



(12) 发明专利

(10) 授权公告号 CN 101015173 B

(45) 授权公告日 2013.06.19

(21) 申请号 200580029947.4

H04L 12/70(2013.01)

(22) 申请日 2005.08.31

(56) 对比文件

(30) 优先权数据

04104326.6 2004.09.08 EP

W0 2004025921 A, 2004.03.25, 全文.

US 2003095521 A1, 2003.05.22, 全文.

EP 0600695 A, 1994.06.08, 全文.

(85) PCT申请进入国家阶段日

2007.03.07

W0 2004036467 A, 2004.04.29, 全文.

W0 2004064339 A, 2004.07.29, 全文.

(86) PCT申请的申请数据

PCT/IB2005/052854 2005.08.31

US 2003065952 A1, 2003.04.03, 说明书

第1页0011、第2页0031、第3页0042、第4页0054-0058、图1、图2.

(87) PCT申请的公布数据

W02006/027725 EN 2006.03.16

CN 1444386 A, 2003.09.24, 说明书第7页第

10-21行、第8页第3段.

(73) 专利权人 皇家飞利浦电子股份有限公司

地址 荷兰艾恩德霍芬

审查员 范文婧

(72) 发明人 马克·沃克莱尔 哈维尔·塞雷特

莱昂内尔·G·艾蒂安

菲利普·托伊文

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 王英

(51) Int. Cl.

H04L 12/28(2006.01)

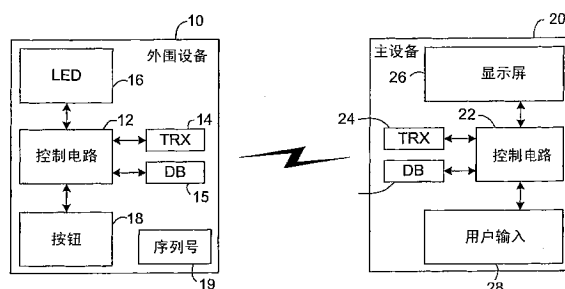
权利要求书4页 说明书10页 附图7页

(54) 发明名称

配对方法及相应的通信设备

(57) 摘要

在主通信设备和外围通信设备之间实现配对,以建立自组织无线或有线网络。在主设备上显示唯一相关于外围设备的设备ID。为了接受这个配对,用户需要确认显示在主设备上的设备ID与印在外围设备上的设备ID是匹配的,随后通过按压外围设备上的键,来完成配对过程,或者,如果在设备中实现了近距离通信(NFC)技术的话,则通过使外围设备与主设备相接触或靠得足够近,来完成配对过程。这样,无需外围设备上复杂的用户界面就实现了安全配对。



1. 一种将可信设备和第二设备予以配对的方法,所述方法包括:
所述第二设备接收要将所述第二设备与第一设备予以配对的请求;
所述第一设备和所述第二设备相互认证,以及,所述第二设备从所述第一设备获取与所述第一设备相关的设备 ID;
将所述第一设备设置为可信模式,在可信模式下,所述第一设备不与除所述第二设备之外的其它任何设备进行配对过程;
所述第二设备或用户从所述可信设备获取设备 ID;
所述第二设备或用户将来自所述可信设备的设备 ID 和在所述认证步骤中获取的设备 ID 进行比较;
如果相关于所述第一设备的设备 ID 和从所述可信设备获取的设备 ID 相匹配,则所述第二设备或用户将所述第一设备认定为所述可信设备,并向所述可信设备发送配对接受;以及
响应于接收到用户输入所述可信设备的第二配对接受,将所述可信设备和所述第二设备予以配对。
2. 如权利要求 1 所述的方法,
其中,从所述可信设备获取设备 ID 的步骤包括:用户阅读印在所述可信设备上的设备 ID;以及
其中,比较步骤包括:用户将显示在所述第二设备上的相关于所述第一设备的设备 ID 和印在所述可信设备上的设备 ID 进行视觉比较。
3. 如权利要求 1 所述的方法,其中,从所述可信设备获取设备 ID 的步骤包括:
激活介于所述可信设备和所述第二设备之间的短距离无线电链接;以及
将所述可信设备的设备 ID 发送给所述第二设备。
4. 如权利要求 3 所述的方法,其中,激活所述短距离无线电链接的步骤包括:
将所述第二设备与所述可信设备在物理上相接触。
5. 如权利要求 3 所述的方法,其中,激活所述短距离无线电链接的步骤包括:
移动所述第二设备,使之靠近所述可信设备。
6. 如权利要求 3、4 或 5 所述的方法,其中,所述短距离无线电链接使用近距离通信协议。
7. 如权利要求 3、4 或 5 所述的方法,其中,所述可信设备的设备 ID 存储于 RFID 标签中。
8. 如权利要求 1 所述的方法,其中,所述第一和第二设备:
在所述相互认证期间或在所述相互认证之后,建立公共密钥;
使用共享的公共密钥,以确保所述第一和第二设备之间的多个后续消息的真实性和先后顺序。
9. 如权利要求 1 所述的方法,其中,所述第二配对接受包括:
在所述可信设备上的单次按键。
10. 如权利要求 1 所述的方法,还包括:
在将所述第一设备设置为所述可信模式之后,所述第一设备告知所述第二设备,当所述第一设备处于所述可信模式下时,所述第一设备排它性地仅与所述第二设备配对。

11. 如权利要求 1 所述的方法,所述方法包括:

响应于接收到所述要将所述第二设备和所述第一设备予以配对的请求,从所述第二设备发送信标信号,其中,所述信标信号指明所述第二设备的 ID;以及

响应于从所述第二设备接收到所述信标信号,从所述第一设备发送响应信号。

12. 如权利要求 11 所述的方法,其中,所述信标信号中的所述第二设备的 ID 是唯一的。

13. 如权利要求 11 所述的方法,包括:

通过随机过程,生成所述第二设备的 ID。

14. 如权利要求 13 所述的方法,其中,所述随机过程两次生成的第二设备 ID 相同的概率是可忽略的。

15. 如权利要求 12、13 或 14 所述的方法,其中,所述第二设备的唯一 ID 可以从所述第二设备认证中直接计算出来。

16. 如权利要求 1 所述的方法,所述方法包括:

在认证所述第一设备后,在所述第一设备上指明所述第一设备处于配对过程中。

17. 如权利要求 16 所述的方法,包括:

通过所述第一设备上的指示灯,在所述第一设备上指明所述第一设备处于配对过程中。

18. 如权利要求 1 所述的方法,其中,与所述第一设备相关的设备 ID 唯一标识所述第一设备。

19. 如权利要求 18 所述的方法,包括:

通过随机过程,生成所述第一设备的 ID。

20. 如权利要求 19 所述的方法,其中,所述随机过程两次生成的第一设备 ID 相同的概率是可忽略的。

21. 如权利要求 18、19 或 20 所述的方法,其中,与所述第一设备相关的设备 ID 可以从所述第一设备认证中直接计算出来。

22. 如权利要求 1 所述的方法,其中,在配对步骤之后,所述方法还包括:

在所述第一和第二设备之间建立安全的自组织无线网络。

23. 如权利要求 22 所述的方法,其中,在所述第一和第二设备之间建立起安全的自组织无线网络之后,所述方法包括:

在所述第一和第二设备之间建立无线 USB 连接。

24. 一种外围通信设备,包括:

向主通信设备认证外围通信设备并且向所述主通信设备发送外围通信设备 ID 的模块;

向所述外围通信设备认证所述主通信设备并且接收所述主通信设备的 ID 的模块;

将所述外围通信设备设置为可信模式的模块,在所述可信模式下,所述外围通信设备不与除所述主通信设备之外的其它任何设备进行配对过程;

从用户接收配对接受输入并响应于所述配对接受输入而确认与所述主通信设备进行配对的模块。

25. 如权利要求 24 所述的外围通信设备,其中,所述外围通信设备还包括第二模块,所述第二模块用于向所述主通信设备发送所述外围通信设备 ID,所述第二模块使用短距离无

线电链接。

26. 如权利要求 25 所述的外围通信设备,其中,所述短距离无线电链接使用近距离通信协议。

27. 如权利要求 25 所述的外围通信设备,其中,所述第二模块包括 RFID 标签。

28. 如权利要求 24 至 27 中任一权利要求所述的外围通信设备,其中,所述外围通信设备还包括:

在与所述主通信设备进行认证期间或与所述主通信设备进行认证之后,与所述主通信设备建立公共密钥的模块;

使用所述密钥生成多个消息的模块,所述主通信设备能够验证所述多个消息的真实性、完整性和先后顺序;

验证由所述主通信设备用所述密钥生成的所述多个消息的真实性、完整性和先后顺序的模块。

29. 如权利要求 24 所述的外围通信设备,其中,所述外围通信设备 ID 唯一标识所述外围通信设备。

30. 如权利要求 24 所述的外围通信设备,其中,所述外围通信设备 ID 是随机过程的结果。

31. 如权利要求 30 所述的外围通信设备,其中,所述随机过程两次生成的外围通信设备 ID 相同的概率是可忽略的。

32. 如权利要求 24 所述的外围通信设备,所述外围通信设备包括:

从所述主通信设备接收信标信号并且发送响应信号的模块。

33. 如权利要求 24 所述的外围通信设备,所述外围通信设备包括:

指明模块,用于在认证所述外围通信设备后指明所述外围通信设备处于配对过程中。

34. 如权利要求 33 所述的外围通信设备,其中,所述指明模块包括所述外围通信设备上的灯。

35. 如权利要求 24 所述的外围通信设备,其用于与所述主通信设备建立无线 USB 连接。

36. 如权利要求 24 所述的外围通信设备,其用于与所述主通信设备建立网际协议连接。

37. 如权利要求 24 所述的外围通信设备,其中,来自用户的配对接受输入包括一次单独的按键。

38. 一种主通信设备,包括:

接收要将所述主通信设备与外围通信设备予以配对的请求的模块;

认证所述外围通信设备并从所述外围通信设备获取与所述外围通信设备相关的设备 ID 的模块;

向所述外围通信设备进行认证并向所述外围通信设备发送主通信设备 ID 的模块;

获取与可信设备相关的设备 ID 的模块;以及

将与所述外围通信设备相关的设备 ID 跟与所述可信设备相关的设备 ID 予以比较的模块;

当与所述外围通信设备相关的设备 ID 跟与所述可信设备相关的设备 ID 相匹配时,响应于从所述外围通信设备接收的配对确认,将所述主通信设备和所述外围通信设备予以配

对的模块。

39. 如权利要求 38 所述的主通信设备,其中,所述获取与所述外围通信设备相关的设备 ID 的模块包括与所述外围通信设备建立短距离无线电链接的模块。

40. 如权利要求 39 所述的主通信设备,其中,所述短距离无线电链接使用近距离通信协议。

41. 如权利要求 38 所述的主通信设备,其中,所述主通信设备还包括:

在与所述外围通信设备进行认证的期间或与所述外围通信设备进行认证之后,与所述外围通信设备建立公共密钥的模块;

使用所述密钥生成多个消息的模块,所述外围通信设备能够验证所述多个消息的真实性、完整性和先后顺序;

验证由所述外围通信设备用所述密钥生成的多个消息的真实性、完整性和先后顺序的模块。

42. 如权利要求 38 所述的主通信设备,其中,响应于接收到所述要将所述主通信设备和所述外围通信设备予以配对的请求,所述主通信设备发送信标信号,其中,所述信标信号指明所述主通信设备的 ID。

43. 如权利要求 38 所述的主通信设备,其中,与所述外围通信设备相关的设备 ID 唯一地标识了所述外围通信设备。

44. 如权利要求 38 所述的主通信设备,其中,与所述外围通信设备相关的设备 ID 是随机过程的结果。

45. 如权利要求 44 所述的主通信设备,其中,所述随机过程两次生成的与所述外围通信设备相关的设备 ID 相同的概率是可忽略的。

46. 如权利要求 38 所述的主通信设备,其中,所述主通信设备 ID 唯一地标识了所述主通信设备。

47. 如权利要求 38 所述的主通信设备,其用于与所述外围通信设备建立安全无线 USB 连接。

48. 如权利要求 38 所述的主通信设备,其用于与所述外围通信设备建立网际协议连接。

49. 如权利要求 38 所述的主通信设备,其中,所述主通信设备包括委托设备和受托设备,其中,所述委托设备向所述受托设备转发要将所述主通信设备与外围通信设备予以配对的请求,以及其中,所述受托设备代表所述委托设备,执行权利要求 1 所述的配对过程的至少一部分。

配对方法及相应的通信设备

发明领域

[0001] 本发明涉及有线和无线通信设备,具体而言,涉及实现有线或无线通信设备安全配对的方法和装置。

技术背景

[0002] 自组织无线网络日益普及,其中适当装配的无线设备可以相互间无线通信,从而避免了通过电缆连接两个设备的必要。

[0003] 为了使两个孤立的无线设备能够相互间安全地通信,并避免第三方设备探测和/或篡改从这两个设备之一发射的数据的可能性,就需要将上述设备予以配对。这个配对过程包括在所涉及的设备之间传送和建立“可信基础”信息。所述“可信基础”信息的作用是确保设备只与用户指定为可信的(例如,由于用户拥有或控制对方设备)通信对方进行通信。

[0004] 有很多无线通信标准,例如,蓝牙和 IEEE 802.11b/g,它们中的每一个都包括设备配对的机制。这些机制包括:用户输入一连串的符号(例如蓝牙的 10 进制数字,IEEE 802.11b 的无线等效私密(WEP)协议的 16 进制或 ASCII 字符),或者,使用副通信信道,该副通信信道由于其物理属性(例如 IEEE 802.11 接入点的以太网线,或近距离通信(NFC)),因此是安全的或被视为是安全的。

[0005] 然而,这些现有的配对机制是较难应用的,并且也可能极大地增加对设备的要求,这意味着很难将其成功地实现于商用产品中。这也就意味着很多部署都是不安全的。例如,可以在不加密的情况下实现 IEEE 802.11 网络,导致的结果是存在第三方偷听和/或篡改两个设备之间通信的隐患。在其它情况下,可能只为了实现配对操作的目的,无线设备就需要配备一个 USB 连接器,这毫无必要地增加了设备的成本。

[0006] 在主设备通过电缆或其它物理连接器直接或间接地连接到外围设备的有线网络中,配对机制的很多上述缺点也同样存在。

[0007] 因此,就存在着既不需要符号输入也不需要副安全通信信道的就能够实现通信设备简单安全配对的方法和装置的需求。

发明内容

[0008] 在本发明的一个方案中,提供了一种将可信设备和第二设备予以配对的方法,所述方法包括:所述第二设备接收要将所述第二设备与第一设备予以配对的请求;所述第一设备和所述第二设备相互认证,以及,所述第二设备从所述第一设备获取与所述第一设备相关的设备 ID;将所述第一设备设置为可信模式,在可信模式下,所述第一设备不与除所述第二设备之外的其它任何设备进行配对过程;所述第二设备或用户从所述可信设备获取设备 ID;所述第二设备或用户将来自所述可信设备的设备 ID 和在所述认证步骤中获取的设备 ID 进行比较;如果相关于所述第一设备的设备 ID 和从所述可信设备获取的设备 ID 相匹配,则所述第二设备或用户将所述第一设备认定为所述可信设备,并向所述可信设备发送配对接受;以及响应于接收到用户输入所述可信设备的第二配对接受,将所述可信设备

和所述第二设备予以配对。

[0009] 在如上所述的方法中,从所述可信设备获取设备 ID 的步骤包括:用户阅读印在所述可信设备上的设备 ID;并且,比较步骤包括:用户将显示在所述第二设备上的相关于所述第一设备的设备 ID 和印在所述可信设备上的设备 ID 进行视觉比较。

[0010] 在如上所述的方法中,从所述可信设备获取设备 ID 的步骤包括:激活介于所述可信设备和所述第二设备之间的短距离无线电链接;以及,将所述可信设备的设备 ID 发送给所述第二设备。其中,激活所述短距离无线电链接的步骤包括:将所述第二设备与所述可信设备在物理上相接触。可替换地,激活所述短距离无线电链接的步骤包括:移动所述第二设备,使之靠近所述可信设备。其中,所述短距离无线电链接使用近距离通信协议;所述可信设备的设备 ID 存储于 RFID 标签中。

[0011] 在如上所述的方法中,所述第一和第二设备在所述相互认证期间或在所述相互认证之后,建立公共密钥;使用共享的公共密钥,以确保所述第一和第二设备之间的多个后续消息的真实性和先后顺序。所述第二配对接受包括:在所述可信设备上的单次按键。

[0012] 如上所述的方法还包括:在将所述第一设备设置为所述可信模式之后,所述第一设备告知所述第二设备,当第一设备处于所述可信模式下时,所述第一设备排它性地仅与所述第二设备配对。

[0013] 如上所述的方法还包括:响应于接收到所述要将所述第二设备与所述第一设备予以配对的请求,从所述第二设备发送信标信号,其中,所述信标信号指明所述第二设备的 ID;以及响应于从所述第二设备接收到所述信标信号,从所述第一设备发送响应信号。其中,所述信标信号中的所述第二设备的 ID 是唯一的。该方法还包括:通过随机过程,生成所述第二设备的 ID。其中,所述随机过程两次生成的第二设备 ID 相同的概率是可忽略的。并且其中,所述第二设备的唯一 ID 可以从所述第二设备认证中直接计算出来。

[0014] 如上所述的方法还包括:在认证所述第一设备后,在所述第一设备上指明所述第一设备处于配对过程中。该方法还包括:通过所述第一设备上的指示灯,在所述第一设备上指明所述第一设备处于配对过程中。

[0015] 在如上所述的方法中,与所述第一设备相关的设备 ID 唯一标识所述第一设备。该方法包括:通过随机过程,生成所述第一设备的 ID。其中,所述随机过程两次生成的第一设备 ID 相同的概率是可忽略的。并且其中,与所述第一设备相关的设备 ID 可以从所述第一设备认证中直接计算出来。

[0016] 在如上所述的方法中,在配对步骤之后,所述方法还包括:在所述第一和第二设备之间建立安全的自组织无线通信网络。其中,在所述第一和第二设备之间建立起安全的自组织无线通信网络之后,所述方法包括:在所述第一和第二设备之间建立无线 USB 连接。

[0017] 在本发明的另一个方案中,提供了一种外围通信设备,包括:向主通信设备认证外围通信设备并且向所述主通信设备发送外围通信设备 ID 的模块;向所述外围通信设备认证所述主通信设备并且接收所述主通信设备的 ID 的模块;将所述外围通信设备设置为可信模式的模块,在所述可信模式下,所述外围通信设备不与除所述主通信设备之外的其它任何设备进行配对过程;从用户接收配对接受输入并响应于所述配对接受输入而确认与所述主通信设备进行配对的模块。

[0018] 在上述方案中,所述外围通信设备还包括第二模块,所述第二模块用于向所述主

通信设备发送所述外围通信设备 ID,所述第二模块使用短距离无线电链接。其中,所述短距离无线电链接使用近距离通信协议;所述第二模块包括 RFID 标签。

[0019] 在上述方案中,所述外围通信设备还包括:在与所述主通信设备进行认证期间或与所述主通信设备进行认证之后,与所述主通信设备建立公共密钥的模块;使用所述密钥生成多个消息的模块,所述主通信设备能够验证所述多个消息的真实性、完整性和先后顺序;验证由所述主通信设备用所述密钥生成的所述多个消息的真实性、完整性和先后顺序的模块。

[0020] 在上述方案的外围通信设备中,所述外围通信设备 ID 唯一标识所述外围通信设备;所述外围通信设备 ID 是随机过程的结果。其中,所述随机过程两次生成的外围通信设备 ID 相同的概率是可忽略的。

[0021] 在上述方案中,所述外围通信设备包括:从所述主通信设备接收信标信号并且发送响应信号的模块。所述外围通信设备包括:指明模块,用于在认证所述外围通信设备后指明所述外围通信设备处于配对过程中。其中,所述指明模块包括所述外围通信设备上的灯。

[0022] 在上述方案中,所述外围通信设备用于与所述主通信设备建立无线 USB 连接;用于与所述主通信设备建立网际协议连接。其中,来自用户的配对接受输入包括一次单独的按键。

[0023] 在本发明的另一个方案中,提供了一种主通信设备,包括:接收要将所述主通信设备与外围通信设备予以配对的请求的模块;认证所述外围通信设备并从所述外围通信设备获取与所述外围通信设备相关的设备 ID 的模块;向所述外围通信设备进行认证并向所述外围通信设备发送主通信设备 ID 的模块;获取与可信设备相关的设备 ID 的模块;以及将与所述外围通信设备相关的设备 ID 跟与所述可信设备相关的设备 ID 予以比较的模块;当与所述外围通信设备相关的设备 ID 跟与所述可信设备相关的设备 ID 相匹配时,响应于从所述外围通信设备接收的配对确认,将所述主通信设备和所述外围通信设备予以配对的模块。

[0024] 在上述方案的主通信设备中,所述获取与所述外围通信设备相关的设备 ID 的模块包括与所述外围通信设备建立短距离无线电链接的模块。所述短距离无线电链接使用近距离通信协议。

[0025] 在上述方案中,所述主通信设备还包括:在与所述外围通信设备进行认证的期间或与所述外围通信设备进行认证之后,与所述外围通信设备建立公共密钥的模块;使用所述密钥生成多个消息的模块,所述外围通信设备能够验证所述多个消息的真实性、完整性和先后顺序;验证由所述外围通信设备用所述密钥生成的多个消息的真实性、完整性和先后顺序的模块。

[0026] 在上述方案中,响应于接收到所述要将所述主通信设备和所述外围通信设备予以配对的请求,所述主通信设备发送信标信号,其中,所述信标信号指明所述主通信设备的 ID。并且其中,与所述外围通信设备相关的设备 ID 唯一地标识了所述外围通信设备。

[0027] 在上述方案的主通信设备中,与所述外围通信设备相关的设备 ID 是随机过程的结果。其中,所述随机过程两次生成的与所述外围通信设备相关的设备 ID 相同的概率是可忽略的。

[0028] 在上述方案的主通信设备中,所述主通信设备 ID 唯一地标识了所述主通信设备。

[0029] 在上述方案中,所述的主通信设备用于与所述外围通信设备建立安全无线 USB 连接;用于与所述外围通信设备建立网际协议连接。

[0030] 在上述方案中,所述主通信设备包括委托设备和受托设备,其中,所述委托设备向所述受托设备转发要将所述主通信设备与外围通信设备予以配对的请求,并且其中,所述受托设备代表所述委托设备,执行权利要求 1 所述的配对过程的至少一部分。

[0031] 因此本发明能使用户简单地执行设备配对,而不需要大幅增加设备(特别是那些为需要丰富功能用户界面的应用而构建的设备,例如,无线 USB“存储钥匙”)。因此,本发明提供的方法和装置能够以直截了当的方式,实现相对廉价设备的配对。从而,提高了用无线和有线网络实际实施的安全级别。

附图说明

[0032] 图 1 的框图示出了根据本发明的一个方面包括无线通信设备的自组织无线通信网络;

[0033] 图 2 示出了根据本发明第二方面在图 1 网络中执行的方法;

[0034] 图 3 的流程图进一步示出了图 2 的方法;

[0035] 图 4 的状态图示出了图 1 网络的设备中一个设备的运行;

[0036] 图 5 的状态图示出了图 1 网络中其它设备的运行;

[0037] 图 6 示出了根据本发明另一个实施例在图 1 网络中执行的方法;

[0038] 图 7 的流程图进一步示出了图 6 的方法。

具体实施方式

[0039] 虽然在本文中将根据本发明描述成实现在无线网络方式中,但应理解的是,本发明也适用于主设备通过电缆或其它物理连接器直接或间接连接到外围设备的有线网络。

[0040] 图 1 的框图示出的两个电子设备 10 和 20 通过无线连接形成了自组织无线网络。

[0041] 在所示出的本发明的这个实施例中,第一电子设备 10 作为外围设备,而第二电子设备 20 作为主设备。例如,第一电子设备 10 可以是便携式存储器设备、移动电话免提装置或无线网络接入点(例如 Wi-Fi 接入点),而第二电子设备 20 可以是照相机、移动电话或个人计算机,所形成的自组织无线网络使数据能够从第一设备 10 传输到第二设备 20。在这种情况下,所形成的自组织无线网络根据无线 USB(通用串行总线)(WUSB)协议使第一设备 10 和第二设备 20 能够通信。但是,第一和第二设备可以根据任何无线或有线协议进行通信,例如,IEEE 802.15 和 IEEE 802.11 标准系列、蓝牙、Zigbee、以太网或 IP 等。

[0042] 应该理解的是,第一和第二电子设备都可能是很复杂的,因此,为了易于理解,本文中只将它们描述到能够理解本发明的程度上,也就是说,能够理解将通信设备予以配对以实现在其间安全通信的方法的程度上。

[0043] 外围第一电子设备 10 的控制电路 12 的形式是经过适当编程的处理器。控制电路 12 也具有实现设备 10 的主要功能所需的其它特征,但这里只描述与设备配对建立相关的那些特征。将控制电路 12 连接到收发器(TRX)电路 14,该收发器电路 14 处理与能够使用同一无线协议的其它电子设备的无线电频率通信。

[0044] 控制电路 12 连接到数据库(DB)15,后者储存着与设备 10 进行配对的设备相关的

信息。

[0045] 由于第一电子设备的运行相对简单,因此并没有提供复杂的用户界面。而只提供了 LED 16 和单个按钮 18,LED 16 在控制电路 12 的控制下运行,用户可以按下按钮 18 来向控制电路 12 发送信号。

[0046] 唯一标识第一电子设备 10 的序列号 19 以用户可读的形式写在设备的外面。

[0047] 主第二电子设备 20 的控制电路 22 的形式是经过适当编程的处理器。控制电路 22 也具有实现设备 20 的主要功能所需的其它特征,但这里只描述与设备配对建立相关的那些特征。将控制电路 22 连接到收发器(TRX)电路 24,该收发器电路 24 处理与能够使用同一无线协议的其它电子设备的无线电频率通信。

[0048] 控制电路 22 也连接到数据库(DB)25,后者储存着与设备 20 进行配对的设备相关的信息。

[0049] 由于第二电子设备比第一电子设备复杂的多,因此提供了较复杂的用户界面。在本实例中,提供了在控制电路 22 的控制下运行的显示屏 26,其可以向用户显示诸如详细消息或菜单选项之类的信息。第二电子设备也配备有用户输入 28,其例如可以包括小键盘和一个或多个滚动键,使用户能够从提供的菜单中进行选择,以向控制电路 22 发送信号。

[0050] 在图 2 至 7 所示的本发明的实施例中,用户希望将“可信”主设备 20 与“可信”外围设备 10 予以配对。如果,例如,用户拥有主设备或外围设备,且它们正是用户希望配对的设备,则该主设备和外围设备被视为是受“可信”的。因此,处于主设备 20 射程范围内的第三方设备不被视为是受“可信”的设备。

[0051] 简要地说,图 2 至 7 所示的方法提供了将第一通信设备 10 (外围设备)与第二通信设备 20 (主设备)予以配对的手段。首先,在第二设备和第一设备之间执行相互认证。在这个阶段,与第二设备通信的第一设备有可能不是用户拥有的第一设备(即,其不是“可信”设备)。

[0052] 因此,根据本发明各种实施例的方法提供了一种验证手段,用户通过该验证手段,能够验证与第二设备通信的第一设备确实是“可信”设备,或者反之。此外,这些方法对不同类型的攻击具有很好的鲁棒性。

[0053] 下面将结合示出了在设备间发送信号的图 2、示出了主设备 20 执行的步骤的图 3、示出了外围设备 10 状态的图 4 以及示出了主设备 20 状态的图 5,描述根据本发明第一实施例的第一和第二电子设备 10 和 20 的配对过程。

[0054] 如图 2 所示,配对过程可以开始于第一和第二电子设备 10 和 20 都加电的时候(在图 2 中分别是步骤 S1 和 S2)。设备都进入了其相应的空闲状态 102 和 202。

[0055] 当用户为了,例如,能够在第一和第二电子设备 10 和 20 之间传输数据,而希望在这两个设备之间建立自组织无线网络时,用户按所需的那样对设备 20 进行操作,以控制该处理过程。例如,为了初始化这个处理过程,用户可以使用用户输入 28 从菜单中选择配对选项。

[0056] 然后,在图 3 的步骤 P1 中,主设备 20 搜寻附近的外围设备。具体而言,其通过发送包括其 ID 的信标信号(图 2 中的 S3)来搜寻附近的外围设备。

[0057] 外围设备 10 检测到 ID 信号,并进入其链接初始化状态 106 的信标检测子状态 104。然后,外围设备 10 回复一个包括其 ID 的声明(图 2 的 S4),并进入其声明的子状态

108。

[0058] 在图 3 处理过程的步骤 P2 中,主设备 20 接收到外围设备 ID,然后将其传递给步骤 P3,在步骤 P3 中执行相互认证过程。

[0059] 在本发明的这个示出的实施例中,相互认证过程通常是基于使用“公钥”密码的传统密码认证过程。第一和第二设备 10 和 20 进入其相应的认证状态 110 和 204。主设备 20 向外围设备 10 发送不可预测的挑战(图 2 中的 S5)。随后,外围设备 10 通过利用私钥的信息,以生成也包括其自身公钥的响应,来处理该挑战(图 2 的 S6)。最后,主设备使用传送过来的与外围设备的私钥唯一对应的公钥,来验证响应的正确性。

[0060] 随后,重复挑战—响应消息交换(图 2 中的 S5 和 S6),其中主设备和外围设备的角色交换,从而实现相互认证。例如根据 STS (站对站) 协议、SSL (安全套接层) 协议或 SSH (安全外壳) 协议,为了最小化消息交换的次数,如何捎带这两个设备发出的挑战 and 响应在本领域内是众所周知的。

[0061] 本领域普通技术人员应理解的是,相互设备认证可以使用各种不同的协议和算法。能够使用的协议包括,例如, EAP-TTLS、EAP-PEAP、STS、Diffie-Hellman 或 EC/DH。能够使用的算法包括,例如, RSA、DSA 或 ECDSA。

[0062] 已知的是,可以使用三种主要技术将公钥与设备 ID 相对应。一种是使用由可信机构签署的将这两个值绑定在一起的证书(例如 X509)。另一种是执行公钥的密码摘要(例如 SHA-1),以直接获得设备 ID。第三种是执行包含公钥的文件(例如 X509 证书)的密码摘要(例如 SHA-1)。

[0063] 在这种情况下,当与主设备 20 进行认证时,外围设备 10 将其自己的打印序列号 19 与其公钥相对应。

[0064] 在本领域中还已知的是,发送的设备 ID 可以是随机过程的结果,例如其可以是使用随机(或伪随机)数生成的,该随机过程两次生成同样设备 ID 的概率是可忽略的。

[0065] 作为认证过程的副产品,主设备 20 和外围设备 10 生成公共密钥,其用于保证在两个设备之间所有后续消息交换的安全。

[0066] 当执行了认证过程后,第一和第二设备 10 和 20 在它们对应的配对设备数据库 15 和 25 中检查它们是否实际上已经与相应的其它设备配对了。如果是的话,则第一和第二设备 10 和 20 进入它们对应的已配对状态 112 和 206,于是,它们就能够执行安全无线(或有线)通信(状态 114 和 208),直到它们中的一个或两个断电的时候为止。

[0067] 另一方面,如果第一和第二设备确定它们还没有与相应的其它设备进行配对(图 2 中 S7),则第一和第二设备 10 和 20 进入它们对应的准备配对状态 116 和 210。

[0068] 在图 3 所示的处理过程的步骤 P4 中,主设备 20 请求初始化与外围设备 10 的配对过程。具体而言,它发送一个配对请求信号(图 2 中的 S8)给外围设备,第一和第二设备 10 和 20 进入它们对应的配对状态 118 和 212。然后,外围设备 10 返回一个配对开始信号(图 2 中的 S9)给主设备 20,第一和第二设备 10 和 20 进入它们对应的配对开始状态 120 和 214。

[0069] 于是,在本发明的这个示出的实施例中,外围设备 10 上的 LED16 开始闪烁,以向用户表明配对已经在处理过程中(图 2 中的 S 10 和 S11)。也可以使用其它简单的信令机制。在这个阶段(图 3 过程中的步骤 P5),外围设备 10 进入这里被称作“可信关键部分”的状态。在可信关键部分中,保证第一可信设备只与用于配对目的的特定第二设备进行通信。

[0070] 在图 3 所示的处理过程的步骤 P6 中,主设备 20 将外围设备 10 的 ID 呈现给用户。具体而言,其在显示屏 26 上(图 2 中的 S12)显示外围设备的 ID。在本发明的这个示出的实施例中,该 ID 唯一地标识了外围设备 10。但是,在本发明的其它实施例中,ID 可以仅仅标识外围设备,这样一来,附近其它任何外围设备能共享这个 ID 就变得非常不太可能。例如,ID 可以是对外围设备 10 的公钥执行哈希函数的结果。

[0071] 于是,在本发明的这个示出的实施例中,用户为了确认(图 3 中的步骤 P7)所述两个 ID 相匹配,所需要做的只是将实际印在第一设备 10 上面的设备 ID 19 与在第二设备 20 的显示屏 26 上显示的设备 ID 相比较。如果相匹配,则用户例如通过按压在主设备 20 上用户输入 28 上的“OK”键(图 2 中的 S13),就接受了所呈现的设备 ID (图 3 中的步骤 P8)。

[0072] 如果,例如在这个阶段,外围设备 10 从第三方主设备接收到第二配对请求信号(图 2 的 S14),则其返回配对等待信号(图 2 中的 S15),这样,与第三方设备进行配对就不会继续下去。

[0073] 否则,主设备 20 届时向外围设备 10 发送配对确认信号(图 2 中的 S16),并在其显示屏 26 上向用户呈现一条消息,以表明用户可以通过按压第一设备 10 上的按钮 18 来接受配对(图 2 中的 S17)。这样,就不用再输入密码或复杂的符号序列了。随后,第一和第二设备 10 和 20 进入它们对应的配对确认状态 122 和 216。

[0074] 然后,外围设备 10 发送配对应答信号(图 2 中的 S18)给主设备 20,该主设备 20 进入其配对应答状态 218,而此时外围设备 10 退出可信关键部分(图 3 过程中的步骤 P9),LED 16 停止闪烁。

[0075] 在图 3 所示的处理过程的步骤 P10 中,配对过程完成了,第一和第二设备 10 和 20 随后进入它们对应的已配对状态 112 和 206,主设备 20 在其显示屏 26 上确认其已经与外围设备 10 配对了(图 2 中的 S19)。最后,设备 10 和 20 都在其对应的配对设备数据库 15 和 25 中存储另一方设备的标识符。

[0076] 如图 2 所示,在第一设备 10 进入其配对开始状态 120 时启动定时器。如果在设定的时间段内(此例中是 30 秒)配对没有完成,则第一设备 10 返回到其准备配对状态 116,并向第二设备 20 发送一个配对等待消息。接收到这个消息后,第二设备 20 通过在其显示屏 26 上显示消息,将该情况告知用户,一旦配对等待消息中指定的时间(例如 30 秒)结束后,就返回到其准备配对状态 210。

[0077] 由于用户信任第一设备(例如因为用户拥有该设备),并且用户信任第二设备(例如,因为用户拥有该设备),因此这个配对协议的安全性就提高了。结果是,第二设备没有欺骗用户,第一设备也没有欺骗用户,具体而言就是,第一设备没有欺骗第二设备。

[0078] 在本发明的另一个实施例中,第一电子设备 10 和第二电子设备 20 包括与相应的收发器电路 14 和 24 分开的附加电路,其实现短距离无线电链路上设备之间的通信。该短距离无线电链路使用的协议不同于设备之间主要传输所使用的协议。该附加电路可使用的一种这样协议可以由 ECMA 在近距离通信(NFC)接口和协议(NFCIP-1)中提出的协议,其在 13.56MHz 上发送。在另一个实施例中,第二电子设备 20 包括与收发器电路 24 分开的附加电路,其实现与第一电子设备 10 中的 NFC 令牌(例如 RFID 标签)通信。

[0079] 图 6 和 7 示出了根据本发明另一个实施例执行的方法。图 6 的中步骤 S1 至 S11 的描述以及图 7 中的步骤 P1 至 P5 的描述,和上面结合图 2 和 3 的对应描述是一样的。

[0080] 在图 6 中的步骤 S11 和图 7 中的步骤 P5 后,第一设备 10 处于“可信关键部分”状态,在该状态中,其保证一次只与一个第二设备进行配对过程。

[0081] 在图 7 示出的处理过程的步骤 P6A 中,主设备 20 向用户呈现指令,该指令使用另一种协议初始化设备之间的通信。具体而言,如果协议是 NFC 协议,则设备 20 在显示屏 26 上显示(图 3 中的 S20)将主设备 20 与可信外围设备 10 (即用户拥有的外围设备)相接触的指令。或者,可以将主设备 20 与可信外围设备 10 靠得足够近,从而使用 NFC 协议初始化通信。

[0082] 一旦用户将两个设备相接触或将两个设备靠得足够近(图 6 中的 S21 和图 7 中的 P7A),就激活了 NFC 接口,于是,就将外围设备 10 的 ID (在步骤 P2 中,如果第一设备 10 确实是可信外围设备的话,则也将其提供给第二设备)发送给第二设备 20 (步骤 S22)。除了将这两个设备接触或接近之外,这个传输过程不需要用户进行任何干预。在另一个实施例中,将 NFC 接口激活,信号激活 NFC 令牌,该 NFC 令牌将外围设备 ID 发送给第二设备 20。

[0083] 在本发明的这个实施例中,ID 唯一地标识了外围设备 10。但是,在本发明的其它实施例中,ID 可以仅仅标识外围设备,这样一来,附近其它任何外围设备能共享这个 ID 就变得非常不太可能。例如,ID 可以是对外围设备 10 的公钥执行哈希函数的结果。

[0084] 在本发明这个示出的实施例中,第二设备 20 将在步骤 S22 和 P7A 中接收的设备 ID 与步骤 P2 中从第一设备接收的设备 ID 相比较,从而确认(图 7 中的步骤 P7B)两个 ID 相匹配。

[0085] 如果,例如在这个阶段,外围设备 10 从第三方主设备接收到第二配对请求信号(图 6 中的 S14),则其返回配对等待信号(图 6 中的 S15),并且不会继续与第三方设备进行配对。

[0086] 否则,如果第二设备 20 确定 ID 确实匹配,则第二设备 20 接受第一设备 10 (图 7 中的步骤 P7B),并向外围设备 10 发送配对确认信号(图 6 中的 S16),并在其显示屏 26 上向呈现消息,表明用户可以通过按压第一设备 10 上的按钮 18 (图 7 中的步骤 P8)来接受配对(图 6 中的 S17)。这样,就不用再输入密码或复杂的符号序列了。第一和第二设备 10 和 20 随后进入它们对应的配对确认状态 122 和 216。

[0087] 然后,外围设备 10 发送配对应答信号(图 6 中的 S18)给主设备 20,该主设备 20 进入其配对应答状态 218,而此时外围设备 10 退出可信关键部分(图 7 过程中的步骤 P9),LED 16 停止闪烁。

[0088] 在图 7 所示的处理过程的步骤 P10 中,配对过程完成,第一和第二设备 10 和 20 随后进入它们对应的已配对状态 112 和 206,主设备 20 在其显示屏 26 上确认其已经与外围设备 10 配对了(图 6 中的 S19)。最后,设备 10 和 20 都在其对应的配对设备数据库 15 和 25 中存储另一方设备的标识符。

[0089] 跟本发明的第一实施例相同,在第一设备 10 进入其配对开始状态 120 时启动定时器。如果在设定的时间段内(此例中是 30 秒)配对没有完成,则第一设备 10 返回到其准备配对状态 116,并向第二设备 20 发送一个配对等待消息。接收到这个消息后,第二设备 20 通过在其显示屏 26 上显示消息,将该情况告知用户,一旦配对等待消息中指定的时间(例如 30 秒)结束后,就返回到其准备配对状态 210。

[0090] 为了说明这个配对过程的安全性,将考虑系统对攻击该过程的各种尝试做出的反

应。

[0091] 在第一种可能的攻击中,第三方的外围设备与用户的外围设备 10 是相同的类型。如果第三方的外围设备使用其自己的声明来响应信标信号(图 2 中的 S3),并成功地与主设备 20 进行认证的话,则结果将是,在本发明第一实施例在图 3 过程内的步骤 P6 中,呈现在主设备 20 的显示屏 26 上的将是第三方外围设备的设备 ID。然后,用户可以通过例如按压第二设备 20 的用户输入 28 上的“NO”键,来拒绝请求的配对。

[0092] 因此,尽管其验证了第三方设备,但用户的主设备 20 不会欺骗用户,所以,其呈现的设备 ID 不匹配印在用户外围设备 10 (可信设备)上的设备 ID。因此,用户拥有发现攻击并拒绝配对所需的所有信息。

[0093] 在本发明的另一个实施例中,设备使用 NFC 或另一个短距离无线电链接,此时,执行图 7 中步骤 P6A 的结果将是,用户的外围设备 10 的 ID 将被发送给主设备 20。随后,将该 ID 与在声明步骤中(图 6 的 S4)从第三方外围设备接收的 ID 相比较。主设备 20 将确定这两个 ID 不匹配,并拒绝配对。

[0094] 在第二种可能的攻击中,第三方的主设备与用户的主设备 20 可能相同或不同。当外围设备 10 处于其准备配对状态 210 且在从用户主设备 20 发送配对请求(图 2 或图 6 中的 S8)前的这个时候,第三方主设备初始化与外围设备的配对过程。作为响应,外围设备 10 的 LED 16 开始闪烁,如上所述。但是,用户主设备 20 能够确定第三方设备当前正与外围设备进行配对,并可以将其显示在它的显示屏 26 上,以警告用户。同时,该用户主设备 20 进入它的配对等待状态 220。由于用户不了解此第三方设备的情况,所以他不会按压外围设备上的按钮 18,而是等待 LED 16 停止闪烁。当 LED 16 停止闪烁时,外围设备使第三方设备在一段时间内处于“隔离”状态,并可恢复与用户主设备 20 的配对过程。

[0095] 因此,当用户的外围设备 10 进入可信关键状态时,响应于配对请求信号 S8,其将会通过回复一个配对等待信号,将其此时不能进行配对的情况告知用户主设备 20。这是由上述可信流程来保证的。这使得用户主设备 20 能够在其显示屏 26 上列出外围设备 10,同时警告用户外围设备 10 正在与第三方设备配对。因此,用户同样拥有发现该情况并拒绝跟第三方设备进行配对所需的所有信息。

[0096] 在第三个可能的攻击中,第三方的主设备可能与用户的主设备 20 相同或不同类型。当外围设备 10 处于其配对状态 212 的时候,第三方搜寻用户的外围设备,并指示它自己的主设备开始配对过程。如上所述,外围设备 10 从第三方主设备接收到第二配对请求信号(图 2 和 6 中的 S14),并返回配对等待信号(图 2 和 6 中的 S15),以拒绝第三方配对请求,并且不会继续与第三方设备进行配对。

[0097] 因此,无论第三方设备采用何种实施方式,这些攻击都能被拒绝。

[0098] 为了保证用户了解需要遵从的处理过程,为了成功阻止对配对过程的攻击,第二设备 20 的显示屏 26 上将向用户提供合适的指示,从而可以指示用户只响应来自第二设备 20 的指示而操纵可信外围设备 10。

[0099] 在本发明的另一个实施例中,可以将上述主设备的功能分在两个成对设备中,即分在委托设备和受托设备中,委托设备和受托设备一起充当一个单独的主设备,以用于将委托设备和外围设备予以配对。

[0100] 在这个实施例中,委托设备把实施配对过程的职责委托给委托设备自身和已跟委

托设备完成配对的受托设备的外围设备。这种委托可以使用 RADIUS 协议来实现。

[0101] 由此,即便当两个设备之一的用户界面非常简单时,例如当仅一个 LED 作为显示装置和仅一个按钮作为用户输入时,本发明也提供了实现将这两个设备进行安全配对的配对过程。

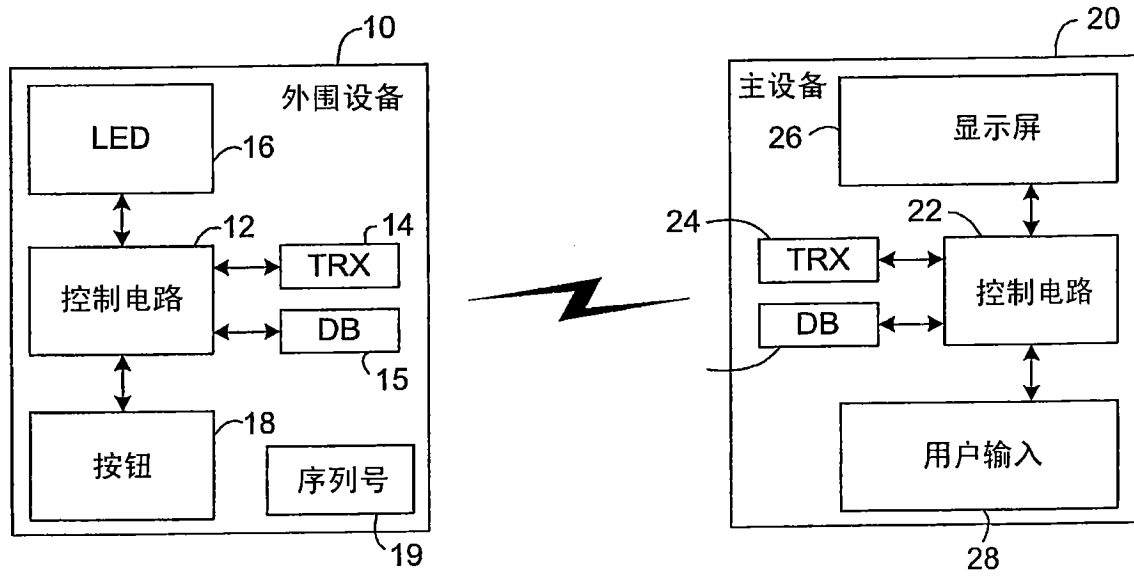


图1

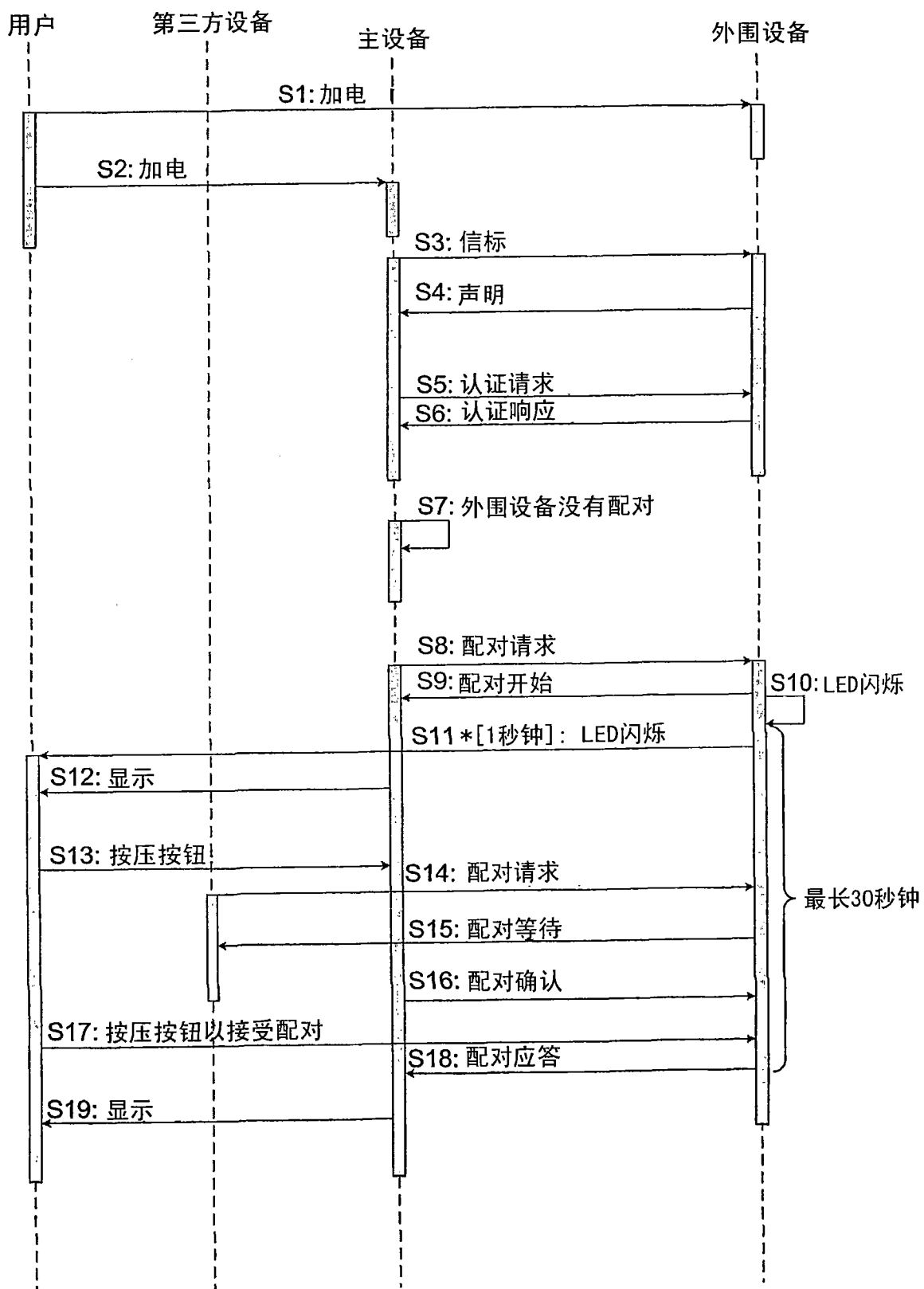


图2

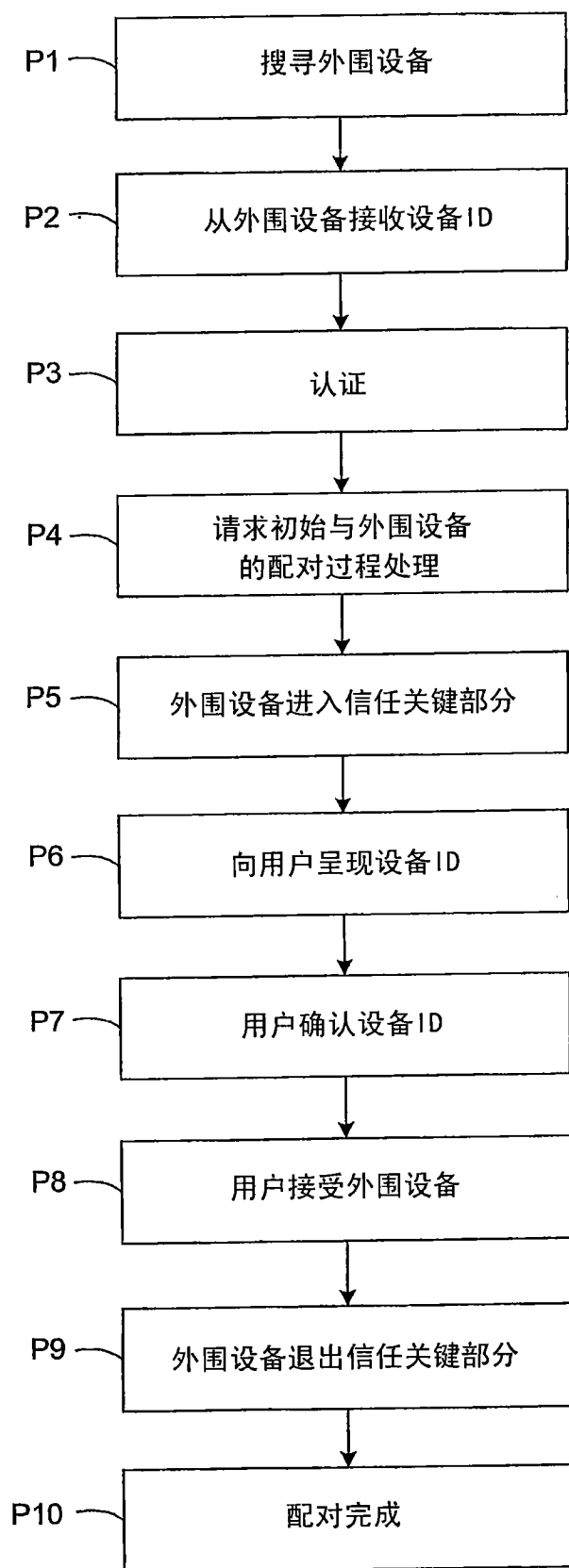


图3

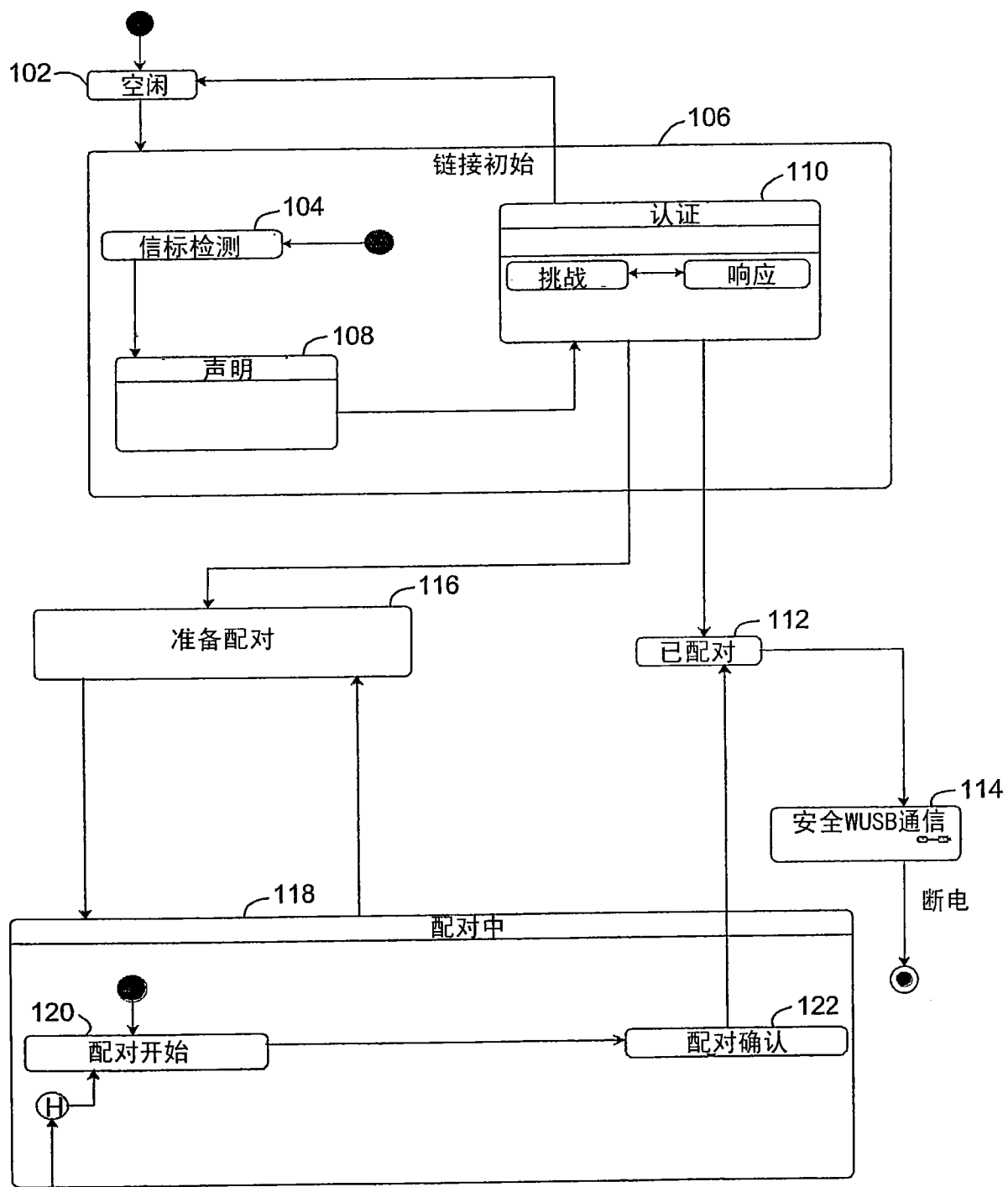


图4

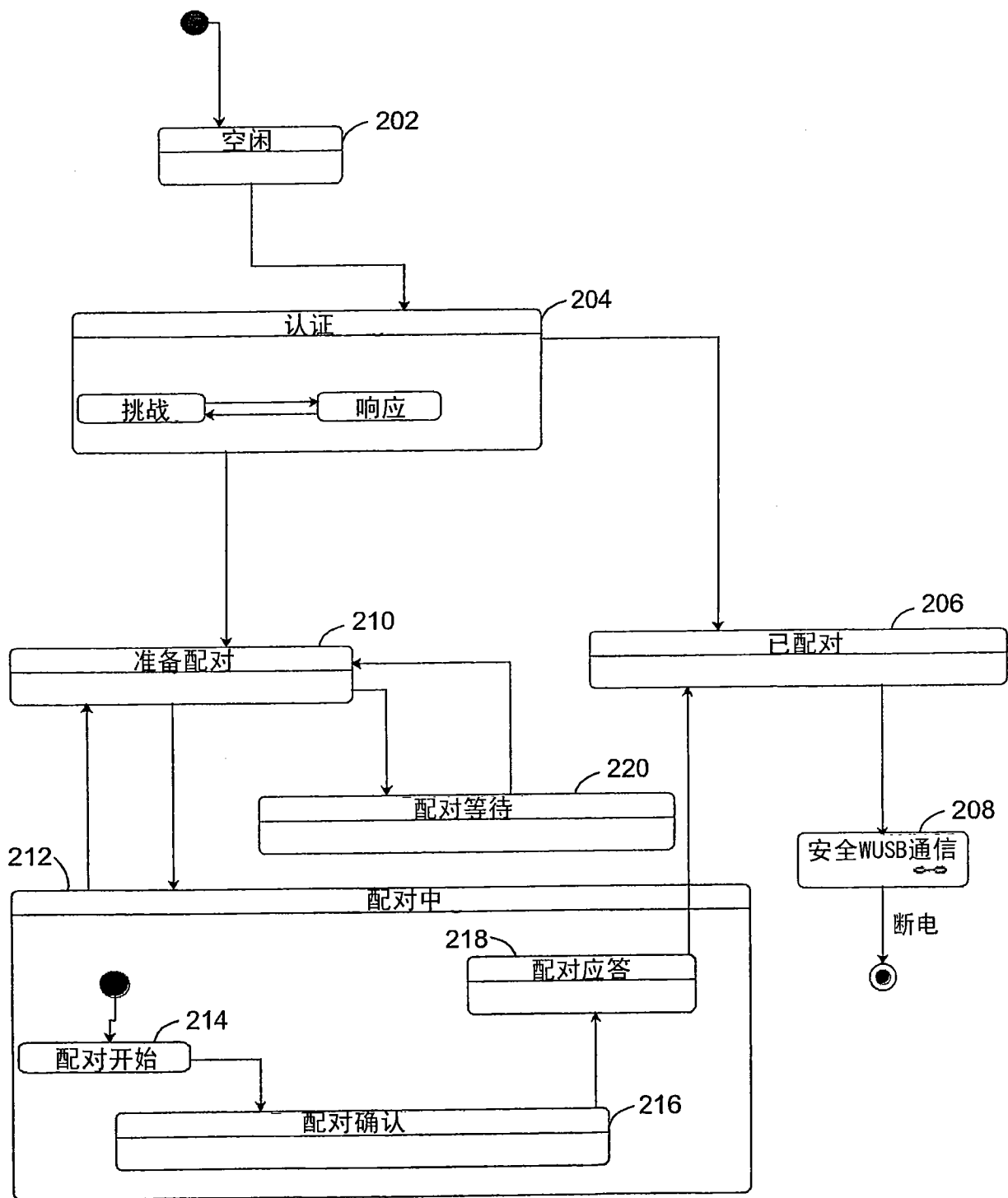


图5

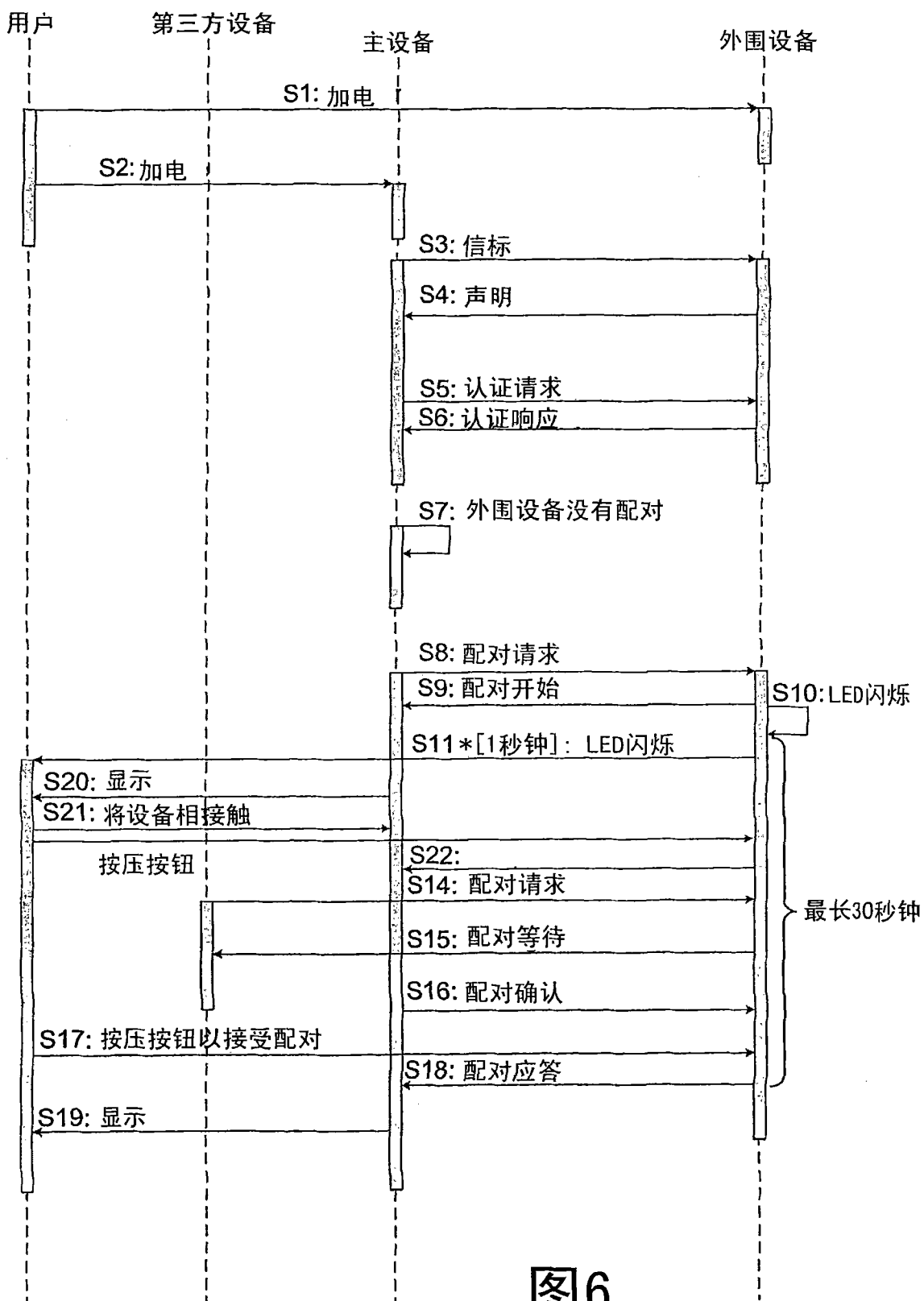


图6

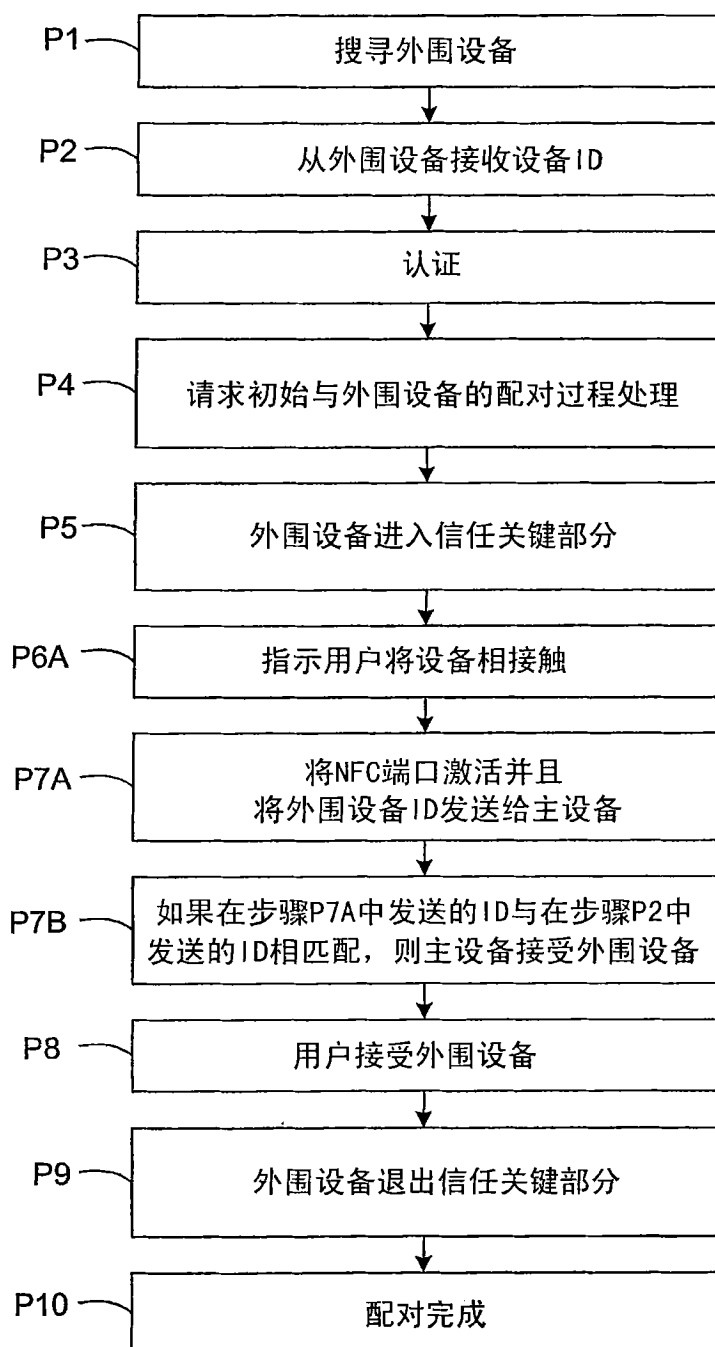


图7