解锁所述智能设备的通信。



1. 一种可穿戴电子设备,包括:
生物计量传感器;以及
逻辑,在硬件中实现所述逻辑的至少部分,所述逻辑配置成用于:
接收指示生物计量输入的输入数据;
至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;
建立到智能设备的无线连接;
判定所述智能设备是否被包括在一个或多个智能设备的信任组中;
以及
当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。
2. 如权利要求1所述的可穿戴电子设备,其中,所述逻辑配置成用于从所述智能设备和云中的一项接收所述经授权用户的所述至少一个生物计量凭证。
3. 如权利要求2所述的可穿戴电子设备,进一步包括:
一个或多个存储器元件,其中,所述逻辑配置成用于将所述至少一个生物计量凭证存储在所述一个或多个存储器元件中。
4. 如权利要求1所述的可穿戴电子设备,其中,所述逻辑配置成用于:当唯一地标识所述智能设备的信息被存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中。
5. 如权利要求4所述的可穿戴电子设备,其中,所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。
6. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述逻辑配置成用于:
接收指示其他生物计量输入的其他输入数据,其中,所述通信包括所述其他输入数据。
7. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述逻辑配置成用于:
当未成功地认证所述输入数据时,不发送用于解锁所述智能设备的所述通信。
8. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述逻辑进一步配置成用于:
将认证结果发送到所述智能设备,其中,所述认证结果指示是否成功地认证了所述输入数据。
9. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述生物计量传感器包括语音传感器,其中,所述逻辑配置成用于:基于验证所述输入数据中的语音触发以及验证由所述输入数据表示的语音对应于所述经授权用户的语音来认证所述输入数据。
10. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述生物计量传感器包括语音传感器、指纹传感器、眼部传感器和手部传感器中的一个。
11. 如权利要求1至5中的任一项所述的可穿戴电子设备,其中,所述逻辑配置成用于:
接收指示用于访问所述智能设备上的应用或服务用户输入的其他输入数据;以及
将所述其他输入数据发送到所述智能设备。
12. 如权利要求11所述的可穿戴电子设备,其中,所述用户输入的类型与所述生物计量输入的类型不同。
13. 至少一种计算机可读存储介质,包括用于可穿戴电子设备的指令,当由至少一个处

理器执行所述指令时,所述指令使所述至少一个处理器:

接收指示生物计量输入的输入数据;

至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;

建立到智能设备的无线连接;

判定所述智能设备是否被包括在一个或多个智能设备的信任组中;以及当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。

14. 如权利要求13所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

从所述智能设备和云中的一个接收所述经授权用户的所述至少一个生物计量凭证。

15. 如权利要求14所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

将所述至少一个生物计量凭证存储在一个或多个存储器元件中。

16. 如权利要求13所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

当唯一地标识所述智能设备的信息存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中。

17. 如权利要求16所述的至少一种计算机可读存储介质,其中,所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。

18. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

接收指示其他生物计量输入的其他输入数据,其中,所述通信包括所述其他输入数据。

19. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

当未成功地认证所述输入数据时,不发送用于解锁所述智能设备的所述通信。

20. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

将认证结果发送到所述智能设备,其中,所述认证结果指示是否成功地认证了所述输入数据。

21. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,所述生物计量传感器包括语音传感器,其中,当由所述至少一个处理器执行所述指令时,所述指令配置成用于:基于验证所述输入数据中的语音触发以及验证由所述所述输入数据表示的语音对应于所述经授权用户的语音来认证所述输入数据。

22. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,所述生物计量传感器包括语音传感器、指纹传感器、眼部传感器和手部传感器中的一个。

23. 如权利要求13至17中的任一项所述的至少一种计算机可读存储介质,其中,当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:

接收指示用于访问所述智能设备上的应用或服务的用户输入的其他输入数据;以及

将所述其他输入数据发送到所述智能设备。

24. 一种用于可穿戴电子设备的方法,包括以下步骤:

接收指示生物计量输入的输入数据;

至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;

建立到智能设备的无线连接;

判定所述智能设备是否被包括在一个或多个智能设备的信任组中;以及

当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。

25. 如权利要求24所述的方法,进一步包括以下步骤:

当唯一地标识所述智能设备的信息被存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中,其中,所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。

跨智能设备的信任组扩展用户认证

技术领域

[0001] 本文中描述的实施例总体上涉及电子设备上的用户认证,并且更具体地涉及跨智能设备的信任组扩展用户认证。

背景技术

[0002] 最终用户具有比之前更多的电子设备选择。许多突出的技术趋势当前正在进行中(例如,移动电子设备、更小的电子设备、增加的用户连接性,等等),并且这些趋势正在改变电子设备局面。这些技术趋势之一是通过多个电子设备的增强的用户移动性/连接性,有时将此称为个人生态系统。用户可以使用生态系统中的多个电子设备(例如,可穿戴电子设备、电话、膝上型计算机、平板等)而被“连接”(例如,流送音乐/视频,在网上冲浪,用消息联系朋友、阅读电子邮件,等等)。通常,用户不得不单独地登录生态系统中的多个电子设备中的每一个电子设备来使用这些设备,这会对用户增加不便性。因此,存在对改善用于登录生态系统中的多个电子设备的手段的需要。

附图说明

[0003] 在所附附图的图示中以示例方式而非限制方式示出实施例,在附图中,相同的参考指示类似的元件,并且在附图中:

[0004] 图1是示出根据本公开的实施例的、与在信任组中跨智能设备扩展用户认证相关联的组件的简化框图;

[0005] 图2是示出根据本公开的实施例的示例信任组的简化框图;

[0006] 图3A是示出根据本公开的实施例的示例无线头戴式耳机的简化正视图;

[0007] 图3B是示出根据本公开的实施例的示例无线头戴式耳机正由用户穿戴的简化正视图;

[0008] 图4是示出根据本公开的实施例的与扩展用户认证相关联的活动的简化流程图;

[0009] 图5是示出根据本公开的实施例的与扩展用户认证相关联的活动的简化流程图;

[0010] 图6是示出根据本公开的实施例的与扩展用户认证相关联的活动的简化流程图;

[0011] 图7是示出与本公开的实施例相关联的活动的简化流程图;

[0012] 图8是示出与本公开的实施例相关联的活动的简化流程图;

[0013] 图9是示出与本公开的实施例相关联的活动的简化流程图;

[0014] 图10是与本公开的示例片上生态系统(SOC)相关联的简化框图;以及

[0015] 图11是可以用于执行与本公开相关联的活动的示例逻辑的简化框图。

[0016] 附图的图示不一定是按比例绘制的,因为可以显著地改变它们的尺度而不背离本公开的范围。

具体实施方式

[0017] 以下具体实施方式陈述与跨智能设备的信任组来扩展用户认证有关的装置、方法

和系统的实施例。为了方便起见,可参照一个实施例来描述特征(诸如例如,(多个)结构、(多个)功能和/或(多个)特性);然而,可以用所描述的特征中的任何一个或多个合适的特征来实现各实施例。

[0018] 图1是示出与在信任组中跨智能设备扩展用户认证相关联的示例组件的简化框图。可穿戴设备40经由安全网络50以及相应的无线适配器41和21来与智能设备20通信。可穿戴设备40可以包括用于执行与在信任组中扩展用户认证相关联的操作的生物计量认证模块42、通信模块48以及配置模块44。可穿戴设备40还可以存储(或通过网络访问)包括可穿戴设备40和智能设备20的经授权用户的至少一个生物计量凭证的生物计量凭证文件43。信任组表45也存储在可穿戴设备40中(或可由可穿戴设备40通过网络访问),并且包括唯一地标识信任组中的智能设备(可能包括其他可穿戴设备)的信息。在一个特定示例中,此信息可以包括对应于智能设备20相对应的设备标识符(“设备ID”)到与可穿戴设备40与智能设备20之间的无线连接相关联的共享秘密的映射。信任组表45可以包括专用于信任组中的每一个智能设备的类似映射。

[0019] 智能设备20可以包括用于执行与跨智能设备的信任组来扩展用户认证相关联的操作的注册模块28和安全代理(proxy)22。当对用户的认证从可穿戴设备40扩展到智能设备20时,由安全代理22启用操作系统(OS)解锁26。个人助理应用24是当将对用户的认证从可穿戴设备40扩展到智能设备20时可以由此用户经由可穿戴设备40访问的应用的示例。

[0020] 为了示出其中跨信任组中的智能设备扩展用户认证的系统的某些示例特征,理解可以横越网络环境的通信以及其中设备可能尤其有益的场景是重要的。以下基础信息可以视为可以从中适当地解释本公开的基础。

[0021] 个人生态系统是新兴的趋势,在此趋势中,多个单独的智能电子设备互连以便成为设备的所有者(或用户)提供各种服务的设备的个人网络。智能电子设备(本文中也称为“智能设备”)是能够经由各种协议与其他设备和/或网络进行语音、音频、媒体或数据交换的电子设备、组件、元件或对象。智能设备的示例可以包括但不限于,移动电子设备、可穿戴电子设备、智能电器、嵌入式控制器、汽车资讯娱乐系统、导航系统、某些台式计算机和膝上型计算机,等等。移动电子设备旨在包括智能移动电话(智能电话)、平板、平板手机、膝上型计算机、超极本、个人数字助理(PDA)、便携式导航系统、多媒体小配件(例如,相机、视频和/或音频播放器等)、游戏系统、其他手持式电子设备,等等。可穿戴电子设备(在本文中也称为“可穿戴设备”)旨在包括能够在无线网络环境中进行语音、音频、媒体或数据交换并且可以由用户(例如,通过附连至用户的身体部位或衣服(例如,手镯、头戴式耳机、手表、眼镜、具有夹具的设备,等等))穿戴的任何智能设备。

[0022] 许多用户已累积了多个智能设备。如果在用户拥有的智能设备中的任一个中配置认证,则通常此用户单独地登录到这些设备中的每一个设备以访问由特定设备提供的信息或服务。随着可穿戴电子设备激增,用户可能也累积了多个可穿戴电子设备。对每一个可穿戴设备的单独的认证要求可能增加用户管理多个设备上的多个认证的负担。随着电子设备的用户高速缓存继续增加时,这可能变得尤其累赘。

[0023] 人们也已经变得日益依附于他们的移动电子设备(在本文中也称为“移动设备”)。可以看到人们在他们生活的各个方面(包括业务、社交和个人时间)携带他们的移动电话(和其他移动设别)并与其交互。访问生态系统内的多个移动设备和其他智能设备可能是麻

烦且不方便的,当由于专用于特定设备的认证要求而要求多个认证时尤其如此。对于改善用户更容易地访问他们的生态系统内的多个智能设备的能力具有期望。

[0024] 一些可穿戴电子设备设计成用于与用户的智能设备中的一个或多个进行通信(例如,与其配对),以用于某些用途。例如,能以无线通信能力(诸如,蓝牙™)来配置头戴式耳机可以配置有无线通信能力,这允许头戴式耳机与移动设备或其他智能电子设备之间的音频通信。然而,一般而言,此类头戴式耳机将所有音频传送到移动设备以进行处理,但是不在头戴式耳机上执行任何用户/说话者认证。因此,此类可穿戴设备不能减轻用户在多个设备上进行多个认证的负担。

[0025] 如本文中所示和所述的可穿戴电子设备克服了这些问题中的许多问题,并且为期望对多个智能电子设备进行安全、方便访问的用户提供解决方案。本文中描述的特定实施例提供了具有生物计量认证能力的可穿戴电子设备(例如,头戴式耳机、电子手表或手镯、电子眼镜,等等)。可穿戴设备的用户在主智能设备(诸如,智能电话)上注册他的生物计量特性(例如,语音、指纹、眼睛、面部特征、手部特征、脉搏,等等),以便启用对特定特性的生物计量认证。对于语音通信,可穿戴设备的用户还可以注册用户定义的语音触发,此语音触发是除语音本身之外还可经认证的特定的单词或短语。注册模块可以基于来自用户的生物计量输入而在智能设备上生成至少一个用户特定的生物计量凭证。用户特定的生物计量凭证可以通过安全无线或有线连接被传送到可穿戴设备,并且被存储在可穿戴电子设备的存储器元件中。此外,标识主智能设备的信息由可穿戴设备存储以指示主智能设备是可穿戴设备的信任组的部分。此标识信息可以包括例如,智能设备的标识符以及同可穿戴设备与智能设备之间的安全无线连接相关联的安全信息。

[0026] 当用户基于用户特定的生物计量凭证向可穿戴设备认证时,可穿戴设备建立到信任组中的、当前通过安全无线连接可访问的智能设备的安全无线连接。为了易于引用,以下描述可以引用基于多个生物计量凭证对用户的认证。然而,将理解的是,可穿戴设备可以配置成用于允许用户基于单个生物计量凭证或多个生物计量凭证来进行认证。此外,可穿戴设备的一些实施例可以配置成用于接受其他类型的认证凭证(例如,密码、通行码,等等)。当已经提供了适当的生物计量凭证时,所访问的智能设备可以解锁其操作系统,以便允许用户例如经由语音命令通过可穿戴设备而到在智能设备上运行的个人助理(PA)应用来与智能设备交互。PA应用可以具有对智能设备上的安全应用和数据的访问权,并且因此将对此类应用和数据的访问权提供给用户,而无需用户物理地操纵或以其他方式处置智能设备。因此,可穿戴电子设备可以提供对用户的生物计量认证,以便允许与用户的智能设备的信任组内的其他电子设备的交互和/或对用户的智能设备的信任组内的其他电子设备的控制。

[0027] 再次转向图1,图1示出用于促进系统将用户认证从可穿戴电子设备扩展到信任组中的智能设备的网络环境。在讨论与图1的架构相关联的潜在流程之前,提供有关可能与图1中示出的网络环境和组件关联的可能组件和基础设施中的一些的讨论。

[0028] 在一个或多个实施例中,能以无限适配器41和42供应可穿戴电子设备40和智能设备20。无线适配器可以包括无线通信电路(例如,Wi-Fi模块、蓝牙™模块、近场通信(NFC)模块或其他无线通信电路)以允许可穿戴电子设备40和智能设备20彼此通信,以及潜在地通过无线连接而与其他电子设备或网络进行通信。无线通信可以包括无线技术(例如,2012年

3月29日发布的电子与电气工程师协会(IEEE)标准802.11™-2012、2012年8月17日发布的IEEE标准802.16™-2012、WiFi、WiMax、专用短距离通信(DSRC)等)、卫星、蜂窝技术(例如,3G/4G/5G/nG,等等)、其他射频(例如,近场通信(NFC)、射频识别(RFID)等)和/或促进网络环境中的无线通信的任何其他联网协议。在实施例中,可结合可穿戴电子设备40和/或智能设备20来供应多个天线,所述多个天线可以与无线连接活动相关联。在特定实施例中,可穿戴设备10能以低功率“总是收听”模式操作以促进与其他电子设备之间的无线通信。

[0029] 在至少一个实施例中,经由网络50的无线连接可以是安全无限个域网(WPAN)(例如,蓝牙™、不可见红外光、Wi-Fi、WiDi,等等),此安全WPAN用于将可穿戴设备40互连到相对小的区域内的安全网络50、智能设备20以及可能的其他电子设备。在另一实施例中,无线连接可以是安全无限局域网(WLAN),此安全WLAN使用无线分布方法(通常通过对因特网访问的接入点来提供连接)、在相对短的距离上将可穿戴设备40链接到安全网络50、智能设备20以及可能的其他电子设备。扩展频谱或OFDM技术的使用可以允许可穿戴设备在局域覆盖范围内到处移动但仍保持连接到网络50、智能设备20以及可能的其他电子设备。在一些实施例中,无线连接还可以包括任何蜂窝无线(例如3G/4G/5G/nG、LTE,等等)、卫星或到网络50的其他类似连接。在特定实施例中,网络50表示可穿戴设备40与智能设备20之间的蓝牙™安全无线连接。

[0030] 在至少一些实施例(诸如,基于云的实施例)中,网络50可以包括用于接收和传输通过网络50传播的信息分组的经互连的通信路径的一系列点或节点。网络50可以提供通信接口,并且可以是任何局域网(LAN)、无线局域网(WLAN)、城域网(MAN)、内联网、外联网、WAN(例如,因特网)、虚拟私有网(VPN)或促进网络环境中的通信的任何其他适当的架构或系统。网络50可以包括有线技术(例如,以太网、T1线等)以及本文中先前讨论的任何无线技术。网络50可以包括通过通信介质而耦合到彼此(并且彼此通信)的任何数量的硬件或软件元件。

[0031] 网络50的此类配置可以特别适合于系统的基于云的实施例,在此基于云的实施例中,注册过程包括:将用户特定的生物计量凭证推送至云。随后,以生物计量认证能力和安全无线能力供应的任何可穿戴设备或其他电子设备可与云中的信息同步。此类信息可以包括但不一定限于:生物计量凭证;以及可能的标识与可穿戴设备40形成信任组的智能设备的信息。

[0032] 云旨在是指可由电子设备(诸如,可穿戴设备40和智能设备20)通过WAN(诸如,因特网)或其他合适的网络远程地访问的服务(例如,计算服务、存储服务)。云可以包括能够主管云的服务并且能够将智能设备20和可穿戴设备40链接到那些服务的任何一个或多个网络元件。如本文中所使用,术语“网络元件”旨在涵盖服务器、路由器、交换机、网关、桥、负载均衡器、防火墙、内联服务节点、代理、处理器、模块或可操作以便在网络环境中交换信息的任何其他合适的设备、组件、元件、专有电器或对象。此网络元件可以包促进成其操作的任何合适的硬件、软件、组件、模块、接口或对象。这可以包括允许对数据或信息的有效交换的适当的算法和通信协议。

[0033] 在用于跨智能设备来扩展认证的系统的至少一个实施例中,智能设备20可以是主设备或副设备。主设备可以由用户用于注册此用户的生物计量凭证,以便与可穿戴设备40形成信任组,并且允许由可穿戴设备40对用户的认证。由用户注册的生物计量凭证的类型

取决于在智能设备20中供应的生物计量认证能力的类型(例如,生物计量传感器以及相关电路和逻辑的类型)。当以与在可穿戴设备40中供应的生物计量认证能力相同类型的生物计量认证能力来供应时,智能设备可以充当主设备。例如,如果可穿戴设备40是头戴式耳机且具有语音认证能力,则如果智能设备20也具有语音认证能力,它就可以是主设备。在另一示例中,如果可穿戴设备40是可穿戴手腕(例如,手镯、手表等)且具有指纹认证能力,则如果智能设备20也具有指纹认证能力,它就可以是主设备。

[0034] 现在将描述当智能设备20充当主设备时此智能设备20及其组件和功能。智能设备20和可穿戴设备40包括用于感测人类用户的特定生物特性的相应的生物计量传感器40和29。如本文中所使用,‘感测’旨在意味着检测、扫描、测量和/或识别所感测的特定生物特性。生物计量技术可以用于感测并分析人体特性,诸如但不限于,语音模式、话语、指纹、视网膜和/或虹膜、面部特征、手部特征、掌纹和脉搏特征。生物计量传感器(诸如,49和29)可以配置成用于感测用户的特定生物计量特性。例如,指纹传感器可以用于感测指纹,话筒可以用于感测语音(用于语音标识和话语识别两者),眼部传感器可以用于感测视网膜和/或虹膜,面部传感器可以用于感测面部特征,手部传感器可以用于感测手部测量/几何结构和/或掌纹,并且脉搏传感器可以用于感测脉搏特征。

[0035] 在智能设备20中,注册模块28结合生物计量传感器29一起使得用户能够生成一个或多个生物计量凭证且能够向可穿戴设备40注册其生物计量特性以形成信任组。注册模块28可以配置成用于接收并处理生物计量输入数据,此生物计量输入数据指示由生物计量传感器29感测到的用户生物计量输入。用户生物计量输入是由用户提供的、由生物计量传感器29感测的生物计量特性(例如,语音、指纹、眼睛、手部、脉搏,等等)。注册模块28可以生成生物计量凭证文件,此生物计量凭证文件可以被推送到可穿戴设备40或基于云的实现方式中的云。

[0036] 安全代理22可以配置为智能设备20的操作系统的部分,或者可以被单独地安装。在至少一个实施例中,安全代理22控制当可穿戴设备40尝试将对用户的认证扩展到智能设备时是否解锁智能设备20的操作系统。当除非提供适当的认证凭证(例如,生物计量凭证、密码、通行码、个人标识号(PIN),等等),否则用户无法访问智能设备的任何应用、数据和/或其他能力时,本文中将智能设备(或智能设备的操作系统)称为“被锁定”,。在至少一个实施例中,安全代理22可以配置成用于允许在可穿戴设备40和/或智能设备20和/或安全代理22(或任何其他组件)之间执行任何合适的授权、认证等(即,“解锁”)。这可以包括任何类型的解锁、释放、暴露、开放、启用或以其他方式授权对可穿戴设备40和/或智能设备20的一个或多个功能的访问。

[0037] 智能设备20还可以配置成用于经由触摸屏、键盘或任何其他合适的输入设备来从用户接收适当的认证凭证。这些认证凭证可以与可穿戴设备40用于认证用户的认证凭证相同或不同。或者,智能设备20可以配置为使得它不要求用于用户经由触摸屏、键盘或任何其他合适的输入设备来访问其应用、数据和/或其他能力的认证凭证。然而,在此场景中,可穿戴设备40仍可认证用户以使得此用户能够经由可穿戴设备40来访问智能设备20。此外,当智能设备20的操作系统被锁定时(例如,由于还未提供适当的认证凭证,由于因不活动已经自动地锁定操作系统,等等),取决于其特定配置,智能设备仍可使其其他应用运行和/或可以与其他设备和/或网络通信(例如,接收文本消息、接收电子邮件、接收电话呼叫,等等)。

[0038] 安全代理22可以配置成:当从可穿戴设备40接收到可信任请求时,如由OS解锁26所指示来解锁智能设备20的操作系统。在至少一个实施例中,可穿戴设备40仅在已经成功地认证用户之后才将来自此用户的可信任请求发送到智能设备20。因此,除非请求基于由可穿戴设备对用户的成功的生物计量认证是可信任的,否则安全代理22不接收来自可穿戴设备40的任何请求或其他通信。安全代理22可以配置成用于理解在智能设备20与可穿戴设备40之间使用的这个认证协议。因此,在本实施例中,安全代理22可以将来自可穿戴设备40接收到的任何请求接受为可信任的请求,并且可以在每当接收到请求时就解锁操作系统。

[0039] 请求是从另一设备接收到的通信。请求可以是来自可穿戴设备40发送到智能设备20的命令(例如,用于允许语音识别的命令)或从可穿戴设备40上的用户输入中产生的、能够与智能设备20的应用或服务交互的输入数据。可以从在对用户的认证时使用的相同类型的生物计量输入(例如,语音)中产生请求。或者,对用户的认证可以基于一种类型的生物计量输入,而由用户作出的访问智能设备20的请求可以基于另一类型的输入。例如,可穿戴电子手表可以具有允许对用户的语音认证的语音认证能力。如果手表还具有触摸屏显示器,则在认证了用户之后,此手表可以允许来自用户的触摸输入与此手表连接到的智能设备通信。

[0040] 在至少一个实施例中,安全代理22可以配置成:在验证了接收到的请求由可穿戴设备40而不是某个其他设备发送之后,解锁智能设备20的操作系统。在本实施例中,当通过接收到来自另一设备的请求而苏醒之后,安全代理22可以将标识此请求的发送设备的查询发送到操作系统。如果此请求由可穿戴设备40发送,则安全代理22可以解锁操作系统。否则,安全代理22可以保持操作系统被锁定。在蓝牙用于将智能设备20与可穿戴设备40链接并且用户将访问个人助理应用24的语音请求发布至可穿戴设备40的一个实施例中,安全代理22可以查询操作系统,以便在接收到允许智能电话上的语音识别的特定AT命令(例如,AT+BVRA=1)时确定发送设备的身份。基于无线连接的链接密钥和发送设备的设备标识符,安全代理22可以判定此AT命令是否是从可穿戴设备40接收到的。

[0041] 一旦由安全代理22解锁了操作系统,则如果以个人助理应用24供应了智能设备20,个人助理应用24就可通过安全无线连接接收来自可穿戴设备40的语音请求并响应于此语音请求。个人助理应用是可以基于用户输入以及由此个人助理应用获取的其他信息(例如,GPS位置、来自在线源的信息,诸如,天气、交通、新闻、股价、用户安排、零售价格,等等)来为用户执行任务或服务的智能软件代理设备(agent)的示例。个人助理应用在移动电话、平板和其他智能设备上正变得越来越常见。个人助理应用经常配置成用于响应于来自用户的语音请求(例如,命令、指令等)。相应地,能以用于接收直接从用户到个人助理应用24的语音请求的语音传感器(例如,生物计量传感器29或另一传感器)以及相关电路和逻辑。然而,一旦在可穿戴设备40与智能设备20之间建立安全无线连接,并且由安全代理22解锁了操作系统,则个人助理应用24可以响应于经由可穿戴设备40、来自用户的语音请求。

[0042] 在其他实施例中,智能设备上除个人助理应用之外的应用可以接收并响应于来自可穿戴设备的可信任的请求。在一些实例中,这些其他应用可以响应于来自用户的触摸输入或其他类型的输入而不是语音输入。例如,可穿戴设备40可以具有触摸屏显示器,并且一旦用户在可穿戴设备40上经由用户的生物计量凭证(例如,语音、指纹、眼睛、手部、脉搏,等等)经认证,随后,此用户可提供适当的触摸输入以便与智能设备上的应用交互。

[0043] 在一些实施例中,由可穿戴设备40发送到安全代理22的通信包括认证结果,此认证结果指示来自用户的生物计量输入数据成功地经认证(通过)还是没有成功地经认证(失败)。在至少一个实施例中,安全代理22可以通过基于认证结果实现各种安全等级来允许对应用和服务的选择性访问。为了实现多个安全等级,安全代理22可以基于认证结果来确定哪些应用/服务允许用户访问和/或哪些应用/服务阻止用户访问。例如,当认证结果指示“通过”(即,用户成功地向可穿戴设备认证)时,安全代理22可以配置成用于允许对由用户请求的任何应用或服务的无限制访问。当认证结果指示“失败”(即,用户未成功地向可穿戴设备认证)时,则智能设备20可以配置成用于允许用户访问不涉及机密或个人信息的公共服务或应用。此类公共服务或应用的示例潜在地可以是天气查询、股价更新、信息互联网查询,等等。

[0044] 副智能设备是加入已经由可穿戴设备40和主智能设备形成的信任组的智能设备。副智能设备可以具有与主智能设备(诸如,智能设备20)的相同的组件中的至少一些。例如,副智能设备包括无线适配器、安全代理和注册模块。副智能设备可以或不包括生物计量传感器。生物计量传感器对于副智能设备加入信任组不是必需的,因为信任组的存在指示了用户已经注册了此用户的生物计量特性且已经经由主智能设备将生物计量凭证提供给可穿戴设备。如果副智能设备包括个人助理应用,则如果可穿戴设备是语音使能的以便从用户接收语音请求,此用户就可以与副智能设备交互。副智能设备还包括注册模块,但是它可以与主智能设备上的注册模块略微不同地运作。当用户希望将副智能设备添加到可穿戴设备的信任组时,可以启动副智能设备上的注册模块。注册模块建立到可穿戴设备的无线连接,并且发送查询以便判定此注册模块是否已经是信任组的部分以及可穿戴设备提供了什么类型的能力。如果副智能设备还不是信任组的部分,并且如果可穿戴设备的能力指示它可以通过无线连接来扩展认证,则副智能设备可以将加入信任组的请求发送到可穿戴设备。

[0045] 在可穿戴设备40中,生物计量凭证文件43可以包括由主智能设备(例如,智能设备20)推送到可穿戴设备40的生物计量凭证。生物计量凭证包括生物计量信息,此生物计量信息指示当用户在系统中注册时由主智能设备捕捉的、来自此用户的生物计量输入。生物计量信息可以包括表示特定生物计量特性的用户特定属性的数据。一般而言,每个用户具有针对用于认证的特定类型的生物计量特性的唯一生物计量信息(例如,唯一的语音模式、唯一的指纹、唯一的眼部测量、唯一的手部特征、唯一的脉搏特征,等等)。随后,可将用户特定的生物计量凭证与指示由可穿戴设备40捕捉到的生物计量输入的接收到的生物计量输入数据进行比较。在一些实施例中,可由主智能设备将生物计量凭证可以推送到云,随后由可穿戴设备40检索生物计量凭证供本地存储,或者在每当捕捉到生物计量输入时由可穿戴设备40检索生物计量凭证。

[0046] 在可穿戴设备40中,生物计量传感器49结合生物计量认证模块42和生物计量凭证文件43一起使用户能够提供生物计量输入(例如,语音输入、指纹输入、眼部输入、手部输入、脉搏输入,等等)并且能够经认证且被允许访问信任组中的其他智能设备。生物计量输入可以转换为另一形式(例如,模拟信号被转换为数字信号)以产生生物计量输入数据,可以由生物计量认证模块42处理此生物计量输入数据。一般而言,生物计量认证模块42可以尝试通过将生物计量输入数据与生物计量凭证文件43中的生物计量凭证进行比较来认证

此生物计量输入数据。如果生物计量输入数据对应于生物计量凭证,则生物计量输入数据(以及用户)成功地经认证。如果生物计量输入数据不对应于生物计量凭证,则生物计量输入数据(以及用户)未成功地经认证。

[0047] 在以用于语音认证的语音传感器配置的实施例中,生物计量认证模块28可以提供语音识别操作和言语识别操作两者。例如,语音识别凭证可以用于验证说话者实际上是经授权的用户,而言语识别凭证可以用于验证说话者的单词包括预期的语音触发(即,指示通过可穿戴设备来访问另一设备的命令的特定单词或短语)。在本实施例中,除非经授权用户提供了此特定的语音触发,否则经授权的用户无法经认证以将认证扩展到其他设备。作为说明,语音触发可以是“你好,智能设备”。如果用户成功地经认证,则生物计量认证模块42可以提供允许在智能设备20上进行语音识别的适当的命令(例如,针对蓝牙,AT+BVRA=1)。

[0048] 可以在可穿戴设备40中提供信任组表45,以便存储唯一地标识与可穿戴设备40相关联的信任组中的智能设备的信息。在一个示例中,信任组表45可以包括信任组中的每一个智能设备的设备标识符(“设备ID”)。唯一地标识智能设备的任何信息可以用作设备ID,或者可以被映射到设备ID,或者能以任何其他可能的方式配置以将信任组中的智能设备彼此区分。在一个可能的实现方式中,设备ID可以是至另一表的索引,所述另一表包含唯一地标识信任组中的每一个智能设备的信息。在一个可能的实现方式中,每一个设备ID可以被映射到与可穿戴设备40与对应于那个设备ID的智能设备之间的安全无线连接相关联的不同的共享秘密(或其他连接特定的安全信息)。例如,特定的共享秘密可以用于保护可穿戴设备40与智能设备之间的无线连接的安全,这对应于映射到特定共享秘密的设备ID。特定的共享秘密可以用于加密通过可穿戴设备40与智能设备20之间的无线连接而发送的通信。当蓝牙用于在信任组中的可穿戴设备40与智能设备之间建立无线连接时,共享秘密通常被称为“链接密钥”。将显而易见的是,可以使用其他类型的唯一标识信息(例如,介质访问控制(MAC)等)而不是共享秘密或链接密钥。对这些其他类型的唯一标识信息的使用以及以唯一标识信息实现信任组表的特定方式可以基于可穿戴设备10的特定需要和实现准则。

[0049] 在至少一些实施例中,可以使用任何合适的映射、标记或链接技术(例如,列表、表、关联数组、指针、索引、图表、链表、文件名、关系型数据库、散列表等)或表示设备ID与安全信息之间的关系、连接或链接的任何其他技术或机制来将设备ID映射到信任组中的智能设备的无线连接安全信息(例如,共享秘密、链接密钥,等等)或其他唯一标识信息。例如,如先前所述,通常用于组织电子信息的数据结构的简单表配置或索引表配置是实现信任组表45的一种可能的方式。然而,将认识到能以各种其他方式对信任组表45进行建模,并且这些其他配置可以基于给定实现方式的特定偏好和需要。

[0050] 可以在可穿戴设备40中提供配置模块44以配置注册数据(生物计量凭证),诸如,用于语音使能认证的语音数据或用于指纹使能认证的指纹数据。可以从智能设备20或在基于云的实施例中从云接收这些生物计量凭证。配置模块44还可以设置信任组中的可穿戴设备40与其他智能设备(诸如,智能设备20)之间的信任关系。例如,配置模块44可以在信任组表45中提供设备标识符到共享秘密的映射。配置模块44还可以打开可穿戴设备40的生物计量认证,并且将可穿戴设备40配置成如果生物计量认证不成功则苏醒(或不苏醒)。配置相关的动作可以基于在主智能设备上(例如,经由注册模块28)提供的且被推送到可穿戴设备40的用户输入。可穿戴设备40还可以包括用于控制与注册模块28之间的专有通信的通信模

块48。

[0051] 图2是示出信任组10的示例的简化框图。信任组10最初可由主可穿戴设备60和主智能设备70形成。随后,可以(或不)将其他智能设备和/或可穿戴设备添加到信任组10。为了说明性目的,以具有多个副智能设备72(1)-72(N)和副智能设备73示出信任组。然而,一旦由两个主设备形成了信任组,任何数量的副智能设备和/或任何数量的副可穿戴设备就可以被添加到这个组。

[0052] 为了形成信任组10,在主智能设备70上注册用户的生物计量凭证,并且将此生物计量凭证安全地传送到主可穿戴设备60。此外,多个设备必须能够在它们之间建立安全无线连接61。如果可以建立安全无线连接,则标识主智能设备70的信息可以由主可穿戴设备60存储以指示主智能设备70是信任组10的部分。此信息可以包括例如主智能设备70的标识符以及与安全无线连接61相关联的安全信息。

[0053] 在至少一个实施例中,可以使用蓝牙、以安全的方式来建立无线连接61,蓝牙是用于电子设备的短距离射频频带无线互连的无线技术标准。此标准由蓝牙®特殊兴趣小组管理,此小组采用蓝牙规范版本4.0(2010年6月)以及后续附录。

[0054] 使用蓝牙,可以通过首先“配对”两个电子设备来建立安全无线连接。在配对过程中,经配对的第一和第二设备通过创建也被称为“链接密钥”的共享秘密来建立关系。当由这两个设备存储链接密钥时,可将这两个设备称为是“经配对”或“经绑定”。可以通过由第一设备通过以加密方式认证第二设备的身份以确保此第二设备是第一设备最初配对到的正确设备来建立到此第二设备的安全无线连接(或反之亦然)。此外,可以使用链接密钥来加密这些设备之间的通信,从而防止窃取或滥用在这些设备之间交换的数据。

[0055] 用户可以经由安全无线连接61或经由到主可穿戴设备60的任何其他安全连接来将他的生物计量凭证从主智能设备70传送到主可穿戴设备60。一般而言,用户可以将他的生物计量凭证传送到与用户的生物计量凭证相同的生物计量特性(例如,语音、指纹、眼睛、手部、脉搏等等)的生物计量标识能力启用的任何其他电子设备。可以经由安全无线连接(例如,蓝牙)或其他安全无线或有线信道来实现此传送。在至少一个实施例中,生物计量凭证文件可以是基于云的。在本实施例中,生物计量凭证被传送到云,随后被传送到主可穿戴设备60,并且可能传送到以相同的生物计量标识能力启用的其他电子设备。因此,主智能设备(和副智能设备)被包括在多个信任组中是可能的。

[0056] 主可穿戴设备60可以通过在主智能设备60与每一个副智能设备72(1)、72(2)至72(N)之间建立分开且安全的无线连接来将副智能设备72(1)-72(N)添加到信任组10中。在至少一个实施例中,蓝牙可以用于安全地将每一个副智能设备72(1)-72(N)分别配对到主可穿戴设备。可以使用在配对过程期间生成的安全协议(例如,链接密钥)来建立安全无线连接62(1)、62(2)至62(N)。当可以建立安全无线连接62(1)-62(N)时,则标识副智能设备72(1)-72(N)的信息可以由主可穿戴设备60存储,以便指示副智能设备72(1)-72(N)是信任组10的部分。

[0057] 信任组中的主可穿戴设备还可以将一个或多个其他可穿戴设备添加到信任组。如图2中所示,主可穿戴设备60通过在主可穿戴设备60与副可穿戴设备73之间建立安全无线连接63来将副可穿戴设备73添加到信任组10。在至少一个实施例中,蓝牙可以用于安全地将副可穿戴设备73配对到主可穿戴设备60。可以使用在配对过程期间生成的安全协议(例

如,链接密钥)来建立安全无线连接63。当可以建立安全无线连接63时,标识副可穿戴设备73的信息可以由主可穿戴设备60存储,以便指示副可穿戴设备73是信任组10的部分。

[0058] 取决于所使用的可穿戴设备和智能设备的特定类型,将副可穿戴设备添加到信任组可以允许高级使用案例。在至少一些高级使用案例中,主可穿戴设备可以充当对于信任组中的其他可穿戴设备的代理或对等设备。例如,当主可穿戴设备60是包括音频但不包括视频的头戴式耳机并且副可穿戴设备73包括显示屏(例如,可穿戴手腕,诸如,智能手表等)时,一个可能的高级使用案例涉及分离的视听模型。在这个场景中,可以在副可穿戴设备73的显示屏中显示视频,同时可以通过主可穿戴设备60听到对应的音频。另一可能的高级使用案例包括立体声音乐能力,其中,两个物理上分开的单声道头戴式耳机一起工作以将立体声音乐提供给用户。

[0059] 在用户的生物计量凭证存储在主可穿戴设备60中或以其他方式可用于主可穿戴设备60并且主智能设备70已经被添加到信任组10之后,用户可以经由主可穿戴设备60来访问主智能设备70。当主可穿戴设备60以用户的生物计量凭证认证了用户且将此认证扩展到主智能设备70时,启用此访问。随后,当每一个副智能设备或副可穿戴设备加入信任组10时,用户也可以经由主可穿戴设备60来访问那些设备。当主可穿戴设备60以用户的生物计量凭证认证了用户且将此认证扩展到特定的副智能设备72(1)-72(N)或副可穿戴设备73时,启用此访问。当认证被扩展到主或副设备时,用户可以将命令或请求发布到主可穿戴设备当前被连接到的特定的主或副设备。

[0060] 此外,在信任组中使用的生物计量认证机制基于主可穿戴设备60和主智能设备71的特定生物计量标识能力。在一个示例中,如果主可穿戴设备60是语音使能的,并且主智能设备71注册用户的语音特性,则用户可以通过向其话筒说话来向语音使能的主可穿戴设备60(例如,头戴式耳机、语音使能的手表,等等)认证。在至少一些实施例中,用户还可能需要提供语音触发(例如,认证用户以及连接到信任组中的另一设备所需的指定的单词或短语)。在另一示例中,如果主可穿戴设备60是指纹使能的,并且主智能设备71注册用户的指纹特性,则用户可以通过将他一个或多个指纹提供给显示屏的指纹传感器区域来向指纹使能的主可穿戴设备60(例如,指纹使能的手表等)认证。这些是可以在信任组中如何使用不同的生物计量能力的说明性示例,并且不旨在是限制性的。实际上,可以使用任何语音使能的可穿戴设备(例如,头戴式耳机、语音使能的手表)、指纹使能的可穿戴设备(例如,指纹使能的手表等)或具有其他生物计量标识能力(例如,眼睛、手部、脉搏等)的任何可穿戴设备来形成信任组。

[0061] 在一个示例中,如果生物计量认证机制使用语音和/或言语认证,则用户可以通过向他的话筒说话来向语音使能的主可穿戴设备60(例如,头戴式耳机、语音使能的手表等)认证。在至少一些实施例中,用户还可能需要提供语音触发(例如,认证用户以及连接到信任组中的另一设备所需的指定的单词或短语)。在另一示例中,如果生物计量认证机制是指纹认证,则用户可以通过将他一个或多个指纹提供给显示屏的指纹传感器区域来向指纹使能的主可穿戴设备60(例如,指纹使能的手表等)认证。因此,可以使用任何语音使能的可穿戴设备(例如,头戴式耳机、语音使能的手表)、指纹使能的可穿戴设备(例如,指纹使能的手表等)或具有其他生物计量标识能力(例如,眼睛、手部、脉搏等)的其他可穿戴设备来形成信任组。

[0062] 转向图3A和图3B,示出根据本公开的至少一个实施例的示例可穿戴设备90的简化正视图。可穿戴设备90是头戴式耳机,此头戴式耳机包括耳套圈92、听筒(earpiece)94和设置在扩展件98中的话筒96。在一个或多个实施例中,可穿戴电子设备90的组件(例如,耳套圈92、听筒94、话筒96、扩展件98)可以由包括金属和金属合金(例如,不锈钢、铝、锡、铁、金、银、铂、钛等)、合成聚合物(塑料、橡胶、松紧带、碳纤维、注塑成型品)、上述各项的组合等的一种或多种材料形成。可穿戴设备90能以适配由具有不同身体比例(例如,外耳尺度、下颌尺度、耳廓尺度,等等)的各种用户穿戴的各种尺寸来制造。或者,可穿戴设备90的某些部分(例如,耳套圈92、话筒96、扩展件98)能以一个尺寸来制造,并具有可调整的耳机94以适配由具有不同外耳和耳廓尺度的各种用户穿戴。

[0063] 尽管可穿戴设备90被示出为单个耳部设备,但是将显而易见的是,可以使用众多其他设计,包括例如,具有双听筒的头带型头戴式耳机或具有双听筒的颈带型头戴式耳机。总之,使用户双耳中的一个或两个耳朵能够接收从由可穿戴电子设备90接收到的无线信号中产生的声波以及使用户能够使用话筒96来发送语音通信的任何配置。如图3A中所示,话筒96可以设置在扩展件98的远端。在其他配置中,话筒96可以设置在靠近扩展件98的近端,并且传声筒将声音从扩展件98的远端携带到话筒。

[0064] 可穿戴设备90可以包括耦合到多个电子组件的电路板,所述多个电子组件包括任何类型的组件、元件、电路等。话筒96是将声波转换为电信号的语音传感器。话筒96可以包括当由声波冲击时振动的隔膜,此隔膜使话筒96中的其他组件振动。这些振动可以被转换为电流,此电流变为音频信号。音频信号可以从模拟数据转换为数字数据,此数字数据是指来自用户的生物计量输入的“输入数据”的一个示例形式。

[0065] 图3B是示出用户100穿戴可穿戴电子设备90的简化正视图。耳套圈92围绕用户100的耳朵102的外部而固定。这个位置允许听筒94停留在耳朵102的耳道的入口处的外耳中。这个位置也允许将扩展件98沿用户的脸颊从听筒94向用户的嘴部104定位,语音声波源于此。

[0066] 转向图4,图4是示出可以与本文中描述的实施例相关联的活动的可能的流程400的流程图。在至少一个实施例中,一组或多组操作形式的逻辑对应于图4的活动。在示例中,智能设备(诸如,图1的智能设备20)可以执行这些组操作中的一个或多个操作。此智能设备可以包括用于执行此类操作的装置,包括例如一个或多个处理器(例如,本文中至少参照图10的处理器1000进一步所述的处理器)。在至少一个实施例中,注册模块28配置成用于当由一个或多个处理器执行时来执行这些组操作中的一个或多个操作。

[0067] 流程400可以开始于402处,在402处,启动主智能设备上的主注册模块。注册模块可以提供指示用户如何提供向可穿戴设备注册所需的特定生物计量输入(例如,语音、指纹、眼睛、面部、手部,等等)的用户接口。一旦用户已经提供了适当的生物计量输入,在404处,注册模块可以生成具有用户的生物计量凭证的生物计量凭证文件。在406处,主智能设备建立到可穿戴设备的安全连接。此安全连接可以是先前在主智能设备与可穿戴设备之间配置的安全无线连接(例如,蓝牙)。然而,在408处,任何其他有线或无线连接可以用于将生物计量凭证文件发送到可穿戴文件。在其他实施例中,在基于云的实现方式中,生物计量凭证文件可以发送到云。在这个场景中,可穿戴设备从云接收生物计量凭证文件。

[0068] 转向图5,图5是示出可以与本文中描述的实施例相关联的活动的可能的流程500

的流程图。在至少一个实施例中，一组或多组操作形式的逻辑对应于图5的活动。在示例中，可穿戴设备（诸如，图1的可穿戴设备40）可以执行这些组操作中的一个或多个操作。此可穿戴设备可以包括用于执行此类操作的装置，包括例如一个或多个处理器（例如，本文中至少参照图10的处理器1000进一步所述的处理器）。在至少一个实施例中，配置模块44配置成用于当由一个或多个处理器执行时以：当主智能设备注册用户的生物计量凭证并与可穿戴设备40形成信任组时来执行这些组操作中的一个或多个操作。

[0069] 流程500可以开始于500处，在500处，可穿戴设备建立到主智能设备的安全无线连接（或其他安全连接）。在至少一个实施例中，此可以连接可以在已经生成生物计量凭证文件之后由主智能设备发起。在建立了安全连接之后，在504处，可穿戴设备从主智能设备接收生物计量凭证文件。在506处，生物计量凭证文件可以存储在可穿戴设备中（例如，生物计量凭证文件43）。

[0070] 在508处，确定主智能设备的唯一标识信息。在本示例中，确定与在可穿戴设备与主智能设备之间配置的安全无线连接相关联的无线连接安全信息。在至少一个实施例中，此无线连接安全信息包括安全无线连接的共享秘密。在蓝牙™无线连接中，例如，共享秘密是当设备经配对时所确定的链路密钥。在510处，共享秘密可以被映射到设备标识符，并且可存储在信任组表45中。当向可穿戴设备注册来自主智能设备的生物计量凭证时，在可穿戴设备与主智能设备之间形成信任组（如在504和506处所指示），并且以唯一地标识主智能设备的信息来更新信任表45。

[0071] 转向图6，图6是示出可以与本文中描述的实施例相关联的活动的可能的流程600的流程图。在至少一个实施例中，一组或多组操作形式的逻辑对应于图6的活动。在示例中，副智能设备（此副智能设备能以如本文中先前所述的、类似于图1的智能设备20方式来配置）可以执行这些组操作中的一个或多个操作。此副智能设备可以包括用于执行此类操作的装置，包括例如一个或多个处理器（例如，本文中至少参照图10的处理器1000进一步所述的处理器）。在至少一个实施例中，副智能设备的注册模块配置成用于当由一个或多个处理器执行时来执行这些组操作中的一个或多个操作。

[0072] 流程600可以开始于602处，在602处，启动副智能设备上的注册模块。在604处，副智能设备建立到可穿戴设备的安全无线连接。一旦建立了安全无线连接，在606处，副智能设备就可以将用于判定副智能设备是否已经加入信任组的查询发送到可穿戴设备。此外，在相同的或不同的查询中，副智能设备还向可穿戴设备查询以确定其能力（例如，语音使能的认证、指纹使能的认证、它是否已经被供应用户的生物计量凭证以及它是否已经形成信任组，等等）。如果来自可穿戴设备的响应确认了副智能设备已经加入信任组，则如在608处所确定，流程600可以结束。如果来自可穿戴设备的响应指示了副智能设备不是信任组的当前成员，则在610处，可以作出关于以下内容的判定：相同的响应（或不同的响应）是否指示了可穿戴设备具有生物计量认证能力，此可穿戴设备是否被供应来自主智能设备的生物计量凭证，以及是否已经形成信任组。如果可穿戴设备不具有生物计量认证能力，或如果还未供应生物计量凭证或还未形成信任组，则流程600可以结束。然而，如果可穿戴设备确实具有生物计量认证能力，并且如果已经供应生物计量凭证且已经形成信任组，则在612处，副智能设备可以将被添加到信任组中的请求发送到可穿戴设备。

[0073] 转向图7，图7是示出可以与本文中描述的实施例相关联的活动的可能得流程700

的流程图。在至少一个实施例中，一组或多组操作形式的逻辑对应于图7的活动。在示例中，可穿戴设备（诸如，图1的可穿戴设备40）可以执行这些组操作中的一个或多个操作。此可穿戴设备可以包括用于执行此类操作的装置，包括例如一个或多个处理器（例如，本文中至少参照图10的处理器1000进一步所述的处理器）。在至少一个实施例中，当副智能设备请求进入信任组时，配置模块44配置成用于当由一个或多个处理器执行时以：当副智能设备请求进入信任组时来执行这些组操作中的一个或多个操作。

[0074] 流程700可以开始于702处，在702处，可穿戴设备建立到副智能设备的安全无线连接。在至少一个实施例中，可以在启动了副智能设备上的注册模块之后，由副智能设备发起此连接。在建立了安全连接之后，在704处，可穿戴设备可以从副智能设备接收用于判定此副智能设备是否已经加入信任组的查询。此外，在相同的或不同的查询中，副智能设备还向可穿戴设备查询以确定其能力（例如，语音使能的认证、指纹使能的认证、它是否已经被供应用户的的生物计量凭证以及它是否已经形成信任组，等等）。在706处，可穿戴设备可以向信任组表45搜索对应于副智能设备的设备标识符。如果发现了设备标识符，则此副智能设备是信任组的部分。否则，此副智能设备不是信任组的部分。在708处，可穿戴设备可以将指示副智能设备是否是信任组的成员的响应发送到此副智能设备。此外，可穿戴设备可以将关于此可穿戴设备的能力以及此可穿戴设备是否已经配置了生物计量凭证以及是否已经形成信任组的信息发送到副智能设备。

[0075] 如果副智能设备被确定为不是由可穿戴设备和至少一个其他智能设备形成的信任组的部分，则在710处，可穿戴设备可以接收将副智能设备添加至信任组的请求。在712处，可穿戴设备可以确定共享秘密（例如，用于蓝牙连接的链接密钥）或智能设备的其他唯一标识信息，并且在714处，可穿戴设备可以将对应于副智能设备的设备标识符映射到信任组表45中的共享秘密。

[0076] 转向图8，图8是示出可以与本文中描述的实施例相关联的活动的可能的流程800的流程图。在至少一个实施例中，一组或多组操作形式的逻辑对应于图8的活动。在示例中，可穿戴设备（诸如，图1的可穿戴设备40）可以执行这些组操作中的一个或多个操作。此可穿戴设备可以包括用于执行此类操作的装置，包括例如一个或多个处理器（例如，本文中至少参照图10的处理器1000进一步所述的处理器）。在至少一个实施例中，生物计量认证模块42配置成用于当由一个或多个处理器执行时来执行这些组操作中的一个或多个操作。

[0077] 流程800可以开始于802处，在802处，可穿戴设备根据在此设备上供应的生物计量传感器的特定类型来接收生物计量输入数据（例如，语音数据、指纹数据，等等）。在804处，作出关于生物计量认证是否已经成功的判定。一般而言，可以在生物计量输入数据与先前在可穿戴设备上注册的生物计量凭证之间进行比较。如果生物计量输入数据对应于生物计量凭证，则生物计量输入数据经认证。否则，生物计量认证失败。

[0078] 然而，对于语音使能的生物计量认证，可以执行语音识别和言语识别两者。可以使用在生物计量输入数据与先前在可穿戴设备上注册的生物计量凭证之间进行的前述比较来执行语音识别。言语识别可以用于判定是否由用户说出特定的语音触发。如果认证确定的任一部分失败，则生物计量输入数据（以及用户）可能未经认证。如果如在804处确定，生物计量认证不成功，则在814处，可以采取适当的动作。例如，可将认证结果（例如，‘失败’）发送到它当前连接到的（主或副）智能设备。此外，可穿戴设备可以防止指示来自用户的输

入的任何附加输入数据被发送到智能设备。

[0079] 然而,如果如在804处所确定,认证成功,则在806处,可穿戴设备可以在此可穿戴设备的无线范围内建立到智能设备的安全无线连接。在808处,可以作出关于智能设备是否在信任组中的判定。这可以通过搜索信任组表45来找到对应于智能设备的设备标识符来确定。在至少一个实施例中,如果智能设备的设备标识符被映射到信任组表45中的共享秘密,则此智能设备被确定为在信任组中。如果智能设备不在信任组中,则在814处,如先前所描述,可以采取适当的行动。然而,如果智能设备在信任组中,则在810处,生物计量认证被扩展到智能设备。这可以通过发送指示认证成功的认证结果来实现。

[0080] 在另一实现方式中,指示由可穿戴设备捕捉到的其他输入的其他输入数据可以作为认证成功指示被转发到智能设备。对于语音使能的认证以及与智能设备的交互,可以在待认证的生物计量输入之后单独地捕捉其他输入。例如,语音触发(诸如,“你好,智能设备”)可以被首先说出,随后,可以进行询问,诸如“今天天气怎么样?”或者,可以与待认证的生物计量输入一起并发地捕捉其他输入。例如,可以在多个单词之间没有停顿地说出与查询相组合的语音触发,诸如,“你好,智能设备,今天天气怎么样”。在812处,可将指示由可穿戴设备捕捉到的其他输入的其他输入数据发送到智能设备,直到经认证的会话结束或者直到接收到另一语音触发(在语音使能的认证的情况下)为止。

[0081] 转向图9,图9是示出可以与本文中描述的实施例相关联的活动的可能的流程900的流程图。在至少一个实施例中,一组或多组操作形式的逻辑对应于图9的活动。在示例中,(主或副)智能设备(诸如,图1的智能设备20)可以执行这些组操作中的一个或多个操作。此智能设备可以包括用于执行此类操作的装置,包括例如一个或多个处理器(例如,本文中至少参照图10的处理器1000进一步所述的处理器)。在至少一个实施例中,安全代理22配置成用于当由一个或多个处理器执行时来执行这些组操作中的一个或多个操作。

[0082] 流程900可以开始于902处,在902处,(主或副)智能设备从可穿戴设备接收通信。在904处,智能设备可以基于唯一地标识可穿戴设备的信息来确定可穿戴设备的身份。在一个实施例中,智能设备可以使用对应于可穿戴设备的设备标识符与到可此可穿戴设备的无线连接的共享秘密之间的映射。在906处,基于设备ID和共享秘密,作出关于可穿戴设备是否在信任组中的判定。如果如在906处所确定,可穿戴设备不在信任组中,则流程900可以结束,并且操作系统可以保持锁定。然而,如果可穿戴设备在信任组中,则在908处,安全代理可以解锁智能设备的操作系统。在至少一个实施例中,仅当用户已经认证时,可穿戴设备才发送通信。因此,每当智能设备从可穿戴设备接收到通信时,此智能设备解锁操作系统。在一些其他实施例中,可以由安全代理基于安全等级来控制对服务和应用的访问。可以基于安全代理从可穿戴设备接收到的认证结果来确定安全等级以及是否将解锁操作系统。在910处,安全代理可以允许经由可穿戴设备来与用户通信,直到经认证的会话结束或如安全等级所准许。

[0083] 图10是与本公开的示例生态系统SOC 1000相关联的简化框图。本公开的至少一个示例实现方式可以包括本文中讨论的可穿戴电子设备特征和/或智能设备特征与ARM组件的集成。例如,图10的示例可以与任何ARM核(例如,A-9、A-15等等)相关联。此外,架构可以是任何类型的可穿戴电子设备、智能设备、平板、智能电话(包括安卓™电话、i-Phones™)、i-Pad™、谷歌Nexus™、微软Surface™、视频处理组件、膝上型计算机(包括任何类型的笔记

本计算机)、超极本™、任何类型的触摸使能的输入设备等的部分。

[0084] 在图10的示例中,ARM生态系统SOC 1000可以包括多个核1006-1007、L2高速缓存控件1008、总线接口单元1009、L2高速缓存1010、图形处理单元(GPU)1015、互连1002、视频编解码器1020以及有机发光二极管(OLED)显示器接口1025,此OLED接口1025可以与耦合到OLED的移动行业处理器接口(MIPI)/高清晰度多媒体接口(HDMI)链路相关联。

[0085] ARM生态系统SOC 1000还可以包括订户身份模块(SIM)接口1030、引导只读存储器(ROM)1035、同步动态随机存取存储器(SDRAM)控制器1040、闪存控制器1045、串行外围接口(SPI)控制器1050、合适的功率控件1055、动态RAM(DRAM)1060以及闪存1065。此外,一个或多个实施例包括一个或多个通信能力、接口和特征,诸如,蓝牙™1070、3G/4G调制解调器1075、全球定位系统(GPS)1080以及802.11WiFi 1085的实例。

[0086] 在操作中,图10的示例可以提供处理能力以及相对低的功耗从而允许各种类型的计算(例如,移动计算)。此外,此类架构可以允许任何数量的软件应用(例如,安卓™、Adobe® Flash® 播放器、Java平台标准编辑(Java SE)、JavaFX、Linux、微软Windows Embedded、塞班和乌班图(Ubuntu),等等)。在至少一个实施例中,核处理器可以用耦合低时延2级高速缓存实现乱序超标量流水线。

[0087] 转向图11,图11是示出可以与本文中讨论的可穿戴电子设备40相关联的潜在电子设备和逻辑的简化框图。在至少一个示例实施例中,系统1100可以包括触摸控制器1102、指纹传感器控制器1104、一个或多个处理器1106、耦合到(多个)处理器1106中的至少一个处理器的系统控制逻辑1108、耦合到系统控制逻辑1108的系统存储器1110、耦合到系统控制逻辑1108的非易失性存储器和/或(多个)存储设备1134、耦合到系统控制逻辑1108的显示控制器1114、耦合到一个或多个显示设备1112的显示控制器1114、耦合到系统控制逻辑1108的功率管理控制器1120和/或耦合到系统控制逻辑1108的通信接口1118。

[0088] 因此,可结合本公开的教导来使用任何可穿戴电子设备系统的基本构建块(例如,处理器、控制器、存储器、I/O、显示器,等等)。某些组件可以是分立的,或者可以集成到片上系统(SoC)中。一些通用系统实现方式可以包括某些类型的形状因子,按此形状因子,系统1100是更通用化壳体的部分。在替代实现方式中,某些替代实施例而不是可穿戴电子设备与其它智能设备(诸如,移动电话、平板设备等)打交道。

[0089] 在至少一个实施例中,系统控制逻辑1108可以包括任何合适的接口控制器,此合适的接口控制器用于提供到至少一个处理器1106和/或到与系统控制逻辑1108通信的任何合适的设备或组件的任何合适的接口。在至少一个实施例中,系统控制逻辑1108可以包括用于提供到系统存储器1110的接口的一个或多个存储器控制器。系统存储器1110可以用于例如为系统1100加载和存储数据和/或指令。在至少一个实施例中,系统存储器1110可以包括任何合适的易失性存储器,诸如例如,合适的动态随机存取存储器(DRAM)。在至少一个实施例中,系统控制逻辑1108可以包括用于提供到显示设备1112、触摸控制器1102和非易失性存储器和/或(多个)存储设备1134的接口的一个或多个I/O控制器。

[0090] 非易失性存储器和/或(多个)存储设备1134可以用于存储例如软件1130内的数据和/或指令。非易失性存储器和/或(多个)存储设备1134可以包括任何合适的非易失性存储器(诸如例如,闪存存储器)和/或可以包括任何合适的(多个)非易失性存储设备(诸如例如,一个或多个硬盘驱动器(HDD)、固态驱动器(SSD),等等)。

[0091] 功率管理控制器1120可以包括配置成用于控制各种功率管理和/或功率节省功能的功率管理逻辑1132。在至少一个实施例中,功率管理控制器1120配置成用于减少当可穿戴设备处于不活跃状态(例如,不是正在被访问,等等)时以降低的功率操作或被关闭的系统1100的组件或设备的功耗。例如,在至少一个实施例中,当可穿戴电子设备处于不活跃状态时,功率管理控制器1120执行以下操作中的一项或多项:关闭显示器的未使用部分和/或与其相关联的任何背光;如果在关闭配置下需要更少的计算功率,则允许(多个)处理器1106中的一个或多个处理器进入低功率状态;以及当电子设备处于不活跃状态时,将可能未被使用的任何设备和/或组件(例如,无线模块)关机。

[0092] (多个)通信接口1118可以为系统1100提供用于通过一个或多个网络和/或与任何其他合适的设备通信的接口。(多个)通信接口1118可以包括任何合适的硬件和/或固件。在至少一个示例实施例中,(多个)通信接口1118可以包括例如,网络适配器、无线网络适配器、电话调制解调器和/或无线调制解调器。在至少一个实施例中,系统控制逻辑1108可以包括用于提供到任何(多个)合适的输入/输出设备的接口的一个或多个I/O控制器,所述输入/输出设备诸如例如,音频设备、相机或摄像机,所述音频设备用于帮助将声音转换为对应的数字信号和/或帮助将数字信号转换为对应的声音。

[0093] 对于至少一个实施例,至少一个处理器1106可以与系统控制逻辑1108的一个或多个控制器的逻辑封装在一起。在至少一个实施例中,至少一个处理器1106可以与系统控制逻辑1108的一个或多个控制器的逻辑封装在一起以形成封装中系统(SiP)。在至少一个实施例中,至少一个处理器1106可以与系统控制逻辑1108的一个或多个控制器的逻辑集成在相同的管芯上。对于至少一个实施例,至少一个处理器1104可以与系统控制逻辑1108的一个或多个控制器的逻辑集成在相同的管芯上以形成片上系统(SoC)。

[0094] 对于触摸控制,触摸控制器1102可以包括触摸传感器接口电路1124和触摸控制逻辑1126。触摸传感器接口电路1124可以耦合到一个或多个触摸传感器1122,以便检测显示器(例如,至少一个显示设备1112)的第一触摸表面层和第二触摸表面层上方的(多个)触摸输入。触摸传感器接口电路1124可以包括任何合适的电路,此合适的电路可以例如至少部分地取决于用于触摸输入设备1116的触敏技术,所述触摸输入设备1116可包括一个或多个触摸传感器1122。在一个实施例中,触摸传感器接口电路1124可以支持任何合适的多点触摸技术。在至少一个实施例中,触摸传感器电路1124可以包括用于将对应于第一触摸表面层和第二表面层的模拟信号转换为任何合适的数字触摸输入数据的任何合适的电路。用于至少一个实施例的合适的数字触摸输入数据可以包括例如触摸位置或坐标数据。

[0095] 触摸控制逻辑1126可以经耦合,以便以任何合适的方式帮助控制触摸传感器接口电路1124,从而检测第一触摸表面层和第二触摸表面层上方的触摸输入。用于至少一个示例实施例的触摸控制逻辑1126还可以经耦合,以便以任何合适的方式输出对应于由触摸传感器接口电路1124检测到的触摸输入的数字触摸输入数据。可以使用可以例如至少部分地取决于用于触摸传感器接口电路1124的电路的任何合适的逻辑(包括任何合适的硬件、固件和/或软件逻辑(例如,非暂态有形介质))来实现触摸控制逻辑1126。用于至少一个实施例的触摸控制逻辑1126可以支持任何合适的多点触摸技术。

[0096] 触摸控制逻辑1126可以经耦合,以便将数字触摸输入数据输出到系统控制逻辑1108和/或至少一个处理器1106以进行处理。用于至少一个实施例的至少一个处理器1106

可以执行任何合适的软件以处理来自触摸控制逻辑1126的数字触摸输入数据。合适的软件可以包括例如,任何合适的驱动器软件和/或任何合适的应用软件。

[0097] 对于指纹传感器控制,指纹传感器控制器1104可以包括触摸传感器接口电路1138和指纹传感器控制逻辑1140。指纹传感器接口电路1138可以耦合到指纹传感器1136,以便控制指纹传感器1136的操作并接收可以使用指纹传感器1136而在显示器(例如,至少一个显示设备1112)的表面层上方捕捉到的一个或多个所捕捉的指纹。指纹传感器接口电路1138可以包括可以例如至少部分地取决于用于指纹传感器1136的指纹传感器技术的任何合适的电路。在一个或多个实施例中,指纹传感器接口电路1138可以支持任何合适的多点指纹捕捉技术。在至少一个实施例中,指纹传感器接口电路1138可以包括用于将对应于捕捉到的指纹的模拟信号转换为任何合适的数字指纹数据的任何合适的电路。用于至少一个实施例的合适的数字指纹数据可以包括例如,指纹图像或指纹的电容性突起/凹陷测量数据。

[0098] 对于生物计量传感器,一个或多个生物计量传感器控制器1104可以包括生物计量传感器接口电路1142和生物计量传感器控制逻辑(例如,用于语音传感器控制、指纹传感器控制、眼部传感器控制、面部特征传感器控制、手部传感器控制,等等)。生物计量传感器接口电路1142可以耦合到生物计量传感器(例如,话筒、指纹传感器、眼部传感器(视网膜和/或虹膜)、面部特征传感器、手部传感器(几何特征和/或掌纹),等等),以便控制特定生物计量传感器的操作以及接收特定输入(例如,语音模式、指纹、视网膜和/或虹膜测量、手部几何特征、掌纹,等等)。生物计量传感器接口1142可以包括可以例如至少部分地取决于用于特定的生物计量传感器的特定技术(例如,语音和/或言语传感器技术、指纹传感器技术、面部特征传感器技术、手部几何结构传感器技术、掌纹传感器技术,等等)的任何合适的电路。例如,用于指纹传感器的生物计量传感器接口电路1142可以支持多点指纹捕捉技术。在另一示例中,用于话筒的生物计量传感器接口电路1142可以支持语音识别(即,基于语音模式对特定用户的标识)和言语识别(即,对特定讲话内容的识别)两者。取决于所使用的特定生物计量传感器,输入传感器接口电路1142还可以包括用于将模拟信号转换为任何合适的数字数据的合适的电路。

[0099] 生物计量传感器控制逻辑1144可以经耦合,以便以任何合适的方式控制生物计量传感器接口电路1142,从而控制特定的生物计量传感器并且捕捉适当的数据。对于至少一个实施例,生物计量传感器控制逻辑1144还可以经耦合,以便以任何合适的方式输出由生物计量传感器接口电路1142检测到的数字数据。可以使用可以例如至少部分地取决于用于生物计量传感器接口电路1142的任何合适的逻辑(包括任何合适的硬件、固件和/或软件逻辑(例如,非暂态有形介质))来实现生物计量传感器控制逻辑1144。对于至少一个实施例,生物计量传感器控制逻辑1144可以支持任何合适的语音识别技术、言语识别技术、视网膜和/或虹膜识别数据、单点或多点指纹捕捉技术、手部测量技术、掌纹捕捉技术以及与所使用的特定传感器相关联的任何其他技术。

[0100] 生物计量传感器控制逻辑1144可以经耦合,以便将数字数据(例如,语音数据、指纹数据、眼部数据、手部数据、掌部数据)输出到系统控制逻辑1108和/或至少一个处理器1106以进行处理。用于至少一个实施例的至少一个处理器1106可以执行任何合适的软件以处理来自生物计量传感器控制逻辑1144的数字数据输出。例如,在一个或多个实施例中,可

处理数字数据,以便基于被可能存储在非易失性存储器和/或存储设备734中或在云中的合适的存储设备中的经授权用户的生物计量凭证来验证此数字数据。合适的软件可以包括例如任何合适的驱动器软件和/或任何合适的应用软件。如图11中所示,系统存储器1110可以存储合适的软件1128和/或非易失性存储器和/或(多个)存储设备可以存储任何合适的软件1134。

[0101] 将显而易见的是,取决于特定的可穿戴电子设备或智能设备,未在图10至图11中示出的其他组件可能存在于特定的可穿戴电子设备或智能设备中。相反,不是图10至图11中示出的所有组件都将一定存在于特定的可穿戴电子设备或智能设备中。作为示例,头戴式耳机可能不包括允许视频显示和交互的组件(例如,视频编解码器1020、OLED视频接口1025、显示控制器1114、显示设备712、触摸输入设备1116、触摸传感器722、触摸控制器1102、触摸传感器接口电路1124、触摸控制逻辑1126)。在另一示例中,在主智能设备已经向可穿戴电子设备注册了用户的认证凭证之后被添加到信任组中的副智能设备可以或可以不包括任何生物计量技术(例如,生物计量传感器1136、生物计量传感器控制器1104、生物计量传感器接口电路1138、生物计量传感器控制逻辑1140)。

[0102] 注意,在一些示例实现方式中,可以结合在一个或多个有形的非暂态计算机可读存储介质(例如,在专用集成电路(ASIC)中、在数字信号处理器(DSP)指令、将由处理器或其他类似的机器执行的软件(潜在地包括目标代码和源代码)等)中编码的逻辑来实现本文中概述的功能。在这些实例中的一些中,存储器元件可存储用于本文中描述的操作的数据。这可以包括存储器元件能够存储经执行以实现本文中描述的活动的软件、逻辑、代码或处理器指令。处理器可以执行与这些数据相关联的任何类型的指令以实现本文中详细描述的操作。在一个示例中,处理器可以将元件或制品(例如,数据)从一个状态或事物变换为另一状态或事物。在另一示例中,能以固定逻辑或可编程逻辑(例如,由处理器执行的软件/计算机指令)来实现本文中概述的活动,并且本文中标识的元件可以是某种类型的可编程处理器、可编程数字逻辑(例如,现场可编程门阵列(FPGA)、DSP、可擦可编程只读存储器(EPROM)、电擦可编程只读存储器(EEPROM))或可以包括数字逻辑、软件、代码、电子指令的ASIC或上述各项的任何合适的组合。

[0103] 当适当时并且基于特定的需要,可穿戴设备(例如,40、60、90)、智能设备(例如,20、71、72(1)-72(N))以及云中的网络元件可以将数据和信息保持在任何合适的存储器元件(例如,随机存取存储器(RAM)、只读存储器(ROM)、可编程ROM(PROM)、可擦PROM(EPROM)、电EPROM(EEPROM)、盘驱动器、软盘、紧致盘ROM(CD-ROM)、数字多功能盘(DVD)、闪存、磁光盘、专用集成电路(ASIC)或能够存储数据和信息的其他类型的非易失性机器可读存储介质)、软件、硬件、固件中或保持在任何其他合适的组件、设备、元件或对象中。本文中讨论的存储器项中的任一者应当解释为被涵盖在广义术语“存储器元件”中。此外,在可穿戴设备、智能设备以及云中的网络元件中使用、存储、跟踪、发送、或接收的信息可以在任何存储结构中提供,所述存储结构包括但不限于,储存库、数据库、寄存器、队列、表或高速缓存,可以在任何合适的时间帧处引用所有这些。任何此类存储结构(例如,信任组表45、生物计量凭证文件43等)也可包括在如本文中使用的广义术语“存储器元件”中。

[0104] 重要的是要注意到,仅为了示例和教导的目的而仅提供除其他协议和关系(例如,特定的操作、定时间隔,等等)之外的本文中概述的所有规范、尺度和关系(例如,尺寸、材

料,等等)。可显著地改变这些数据中的每一个数据,而不背离本公开的精神或所附权利要求书的范围。这些规范应用于非限制性示例,相应地,它们应当如此来解释。

[0105] 本领域技术人员可以确定许多其他改变、替换、变化、更改和修改,并且本公开旨在将所有此类改变、替换、变化、更改和修改涵盖为落在所附权利要求书的范围内。为了辅助美国专利商标局(USPTO),并且另外辅助对本申请颁证的任何专利的任何读者解释本申请所附的权利要求书,申请人希望注明本申请人:(a)不旨在在所附权利要求书中的任何权利要求调用35U.S.C. 章节112第(6)段,因为它存在于本申请的提交日期,除非在特定的权利要求中专门使用单词“用于……的装置”或“用于……的步骤”;以及(b)不旨在通过在说明书中的任何陈述以便以未以其他方式在所附权利要求书中反映的任何方式来限制本公开。

[0106] 其他注释和示例

[0107] 以下示例涉及根据本说明书的实施例。注意,还可参照本文中描述的方法和过程来实现以上描述的装置和系统的所有任选特征,并且示例中的细节可以在一个或多个实施例中的任何地方使用。

[0108] 示例1是一种可穿戴电子设备,包括:生物计量传感器;以及逻辑,在硬件中实现所述逻辑的至少部分,所述逻辑配置成用于:接收指示生物计量输入的输入数据;至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;建立到智能设备的无线连接;判定所述智能设备是否被包括在一个或多个智能设备的信任组中;以及当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。

[0109] 在示例2中,示例1的主题可以选地包括:所述逻辑配置成用于:从所述智能设备和云中的至少一个接收所述经授权用户的所述至少一个生物计量凭证。

[0110] 在示例3中,示例1至2中任一项的主题可以任选地包括一个或多个存储器元件,其中,所述逻辑配置成用于将所述至少一个生物计量凭证存储在所述一个或多个存储器元件中。

[0111] 在示例4中,示例1至3中的任一项的主题可以任选地包括:所述逻辑配置成用于:当唯一地标识所述智能设备的信息被存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中。

[0112] 在示例5中,示例4的主题可以任选地包括:所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。

[0113] 在示例6中,示例1至5中的任一项的主题可以任选地包括:所述逻辑配置成用于:接收指示其他生物计量输入的其他输入数据,其中,所述通信包括所述其他输入数据。

[0114] 在示例7中,示例1至6中任一项的主题可以任选地包括:所述逻辑配置成用于:当未成功地认证所述输入数据时,不发送用于解锁所述智能设备的所述通信。

[0115] 在示例8中,示例1至6中的任一项的主题可以任选地包括:所述逻辑进一步配置成用于:将认证结果发送到所述智能设备,其中,所述认证结果指示是否成功地认证了所述输入数据。

[0116] 在示例9中,示例1至8中的任一项的主题可以任选地包括:所述生物计量传感器包括语音传感器,其中,所述逻辑配置成用于:基于验证所述输入数据中的语音触发以及验证由所述输入数据表示的语音对应于所述经授权用户的语音来认证所述输入数据。

[0117] 在示例10中,示例1至8中的任一项所述的主体可以任选地包括:所述生物计量传感器包括语音传感器、指纹传感器、眼部传感器和手部传感器中的一个。

[0118] 在示例11中,示例1至5和7至10中的任一项所述的主体可以任选地包括:所述逻辑配置成用于:接收指示用于访问所述智能设备上的应用或服务的用户输入的其他输入数据;以及将所述其他输入数据发送到所述智能设备。

[0119] 在示例12中,示例11的主题可以任选地包括:所述用户输入的类型与所述生物计量输入的类型不同。

[0120] 示例13是至少一种计算机可读存储介质,包括用于可穿戴电子设备的指令,当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:接收指示生物计量输入的输入数据;至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;建立到智能设备的无线连接;判定所述智能设备是否被包括在一个或多个智能设备的信任组中;以及当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。

[0121] 在示例14中,示例13的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:从所述智能设备和云中的一个接收所述经授权用户的所述至少一个生物计量凭证。

[0122] 在示例15中,示例13至14中的任一项的主题可以任选地包括:当由所述至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:将所述至少一个生物计量凭证存储在一个或多个存储器元件中。

[0123] 在示例16中,示例13至15中的任一项的主题可以可选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:当唯一地标识所述智能设备的信息存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中。

[0124] 在示例17中,示例16的主题可以任选地包括:所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。

[0125] 在示例18中,示例13至17中的任一项的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:接收指示其他生物计量输入的其他输入数据,其中,所述通信包括所述其他输入数据。

[0126] 在示例19中,示例13至18中任一项所述的主体可以可选地包括当该指令由至少一个处理器执行时,该指令致使该至少一个处理器:当未成功地认证该输入数据时不发送用于解锁该智能设备的该通信。

[0127] 在示例20中,示例13至18中的任一项所述的主体可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:将认证结果发送到所述智能设备,其中,所述认证结果指示是否成功地认证了所述输入数据。

[0128] 在示例21中,示例13至20中的任一项的主题可以任选地包括:所述生物计量传感器包括语音传感器,其中当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:基于验证所述输入数据中的语音触发以及验证以后所述输入数据表示的语音对应于所述经授权用户的语音来认证所述输入数据。

[0129] 在示例22中,示例13至20中的任一项的主题可以任选地包括:所述生物计量传感

器包括语音传感器、指纹传感器、眼部传感器和手部传感器中的一个。

[0130] 在示例23中,示例13至17和19至22中的任一项所述的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:接收指示用于访问所述智能设备上的应用或服务的用户输入的其他输入数据;以及将所述其他输入数据发送到所述智能设备。

[0131] 在示例24中,示例23所述的主题可以任选地包括:所述用户输入的类型与所述生物计量输入的类型不同。

[0132] 示例25是一种用于可穿戴电子设备的方法,包括以下步骤:接收指示生物计量输入的输入数据;至少部分地基于经授权用户的至少一个生物计量凭证来尝试认证所述输入数据;建立到智能设备的无线连接;判定所述智能设备是否被包括在一个或多个智能设备的信任组中;以及当成功地认证了所述输入数据并且当所述信任组包括所述智能设备时,发送用于解锁所述智能设备的通信。

[0133] 在示例26中,示例25的主题可以任选地包括以下步骤:从所述智能设备和云中的一个接收所述经授权用户的所述至少一个生物计量凭证。

[0134] 在示例27中,示例25至26中的任一项的主题可以任选地包括以下步骤:将所述至少一个生物计量凭证存储在所述一个或多个存储器元件中。

[0135] 在示例28中,示例25至27中的任一项的主题可以任选地包括以下步骤:当唯一地标识所述智能设备的信息被存储在与所述信任组相关联的存储器元件中时,确定所述智能设备被包括在所述信任组中。

[0136] 在示例29中,示例28的主题可以任选地包括:所述存储器元件包括所述智能设备的设备标识符与用于保护所述无线连接的共享秘密之间的映射。

[0137] 在示例30中,示例25至29中的任一项的主题可以任选地包括以下步骤:接收指示其他生物计量输入的其他输入数据,其中,所述通信包括所述其他输入数据。

[0138] 在示例31中,示例25至30中的任一项的主题可以任选地包括:当未成功地认证所述输入数据时,不发送用于解锁所述智能设备的所述通信。

[0139] 在示例32中,示例25至30中的任一项的主题可以任选地包括以下步骤:将认证结果发送到所述智能设备,其中,所述认证结果指示是否成功地认证了所述输入数据。

[0140] 在示例33中,示例25至32中的任一项的主题可以任选地包括:所述生物计量传感器包括语音传感器,其中,所述方法可以任选地包括以下步骤:基于验证所述输入数据中的语音触发以及验证由所述输入数据表示的语音对应于所述经授权用户的语音来认证所述输入数据。

[0141] 在示例34中,示例25至32中的任一项的主题可以任选地包括:所述生物计量传感器包括语音传感器、指纹传感器、眼部传感器和手部传感器中的一个。

[0142] 在示例35中,示例25至29和31至34中的任一项的主题可以任选地包括以下步骤:接收指示用于访问所述智能设备上的应用或服务的用户输入的其他输入数据;以及将所述其他输入数据发送到所述智能设备。

[0143] 在示例36中,示例35的主题可以任选地包括:所述用户输入的类型与所述生物计量输入的类型不同。

[0144] 示例37是一种用于将认证扩展到智能设备的设备,所述设备包括用于执行如示例

25至36中的任一项的方法的装置。

[0145] 在示例38中,示例37的主题可以任选地包括:用于执行所述方法的、包括至少一个处理器和至少一个存储器元件的装置。

[0146] 在示例39中,示例38的主题可以任选地包括:所述至少一个存储器元件包括机器可读指令,当执行所述机器可读指令时,所述机器可读指令使所述设备执行示例25至36中的任一项的方法。

[0147] 在示例40中,示例37至39中的任一项的主题可以任选地包括:所述设备是可穿戴设备。

[0148] 示例41是至少一种计算机可读存储介质,包括用于智能设备的指令,当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:生成用户的至少一个生物计量凭证;将所述至少一个生物计量凭证发送到可穿戴电子设备;在所述智能设备上接收通信;确定所述通信的发送方的身份信息;以及当所述身份信息指示所述发送方是所述可穿戴电子设备时,解锁所述智能设备。

[0149] 在示例42中,示例41的主题可以任选地包括:所述身份信息包括与对应于所述发送方的设备标识符以及与所述智能设备与所述发送方之间的无线连接相关联的共享秘密。

[0150] 在示例43中,示例41至42中的任一项的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:在接收到所述通信之前,确定所述可穿戴电子设备的身份信息;以及存储所述可穿戴电子设备的所述身份信息。

[0151] 在示例44中,示例43的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:对所述发送方的所述身份信息与所述可穿戴电子设备的所存储的身份信息进行比较,以便判定所述发送方是否是所述可穿戴电子设备。

[0152] 在示例45中,示例41至44中的任一项的主题可以任选地包括:所述至少一个生物计量凭证基于所述用户的生物计量特性,所述生物计量特性包括语音、指纹、眼睛、面部特征和手部特征中的一项。

[0153] 在示例46中,示例41至45中的任一项的主题可以任选地包括:所述通信包括用于由所述智能设备启用语音识别的命令,并且当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:从所述可穿戴电子设备接收包括语音输入数据的后续通信。

[0154] 在示例47中,示例46所述的任一项的主题可以任选地包括:当所述指令由至少一个处理器执行时,所述指令使所述至少一个处理器:将所述语音输入数据提供给所述智能设备上的个人助理应用。

[0155] 在示例48中,示例41至47中的任一项的主题可以任选地包括:当由至少一个处理器执行所述指令时,所述指令使所述至少一个处理器:接收认证结果,所述认证结果指示对指示用户的生物计量输入的输入数据的认证是否成功;以及基于所述认证结果而允许对所述智能设备上的应用和服务的选择性访问。

[0156] 示例49是一种用于保护智能设备上的私有数据的方法,所述方法包括以下步骤:生成用户的至少一个生物计量凭证;将所述至少一个生物计量凭证发送到可穿戴电子设备;在所述智能设备上接收通信;确定所述通信的发送方的身份信息;以及当所述身份信息指示所述发送方是所述可穿戴电子设备时,解锁所述智能设备。

[0157] 在示例50中,示例49的主题可以任选地包括:所述身份信息包括对应于所述发送

方的设备标识符以及与所述智能设备与所述发送者之间的无线连接相关联的共享秘密。

[0158] 在示例51中,示例49至50中的任一项的主题可以任选地包括以下步骤:在接收到所述通信之前,确定所述可穿戴电子设备的身份信息;以及存储所述可穿戴电子设备的所述身份信息。

[0159] 在示例52中,示例51的主题可以任选地包括以下步骤:将所述发送方的所述身份信息与所述可穿戴电子设备的所存储的身份信息进行比较,以便判定所述发送方是否是所述可穿戴电子设备。

[0160] 在示例53中,示例49至52中的任一项的主题可以任选地包括:所述至少一个生物计量凭证基于所述用户的生物计量特性,所述生物计量特性包括语音、指纹、眼睛、面部特征和手部特征中的一项。

[0161] 在示例54中,示例49至53中的任一项的主题可以任选地包括:所述通信包括用于由所述智能设备启用语音识别的命令,并且进一步包括以下步骤:从所述可穿戴电子设备接收包括语音输入数据的后续通信。

[0162] 在示例55中,示例54的主题可以任选地包括以下步骤:将所述语音输入数据提供给所述智能设备上的个人助理应用。

[0163] 在示例56中,示例49至55中的任一项的主题可以任选地包括:接收认证结果,所述认证结果指示对指示用户的生物计量输入的输入数据的认证是否成功;以及基于所述认证结果而允许对所述智能设备上的应用和服务的选择性访问。

[0164] 示例57可包括一种用于保护数据的设备,所述设备包括用于执行如示例49至56中的任一项的方法的装置。

[0165] 在示例58中,示例57的主题可以任选地包括:用于执行所述方法的装置包括至少一个处理器和至少一个存储器元件。

[0166] 在示例59中,示例58的主题可以任选地包括:所述至少一个存储器元件包括机器可读指令,当执行所述机器可读指令时,所述机器可读指令使所述设备执行示例49至56中的任一项的方法。

[0167] 在示例60中,示例57至59中的任一项的主题可以任选地包括:所述设备是智能设备。

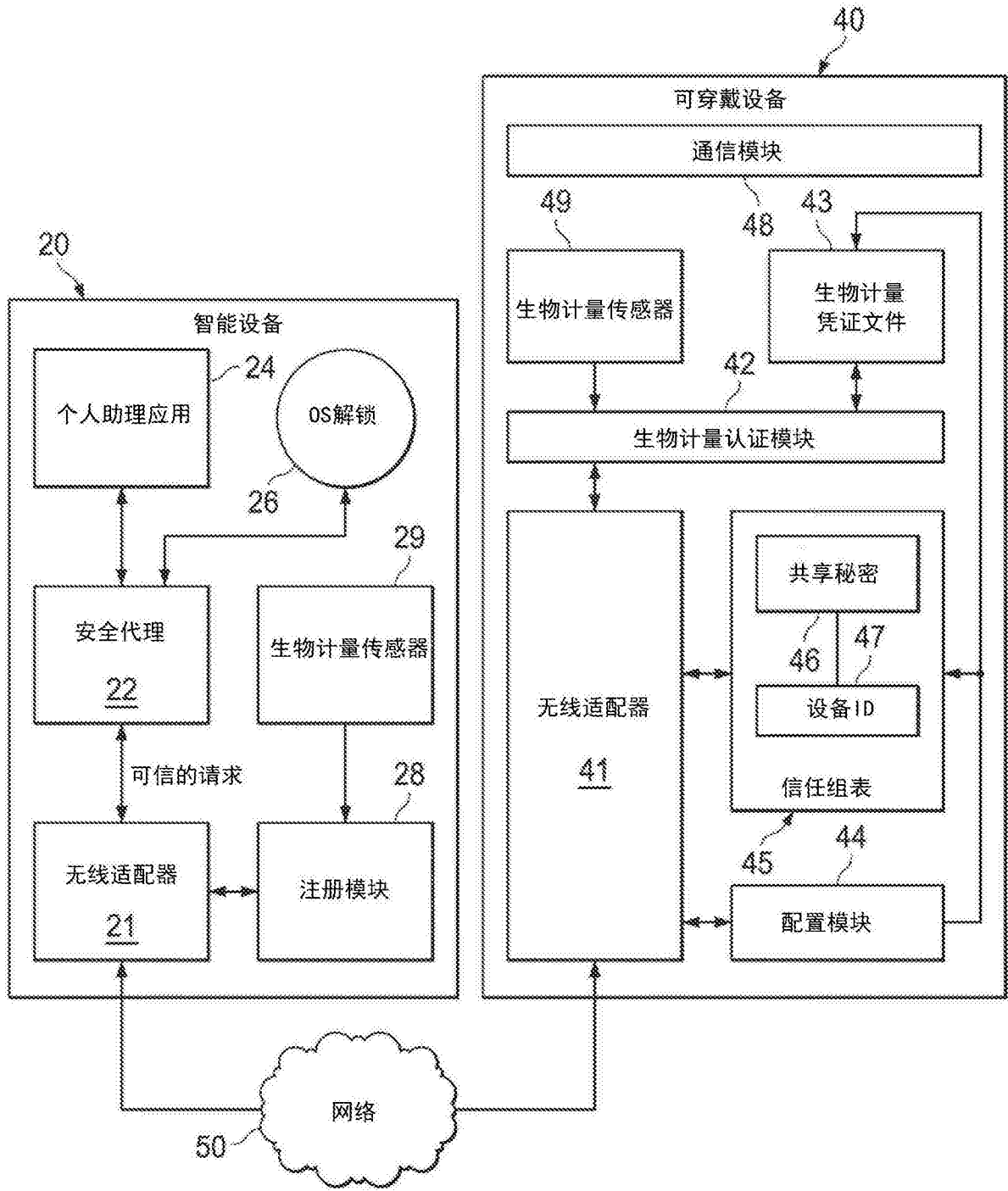


图1

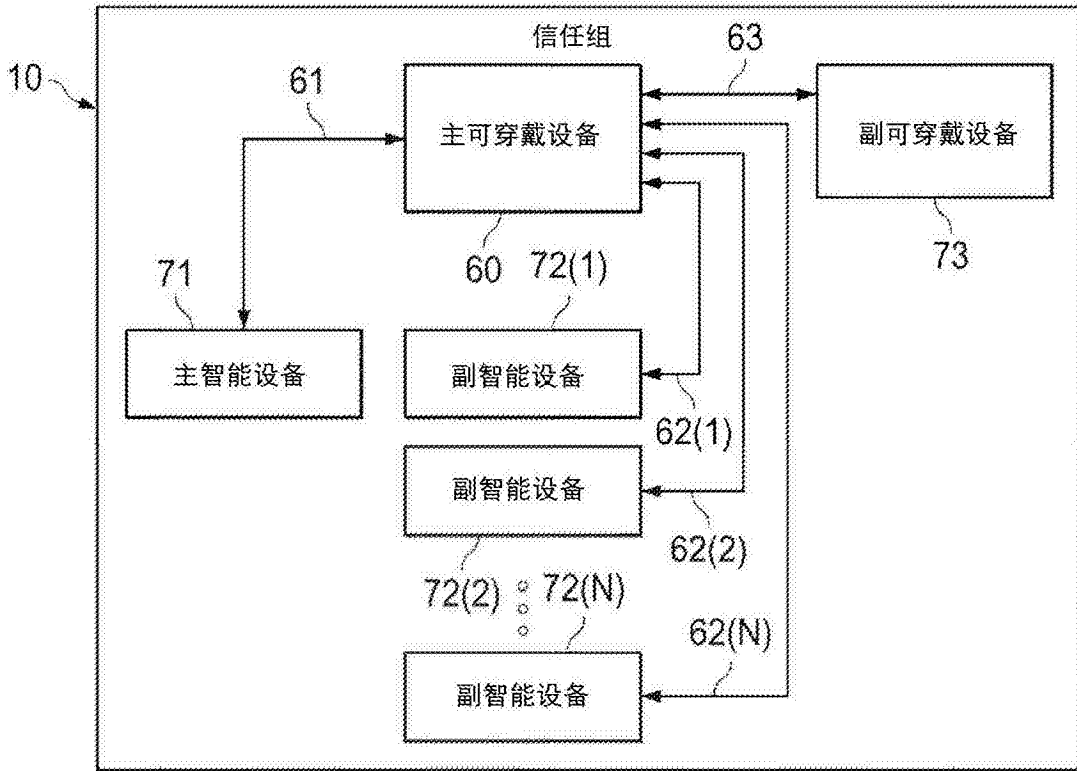


图2

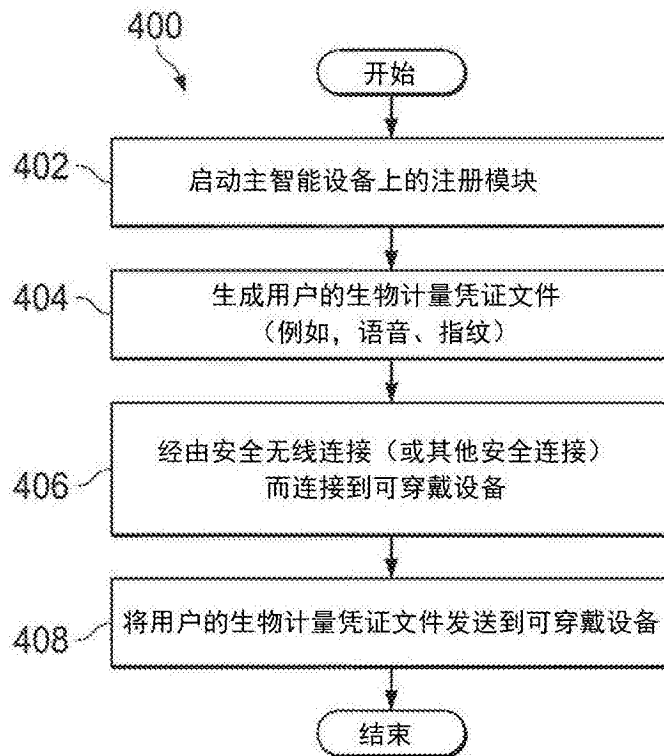


图4

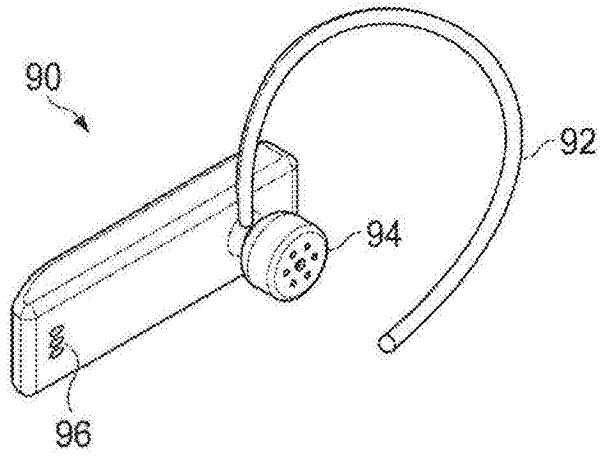


图3A

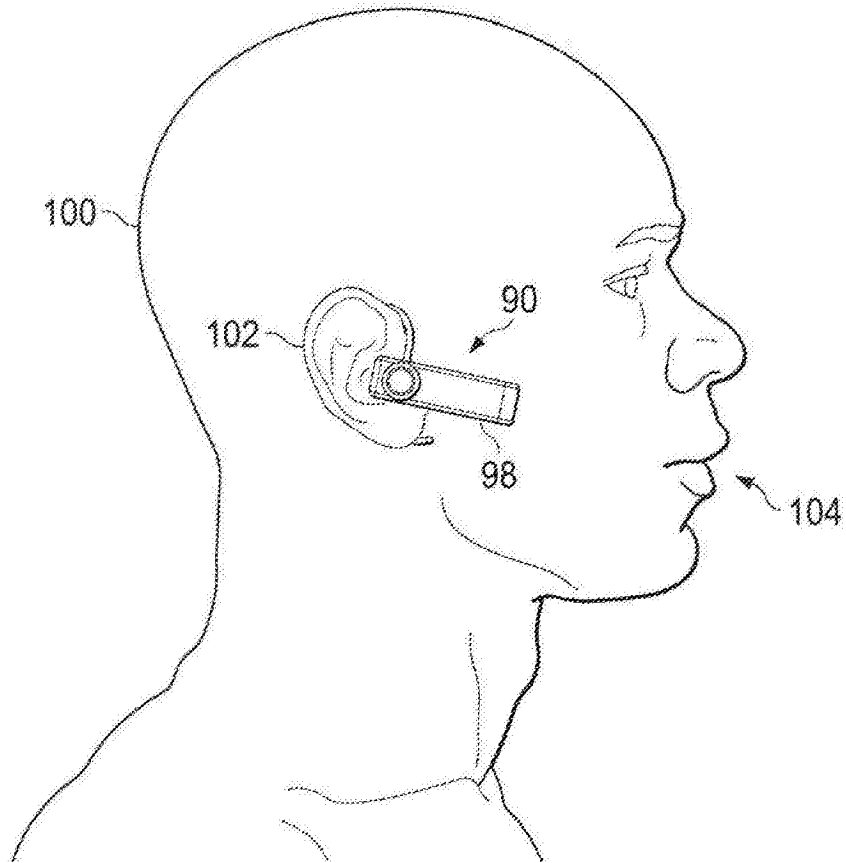


图3B

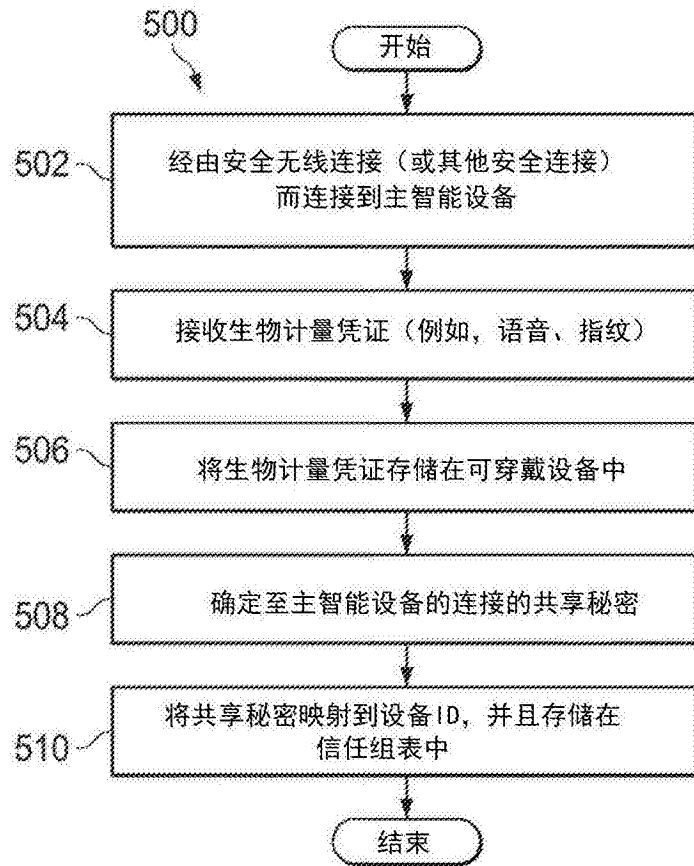


图5

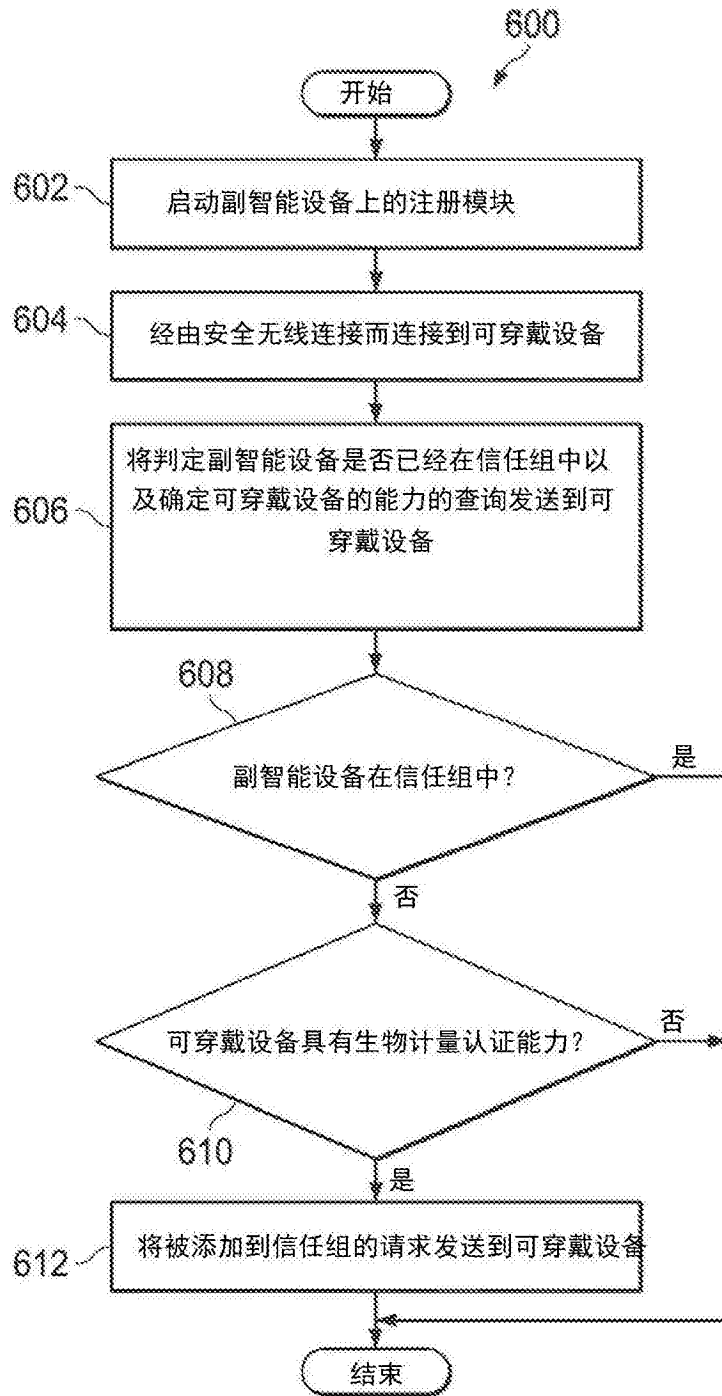


图6

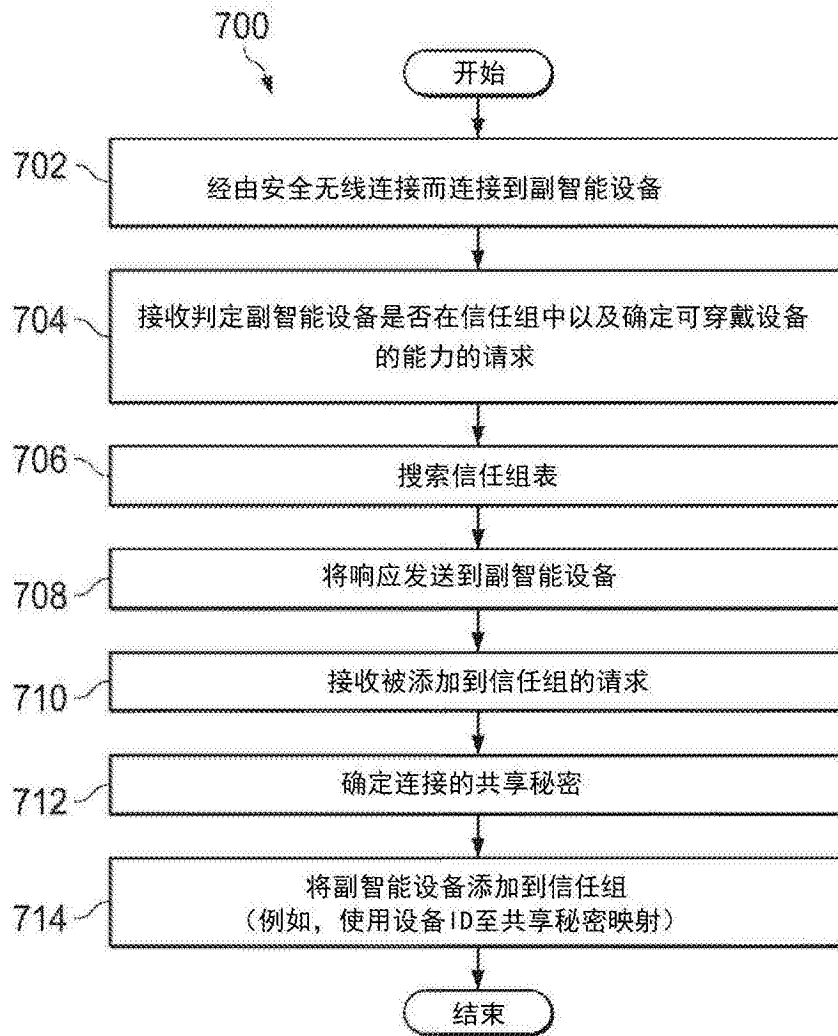


图7

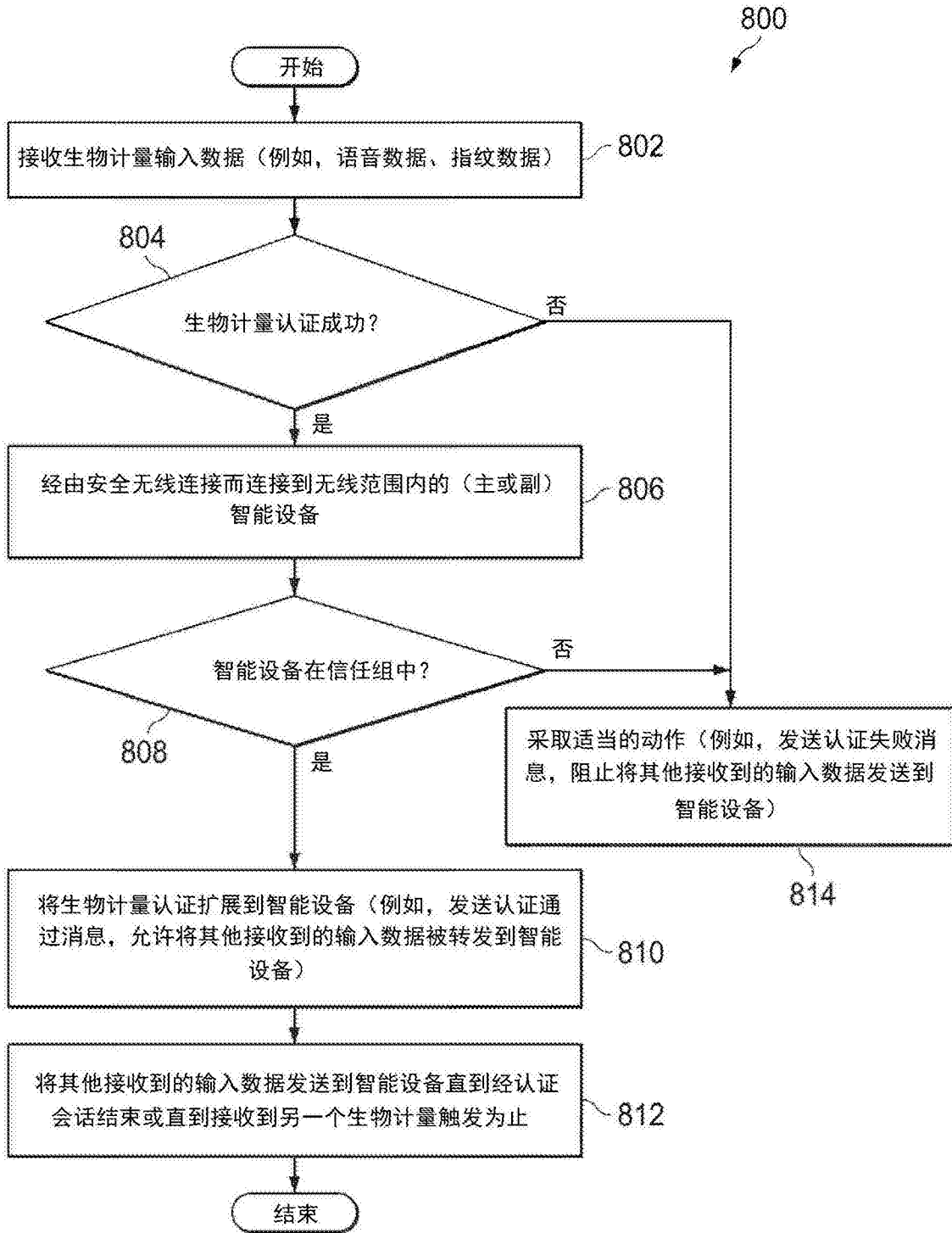


图8

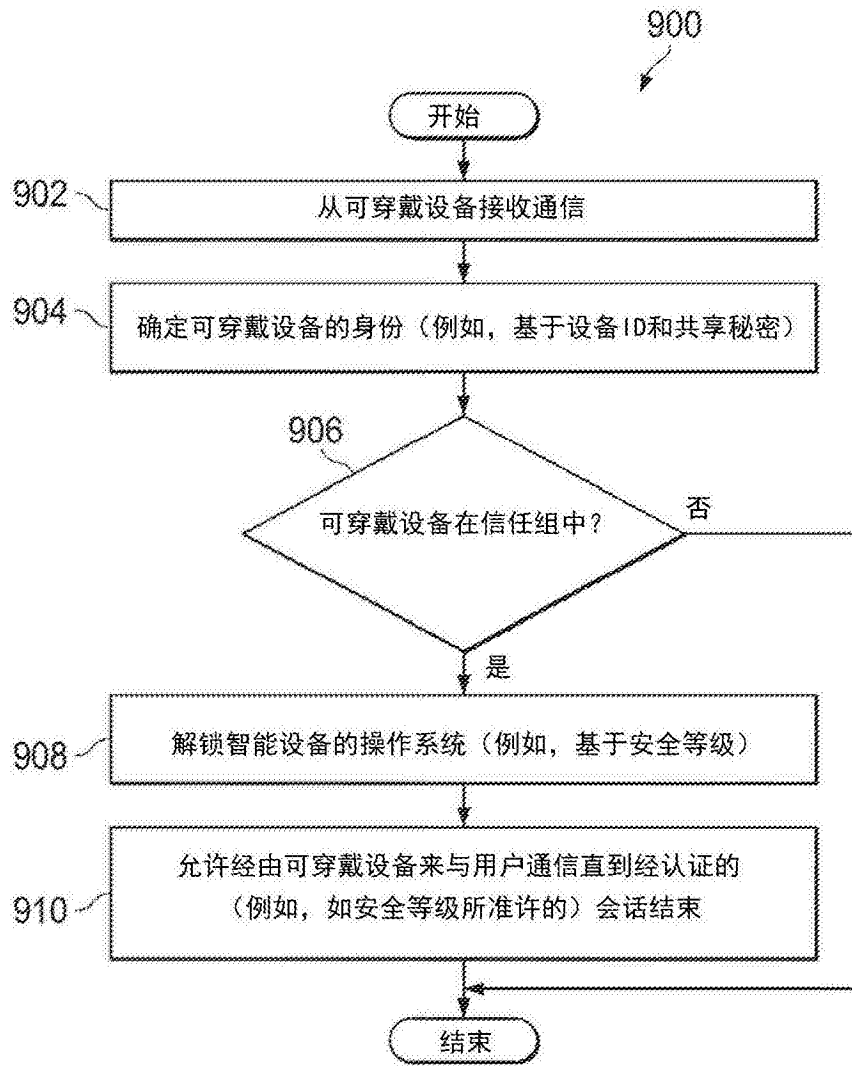


图9

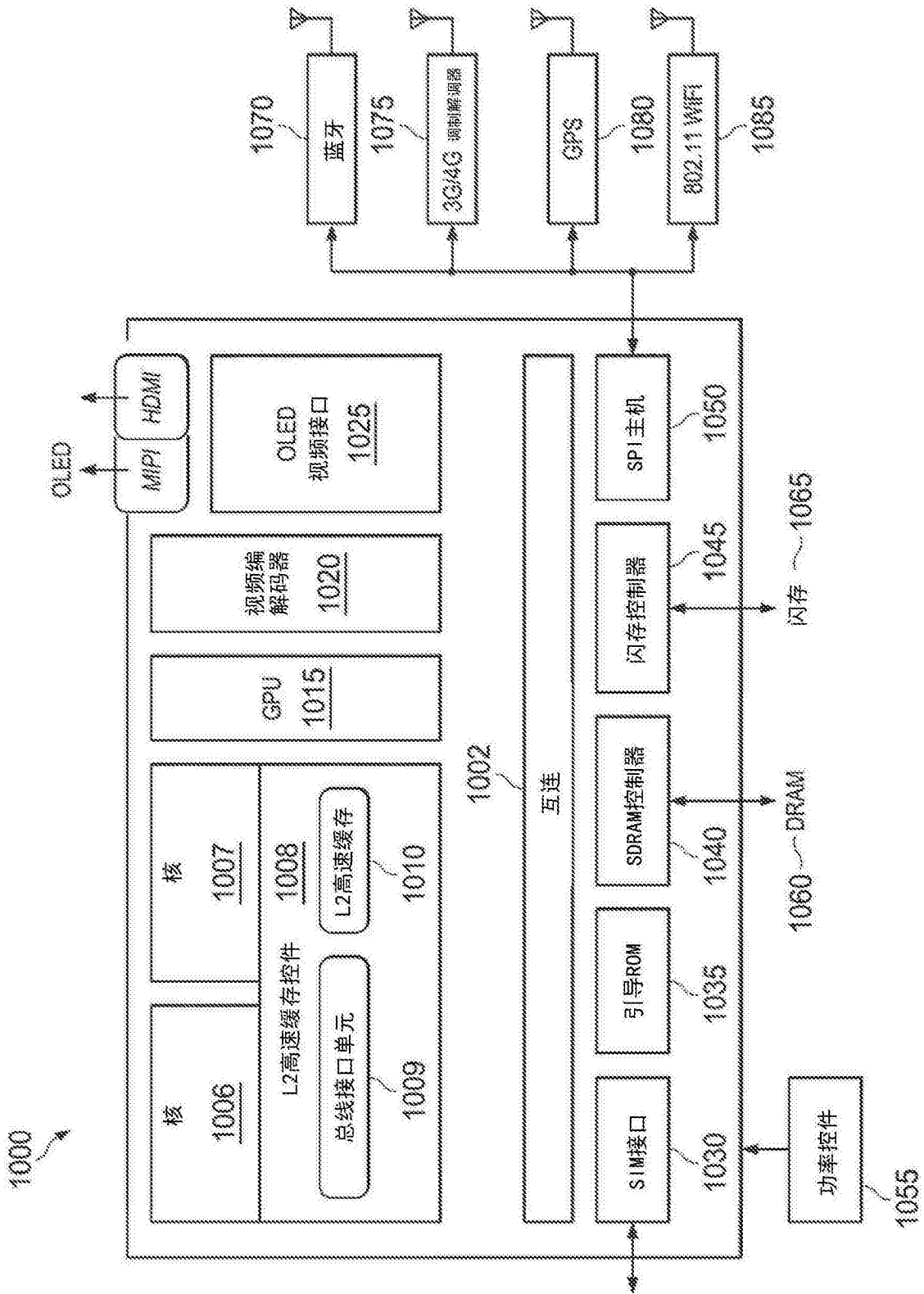


图10

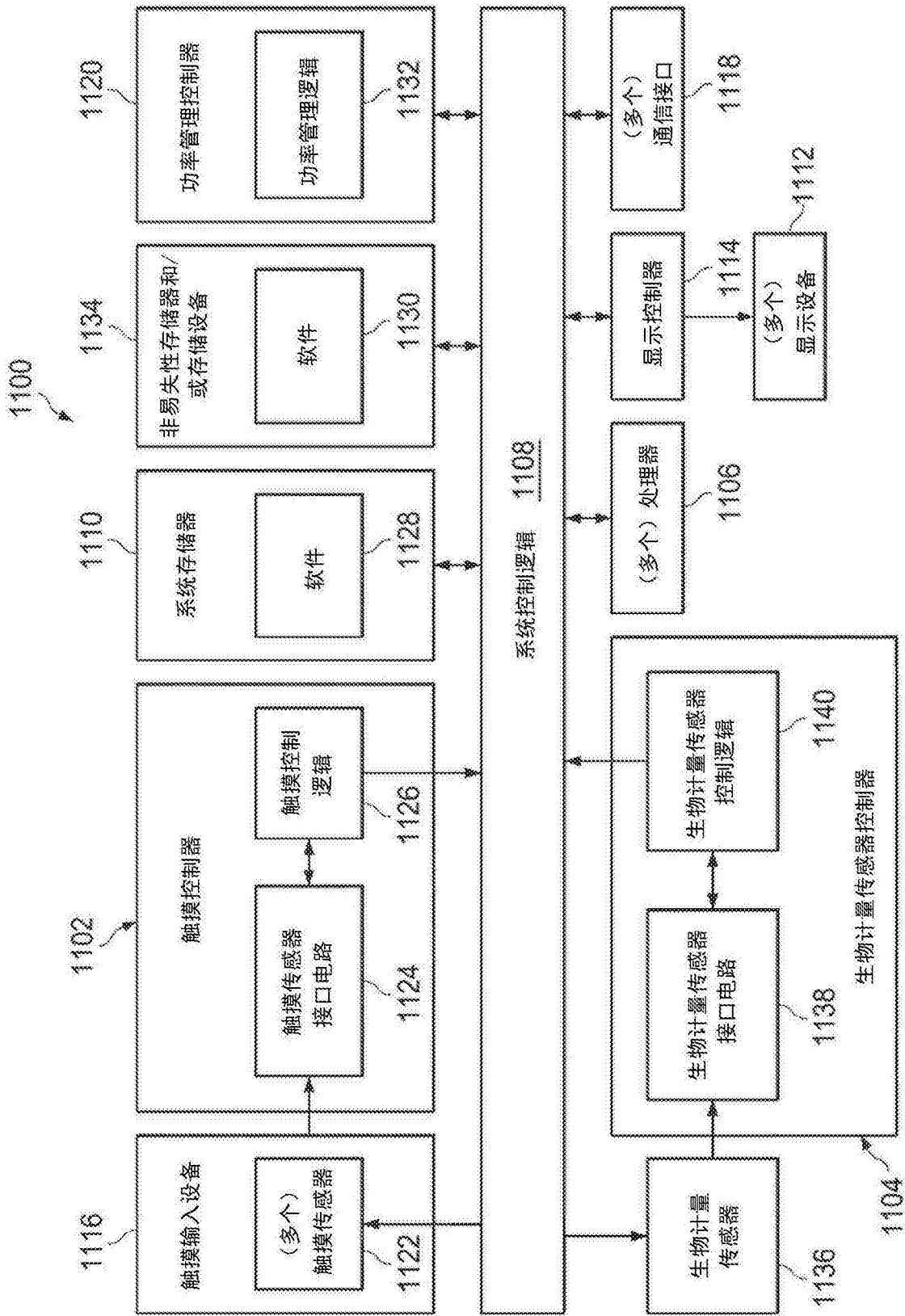


图11