



WLAN 无感知认证关键技术探讨

李林江

(中国电信股份有限公司广东研究院艾特实验室 广州 510630)

摘 要: WLAN 无感知认证是一种由终端自动识别的接入认证方式, 为用户提供方便快捷的 WLAN 接入服务, 极大地改变传统繁琐的接入方式, 有效地提升用户感知。首先介绍 WLAN 业务现状及认证存在的问题, 通过对 IEEE 802.1x 体系结构及认证方式的分析, 探讨基于 EAP 身份认证协议的无感知认证方式的技术原理、网络结构、认证流程等关键技术, 并对 3 种主流的无感知认证方法进行详细的分析比较, 最后对其应用推广进行总结。

关键词: WLAN; 无感知认证; PEAP; EAP-SIM/AKA; MAC

doi: 10.3969/j.issn.1000-0801.2013.09.008

Study on Key Technology of WLAN Service Non-Sense Authentication Method

Li Linjiang

(Information Technology Lab, Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: WLAN service non-sense authentication is one kind of automatic identification access authentication method, which can provide users with convenient WLAN access service, change the traditional cumbersome access ways, enhance the user perception. The current situation and the problems in access authentication of WLAN service were introduced, the IEEE 802.1x architecture and authentication method were analyzed, the key technology of non-sense authentication based on the EAP for principle, network structure and the certification process were discussed, and the main non-sense authentication method were compared. Finally, its application promotion were summarized.

Key words: wireless local area network, service non-sense authentication, protected extensible authentication protocol, EAP-SIM/AKA, MAC

1 前言

近年来, 由于 WLAN (wireless local area network, 无线局域网) 的低成本和便携性, 被广泛应用在互联网接入领域中。越来越多的移动设备 (笔记本、智能手机和 PDA 等) 开始支持 IEEE 802.11 标准。随着智能手机、平板电脑的广泛应用, 用户对 WLAN 的认知度和依赖程度越来越大, 更加关注网络安全和服务质量问题, 然而传统的 Web portal、cookie 认证和客户端登录流程复杂、便利性差等原

因严重影响了用户的体验。因此, 如何提供快速、优质的网络服务和业务体验, 提升用户感知, 提高用户满意度已成为电信运营商日益关注的焦点。

2 IEEE 802.1x 认证技术

为了解决 IEEE 802.11 的安全问题, IEEE 802 工作组制定了 IEEE 802.1x 标准。IEEE 802.1x 是一种基于端口的网络接入控制协议, 为用户提供了标准的认证和鉴权框架, 实现网络接入设备对所接入的用户设备进行端口的认

证和控制,如果用户设备能够通过认证服务器的认证和授权,便可以访问局域网中的资源;如果不能通过认证,则无法访问局域网中的资源。

2.1 IEEE 802.1x 的体系结构

IEEE 802.1x 的体系结构采用典型的客户端/服务器方式,包括 3 个实体:客户端、设备端和认证服务器^[1],如图 1 所示。

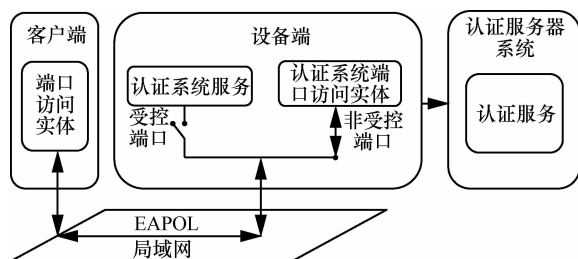


图 1 IEEE 802.1x 认证系统的体系结构

- 客户端:接入认证请求端,位于局域网一侧的实体。客户端用户通过发送EAPOL (extensible- authentication- protocol over LAN, 局域网可扩展认证协议) 发起 IEEE 802.1x 认证。
- 设备端:对客户端进行认证,通常为支持 IEEE 802.1x 协议的网络设备(胖 AP 或集中控制型 AC), 为客户端提供接入局域网的端口,分为受控端口和非受控端口,既可以是物理端口,也可以是逻辑端口。
- 认证服务器:为设备端提供认证服务,通常为 RADIUS(remote authentication dial-in user service, 远程认证拨号用户服务)服务器,主要实现对用户的认证、授权和计费等功能^[1]。

2.2 IEEE 802.1x 认证的工作机制

在 IEEE 802.1x 认证系统中,设备端主要对认证信息起传递作用,并把认证服务器认证的结果作用到端口,其本身并不参与具体的认证过程^[1],因此需要通过上层的协

议协助完成认证,EAP(extensible authentication protocol,可扩展的认证协议)用于实现客户端、设备端和认证服务器之间认证信息的交换。

- 在客户端与设备端之间,EAP 报文采用 EAPOL 消息封装格式,应用于局域网环境中。
- 在设备端与认证服务器之间,EAP 报文传递和交换方式有两种:一种由设备端进行中继,使用 EAPOR (EAP over RADIUS, 可扩展的远程拨号认证协议) 消息封装格式,承载于 RADIUS 协议中;另一种由设备端进行终结,利用 PAP 或 CHAP 的报文与认证服务器进行认证交互。
- 当客户端认证通过后,认证服务器将认证的用户信息传递给设备端,设备端再根据认证服务器反馈的信息(接受或拒绝)决定受控端口为授权或非授权状态。

3 WLAN 无感知认证关键技术

WLAN 无感知认证技术是一种由终端自动识别的接入认证方式,当用户使用具有 Wi-Fi 功能的手机或平板电脑时,通过首次简单的配置后,以后无需用户参与即可自动完成接入认证服务^[2]。WLAN 无感知认证主要基于 IEEE 802.1x/EAP 的集中式处理方式,采用 EAP 作为认证体系的消息传递机制。IEEE 802.1x 是一种基于端口的网络接入控制协议,为用户提供了标准的认证和鉴权框架,实现网络接入设备对所接入的用户设备进行端口的认证和控制^[2]。EAP 基于服务器/客户端的体系结构,提供了一些常见的功能和认证所需的身份验证机制,在此框架内大约有几十种不同的认证方法,常用的方法包括 LEAP、PSK、TLS、FAST、PEAP、TTLS、SIM/AKA 等^[3],如图 2 所示。

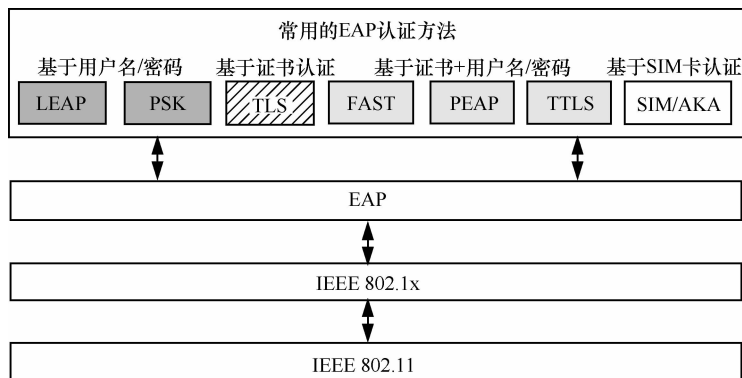


图 2 常见的 EAP 认证方法



根据调查,无感知认证主流的身份认证技术主要有 PEAP、EAP-SIM/AKA 及 MAC 地址认证方式。绝大多数智能终端及笔记本电脑都可通过以上方式进行用户身份认证和自动接入,避免传统 Web+portal 认证方式带来的繁琐操作,极大地提升了用户的业务使用体验。以下分别对这 3 种主流认证方式的技术原理进行简要分析。

3.1 PEAP 认证技术原理

PEAP 是 EAP 认证方法的一种实现方式,网络侧通过用户名/密码对终端进行认证,终端侧通过服务器证书对网络侧进行认证。用户首次使用 PEAP 认证时,需输入用户名和密码,后续接入认证无需用户进行任何手工操作,由终端自动完成。PEAP 的认证安全性较高,具体体现在以下几个方面。

- PEAP 客户端和 PEAP 认证服务器之间使用 TLS (transport layer security,安全传输层)协议创建加密通道。
- 在建立 TLS 隧道时,终端需要对认证服务器进行证书验证,防止网络侧的仿冒行为。
- 支持双向认证,用户认证采用 MS-CHAP-V2 (microsoft-challenge-handshake-authentication-protocol-version 2,微软质询握手鉴别协议)认证方式,不仅支持服务器对用户的认证,而且支持用户对服务器的认证。

PEAP 认证技术原理为:基于 EAP 认证协议框架,使用证书+用户名密码实现用户 WLAN 接入鉴权。终端与网络关联后,首先基于证书认证网络侧身份,建立 TLS 隧道,将存储在终端中的用户名/密码发送给网络侧进行用户身份认证,认证通过后 AC 分配 IP 地址进行互联网访问^[4]。PEAP 认证系统主要网元包括 WLAN 终端、WLAN 设备、AAA 服务器,如图 3 所示。

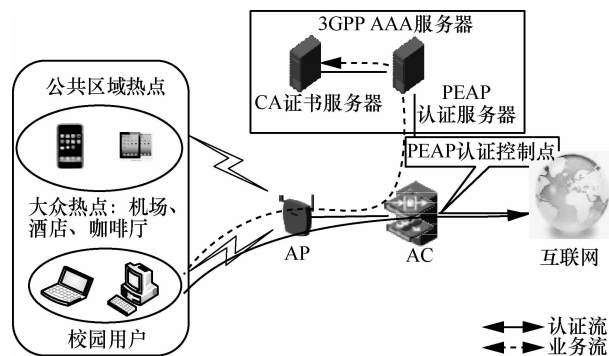


图 3 PEAP 认证系统网络结构

PEAP 认证系统主要网元介绍如下。

- WLAN 终端:为认证接入请求点,具备 Wi-Fi 功能的终端设备。当用户终端连接无线网络时,向 PEAP 认证系统发起身份鉴权请求,功能相当于 IEEE 802.1x 架构中的客户端;
- WLAN 设备:主要由 AP 和 AC 两大实体组成,其在 PEAP 认证中负责用户终端的接入鉴权,AP 网元应支持 IEEE 802.11i 的加密功能,AC 网元应支持 IEEE 802.1x 认证功能。
- 3GPP AAA 服务器:为 PEAP 用户认证的执行点,其在 PEAP 认证体系里主要由 CA 证书服务器和 PEAP 认证服务器两部分组成,实现 CA 证书授权和 PEAP 认证功能。

PEAP 认证总体流程主要有认证初始化、隧道建立、认证过程、地址分配以及计费开始 5 个阶段,如图 4 所示。

PEAP 认证流程简要说明如下。

(1)认证初始化:首先终端和 WLAN AN 建立关联,然后终端向 3GPP AAA 服务器发起鉴权请求。

(2)建立 TLS 隧道:基于证书认证网络侧身份,建立 TLS 隧道。客户端采用证书认证服务器,完成 TLS 握手,建立 PEAP 客户端和认证服务器之间的安全通道^[4,5]。

(3)认证过程:客户端和认证服务器之间基于用户名/密码进行 EAP 身份验证。整个 EAP 通信包括 EAP 协商在内,都通过 TLS 通道进行。服务器对用户和客户端进行身份验证,具体方法由 EAP 类型决定,在 PEAP 内部选择使用(如 EAP-MS-CHAPv2)^[6]。

(4)IP 地址分配:PEAP 认证完成后,WLAN 终端开启 DHCP 交互流程,并获取合法的 IP 地址,用户可以通过无线网络访问互联网资源。

(5)计费:包括计费开始、计费更新和计费结束三大流程,实现用户上网流量统计、在线时长和计费等功能。WLAN AN 作为计费的前端,主要将采集的原始数据传递给 RADIUS 服务器,由 RADIUS 服务器生成用户 WLAN 业务计费清单^[1]。

3.2 EAP-SIM 认证技术原理

EAP-SIM 认证也是 EAP 认证方法的一种实现方式,使用标准的 EAP-SIM/AKA 作为 Wi-Fi 终端接入认证机制,用户连接无线网络时不需要手动输入认证信息,通过 SIM 卡自动完成认证,提供良好的用户体验。另外,EAP-SIM 认证提供很高的安全性,主要体现在如下几个方面:

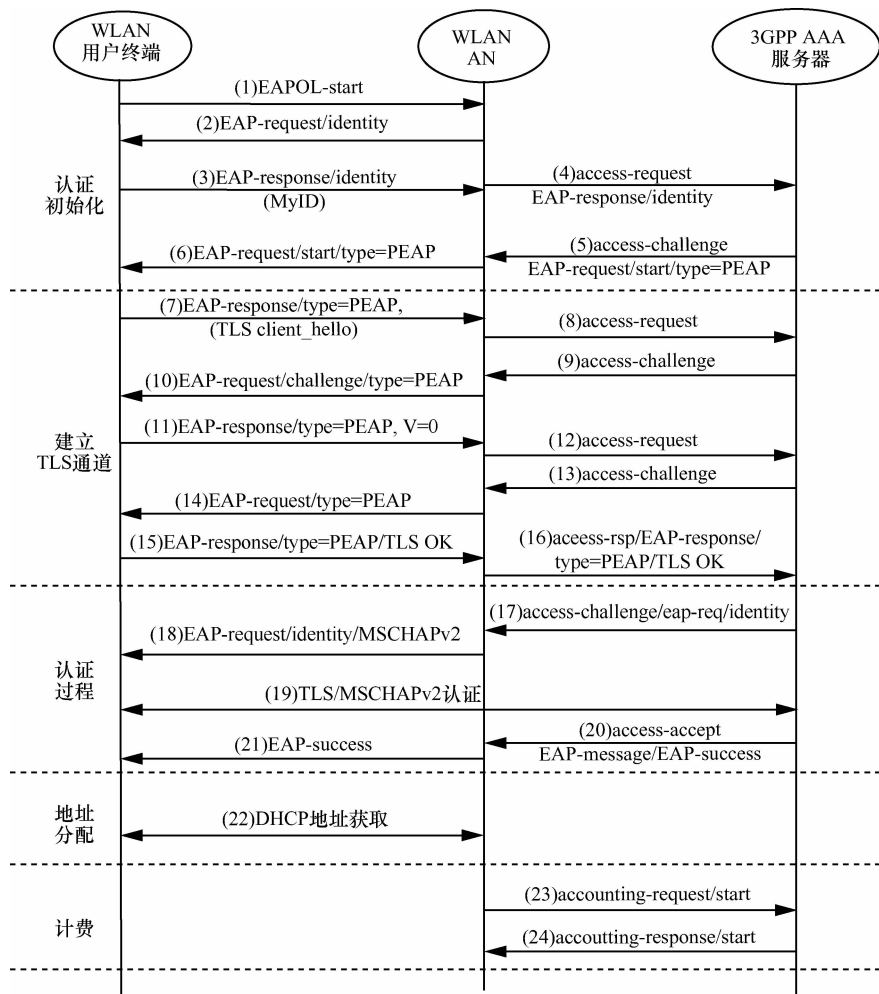


图 4 PEAP 认证总体接入流程

- 通过 SIM 卡进行认证密钥分发,有效防止密钥泄露和盗用;
- 支持伪随机用户名,防止用户真实身份泄露;
- 支持双向认证,服务器对用户的认证和用户对服务器的认证;
- 接入控制采用 IEEE 802.1x 技术进行端口级别管理,提高接入控制能力和安全性。

EAP-SIM 认证技术原理: 基于 EAP 认证协议框架,通过 SIM 卡的认证密钥分发实现用户的 Wi-Fi 接入鉴权。终端首次登录时,需将 SIM 卡的 IMSI 信息上报 3GPP AAA 服务器,3GPP AAA 服务器根据 HLR 鉴权和签约信息与终端交互完成认证,后续终端可直接使用网络分配的伪标识进行认证。认证通过后,AC 才为用户分配 IP 地址进行互联网网络访问。EAP-SIM 认证系统主要网元有 WLAN 终端、WLAN 设备、AAA 服务器以及 HLR 系统,如图 5 所示。

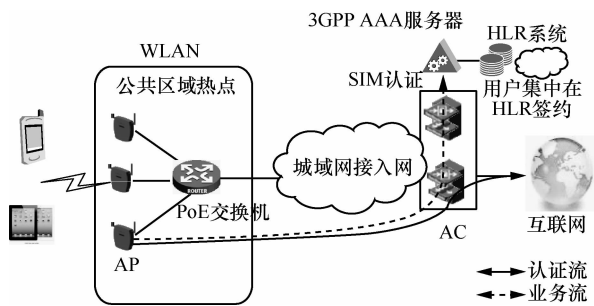


图 5 EAP-SIM 认证网络结构

EAP-SIM 认证主要网元及终端说明如下。

- WLAN 终端: 为 EAP-SIM 认证中的接入请求系统,主要指智能手机、平板电脑或带内置无线网卡的电脑等设备。当用户进行 EAP-SIM 认证时,WLAN 用户终端发起鉴权请求。
- WLAN 设备: 包括 AP 和 AC 两大实体,其在 EAP-SIM 认证中负责用户终端的接入鉴权,AP 网元应支持



IEEE 802.11i 的加密功能,AC 网元应支持 IEEE 802.1x 认证功能。

- 3GPP AAA 服务器:为 SIM 用户认证的执行点,实现用户的认证、授权和计费功能,另外还包括业务功能域、协议与接口域、管理域等功能模块。
- HLR 系统:在 SIM 认证体系中实现用户鉴权和签约信息的存储,与 3GPP AAA 服务器连接,完成鉴权和签约信息的交互。

EAP-SIM 认证总体接入流程主要有建立 IEEE 802.11 关联、认证授权、IP 地址分配、计费 5 个阶段,如图 6 所示。

EAP-SIM 认证流程说明如下。

(1)建立关联:首先终端和 WLAN AN 建立关联,然后终端向 3GPP AAA 服务器发起鉴权请求。

(2)认证授权:WLAN 终端与 3GPP AAA 服务器之间开始 EAP-SIM/AKA 认证阶段,进行双向身份认证,生成会话密钥,只有双向认证通过之后,服务器端才发送 EAP success 消息给客户端,客户端才可以接入网络。

(3)IP 地址分配:EAP-SIM/AKA 认证完成后,WLAN 终端开启 DHCP 交互流程,并获取合法的 IP 地址,用户可以通过无线网络访问互联网资源。

(4)计费:包括计费开始、计费更新和计费结束三大流

程,实现用户上网流量统计、在线时长和计费等功能。WLAN AN 作为计费的前端,主要将采集的原始数据传递给 RADIUS 服务器,由 RADIUS 服务器生成用户 WLAN 业务计费清单。

3.3 MAC 地址认证技术原理

由于手机终端和平板电脑操作的局限性,目前 portal 认证方式或客户端软件完成整个认证过程操作步骤相对复杂、技术性要求比较高,与 2G/3G 体验差距较大。而 EAP-SIM 认证受限于终端和网络,无法在短期内形成规模,MAC 地址认证方案主要针对以上问题进行优化,利用终端 MAC 地址作为认证的交互信息,同时通过短信进行身份信息校验,附着即认证,可有效提升用户体验。

MAC 地址认证技术原理:基于 EAP 认证协议框架,通过终端 MAC 地址和用户名/密码信息验证接入用户的合法性。用户首次登录时,Web 认证通过后,网络侧绑定终端网卡 MAC 地址与手机号码。当用户再次接入相同 WLAN,不必重复登录,认证服务器会根据保存的信息,让用户自动接入 WLAN,并可以通过短信的方式提醒用户。MAC 地址认证系统的主要网元有 WLAN 终端、WLAN 设备、AAA 服务器、MAC 绑定服务器、短信网关,如图 7 所示。

MAC 地址认证主要网元及终端说明如下。

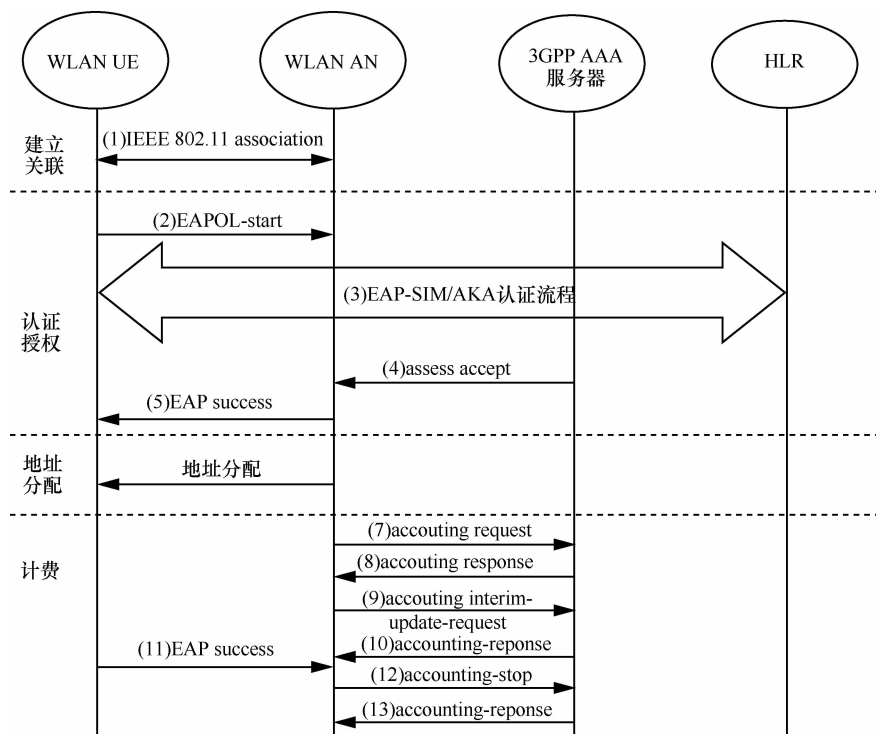


图 6 EAP-SIM 认证总体接入流程

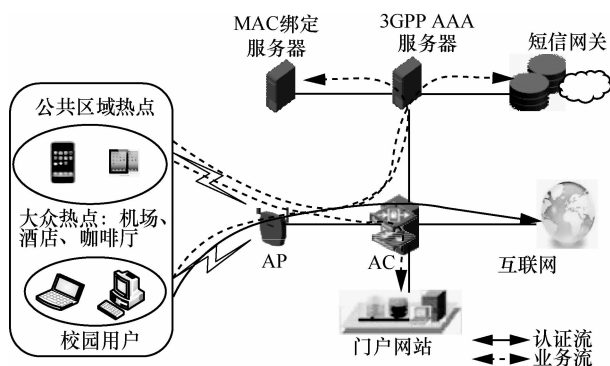


图 7 MAC 地址认证网络结构

- WLAN 终端: 为 MAC 地址认证中的接入请求系统, 主要指智能手机、平板电脑或带内置无线网卡的电脑等设备。当用户进行 MAC 地址认证时, WLAN 用户终端发起鉴权请求。
- WLAN 设备: 主要由 AP 和 AC 两大实体组成, 其在 MAC 地址认证中负责 WLAN 用户终端的接入鉴权。
- MAC 绑定服务器: 核对用户 MAC 地址的有效性, 保存手机 MAC 地址、用户名/密码的对应关系。可查询 MAC 绑定信息及状态管理, 包括 MAC、手机号码、信息校验及绑定状态等管理。
- 3GPP AAA 服务器: 为 MAC 地址认证体系中用户认证的执行点, 负责对 WLAN 用户终端认证和授权功能, 对应 IEEE 802.1x 架构中的认证服务器系统。
- 短信网关: 短信提示及用户交互功能, 主要用于用户绑定、解除捆绑等短信内容。

MAC 认证总体接入流程包括无线建立关联、地址分配、认证授权、计费几个阶段, 总体接入流程如图 8 所示。

MAC 地址认证接入流程说明如下。

(1) 认证初始化: 用户附着 WLAN, 终端和 AP/AC 建立关联。

(2) 地址分配: 终端向 AP/AC 发起 IP 地址请求, 通过 DHCP 获取 IP 地址, 同时 AC 监测用户上网流量。

(3) 认证授权: 主要分为 MAC 地址检查和 portal 认证 2 个阶段。AC 设置一定的流量阈值, 达到阈值即向 MAC 服务器发起 MAC 查询请求, 查询是否绑定。若 MAC 地址已绑定, 则携带账号、密码等信息向 AC 发起 portal 认证, AC 封装认证请求报文, 向 3GPP AAA 服务器发起认证请求, 请求通过后 AC 放行用户访问 Internet, 并告知用户上线。若 MAC 地址未绑定, 则 AC 向智能终端推送 portal 页面, 进行正常认证流程, 并且 3GPP AAA 服务器将用户账

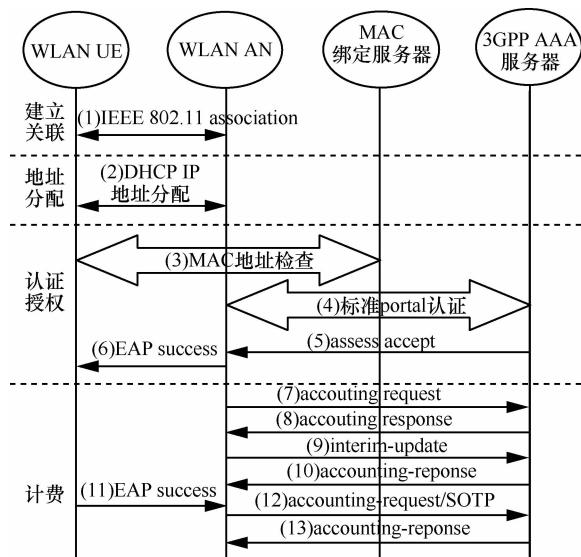


图 8 MAC 地址认证总体接入流程

号和 MAC 进行绑定。绑定操作完成后, 3GPP AAA 服务器调用短信网关程序下发短信。

(4) 计费: 包括计费开始、计费更新和计费结束三大流程, 实现用户上网流量统计、在线时长和计费等功能。WLAN AN 作为计费的前端, 主要将采集的原始数据传递给 RADIUS 服务器, 由 RADIUS 服务器生成用户 WLAN 业务计费清单。

4 PEAP/SIM/MAC 认证方式对比

与传统的认证方式不同, 无感知认证技术为用户提供方便快捷的 WLAN 接入服务, 极大地改变传统繁琐接入认证模式, 有效提升用户感知。以下分别从用户体验、终端兼容性、安全性以及改造成本方面对 3 种无感知认证方式进行对比。

- 用户体验: 当用户终端开通无感知认证功能, 无论是使用 PEAP 认证、EAP-SIM 认证或 MAC 地址认证, 只要在运营商 Wi-Fi 网络覆盖的区域内, 均可享受自动登录体验。不同的是, PEAP 与 MAC 地址首次认证时需要配置用户名和密码的登录信息, 而 EAP-SIM 认证首次登录不需要配置相关用户信息, 完全由终端自动处理, 认证过程相对简单, 但是无法实现机卡分离, 因此平板电脑用户无法通过 EAP-SIM 认证接入。
- 终端兼容性: 根据目前市面上主流的智能终端的测试和研究, 得出无感知认证方式的兼容性结果, 见表 1。



表 1 无感知认证方式的兼容性对比

终端	iPhone	BlackBerry	Android	Symbian	Windows Mobile
验证的操作系统	iOS 3 以上	OS 5.0/6.0	Android 2.1 以上	S60 V3/V5	6.5 以上
EAP-SIM	支持	支持	不支持	支持	不支持
PEAP	支持	支持	支持	支持	支持
MAC	支持	支持	支持	支持	支持

从表 1 可以看出,3 种主流的无感知认证方式 PEAP 与 MAC 兼容性相对较好,支持所有类型的智能终端,而 Android 和 Windows Mobile 的智能终端都不支持 EAP-SIM 认证,但 PEAP 认证存在证书兼容性问题,部分 Windows Mobile 终端需要手工安装证书才能使用 PEAP 认证。

- 安全性:3 种认证方式中,EAP-SIM 的安全性最好,由于直接与 SIM 卡绑定,共用 SIM 卡的鉴权方式;PEAP 的安全性次之;而 MAC 地址的安全性是最差的,因为 MAC 地址属于半公开信息,黑客窃取和伪造比较简单,只需要伪造用户 MAC 地址即可接入。表 2 给出了这几种认证协议在一些安全特性上的比较结果。
- 改造成本:由于受到 2G/3G 网络 HLR-license 因素的影响,EAP-SIM 改造成本较高。EAP-PEAP、MAC 方式改造成本较小,PEAP 认证需要 3GPP AAA 服务器配置认证证书,需评估不同服务器证书与各类终端的兼容性,如果服务器证书与终端预置证书验证不匹配 PEAP 认证可能失败。

表 2 无感知认证方式的安全性对比

认证方式	EAP-SIM	PEAP	MAC 地址
认证机制	使用 SIM 卡身份认证	基于证书+用户名密码实现身份认证	使用 MAC 地址身份认证
密钥管理	否	是	是
配置难度	容易	一般	容易
安全性	高	一般	低

综上所述,EAP-SIM/AKA 认证方式的优势在于加密性能最好,仿制可能性小;与 SIM 卡绑定,解决了换机问题;支持 WLAN 作为通信网统一认证上网,统一接入分组业务。而它的劣势在于对手机要求较高,手机操作系统支持少,网络改造较多,portal 认证不兼容。PEAP 认证方式的优势在于认证兼容性较好,加密方式较好,兼容现有 portal 认证方式;而劣势同样是对手机要求较高,网络改造较大。MAC 认证方式的优势在于终端适配和认证兼容性较好,支持大部分 WLAN 终端和兼容现有 portal 认证方式,劣势在于 MAC 地址仿冒问题很难根本

性解决^[6,7]。

5 结束语

通过以上介绍可以看出,目前主流的 3 种无感知技术方案都以简化用户认证流程、提升用户感知为目的,向用户提供更好的 WLAN 业务,使用户能够更加方便、快捷、自由地使用 WLAN 业务,各自存在一定的优缺点。如何能将其优点相结合,提出更加优化和完善的解决方案是未来研究的重点。未来 WLAN 业务的发展趋势需要实现 WLAN 与 2G/3G 网络的融合及统一,以 WLAN 分流 2G 网络数据流量、缓解无线网络压力为发展目标,引导更多的手机流量迁移到 WLAN,提高电信运营商在 WLAN 领域的市场竞争力,树立良好的企业形象。

参考文献

- 1 刘晓峰. IEEE 802.1x/EAP 认证方法的研究与分析. 赤峰学院学报,2012(7)
- 2 刘长瑞,聂明. 无感知 WLAN 业务认证方式的分析. 电信工程技术与标准化,2012(8)
- 3 柳瑞芸,彭宇,张旭平. 基于 EAP 的 WLAN 认证技术. 通信技术,2004(2):56~58
- 4 贾立波,陈科学,贾从茂等. IEEE 802.1x/PEAP 认证方法的研究和应用. 网络安全技术与应用,2009(5)
- 5 王璐,曹秀英. EAP 协议及其应用. 通信技术,2002(7)
- 6 管政,李勇. EAP-PEAP 自动认证应用于运营商 WLAN 网络的组网方案. 广东通信技术,2012(8)
- 7 Lei J, Fu X M, Hogrefe D. Comparative studies on authentication and key exchange methods for IEEE 802.11 wireless LAN. Computers and Security, 2007(26):401~409

作者简介



李林江,男,中国电信股份有限公司广东研究院艾特实验室工程师,主要研究方向为 PON、WLAN、IP 与多媒体子系统。

(收稿日期:2013-06-05)