[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 03159178.7

[45] 授权公告日 2007 年 8 月 29 日

[11] 授权公告号 CN 100334850C

[22] 申请日 2003.9.10 [21] 申请号 03159178.7

[73] 专利权人 华为技术有限公司

地址 518057 广东省深圳市科技园科发路华为用服大厦

[72] 发明人 赵 毅 潘 强 欧阳容冰 高江海 李小燕 陈殿福 林 明 汪 静 陈卫民 郑小春 彭文钦 谢 铃 谢 南 靳广亮

[56] 参考文献

CN1414731A 2003.4.30

CN1435985A 2003.8.13

US2003055924A1 2003.3.20

GB2379040A 2003.2.26

JP2003186837A 2003.7.4

无线局域网技术和应用 王军明，伏海文，现代电信技术，第 11 期 2002

移动运营商 WLAN 的用户认证 夏国良，通讯世界，第 4 期 2003

审查员 张江波

[74] 专利代理机构 北京德琦知识产权代理有限公司

代理人 张颖玲

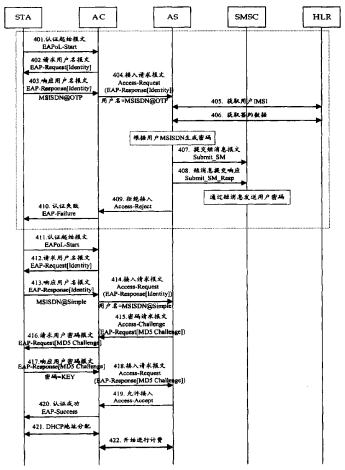
权利要求书 3 页 说明书 11 页 附图 3 页

[54] 发明名称

一种无线局域网接入认证的实现方法

[57] 摘要

本发明公开了一种无线局域网接入认证的实现方法，包括：a)当前无线局域网用户终端作为客户端，通过设备端将自身的用户标识信息发送给认证服务器，发起接入认证；b)认证服务器根据所收到的用户标识信息，判断是否需要获取一次性密码(OTP)，如果是，则认证服务器随机生成本次认证所需的 OTP，然后将所生成的密码传输给客户端，同时向设备端发送拒绝接入报文，执行步骤 c；否则，进行正常的接入认证，结束当前流程；c)收到密码的客户端再次向设备端发起认证流程，该收到密码的客户端将自身的用户名和所收到的密码通过设备端发送给认证服务器，完成自身的无线局域网接入认证。 该方法可提高 WLAN 接入认证的安全性和可靠性。



1、一种无线局域网接入认证的实现方法，其特征在于，该方法包括以下步骤：

a. 当前无线局域网用户终端作为客户端，通过设备端将自身的用户标识信息发送给认证服务器，发起接入认证；

b. 认证服务器根据所收到的用户标识信息，判断是否需要获取一次性密码OTP，如果是，则认证服务器随机生成本次认证所需的OTP，然后将所生成的密码传输给客户端，同时向设备端发送拒绝接入报文，执行步骤 c；否则，进行正常的接入认证，结束当前流程；

c. 收到密码的客户端再次向设备端发起认证流程，该收到密码的客户端将自身的用户名和所收到的密码通过设备端发送给认证服务器，完成自身的无线局域网接入认证。

2、根据权利要求 1 所述的方法，其特征在于，当前无线局域网用户终端作为客户端以 802.1X 方式发起接入认证；

则步骤 a 为：当前无线局域网用户终端作为客户端向设备端发送认证起始报文，设备端收到后向客户端请求用户名，客户端向设备端返回携带有用户标识字段的响应报文，设备端收到后，将该响应报文透传给认证服务器；

步骤 b 为：认证服务器对所收到的响应报文进行解析，并根据解析出的用户标识字段判断是否需要获取 OTP，如果是，则认证服务器随机生成本次认证所需的 OTP，然后将所生成的密码传输给客户端，同时向设备端发送拒绝接入报文，执行步骤 c；否则，进行正常的 802.1X 认证，结束当前流程；

步骤 c 为：收到密码的客户端再次向设备端发送认证起始报文，重新发起 802.1X 认证流程，该收到密码的客户端将自身的用户名和所收到的密码通过设备端发送给认证服务器，完成自身的无线局域网接入认证。

3、根据权利要求 1 所述的方法，其特征在于，当前无线局域网用户终端作为客户端以 PPPoE 方式发起接入认证；

则步骤 a 为：当前无线局域网用户终端作为客户端，先通过 PPPoE 发现阶段报文交互找到当前可用的设备端，再将自身的用户标识信息通过所发现的可用设备端发送给认证服务器。

4、根据权利要求 2 所述的方法，其特征在于，步骤 a 中所述客户端向设备端发送响应报文为：客户端向设备端发送表示需要获取 OTP 的响应报文。

5、根据权利要求 4 所述的方法，其特征在于，步骤 a 中客户端向设备端发送以用户名@OTP 为用户标识字段的响应报文，则步骤 b 中所述判断为：认证服务器判断解析出的域名部分是否为 OTP，如果是，则需要获取 OTP；否则，不需要获取 OTP，进行正常的 802.1X 认证。

6、根据权利要求 2 所述的方法，其特征在于，步骤 b 进一步包括：认证服务器在生成 OTP 之前，先根据所收到响应报文中的用户名信息，从归属位置寄存器中获取当前客户端的签约信息，并根据所获得的签约信息判断当前客户端是否具有 WLAN 业务权限，如果有，再随机生成本次认证所需的 OTP；否则，向设备端返回拒绝接入消息。

7、根据权利要求 1 或 2 所述的方法，其特征在于，步骤 b 中所述将生成密码传输给客户端为：认证服务器将所生成的密码以短消息方式发送给当前客户端对应的手机用户。

8、根据权利要求 7 所述的方法，其特征在于，所述以短消息方式发送进一步包括：认证服务器将所生成的密码通过短消息点对点协议打包成短消息，提交给短消息服务中心，再由短消息服务中心将含有密码的短消息发送给当前客户端对应的手机用户。

9、根据权利要求 8 所述的方法，其特征在于，该方法进一步包括：短消息服务中心收到含有密码的短消息后，向认证服务器回送表示成功接收短消息的响应报文。

10、根据权利要求 1 或 2 所述的方法，其特征在于，步骤 b 所述随机生成 OTP 为：认证服务器根据所收到的用户标识信息，解析出用户名；认证服务器

根据解析出的用户名随机生成本次认证所需的 OTP。

11、根据权利要求 10 所述的方法，其特征在于，所述用户名为当前无线局域网用户终端的移动台国际综合业务数字网 ISDN 号码。

12、根据权利要求 1 或 2 所述的方法，其特征在于，步骤 b 中所述的拒绝接入报文中携带有本次失败的原因。

13、根据权利要求 12 所述的方法，其特征在于，所述拒绝接入报文中失败原因的携带格式为：[OTP] Error code =失败原因对应的取值；Message =失败原因值的含义。

14、根据权利要求 12 所述的方法，其特征在于，步骤 b 中设备端收到携带有失败原因的拒绝接入报文后，根据具体的失败原因向客户端发送响应的失败原因提示。

15、根据权利要求 1 或 2 所述的方法，其特征在于，该方法进一步包括：为每个生成的 OTP 设置一个使用有效期。

16、根据权利要求 15 所述的方法，其特征在于，步骤 c 中收到密码的客户端在该密码对应的使用有效期内随时向设备端发送接入认证请求，触发接入认证流程。

17、根据权利要求 1 或 2 所述的方法，其特征在于，该方法进一步包括：预先建立认证服务器与短消息服务中心的虚连接。

一种无线局域网接入认证的实现方法

技术领域

本发明涉及接入认证技术，特别是指一种在无线局域网中实现一次性密码接入认证的方法。

背景技术

随着用户对无线接入速率的要求越来越高，无线局域网（WLAN，Wireless Local Area Network）应运而生，它能在较小范围内提供高速的无线数据接入，是目前IT行业最热门的技术之一，也是现在最流行的无线接入方式。无线局域网包括多种不同技术，目前应用较为广泛的一个技术标准是IEEE 802.11b，它采用2.4GHz频段，最高数据传输速率可达11Mbps，使用该频段的还有IEEE 802.11g和蓝牙(Bluetooth)技术，其中，802.11g最高数据传输速率可达54Mbps。其它新技术诸如IEEE 802.11a和ETSI BRAN Hiperlan2都使用5GHz频段，最高传输速率也可达到54Mbps。

目前的WLAN网络主要采用802.1X系列协议，所谓802.1X协议是2001年6月电气和电子工程师协会（IEEE）标准化组织正式通过的基于端口的网络访问控制协议。IEEE 802.1X定义了基于端口的网络接入控制协议，其中，端口可以是物理端口，也可以是逻辑端口。

IEEE 802.1X的体系结构如图1所示，802.1X系统共有三个实体：客户端系统（Supplicant System）、设备端系统（Authenticator System）、认证服务器系统（Authentication Server System）。在客户端进一步包括客户端端口状态实体（PAE），在设备端进一步包括设备端系统提供的服务和设备端端口状态实体，在认证服务器系统中进一步包括认证服务器；该认证服务器与设备端的端口状态实体相连，通过扩展认证协议（EAP）来交换设备端和认证服务器间的认证

信息，客户端的端口状态实体直接连到局域网（LAN）上，设备端的服务和端口状态实体分别通过受控端口（Controlled Port）和非受控端口连接于局域网上，客户端和设备端通过客户端和设备端间的认证协议（EAPoL）进行通信。其中，Controlled Port 负责控制网络资源和业务的访问。

如图 1 所示，设备端系统的内部有受控端口（Controlled Port）和非受控端口（Uncontrolled Port），该非受控端口始终处于双向连通状态，主要用来传递 EAPoL 协议帧，可保证随时接收和发送 EAPoL 协议帧；而受控端口只有在认证通过，即授权状态下才打开，用于传递网络资源和服务，也就是说，在认证未通过时该受控端口为未授权端口，受控端口可配置为双向受控、仅输入受控两种方式，以适应不同应用环境的需要。

基于图 1 所示的结构，IEEE 802.1X 认证的基本实现过程如图 2 所示，包括以下步骤：

步骤 201：当用户登录网络时，客户端收到用户登录信息后，向设备端发送认证起始报文 EAPoL-Start，触发认证过程。这里，如果客户端是动态分配地址的，认证起始报文也可能是 DHCP 请求报文；如果客户端是手工配置地址的，认证起始报文还可能是 ARP 请求报文。

步骤 202~203：设备端收到客户端发来的 EAPoL-Start 报文后，向客户端发出请求用户名报文 EAP-Request[Identity]，请求用户名；客户端收到后，将用户名通过响应用户名报文 EAP-Response[Identity]发给设备端。

步骤 204：设备端收到客户端的 EAP-Response[Identity]报文后，通过接入请求报文 Access-Request(EAP-Response[Identity])将用户名透传给认证服务器。

步骤 205：认证服务器收到接入请求报文后，向设备端发出请求用户密码报文 EAP-Request[MD5 Challenge]，并通过密码请求报文 Access-Challenge（EAP-Request[MD5 Challenge]）透传给设备端，向客户端进行 MD5 质询。

步骤 206~208：设备端收到认证服务器发来的 EAP-Request[MD5 Challenge]报文后，通过 EAP-Request[MD5 Challenge]透传给客户端；客户端收到后，将

密码通过响应用户密码报文 EAP-Response[MD5 Challenge]发给设备端；设备端再通过 Access-Request（EAP-Response[MD5 Challenge]）报文透传给认证服务器。

步骤 209~210：认证服务器根据收到的报文进行认证，然后将认证结果通过 Access-Accept 或 Access-Reject 报文发送给设备端；设备端收到后，再将认证结果通过 EAP-Success 或 EAP-Failure 报文透传给客户端，通知用户认证成功或失败。

现有技术中，从个人终端的操作方式来看，WLAN 主要的接入认证方式有两种：基于 EAP-SIM 的认证方式和基于用户名/密码的认证方式，其中 EAP-SIM 方式是利用用户识别模块（SIM）卡，通过 IEEE 802.1X 接入实现统一认证、计费。在基于用户名/密码的方式中，又分为两种方式：固定的用户名/密码和一次性密码（OTP，One Time Password）方式，其中 OTP 方式是指每次采用不同的密码进行接入认证。

通常，WLAN 接入认证采用固定用户名/密码方式，该方式是指用户通过开户向运营商申请一个用户名/密码、或者通过购买预付费卡获得一个固定的用户名/密码，然后进行 802.1x 客户端接入认证。在这种方式中，用户在一段时间内上网都是用同一个用户名/密码。如此，密码容易被盗取，致使安全性降低。

发明内容

有鉴于此，本发明的主要目的在于提供一种无线局域网接入认证的实现方法，可提高 WLAN 接入认证的安全性和可靠性。

为达到上述目的，本发明的技术方案是这样实现的：

一种无线局域网接入认证的实现方法，该方法包括以下步骤：

a. 当前无线局域网用户终端作为客户端，通过设备端将自身的用户标识信息发送给认证服务器，发起接入认证；

b. 认证服务器根据所收到的用户标识信息，判断是否需要获取一次性密码 OTP，如果是，则认证服务器随机生成本次认证所需的 OTP，然后将所生成的

密码传输给客户端，同时向设备端发送拒绝接入报文，执行步骤 c；否则，进行正常的接入认证，结束当前流程；

c. 收到密码的客户端再次向设备端发起认证流程，该收到密码的客户端将自身的用户名和所收到的密码通过设备端发送给认证服务器，完成自身的无线局域网接入认证。

上述方案中，当前无线局域网用户终端作为客户端以 802.1X 方式发起接入认证；

则步骤 a 为：当前无线局域网用户终端作为客户端向设备端发送认证起始报文，设备端收到后向客户端请求用户名，客户端向设备端返回携带有用户标识字段的响应报文，设备端收到后，将该响应报文透传给认证服务器；

步骤 b 为：认证服务器对所收到的响应报文进行解析，并根据解析出的用户标识字段判断是否需要获取 OTP，如果是，则认证服务器随机生成本次认证所需的 OTP，然后将所生成的密码传输给客户端，同时向设备端发送拒绝接入报文，执行步骤 c；否则，进行正常的 802.1X 认证，结束当前流程；

步骤 c 为：收到密码的客户端再次向设备端发送认证起始报文，重新发起 802.1X 认证流程，该收到密码的客户端将自身的用户名和所收到的密码通过设备端发送给认证服务器，完成自身的无线局域网接入认证。

上述方案中，当前无线局域网用户终端作为客户端以 PPPoE 方式发起接入认证；则步骤 a 为：当前无线局域网用户终端作为客户端，先通过 PPPoE 发现阶段报文交互找到当前可用的设备端，再将自身的用户标识信息通过所发现的可用设备端发送给认证服务器。

基于 802.1X 进行认证时，步骤 a 中所述客户端向设备端发送响应报文为：客户端向设备端发送表示需要获取 OTP 的响应报文。其中，步骤 a 中客户端向设备端发送以用户名@OTP 为用户标识字段的响应报文，则步骤 b 中所述判断为：认证服务器判断解析出的域名部分是否为 OTP，如果是，则需要获取 OTP；否则，不需要获取 OTP，进行正常的 802.1X 认证。

基于 802.1X 进行认证时，步骤 b 进一步包括：认证服务器在生成 OTP 之前，先根据所收到响应报文中的用户名信息，从归属位置寄存器中获取当前客户端的签约信息，并根据所获得的签约信息判断当前客户端是否具有 WLAN 业务权限，如果有，再随机生成本次认证所需的 OTP；否则，向设备端返回拒绝接入消息。

上述方案中，步骤 b 中所述将生成密码传输给客户端为：认证服务器将所生成的密码以短消息方式发送给当前客户端对应的手机用户。所述以短消息方式发送进一步包括：认证服务器将所生成的密码通过短消息点对点协议打包成短消息，提交给短消息服务中心，再由短消息服务中心将含有密码的短消息发送给当前客户端对应的手机用户。那么，该方法进一步包括：短消息服务中心收到含有密码的短消息后，向认证服务器回送表示成功接收短消息的响应报文。

上述方案中，步骤 b 所述随机生成 OTP 为：认证服务器根据所收到的用户标识信息，解析出用户名；认证服务器根据解析出的用户名随机生成本次认证所需的 OTP。其中，所述用户名为当前无线局域网用户终端的移动台国际 ISDN（综合业务数字网）号码。

上述方案中，步骤 b 中所述的拒绝接入报文中携带有本次失败的原因。其中，所述拒绝接入报文中失败原因的携带格式为：[OTP] Error code =失败原因对应的取值；Message =失败原因值的含义。步骤 b 中设备端收到携带有失败原因的拒绝接入报文后，根据具体的失败原因向客户端发送响应的失败原因提示。

该方法进一步包括：为每个生成的 OTP 设置一个使用有效期。则步骤 c 中收到密码的客户端在该密码对应的使用有效期内随时向设备端发送接入认证请求，触发接入认证流程。

该方法进一步包括：预先建立认证服务器与短消息服务中心的虚连接。

因此，本发明所提供的无线局域网接入认证的实现方法，将 OTP 和 WLAN 相结合，在 WLAN 的组网方式中用 OTP 认证方式实现用户的上网控制，通过 IEEE 802.1X 来实现 OTP 取密码、认证全流程，在一定的时限内保证密码有效，并使用户每次上网所采用的密码均不相同，从而减少了密码被盗的可能性，为

WLAN 接入认证提供了一种安全可靠性高、方便易用的认证模式，更有效地保证了用户利益。

另外，采用一次性密码的实现方式，不仅操作灵活、易于实现；而且，弥补了 802.1X 只能通过固定用户名/密码方式进行认证的缺陷，丰富了 WLAN 的接入认证手段。并且，通过 IEEE 802.1X 接入方式实现 OTP，充分利用了 IEEE 802.1X 基于端口认证的优势和安全度高的特点，切实可行。

附图说明

图 1 为 IEEE 802.1X 的体系结构示意图；

图 2 为 802.1X 接入认证的实现流程图；

图 3 为本发明实现 OTP 接入认证一实施例的 WLAN 组网结构示意图；

图 4 为本发明中基于 802.1X 的 OTP 接入认证实现的流程图。

具体实施方式

本发明的核心思想是：在采用 OTP 方式实现 WLAN 的接入认证时，先利用 802.1X 的接入过程获取本次认证所需的一次性密码；然后，再利用所获取的密码进行真正的 802.1X 认证过程，完成 WLAN 的接入认证。也就是说，本发明通过两次 802.1X 接入过程实现了 OTP 的密码获取和接入认证的全过程。这里，每次的一次性密码由认证服务器随机生成。

下面结合附图及具体实施例对本发明再作进一步详细的说明。

图 3 为本发明中以 OTP 方式实现 WLAN 接入认证的一实施例的组网结构示意图，如图 3 所示，接入点（AP）为 WLAN 业务网络中的小型无线基站设备，用于完成 802.11b 系列标准的无线接入功能；接入控制设备（AC），用于控制用户接入 WLAN 网络；认证服务器（AS），用于对用户进行认证、授权和计费；短消息服务中心（SMSC），用于将 OTP 密码通过短消息方式发送给用户；归属位置寄存器（HLR），用于存储用户信息；计费网关（CG），用来根据所收到的通信信息生成计费话单；计费中心（BOSS），用于对用户进行计费，主要

是接收和记录网络传来的用户计费信息，并进行统计和控制，其中用户计费信息可以包括在线计费用户的在线费用信息。

通常，在无线局域网中，WLAN 用户终端通过自身当前所属的 AP 接入 WLAN 网络，并经由 AC 到 AS 上进行接入认证，认证通过后，即可在 WLAN 中进行通信。对于 802.1X 接入认证来说，WLAN 用户终端就是客户端，AC 相当于设备端，AS 相当于认证服务器。

本发明先通过 802.1X 认证过程中，WLAN 用户终端 STA 响应用户名报文请求，向 AC 发送自身用户名的步骤，利用特殊的格式通知 AC 要获取一次性密码；AS 随机生成本次、当前用户终端的一次性密码后，通过安全的方式将所生成的密码通知当前发起接入认证的 WLAN 用户，比如：通过短消息方式；同时，AS 还通过发送拒绝接入消息结束本次认证过程；当前用户收到一次性密码后重新发起 802.1X 认证过程，完成 WLAN 的接入认证。

基于图 3 所示的网络结构，以将一次性密码以短消息方式发送给 WLAN 用户为例，说明本发明的具体实现流程。本实施例中，由于采用短消息发送一次性密码方式，所以在 AS 正常运行后，首先要建立与 SMSC 之间的发送虚连接，具体过程是：AS 向 SMSC 传送发送绑定报文 bind_transmitter，请求建立 AS 与 SMSC 之间的发送虚连接；SMSC 收到后，则向 AS 回送发送绑定响应报文 bind_transmitter_resp，表示建立虚连接成功。

如图 4 所示，本实施例以 OTP 方式实现 WLAN 接入认证具体包括：

步骤 401~403：与现有技术中的步骤 201~203 类似，不同的是：用户登录时，在客户端上输入 MSISDN@OTP 并通过 AP 向 AC 发送 EAPoL-Start，发起认证过程；然后，客户端在收到 AC 发来的请求用户名报文后，在用户名响应报文中将 MSISDN@OTP 发送给 AC。

这里，MSISDN@OTP 为用户标识字段，也就是用户标识信息，包括用户名和域名两部分，其中 MSISDN 为用户名部分，OTP 为域名部分，客户端以 OTP 为域名来表示需要获取一次性密码，当然，认证系统也可以定义其它特殊

的域名来表示。而且，认证系统还可以采用其它形式来表示需要获取一次性密码，比如：通过扩展消息属性、字段，增加表示获取密码的字段等方式。

步骤 404：AC 在收到用户的 EAP-Response[Identify]报文后，将该 EAP-Response[Identify]报文进行封装后发送给 AS，即发接入请求报文 Access-Request 给 AS。

这里，假定设备端 AC 与认证服务器 AS 之间通过 EAPoR(EAP over Radius) 协议进行通信，则 AC 将 EAP-Response[Identify]报文封装在用户远程拨号认证服务（RADIUS）报文中，通过 EAPoR 报文形式发送给 AS。

步骤 405~406：AS 收到接入请求报文后，解析出报文中的用户标识字段，并根据其中“@”后的域名部分确定是否为 OTP 取密码流程，如果“@”后为“OTP”，则当前为 OTP 取密码流程，否则，为正常的 802.1X 认证过程，按现有技术的处理流程完成认证即可。

如果是 OTP 取密码流程，则 AS 可根据需要直接生成本次的一次性密码，此种情况下，直接执行步骤 407；或者，AS 在进行 WLAN 业务权限判定后再确定是否生成一次性密码，这种情况下，AS 先根据用户标识字段中的 MSISDN 向 HLR 发起取用户国际移动用户标识（IMSI）的消息；AS 获取用户 IMSI 后，再向 HLR 发送取用户签约数据报文，要求获取该用户的签约信息，以检查该用户的 WLAN 业务属性，进而判断该用户是否有权限进行 OTP 业务。这里，如果当前用户终端不具备 WLAN 业务权限，则 AS 会向 AC 发送拒绝接入消息，AC 再向当前用户终端发送接入失败的报文，结束本次接入认证流程。

步骤 407~408：AS 根据解析出的、用户的 MSISDN 随机生成一次性密码 Key，然后，AS 将生成的密码 Key 通过短消息点对点协议（SMPP）打包成短消息的形式，通过提交短消息报文 Submit_SM 将密码 Key 发送给 SMSC；SMSC 收到后，向 AS 发送短消息提交响应报文 Submit_SM_resp，对 Submit_SM 消息进行响应，表示成功收到短消息；之后，SMSC 再通过短消息向当前用户的手机发送 AS 生成的密码 Key。

本步骤中，AS 也可以不根据用户的 MSISDN 生成一次性密码，AS 可以根据任意的密码生成算法，比如：利用随机数、随机种子加上某种现有的加密算法获得一个加密密钥，将该密钥作为一次性密码。另外，AS 也可以通过其它协议方式将短消息打包，提交给 SMSC，比如：通过七号信令方式打包。

步骤 409~410：当 AS 成功的将密码发给短消息中心后，AS 向 AC 发送拒绝接入报文 Access-Reject，该报文中可以携带本次失败的原因。

为了实现失败原因值的下发，可以扩展 Radius 标准消息的属性 Reply-Message，按照格式“[OTP] Error code = <code>; Message = <string>”定义一系列相关的失败原因，其中，Error code 为失败原因对应的取值，Message 是指该失败原因值的含义，即表示何种失败，AC 可以根据 code 值的不同向用户输出不同的提示。

AC 在收到 AS 下发的 Access-Reject 报文后，解析出具体的失败原因，然后通知用户。在本实施例中，AC 在收到 AS 的拒绝接入报文 Access-Reject 后，剥离出其中的失败报文 EAP-Failure，发送给客户端，同时，AC 可以根据失败原因向用户提示“密码已通过短消息发送”。

上述步骤 401~410 即为 OTP 密码获取流程，如图 4 中虚线框内步骤所示，获取密码后，当前用户终端即可使用所获得的密码进行接入认证，即执行步骤 411~422。获取密码后，当前用户终端可以立即进行接入认证，也可以在间隔一段时间后再进行接入认证，因此可以对每个一次性密码设置一个使用有效期，有效期的值可实时设定，也可预先设定一个默认值，比如：设有效期默认值为半小时，那么，当前用户终端在半小时内随时都可以利用所获取的一次性密码发起一次 802.1X 认证。

步骤 411：用户在获取一次性密码后，在客户端上输入 MSISDN@Simple 以及从手机中得到的密码，再通过 EAPoL_Start 报文重新发起新的一次 802.1x 接入认证流程。这里，采用 Simple 作为域名只是为了区别于密码获取的认证过程，说明本次为正常认证流程，实际上该域名可根据运营商需要任意设置。

步骤 412~414：AC 收到认证起始报文 EAPoL_Start 后，向客户端发送 EAP-Request[Identity]，要求客户端将用户名 Identity 送上来；客户端响应 AC 请求，发送 EAP-Response[Identity]，将 MSISDN@Simple 发送给 AC；AC 收到后，再将 EAP-Response[Identify]报文封装在 RADIUS 报文里，通过 EAPoR 报文形式发送给 AS。

步骤 415~417: AS 向 AC 发送密码请求报文 Access-Challenge（EAP-Request [MD5 Challenge]），请求密码进行认证；AC 收到密码请求报文后，剥离出其中的 EAP-Request[MD5 Challenge]报文，发送给客户端，请求 MD5 认证；客户端收到 EAP-Request[MD5 Challenge]报文后，按照 MD5 加密算法对用户输入的密码，即本次采用的一次性密码 Key 进行加密，然后通过密码响应报文 EAP-Response[MD5 Challenge]将密码回应给 AC。

步骤 418~420：AC 收到客户端响应后，将 EAP-Response[MD5 Challenge] 报文封装在 Radius 请求报文里发送给 AS，作为 Access-Challenge（EAP-Request [MD5 Challenge]）的响应；AS 收到 Access-Request（EAP-Response[MD5 Challenge]）报文后，按照同样的 MD5 加密算法对曾产生的、对应当前用户终端的一次性密码 Key 进行加密，然后判断加密后的结果是否与从报文中解析出的密码相同，如果相等，则 AS 向 AC 发送认证成功报文 Access-Accept；否则，发送认证拒绝报文 Access-Reject；

AC 如果收到 Access-Accept 报文，则向客户端发送认证成功报文 EAP-Success，标识接入认证成功；否则，向客户端发送认证失败报文 EAP-Failure，标识接入认证失败。

步骤 421~422：接入成功后，客户端进行 DHCP，并开始进行计费。

当然，WLAN 还可以通过 PPPoE 方式实现 OTP 的接入认证，该方式以当前用户终端作为 PPPoE 客户端，通过输入用户的手机号申请密码，认证服务器通过短消息将所生成的密码发送到提出申请用户的手机上，然后获取密码的用户再通过输入从手机中获取的密码进行接入认证。其中，PPPoE 具体要经过两个过

程进行接入：发现阶段和会话阶段，发现阶段可分为四步，其实这个过程也是PPPOE四种数据报文的交换的一个过程。当完成这四步后，用户主机与设备端双方就能获知对方的MAC地址和唯一的会话ID号，从而进入到会话阶段；会话阶段就是典型的PPP过程，在链路协商的时候，先与设备端协商认证方式，比如：采用PAP或CHAP认证方式，然后设备端通过Radius报文将用户的标识信息，如MSISDN@domain信息送到认证服务器，实现整个过程。

以上所述，仅为本发明的较佳实施例而已，并非用来限定本发明的保护范围。

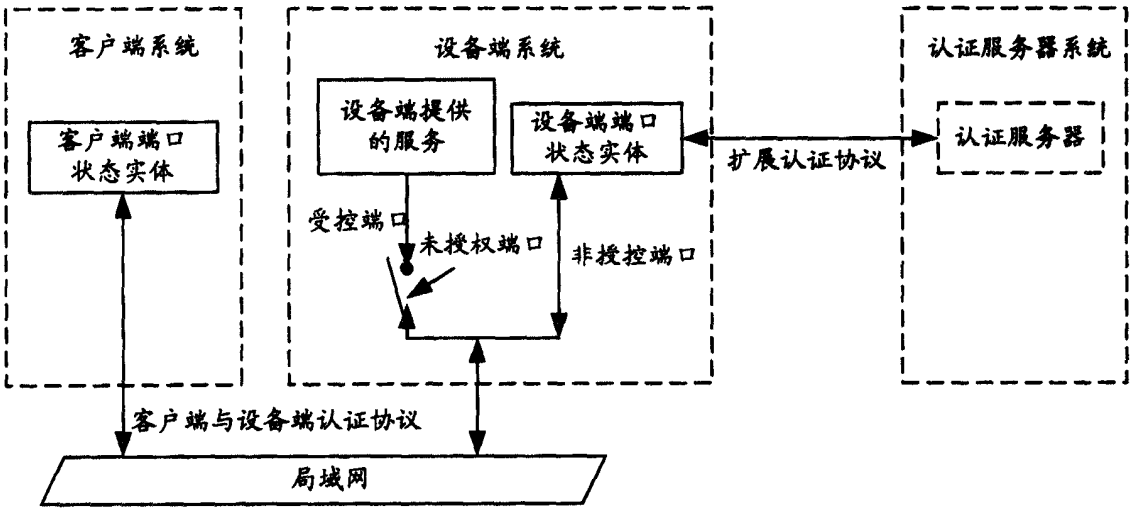

客户端系统
客户端端口
状态实体
设备端系统
设备端提供
的服务
设备端端口
状态实体
受控端口
未授权端口
非授控端口
扩展认证协议
认证服务器系统
认证服务器
客户端与设备端认证协议
局域网

图 1

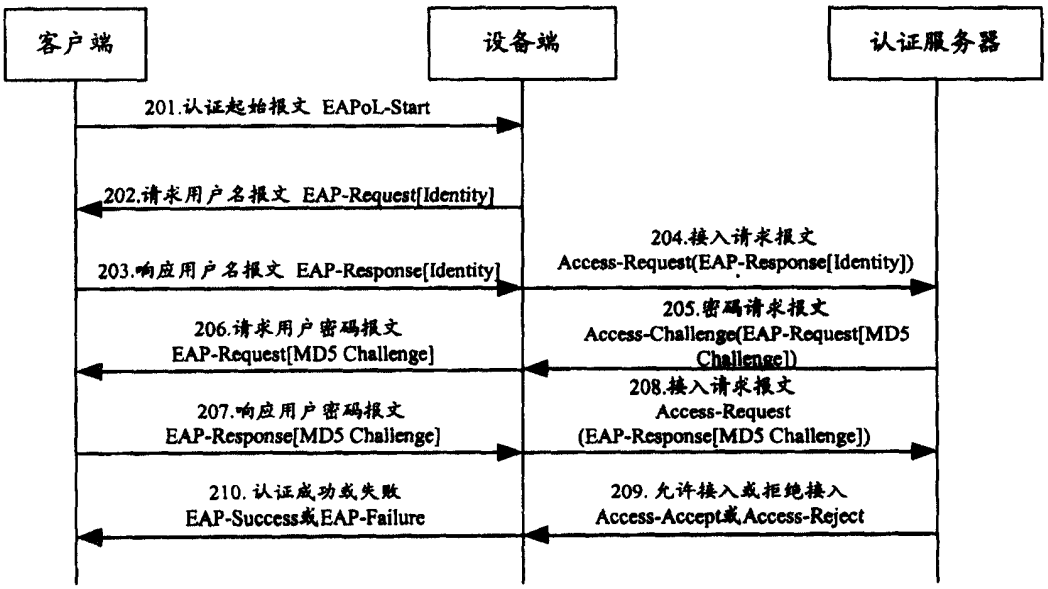

客户端
设备端
认证服务器
201.认证起始报文 EAPoL-Start
202.请求用户名报文 EAP-Request[Identity]
203.响应用户名报文 EAP-Response[Identity]
204.接入请求报文
Access-Request(EAP-Response[Identity])
205.密码请求报文
Access-Challenge(EAP-Request[MD5 Challenge])
206.请求用户密码报文
EAP-Request[MD5 Challenge]
207.响应用户密码报文
EAP-Response[MD5 Challenge]
208.接入请求报文
Access-Request
(EAP-Response[MD5 Challenge])
210. 认证成功或失败
EAP-Success或EAP-Failure
209. 允许接入或拒绝接入
Access-Accept或Access-Reject

图 2

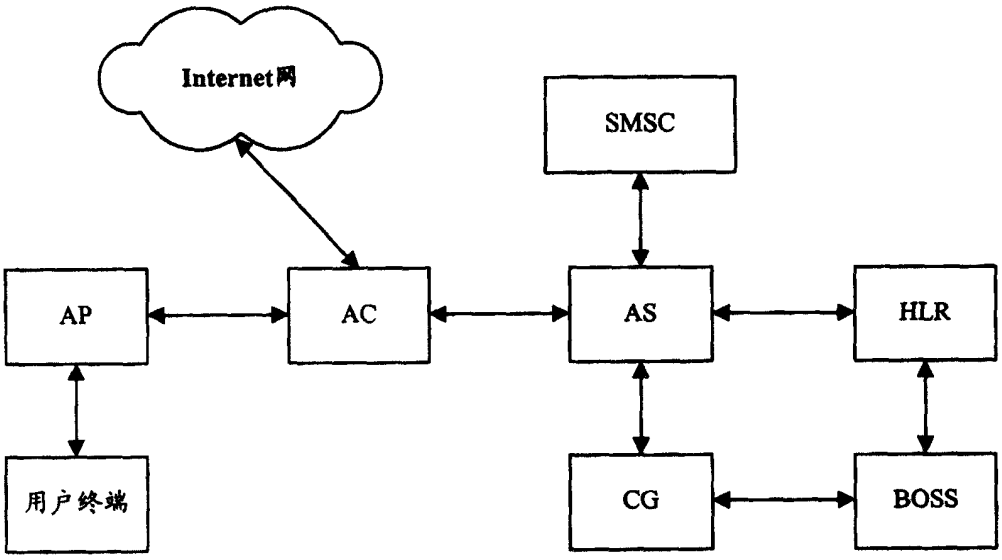

Internet网
SMSC
AP
AC
AS
HLR
用户终端
CG
BOSS

图 3

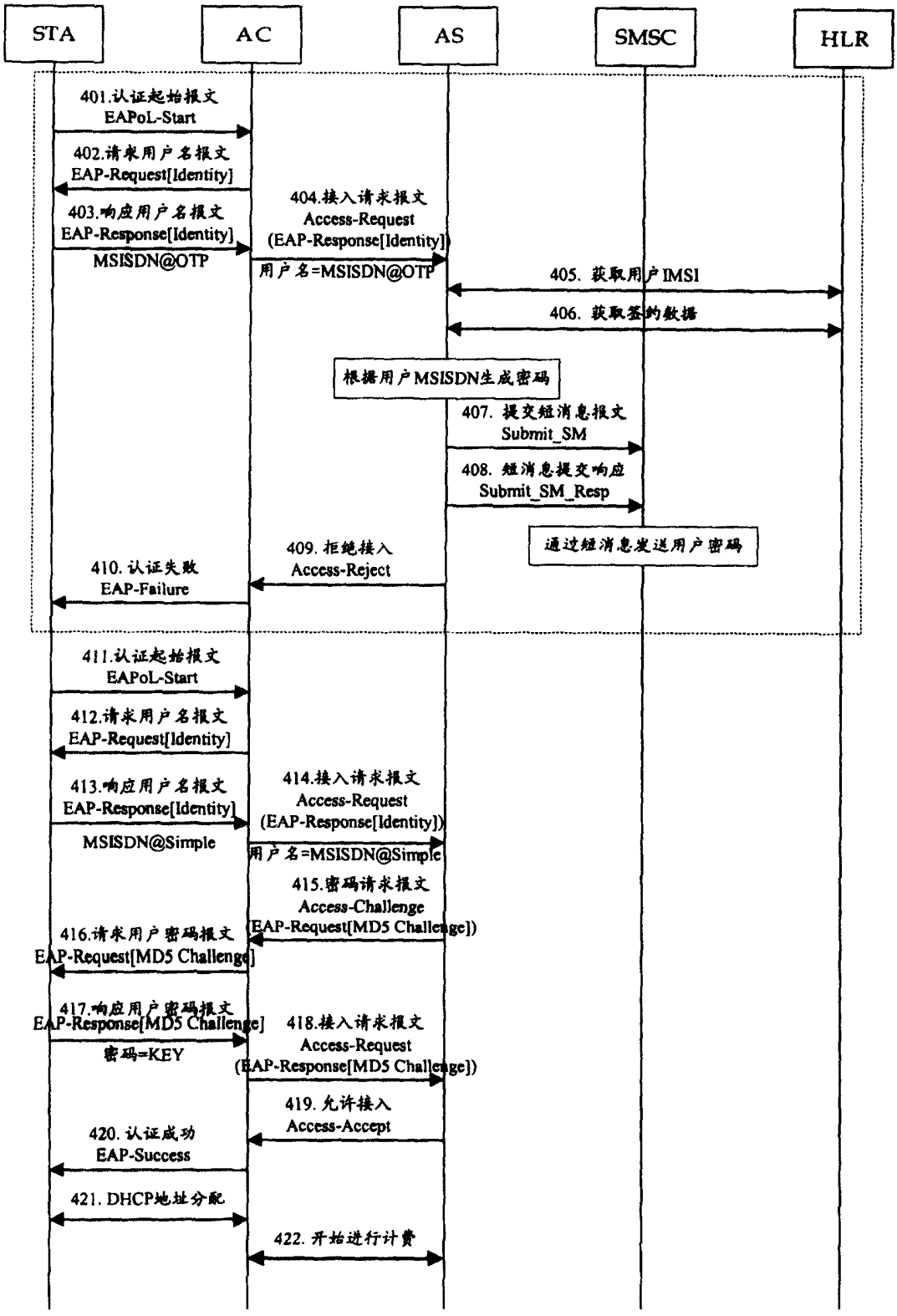

STA
AC
AS
SMSC
HLR
401.认证起始报文
EAPoL-Start
402.请求用户名报文
EAP-Request[Identity]
403.响应用户名报文
EAP-Response[Identity]
MSISDN@OTP
404.接入请求报文
Access-Request
(EAP-Response[Identity])
用户名=MSISDN@OTP
405. 获取用户IMSI
406. 获取签约数据
根据用户MSISDN生成密码
407. 提交短消息报文
Submit_SM
408. 短消息提交响应
Submit_SM_Resp
通过短消息发送用户密码
409. 拒绝接入
Access-Reject
410. 认证失败
EAP-Failure
411.认证起始报文
EAPoL-Start
412.请求用户名报文
EAP-Request[Identity]
413.响应用户名报文
EAP-Response[Identity]
MSISDN@Simple
414.接入请求报文
Access-Request
(EAP-Response[Identity])
用户名=MSISDN@Simple
415.密码请求报文
Access-Challenge
(EAP-Request[MD5 Challenge])
416.请求用户密码报文
EAP-Request[MD5 Challenge]
417.响应用户密码报文
EAP-Response[MD5 Challenge]
密码=KEY
418.接入请求报文
Access-Request
(EAP-Response[MD5 Challenge])
419. 允许接入
Access-Accept
420. 认证成功
EAP-Success
421. DHCP地址分配
422. 开始进行计费

图 4