(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101621798 B
(45)授权公告日 2012.11.14

(21)申请号 200910158679.6
(22)申请日 2003.08.13
(30)优先权数据
60/403,495 2002.08.14 US
(62)分案原申请数据
03823011.9 2003.08.13
(73)专利权人 汤姆森特许公司
地址 法国布洛涅－比扬库尔
(72)发明人 张俊彪
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 吕晓章
(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 76/02(2009.01)
H04W 84/12(2009.01)
H04W 88/02(2009.01)
(56)对比文件
CN 1351789 A,2002.05.29,
CN 1444362 A,2003.09.24, 全文.
CN 1351789 A,2002.05.29,
US 2002/0037708 A1,2002.03.28,
US 2002/0037708 A1,2002.03.28,
审查员 张嘉凯

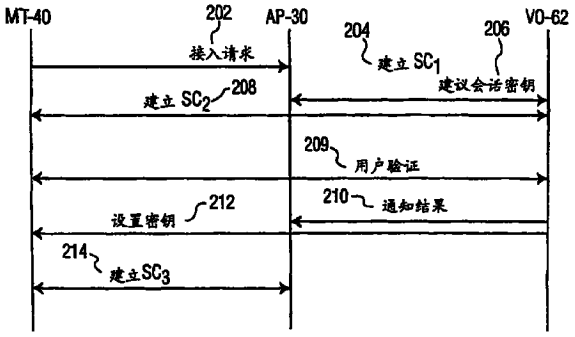
权利要求书 1 页 说明书 4 页 附图 3 页

(54)发明名称

支持多个虚拟操作员的公共无线局域网的会话密钥管理

(57)摘要

一种用于管理会话密钥的方法和装置，其用于使得移动终端可以接入无线局域网(WLAN)。本发明提供了：在接入点和虚拟操作员之间建立第一安全信道，并且从接入点向虚拟操作员建议会话密钥。在虚拟操作员和用户之间建立第二安全信道，并且在用户认证成功时经由第二安全信道向用户发送会话密钥。移动终端使用会话密钥来接入WLAN。按照本发明的一种移动终端，包括：用于发送接入WLAN的请求的部件；以及用于经由安全信道与服务提供商虚拟操作员进行通信以认证所述移动终端的部件，其中所选的会话密钥经由所述安全信道被传送给所述移动终端，以及，其中在接收到所选的会话密钥后，所述移动终端使用所述会话密钥来进行通信。



CN 101621798 B

1. 一种移动终端，包括：

用于发送在接入点 AP 接入无线局域网 WLAN 的请求的部件；以及

用于经由第二安全信道与服务提供商虚拟操作员进行通信以认证所述移动终端的部件，其中所选的会话密钥经由所述第二安全信道被传送给所述移动终端，所选的会话密钥由所述 AP 预先选择并且由所述 AP 经由第一安全信道传送给所述虚拟操作员，以及在接收到所选的会话密钥后，所述移动终端使用所述会话密钥来进行通信。

2. 按照权利要求 1 的移动终端，其中一旦用户认证成功，所述服务提供商虚拟操作员向 AP 通知，并且然后所述移动终端使用所述会话密钥来与 AP 进行通信。

3. 按照权利要求 1 的移动终端，其中所述虚拟操作员包括 Internet 服务提供商、蜂窝提供商和信用卡提供商中的一个。

支持多个虚拟操作员的公共无线局域网的会话密钥管理

[0001] 本申请是申请日为 2003 年 08 月 13 日、申请号为 03823011.9、发明名称为“支持多个虚拟操作员的公共无线局域网的会话密钥管理”的发明专利申请的分案申请。

技术领域

[0002] 本发明一般涉及网络通信，具体涉及用于在支持第三方虚拟操作员的公共无线局域网 (WLAN) 环境中管理对会话密钥的接入的机制。

背景技术

[0003] 当前的无线局域网 (WLAN) 认证、授权和计费 (AAA) 解决方案没有对 WLAN 操作员提供保持与多个虚拟操作员的业务关系的足够支持，具体上是相对于用于 WLAN 接入的会话密钥的管理。不能正确地控制和管理会话密钥会导致可能的安全和管理问题。

[0004] WLAN 正在被越来越多地部署在诸如旅馆、飞机场和快餐店的热点中。一种健全的和有效的 AAA（认证、授权和计费）解决方案对于使能安全的公共无线 LAN 接入很重要。具体上，这样的 AAA 解决方案应当能够支持虚拟操作员概念，其中，诸如 ISP、蜂窝操作员和预付卡提供者的第三方提供者向公共 WLAN 和无线用户提供 AAA 服务。以这种方式，无线用户不必每次他们去不同的热点时打开帐户或通过信用卡支付；相反，他们可以使用现有的 ISP 帐户、蜂窝帐户或在任何地方购买的预付卡来获得对于公共 WLAN 的接入。这可以大大地增加 WLAN 操作员以及第三方虚拟操作员的商业机会。但是，当前的无线 LAN 接入方案全部被设计用于其中仅仅使用单个认证服务器的本地配置中，诸如联合环境。例如，IEEE 802.11 标准组织选择 IEEE 802.1x 来作为 WLAN 接入控制的解决方案，并且当前的使用模式使用认证服务器来控制会话密钥分配。当这对于联合环境等足够时，在可以共存属于不同的商业实体的多个认证服务器的公共热点中存在一定的问题。如果完全可能的话，对于这些认证服务器很难协调接入点的密钥分配。

[0005] 现在说明当前的密钥分配。在一种情况下，在公共 WLAN 热点中的移动用户与 WLAN 接入点没有预先的信任关系。用户意欲使用第三方服务提供者（例如因特网服务提供商 (ISP)）来作为信任桥接实体。服务提供商可以被称为虚拟操作员。用户与这个虚拟操作员保持一个帐户，所述虚拟操作员与 WLAN 操作员具有业务关系。因为用户与虚拟操作员具有已经建立的信任关系，因此她能够以安全的方式向虚拟操作员认证她本身。虚拟操作员然后安全地向用户以及 WLAN 接入点发送会话密钥（因为虚拟操作员也与 WLAN 具有信任关系）。因为这个共享的会话密钥，无线 LAN 于是知道用户被授权来接入网络，因此准许用户接入。注意，在这个方案中，虚拟操作员分配会话密钥，因为它与用户和 WLAN 都具有信任关系。

[0006] 会话密钥用于本地接入，应当对于 WLAN 接入点是本地的，例如被接入点分配和保持。当存在多个虚拟操作员时，上述的密钥管理方案在至少两个区域有问题。首先，对于虚拟操作员，经常有的问题是：对于术语不同实体的成千上万的接入点分配和管理会话密钥，即，对于不同类型的接入点提供不同的加密算法和密钥长度。其次，对于接入点，可能难于

保证多个虚拟操作员以一致的方式来分配会话密钥，例如，必须保证两个用户不同时使用由两个不同的虚拟操作员分配的相同密钥。

[0007] 主要困难是接入点不与无线用户共享秘密，因此从接入点向用户直接发送会话密钥是不安全的。对于这个问题的解决方案是虚拟操作员在成功的用户认证后向接入点 (AP) 通知用户的公共密钥。AP 然后使用用户的公共密钥来加密会话密钥，然后向用户发送结果。因为仅仅那个特定的用户能够使用她的对应私有密钥来解密会话密钥，因此可以在 AP 和无线用户之间能安全地建立会话密钥。但是，这个方案需要使用公共 / 私有密钥，它们可能与在无线用户和认证服务器之间的实际的认证方法不兼容。有可能用户需要保存两种不同类型的密钥（用于解密会话密钥的私有密钥和用于使用认证服务器认证的密码类型密钥）。这不仅增加客户机软件的复杂性，而且增加了安全保存密钥的困难。此外，这种方案不用正成为 WLAN 安全的标准 IEEE 802.1x 进行工作。

[0008] 因此，需要一种解决方案，其中密钥被接入点本地分配和管理，并且，无线用户能够安全地获得会话密钥而没有与接入点的预先信任关系。

发明内容

[0009] 本发明描述了一种有效的处理这个问题的机制。会话密钥被 WLAN 本地分配和管理（因为这些密钥用于本地接入控制），但是，它们可以安全地被分配到与它们对应的虚拟操作员保持信任关系的无线用户。

[0010] 一种无线局域网的会话密钥管理的方法，包括 :在接入点和虚拟操作员之间建立第一安全信道，并且从接入点向虚拟操作员建议会话密钥。在虚拟操作员和用户之间建立第二安全信道，并且由虚拟操作员发送会话密钥，以使能在接入点和用户之间的通信。

[0011] 一种用于无线局域网的会话密钥管理的系统，包括 :接入点，它在接入点和虚拟操作员之间建立第一安全信道。从接入点向虚拟操作员建议会话密钥。虚拟操作员在用户的认证后，在虚拟操作员和用户之间建立第二安全信道，虚拟操作员设置会话密钥，以使能在接入点和用户之间的通信。

[0012] 按照本发明的一个方面，提供一种移动终端，包括 :用于发送接入 WLAN 的请求的部件 ;以及用于经由安全信道与服务提供商虚拟操作员进行通信以认证所述移动终端的部件，其中所选的会话密钥经由所述安全信道被传送给所述移动终端，以及，其中在接收到所选的会话密钥后，所述移动终端使用所述会话密钥来进行通信。

附图说明

[0013] 根据现在参照附图详细说明的说明性实施例，本发明的优点、特征和各种附加特点将会变得更加清楚，其中 :

[0014] 图 1 是按照本发明的一个实施例的示例系统 ;

[0015] 图 2 是按照本发明的一个实施例的用于实现会话密钥管理的方法的说明性步骤的流程图 ;

[0016] 图 3 是按照本发明的另一个实施例的、无线局域网的会话密钥管理的另一种说明性方法的图。

[0017] 应当明白，附图是为了图解本发明的思想，而不必用于说明本发明的仅仅可能的

配置。

具体实施方式

[0018] 本发明一般涉及网络通信，具体涉及用于在支持第三方虚拟操作员的公共无线局域网 (WLAN) 环境中管理接入会话密钥的机制。这样的虚拟操作员可以包括因特网服务提供商 (ISP)、蜂窝操作员或预付卡提供商。为了最大化收入来源，公共无线局域网 (WLAN) 可以与多个虚拟操作员保持业务关系。

[0019] 应当明白，以 WLAN 系统来说明本发明，所述 WLAN 系统诸如符合 IEEE802.11、Hiperlan 2 和 / 或超宽带标准的那些；但是，本发明范围更宽，并且可以被应用到用于其他通信系统的其他系统管理方案。另外，本发明可以被应用到任何网络系统，包括电话、电缆、计算机（因特网）、卫星等。

[0020] 现在具体详细地参考附图，其中在几个视图中类似的附图标记表示类似或相同的元件，首先参见图 1，公共无线局域网 (WLAN)14 包括 WLAN 热点 31 的接入点 30。WLAN 14 可以使用例如 IEEE 802.11 和 HIPERLAN2 标准。WLAN 14 可以包括在诸如因特网 7 的外部网络之间的防火墙 22。终端用户或移动单元 40 可以使用例如 HTTPS 通道或其他安全的信道 64 来通过因特网 7 从 WLAN 14 接入虚拟操作员 62，如在此所述。

[0021] 分散在蜂窝网络的小区之间或之内的是无线局域网 14。按照本发明，从虚拟操作员 62 向用户 40 发送会话密钥 60。虚拟操作员 62 可以包括因特网服务提供商 (ISP)，蜂窝操作员或预付卡提供商或其他实体，它们通过通信网络提供服务。为了最大化收入来源，公共无线局域网 (WLAN) 可以与多个虚拟操作员保持业务关系。但是，在保持足够的系统安全性的同时，保持多个虚拟操作员很难。

[0022] 因为虚拟操作员 62 和用户 (MS 40) 共享诸如安全信道的秘密或使用共享的信息段或代码，因此可以通过在其间的安全信道 64 来发送密钥 60。但是，取代具有确定和保持会话密钥 60 的虚拟操作员 62，所述密钥被 WLAN 接入点 30 选择，然后向虚拟操作员提示。可以通过多种方法来选择密钥，包括例如随机数量产生、从预存的多个密钥选择等。

[0023] 参见图 2，用于实现本发明的实施例被说明性地描述如下。在方框 102 中，用户（移动终端 (MT)）在接入点 (AP)30 请求无线 LAN 接入，并且指定虚拟操作员 (VO)62。在方框 104，AP 30 建立与虚拟操作员 62 的安全信道 SC_1。通过 SC_1 在 AP 30 和虚拟操作员 62 之间进行所有随后的通信。在方框 106，用户与虚拟操作员 62 建立安全信道 SC_2，并且通过 SC_2 用虚拟操作员认证她自己。这可以包括将会话密钥保存直到成功的用户认证。

[0024] 在方框 108，虚拟操作员在成功的用户认证后向 AP 30 通知结果，并且通过 SC_1 向 AP 30 查询会话密钥 60。如果会话密钥被保存，则如果认证不成功就去除它。在方框 110，AP 30 选择会话密钥 60 并且将其通过 SC_1 向虚拟操作员 62 发送。在方框 112，虚拟操作员通过 SC_2 向用户发送这个会话密钥。在方框 114，用户和 AP 30 开始使用会话密钥来用于在它们之间的后续通信（安全信道 SC_3）。

[0025] 参见图 3，可以如图所示进一步将图 2 所示的方法在速度和效率上进行改善。取代在成功的认证后使虚拟操作员询问会话密钥，AP 30 就在建立 SC_1 后提供建议的会话密钥，并且在接入点 30 将此密钥“保存”在存储器 24 中。在成功的用户认证后，AP 30 被虚拟操作员通知，并且对于 SC_3 开始使用这个密钥。在不成功的认证的情况下（例如在用户进行

一定数量的不成功尝试后），也通知 AP 30，并且从“保存”列表 24 中去除所述密钥。这防止了拒绝服务的攻击，其中攻击者持续进行不成功的认证尝试。如果 AP 没被通知不成功的认证，则所建议的密钥将积累在 AP 的存储器中。认证步骤可以包括如下。

[0026] 在步骤 202，用户在 AP 30 请求无线 LAN 接入，并且指定虚拟操作员 62。在步骤 204，AP 30 与虚拟操作员 62 建立安全信道 SC_1。通过 SC_1 在 AP 和虚拟操作员之间进行所有随后的通信。在步骤 206，AP 30 向虚拟操作员 62 发送所建议的会话密钥，并且将这个密钥“保存”。在步骤 208，用户与虚拟操作员 62 建立安全信道 SC_2，并且在方框 209 通过 SC_2 用虚拟操作员 62 认证她本身。在步骤 210，虚拟操作员 62 向 AP 30 通知认证结果，并且 AP 30 从所述“保存”列表去除所建议的密钥。在方框 212，在成功的认证后，虚拟操作员 62 向用户发送会话密钥。在方框 214，用户和 AP 30 开始使用会话密钥来用于在它们之间（安全信道 SC_3）的后续通信。

[0027] 图 3 的方法为什么更有效的原因是因为它比图 2 的方法节省了一个往返行程的通信时间，例如，虚拟操作员不必等待直到认证结束，以向 AP 查询会话密钥，并且向用户通知所述密钥。虽然在步骤 206 中 AP 需要向虚拟操作员发送所建议的密钥，但是这可以与步骤 208 并行进行。因此，总的来说，避免了往返行程。在其他实施例中，可以伴随步骤 208 顺序地执行步骤 206。

[0028] 应当明白，可以在移动终端、接入点和 / 或蜂窝网络中例如以各种形式的硬件、软件、固件、专用处理器或其组合来实现本发明。最好，本发明实现为硬件和软件的组合。而且，所述软件最好实现为在程序存储器上确实地包含的应用程序。所述应用程序可以被上载到包括任何适用的架构的机器并且由其执行。最好，在计算机平台上实现所述机器，所述计算机平台具有硬件，诸如一个或多个中央处理单元 (CPU)、随机存取存储器 (RAM) 和输入 / 输出 (I/O) 接口。所述计算机平台也包括操作系统和微指令代码。在此所述的各种处理和功能可以或者是经由操作系统执行的微指令代码的一部分或应用程序的一部分（或其组合）。另外，各种其他的外围器件可以连接到计算机平台，诸如附加的数据存储器和打印设备。

[0029] 还应当明白，因为附图中所述的构成系统部件和方法步骤的一些可以用软件来实现，因此在系统部件（或处理步骤）之间的实际连接可以根据本发明所编程的方式而不同。在此提供示教的情况下，在本领域的普通技术人员将能够考虑本发明的这些和类似的实现方式或配置。

[0030] 在已经描述了支持多个虚拟操作员的公共无线局域网的会话密钥管理的优选实施例（它们意欲是说明性和非限定性的）的情况下，可以注意到，本领域的技术人员可以根据上述教程来进行修改和改变。因此，应当明白，可以在由所附的权利要求概述的本发明的范围和精神内公开的本发明的特定实施例中进行改变。在已经以专利法所要求的详细程度来描述了本发明的情况下，在所附的权利要求中给出了由专利证书要求保护和期望保护的内容。

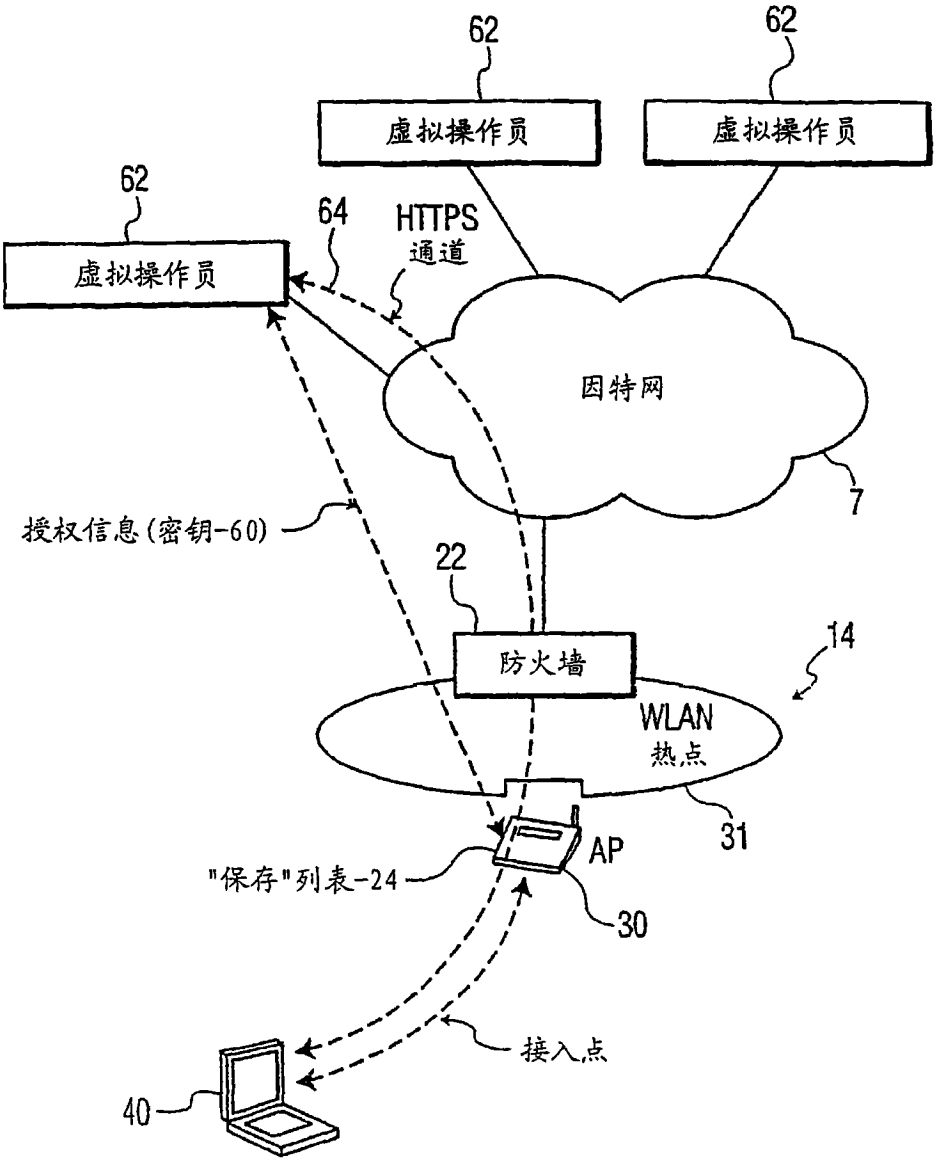

62
62
虚拟操作员
虚拟操作员
62
64
HTTPS
通道
虚拟操作员
因特网
7
授权信息(密钥-60)
22
防火墙
14
WLAN
热点
31
AP
"保存"列表-24
30
接入点
40

图 1

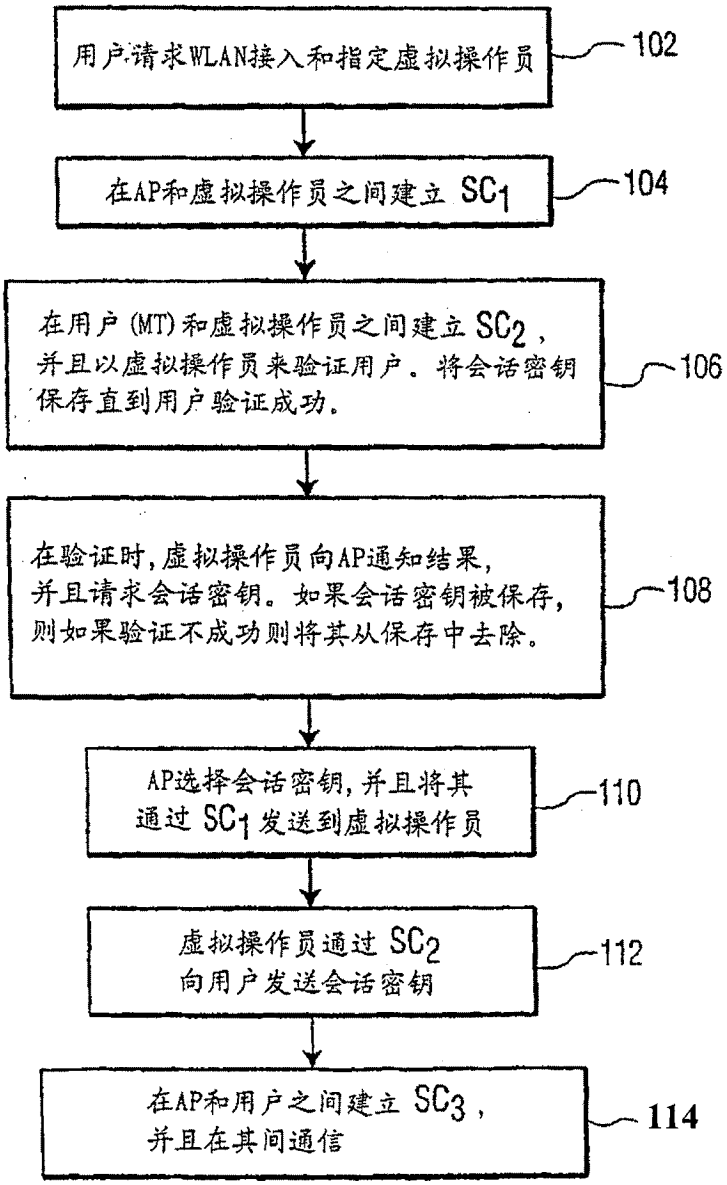

用户请求WLAN接入和指定虚拟操作员
102
在AP和虚拟操作员之间建立 SC1
104
在用户(MT)和虚拟操作员之间建立 SC2，并且以虚拟操作员来验证用户。将会话密钥保存直到用户验证成功。
106
在验证时，虚拟操作员向AP通知结果，并且请求会话密钥。如果会话密钥被保存，则如果验证不成功则将其从保存中去除。
108
AP选择会话密钥，并且将其通过 SC1 发送到虚拟操作员
110
虚拟操作员通过 SC2 向用户发送会话密钥
112
在AP和用户之间建立 SC3，并且在其间通信
114

图 2

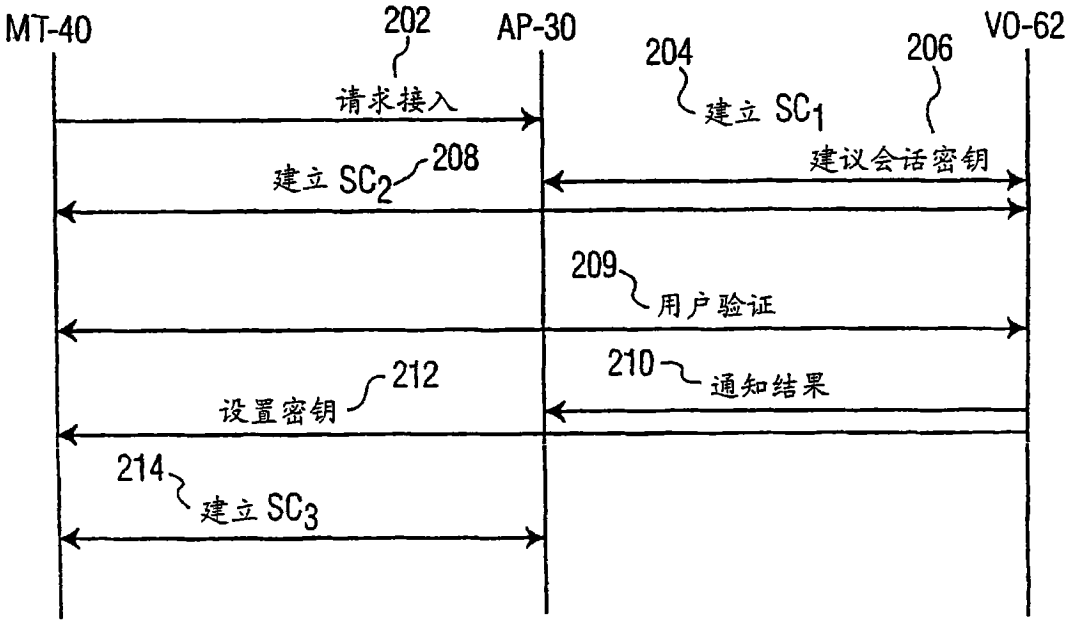

MT-40
202
AP-30
204
206
VO-62
请求接入
建立 SC1
建立 SC2
208
建议会话密钥
209
用户验证
210
通知结果
212
设置密钥
214
建立 SC3

图 3