(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108023731 A
(43)申请公布日 2018.05.11

(21)申请号 201711077975.4

(22)申请日 2017.11.06

(30)优先权数据
16306445.4 2016.11.04 EP
17305661.5 2017.06.06 EP

(71)申请人 汤姆逊许可公司
地址 法国伊西莱穆利诺

(72)发明人 N.勒斯夸尔内克 C.诺伊曼
O.赫恩

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 张贵东

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/14(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

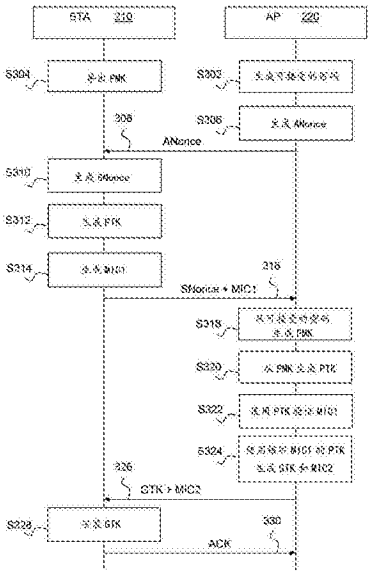
权利要求书2页 说明书8页 附图4页

(54)发明名称

用于客户端设备认证的设备和方法

(57)摘要

接入点接收来自客户端的第一一次性随机数(SNonce)和用于第一一次性随机数的第一密码散列(MIC1),使用从第二密钥(PMK)导出的第一密钥(PTK)计算第一密码散列,第二密钥(PMK)是在客户端上输入的或从在客户端上输入的密令导出的;从存储的主要输入和在导出时有效的至少一个存储的次要输入的每一个导出第一密钥(PTK),存储的主要输入和至少一个存储的次要输入的每一个是密令和第二密钥(PMK)中的一个;使用每一个导出的第一密钥(PTK)验证密码散列(MIC1)以找到校验第一密码散列(MIC1)的导出的第一密钥;使用校验第一密码散列(MIC1)的导出的第一密钥生成第三密钥(GTK)和第二密码散列(MIC2);以及发送第三密钥(GTK)和第二密码散列(MIC2)到客户端。



CN 108023731 A

1.一种用于在接入点(220)进行客户端认证的方法,所述方法包括在接入点(220)的至少一个硬件处理器(221)中:

接收来自客户端(210)的第一一次性随机数(SNonce)和用于第一一次性随机数的第一密码散列(MIC1),使用从第二密钥(PMK)导出的第一密钥(PTK)计算所述第一密码散列,所述第二密钥(PMK)是在客户端(210)上输入的或从在客户端(210)上输入的密令导出的;

从在导出时有效的存储的主要输入和至少一个存储的次要输入的每一个导出(S318、S320)第一密钥(PTK),所述存储的主要输入和所述至少一个存储的次要输入的每一个是密令和第二密钥(PMK)中的一个;

使用每一个导出的第一密钥(PTK)验证(S322)所述密码散列(MIC1)以找到校验所述第一密码散列(MIC1)的导出的第一密钥;

使用所述校验所述第一密码散列(MIC1)的导出的第一密钥生成(S324)第三密钥(GTK)和第二密码散列(MIC2);以及

发送所述第三密钥(GTK)和所述第二密码散列(MIC2)到客户端(210)。

2.如权利要求1所述的方法,其中每个存储的次要输入具有定义的、有限的有效性时段或每个存储的次要输入对应于具有至少一个打字错误的主要输入。

3.如权利要求1所述的方法,其中所述接入点(210)是Wi-Fi接入点,以及所述方法进一步包括发送(S308)第二一次性随机数(ANonce)到客户端(210),以及其中进一步从所述第一一次性随机数(SNonce)和所述第二一次性随机数(ANonce)导出所述第一密钥(PTK)。

4.如权利要求1所述的方法,其中使用从所述校验所述第一密码散列(MIC1)的导出的第一密钥生成的加密密钥将所述第三密钥(GTL)加密并发送。

5.如权利要求2所述的方法,进一步包括当存储的次要输入变得无效时,更新所述第三密钥。

6.一种接入点(220),包括:

通信接口(223),配置成:

接收来自客户端(210)的第一一次性随机数(SNonce)和用于第一一次性随机数的第一密码散列(MIC1),使用从第二密钥(PMK)导出的第一密钥(PTK)计算所述第一密码散列,所述第二密钥(PMK)是在客户端(210)上输入的或从在客户端(210)上输入的密令导出的;以及

发送第三密钥(GTK)和第二密码散列(MIC2)到客户端(210);

存储器,配置成存储主要输入和至少一个次要输入,所述主要输入和所述至少一个次要输入的每一个是密令和第二密钥(PMK)中的一个;以及

至少一个硬件处理器(221),配置成:

从在导出时有效的所述存储的主要输入和至少一个次要输入的每一个导出第一密钥(PTK);

使用每一个导出的第一密钥(PTK)验证所述密码散列(MIC1)以找到校验所述第一密码散列(MIC1)的导出的第一密钥;以及

使用所述校验所述第一密码散列(MIC1)的导出的第一密钥生成所述第三密钥(GTK)和所述第二密码散列(MIC2)。

7.如权利要求6所述的接入点,其中每个存储的次要输入具有定义的、有限的有效性时

段或每个存储的次要输入对应于具有至少一个打字错误的主要输入。

8.如权利要求6所述的接入点，其中所述接入点(210)是Wi-Fi接入点，以及所述通信接口(223)进一步配置成发送(S308)第二一次性随机数(ANonce)到客户端(210)，以及其中所述至少一个硬件处理器(221)配置成进一步从所述第一一次性随机数(SNonce)和所述第二一次性随机数(ANonce)导出所述第一密钥(PTK)。

9.如权利要求6所述的接入点，其中所述至少一个硬件处理器(221)进一步配置成，在发送到客户端(210)之前，使用从所述校验所述第一密码散列(MIC1)的导出的第一密钥生成的加密密钥将所述第三密钥(GTL)加密。

10.如权利要求8所述的接入点，其中所述至少一个硬件处理器(221)进一步配置成仅在所述存储的次要输入的有效性时段期间从存储的次要输入导出第一密钥(PTK)。

11.如权利要求7所述的接入点，其中所述至少一个硬件处理器(221)进一步配置成当存储的次要输入变得无效时，更新所述第三密钥。

12.一种用于在Wi-Fi受保护访问(WPA)2企业认证器设备(230)处认证客户端设备(210)的方法，所述方法包括：

发送(S404)会话标识符(SId)和第一挑战(Ach)到所述客户端设备(210)；

从所述客户端设备(210)接收用户名、第二挑战(SCh)和用于第一挑战(Ach)、第二挑战(SCh)、会话标识符(SId)和密令(PW)的密码散列(H)；

验证(S410)有效的存储的主要密令或至少一个有效的存储的次要密令是否校验所述密码散列(H)，每个存储的次要密令在有限的、定义的有效性时段期间是有效的或每个存储的次要输入对应于具有至少一个打字错误的主要输入；

在密令校验所述密码散列(H)的情况下：

发送(S412)指示成功认证的消息到客户端(210)；以及

执行与客户端设备(210)的握手(S414)以采用密钥。

13.一种Wi-Fi受保护访问(WPA)2企业认证器设备(230)，包括：

通信接口，配置成：

发送会话标识符(SId)和第一挑战(Ach)到所述客户端设备(210)；

以及

从所述客户端设备(210)接收用户名、第二挑战(SCh)和用于第一挑战(Ach)、第二挑战(SCh)、会话标识符(SId)和密令(PW)的密码散列(H)；以及

至少一个硬件处理器，配置成：

验证有效的存储的主要密令或至少一个有效的存储的次要密令是否校验所述密码散列(H)，每个存储的次要密令在有限的、定义的有效性时段期间是有效的或每个存储的次要输入对应于具有至少一个打字错误的主要输入；以及

在密令校验所述密码散列(H)的情况下：

经由所述通信接口发送指示成功认证的消息到客户端(210)；以及执行与客户端设备(210)的握手以采用密钥。

用于客户端设备认证的设备和方法

技术领域

[0001] 本公开一般地涉及网络安全，并且具体地涉及网络中的客户端设备认证。

背景技术

[0002] 本部分想要向读者介绍领域的各个方面，其可能涉及下面描述和/或要求保护的本公开的各个方面。相信该讨论有助于向读者提供背景信息以帮助更好的理解本公开的各个方面。相应地，应当了解从这个角度理解这些陈述，而不是作为现有技术的承认。

[0003] 在无线通信中，经常希望的是将对所谓的接入点的接入限制为仅用于认证的客户端设备，在这里将使用最普遍的无线网络技术Wi-Fi作为非限制性的说明性示例。

[0004] 用于认证客户端设备的第一种方案是通过证书的使用，然而由于这样需要复杂的安装和管理，该方案在很多情况下是不合适的。

[0005] 第二种方案使用用户在客户端设备上输入的共享的秘密(secret)，该客户端设备然后向接入点证明了解该共享秘密。

[0006] 例如，第二方案广泛的在Wi-Fi受保护访问(Wi-Fi Protected Access,WPA)个人(也称作WPA-PSK(预共享密钥))中使用，其具有在IEEE 802.11i中描述并在图1中图示的称为WPA2个人的第二版本。

[0007] 在步骤S102和S104中，客户端设备STA和接入点AP彼此独立地使用将共享密令(passphrase)、称为服务集标识符(Service Set Identifier,SSID)的网络标识符以及SSID的长度作为输入的密钥导出函数(称为基于密码的密钥导出函数2(Password-Based Key Derivation Function 2,PBKDF2))，导出成对主密钥(Pairwise Master Key,PMK)。可替代地，可以将PMK输入为64位十六进制数的字符串。

[0008] 在步骤S106中，AP生成随机数(即一次性随机数(nonce))ANonce，它在消息108中发送到STA。

[0009] 在步骤S110中，STA生成随机数(即一次性随机数)SNonce，并且在步骤S112中，从各一次性随机数中生成成对临时密钥(Pairwise Transient Key,PTK)、PMK以及接入点AP和客户端设备STA的介质访问控制(Media Access Control,MAC)地址。然后，在步骤S114中，STA生成用于SNonce的消息完整性编码(Message Integrity Code,MIC)；MIC是SNonce的键控密码散列(keyed cryptographic hash)(HMAC-SHA1或AES-CMAC)。MIC使用128位PTK作为密钥。然后，STA在消息116中将SNonce和MIC发送到AP。

[0010] 当接收到SNonce和MIC时，在步骤S118中，AP以与步骤S112中STA所做的相同的方式导出PTK。在步骤S120中，AP验证MIC是正确的。在这个时候，认证STA和AP并已经互相导出相同的PTK。

[0011] AP向STA发送包括组临时密钥(Group Temporal Key,GTK)和使用(使用PTK的128-256位加密的)第二MIC保护的序列号。当接收到消息122时，STA在步骤S124中安装GTK，其然后可以用以将数据包发送到由AP管理的无线网络。最后，STA将确认126发送到AP。

[0012] 另一种可能性是WPA-企业(WPA-Enterprise)，其以不同的方式工作以提供扩展认

证协议(Extensible Authentication Protocol,EAP)。在许多EAP协议之中,最常见的是受保护的扩展认证协议(Protected Extensible Authentication Protocol,PEAP)、传输层安全协议(Transport Layer Security,TLS)以及基于隧道的传输层安全协议(Tunnelled Transport Layer Security,TTLS)。在这些之中,TLS需要在客户端和服务器两边的证书,而TTLS和PEAP相当类似,他们都具有在服务器上的证书以及由客户端输入的密码。

[0013] 作为示例,如下,PEAP使用微软的挑战握手认证协议,第2版(MS-CHAPv2)来交换密码。客户端和认证器(RADIUS服务器)通过AP建立隧道。认证器将会话标识(Session ID)以及第一挑战发送给客户端,客户端回复用户名称、第二挑战以及挑战的散列、会话标识和用户的密码的MD4散列。RADIUS服务器检查散列并视情况回应成功或失败,并通知AP接受客户端,这导致AP发起与客户端的四次握手以通过共享的密钥。

[0014] 共享的秘密和密码的问题在于输入它们是一个容易导致错误的任务,特别是当要输入的是长或复杂的数据的时候,如Wi-Fi经常遇到的为了提供可接受的安全水平的情况。在缓和这个问题的尝试中,以及提出了使用Wi-Fi保护设置(Wi-Fi Protected Setup,WPS)。然而,许多设备(如iOS设备)不支持WPS,以及WPS的一些实现已经苦恼于安全问题,因此限制了它们的使用。

[0015] 在“pASSWORD tYPOS and How to Correct Them Securely”中,Chatterjee等人的提出了容忍密码中的打字错误的认证方法。尽管这篇文献提供了一些正式的评估,但仅仅提出了理论的解决方案,而没有提供任何实现或如何将这样的方法整合进已经存在的认证协议。

[0016] 在EP 2947591、EP 2876569、EP 3067811、US 2015/0363588以及US 2015/0363593中已经描述了其他容忍打字错误的解决方案,其都需要客户端的修改,以及在US 9280657中服务器学习接受跟随有正确的密码的错误密码的输入。同样的,这些传统的解决方案具有缺点。

[0017] 基于如Wi-Fi技术的网络中的共享秘密和密码的另一个问题在于他们使用单个共享秘密或密码。例如,为了准许访客连接到网络,这可以通过给任一访客网络密码完成。这意味着知道网络密码改变,访客都可以继续连接到网络,由于改变网络密码需要改变每个应当具有网络连接的客户端上的密码,这是不方便的。

[0018] 另一方面,网关可以使用第二SSID以向访客提供例如网络连接,但是由于第二SSID是不同于第一SSID的,这将使得不能访问第一SSID的网络。

[0019] 不同的解决方案是使用一次性的密码,但这样是典型的不准许访客访问与用户使用的网络相同的网络。

[0020] 应当注意到,希望具有克服至少部分的涉及在无线通信网络中共享密钥的输入的传统问题的解决方案。

发明内容

[0021] 在第一方面,本原理针对用于在接入点的客户端认证的方法。接入点的至少一个硬件处理器从客户端接收第一一次性随机数(nonce)以及用于第一一次性随机数的第一密码散列,使用从第二密钥导出的第一密钥计算所述第一密码散列,第二密钥是在客户端上输入的或从客户端输入的密令导出的;从在导出时有效的存储的主要输入以及至少一个存

储的次要输入的每一个导出第一密钥，存储的主要输入和至少一个存储的次要输入的每一个是第二密钥和密令中的一个；使用每个导出的第一密钥寻找校验第一密码散列的导出的第一密钥验证密码散列；使用导出的校验第一密码散列的第一密钥生成第三密钥和第二密码散列，并将第三密钥和第二密码散列发送到客户端。

[0022] 第一方面的各种实施例包括：

[0023] 每个存储的次要输入具有定义的、有限的有效性时段或对应于具有至少一个打字错误的主要输入。当存储的次要输入变得无效时，可以更新第三密钥。

[0024] 接入点是Wi-Fi接入点，其也发送第二一次性随机数到客户端，以及进一步从第一一次性随机数和第二一次性随机数得到第一密钥。

[0025] 使用从校验第一密码散列的导出的第一密钥生成的加密密钥加密并发送第三密钥。

[0026] 在第二方面，本原理针对一种接入点；包括通信接口，配置成从客户端接收第一一次性随机数以及用于第一一次性随机数的第一密码散列，使用从第二密钥导出的第一密钥计算所述第一密码散列，第二密钥是在客户端上输入的或从客户端输入的密令导出的，并向客户端发送第三密钥以及第二密码散列；存储器，配置成存储主要输入和至少一个次要输入，主要输入和至少一个次要输入的每一个是第二密钥和密令中的一个；以及至少一个硬件处理器，配置成从在导出时有效的存储的主要输入和至少一个次要输入的每一个导出第一密钥，使用每个导出的第一密钥验证密码散列以找到校验第一密码散列的导出的第一密钥，并使用校验第一密码散列的导出的第一密钥生成第三密钥和第二密码散列。

[0027] 第二方面的各种实施例包括：

[0028] 每个存储的次要输入具有定义的、有限的有效性时段或对应于具有至少一个打字错误的主要输入。当存储的次要输入变得无效时，可以更新第三密钥。

[0029] 该接入点是Wi-Fi接入点，以及通信接口进一步配置成将第二一次性随机数发送给客户端，并且其中至少一个硬件处理器配置成进一步从第一一次性随机数和第二一次性随机数导出第一密钥。至少一个硬件处理器可以进一步配置成仅在存储的次要输入有效性时段期间从存储的次要输入导出第一密钥。

[0030] 至少一个硬件处理器进一步配置成，在发送到客户端之前，使用从核对第一密码散列的导出的第一密钥生成的加密密钥加密第三密钥。

[0031] 在第三方面，本原理针对用于在Wi-Fi受保护访问2企业(Wi-Fi Protected Access 2Enterprise)认证器设备上认证客户端设备的方法，该方法通过将会话标识符和第一挑战发送到客户端设备；接收来自客户端设备的用户名、第二挑战和用于第一挑战、第二挑战、会话标识符和密令的密码散列；验证有效的存储的主要密令或至少一个有效的存储的次要密令是否校验密码散列，在有限的定义的有效性时段期间每个存储的次要密令是有效的或每个存储的次要密令对应于具有至少一个打字错误的主要输入，以及在密令校验密码散列的情况下，向客户端设备发送指示成功验证的消息并与客户端设备执行握手以采用密钥。

[0032] 在第四方面，本原理针对Wi-Fi受保护访问2企业认证器设备，其包括通信接口，配置成将会话标识符和第一挑战发送到客户端设备，并从客户端设备接收用户名、第二挑战以及关于第一挑战、第二挑战、会话标识符和密令的密码散列；以及至少一个硬件处理器，

配置成验证有效的存储的主要密令或至少一个有效的存储的次要密令是否校验密码散列，每个存储的次要密令在有限的定义的有效性时段期间是有效的或每个存储的次要输入对应于具有至少一个打字错误的主要输入，以及在密令校验密码散列的情况下，经由通信接口将指示成功验证的消息发送到客户端设备，并执行与客户端设备的握手以采用密钥。

[0033] 在第五方面，本原理针对一种计算机程序，其包括由处理器可执行的用于实现根据第一方面的任何实施例的方法的步骤的程序代码指令。

[0034] 在第六方面，本原理针对一种计算机程序产品，其存储在非暂态的计算机可读介质上，并包括由处理器可执行的用于实现根据第一方面的任何实施例的方法的步骤的程序代码指令。

附图说明

[0035] 现在将参照附图通过非限制性的示例描述本原理的优选的特征，其中：

[0036] 图1图示了传统的Wi-Fi受保护访问(WPA)个人协议；

[0037] 图2图示了根据本原理的第一实施例的示例性的系统；

[0038] 图3图示了根据本原理的实施例的用于设备插入的示例性的方法；以及

[0039] 图4图示了根据本原理的进一步的实施例的用于设备插入的示例性的方法。

具体实施例

[0040] 图2图示了根据本原理的第一实施例的示例性的系统200。系统200包括客户端设备(STA)210、以及接入点(AP)220(如网关)。接入点220配置成接合到本地网络240以及外部网络250(如互联网)，通过这样可以在另一网络(未示出)中为设备建立连接。在示例性的系统中，本地网络240是Wi-Fi网络。

[0041] 客户端设备210以及接入点220每一个包括至少一个硬件处理单元(处理器)211、221、存储器212、222以及至少一个配置成与其他设备通信的通信接口213、223(以Wi-Fi接口为示例)。技术人员将了解为了清楚性的原因，图示的设备是非常简化的，以及此外实际的设备将包括特征如内部连接和电源。非暂态的存储介质260存储当由处理器执行时，执行下文中进一步描述的接入点220的功能的指令。

[0042] 可能连接到本地网络240的客户端设备210进一步包括用户接口214。例如，客户端设备可以是笔记本电脑、智能电话或平板。

[0043] 接入点220配置成执行传统的接入点功能如接合本地网络240和外部网络250。多个客户端设备可以连接到本地网络240或者通过本地网络240连接，或一个作为接入点220的本地网络可以提供多个本地网络，例如以分离的子网络的形式。典型地，准许任何证明共享的网络密码(如网络密钥)的了解的设备接入本地网络240。

[0044] 外部网络250可以用以连接服务器和其他设备，可能是通过其他接入点(未示出)。

[0045] 图3图示了根据本原理的实施例的设备插入的示例性的方法。

[0046] 在步骤S302中，接入点(AP)220的处理器221从接入点220的配置中的主密令组生成有限的一组错误但可接受的密码，该组包括主密令。换句话说，处理器221生成并存储一组密令，包括原始的、正确的密令以及包括至少一个错误的若干变体密令。优选的是引入的错误对应于共同的错误，如例如(括号内是用于32字符密令的包括原始密令的变体的数

量)：

[0047] ●在任意随机位置省略字符(33)；

[0048] ●插入大写(2)

[0049] ●每4个字符添加空格(9)

[0050] ●将I(大写的i)替换为l(小写的L)

[0051] ●将0(零)替换为O(2)

[0052] ●将一个字符(任意一个)替换为4个最邻近中的一个(4*32+1＝129)

[0053] ●将一个或两个字符(任意两个)替换为4个最邻近中的一个$((\binom{32}{2}*4+32*4+1=2113))$

[0054] ●它们的任何组合(变体的数量的乘积,5020488)。注意即使当接受这样的错误的任何组合时,它最多移除熵的23位。如果字符是出厂设置密令中常见的十六进制数(0-9A-F),原始的熵是32*4＝128位。接受所有这些错误留下(至少)熵的105位,这在许多情况下仍然足够的。

[0055] 在一个变体中,接入点(AP)220的处理器221生成一组可接受的密令组,包括主要的、默认的密令以及至少一个有效的次要密令。主密令典型地是由网络的常规用户使用的密令,并且保持有效直到由例如网络的管理员或用户改变时才改变。次要密令是由例如网络的访客使用的密码,它的有效性典型地在时间上受限制,但它也可以直到撤销时都有效。

[0056] 在这个变体中,处理器221可以配置成生成每个对一天有效的多个次要密令。然后,可接受的密令组包括主密令以及对当前一天有效的次要密令。例如,每一天处理器可以使用例如迭代的单向散列法生成用于当前一天以及用于接下来的N天的次要密令。这些次要密令可以显示在AP(未示出)的用户界面中或发送到已经使用主密令连接的用户的设备上用于在它的UI214上显示,或发送到运行专用应用的设备。通过使处理器221生成多个次要密令,访客可以在多天期间立即被准许接入。

[0057] 在变型的一个实施例中,接入点包括“访客WPS按钮”。该按钮实现与WPS相同的机制,除了将这一天的密令推送给客户端(而不是默认密令)。

[0058] 在变型的一个实施例中,用户激活访客设备上的Wi-Fi受保护设置按钮,激活AP220上的Wi-Fi受保护设置按钮。然后,AP和访客设备执行Diffie-Hellman密钥交换,在其后AP将这一天的密令发送到访客设备,访客设备在网络连接期间使用该密令,在其后AP执行如上文中描述的认证。

[0059] 与图1中描述的传统协议的重要区别在于,接入点220不必要在一开始导出PMK,但是可以等待直到它从客户端设备(STA)210接收到SNonce+MIC。注意到对于客户端设备210协议保持没有改变。

[0060] 在步骤S304中,客户端设备210导出使用密钥导出函数(例如,PBKDF2)导出成对主密钥(Pairwise Master Key,PMK),该密钥导出函数将输入密令、称为服务集标识符(SSID)的网络标识符以及SSID的长度作为输入。可替代地,PMK可以输入为64位十六进制数的字符串。

[0061] 在步骤S306中,接入点220生成在消息308中发送到客户端设备210的随机数ANonce。

[0062] 在步骤310中,客户端设备210生成另一随机数SNonce,并在步骤S312中从各一次

性随机数、PMK和客户端设备210和接入点220的介质访问控制(Media Access Control，MAC)地址生成成对临时密钥(Pairwise Transient Key,PTK)。然后，客户端设备210在步骤S314中生成用于SNonce的消息完整性编码(Message Integrity Code,MIC)(图3中的MIC1)；MIC1是SNonce的键控密码散列(keyed cryptographic hash)(HMAC-SHA1或AES-CMAC)。MIC使用128位PTK作为密钥。然后，客户端210在消息316中将SNonce和MIC1发送到接入点220。

[0063] 当接收到SNonce和MIC1后，接入点220在步骤S318中从可接受的密令组中的每个密令导出PMK。生成的各PMK可以替代或附加于可接受的密令组而存储。可替代地，在将PMK输入为64位十六进制数的字符串的情况下，接入点220导出并存储正确的PMK中可接受的PMK。注意到这个步骤可以提前执行，例如在步骤S302后。

[0064] 在步骤S320中，接入点220使用与步骤S312中客户端设备210使用的相同的生成方法为S318中生成的每个PMK生成PTK。

[0065] 在步骤S322中，接入点220验证MIC1对于步骤S320中生成的任何PTK是正确的。如果PTK能够通过MIC1的验证，那么将这个PTK设置为当前的PTK。在这个时候，接入点220和客户端设备210是认证的，并互相(从主密令或次要密令)生成相同的PTK。注意到如果没有PTK能够通过MIC的验证，那么客户端设备210是非认证的，正如图1中图示的传统方法中输入了不正确的密令。

[0066] 在步骤S324中，接入点220生成群组临时密钥(Group Temporal Key,GTK)和使用第二MIC保护的(使用PTK的128-256位加密的)序列号(图3中的MIC2)，它们在消息326中发送到客户端设备210。当接收到消息326后，客户端设备210在步骤S328中安装GTK，然后GTK可以用以向由接入点220管理的无线网络发送包。最后，客户端设备210将应答330发送到接入点220。

[0067] 可以看到，接入点220尝试找到可接受的密令组中的密令，在该密令下接收的MIC、MIC1是有效的。如果找到了这样的密令，那么可以认证客户端，并且将该密令用作余下的交换(即导出PTK、加密GTK以及签名消息)的基础。

[0068] 接入点优选地存储由给定的客户端设备(通过它的MAC地址识别)使用的PMK。换句话说，接入点存储PMK，从该PMK生成通过MIC验证的PTK。这样，下一次客户端设备连接时，接入点检索存储的PMK，这样可以减少在重新连接时猜测的密令的数量。

[0069] 在时间有限的密令的变型中，接入点220优选地撤销不再有效的次要密钥，如当密钥有效的一天结束时，撤销当天密钥。

[0070] 用于次要密钥撤销的简单方法是无论次要密钥什么时候期满，接入点220更新GTK。可以使用IEEE 802.11i中定义的所谓的群组密钥握手机制更新GTK。自然地，也可以使用其他合适的机制。

[0071] 用于次要密钥撤销的更复杂的方法是接入点220保持追踪次要密钥是否已经由客户端设备使用。在次要密钥还没有被使用的情况下，那么在次要密钥期满时没有必要更新GTK。仅仅当期满的次要密钥在有效性期间被使用时更新GTK，例如使用群组密钥握手机制。

[0072] 本原理扩展到基于密码的WPA2企业(PEAP/EAP-TTLS)的情况。对于Wi-Fi，尝试可接受的密码组以确定认证是否成功。

[0073] 图4图示了根据本原理的进一步的实施例的设备插入的示例性的方法。

[0074] 图4图示了可以与图2中的相同的客户端设备210。尽管为了简洁的原因没有图示，该图也示出了认证器230，其包括至少一个硬件处理单元(处理器)、存储器以及至少一个配置成与其他设备通信的通信接口。

[0075] 在步骤S402中，客户端设备210通过接入点(图2中的220)与认证器设备230(如RADIUS服务器)建立传输层安全协议(Transport Layer Security，TLS)隧道。认证器230在消息404中将会话标识(SId)和挑战(ACh)发送到客户端设备210。客户端设备210在步骤S406中生成包括用户名、挑战(SCh)和各挑战(ACh、SCh)、会话ID(SId)和用户密码的MD4散列的消息408。将消息408发送到认证器230。至此，该方法对应于传统方法。

[0076] 在步骤S410中，认证器230校验是否用于用户的可接受的用户密码组中的任何用户密码校验散列H；换句话说，可接受的用户密码组中的计算的各挑战(ACh、SCh)、会话ID(SId)和用户密码的MD4散列是否与在消息408中接收的散列H相同。

[0077] 然后，认证器230将消息412发送到客户端设备210。如果组中没有密码校验散列H，那么消息412指示失败，客户端设备210没有认证并且该方法终止。然而，如果密码校验散列H，那么消息412指示成功并认证客户端设备。然后，客户端设备210和认证器在步骤S414中启动传统的四次(4-way)握手以采用密钥。

[0078] 如将了解的是，本原理对现有的客户端有效，并仅仅根据实施例要求在接入点或RADIUS服务器上的修改。进一步的，因为原始的密令或密码是组的一部分，该方法是向后兼容的。

[0079] 应当理解图中示出的元素可以以各种硬件、软件或其组合的形式实现。优选地，这些元素由一个或多个适当地编程的通用用途的设备上的软件和硬件的组合实现，通用用途的设备可以包括处理器、存储器和输入/输出界面。

[0080] 本描述图示了本公开的原理。因此，将了解的是，尽管这里没有明确的描述或示出，本领域技术人员能够想出各种体现公开的原理并在其范围以内的布置。

[0081] 这里引用的所有示例和条件语言旨在用于教育目的，以帮助读者理解公开的原理以及发明人为促进本领域而贡献的概念，并且将被解释为不限于这些具体引用的示例和条件。

[0082] 此外，这里陈述本公开的原理、各方面和各实施例的所有陈述以及其具体示例旨在涵盖其结构和功能等同物。此外，旨在这样的等同物包括当前已知的等同物以及将来开发的等同物，即，开发的执行相同功能的任何元件，而不管结构如何。

[0083] 因此，例如，本领域技术人员将了解这里呈现的框图表示体现公开的原理的图示性的电路的概念图。类似地，应当了解，任何流程图表、流程图、状态转换图、伪代码等代表可以在计算机可读介质中实质上表示并且由计算机或处理器执行的各种过程，无论这样的计算机还是处理器是否明确示出。

[0084] 图中示出的各种元素的功能可以通过使用专用硬件以及能够与适当软件相关联地执行软件的硬件提供。当由处理器提供时，可以由单个专用处理器、单个共享处理器或多个单独的处理器提供功能，这些处理器中的一些可以共享。此外，术语“处理器”或“控制器”的明确使用不应解释为仅仅涉及能够执行软件的硬件，并且可以隐含地包括数字信号处理器(DSP)硬件，用于存储软件的只读存储器(ROM)，随机存取存储器(RAM)和非易失性存储器。

[0085] 还可以包括常规和/或定制的其他硬件。类似地，图中所示的任何开关仅是概念性的。它们的功能可以通过程序逻辑的操作、通过专用逻辑、通过程序控制和专用逻辑的交互，甚至手动地执行，实现者可以从上下文中更具体地理解的可选的特定技术。

[0086] 在这里的权利要求中，表示为用于执行指定功能的任何元素旨在包含执行该功能的任何方式，包括例如a)执行该功能的电路元件的组合或b)任何形式的软件，因此，包括固件，微代码等，以及用于执行该软件以执行该功能的适当的电路组合。由这样的权利要求限定的公开内容在于，由各种所引用的部件提供的功能以权利要求所要求的方式组合并汇集在一起。因此认为可以提供这些功能的任何部件等同于这里示出的那些。

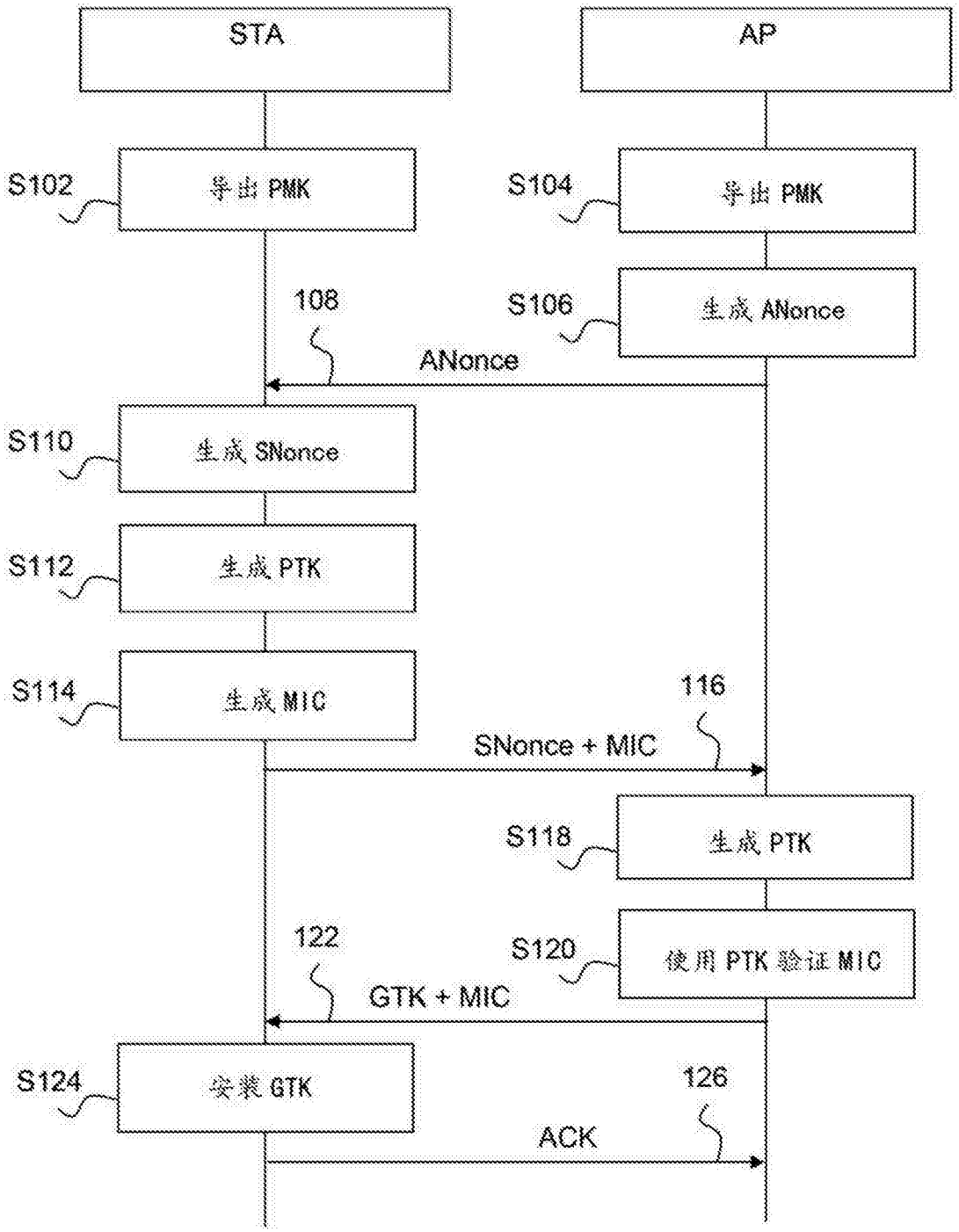

STA
AP
S102
导出 PMK
S104
导出 PMK
108
S106
生成 ANonce
ANonce
S110
生成 SNonce
S112
生成 PTK
S114
生成 MIC
116
SNonce + MIC
S118
生成 PTK
122
S120
使用 PTK 验证 MIC
GTK + MIC
S124
安装 GTK
126
ACK

图1

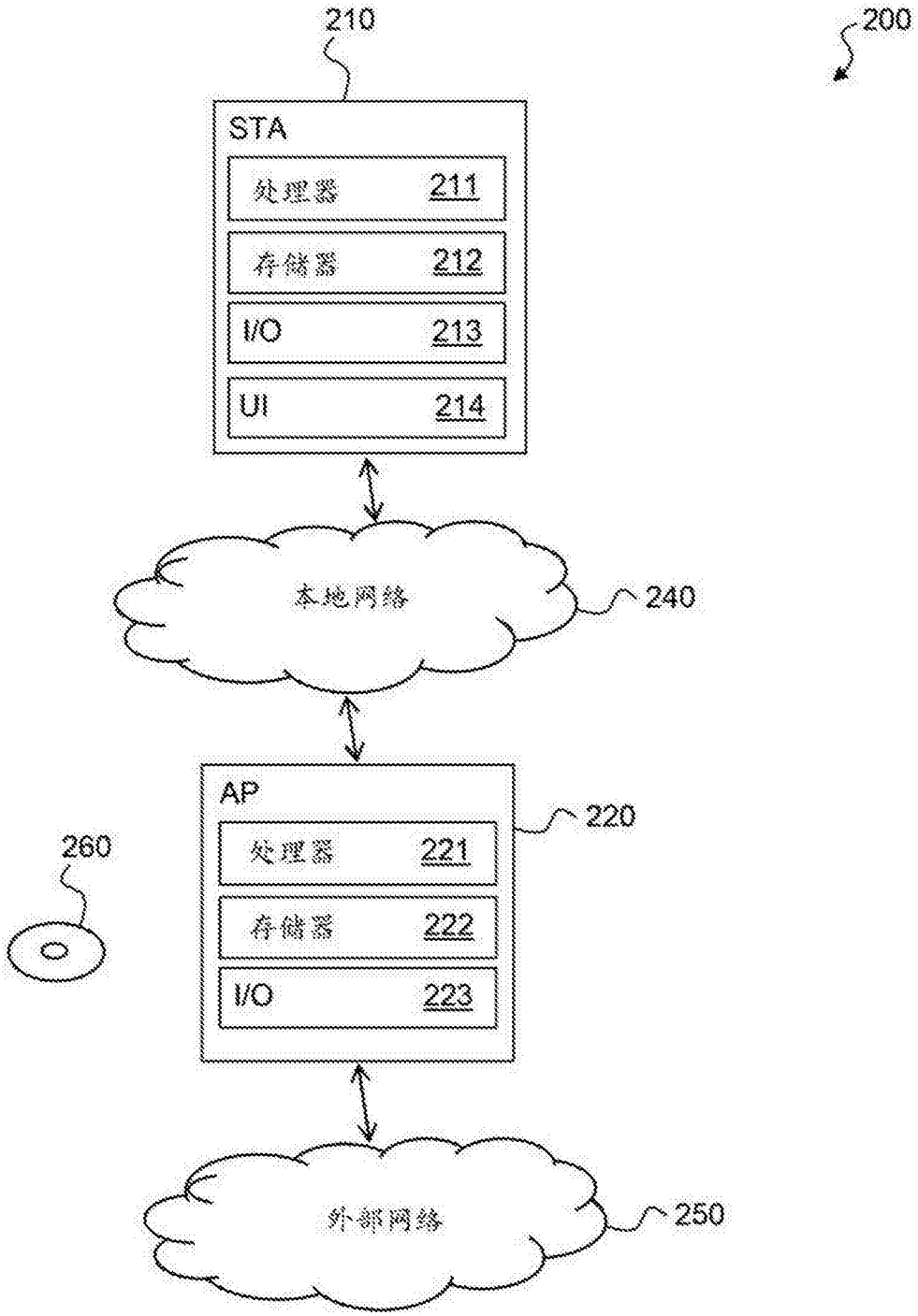

210
200
STA
处理器 211
存储器 212
I/O 213
UI 214
本地网络
240
AP
220
处理器 221
存储器 222
I/O 223
260
外部网络
250

图2

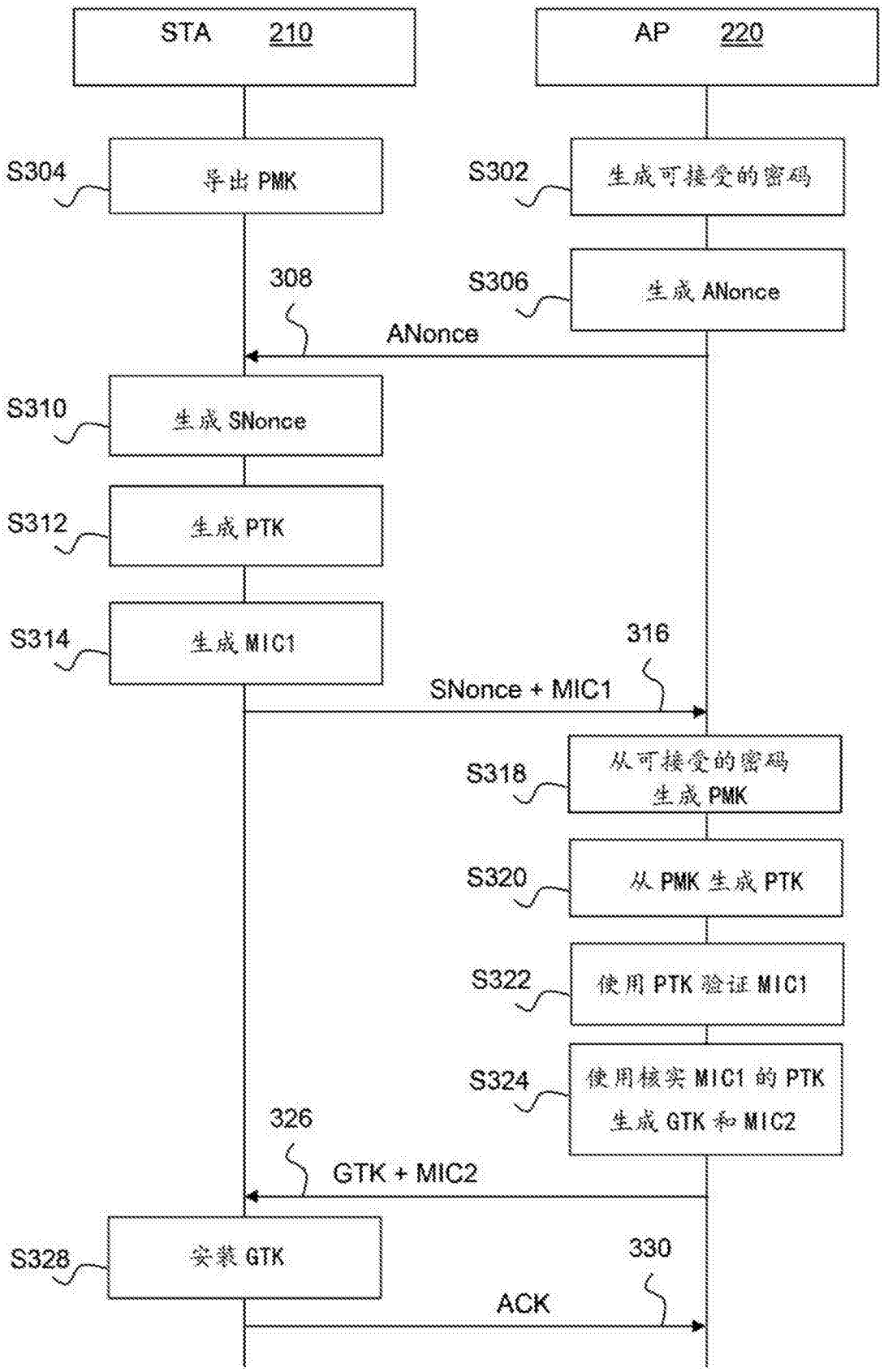

STA 210
AP 220
S304
导出 PMK
S302
生成可接受的密码
308
S306
生成 ANonce
ANonce
S310
生成 SNonce
S312
生成 PTK
S314
生成 MIC1
316
SNonce + MIC1
S318
从可接受的密码
生成 PMK
S320
从 PMK 生成 PTK
S322
使用 PTK 验证 MIC1
S324
使用核实 MIC1 的 PTK
生成 GTK 和 MIC2
326
GTK + MIC2
S328
安装 GTK
330
ACK

图3

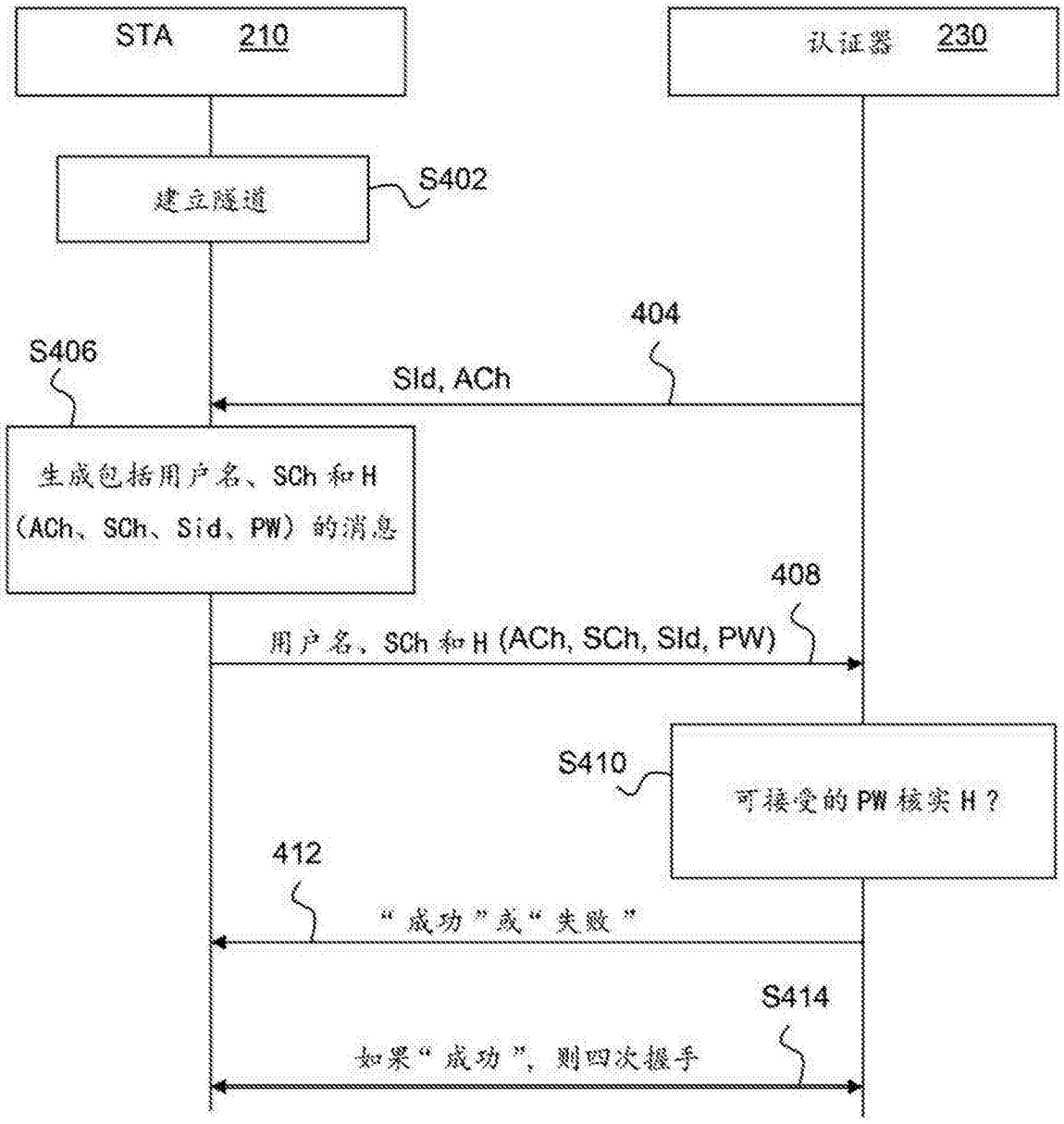

STA 210
认证器 230
建立隧道
S402
404
S406
SId, ACh
生成包括用户名、SCh 和 H
(ACh、SCh、Sid、PW) 的消息
408
用户名、SCh 和 H (ACh, SCh, SId, PW)
S410
可接受的 PW 核实 H？
412
“成功”或“失败”
S414
如果“成功”，则四次握手

图4