[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)

[12] 发明专利说明书

专利号 ZL 02828879.3

[45] 授权公告日 2008 年 1 月 30 日

[11] 授权公告号 CN 100366007C

[22] 申请日 2002.5.1 [21] 申请号 02828879.3
[86] 国际申请 PCT/EP2002/004865 2002.5.1
[87] 国际公布 WO2003/094438 英 2003.11.13
[85] 进入国家阶段日期 2004.11.1
[73] 专利权人 爱立信电话股份有限公司
地址 瑞典斯德哥尔摩
[72] 发明人 赫苏斯·安赫尔·德·格雷戈里奥·罗德里格斯
米格尔·安赫尔·蒙哈斯·略化特
[56] 参考文献
CN1341338A 2002.3.20
WO0176297A1 2001.10.11
WO0211468A2 2002.2.7
US2002012433A1 2002.1.31
CN1248367A 2000.3.22
审查员 杨继彬
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 李亚非 刘 杰

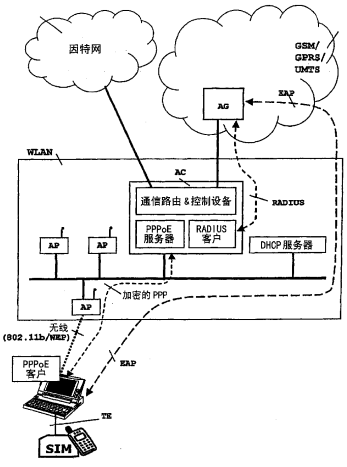
权利要求书 4 页 说明书 12 页 附图 4 页

[54] 发明名称

用于在无线局域网接入的基于 SIM 的鉴权和加密的系统、设备和方法

[57] 摘要

本发明涉及一种系统、设备和方法，用于对接入 WLAN 的用户进行基于 SIM 的鉴权以及用于保护终端设备和移动网络之间的路径的层 2 加密机制，而无需提供 IP 连接。 因此，本发明提供了一种方法，用于针对终端和接入控制器之间的 AKA 对话建立 PPP 通道，所述接入控制器用于接入属于 SIM 的移动网络。 本发明还提供了一种接入控制器(AC)，包括以太网点对点(PPPoE)服务器，用于针对相同目的挖掘在终端种安装的 AKA 对话形式的 PPP 客户，还包括业务路由器和 RADIUS 客户。 因此，将包括 RADIUS 客户的 AC 插入到从 WLAN 种的接入点(AP)接入的 RADIUS 代理和其中执行基于 SIM 的鉴权的移动网络之间。



1. 一种电信系统中的方法，用于允许针对作为公共陆地移动网络订户的无线局域网用户进行基于 SIM 的鉴权，该方法包括步骤：

（a）无线终端通过可接入的接入点接入无线局域网；

（b）该无线终端发现插入在接入点和公共陆地移动网络之间的接入控制器；

（c）在无线终端和公共陆地移动网络之间通过该接入控制器执行询问—响应鉴权过程，无线终端配备有 SIM 卡并适于读取其数据；

所述方法的特征在于，

步骤（c）中的询问—响应鉴权过程的提交在向用户提供 IP 连接之前发生，在以下组件中携带所述询问—响应鉴权过程的提交；

- 在无线终端和接入控制器之间的点对点层 2 协议（PPPoE）上；以及

- 在位于公共陆地移动网络和接入控制器之间的应用层处的鉴权协议上；以及

所述方法还包括步骤：

（d）一旦公共陆地移动网络对所述用户有效地进行了鉴权，则通过发送已分配的 IP 地址和其它网络配置参数来向无线终端处的用户提供 IP 连接。

2. 根据权利要求 1 所述的方法，其中，发现接入控制器的步骤（b）包括步骤：在位于无线终端的以太网上点对点（PPPoE）协议客户和位于接入控制器上的以太网上点对点（PPPoE）协议服务器之间建立点对点协议会话。

3. 根据权利要求 1 所述的方法，其特征在于，执行询问—响应鉴权过程的步骤（c）包括以下步骤：

（c1）将来自无线终端的用户标识符通过接入控制器发送到公共陆地移动网络；

（c2）在无线终端通过接入控制器接收来自公共陆地移动网络的鉴权询问；

（c3）在无线终端从所接收的询问中导出加密密钥和鉴权响应；

（c4）将来自无线终端的鉴权响应通过接入控制器发送到公共陆地移动网络；

（c5）在接入控制器处接收来自公共陆地移动网络的加密密钥；以及

（c6）在接入控制器处提取所接收的加密密钥，用于进一步加密与无线终端通信的通信路径。

4. 根据权利要求 2 所述的方法，其特征在于还包括步骤：为了向公共陆地移动网络提交，将在点对点层 2 协议（PPPoE）上接收的鉴权信息向上传送到位于应用层处的鉴权协议。

5. 根据权利要求 4 所述的方法，其特征在于还包括步骤：为了向无线终端提交，将在应用层处设置的鉴权协议上接收的鉴权信息向下传送到在点对点层 2 协议（PPPoE）上。

6. 根据权利要求 3 所述的方法，其特征在于还包括步骤：利用前面在接入控制器和无线终端处导出的加密密钥，在无线终端处建立对称的加密路径。

7. 根据权利要求 1 所述的方法，其特征在于，在发送 IP 地址的步骤（d）之前，该方法包括：向动态主机配置协议服务器请求这种 IP 地址的步骤。

8. 根据权利要求 1 所述的方法，其特征在于，接入控制器和公共陆地移动网络之间的通信通过所述公共陆地移动网络的鉴权网关。

9. 根据权利要求 8 所述的方法，其特征在于，接入控制器和鉴权网关之间的通信通过无线局域网的鉴权服务器，所述鉴权服务器负责鉴权不是移动订户的所述无线局域网的本地用户。

10. 根据权利要求 3 所述的方法，其特征在于步骤 c1）中的用户标识符包括网络接入标识符。

11. 根据权利要求 3 所述的方法，其特征在于步骤 c1）中的用户标识符包括全球移动用户身份。

12. 根据权利要求 1 所述的方法，其特征在于步骤 c）中位于应用层处的鉴权协议是可扩展鉴权协议。

13. 根据权利要求 12 所述的方法，其特征在于在 RADIUS 协议上传输该可扩展鉴权协议。

14. 根据权利要求 12 所述的方法，其特征在于在 Diameter 协议上传输该可扩展鉴权协议。

15. 一种电信系统中的接入控制器，所述系统包括具有至少一个

接入点的无线局域网，公共陆地移动网络和至少一个提供有 SIM 卡并适于读取其用户数据的终端设备，其特征在于，所述接入控制器包括:

（a）点对点层 2 协议(PPPoE)服务器，用于与无线终端进行通信，并且被安排用来为询问—响应鉴权过程建立隧道;

（b）位于 OSI 应用层的鉴权协议，用于与公共陆地移动网络进行通信；以及

（c）向无线终端发送已分配的 IP 地址和其它网络配置参数的装置，用于在电信系统的终端设备和公共陆地移动网络之间成功地执行询问—响应鉴权过程之后提供 IP 连接。

16. 根据权利要求 15 所述的接入控制器，其特征在于还包括:

（a）用于将在点对点层 2 协议(PPPoE)上接收的信息向上传送到位于应用层的鉴权协议的装置；以及

（b）用于将在位于应用层的鉴权协议上接收的信息向下传送到在点对点层 2 协议(PPPoE)上的装置。

17. 根据权利要求 16 所述的接入控制器，其特征在于还包括: 请求装置，在无线终端和公共陆地移动网络之间成功的询问—响应鉴权过程之后，用于请求来自动态主机配置协议服务器的 IP 地址。

18. 根据权利要求 17 所述的接入控制器，其特征在于适于通过接入点，与无线终端进行通信。

19. 根据权利要求 17 所述的接入控制器，其特征在于适于通过鉴权网关，与公共陆地移动网络进行通信。

20. 根据权利要求 19 所述的接入控制器，其特征在于适于通过负责鉴权无线局域网的本地用户的鉴权服务器，与鉴权网关进行通信。

21. 根据权利要求 15 的接入控制器，其特征在于，位于应用层处的鉴权协议是可扩展鉴权协议。

22. 根据权利要求 21 所述的接入控制器，其特征在于，在 RADIUS 协议上传输可扩展鉴权协议。

23. 根据权利要求 21 所述的接入控制器，其特征在于，在 Diameter 协议上传输可扩展鉴权协议。

24. 一种具有用于执行询问—响应鉴权过程的装置的无线终端，该无线终端包括以下用途: 用作为点对点层 2 协议(PPPoE)客户并且在所述点对点层 2 协议上具有可扩展鉴权协议，该无线终端其特征在于，

在执行了一个成功的询问—响应鉴权过程之后接收一个 IP 地址，该 IP 地址可用于获得 IP 连接。

25. 一种电信系统，包括具有至少一个接入点的无线局域网，公共陆地移动网络和至少一个提供有 SIM 卡并适于读取其用户数据的终端设备，其特征在于，所述系统还包括如权利要求 15 所述的接入控制器，用于允许对作为公共陆地移动网络的订户的无线局域网用户进行基于 SIM 的用户鉴权。

用于在无线局域网接入的基于SIM的鉴权和加密的系统、设备和方法

技术领域

一般地，本发明涉及在无线局域网环境中的鉴权和加密机制。更具体地，本发明关于针对基于SIM的鉴权和第2层加密机制的设备、系统和方法，用于保护来自上层终端设备的通信路径。

背景技术

在1999年，IEEE公布了速率为11Mbps的用于无线局域网接入的802.11b规范。该标准得到工业界的广泛支持并在企业公司和例如机场、饭店、咖啡馆等的公共接入集中的地区具有巨大的安装基础。

802.11b标准在一定程度上提出了鉴权、接入控制机制和机密性，但是仅限于无线路径。在此方面，该标准中定义了两种鉴权方法，即“开放系统”和“共享密钥”。

当使用开放系统时，终端设备（TE）中的WLAN卡宣布其希望与WLAN接入点（下文中缩写为AP）进行关联。不进行鉴权，只是应用一些基本的接入控制机制，例如媒体接入控制（MAC）滤波器和服务设置标识符（SSID）。

设置这些MAC滤波器以进行工作，以便只允许其MAC地址属于例如接入控制列表的由AP保存的列表的WLAN卡与AP进行关联。这种接入控制机制具有有限的效用，由于要关联的实体的身体实际上不属于用户，而是属于设备自身。如果终端或卡被盗，则没有基于用户的鉴权以防止使用被盗的设备接入到资源。此外，由于WLAN卡的MAC地址总是在WLAN帧的头标出现，所以MAC地址欺骗是一种微不足道的攻击。这是特别有关系的，因为市场上的大多数WLAN卡仅通过软件手段就能改变其MAC地址。

另一个接入控制机制是前述的服务设置标识符（SSID），其为文字数字码，用来识别终端设备（TE）要关联的WLAN的情况。给定的AP仅允许提供了正确的SSID的WLAN卡进行关联。然而，由于通常由AP对此标识符进行广播，甚至没有改变由销售商设置的默认值时，该接入控制机制就因为会出现许多众所周知的攻击而再次无用了。

上述的第二个鉴权方法是所谓的共享密钥。将此过程嵌入在由有线对等秘密(WEP)标准提供的基本机密机制中，所述标准是基于RC4的对称加密算法。如此通过利用应答响应机制来执行鉴权，在该机制中，作为两方的WLAN卡和AP显示出拥有相同的密钥。然而，将该密钥安装并存储在终端设备（TE）中，因此其遭遇到与讨论MAC滤波器时所描述的同样的缺点。

此外，近年来发表的大量论文示出了机密机制本身的基础缺陷，即，WEP标准的缺陷。由于在WEP帧中以明文发送算法的初始化矢量，这些缺陷首先是静态WEP标准密钥的使用，其使得攻击者发现密钥本身。例如，仅查看通信量的WLAN卡的许多被动攻击也可以推导出密钥。

开始时，似乎仅利用更好的密钥管理来更新密钥并增加其长度，例如从40位到128位，算法能够更安全或至少足够安全到获得可接受的安全性。但是，越来越多的近来的报告已经证实这样的算法设计不能提供可接受的安全水准。

现在，工业界和代表性讨论会作出了努力来解决目前应用标准中的缺陷。当前IEEE正在定义新标准来改善现有的802.11b标准的鉴权机制，将该结果公布为所谓的802.1x标准：“基于端口的网络接入控制”，但是该工作尚未完成。此外，该方法只考虑到鉴权，因此仍需要合适的机密算法。在此方面，当前趋势提出基于所谓的高级加密系统（AES）协议的协议可以取代WEP。然而，正如802.1x中提出的基于端口的鉴权机制，其对TE操作系统和在AP的应用软件中具有显著的影响，这是由于802.1x只是寻求基于WEP的鉴权机制的替代品和WEP本身。

简而言之，由于将不得不取代或至少升级给定WLAN的所有AP，则将仍具有上述缺陷的新标准802.1x的大量采用将引起在WLAN设备上新的投资。此外，稍微显而易见的是，任何WLAN机密机制只提供对无线路径的保护，即在WLAN卡和AP之间路径的保护。然而，根据没有加密AP之外的相应以太网业务。

因此，此阶段本发明的重要目的是提供设备和方法，用于允许WLAN用户的有效的鉴权机制以及贯穿从所述用户的终端设备开始的整个通信路径的完全加密机制。

简而言之，正如以上广泛所述，当将 WLAN 卡的物理 MAC 地址用于鉴权 TE 时，当前的 WLAN 应用标准，即 802.11 中的鉴权不存在，或鉴权基于设备。从适于维护可接受的安全性的不同小区中没有发现通过例如以其不稳定而知名的 WLAN 中的 WEP 协议获得的加密，对于大量特定配置而言这显然是无法实现的。

作为对比，例如 GSM，GPRS，或 UMTS 的传统或新的公共陆地移动网络中的鉴权是利用 SIM 卡和一套证明安全的协议和称为“鉴权和密钥许可协议”（以下简称为 AKA）的算法来实现的。由于针对个人应用而设计 SIM 并且通过 PIN 对其进行保护，因此所谓的基于 SIM 的鉴权是基于用户的。

现在，移动运营商想要通过宽带接入扩展其在接入网络中的供应商品，并且主要由于在 WLAN 中未许可的频谱带的使用，WLAN 技术使直到 11Mbps 的访问速率成为可能，同时保持极低的使用成本。移动运营商能够通过安装其自身的 WLAN 或通过签署同意现有的 WLAN 运营商来实现，但是无论怎样，安全性的要求至少应该和在移动接入运营商的核心网络的环境下一样强。

为了实现该目的，WLAN 运营商必须提供暗示拥有 SIM 卡的鉴权和加密机制。必须由移动运经营商来发行该 SIM 卡并且该 SIM 是与用于移动接入的相同的 SIM，或是只为 WLAN 接入的目的而发行的 SIM。

由第三方经营的传统 WLAN 也可具有其自身的本地用户，并且针对所述本地而进行的鉴权完全由 WLAN 的运营商负责。例如，本地用户的鉴权可能只是根据用户身份加上密码，或甚至根本没有安全性。但是，对于那么移动运营商的订购用户，通过所述的 WLAN 的鉴权和其它安全性问题应当与其在移动运营商的网络中问题是相同的。另一方面，只通过移动运营商使用和运营的 WLAN 应该拒绝接入不属于该移动运营商的用户，并且应该只执行基于 SIM 卡的鉴权机制。

然而，任何试图在 WLAN 中引入新的和更安全的用于鉴权和加密的机制都必须针对在当前的 WLAN 方案中产生尽可能少的影响。

标题为“Arranging Data Ciphering in a Wireless Telecommunication System”的美国专利申请公开 2002/0009199 中描述了相当令人感兴趣的尝试，以解决上述问题。基于该申请的教导也介

绍了一种基于 SIM 的鉴权方案。

然而，基于 SIM 的鉴权方案用于导出密钥，用作 802.11 本地 WEP 算法的密钥，用于 TE 和 AP 之间的通信加密。在现有 WEP 容量上该申请引入的主要优点是增加了每段时间更新一次密码的新机制。此外，该申请基本是现在的 WEP 标准的修改版，并没有解决上述的原始 WEP 版的基本问题。

然而，工业上的不同部门已经估计到公知的 WEP 攻击能在少于两个小时内猜到 WEP 密码。显然，与原始 WEP 版相同，如果 WEP 密码是静态的并且从来不更新，那么问题会非常重大。结果，利用美国 2002/0009199 中介绍的方法，将问题限定在给定的会话持续时间的界限内，而且，如果会话延长超过几个小时，就会产生前述的问题。对于那些在当前公共陆地移动网络发现的网络，提供同样的安全水平显然是不够的。

在此方面，本发明的目的是为实现更高的安全水平，允许运营商选择能够更好满足其安全需求的加密算法。注意，在安全水平和性能之间通常存在平衡。因此，以下可以是本发明所考虑的其它目的：例如具有 128、168 和 256 位等长度的支持密钥的附加特征；以及支持例如 AES 等最新的最安全的算法，和密钥旋转过程。

此外，根据上述申请美国 2002/0009199，由于 WEP 只适用于无线路径，加密路径是从移动终端到 AP。在此方面，支持在 AP 以外建立的加密路径以及还覆盖 WLAN 的有线部分是本发明的另一个目的。

此外，美国 2002/0009199 教导在运行鉴权处理之前完成 IP 地址的分配，因此，恶意用户可能会发起一整套公知的攻击。然而，如果用户在有效地进行鉴权之前没有办法得到 IP 连接，将很大程度地减小风险。因此，本发明的另一个目的是提供一种鉴权机制，在 IP 连接到所述用户这前用于对用户执行鉴权。

另一方面，专利申请美国 2002/012433 和 WO 01/76297 通过一些共有的典型实施例公开了一种系统，其中无线适应终端能通过无线 IP 接入网络连接到家庭移动网络。该家庭移动网络用于以基于 SIM 的鉴权来鉴权用户，而无线 IP 接入网络允许用户一旦被鉴权就接入因特网。该无线终端，无线 IP 地址网络和移动网络均利用移动 IP 协议进行通信。系统还包括公共接入控制器，用于控制来自无线接入网络的连接

到因特网服务的接入。该公共接入控制器将 IP 地址分配给无线终端，在建立到因特网的连接之前鉴权该无线终端，并且在无线终端和家庭移动网络之间中继鉴权消息。此外，无线终端和公共接入控制器之间的接口是基于接口的 IP，其中公共接入控制器和无线终端通过各自 IP 地址互相识别。公共接入控制器和无线终端利用基于 IP 的协议这一事实使得有必要从最初就向无线终端分配 IP 地址，在建立安全信道通信之前，将该 IP 地址从公共接入控制器发送到无线终端。因此，由于存在在执行鉴权步骤之前进行分配 IP 地址的事实，所以出现了与上述申请 US2002/0009199 同样的问题，因此恶意用户可能发动一整套众所周知的攻击。

总之，本发明一个重要的目的是提供一种系统、设备和方法，用于允许有效的基于 SIM 的用户鉴权和为订购了公共陆地移动网络的 WLAN 用户建立起始于 TE 的完全加密路径。另一个具体的重要目的是可以在 IP 连接到所述用户之前执行基于 SIM 的用户鉴权。

本发明的另一个目的是支持可变长度的密钥、在运营商选择下使用安全算法和提供密钥旋转过程。

本发明的另一个目的是在最小影响传统 WLAN 的环境下实现之前的目的。

发明内容

利用一种方法来实现本发明的目的，通过数据链路层（layer=2）鉴权机制，对作为公共陆地移动网络的订户的无线局域网用户进行基于 SIM 的鉴权。该方法重要的方面在于当鉴权处理成功完成时，只将 IP 连接提供给用户。

根据本发明的电信系统中的方法，用于允许针对作为公共陆地移动网络订户的无线局域网用户进行基于 SIM 的鉴权，该方法包括步骤：（a）无线终端通过可接入的接入点接入无线局域网；（b）该无线终端发现插入在接入点和公共陆地移动网络之间的接入控制器；（c）在无线终端和公共陆地移动网络之间通过该接入控制器执行询问—响应鉴权过程，无线终端配备有 SIM 卡并适于读取其数据；其中步骤（c）中的询问—响应鉴权过程的提交在向用户提供 IP 连接之前发生，在以下组件中携带所述询问—响应鉴权过程的提交； 在无线终端和接入控制器之间的点对点层 2 协议上；以及在位于公共陆地移动网

络和接入控制器之间的应用层处的鉴权协议上；以及所述方法还包括步骤：（d）一旦公共陆地移动网络对所述用户有效地进行了鉴权，则通过发送已分配的 IP 地址和其它网络配置参数来向无线终端处的用户提供 IP 连接。

根据本发明的电信系统中的接入控制器，所述系统包括具有至少一个接入点的无线局域网，公共陆地移动网络和至少一个提供有 SIM 卡并适于读取其用户数据的终端设备，其中所述接入控制器包括：（a）点对点层 2 协议服务器，用于与无线终端进行通信，并且被安排用来为询问—响应鉴权过程建立隧道；（b）位于 OSI 应用层的鉴权协议，用于与公共陆地移动网络进行通信；以及（c）向无线终端发送已分配的 IP 地址和其它网络配置参数的装置，用于在电信系统的终端设备和公共陆地移动网络之间成功地执行询问—响应鉴权过程之后提供 IP 连接。

本发明还提供一种具有用于执行询问—响应鉴权过程的装置的无线终端，该无线终端包括以下用途：用作为点对点层 2 协议客户并且在所述点对点层 2 协议上具有可扩展鉴权协议，在执行了一个成功的询问—响应鉴权过程之后接收一个 IP 地址，该 IP 地址可用于获得 IP 连接。

本发明还提供一种电信系统，包括具有至少一个接入点的无线局域网，公共陆地移动网络和至少一个提供有 SIM 卡并适于读取其用户数据的终端设备，其中所述系统还包括如上所述的接入控制器，用于允许对作为公共陆地移动网络的订户的无线局域网用户进行基于 SIM 的用户鉴权。

因此，利用一种方法来实现本发明的目的，其中，无线终端发现可接入的接入点并请求与无线局域网进行关联，而接入点接受了该请求。然后，无线终端开始寻找插入在接入点和公共陆地移动网络之间的接入控制器。

然后，无线终端在点对点层 2 协议上立即将用户标识符发送到接入控制器，所述控制器将在点对点层 2 协议上接收的用户标识符向上移动到应用层处的鉴权协议。

接下来，接入控制器将用户标识符发送到公共陆地移动网络处的鉴权网关，以发起鉴权过程。

首先，开始鉴权处理，接入控制器接收通过鉴权网关来自公共陆地移动网络的鉴权询问；并在应用层处将在相同协议上接收的鉴权询问向下移动在点对点层 2 协议上。为了得到鉴权响应，由接入控制器将鉴权询问发送给无线终端。

然后，无线终端可以在点对点层 2 协议上立即将鉴权响应发送给接入控制器，接入控制器将在点对点层 2 协议上接收的鉴权响应向上移动到应用层处的鉴权协议。从接入控制器将鉴权响应发送到鉴权网关，所述接入控制器通过鉴权网关接收来自公共陆地移动网络的加密密钥。

接下来，为了利用无线终端进一步加密通信路径，接入控制器提取在应用层处的协议上接收的加密密钥；以及接入控制器将分配的 IP 地址和其它网络配置参数发送到无线终端。

这种设置的优点在于，与无线电通信网络使用的相类似，在整个通信路径中，移动终端添加了安全的鉴权机制，这意味着在无线路径和有线路径上获得了机密性。运营商能够扩展其接入网络，以非常低的成本提供局域的宽带接入（11Mbps）。

此外，为了实现本发明的目的，提供了一种接入控制器，包括位于 OSI 层-2 中的点对点服务器，用于与无线终端进行通信；以及位于 OSI 应用层的鉴权协议，用于与公共陆地移动网络进行通信。此外，该接入控制器还包括传送装置，用于将在点对点层-2 协议上接收的信息向上传送到应用层处的适当鉴权协议。同样，接入控制器还包括传送装置，用于将在应用层处的鉴权协议上接收的信息向下传送到在点对点层 2 协议之上。

为了充分实现本发明的目的，还提供了一种无线终端，包括用途，作为点对点层 2 协议客户并且在点对点层 2 协议上具有可扩展的鉴权协议。

本发明提供的总体解决方案提供了一种通信系统，包括无线局域网，所述无限局域网包括至少一个接入点、公共陆地移动网络、如上所述的至少一个无线终端和上述的接入控制器。

附图说明

结合附图，通过阅读此描述，本发明的特征、目的及其优点将变得显而易见，其中：

图 1 示出了一个优选实施例，其中，通过利用移动和非移动用户能够接入的WLAN接入的传统移动网络用户如何可以被其自身的移动网络鉴权，以及如何具有从TE到自己的移动网络的加密路径。

图 2 示出了与图 1 相比简化的结构，其适用于仅仅由公共陆地移动网络的用户接入的 WLAN。

图 3 是示意性地示出包括 PPPoE 服务器和 RADIUS 客户机的接入控制器的实施例，其中存在可扩展的鉴权协议。

图 4 基本上示出了从 TE 到移动网络并贯穿 WLAN 实体而执行的动作的典型序列，以执行基于 SIM 的用户鉴权。

具体实施方式

下面将描述装置、方法和系统的当前的优选实施例，用于允许有效的基于 SIM 的用户鉴权并用于针对作为公共陆地移动网络的订户的 WLAN 用户，建立始于 TE 的完全的加密路径。根据本发明的一个方面，在 IP 连接所述用户之前执行该基于 SIM 的用户鉴权。

因此，示出了通用环境的图 1 示出了优选实施例的总体框架，其中公共陆地移动网络（GSM/GPRS/UMTS）的订户和其它本地非移动用户接入了无线局域网（WLAN）。图 1 所示该通用环境提出了针对将对现有传统 WLAN 的影响减少到最小的特别简单的结构，以便实现本发明的一个目的。该相当简单的结构涉及不同的来自 WLAN 和来自公共陆地移动网络的实体，将在下文进行描述。此外，图 2 示出了根据本发明的另一个实施例的更简化的结构，用于 WLAN 只接入公共陆地移动网络的订户和没有本地 WLAN 用户。

图 1 和图 2 中的第一实体是终端设备（TE），其配备有必要的硬铁和软件来与用户 SIM 卡连接，并且根据鉴权和密钥许可协议（AKA）发送和接收所需的信令信息。TE 还包括必要的软件来实现以太网上点对点（PPPoE）协议、客户端、从而是 RFC2516 的点对点协议，

这种 PPPoE 客户包含的内容允许在 WLAN 域中建立与特定服务器的点对点协议（PPP）会话。这是一个非常便利的实施例，以便影响现有的鉴权机制，例如可扩展的鉴权协议（EAP），和加密协议，例如根据 REC 1968 的 PPP 加密控制协议（以下称之为“加密的 PPP”），沿着 WLAN 的有线部分扩展了加密路径，从而提供了更高的安全水平。例如 PPPoE 客户的组件是针对所建议的解决方案的核心部分。

根据802.11b标准，图1和图2的环境中的其它实体用作普通标准无线基站的接入点，没有任何附加逻辑电路。与其它可能的解决方案不同，如关于成为标准的802.1x所解释的，本发明提供的方法允许重新使用现有的廉价硬件，没有必要替换或升级在WLAN中的所有AP的硬件。由于与在PPPoE层上执行的安全机制相比，这些WEP自身提供了一点安全，因此，在关闭WEP支持时，可以在该环境下运行这些不变的AP。

根据本发明的一个方面，提供了新的实体，图1和图2中的接入控制器(下文称之为AC)均包括所需的PPPoE服务器功能。通过PPPoE协议中的嵌入机制，即通过由广播消息发起的握手，终端设备（TE）自动地发现该PPPoE服务器。该接入控制器（AC）还包括RADIUS客户功能，其负责收集通过在PPP上携带的EAP属性所接收的客户资格，并且还负责通过现在在RADIUS消息上携带的EAP属性，将其发送到传统的WLAN鉴权服务器（WLAN-AS）。同样，该接入控制器（AC）的组件也是为实现本解决方案的目的的核心部分。

接入控制器和前述的内嵌于终端设备的PPPoE客户都是协同工作的实体，用于接通询问-响应鉴权过程和建立加密路径。

仅在图1所示的最通用环境中示出的其它实体是WLAN-鉴权服务器（WLAN-AS），用于实现不属于移动运营商的本地WLAN用户的本地认证者服务器的功能，因此，可以通过例如普通用户和密码匹配的其它方法鉴权用户。当在公共陆地移动网络运营商的域内接收来自接入控制器的鉴权信息并将之转发到鉴权网关（下文称之为AG）时，该WLAN-AS还起到RADIUS代理的作用。

出于本发明的目的，只需要WLAN-AS，以便鉴权不是公共陆地移动网络的移动订户的自身的WLAN用户。结果，用于只接入移动网络的订户的WLAN可以去除该实体而不会影响所述移动订户的鉴权和加密路径的建立以及本发明的范围。在此方面，图2示出了一个简化结构的实施例，用于如上所述WLAN只接入公共陆地移动网络的订户，因此，其中不包括WLAN-AS。

图1和图2的环境所包括的其它实体是鉴权网关（以下称之为AG），其可以独自或共同作为归属位置寄存器（HLR），用于存储移动订户用户数据。在运营商的域内，该鉴权网关（AG）独自或与HLR

结合作为鉴权后端服务器并负责根据针对传统或例如 GSM、GPRS 和 UMTS 的新公共陆地移动网络的 AKA 协议产生鉴权矢量。这些组件，即 AG 和 HLR 可以是通过移动应用部分（MAP）协议相互通信的物理上分离的实体，或者是作为 RADIUS 服务器和具有内嵌的用户数据库的单一的逻辑实体，用于实现 AKA 中必需的算法，如公知的 A5、A8 等。因此，在后者的方法中，与 HLR 的通信无需如图 2 中典型所示。

总之，接入控制器、嵌入在终端设备中的前述 PPPoE 客户和鉴权网关是实现本发明目的的核心实体。对于这些实体的功能的描述仅是示例性的和非限制性的方式。

参考开放系统互联（OSI）模型，图 3 示出了接入控制器（AC）涉及的不同协议层。位于 IP 层的下面的 PPPoE 服务器包括自然位于以太网层之上的 PPPoE 协议层，其具有内嵌的前述 EAP。同样，RADIUS 客户具有内嵌 EAP 的 RADIUS 协议层，其位于 UDP 层之上，该两层位于 IP 层之上。

另一方面，下面将参考图 4 所示的动作序列，对其中不同元件根据当前优选实施例来执行本发明的某些方面的方式进行描述。

前述的终端设备（TE）配备有移动终端适配器（MTA），允许接入移动终端携带的 SIM 卡。该 TE 具有收发信机，用于和 WLAN 的 AP 的通信（C-401，C-402），并包括合适的软件栈，以根据 RFC2516 来执行 PPPoE 协议。

接入控制器（AC）具有嵌入的 PPPoE 服务器。通过 PPPoE 客户来发现 PPPoE 服务器是该协议自身的整体部分（C-403，C404，C405，C406）。PPP 链路上由 TE 使用的身份是网络接入标识符（NAI），其通过用户输入来建立需要的拨号会话，所用的范围是识别作为给定的移动运营商的订户的用户。由于通过其它方法来完成鉴权，因此不需要密码。可选择的，代替发送 NAI，可以从 SIM 卡取得 IMSI 并作为用户身份发送。如果在明码电文中发送 IMSI 是可接受的（一般不使用明码发送 IMSI），则应当只能使用该方式。

当在 EAP 机制的帮助下接收到用户身份时，接入控制器（AC）具有 RADIUS 客户，用于将鉴权信息发送（C-409）到 WLAN-AS 服务器。在 PPP 和 RADIUS 上运行可扩展的鉴权协议（EAP），以便在 TE 和 AG 之间传送鉴权信息。要在 EAP 中使用的鉴权机制可以是针对公共

陆地移动网络的传统的 AKA。如上所述，WLAN-AS 针对常规 WLAN 用户用作鉴权服务器，其鉴权不是基于 SIM 的，而对于用户的 NAI 领域部分将其识别为移动网络的订户，从而使用基于 SIM 的鉴权的这些用户，其作为鉴权代理服务器。然后，当作为鉴权代理服务器时，WLAN-AS 将接收到的鉴权信息转发（C-410）到鉴权网关（AG）。

当鉴权网关接收到（C-410）鉴权请求时，通过利用 MAP 接口来要求 HRL 提供三维或五维的鉴权矢量（C-411）。为了该任务，鉴权网关（AG）必须了解已经在 RADIUS 消息中发送其 NAI 的订户的 IMSI。例如，可以通过在目录数据库中查找来发现该 IMSI。HLR 以所请求的鉴权信息（C-412）来回应用户。

然后，AG 封装在 EAP 属性中的鉴权矢量的 RAND 分量并在 RADIUS 消息中将其通过 WLAN-AS(C-413)发送返回到 AC(C-414)。注意，对于例如 UMTS 的新移动网络的用户，还需要发送类似 AUTN 的消息。

然后，AP 将接收到的 EAP 信息转发（C-415）到 PPP 消息中的 TE。注意，这里 AC 作为在例如 PPP 和 RADIUS 的“载体”协议之间的 EAP 信息的“通路”。

当 TE 接收到 EAP 信息时，提取 RAND 号码，并利用其询问 SIM 并产生应答（RES），通过在 PPP 和 RADIUS 上传输的 EAP 再次将所述应答送回（C-416，C-417，C-418）到 AG。如前，对于 UMTS 用户，TE 首先根据 AUTN 鉴权网络。在此阶段，必须注意，TE 遵照在 AKA 中定义的标准算法来产生加密密钥。该密钥用作种子，即密钥材料，来导出一个或多个会话密钥，以便与在 RFC 1968 中陈述的 PPP 加密控制协议和例如 PPP 3-DES 加密协议、RFC2420 的任何现有 PPP 加密算法一起使用。

AG 接收（C-418）EAP 响应并检查应答的有效性。之前已经在来自可能与未示出的鉴权中心（AuC）的合作的 HLR 的鉴权矢量中接收到了 AKA 加密密钥（Kc）。然后，AG 将 AKA 加密密钥（Kc）传送给其中设置了 PPPoE 服务器的 AC(C-419，C-420)。可以在传输 EAP 成功的接入接受 RADIUS 消息中进行此操作，但是由于该 EAP 命令不能携带任何附加数据，一个 RADIUS 卖方特定属性（VSA）可以是更有价值的选项。

在该阶段，AC 接收（C-420）接入接受 RADIUS 消息并请求来自动态主机配置协议（DHCP）服务器的 IP 地址，进一步将该 IP 地址发送到 TE。AC 遵照和与 TE 相同的算法，从要和 PPP 加密控制协议一起使用的 AKA 加密密钥（Kc）和选定的 PPP 加密算法（例如 3DES）中导出会话密钥。最后，AC 将 EAP 成功消息，连同其它预定给所述 TE 的配置参数，如 IP 地址，IP 网络掩码、DNS 服务器发送（C-421）给 TE。然后，完全建立了 PPP 链路并准备进入网络阶段。

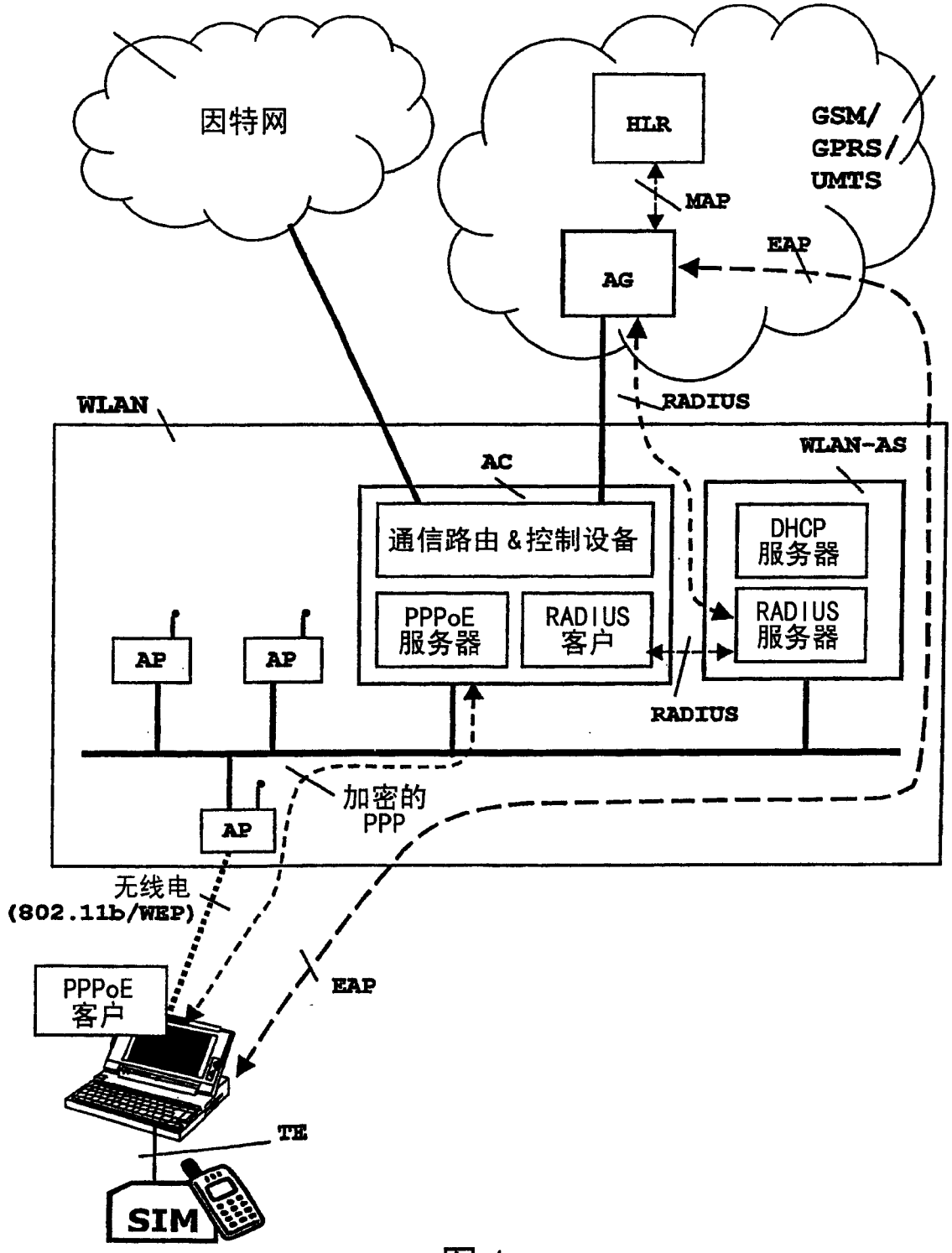

因特网
HLR
GSM/
GPRS/
UMTS
MAP
EAP
AG
RADIUS
WLAN
WLAN-AS
AC
通信路由 &控制设备
DHCP
服务器
PPPoE
服务器
RADIUS
客户
RADIUS
服务器
AP
AP
AP
RADIUS
加密的
PPP
无线电
(802.11b/WEP)
PPPoE
客户
EAP
TE
SIM

图 1

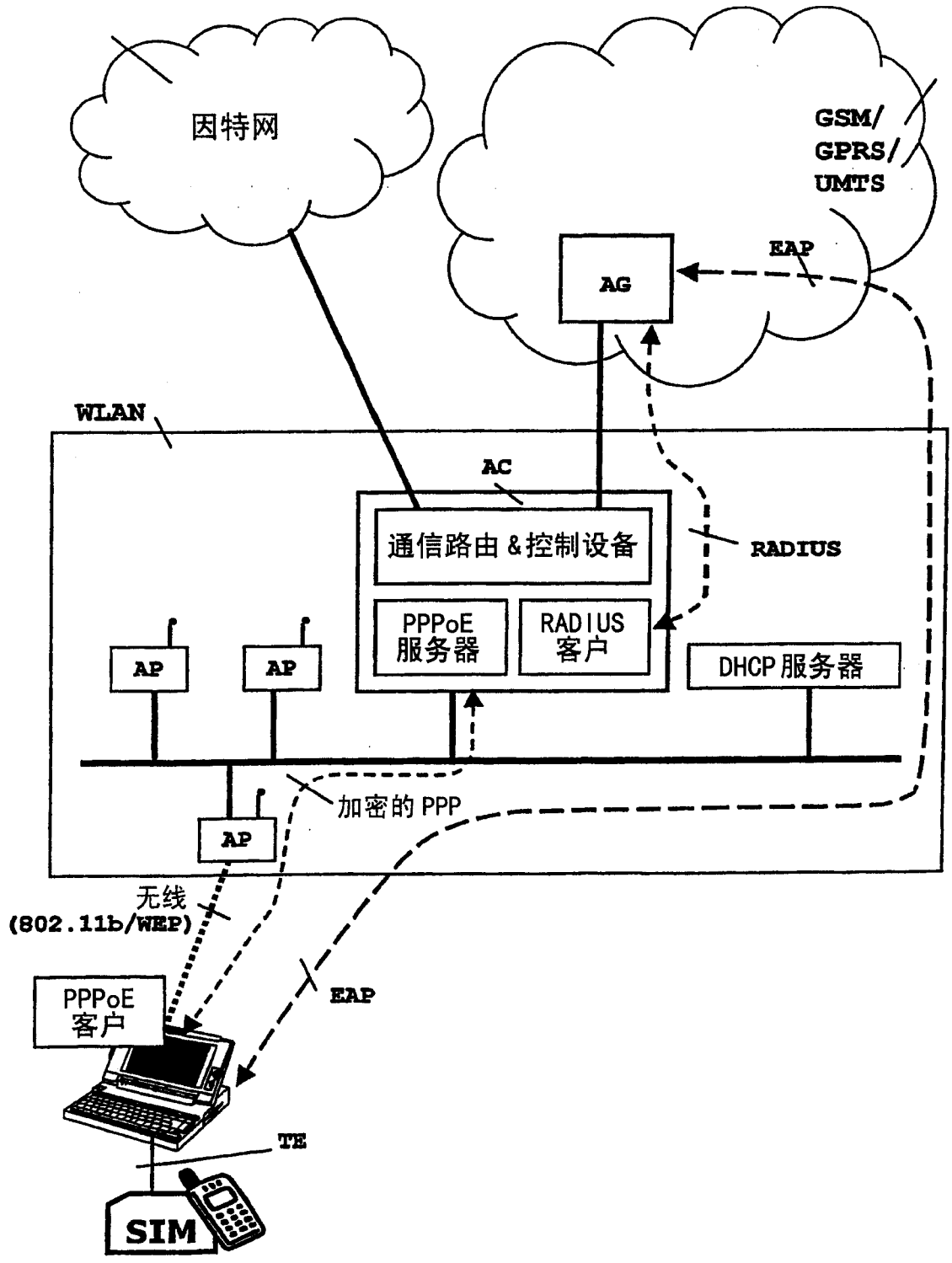

因特网
GSM/
GPRS/
UMTS
EAP
AG
WLAN
AC
通信路由 &控制设备
RADIUS
PPPoE
服务器
RADIUS
客户
DHCP 服务器
AP
AP
AP
加密的 PPP
无线
(802.11b/WEP)
PPPoE
客户
EAP
TE
SIM

图 2

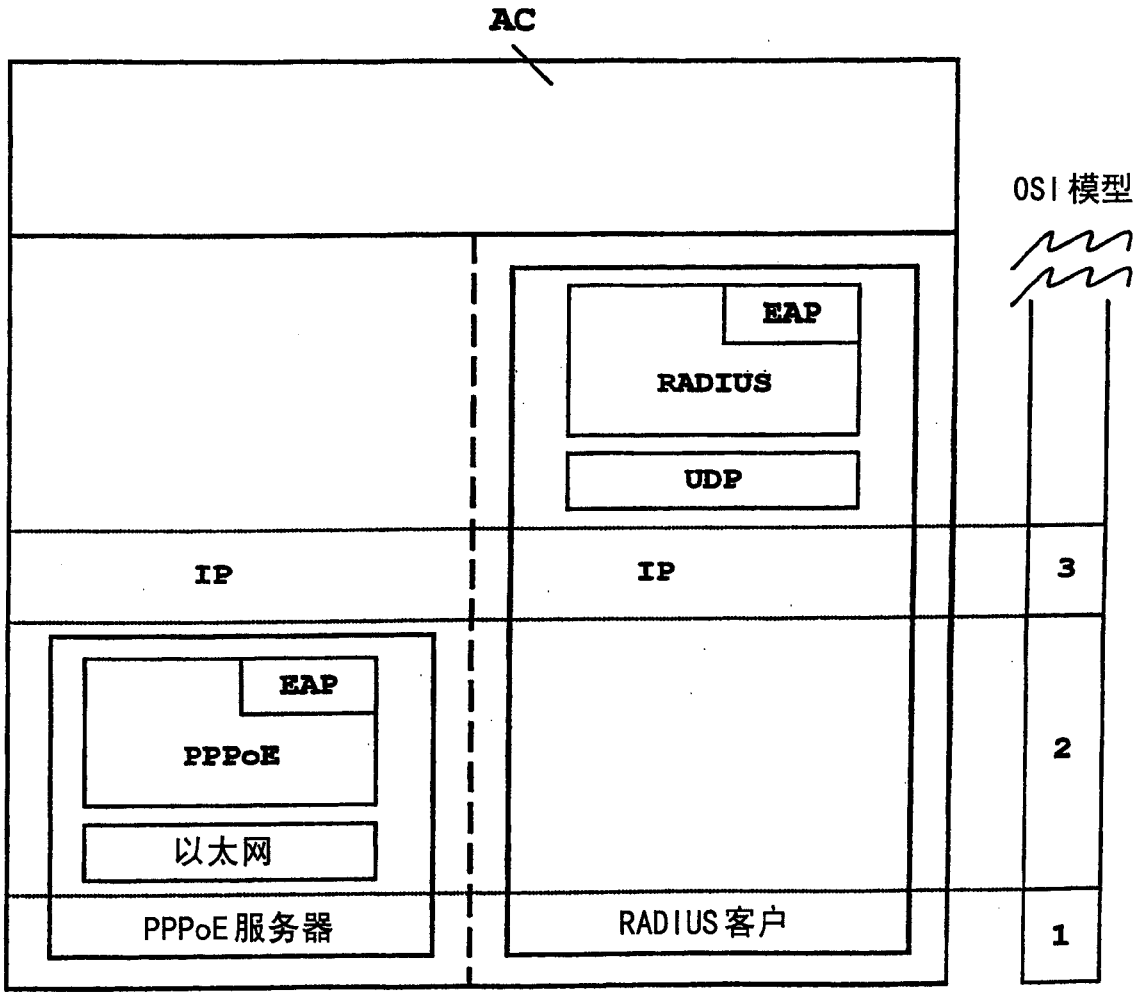

AC
OSI 模型
EAP
RADIUS
UDP
IP
IP
3
EAP
PPPoE
以太网
2
PPPoE服务器
RADIUS客户
1

图 3

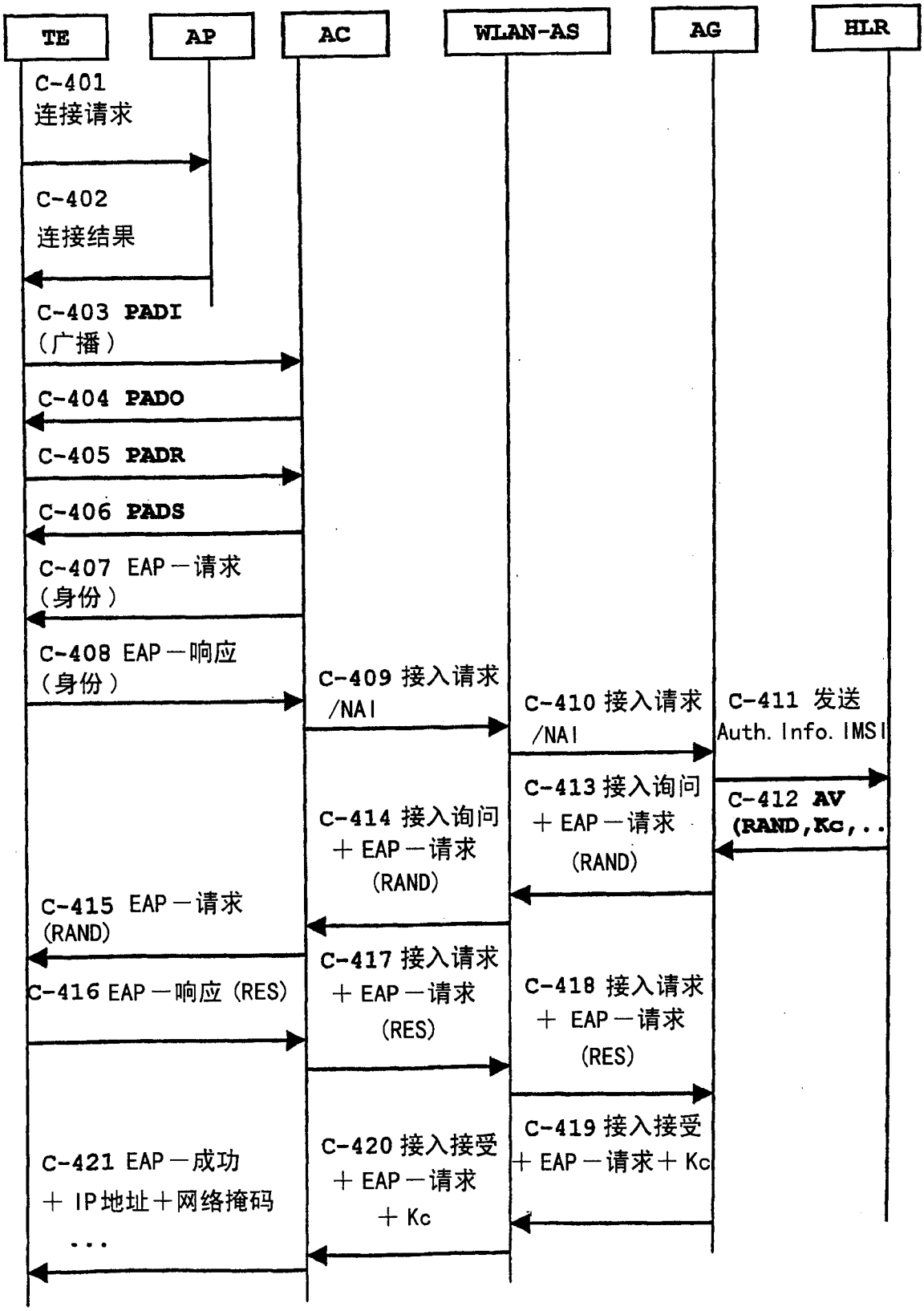

TE
AP
AC
WLAN-AS
AG
HLR
C-401
连接请求
C-402
连接结果
C-403 PADI
（广播）
C-404 PADO
C-405 PADR
C-406 PADS
C-407 EAP－请求
（身份）
C-408 EAP－响应
（身份）
C-409 接入请求
/NAI
C-410 接入请求
/NAI
C-411 发送
Auth. Info. IMSI
C-412 AV
(RAND,Kc,..
C-413 接入询问
＋EAP－请求
(RAND)
C-414 接入询问
＋EAP－请求
(RAND)
C-415 EAP－请求
(RAND)
C-416 EAP－响应 (RES)
C-417 接入请求
＋EAP－请求
(RES)
C-418 接入请求
＋EAP－请求
(RES)
C-419 接入接受
＋EAP－请求＋Kc
C-420 接入接受
＋EAP－请求
＋Kc
C-421 EAP－成功
＋IP地址＋网络掩码
...

图 4