doi:10.3969/j.issn.1000-436x.2012.z1.031

基于融合网络的 WLAN 漫游认证方式研究

刘璋喆，舒华英
（北京邮电大学 经济管理学院，北京 100876）

摘 要：在网络融合的趋势下，通过电信网络为 WLAN 网络提供终端认证将是未来 WLAN 业务认证的主要方式。为高效、安全地实现网间漫游状态下 WLAN 的鉴权认证，本研究分析了在网间漫游状态下 WLAN 的鉴权需求，讨论了鉴权模式、流程和存在的问题，提出了基于 EAP SIM/AKA 协议的、非中转方式的 WLAN 漫游认证方案，并进行了验证。实验结果证明该非中转认证方案可以满足终端在漫游状态下实现 EAP SIM/AKA 认证的需要，同时增强了系统的安全性，降低了投资成本，实现了实时计费。

关键词：认证；WLAN；网络融合；漫游
中图分类号：TP391.44 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0233-06

Research of WLAN authentication in roaming environment with the trend of network integration

LIU Zhang-zhe, SHU Hua-ying
(School of Economy and Management, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In the tendency of network convergence, the method of WLAN network client authentication based on telecommunications network will be the main way of WLAN authentication in the future. In order to make WLAN authentication efficiency and security under roaming condition, WLAN authentication requirements were analyzed, the authentication mode, the process and the existing problems were discussed. An application model and design scheme of WLAN network client authentication based on EAP SIM/AKA protocol with the trend of network integration were proposed and verified. Experimental results show that this application model can complete the EAP SIM/AKA protocol identification of a WLAN client in roaming process, reduce the investment of networks, keep the safety grades of the nodes in the visited WLAN with the initial safety grades, and realize the real-time charging.

Key words: authentication; WLAN; network convergence; roaming

1 引言

信息技术的蓬勃发展和终端功能的迅速提升，催生了产业加速融合的趋势。之前作为移动网络重要补充的 WLAN 网络，越来越受到电信运营企业和手机用户的青睐，基于 EAP SIM/AKA 协议的认证可实现通过移动通信网络为 WLAN 终端完成认证的功能，将 WLAN 与移动通信网络无缝地融合在一起，即使客户在他网漫游期间，也可以通过拜访地移动通信网络的认证功能登录和使用拜访地 WLAN 网络。

2 WLAN 漫游认证方式现状

为了减少网间适配的工作，目前，多数 WLAN 运营企业均采用中转方式实现 WLAN 网间漫游。在中转方式下，拜访地运营企业和归属地运营企业之间需要跨接一家中转商的网络（或网关、HUB），网络之间的认证、计费等消息的传输和网间适配工作均由该中转网络完成。中转方式可实现运营企业

收稿日期：2012-09-26

“一点接入，全球互联”，方便运营企业之间的对账和结算，降低运营企业之间进行网络连接和网络适配的难度。但这种方式也给运营企业网间漫游带来了新的故障点，增加了出现网络故障的概率，同时运营企业还需为中转服务支付费用。

基于中转方式，目前，WLAN 网间漫游的组网结构图如图 1 所示[1]。

归属地和拜访地 WLAN 网络中的 Radius 网元之间通过中转商的 Radius 互联，实现客户的认证消息传递；计费系统也经由中转商的计费系统互联，实现计费信息在拜访地和归属地 WLAN 网络中的传递，为 WLAN 运营企业提供计费对账依据。中转方式下，认证流程和计费流程除了要在拜访地和归属地 WLAN 网络各个网元之间传递外，还必须经过中转网络的 Radius 和计费系统。

3　中转方式中的 WLAN 认证问题

随着互联网业务的蓬勃发展和终端设备能力的提升，越来越多的客户选择在漫游的状态下使用 WLAN 业务。在目前广泛使用的中转方式下，WLAN 认证存在如下几个问题。

1) 认证消息和计费消息都承载在互联网上，安全性较低。

2) 消息均需经由中转商网络中转，增加了网络故障点，网络质量不高。

3) 有一定的计费能力，但仍需改进。

4　2G/3G 与 WLAN 融合网络中非中转方式 WLAN 漫游认证的设计

在网络融合趋势下，为满足 WLAN 网间漫游状态下客户认证和计费的需求，解决目前中转方式下网络安全性低、网络质量不高等问题，应借鉴 2G/3G 网络中的安全性和质量均较高的漫游信令网络，即将 EAP SIM/AKA 认证方式承载于现有移动网络中的漫游信令网上，既保证了安全性，又保证了实时传送，没有增加故障点，成本较低。

本研究提出了一种基于漫游信令网的、非中转方式的 EAP SIM/AKA 认证方案，其组网结构图如图 2

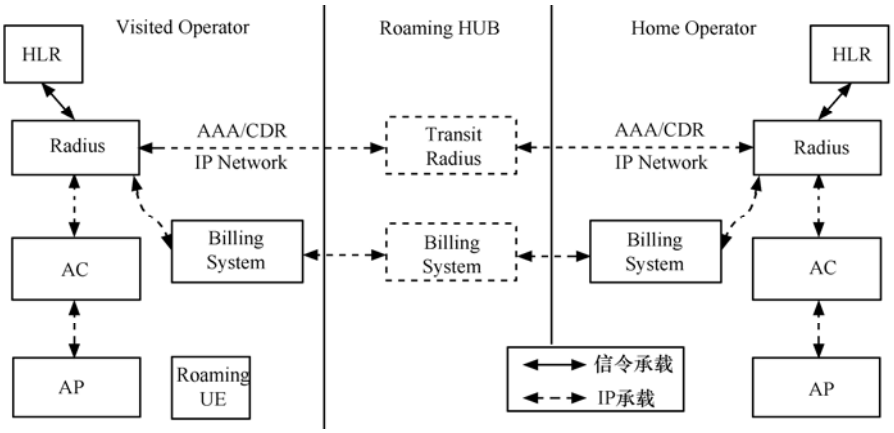

图 1　中转方式下 WLAN 漫游的网结构

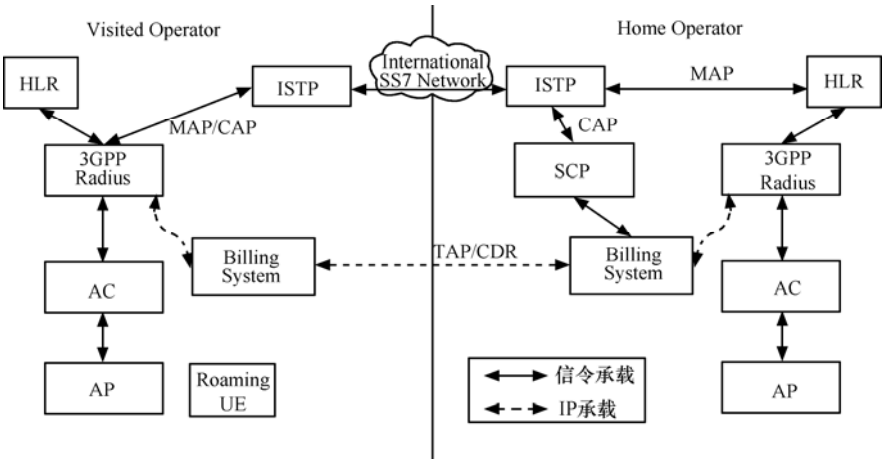

图 2　非中转方式下 WLAN 漫游的网结构

所示。

在基于漫游信令网的认证方案中，归属地 WLAN 网络与拜访地 WLAN 网络通过 2G/3G 网络中的信令设备 ISTP 和国际信令转接网络互联，实现认证消息和计费消息等信息的传递，计费系统之间定期传递话单记录。与中转方式相比，在该方案中省去了中转网络及相关设备，WLAN 网络得以通过现有 2G/3G 网元连接。

该方案具体认证流程与 EAP SIM/AKA 认证方案类似，如图 3 所示[2]。

各步骤说明如下。

1) WLAN UE 和 WLAN AN 建立关联之后，UE 向 WLAN AN 发送 EAPoL-Start，发起鉴权请求。

2) WLAN AN 发送 EAP-Request/Identity 消息到 WLAN UE。

3) WLAN UE 回复 EAP-Response/Identity 消息，向网络发送其用户身份标识信息，身份标识可以为伪随机 NAI 或永久 NAI。

4) WLAN AN 将 EAP 报文使用 RADIUS Access-Request 消息封装，并将 Identity 放在 Radius 的 User-Name 属性中，发送给 3GPP AAA Server。

5) 3GPP AAA Server 收到包含用户身份的 EAP-Response/Identity 报文。

6) 3GPP AAA Server 识别出用户准备使用的认证方法为 EAP-SIM。如果 UE 送上的 Identity 为伪随机 NAI，3GPP AAA Server 检查本地若没有该伪

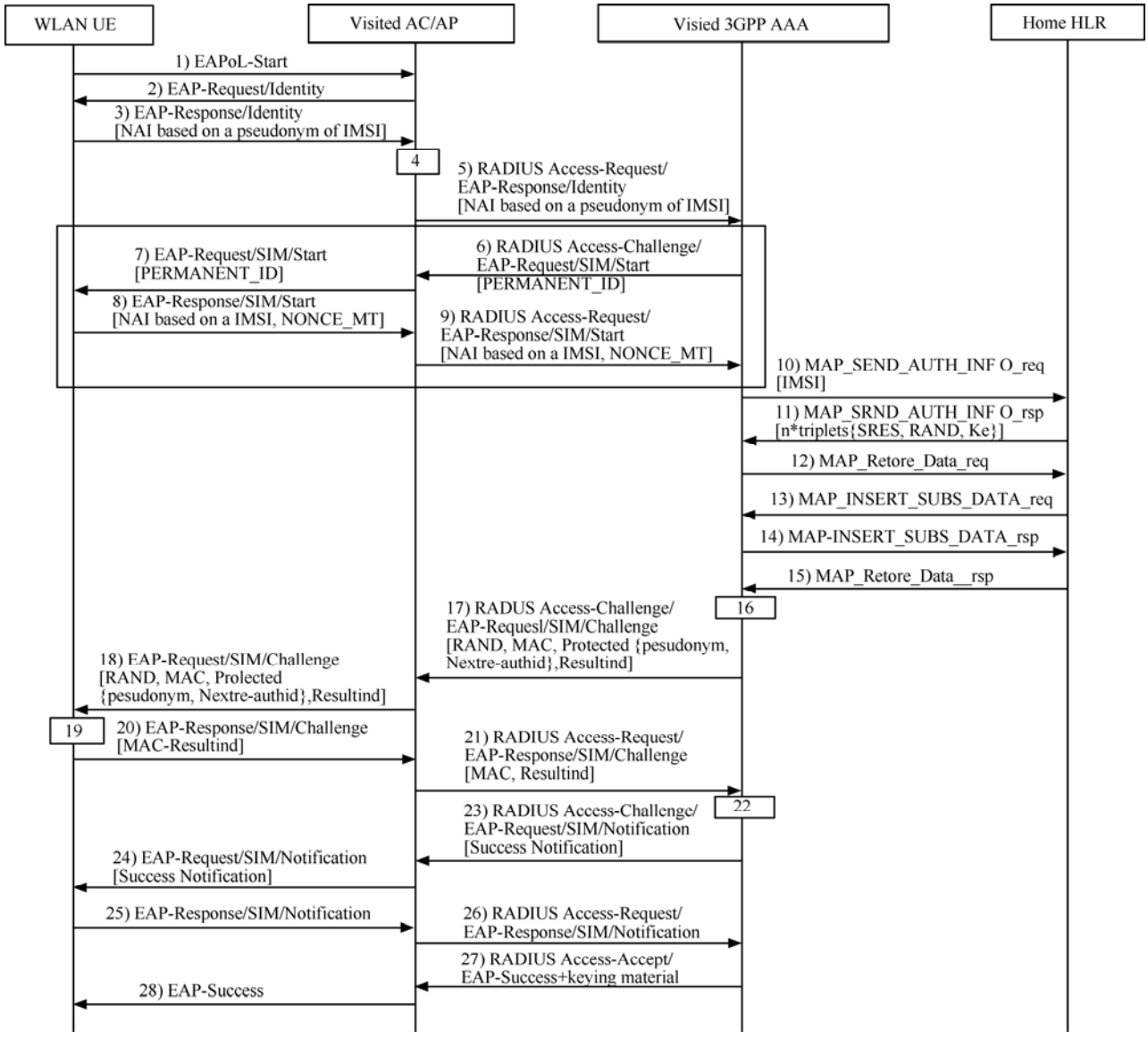

图 3　非中转方式下的认证流程

随机 NAI 与 IMSI 的映射关系，则使用 EAP Request/SIM-Start 消息再次请求永久 NAI(6)、7)、8)、9)步仅用于 WLAN UE 漫游到新的拜访地而使用其他 AAA 分配的伪随机 NAI 接入认证的场景）。EAP 报文封装在 RADIUS Access-Challenge 消息中，发送给 WLAN AN[3]。

7) WLAN AN 转发 EAP-Request/SIM-Start 消息到 WLAN UE。

8) WLAN UE 使用 EAP-Response/SIM-Start 消息携带永久 NAI 进行响应

9) WLAN AN 转发 EAP-Response/SIM-Start 消息携带永久 NAI 到 3GPP AAA Server，EAP 报文封装在 RADIUS Access-Request 消息中。

10) 3GPP AAA Server 检查本地是否缓存可用的鉴权向量，如果没有则向 HLR 发送 MAP_SEND_AUTH_INFO 请求，请求获取 *n* 组鉴权向量（*n* 可配置，取值范围 1~5）。

11) HLR 响应 3GPP AAA Server 鉴权请求，下发 *n* 组鉴权三元组[RAND, SRES, Kc]。

12) 3GPP AAA Server 检查本地是否存在用户的签约信息。如果没有，则 AAA 向 HLR 发起 MAP-RESTORE-DATA 请求，获取用户签约信息。

13) HLR 向 3GPP AAA Server 发起插入用户数据 MAP_INSERT_SUBS_DATA 请求，向 3GPP AAA Server 插入数据。

14) 3GPP AAA Server 响应 HLR 插入用户数据消息，完成用户签约信息获取。

15) HLR 向 3GPP AAA Server 回复 MAP_RESTORE_DATA 响应消息，完成 HLR 的交互流程。如采取从 BOSS 下发用户签约信息至 3GPP AAA Server 的操作，则取消 12)~15)步骤。

16) 3GPP AAA Server 检查用户签约通过后，根据算法生成 TEKs、MSK 和 EMSK（参见 IETF RFC4186），将 *N* 组（默认 *N*=2，可配置，同步设备规范）RAND 串起来后生成一个 *N*×RAND。为支持标识保密功能，3GPP AAA Server 还要生成伪随机 NAI 和快速重鉴权 NAI，用于后续的全鉴权和快速重鉴权过程。

17) 3GPP AAA Server 在 EAP-Request/SIM-Challenge 消息中发送 RAND，一个消息鉴权码（MAC）和 2 个用户标识（伪随机 NAI 和快速重鉴权 NAI）给 WLAN AN，EAP 报文封装在 RADIUS Access-Challenge 消息中。

3GPP AAA Server 可选发送给 WLAN UE 一个指示。指出希望保护最后的成功结果消息（如果结果成功）。

18) WLAN AN 转发 EAP Request/SIM-Challenge 消息到 WLAN UE。

19) WLAN UE 根据每个 RAND 为 128bit，解析出 *m* 个 RAND，依据 GSM 算法得出 K_sres，K_int、K_ency、Session_Key，并且用 K_int 得出 AT_MAC，和接收到的 AT_MAC 进行比较，如果一致，表示 3GPP AAA Server 认证通过。再利用 K_sres 作为 key 用规定的算法生成 MAC_SRES。

20) WLAN UE 使用新密钥素材覆盖整个 EAP 消息计算新消息认证码（MAC, message authentication code）值。WLAN UE 发送包含 RES 和新消息认证码的 EAP Response/SIM-Challenge 消息给 WLAN AN。

如果 WLAN UE 从 3GPP AAA Server 收到认证结果保护指示，则 WLAN UE 必须在此消息中包含结果指示。否则 WLAN UE 必须忽略该指示。

21) WLAN AN 发送 EAP Response/SIM-Challenge 报文到 3GPP AAA Server，EAP 报文封装在 RADIUS Access-Request 消息中。

22) 3GPP AAA Server 利用本端产生的 K_sres 作为 key 生成 MAC_SRES，和接收到的 MAC_SRES 进行比较，如果一致，表示终端认证通过。

23) 如果所有检查都成功，且 3GPP AAA Server 之前发送过认证结果保护标识，则 3GPP AAA Server 必须在发送 EAP Success 消息前发送 EAP Request/SIM/Notification 消息。EAP 报文封装在 RADIUS Access-Challenge 消息中，且用 MAC 保护。

24) WLAN AN 转发 EAP 消息到 WLAN UE。

25) WLAN UE 发送 EAP Response/SIM-Notification。

26) WLAN AN 转发 EAP Response/SIM-Notification 消息到 3GPP AAA Server，EAP 报文封装在 RADIUS Access-Request 消息中。3GPP AAA Server 必须忽略该消息内容。

27) 3GPP AAA Server 发送 EAP-Success 消息到 WLAN AN （可能在发送 EAP Notification 之前，参见第 23)步描述）。如果 3GPP AAA Server 产生了额外的用于 WLAN AN 和 WLAN UE 间链路保护的机密性和/或完整性保护的鉴权密钥，3GPP AAA Server 在 RADIUS Access-Accept 消息中包含这些密

钥素材。

28) WLAN AN 通过 EAP Success 消息通知 WLAN UE 鉴权成功。至此，EAP-SIM 交互已经成功完成，WLAN UE 和 WLAN AN 共享交互过程中生成的密钥素材[4]。

认证处理可能在任何时候失败，例如由于消息校验码检查失败或者 WLAN UE 没有对网络请求给予响应。这种情况下 EAP-SIM 过程将按 IETF RFC 4186 中描述终止。

在非中转方案中，计费信息在拜访地的 Radius 中产生后，将经由拜访地 ISTP、国际信令转接网络发送到归属地的 SCP 设备中，由 SCP 记录计费信息并向拜访地网络反馈应答信息。具体流程如图 4 所示。

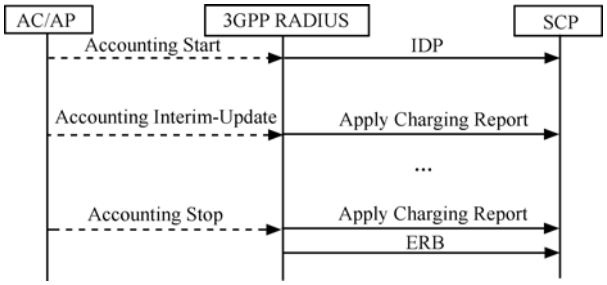

图 4　非中转方式下计费消息流程

非中转方案的计费消息传递周期可根据业务需要调整，通常每 15min 传递一次。

5　非中转方式认证方案的实验验证

为了验证该认证方案的可行性，本研究设计并进行了模拟实验验证。对形成对比效果，在实验室环境下对中转方式和非中转方式分别组网并验证，实验验证的网络拓扑如图 1 和图 2 所示。

在中转和非中转方式下分别进行了 10 组模拟实验，每组进行连续 10 次认证过程，将每组的成功认证平均时间列出，如图 5 所示。

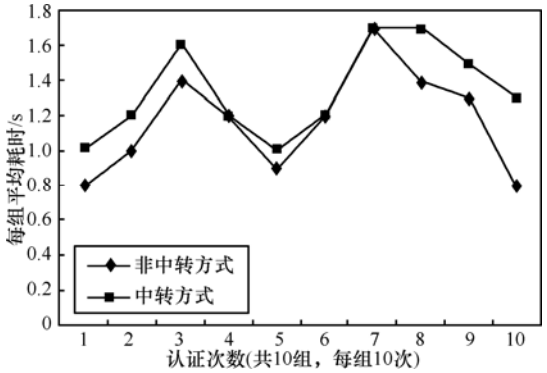

图 5　模拟实验结果

图 5 中横坐标为认证次数，纵坐标为认证协议的执行时间，单位为 s。模拟验证的结果表明，在同等网络环境下中转方式的认证时间大于非中转方式，由于中转方式还需考虑中转网络的时效性和安全性，中转方式的认证时间会比非中转方式更长。

通过以上模拟仿真实验的数据和分析可得出如下结论。

1) 提高效率。避免了对中转网络的依赖，归属地 WLAN 网络和拜访地 WLAN 通过信令直接连接，所以可以大大提高了效率，节省网络资源。

2) 节约认证时间。经实验验证，非中转方式与中转方式的认证原理相同，但由于网络承载的变化，非中转方式用时明显小于中转方式，节约了认证时间。

3) 增强安全性。在中转方式下，认证消息是在公开的互联网承载上传输，虽然有虚拟专网等方式加以保护，但仍比非中转方式下在信令这种私有网络上传输安全。

可以看出，非中转认证方案非常契合 WLAN 认证在网间漫游状态下的实际需求。

6　安全性及效率分析

非中转方式与中转方式相比，并没有改变整个协议交互流程，而且消息的传递次数也没有发生改变，只是用信令网络承载消息的传递，并在信令网上实现对 WLAN 计费信息的传递。

1) WLAN UE 对 WLAN AN 身份的有效认证。WLAN UE 对 WLAN AN 身份的认证依赖于随机数 r_1 的机密性，WLAN UE 发送的 $Ex(r_1)$ 只有 3GPP AAA 服务器才能解密，而 3GPP AAA 服务器发送的 $Ek_1(r_1)$ 只有合法的 WLAN AN 才能正确解密。如果 WLAN UE 接收到 WLAN AN 发送来的正确的 $h(r_1)$，则可以确认 WLAN AN 的合法性[5]。

2) 3GPP AAA 服务器对 WLAN AN 身份的有效认证。3GPP AAA 对 WLAN AN 身份的认证依赖于随机数 r_2 的机密性，3GPP AAA 发送的 $Ek(r_z)$ 只有合法的 WLAN UE 才能正确解密，而 WLAN UE 发送的 Er，(r_z) 只有合法的 WLAN AN 才能正确解密。如果 3GPP AAA 服务器接收到 WLAN AN 发送来的正确的 $h(r_z)$，则可以确认 WLAN AN 的合法性[6,7]。

3) 密钥材料的机密性。3GPP AAA 服务器将用随机数 r_2 加密的密钥材料随同 EAP 成功消息一起

发送给 WLAN AN。由于随机数 r_2 的机密性，可以保证密钥材料不被窃听，从而有效地保证了密钥材料的机密性[8,9]。

4) 对 IMSI 的安全性保护。利用 WLAN UE 和 3GPP AAA 服务器之间的共享密钥 K 对其加密后再进行传输。只有合法的 3GPP AAA 服务器才能正确解密，所以如果 NAI 中含有 IMSI，则 IMSI 是在加密之后传输的，这在一定程度上保证了用户身份信息传输的安全性[10]。

非中转方案在保证原有安全性能的基础上，通过信令传输替代公开的互联网传输，有效地提升了整个认证方式的安全性和效率。

7 结束语

在 WLAN 漫游业务中，认证是一个非常值得研究的问题。通过基于 2G/3G 成熟的、安全的、低成本的漫游信令网络实现 WLAN 认证消息的传递，可摆脱对中转网络的依赖，减少了网络故障点，增强了网络安全性，节约了认证时间和提高了效率。后续 WLAN 漫游的认证问题研究还任重而道远，如加密、完整性、隐私保护等都亟待深入研究。

参考文献：

[1] IEEF Std 802.11i-2004[S]. 2004.

[2] IEEE Std 802.1X-2001[S]. 2001.

[3] BLUNK L, VOLLBRECHT J. PPP, Extensible Authentication Protocol(EAP[S]. RFC2284, 1998.

[4] BLUNK L, *et al.* Extensible Authentication Protocol (EAP)[R]. Internet draft, draft-ietf-eap-rfc2284b-is-04.txt,2003.

[5] 舒华英.比特经济研究[M]. 北京: 人民邮电出版社, 2012.
SHU H Y. Study of Bit-Economy[M]. Beijing: Posts & Telecom Press, 2012.

[6] HAVERINEN H, SALOWEY J. Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)[R]. Internet Draft, draft-haverinen-pppext-eap-sim-13.txt, 2004.

[7] 舒华英.3G 时代中国电信业的机遇与挑战[J]. 北邮电大学学报(社会科学版), 2008, (5):57-60.
SHU H Y. Opportunity and challenge of Chinese telecom industry in 3G era[J]. BUPT Journal, 2008，(5):57-60.

[8] ARKKO J, HAVERINEN H. Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)[R]. Internet Draft, draft-arkko-pppext-eap-aka-15.txt, 2004.

[9] ABOBA B, SIMON D. PPP EAP-TLS Authentication Protocol[S]. IETF RFC 2716,1999.

[10] 3GPP TS33.102 3G Security[S]. Security Architecture.

作者简介：

刘璋誉（1978-），男，河北唐山人，北京邮电大学博士生，主要研究方向为企业管理工程、信息管理。

舒华英（1945-），男，陕西汉中人，北京邮电大学教授、博士生导师，主要研究方向为企业管理工程、管理信息系统与通信网优化规划。