



(12)发明专利申请

(10)申请公布号 CN 108901023 A

(43)申请公布日 2018. 11. 27

(21)申请号 201810886445.2

(22)申请日 2018.08.06

(71)申请人 佛山市甜慕链客科技有限公司

地址 528500 广东省佛山市高明区荷城街道泰和路454号

(72)发明人 刘聪玲

(74)专利代理机构 佛山粤进知识产权代理事务所(普通合伙) 44463

代理人 张敏

(51) Int. Cl.

H04W 12/06(2009.01)

H04L 29/06(2006.01)

H04W 12/02(2009.01)

H04W 76/14(2018.01)

H04W 76/16(2018.01)

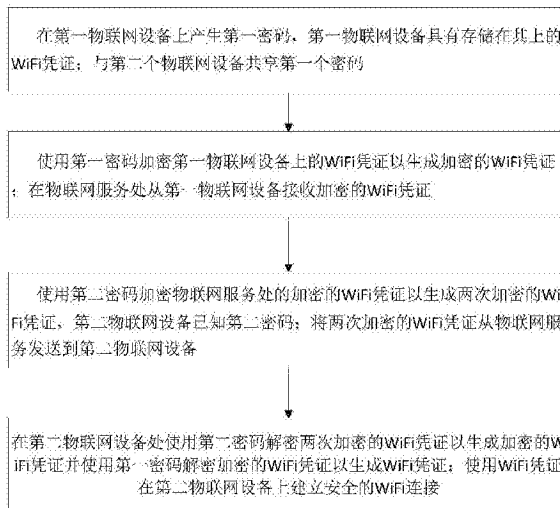
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种在物联网设备之间共享WiFi的方法及系统

(57)摘要

本发明公开了一种在物联网设备之间共享WiFi的方法及系统,包括:第一密码,在物联网服务处从第一物联网设备接收加密的WiFi凭证;使用第二密码加密物联网服务处的加密的WiFi凭证以生成两次加密的WiFi凭证,第二物联网设备已知第二密码;将两次加密的WiFi凭证从物联网服务发送到第二物联网设备;在第二物联网设备处使用第二密码解密两次加密的WiFi凭证以生成加密的WiFi凭证并使用第一密码解密加密的WiFi凭证以生成WiFi凭证;使用WiFi凭证在第二物联网设备上建立安全的WiFi连接。



1. 一种在物联网设备之间共享WiFi的方法,其特征在于,包括:
在第一物联网设备上产生第一密码,第一物联网设备具有存储在其上的WiFi凭证;
与第二个物联网设备共享第一个密码;
使用第一密码加密第一物联网设备上的WiFi凭证以生成加密的WiFi凭证;
在物联网服务处从第一物联网设备接收加密的WiFi凭证;
使用第二密码加密物联网服务处的加密的WiFi凭证以生成两次加密的WiFi凭证,第二物联网设备已知第二密码;
将两次加密的WiFi凭证从物联网服务发送到第二物联网设备;
在第二物联网设备处使用第二密码解密两次加密的WiFi凭证以生成加密的WiFi凭证
并使用第一密码解密加密的WiFi凭证以生成WiFi凭证;使用WiFi凭证在第二物联网设备上建立安全的WiFi连接。
2. 如权利要求1所述的方法,其特征在于,与所述第二物联网设备共享所述第一密码包括:
经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道。
3. 如权利要求2所述的方法,其特征在于,生成所述第一密码包括生成随机随机数。
4. 如权利要求3所述的方法,其特征在于,第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。
5. 如权利要求1所述的方法,其特征在于,还包括:
在物联网服务上生成服务公钥和服务私钥;在物联网设备上生成设备公钥和设备私钥;
将服务公钥从物联网服务发送到物联网设备,并将设备公钥从物联网设备发送到物联网服务;
使用设备公钥和服务私钥生成第二密码;
使用服务公钥和设备私钥生成相同的第二密码。
6. 如权利要求5所述的方法,其特征在于,硬件安全模块(HSM)执行第二密码的生成。
7. 如权利要求2所述的方法,其特征在于,还包括:
在第二物联网设备和客户端设备之间建立蓝牙低功耗(BTLE)通信信道;和
在第一物联网设备和客户端设备之间建立BTLE和/或WiFi连接。
8. 一种在物联网设备之间共享WiFi的系统,其特征在于,包括:
第一物联网设备,用于生成第一密码,第一物联网设备具有存储在其上的WiFi凭证;
第二个装置;
第一物联网设备与第二物联网设备共享第一密码并使用第一密码加密WiFi凭证以生成加密的WiFi凭证;
用于从第一物联网设备接收加密的WiFi凭证的物联网服务;使用第二密码加密加密的WiFi凭证以生成两次加密的WiFi凭证的物联网服务,第二物联网设备已知第二密码;
用于将两次加密的WiFi凭证从物联网服务发送到第二物联网设备的物联网服务;
第二物联网设备,使用第二密码解密两次加密的WiFi凭证,以生成加密的WiFi凭证,并使用第一密码解密加密的WiFi凭证,以生成WiFi凭证;和
第二个用于使用WiFi凭证建立安全WiFi连接的设备。

9. 如权利要求8所述的系统,其特征在于,与所述第二物联网设备共享所述第一密码包括:

经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道;其中生成所述第一密码包括生成随机现时;其中第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。

10. 如权利要求8所述的系统,其特征在于,还包括:

物联网服务,用于生成服务公钥和服务私钥;

物联网设备生成设备公钥和设备私钥;

将服务公钥发送给物联网设备的物联网服务和将设备公钥发送给物联网服务的物联网设备;

其中,使用设备公钥和服务私钥生成第二密码,并且使用服务公钥和设备私钥生成相同的第二密码。

一种在物联网设备之间共享WiFi的方法及系统

技术领域

[0001] 本发明涉及物联网技术领域,具体而言,涉及一种在物联网设备之间共享WiFi的方法及系统。

背景技术

[0002] “物联网”指的是互联网基础设施中唯一可识别的嵌入式设备的互连。最终,物联网有望产生新的,广泛类型的应用,其中几乎任何类型的物理事物都可以提供关于其自身或其周围环境的信息和/或可以通过因特网上的客户端设备远程控制。

[0003] 某些物联网设备可以被配置为通过WiFi网络建立通信信道。通常,当用户添加多个WiFi物联网设备时,用户将需要识别WiFi网络并在设置期间输入每个单独的物联网设备的密码。也就是说,用户需要输入他们的WiFi网络和密码N次才能配置N个设备。用户在设置第一设备时仅进入一次WiFi网络和密码,并且在设置所有后续设备时,他们将自动从任何先前设置的设备获得Wifi网络和密码。也就是说,用户需要输入他们的Wifi网络和密码1次来配置N个设备。

发明内容

[0004] 本发明提出了一种在物联网设备之间共享WiFi的方法,包括:

[0005] 在第一物联网设备上产生第一密码,第一物联网设备具有存储在其上的WiFi凭证;

[0006] 与第二个物联网设备共享第一个密码;

[0007] 使用第一密码加密第一物联网设备上的WiFi凭证以生成加密的WiFi凭证;

[0008] 在物联网服务处从第一物联网设备接收加密的WiFi凭证;

[0009] 使用第二密码加密物联网服务处的加密的WiFi凭证以生成两次加密的WiFi凭证,第二物联网设备已知第二密码;

[0010] 将两次加密的WiFi凭证从物联网服务发送到第二物联网设备;

[0011] 在第二物联网设备处使用第二密码解密两次加密的WiFi凭证以生成加密的WiFi凭证并使用第一密码解密加密的WiFi凭证以生成WiFi凭证;使用WiFi凭证在第二物联网设备上建立安全的WiFi连接。

[0012] 所述的方法,与所述第二物联网设备共享所述第一密码包括:

[0013] 经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道。

[0014] 所述的方法,生成所述第一密码包括生成随机随机数。

[0015] 所述的方法,第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。

[0016] 所述的方法,还包括:

[0017] 在物联网服务上生成服务公钥和服务私钥;在物联网设备上生成设备公钥和设备私钥;

- [0018] 将服务公钥从物联网服务发送到物联网设备,并将设备公钥从物联网设备发送到物联网服务;
- [0019] 使用设备公钥和服务私钥生成第二密码;
- [0020] 使用服务公钥和设备私钥生成相同的第二密码。
- [0021] 所述的方法,硬件安全模块(HSM)执行第二密码的生成。
- [0022] 所述的方法,还包括:
- [0023] 在第二物联网设备和客户端设备之间建立蓝牙低功耗(BTLE)通信信道;和
- [0024] 在第一物联网设备和客户端设备之间建立BTLE和/或WiFi连接。
- [0025] 一种在物联网设备之间共享WiFi的系统,包括:
- [0026] 第一物联网设备,用于生成第一密码,第一物联网设备具有存储在其上的WiFi凭证;
- [0027] 第二个装置;
- [0028] 第一物联网设备与第二物联网设备共享第一密码并使用第一密码加密WiFi凭证以生成加密的WiFi凭证;
- [0029] 用于从第一物联网设备接收加密的WiFi凭证的物联网服务;使用第二密码加密加密的WiFi凭证以生成两次加密的WiFi凭证的物联网服务,第二物联网设备已知第二密码;
- [0030] 用于将两次加密的WiFi凭证从物联网服务发送到第二物联网设备的物联网服务;
- [0031] 第二物联网设备,使用第二密码解密两次加密的WiFi凭证,以生成加密的WiFi凭证,并使用第一密码解密加密的WiFi凭证,以生成WiFi凭证;和
- [0032] 第二个用于使用WiFi凭证建立安全WiFi连接的设备。
- [0033] 所述的系统,与所述第二物联网设备共享所述第一密码包括:
- [0034] 经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道;其中生成所述第一密码包括生成随机现时;其中第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。
- [0035] 所述的系统,还包括:
- [0036] 物联网服务,用于生成服务公钥和服务私钥;
- [0037] 物联网设备生成设备公钥和设备私钥;
- [0038] 将服务公钥发送给物联网设备的物联网服务和将设备公钥发送给物联网服务的物联网设备;
- [0039] 其中,使用设备公钥和服务私钥生成第二密码,并且使用服务公钥和设备私钥生成相同的第二密码。

附图说明

[0040] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制,而是将重点放在示出实施例的原理上。在图中,在不同的视图中,相同的附图标记指定对应的部分。

[0041] 图1是本发明的一种在物联网设备之间共享WiFi的方法的示意图。

具体实施方式

[0042] 为了使得本发明的目的、技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明;应当理解,此处所描述的具体实施例仅用于解释本发明,并不用于限定本发明。对于本领域技术人员而言,在查阅以下详细描述之后,本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内、包括在本发明的范围内,并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征,并且这些特征根据以下将详细描述将是显而易见的。

[0043] 实施例一:

[0044] 如图1所示,是本发明的一种在物联网设备之间共享WiFi的方法的示意图,包括:

[0045] 在第一物联网设备上产生第一密码,第一物联网设备具有存储在其上的WiFi凭证;

[0046] 与第二个物联网设备共享第一个密码;

[0047] 使用第一密码加密第一物联网设备上的WiFi凭证以生成加密的WiFi凭证;

[0048] 在物联网服务处从第一物联网设备接收加密的WiFi凭证;

[0049] 使用第二密码加密物联网服务处的加密的WiFi凭证以生成两次加密的WiFi凭证,第二物联网设备已知第二密码;

[0050] 将两次加密的WiFi凭证从物联网服务发送到第二物联网设备;

[0051] 在第二物联网设备处使用第二密码解密两次加密的WiFi凭证以生成加密的WiFi凭证并使用第一密码解密加密的WiFi凭证以生成WiFi凭证;使用WiFi凭证在第二物联网设备上建立安全的WiFi连接。

[0052] 所述的方法,其中与所述第二物联网设备共享所述第一密码包括:

[0053] 经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道。

[0054] 所述的方法,其中生成所述第一密码包括生成随机随机数。

[0055] 所述的方法,其中第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。

[0056] 所述的方法,还包括:

[0057] 在物联网服务上生成服务公钥和服务私钥;在物联网设备上生成设备公钥和设备私钥;

[0058] 将服务公钥从物联网服务发送到物联网设备,并将设备公钥从物联网设备发送到物联网服务;

[0059] 使用设备公钥和服务私钥生成第二密码;

[0060] 使用服务公钥和设备私钥生成相同的第二密码。

[0061] 所述的方法,其中硬件安全模块(HSM)执行第二密码的生成。

[0062] 所述的方法,还包括:

[0063] 在第二物联网设备和客户端设备之间建立蓝牙低功耗(BTLE)通信信道;和

[0064] 在第一物联网设备和客户端设备之间建立BTLE和/或WiFi连接。

[0065] 实施例二:

[0066] 一种系统,包括:

[0067] 第一物联网设备,用于生成第一密码,第一物联网设备具有存储在其上的WiFi凭证;

- [0068] 第二个装置；
- [0069] 第一物联网设备与第二物联网设备共享第一密码并使用第一密码加密WiFi凭证以生成加密的WiFi凭证；
- [0070] 用于从第一物联网设备接收加密的WiFi凭证的物联网服务；使用第二密码加密加密的WiFi凭证以生成两次加密的WiFi凭证的物联网服务，第二物联网设备已知第二密码；
- [0071] 用于将两次加密的WiFi凭证从物联网服务发送到第二物联网设备的物联网服务；
- [0072] 第二物联网设备，使用第二密码解密两次加密的WiFi凭证，以生成加密的WiFi凭证，并使用第一密码解密加密的WiFi凭证，以生成WiFi凭证；和
- [0073] 第二个用于使用WiFi凭证建立安全WiFi连接的设备。
- [0074] 所述的系统，其中与所述第二物联网设备共享所述第一密码包括：
- [0075] 经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道。
- [0076] 所述的系统，其中生成所述第一密码包括生成随机现时。
- [0077] 所述的系统，其中第一物联网设备经由客户端设备将加密的WiFi凭证发送到物联网服务。
- [0078] 所述的系统，还包括：
- [0079] 物联网服务，用于生成服务公钥和服务私钥；
- [0080] 物联网设备生成设备公钥和设备私钥；
- [0081] 将服务公钥发送给物联网设备的物联网服务和将设备公钥发送给物联网服务的物联网设备；
- [0082] 其中，使用设备公钥和服务私钥生成第二密码，并且使用服务公钥和设备私钥生成相同的第二密码。
- [0083] 所述的系统，还包括：
- [0084] 硬件安全模块(HSM)，用于执行第二个密码的生成。
- [0085] 所述的系统，还包括：
- [0086] 第二个物联网设备包括蓝牙低功耗(BTLE)
- [0087] 通信接口与客户端设备通信；和
- [0088] 第一物联网设备包括WiFi或BTLE通信接口以与客户端设备通信。
- [0089] 实施例三：
- [0090] 一种机器可读介质，其上存储有程序代码，当由一个或多个机器执行时，使得所述机器执行以下操作：在第一物联网设备上生成第一密码，所述第一物联网设备具有存储在其上的WiFi凭证。；
- [0091] 与第二个物联网设备共享第一个密码；
- [0092] 使用第一密码加密第一物联网设备上的WiFi凭证以生成加密的WiFi凭证；
- [0093] 在物联网服务处从第一物联网设备接收加密的WiFi凭证；
- [0094] 使用第二密码加密物联网服务处的加密的WiFi凭证以生成两次加密的WiFi凭证，第二物联网设备已知第二密码；
- [0095] 将两次加密的WiFi凭证从物联网服务发送到第二物联网设备；
- [0096] 在第二物联网设备处使用第二密码解密两次加密的WiFi凭证以生成加密的WiFi凭证并使用第一密码解密加密的WiFi凭证以生成WiFi凭证；使用WiFi凭证在第二物联网设

设备上建立安全的WiFi连接。

[0097] 所述的机器可读介质,其中与所述第二物联网设备共享所述第一密码包括:

[0098] 经由客户端设备在第二物联网设备和第一物联网设备之间建立通信信道。

[0099] 所述的机器可读介质,其中生成所述第一密码包括生成随机随机数。

[0100] 所述的机器可读介质,其中所述第一物联网设备经由所述客户端设备将所述加密的WiFi凭证发送到所述物联网服务。

[0101] 所述的机器可读介质,还包括:

[0102] 在物联网服务上生成服务公钥和服务私钥;在物联网设备上生成设备公钥和设备私钥;

[0103] 将服务公钥从物联网服务发送到物联网设备,并将设备公钥从物联网设备发送到物联网服务;使用设备公钥和服务私钥生成第二密码;

[0104] 使用服务公钥和设备私钥生成相同的第二密码。

[0105] 所述的机器可读介质,其中硬件安全模块(HSM)执行第二密码的生成。

[0106] 所述的机器可读介质,还包括:

[0107] 在第二物联网设备和客户端设备之间建立蓝牙低功耗(BTLE)通信信道;和

[0108] 在第一物联网设备和客户端设备之间建立BTLE和/或WiFi连接。

[0109] 虽然上面已经参考各种实施例描述了本发明,但是应当理解,在不脱离本发明的范围的情况下,可以进行许多改变和修改。也就是说上面讨论的方法,系统或设备等均是示例。各种配置可以适当地省略,替换或添加各种过程或组件。例如,在替代配置中,可以以与所描述的顺序不同的顺序执行方法,和/或可以添加,省略和/或组合各种阶段。而且,关于某些配置描述的特征可以以各种其他配置组合。可以以类似的方式组合配置的不同方面和元素。此外,随着技术的发展许多元素仅是示例而不限制本公开或权利要求的范围。

[0110] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而,可以在没有这些具体细节的情况下实践配置例如,已经示出了众所周知的电路、过程、算法、结构和技术而没有不必要的细节,以避免模糊配置。该描述仅提供示例配置,并且不限制权利要求的范围,适用性或配置。相反,前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下,可以对元件的功能和布置进行各种改变。

[0111] 此外,尽管每个操作可以将操作描述为顺序过程,但是许多操作可以并行或同时执行。另外,可以重新排列操作的顺序。一个过程可能有其他步骤。此外,可以通过硬件、软件、固件、中间件、代码、硬件描述语言或其任何组合来实现方法的示例。当在软件、固件、中间件或代码中实现时,用于执行必要任务的程序代码或代码段可以存储在诸如存储介质的非暂时性计算机可读介质中,并通过处理器执行所描述的任务。

[0112] 综上,其旨在上述详细描述被认为是例示性的而非限制性的,并且应当理解,所述权利要求(包括所有等同物)旨在限定本发明的精神和范围。以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后,技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明权利要求所限定的范围。

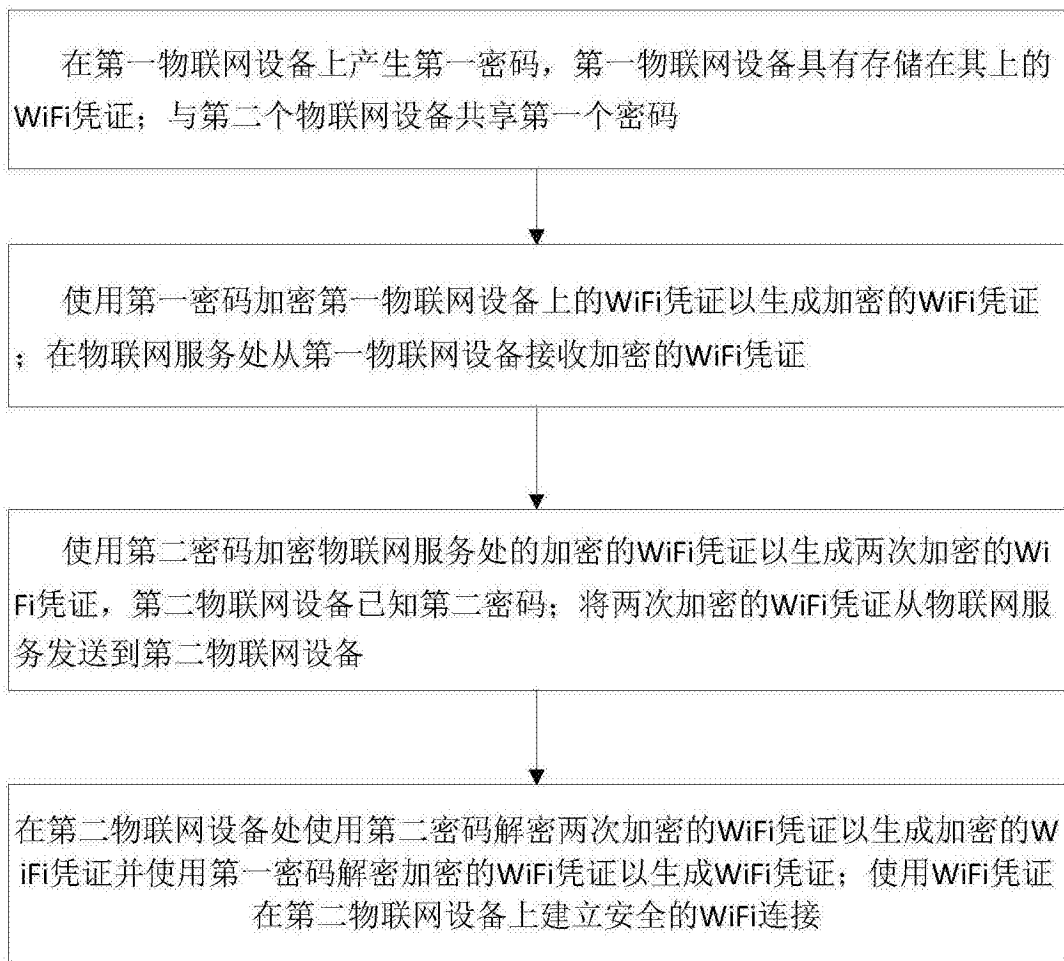


图1