(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 101807998 A
(43)申请公布日 2010.08.18

(21)申请号 200910009511.9

(22)申请日 2009.02.13

(71)申请人 英飞凌科技股份有限公司
地址 德国瑙伊比贝尔格市

(72)发明人 张宁

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 章社杲 李慧

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

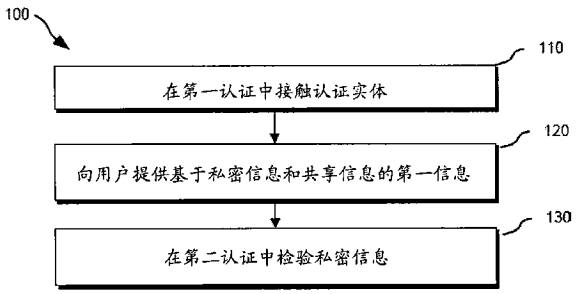
权利要求书 3 页 说明书 11 页 附图 6 页

(54)发明名称

认证

(57)摘要

本发明描述了一种在通信网络中认证用户的方法，包括：在对寻求接入所述通信网络的一个用户的第一认证中接触认证实体；向所述用户提供第一信息，所述第一信息基于该用户的私密信息和共享信息而产生，所述共享信息在一个接入节点群的全部接入节点中共享，所述接入节点群包括至少第一接入节点和一个第二接入节点；以及通过将所述共享信息应用到所述第一信息，在所述用户的第二认证中核查所述私密信息。本发明还涉及相应的装置。



CN 101807998 A

1. 一种在通信网络中认证用户的方法，包括：

在对寻求接入所述通信网络的一个用户的第一认证中接触认证实体；

向所述用户提供第一信息，所述第一信息基于该用户的私密信息和共享信息而产生，所述共享信息在一个接入节点群的全部接入节点中共享，所述接入节点群包括至少第一接入节点和一个第二接入节点；以及

通过将所述共享信息应用到所述第一信息，在所述用户的第二认证中核查所述私密信息。

2. 根据权利要求 1 所述的方法，其中当所述用户在所述第一接入节点处寻求连接到所述通信网络时执行所述用户的第一认证，并且其中当所述用户在所述第二接入节点处寻求连接到所述通信网络时执行所述第二认证。

3. 根据权利要求 1 所述的方法，进一步包括：在所述用户从所述第一接入节点向所述第二接入节点的切换的过程中，将所述私密信息从所述用户传送到所述第二接入节点，并且

基于对所述私密信息的核查，为所述第二接入节点认证所述用户。

4. 根据权利要求 1 所述的方法，其中所述私密信息是在认证所述用户的过程中产生的第一密钥，并且所述共享信息是共享密钥；并且其中产生第一信息包括通过使用所述共享密钥加密至少所述第一密钥。

5. 根据权利要求 4 所述的方法，其中产生所述第一信息包括加密所述第一密钥和所述用户的第一标识符。

6. 根据权利要求 5 所述的方法，其中核查所述私密信息包括：

通过使用所述共享密钥解密所述第一信息，由此提取所述第一密钥和所述第一标识符；

用所述提取的第一密钥解密第二编码信息，由此提取包含在所述第二编码信息中的第二标识符；并且

核查从解密所述第一信息中提取的所述第一标识符是否与从所述第二编码信息中提取的所述第二标识符相匹配。

7. 根据权利要求 6 所述的方法，其中所述第二信息是一个 4 步握手协议的一个消息的一部分。

8. 根据权利要求 6 所述的方法，其中所述第二编码信息进一步包括以下至少一项：

用于产生成对的主密钥的 Nonce；以及

一个时间标记。

9. 根据权利要求 1 所述的方法，其中所述私密信息是成对的临时密钥的一部分。

10. 根据权利要求 1 所述的方法，进一步包括通过将所述共享信息应用到所述第一信息在所述用户的所述第二认证中核查所述私密信息。

11. 根据权利要求 1 所述的方法，进一步包括：新产生第一信息，所述新产生的第一信息不同于前述的第一信息；并且

将所述新产生的第一信息传送给所述用户，所述方法进一步包括：

基于所述新产生的第一信息核查所述用户。

12. 根据权利要求 1 所述的方法，进一步包括：

在核查所述第一信息时产生成对的主密钥；

基于所述成对的主密钥产生成对的临时密钥；

基于所述成对的临时密钥新产生所述私密信息；

基于所述新产生的私密信息以及所述共享信息新产生所述第一信息；

将所述新产生的第一信息传送给所述用户；

基于所述新产生的信息，通过核查所述新产生的信息认证所述用户。

13. 根据权利要求 1 所述的方法，其中所述第一信息是通过使用一个密钥而产生的，并且其中在所述第二认证中，所述密钥是通过使用所述共享信息解密该所述第一信息而从所述第一信息中提取。

14. 根据权利要求 13 所述的方法，进一步包括使用在所述第二认证模式中提取的密钥来解密从所述用户传送的进一步的信息。

15. 根据权利要求 14 所述的方法，其中来自所述用户的进一步的消息包括所述用户的标识符。

16. 根据权利要求 1 所述的方法，其中核查所述私密信息对所述接入节点指明所述用户已经通过所述第一认证进行了认证。

17. 根据权利要求 1 所述的方法，其中所述第一信息仅从所述第一接入节点传送给所述用户，并仅存储在所述用户处。

18. 一种通信系统，包括：

第一接入节点；以及

第二接入节点；

其中

所述第一接入节点被配置为向一位用户提供第一认证，

所述第一认证基于利用认证实体；

所述第一接入节点，被进一步配置为向所述用户提供第一信息，所述第一信息是基于所述用户的私密信息和共享信息而产生的，所述共享信息是在所述通信系统的至少所述第一接入节点和所述第二接入节点中共享；并且

其中所述第二接入节点被配置为在第二认证中认证所述用户，所述第二接入节点包括基于将所述共享信息应用到所述第一信息来核查所述第一信息的实体。

19. 一种通信装置，包括：

第一实体，所述第一实体被配置为从一个用户接收第一信息，所述第一实体是基于所述用户的私密信息和预定信息而产生的；并且

其中所述第一实体进一步被配置为通过将所述预定信息应用到所述第一信息来认证所述用户。

20. 根据权利要求 19 所述的通信装置，其中所述第一信息是在一个接入节点群的各个接入节点中共享的密钥。

21. 根据权利要求 19 所述的通信装置，其中所述通信装置被配置为决定是否执行第一认证或是第二认证，其中所述通信装置进一步被配置为如果要执行所述第一认证则接触认证实体以产生一个成对的主密钥，并且

其中所述通信装置进一步被配置为如果要执行所述第二认证则通过将所述预定信息

应用到所述第一信息来认证所述用户。

22. 一种方法，包括：

在第一认证中，在通信网络的第一接入节点处认证用户，其中在所述第一认证中由加密服务器产生第一成对的主密钥；并且

在第二认证中，在通信网络的第二接入节点处认证所述用户，其中在所述第二认证中，基于由所述用户提交的第一信息以及由所述第二接入节点提交的第二信息产生第二成对的主密钥而不使用所述第一认证服务器。

23. 一种装置，包括：

第一电路，所述第一电路被配置为提供用于数据通信的主密钥；

控制器，所述控制器决定是否使用第一模式或第二模式来产生所述主密钥，其中所述控制器被配置为控制所述第一电路以便在所述第一模式中从远程装置接收的信息中取出所述主密钥，并且其中所述控制器被配置为控制所述第一电路以便在所述第二模式中基于从一个远程装置接收的消息中取出的第一 Nonce 以及由所述第一电路产生的第二 Nonce 以产生所述主密钥。

24. 根据权利要求 23 所述的装置，其中所述装置进一步被配置为在所述第一模式中接收表示一次成功认证的第一信息，并在所述第二模式中开始向所述远程装置传送所述第一信息用于由所述远程装置核查所述第一信息。

认证

技术领域

[0001] 本发明涉及认证技术领域。

背景技术

[0002] 在现代数据通信系统中，安全是主要问题之一。随着越来越多信息在数据通信系统传输以及越来越多的具有安全性关键信息的用户应用程序运行在与此类通信系统连接的装置上，对通信系统入侵或安全相关机制的破坏可具有灾难性后果。为了防止恶意使用者的攻击或入侵，在许多通信网络中要求用户在经由通信网络的接入节点开始数据通信之前进行验证。用于认证的不同机制是公知的，例如根据 IEEE 802.1X 的验证过程。另一方面，现代数据通信要求对通信网络的接入要尽可能容易并且尽可能迅速。现有通信网络可以提供安全验证，例如 IEEE 802.1X 等认证机制，但在提供该认证时耗费了相当多的时间。

发明内容

[0003] 本发明提供了一种在通信网络中认证用户的方法，包括：在对寻求接入所述通信网络的一个用户的第一认证中接触认证实体；向所述用户提供第一信息，所述第一信息基于该用户的私密信息和共享信息而产生，所述共享信息在一个接入节点群的全部接入节点中共享，所述接入节点群包括至少第一接入节点和一个第二接入节点；以及通过将所述共享信息应用到所述第一信息，在所述用户的第二认证中核查所述私密信息。

附图说明

[0004] 图 1 示出了根据一个实施方案的通信网络的方框图；

[0005] 图 2 示出了根据一个实施方案的一个流程图；

[0006] 图 3 示出了根据一个实施方案的一个流程图；

[0007] 图 4 示出了根据一个实施方案的一个流程图；

[0008] 图 5a 到图 5e 示出了根据多个实施方案的流程和消息图。

[0009] 图 6 和图 7 分别示出了用于在请求者（用户）侧执行上述流程的第一示例性装置和认证者（接入节点）侧执行上述流程的装置的一个进一步的实施方案。

具体实施方式

[0010] 以下详细说明阐明了本发明的多个示例性实施方案。该说明不得用作限定意义，而该说明仅出于阐述本发明实施方案的主要原理的目的，而且保护的范围仅由所附权利要求书来确定。

[0011] 进一步地，应当理解，除非另行明确指出，在此所说明各种示例性实施方案的特征可以相互组合。

[0012] 在各个附图中，相同或相似的实体、模块、装置等可以用同一参考号指定。

[0013] 现参见图 1，根据一个实施方案的通信网络 10 具有一个用户 20、一个第一接入节

点 30 和一个第二接入节点 40。该第一接入节点 30 和第二接入节点 40 是一个接入节点群 50 中的接入节点。在此使用的术语“用户”具有宽泛的含义，包括以下装置，例如固定通信装置（个人计算机、机顶盒、打印机或者其他电子固定装置，如通信控制固定装置）和移动通信装置（笔记本电脑、膝上电脑、移动电话、个人数字助理或者其他电子装置，如通信控制家用电器装置）。用户能够通过无线连接，例如无线局域网 (WLAN) 的工作站，和 / 或有线连接，如至少通过第一和第二接入节点的，向通信网络传送数据。通信网络可包括例如无线通信网络例如 WLAN（无线局域网）、有线通信网络例如利用电缆或者电力线连接的家庭网络、或者使用无线和有线连接混合的通信网络例如利用无线 LAN 和电力线连接的家庭网络。为了提供上述通信，用户和接入节点可具有根据对应的通信协议执行数据通信的合适的接收器、发射器或者收发器。在一些实施方案中，通信网络可以是纯共享媒介型。在一个实施方案中，通信网络可实施为无线 LAN（无线局域网），其中接入节点群 50 形成扩展服务组 (ESS)。在其他实施方案中，通信网络可以是被配置为构建家庭网络的一个通信网络群。图 1 进一步示出验证实体 60，该实体至少连接到第一接入节点 30。在各个实施方案中，该验证实体 60 可连接到该接入节点群的每一个接入节点。

[0014] 现在图 2 示出在通信网络例如图 1 所示的通信网络 10 中验证用户的一个方法 100 的一个基本实施方案。

[0015] 在 110，寻求接入通信网络的一个用户在第一验证中接触一个验证实体。

[0016] 在 120，将第一信息提供给用户，该第一信息是基于用户的私密信息和共享信息而产生的。如 120 表明，该共享信息在一个接入节点群的全部接入节点中共享。该接入节点群包括至少一个第一接入节点和一个第二接入节点。为了说明 WLAN 通信的一个实例，该接入节点群可包括一个 WLAN 扩展服务组 (extendedservice set) 的全部接入节点。

[0017] 在 130，通过将共享信息应用到第一信息上，在用户的第二验证中核查该私密信息。

[0018] 在方法 100 中，当用户在第一接入节点寻求连接通信网络时可执行用户的第一验证，当用户在第二接入节点寻求连接通讯网络时可执行第二验证。然而，要注意在各个实施方案中，第一和第二接入节点的每一个都能够提供第一和第二验证。

[0019] 在一个实施方案中，当用户在该接入节点群中的一个接入节点处寻求向通信网络的连接时，执行用户的第一验证，该节点是在一次会话中第一次被访问的接入点，例如第一接入节点。在第一验证后执行后，当用户在该接入节点群的一个或多个节点处寻求向通信网络的进一步连接时，用私密信息的验证来验证该用户。

[0020] 私密信息的验证可以是切换 (hand-off) 过程或者漫游的一部分，其中用户到网络的连接接入点从第一接入点变化为第二接入点。然后，该方法 100 在用户完成从第一接入节点到第二接入节点的切换之前或在其过程中可包括该私密信息从用户到第二接入节点的传送，并且第二接入节点利用基于私密信息验证的第二验证来验证该用户。切换过程发生在当工作站离开一个接入点的基本服务组 (BSS) 进入一个新的接入点时，例如 WLAN 切换中。

[0021] 共享信息可以是一个密钥，该密匙在该接入节点群中的全部接入节点中共享，但它仍然是秘密的。在各个实施方案中，共享信息可包括一个第一共享密钥和一个第二共享密钥。第一共享密钥可用于为第一信息提供加密，而第二共享密钥可用于在第二验证过程

中由用户向其中一个接入节点提交的第一信息的完整性检查或者其他可靠性检查。

[0022] 在第一验证中使用的验证实体可作为验证者在接入节点外部提供，并且在用户外部的一个分离实体中提供。然而，在一个实施方案中，该验证实体也可作为验证者集成在接入节点中。

[0023] 在一个实施方案中，验证实体可以是为接入节点群提供验证的一个验证服务器。然而，该验证服务器可以集成在其中一个接入节点中。在各个实施方案中，验证实体可包括一个 RADIUS(Remote Authentication Dial In User Service，远程验证拨入用户服务）部件或者可以是一个 RADIUS 服务器。该验证服务器可在实例中支持。在实施方案中，该验证实体也可为用户提供验证。在实施方案中，该验证实体可包括提供认证服务的一个 PKI(Public Key Infrastructure，公共密钥基础结构）部件。

[0024] 该第二认证可在没有访问该认证实体的情况下进行或执行，即，没有向认证实体传送任何消息或者从认证实体接收任何消息。如在下面将更详细地说明，通过利用第二认证，在每个接入节点处能够提供快速认证。在此第二认证是基于已经执行了的第一认证，其在认证过程中访问过该认证实体。然后在方法 100 中私密信息的核查可对该接入节点表明用户此前已经由第一认证进行了认证。应当注意，在各个实施方案中，多个接入节点的每一个均能够提供第一和第二认证。在第一认证中，接入节点可担当认证者，但是该认证将实质上由认证实体（例如，由认证服务器）提供。因此，在第一认证中，来自用户的消息经由担当认证者的接入节点向认证实体传送，并从认证实体经由担当认证者的接入节点向用户传送。然而，在第二认证中，该接入节点认证该用户而不需要访问基于此前第一认证的认证者实体。

[0025] 在各个实施方案中第一信息可视为从接入节点传递到用户的“标记”或“标记信息”。在第一认证之后，每当用户想要寻求与接入节点的连接或者联系时，可提交该第一信息。在各个实施方案中，该第一信息能够使节点群的接入节点对第一信息进行核查。因此，在这些实施方案中，一旦用户已经通过第一认证而得到认证，第一信息就可用于提供更容易和更快的认证，这是通过仅仅认证该用户包含有效的第一信息，其中有效第一信息表明该用户已经适当地经过第一认证并且已经适当地通过第一认证进行了确认。

[0026] 在各个实施方案中，第一和第二认证是在认证用户的至少不同的步骤或不同协议中实施的不同的认证过程。例如，在随后将要说明的一个实施方案中，第一认证是根据完全的 IEEE 802.11 标准的认证，其中接入节点是认证者，并且认证实体是提供 RADIUS 服务的认证服务器，而第二认证提供快速认证而不用耗时的完全 802.11 认证方法。在一个实施方案中，第二认证使用该第一信息并修改了 IEEE 802.11i 标准中的 4 路认证过程。例如，这允许产生一个临时密钥所需要的主密钥，而不必访问认证服务器。该主密钥是基于由用户提交的一个 Nonce 以及由接入节点提交的一个 Nonce 由用户在本地产生的。

[0027] 在一个实施方案中，可通过向第一信息应用共享信息，在第二认证中进行对私密信息的核查。该私密信息在一个实施方案中可包括一个密钥。该第一信息可通过对该密钥应用共享信息而产生。在一个实施方案中，该私密信息可以是在用户认证过程中产生的一个成对的临时密钥的一部分或者一段。

[0028] 在一个实施方案中，该方法 100 包括通过使用共享信息作为加密密钥而对私密信息加密。在第二认证中，该私密信息可通过使用共享信息将第一信息解密而从第一信息中

提取。

[0029] 在第二认证过程中，所提取的密钥（私密信息）可用于检查或核查由用户提交的第一信息的完整性和/或保密性。为此目的，该密钥在第二认证模式中可用于对由用户传送的一个或多个消息进行解密。

[0030] 该密钥可以是在第一认证过程中产生的一个密钥。在一个实施方案中，该密钥可以是通过使用一个成对的主密钥而产生的一个成对的临时密钥的一部分，该主密钥此前已经在第一认证过程中由认证服务器产生。

[0031] 在各个实施方案中，第一信息可通过将共享信息不仅应用到密钥而且还应用到其他信息例如一个标识符或者用户的标识符而产生。这样的一个标识符例如可包括在数据通信过程中使用的通信地址，例如 MAC 地址。在各个实施方案中应用共享信息可包括加密处理，其中共享信息是用于加密处理的加密密钥。

[0032] 因此，在一个实施方案中，第一信息可以是来自用共享信息作为加密密钥对由一个主密钥得出的密钥和标识符加密的结果。或者换言之，该方法 100 可包括通过加密第一密钥和用户的标识符而产生该第一信息。在其他实施方案中，第一信息还可包括例如表示时间周期的时间标记（在该时间周期中第一信息被视为有效）的信息和/或从第一信息中提供的信息的单向变换中得到的信息。这样的信息 M 的单向变换的例子是一对 (M, $PRF_K(M)$)，其中 $PRF_K(M)$ 是一个有密钥的伪随机函数，例如 CBC-MAC(Cipher Block Chaining Message Authentication Code) 或者一个有密钥的密码散列函数 (HMAC = Hash Message Authentication Code)。在核查私密信息时，该时长时间可用于认证第一信息的有效期。在第二认证过程中将第一信息提交给接入节点时，该单向变换可用于提供第一信息的完整性和可靠性。这样的检查的一个实施方案修改了方法 100，以便包括通过使用共享密钥解密第一信息。然后，通过解密，提取该密钥和第一标识符。最后，通过检查完整性或可靠性，可核查该第一信息是否已被非法修改。

[0033] 在一个实施方案中的第二编码信息进一步包括用于从一个成对的主密钥和/或一个时间标记中产生成对的暂时密钥的一个 Nonce。

[0034] 当被编码第二信息包含用于从一个成对的主密钥中产生一个成对的临时密钥的一个 Nonce(Number used once，一次使用编号）时，该方法 100 可进一步被修改为包括从被编码的第二信息中提取该 Nonce。该 Nonce 可以是一个随机或者伪随机编号。然后通过使用提取的 Nonce 产生一个成对的暂时密钥。该成对的暂时密钥能够用于在该用户和用户寻求连接的接入点之间进一步的通信。

[0035] 该第一信息可由用户提交作为预定协议中的一条消息或者消息的一部分。例如，该消息可以是在 IEEE 802.11i 中说明的 4 步握手 (Handshake) 协议的修改版本中的一条消息。

[0036] 在各个实施方案中，该消息除了第一信息之外还包括消息完整性代码和/或用于消息通信的 Nonce。

[0037] 在第二认证中提取的密钥可进一步用于解密来自用户的另一条消息。该消息可包括用户的标识符，并且从第二信息提取的标识符可与从解密第一信息中提取的标识符进行比较。

[0038] 第二认证可重复多次，例如为用户提供到通信网络的多次连接。为了说明而不是

限制，一个例子将包括当用户沿WLAN系统的扩展服务组(ESS)移动的情况。在这种情况下，从一个接入点到另一个接入点的传递过程能够以更快速的方式实现。

[0039] 在各个实施方案中，每次执行第二认证就会产生新的第一信息。然后该新的第一信息可传送给用户。当用户连接到接入节点群的另一个接入节点时，用户向对应的接入节点提交该新的第一信息。然后该新的第一信息基于使用该新的第一信息应用共享信息而进行核查。因此，该方法100可包括在第一信息被认证之后，重新产生第一信息。为了获得不同于此前第一信息的新产生的第一信息，以及该新产生的第一信息传送给用户。

[0040] 在一个实施方案中，在第二认证中对用户的核查之后，产生了一个临时的成对主密钥。在一个实施方案中，该成对的临时密钥是基于一个成对的主密钥而产生的，该主密钥在第二认证过程中在产生成对的临时密钥之前产生。然后，方法100可包括当第一信息被认证时产生一个成对的主密钥并且随后基于成对的主密钥产生一个成对的临时密钥。此外，可基于新产生的成对的临时密钥重新产生私密信息。然后，基于新产生的私密信息，通过将共享信息应用到新产生的私密信息，能够重新产生第一信息。最后，将新产生的第一信息传送给用户，供用户在下一次寻求连接到另一个接入节点时使用。

[0041] 应当理解，上述方法100的实施方案及其衍生方案可在接入节点中或通信装置中执行。因此，接入节点或通信装置可被配置为执行方法100的一个或多个上述实施方案或者上述方法的一部分。在其一个实施方案中，通信装置可包括一个第一实体，它被配置为从用户接收第一信息，其中该第一实体是基于用户的私密信息以及预置信息而产生的。该第一实体可实现将预置信息应用到第一信息上，并可进一步被配置以认证该用户。应当注意，该预置信息可以是在上述接入节点群的全部接入节点中共享的信息。而且，还应当理解，该方法100及其衍生方案可在通信网络（例如图1中所示的通信网络）中执行。

[0042] 现在将参见图3说明方法200的进一步的基本实施方案。在方法200中，通过在210利用第一认证，在通信网络的一个第一接入节点处开始认证一个用户。在第一认证中，第一个成对的主密钥(PMK)由一个认证服务器例如RADIUS服务器或者AAA服务器在220产生。然后，在230，在通信网络的第二接入节点处开始对用户的第二认证。在第二认证内，在240，在没有使用认证服务器的情况下产生第二个成对的主密钥。成对的主密钥的产生可基于由用户提交的第一密钥信息以及由第二接入节点提交的第二密钥信息。在一个实施方案中，该第一和第二密钥信息可以是用于产生成对的主密钥的第一和第二Nonce。在一个实施方案中，第一个Nonce可因此在第二接入节点处本地产生，并从第二接入节点向用户传送，同时第二个Nonce可在用户处本地产生，并从用户向第二接入节点传送。在这种情况下，该第二个接入点的信息是被加密。

[0043] 在另一个实施方案中，第二成对的主密钥可由基于从用户传送到第二接入节点的第一nonce以及由第二接入节点提交的第二nonce由第二接入节点在本地产生。

[0044] 应当理解，可提供基本方法200的很多衍生方案，即变体、增补或改进。具体地说，关于基本方法100说明的变体、增补或改进也可提供或结合在方法200中。这里不再明确地说明这些特征，请参考以上说明。

[0045] 还应理解，对于方法200的实施方案和其衍生方案，可以在接入节点和通信装置中执行。因此，接入节点或通信装置可被配置为执行方法200的一个或多个上述实施方案及其衍生方案或者上述方法200的一部分及其衍生方案。而且，还应理解，方法200及其衍

生方案可在通信网络中执行，如图 2 所示的通信网络。

[0046] 下面将参见图 4 说明一个方法 300 的进一步基本实施方案。该方法 300 包括在 310 由一个第一认证对用户进行认证，该第一认证使用了一个认证实体。在 320，基于核实该用户此前已经在第一认证中得到认证，使用第二认证来认证该用户。

[0047] 如上所述，该用户已经在此前于第一认证中得到认证的确认信息可包括在第二认证中由用户向接入节点群的其中一个接入节点提交第一信息。而且，如此前已经提及，该第一信息由在第一认证中由作为标识符的接入节点在第一次认证过程中产生。

[0048] 应理解，可提供基本方法 300 的很多衍生方案，即变体、增补或改进。具体地说，关于基本方法 100 和 200 所说明的变体、增补或改进也可提供或结合在方法 300 中。因此，可参见以上说明。

[0049] 还应当理解，方法 300 及其衍生方案可在接入节点或者通信装置或者通信网络中执行。因此，接入节点或通信装置或通信网络可被配置为执行上述方法 200 的实施方案或者衍生方案的一个或多个或者上述方法 200 及其衍生方案的至少一部分。

[0050] 为说明而非限制的目的，下面将更详细地说明无线局域网的一些实施方案。在进一步解释这些实施方案之前，解释在下面使用的一些语法结构的约定。以下使用的约定如下：A → B：M：A 向 B 发送信息 M；K，K_{XY}，K_X..... ：加密的密钥，其中 K_{XY} 表示在主体 X 和 Y 之间共享的密钥，K_X 表示主体 X 的公共密钥；PRF_n：产生 n 位输出的伪随机函数；L(str，F，L)：利用 IEEE 802.11 位约定，从 str 由左侧开始通过 F+L-1 取出位 F；N，N_a，N_X…. ：Nonce，它代表“使用一次的数字”；这些是从足够大的空间取样的随机数字；N_X 是由要素 X 产生；T_X：由要素 X 产生的时间标记；$\{M\}_K$：表示使用密钥 K 加密消息 M 的结果；$[M]_K$：表示使用密钥 K 对消息 M 单向变换的结果。在实际中，$[M]_K$ 可例如由一对 (M，$PRF_K(M)$) 实现，其中 PRF_K 表示一个有密钥的伪随机函数 (即，CBC-MAC 或有密钥的密码散列函数，HMAC)。K，K′ ：在接入点群 (APs) 中共享的密钥。K 用于加密，K′ 用于产生消息完整性编码 (MIC)(在下列实施方案中，预定接入点群的每个接入点共享相同的 K 和 K′)；K_{AP}：一个接入点的公共密钥；K_{AP}^{-1}：接入点的私钥，其中每一个接入点具有其自己的 KAP 和 K_{AP}^{-1}。

[0051] 现在参见图 5a，根据一个实施方案的流程图 400 包括在 402 设置一个比特位，它表示通过该接入节点群能够利用第二认证来提供快速切换。该设置能够通过设置 IEEE 802.11i 标准中表示节点公布所要求能力的强安全网络 (Robust Security Network，RSN) 域，来与 IEEE 802.11i 标准保持一致，例如在比特位 6 增加“快速切换子域”来完成。将“快速传递”子区域设置为逻辑 1 可表示快速切换机制得到支持，设置为 0 可表示不支持“快速切换”机制。

[0052] 设置“快速切换”子域可在第一次执行与接入节点的连接之前提供。当工作站拥有第一信息时，它将该快速“切换”子区域设置为 1。在该实施方案中，该第一信息也指示为“标记”。在一些实施方案中，该接入节点通过检查工作站的请求帧，可发现工作站是否支持快速切换。

[0053] 在 404，工作站 (STA) 寻求到接入点群的网络连接。

[0054] 在 406，它判断工作站是否是首次连接到接入点群。在一个实施方案中，它还判断工作站和接入节点是否支持“快速切换”协议。如果它们之中任何一个不支持“快速切换“协议，将执行第一认证。在一个实施方案中，可基于用户是否提交第一信息而做出决定，该

第一信息表示工作站此前已经完成了接入节点群的第一认证并已经连接到该群。如果工作站是首次进行连接，该工作站将在408执行第一认证，这将在图5b中进一步详细地说明。如果不是，则工作站将在410执行第二认证，这将在图5c中更详细地说明。

[0055] 在执行第一认证的情况下，在412，如果认证成功，工作站将在414获得允许网络连接，程序在418结束。如果工作站不是首次连接，工作站将在410执行第二认证，这将在图5d中进一步详细说明。如果工作站执行第二认证，并且在416判断第二认证已经成功，该程序进行到414，允许该工作站接入网络。如果不是，则程序将再次在418结束。

[0056] 现在参见图5b，将更详细地说明在408由第一认证进行的认证。

[0057] 如图5b所示，在第一认证420中，由认证服务器产生一个主密钥对(PMK)并且它被传送到作为认证者的接入节点（认证者端口接入实体）。作为请求者的用户能够使用与认证者相同的秘密元素和算法得到相同的主密钥对。图5c表示使用例如EAP(Extensible Authentication Protocol，扩展认证协议）交换机构传送成对的主密钥。基于该成对的主密钥，在422由接入点以4步握手(4步信号交换）过程产生一个临时密钥对。该4步握手过程将在以下更详细地说明。在4步握手过程的消息1中，认证者的Nonce(ANonce)与认证者MAC地址(AA)一起从认证者传送到请求者。消息1可包含进一步的信息例如主密钥对标识(PMKID)。在从认证者接收到消息1后，请求者（用户）现在能够将基于认证者传输的Nonce、其自己的Nonce(SNonce)、认证者的传送地址(AA)及其自己的地址(SPA)放入密码散列表，产生临时密钥对(PTK)：PTK ← PRF_X(PMK，" PairwiseKeyExpansion"，Min(AA，SPA)||Max(AA，SPA)||Min(ANonce，SNonce)||Max(ANonce，SNonce))从上面导出的临时密钥对的不同部分可分配用于通信的不同密钥（子密钥）。因此，临时密钥对分为多个密钥。在临时密钥对中分配的其中一个密钥是快速切换密钥，它构成在产生第一信息中使用的私密信息，用于通过将第一信息用于确认而允许快速切换。通常的临时密钥对在中不包含快速传递认证密钥(FHAK)K_h。与通常的临时密钥对相比，由上述产生的临时密钥对包含附加的比特位，以便反映在临时密钥对内的附加的快速切换认证密钥。在一个实施方案中，该临时密钥对可包括说明快速传递密钥的另外的256个比特(32个字节)。临时密钥对的大小可取决于安全模式。例如，常规临时密钥对在用于TKIP(Temporal Key Integrity Protocol，暂时密钥完整性协议）模式时大小为512，用于CCMP（具有CBC-MAC的计数模式）模式的大小为384。这些大小由会被快速切换认证密钥的附加的比特所扩展。因此，在上面的实施方案中，用于TKIP模式的临时密钥对的大小为512+256 = 768比特，其中快速切换认证密钥K_h可从临时密钥对的比特512到767导出，即K_h ← L(PTK，512，256)。在CCMP模式的情况下，快速切换认证密钥可具有384+256 = 640比特的大小，其中快速切换认认证密钥可从临时密钥对的比特384到639导出，即K_h ← L(PTK，384，256)。

[0058] 在消息2中，请求者向认证者提交其Nonce(SNonce)以及请求者的MAC地址(SPA)。消息2也可包括MIC(MessageIntegrity Code，消息完整性编码）。其后，认证者也能够产生如上所述的临时密钥对。

[0059] 现在也能够导出快速切换认证密钥K_h，该认证者产生第一信息，它在下文中将被称为“标记”。该标记产生如下：$Badge \leftarrow \{SPA, K_h, T_{life}, \lfloor SPA, K_h, T_{life} \rfloor_{K'}\}_K$

[0060] 换言之，该标记的产生是通过用共享密钥K加密以下信息产生：快速切换密钥、请求者MAC地址(SPA)、与表示“标记“的生命期信息（其与主密钥对的生命期相关）、以及由

对快速切换认证密钥的、请求者 MAC 地址 (SPA) 和生命期信息的单向变换产生的消息完整性检查信息。单向变换提供了用于该标记的消息完整性检查能力，它是通过使用单向变换加密的共享 K' 而产生的。

[0061] 在此应当注意，该标记是基于只在认证者和请求者之间共享的私密信息而产生的，即快速切换密钥 K_H 和请求者的 MAC 地址。为了加密这些私密信息并且为了提供给完整性检查，使用了仅仅在接入点群中共享的 K,K'，即它是接入点群的私密信息，而它对接入点群之外的任何其他装置是保密的。这样，该标记的拥有者就可向接入点群的任何其他接入点提供核查标记表示其已经在第一认证中得到了正确的认证，以下将对其进行更详细地说明。

[0062] 在消息 3 中，认证者将一条确认信息和标记一起传送到请求者。消息 3 也可包含用于允许完整性检查的一个消息完整性编码以及其他信息，例如用于下一个多播或者广播帧的序列号。最后，在消息 4 中，请求者向认证者发送确认。

[0063] 现在已经说明了第一认证者 408，以下将参见图 5d 给出在流程图 400 中的第二认证 410 更详细的说明。

[0064] 在第二认证中，在 502，首先由接入点判断用户是否支持快速切换认证。如上所述，在切换过程，该第二认证是需要的，当用户离开第一接入点的基础服务组 (BSS)，并与第二接入点的基础服务组相关联，第二接入点需认证该用户。由于在 402 中已经通过设置相应的比特位来标明快速切换认证，第二认证可通过使用 4 步握手过程提供认证。在 504，主密钥对在请求者（用户）和认证者（接入节点）处本地产生。如以下将要清楚说明的那样，在请求者和认证者处产生的主密钥对可在不同的时间完成，即，不是同时发生的。在 506，临时密钥对在请求者（用户）和认证者（接入节点）处本地产生。如以下将要清楚表述的那样，在请求者和认证者处临时密钥对的产生可在不同的时间完成，即，不是同时发生的。在 508，由请求者提交的标记由认证者进行核查。现在将参见图 5e 提供的使用 4 步握手过程，以更详细的说明上述执行过程。

[0065] 在图 5e 中，4 步握手过程由认证者传送到请求者。该消息 1 包括认证者的一个 Nonce(ANonce') 和另一个 Nonce 即 APMK，二者都由认证者产生。ANonce' 用于完成 4 步信息交换，而 APMK 用于产生新的主密钥对。与这两个 Nonce 一起，该消息 1 包括接入点的公共密钥 K_{AP} 以及由认证者产生的一个时间标记 T_{AP}。在消息 2 中，请求者向认证者传送由请求者产生的 Nonces SNonce' 和 SPMK 以及标记、请求者的 MAC 地址 SPA、时间标记信息 T_{AP} 和消息完整性编码 MIC2。在消息 2 中，SPMK 被认证者的公共密钥 K_{AP} 加密。用快速切换密钥 K_H 对被加密的 SPMK、MAC 地址 SPA 和时间标记信息 T_{AP} 进行加密。换言之，消息 2 包括下列信息 :SNonce' ，$\{SPA, T_{AP}, \{SPMK\}_{K_{AP}}\}_{K_h}$，Badge，MIC2。

[0066] 在根据图 5e 的 4 步握手过程中，在接收到消息 1 之后，请求者能够基于接受的 APMK 和其自身产生的 SPMK 产生新的主密钥对。更详细地，该主密钥对由伪随机函数程序 PRF 产生，该伪随机函数程序具有如下功能 $PMK \leftarrow PRF_{-256}(APMK||SPMK)$，两个 Nonce :APMK 和 SPMK 是其输入。

[0067] 在接收到消息 1 后，请求者还能够使用新的主密钥对和传送的 ANonce' 和基于其自身产生的 SNonce' 来产生临时密钥对。该临时密钥对基于主密钥对用与上述的用

于第一认证的相同方式产生，这是通过 $PTK \leftarrow PRF_{-X}(PMK, \text{“两两密钥扩展”}, Min(AA, SPA)||Mas(AA, SPA)||Min(ANonce', SNonce')||Max(ANonce', SNonce'))$ Note：replace the“两两密钥扩展”with“密钥对扩展”

[0068] 进一步，在接收到消息 2 之后，认证者也能够产生新的主密钥对。更详细地，在接收消息 2 之后，该接入节点用共享的密钥 K 和 K’检查接受到的标记。如果标记正确，认证者将得到快速切换认证密钥 K_H。通过使用该快速切换认证密钥 K_H，认证者能够解密出 SPMK。利用传送的 SPMK 和其自身产生的 APMK，该成对的主密钥由请求者按照 $PMK \leftarrow PRF_{-256}(APMK||SPMK)$ 相同地执行而产生。

[0069] 由于标记是由 $Badge \leftarrow \{SPA, K_h, T_{life}, \lfloor SPA, K_h, T_{life} \rfloor_{K'}\}_K$ 产生，只有有效的认证者才能够通过使用 K 来解密标记而得到 K_h，并通过使用 K′ 来认证消息完整性编码检查标记是否是伪造的。在那之后，认证者能够使用 K_h 来解密 $\{SPA, T_{AP}, \{SPMK\}_{K_{AP}}\}_{K_h}$ 以得到 SPMK，同时，通过核查 T_{AP} 的值并比较从标记提取的 SPA 和存储在消息 2 中的 SPA，接入点 AP 能够检查 K_h 是否新鲜和有效。认证者通过核查从解密 $\{SPA, T_{AP}, \{SPMK\}_{K_{AP}}\}_{K_h}$ 提取的 SPMK，利用在消息 4 中传送的消息完整性编码，能够可选择地或者另外地核查 K_h 的有效性，这将在以下说明。认证者因此能够判定标记是否有效，并且标记是否属于 STA。有效的标记只能是在第一认证中由认证服务器认证成功而获得的信息，因此，对于认证者而言请求者是经过认证的。如果认证者判定标记无效或者生命期已满，认证者将结束第二认证，并将利用认证服务器开始第一认证或一个目前现有的 IEEE 802.11i 协议来认征。

[0070] 进一步，与由请求者执行的产生相同，在接收到消息 2 之后，认证者通过使用刚刚产生主密钥对和传送 SNonce’以及其自身的 ANonce’产生临时密钥对：$PTK \leftarrow PRF_{-X}(PMK, \text{“两两密钥扩展”}, Min(AA, SPA)||Mas(AA, SPA)||Min(ANonce', SNonce')||Max(ANonce', SNonce'))$

[0071] 应进一步注意到，认证者通过核查消息 2 内的 MIC，例如通过使用 KCK(Key Confirmation Key)程序能够检查接收的消息的完整性。如果该检查的结果正确，认证者将产生消息 3，并将其提交给请求者。该消息 3 包含用于消息 1 的相同的 ANonce’，在此新的标记指示为“标记 2“和消息完整性编码 MIC3。”标记 2“通过首先从临时密钥中分配给快速切换密钥的部分中提取新的快速切换认证密钥而产生，例如使用如上所述用于 CCMP 模式的比特 384 到 639，或者用于 TKIP 模式的比特 512 到 767。

[0072] 利用新的快速传递密钥，该认证者产生新的“标记“，这类似于如所述的关于第一认证的”标记“的产生。

[0073] 在接收到消息 3 之后，请求者通过检查消息 3 中的消息完整性编码 MIC3 可以决定认证者不是伪造接入点。只由当认证者能够产生正确的临时密钥对时，消息 3 才会包含由请求者检测的正确的 MIC3。这样，利用上述第二认证，执行了一种双向认证。

[0074] 最后，从请求者传送到认证者的消息 4 包括消息完整性编码 MIC4。如上面描绘的那样，MIC4 能够用于核查 k_H。由于 MIC4 的 KCK 从成对的主密钥 (PMK) 得出，认证者能够从 MIC4 判定 K_h 是否不正确。由于成对的主密钥是由 SPMK 得出，只有正确的 K_h 可将 SPMK 解密。

[0075] 利用上述实施方案，通过在用户（请求者）和接入点（认证者）产生主密钥对可

以避免通过使用耗时的认证例如现有的 IEEE802.1X EAP 认证。因此，减少了切换过程中的传输时间，这对于时间敏感性的应用是重要的，例如 VoWlan(voice over WLAN)。通过使用上述第二认证的过程，用户能够向接入点群的接入点多次认证。第二认证的使用受到“标记“的生命期的限制。一旦”标记“的生命期满（主密钥对的生命期），请求者必须再次使用用于提供认证的第一认证，其中以类似于 IEEE 802.1X EAP 认证的方式来连接认证服务器。因此，只有当一个用户之前已经使用第一认证进行了认证并且”标记“的生命期没有期满时，该用户才能够使用第二认证来进行认证。

[0076] 进一步地，第二认证仅仅使用 4 步信息交换协议，其中交换的 Nonce 用于在用户和接入点处本地产生该主密钥对，而不访问认证服务器，例如 RADIUS 服务器。因此，4 步信息交换协议的使用不仅仅提高了传递性能，而且提供了一种稳固的认证服务。而且，在第二认证中，不必由认证者记录和保持成对的主密钥识别 (PMKID) 的数据库，这不同于使用现有的 802.1X EAP 的认证的情况。

[0077] 另外，这里接入点群中的在各个接入点中用于验证“标记“的共享密钥在用户首次连接到接入点群之前完成共享设置。例如，如果群的这些接入点由同一公司布置，就可以在每个接入点内的配置中设置并维护共享密钥。另外，共享密钥也可以通过使用已有的有线或无线通信信道而共享，例如无线分布系统或者在每个接入点之间以安全方式设置的通用中继装置。每当一个新的接入点加入群中时，这个或这些共享密钥这时可传送到加入的接入点。进一步，这个或这些共享密钥可具有生命周期。在生命期满后，这个或这些共享密钥可由一个或多个新的密钥代替。

[0078] 参见图 6，现在将说明用于在请求者（用户）侧执行上述方法的第一示例性装置 500。例如，该装置 500 可包括一个具有合适硬件或软件的芯片。该装置 500 包括被配置为提供主密钥（例如上述的主密钥队）的第一个电路 502。在装置 500 内提供了一个控制器 504，用于决定是更具上述第一认证的第一模式还是相应于上述第二认证的第二模式来产生该主密钥。该控制器因此被配置为控制第一电路从远程装置（例如用于第一认证的认证者的第一接入点）接收的 EAP(Extensible Authentication Protocol) 消息中提取第一模式内的主密钥。如上所述，已经通过利用认证服务器产生了该第一模式中的主密钥。而且，基于从远程装置（例如用于第二认证的认证者的第二接入点）接收的信息中提取的第一个 Nonce 以及由第一电路产生的第二个 Nonce，控制器被配置为控制第一电路来产生第二模式中的主密钥。如上所述，从其中提取第一个 Nonce 的消息可以是参见图 5e 说明的信号交换的消息 1。

[0079] 以下将参见图 7 说明在认证者（接入节点）侧执行上述方法的装置 600 的一个进一步的实施方案。

[0080] 在图 7 中，装置 600 包括第一实体 602，例如该第一实体可以是在芯片上实施的一个电路，或者使用了固件或软件的一个硬件。该第一实体 602 被配置为从用户接收基于用户私密信息产成的第一信息和预定信息。如上所述，在各个实施方案中，该第一信息是一个密匙，只有寻求认证的用户知晓该密匙。通过向第一信息施加预定信息，该第一实体可进一步被配置为对用户进行认证。使用预定信息例如可包括使用共享密钥 K 和 K’ 对“标记“的解密过程，如以上参见图 5d 和 5e 的说明。

[0081] 尽管图 6 和 7 仅仅示出多个实施方案中的一个，应当理解，这些装置 500 和 600 也

可结合如上所述的进一步的特征和功能。

[0082] 在以上说明中，在此已经说明和示出的实施方案以足够的细节来使本领域技术人员能够实践在此披露的传授内容。其他的实施方案可加以利用并可从此导出，在不脱离本发明范围的情况下，可以做出这些结构和逻辑代替以及改变。

[0083] 因此，这一详细的说明不应在限制性意义来看待，并且不同实施方案的范围仅应由所附权利要求连同这些权利要求有权享有的等效物的全部范围来限定。

[0084] 本发明主题的这些实施方案可在此独立地和 / 或共同地被称为术语“发明”，这仅仅是为了方便，而不是旨在主动地限制本申请的范围为单个发明或发明概念（如果事实上公开了多个发明的话）。因此，尽管在此已经示出和说明了具体实施方案，应当理解，任何打算获得相同目的的装置都可代替所示的具体实施方案。本披露旨在覆盖各种实施方案的任何和全部改编或变体。上述实施方案的组合以及在此没有具体说明的其他实施方案对于阅读了上述说明后的本领域技术人员都将是清楚的。

[0085] 应进一步注意到，在本说明书和权利要求书中使用的具体术语可以在广义上进行解释。例如，在此使用的术语“电路”或“电路系统”应解释的含义是不仅包括硬件，而且包括软件、固件和其任何组合。术语“数据”可解释为包括任何形式的表述，例如模拟信号表述、数字信号表述、载波信号上的调制等。术语“信息”可在任何形式的数字信息外还包括表示信息的其他形式。术语“实体”在各个实施方案中可包括任何器件、装置、电路、硬件、软件、固件、芯片或其他半导体以及各个协议层的逻辑单元或物理实施等。另外，术语“耦合”或“连接”可在广义上解释为不仅包括直接的而且也包括间接的耦合。

[0086] 应进一步注意，与具体实体结合说明的各个实施方案可以在这些实体的实施方式之外还包括以一个或多个子实体或所述实体的子部分的一种或多种实施方式。例如，在此说明的具体实施方案在此实施为发射机、接收机或收发器，它们可以在子实体中实施为例如芯片或电路或者芯片或电路的一部分。

[0087] 于此形成一部分的附图通过展示而非限制的方式示出多个实施方案，其中可执行该主题。

[0088] 在以上详细的说明中，可以看出，为了简化本披露的目的，将不同特征进行分组聚集到单个实施方案中。这种披露方法不应被解释为所反映的意图是所要求保护的实施方案需要比每项权利要求明确列出的内容更多的特征。相反，如以下的权利要求所反映出，发明主题在于比单个披露的实施方案的全部特征要少。因此，以下的权利要求特此结合到详细的说明中，其中每个权利要求可依据其自身作为一个单独的实施方案。尽管每个权利要求依据其自身作为单独的实施方案，应当注意，尽管在权利要求书中一项从属权利要求可指明与一个或多个其他权利要求的具体结合，其他实施方案也可包括该从属权利要求与其他从属权利要求的主题的组合。

[0089] 应进一步注意到，本说明书或权利要求中公开的方法可由一种装置来执行，该装置具有用于执行这些方法的各个步骤的装置。

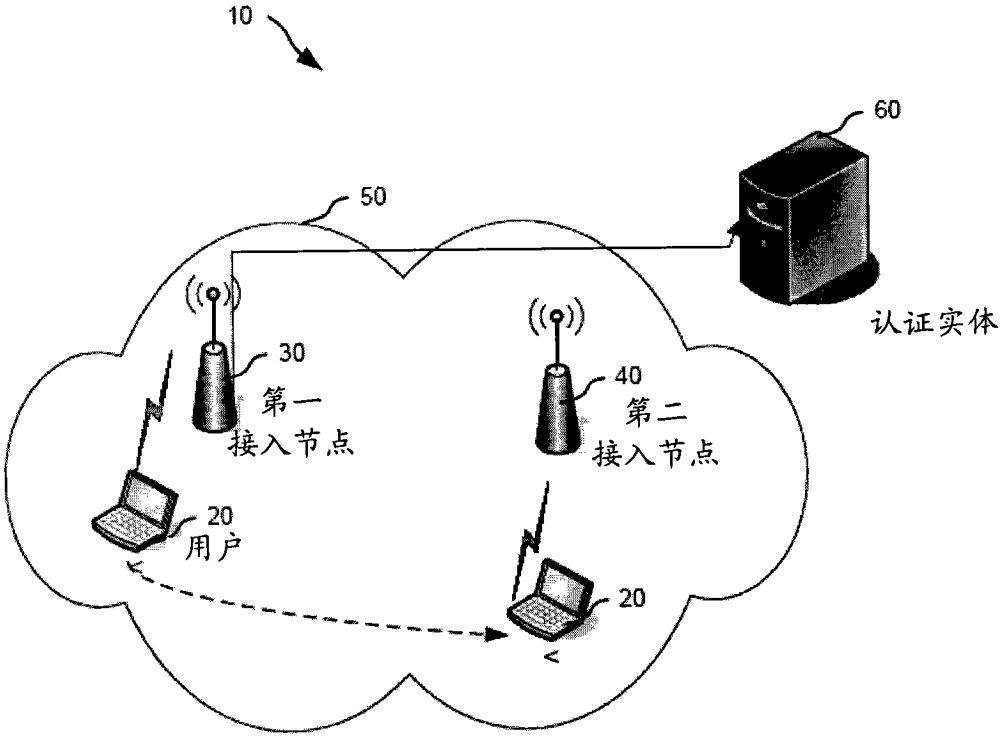

10
60
50
认证实体
30
第一
接入节点
40
第二
接入节点
20
用户
20

图 1

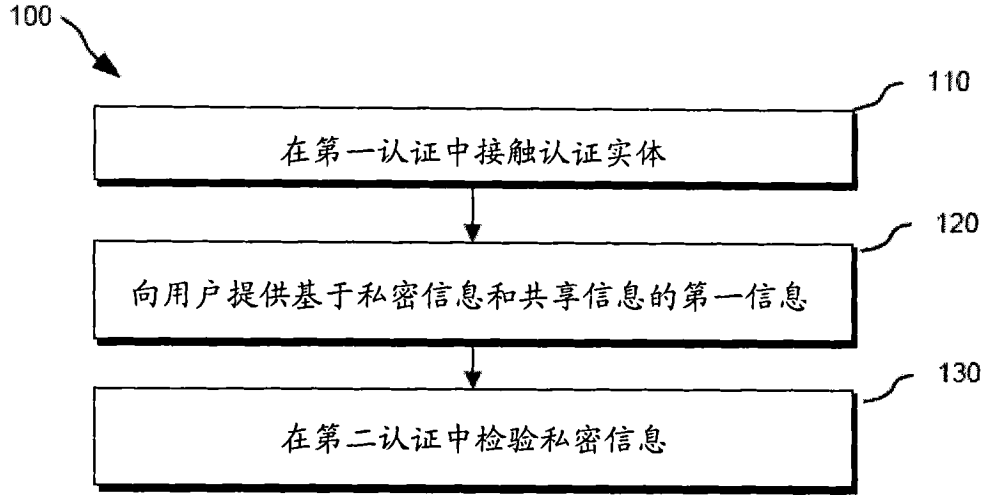

100
110
在第一认证中接触认证实体
120
向用户提供基于私密信息和共享信息的第一信息
130
在第二认证中检验私密信息

图 2

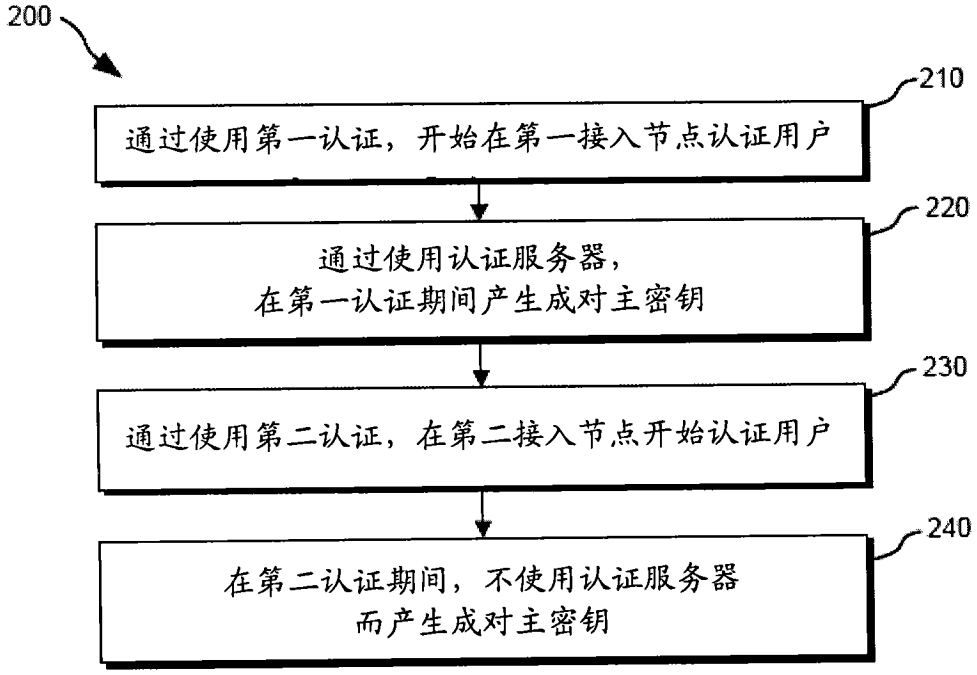

200
210
通过使用第一认证，开始在第一接入节点认证用户
220
通过使用认证服务器，
在第一认证期间产生成对主密钥
230
通过使用第二认证，在第二接入节点开始认证用户
240
在第二认证期间，不使用认证服务器
而产生成对主密钥

图 3

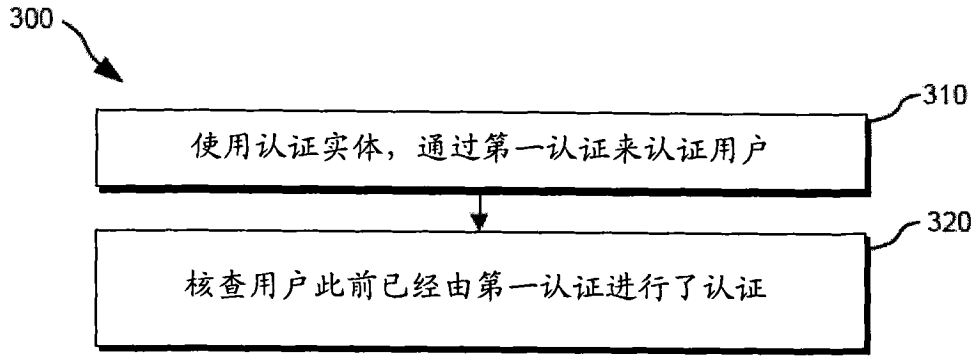

300
310
使用认证实体，通过第一认证来认证用户
320
核查用户此前已经由第一认证进行了认证

图 4

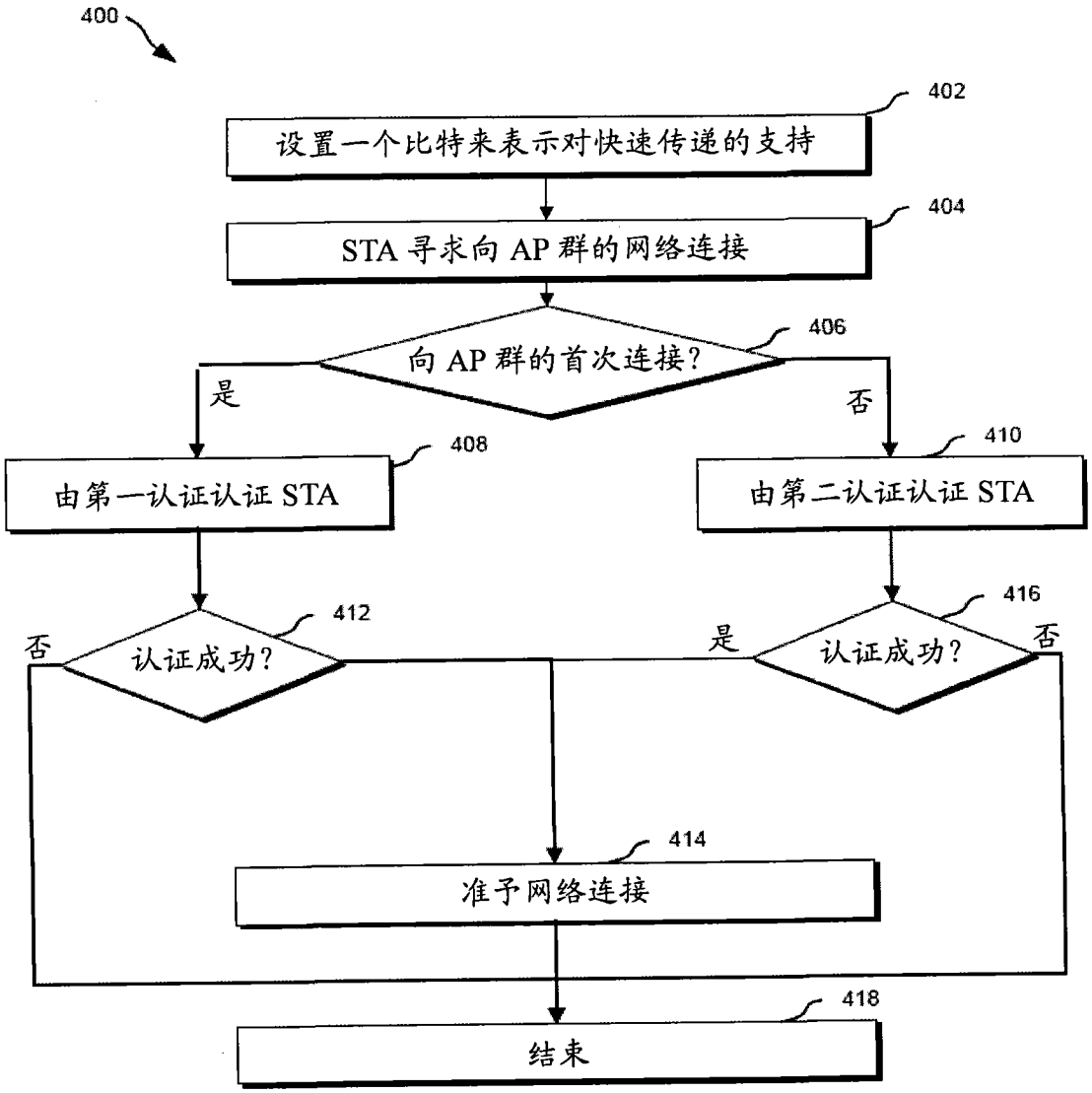

400
402
设置一个比特来表示对快速传递的支持
404
STA 寻求向 AP 群的网络连接
406
向 AP 群的首次连接?
是
否
408
由第一认证认证 STA
410
由第二认证认证 STA
412
否
认证成功?
是
416
认证成功?
否
414
准予网络连接
418
结束

图 5a

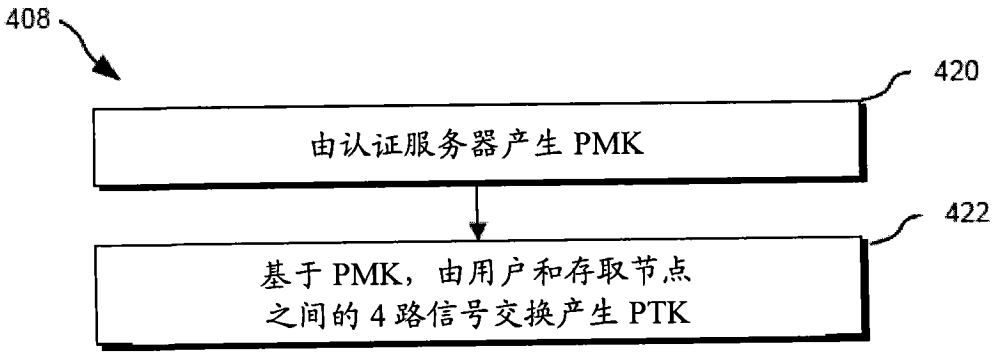

408
420
由认证服务器产生 PMK
422
基于 PMK，由用户和存取节点
之间的 4 路信号交换产生 PTK

图 5b

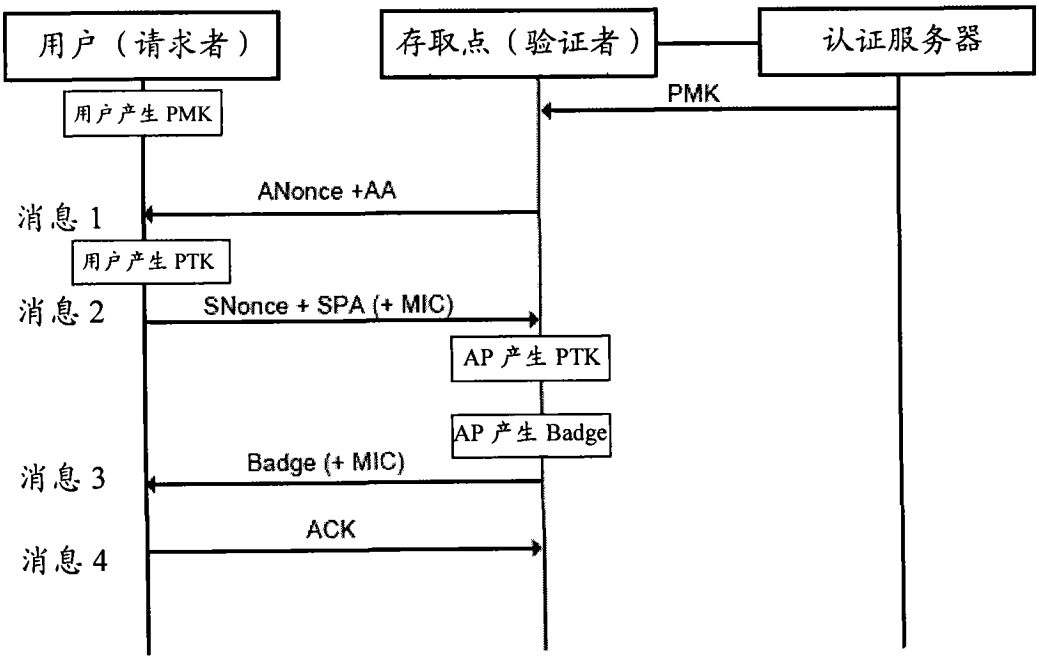

用户（请求者）
存取点（验证者）
认证服务器
用户产生 PMK
PMK
ANonce +AA
消息 1
用户产生 PTK
消息 2
SNonce + SPA (+ MIC)
AP 产生 PTK
AP 产生 Badge
消息 3
Badge (+ MIC)
ACK
消息 4

图 5c

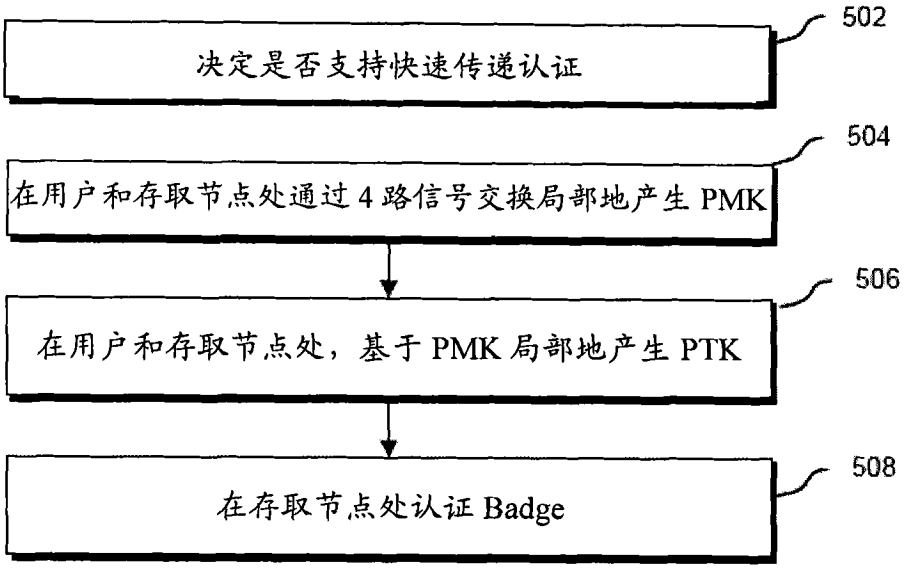

502
决定是否支持快速传递认证
504
在用户和存取节点处通过 4 路信号交换局部地产生 PMK
506
在用户和存取节点处，基于 PMK 局部地产生 PTK
508
在存取节点处认证 Badge

图 5d

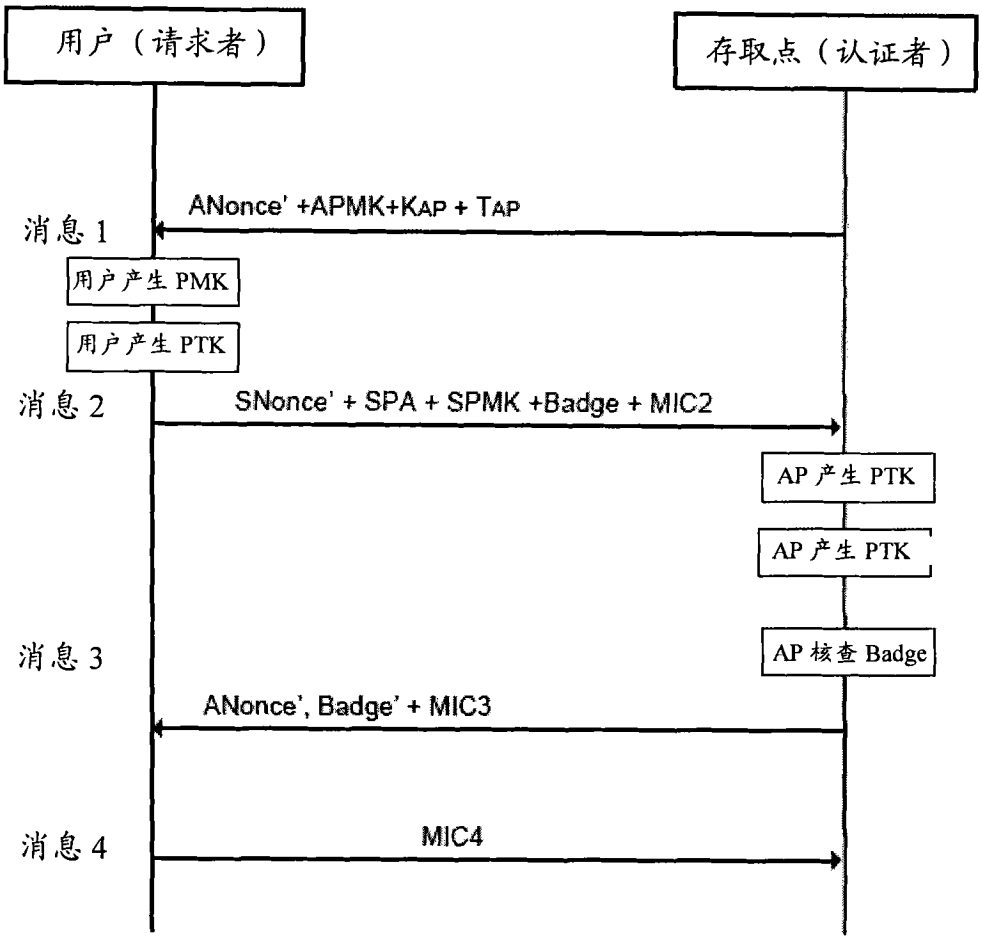

用户（请求者）
存取点（认证者）
消息 1
ANonce' +APMK+KAP + TAP
用户产生 PMK
用户产生 PTK
消息 2
SNonce' + SPA + SPMK +Badge + MIC2
AP 产生 PTK
AP 产生 PTK
消息 3
AP 核查 Badge
ANonce', Badge' + MIC3
消息 4
MIC4

图 5e

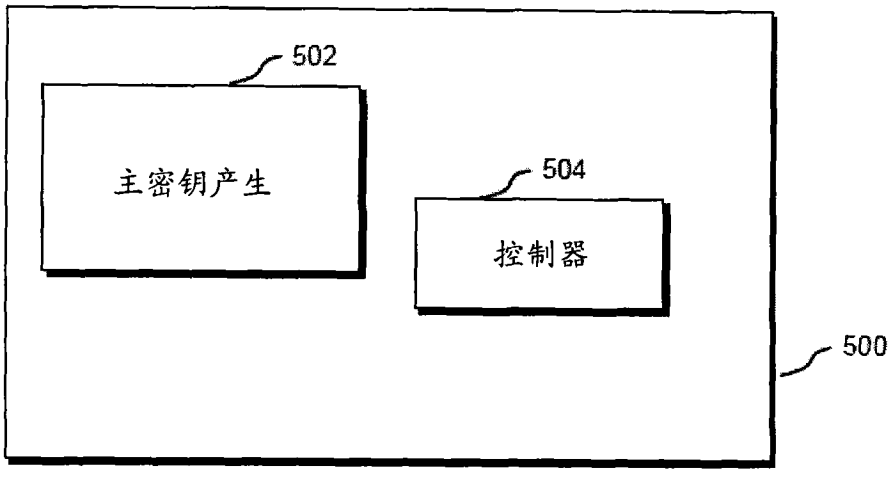

502
主密钥产生
504
控制器
500

图 6

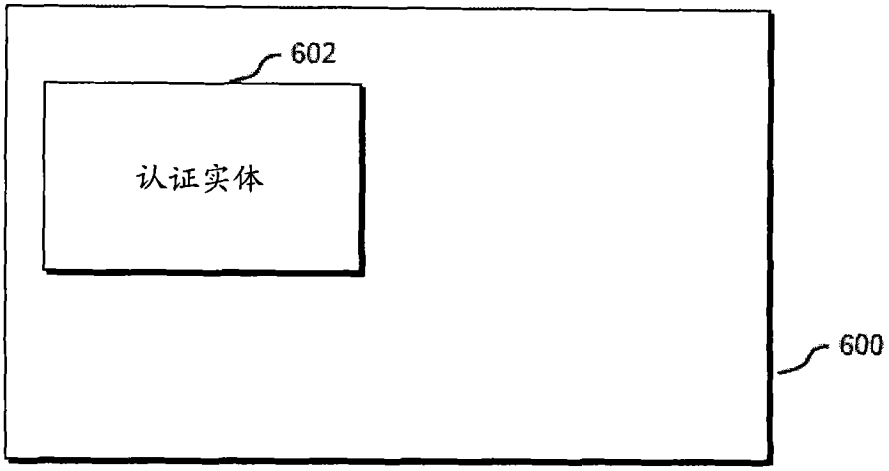


图 7