基于 WAPI 的 WLAN 与 3G 网络安全融合

姜 奇[1)] 马建峰[1)] 李光松[2)] 马 卓[1)]

[1)](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

[2)](信息工程大学信息工程学院信息研究系 郑州 450002)

摘 要 以 3G 和 WLAN 为代表的异构无线网络融合是下一代无线网络发展的必然趋势.安全融合是网络融合面临的主要挑战之一,如何融合不同接入网络的异构安全体系结构、统一用户管理是亟待解决的问题.针对 3G 与基于 WAPI 的 WLAN 之间的安全融合问题,提出了新的基于 USIM 的证书分发协议,给出了松耦合和紧耦合两种安全融合方案,统一了 3G 安全体系与 WAPI 的用户管理,实现了 3G 签约用户基于 WAPI 安全机制的网络接入以及身份隐私保护.利用 CK 模型分析了证书分发协议的身份认证和匿名性,结果表明该协议是可证明安全的.

关键词 异构网络;安全融合;WAPI;匿名性;紧耦合;松耦合

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.01675

Security Integration of WAPI Based WLAN and 3G

JIANG Qi[1)] MA Jian-Feng[1)] LI Guang-Song[2)] MA Zhuo[1)]

[1)](*Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an* 710071)

[2)](*Department of Information Research, Information Engineering University, Zhengzhou* 450002)

Abstract Heterogeneous wireless network integration, typically 3G and WLAN integration, is an inevitable trend. Security is one of the major challenges which heterogeneous wireless network integration faces. How to integrate the vastly different security architectures used in each access network and unify user management is to be solved in urgent need. To achieve the security integration of 3G and WAPI based WLAN, a USIM based certificate distribution protocol is proposed. Two security integration schemes, i.e., loosely coupled and tightly coupled, are presented, which unify user management of 3G security architecture and WAPI, and realize WAPI based network access for 3G subscribers and identity privacy protection. The entity authentication and anonymity of the certificate distribution protocol is analyzed in CK model, and the results show that the protocol is provably secure.

Keywords heterogeneous networks; security integration; WAPI; anonymity; tightly coupled; loosely coupled

1 引 言

异构无线网络融合是下一代无线网络发展的必然趋势.一方面,无线网络技术发展迅速,出现了一系列无线接入技术标准,从无线个域网(WPAN),如蓝牙,到无线局域网(WLAN),再到无线城域网(WMAN)和无线广域网(WWAN),如第三代(3G)

收稿日期:2010-03-23;最终修改稿收到日期:2010-08-05.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z429)和国家自然科学基金(60633020,60702059,60872041)资助.**姜 奇**,男,1983 年生,博士研究生,主要研究方向为安全协议、无线网络安全等.E-mail: jiangqixdu@gmail.com. **马建峰**,男,1963 年生,博士,教授,博士生导师,主要研究领域为信息安全、密码学等. **李光松**,男,1977 年生,博士,讲师,主要研究方向为无线网络安全、密码算法设计与分析等. **马 卓**,男,1980 年生,博士,讲师,主要研究方向为可信计算、网络安全等.

移动通信网络.各种无线接入技术都拥有自己的应用优势和特点,例如具有不同的覆盖范围和带宽限制.因此,任何接入技术都不可能独领风骚,替代其它接入技术.可以预见,各种现有的以及未来可能出现的无线接入技术,既相互竞争,又互相补充,它们将共同存在并构成无处不在的异构无线网络环境.另一方面,随着双模甚至多模终端日益增多,用户希望"永远最佳连接(Always Best Connected,ABC)"[1],即利用接入网络的异构性、以最佳的方式连接到网络,体验各种网络服务,并保持服务的连续性,例如,在任何时间、任何地点高速接入 Internet.因此,异构接入网络之间的融合、无缝切换和透明服务提供方案呼之欲出.

WLAN 和 3G 是目前最具代表性的两种无线通信技术.UMTS(通用移动通信系统)和 CDMA2000 是两种具体的 3G 无线接入网络体系结构.3G 覆盖范围广,支持高速移动,能够提供无处不在的连接;然而,其成本高,且数据传输率还不能满足很多数据业务的需求.WLAN 虽然覆盖范围有限,但是其成本很低,数据传输率高,适合于热区覆盖.显然,两者具有很强的互补性.因此,3G 与 WLAN 融合网络是最具吸引力的,同时也是倍受业界和学术界关注的焦点.3GPP 已制定了 UMTS 与 WLAN 互联方案 3GPP I-WLAN[2],并将 WLAN 纳入了系统架构演进 SAE[3].

安全是 3G-WLAN 融合网络面临的主要挑战之一.融合网络需要同时应对来自 WLAN 和 3G 的安全威胁.由于 3G 和 WLAN 网络体系结构和安全威胁的差异,各自的安全解决方案也存在很大差异[4].UMTS 安全体系的关键组件是认证和密钥协商(AKA)[5],而WLAN则有IEEE802.11i[6]和 WAPI[7]两种不同的安全体系.任何单一的安全解决方案均无法提供完全的安全保证.如何融合不同接入网络的异构安全体系结构,统一用户身份管理是亟待解决的问题.

3GPP TS 33.234[8]定义了 3GPP I-WLAN 的安全体系结构,使用 AAA 和 EAP 技术作为 3GPP 和 WLAN 之间的纽带,采用 EAP AKA[9]使得 UMTS AKA 可以经由 WLAN 在用户终端(User Equipment,UE)和 3GPP 系统之间执行,实现了统一用户身份管理.Tseng[10]提出了基于口令和基于证书两种 3G 和 WLAN 融合网络的认证和计费方法.Tseng 又相继提出了基于 USIM 的证书分发机制,从而实现 3G 和 WLAN 统一用户管理方案[11-12].在文献[11]中,UE 首先利用基于 USIM 的证书分发机制请求临时证书,之后,利用 EAP-TLS 接入网络.文献[12]结合基于 USIM 的证书分发机制和 EAP-TLS,提出了 EAP-UTLS 认证协议.文献[11-12]均未对所提出方案进行形式化分析.

但是,现有方案主要是针对 IEEE 802.11i 和 3G 安全体系的安全融合,尚未有针对 WAPI 和 3G 安全体系的安全融合解决方案.一种显而易见的解决方案是在 UE 向 3G 网络签约注册时,为其颁发用于 WAPI 的证书,并建立证书与国际移动签约用户标识(IMSI)的映射关系.但是,由于 WAPI 机制的局限性,该方案存在如下问题:(1)无法实现用户身份隐私保护,一方面,用户不希望暴露自己的真实身份,即匿名性,另一方面,用户不希望之前的协议执行被第三方关联起来,即不可追踪性.(2)UE 需要预先存储多个运营商的证书以支持漫游.原因在于,现有的 WAPI 标准不支持漫游认证,用户必须拥有相应证书才能接入外地域运营商 WLAN.(3)多个证书导致证书管理复杂,如证书撤销.

本文针对 WAPI 和 3G 安全体系的安全融合问题展开研究.我们提出了新的基于 USIM 的证书分发协议,具有匿名性和不可追踪性,保护了用户身份隐私.同时解决了漫游 UE 与受访域认证服务单元(Authentication Service Unit,ASU)信任关系建立问题.结合证书分发协议和 WAPI-XG1,给出了两种安全融合方案,两种方案的区别在于证书分发与 WAPI-XG1 之间的耦合度.第 1 种称为松耦合,证书分发与 WAPI 相对独立,UE 先使用 3G 接口卡采用证书分发机制申请证书,然后,使用 WLAN 接口卡在 WAPI 机制下接入 WLAN 接入网(Access Network,AN).第 2 种称为紧耦合,即将证书分发叠加到 WAPI 接入认证机制中.两种方案互为补充,实现了 3G 安全体系与 WAPI 用户统一管理及 3G 签约用户基于 WAPI 安全机制的 WLAN 接入.我们利用 CK 模型[13-14]对证书分发方案的身份认证和匿名性进行了形式化分析.

2 背景知识

2.1 相关工作

3G 和 WLAN 各自面对的安全威胁不尽相同,各自的安全解决方案也存在很大差异[4].UMTS 安全体系的关键组件是认证和密钥协商(AKA)[5],用于实现用户与网络之间双向认证,同时协商会话密

钥，包括加密密钥(CK)和完整性密钥(IK)，防止未经授权的“非法”用户接入网络以及未经授权的“非法”网络为用户提供服务. AKA 的挑战/响应机制独立于网络，并可以在其它传输机制中运行，尤其是 IETF 的 EAP 框架. UMTS AKA 依赖终端的防篡改智能卡，该智能卡在 UMTS 中称为 UICC，它运行称为 USIM 的应用程序，由 USIM 在 AKA 执行过程中执行加密算法.

在 WLAN 方面，国内外分别制定了相关安全标准. 在国际上，WEP 协议是 IEEE 802.11 引入的第一个数据链路层安全机制，但是，WEP 早在 2001 年就被发现存在严重安全漏洞[15]. 之后，于 2004 年 6 月通过了新的 WLAN 安全标准 IEEE 802.11i[6] 以弥补 WEP 存在的安全问题. 在国内，2003 年 11 月 1 日正式实施第一个国家标准 GB 15629.11-2003，其中的安全解决方案称为 WLAN 鉴别和保密基础设施(WAPI). 2004 年 3 月，中国 IT 标准化技术委员会的国家宽带无线 IP 标准工作组(BWIPS)发布了 WAPI 的实施方案，对原国家标准 WAPI 的一些安全缺陷进行了修正. 中国宽带无线 IP 标准工作组于 2006 年 7 月 31 日公布了新的国家标准 GB 15629.11-2003/XG1-2006(WAPI-XG1)[7]. WAPI-XG1 是在 WAPI 及其实施方案的基础上提出的新的 WLAN 安全解决方案. 目前，WAPI 已作为 WLAN 接入安全机制独立标准形式成为国际标准. IEEE 802.11i 和 WAPI 均未提供漫游安全解决方案.

为了克服 EAP AKA 所存在的安全问题和低效性，文献[16]采用 EAP TLS 和公钥基础设施(PKI)作为 3G-WLAN 融合网络的认证机制. 文献[17]借助于 PKI，解决了密钥管理及 UE、接入认证服务器和归属认证服务器三方认证问题，其优势在于不需要不同网络运营商之间提供额外的信任管理功能. 文献[18]提出了局部化双重签名认证协议(LDSA)，采用局部化认证方法，如 EAP TLS、EAP TTLS 等，实现 UE 和独立 WLAN 运营商之间的认证和授权，借助于双重签名实现记账和计费. 李亚辉等[19]提出了 EAP AKA 的改进协议 LFSA，结合快速签名给出了离线计费，采用局部化重认证方法提高了接入过程的效率. 同时，在 EAP AKA 的基础之上增加了对 WLAN 接入网络的身份验证.

文献[20]借助于短信服务统一了 WLAN 与 GPRS/UMTS 之间的用户身份管理，使得 UE 认证过程自动完成，无需用户参与. 文献[20]假设 UE 是 GPRS/UMTS 网络签约用户，首先，漫游 UE 经由 GPRS/UMTS 网络向 WLAN 请求临时口令和相应的身份标识. 然后，UE 使用该临时口令和身份标识接入 WLAN. 然而，该方法的缺点在于：GPRS/UMTS 网络和 WLAN 之间的交互过程可能产生性能瓶颈；口令认证的安全强度不高.

Tseng[10] 针对 3G 和 WLAN 融合网络的认证和计费问题，提出了基于口令和基于证书两种方法. 之后，Tseng 又相继提出了基于 USIM 的证书分发机制，从而实现 3G 和 WLAN 统一用户管理方案[11-12]. 在文献[11]中，UE 首先利用基于 USIM 的证书分发机制请求临时证书，之后通过 EAP-TLS 接入网络. 文献[12]结合基于 USIM 的证书分发机制和 EAP-TLS，提出了 EAP-UTLS 认证协议. 然而，文献[12-13]并未给出证书分发机制的安全性证明. 文献[21]进一步提出了轻量级的匿名漫游机制，并采用 BAN 逻辑对方案进行了分析. 但文献[21]的分析仅限于双向认证，未对匿名性进行分析. 我们在本文中提出了新的证书分发机制，并利用 CK 模型对该机制的身份认证和匿名性进行了分析.

2.2　WAPI-XG1 回顾

WAPI-XG1 是在 WAPI 及其实施方案的基础上提出的新的 WLAN 安全解决方案. 它是 WAPI 系列标准中最完善的，并且在 CK 模型下是可证明安全的[22]. 在这里，我们给出 WAPI-XG1 的认证交互过程.

WAPI-XG1 支持两种认证方式：证书和预共享密钥(Pre-Shared Key，PSK). 当采用证书认证方式时，ASU 的基本功能是实现对用户证书的管理和用户身份的认证等. WAPI-XG1 支持两种格式的证书：X.509 v3 和 GBW 证书. UE 和接入点(Access Point，AP)分别拥有证书 $Cert_{UE}$ 和 $Cert_{AP}$. WAPI-XG1 由下面 3 个阶段组成：(1)基于证书的认证阶段，完成 UE 和 AP 之间的双向身份认证，并生成两者之间的基密钥(Base Key，BK)；(2)单播密钥协商阶段，利用 BK 在 UE 和 AP 之间协商会话密钥；(3)一个可选的群组密钥通告阶段，通告 AP 用于群组通信的群组密钥.

当 UE 和 AP 之间采用 PSK 认证方式时，PSK 直接作为 BK 进行单播密钥协商. 在这里，由于篇幅限制，我们仅介绍基于证书的认证阶段，如图 1 所示.

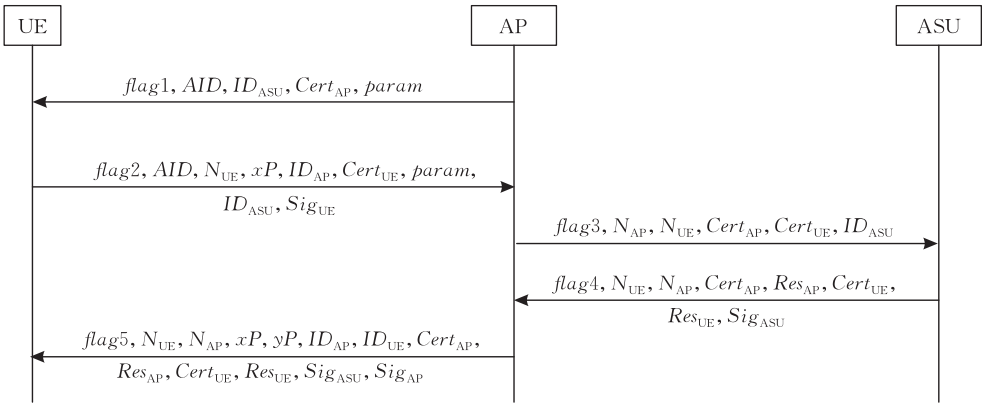


图 1 WAPI-XG1 接入认证协议

(1) 当 UE 关联或重新关联至 AP,UE 和 AP 选择采用证书认证与密钥管理方法,或 AP 的本地策略要求重新进行证书认证过程,或 AP 收到 UE 的预认证开始消息时,AP 向 UE 发送认证激活消息. 认证激活消息主要包括标记信息 $flag1$、认证标识 AID、本地 ASU 的身份标识 ID_{ASU}、AP 证书 $Cert_{AP}$ 和椭圆曲线参数 (G,p,P) 描述 $param$. 设 G 是基于椭圆曲线的加法群,阶为素数 p,生成元为 P.

(2) UE 接收到由 AP 发送的认证激活消息后,产生用于椭圆曲线 DH(ECDH)交换的临时私钥 x、临时公钥 xP 以及随机数 N_{UE}. UE 向 AP 发送接入认证请求消息,包括标记信息 $flag2$、AP 发送的认证标识 AID、随机数 N_{UE}、临时公钥 xP、AP 的身份标识 ID_{AP}、自己的证书 $Cert_{UE}$、椭圆曲线参数 (G,p,P) 描述 $param$、UE 信任的 ASU 列表及 UE 对消息各字段的签名 Sig_{UE}.

(3) AP 收到 UE 发送的接入认证请求消息后,检查 AID 和 Sig_{UE} 的有效性. 若检查通过,AP 生成随机数 N_{AP}. AP 向 ASU 发送证书认证请求消息,包括 UE 和 AP 的 MAC 地址的连接 $flag3$、随机数 N_{AP}、随机数 N_{UE}、AP 证书 $Cert_{AP}$、UE 证书 $Cert_{UE}$ 及 UE 信任的 ASU 列表.

(4) ASU 收到证书认证请求消息后,验证 AP 证书和 UE 证书. ASU 向 AP 发送证书认证响应消息,包括标记信息 $flag4$、随机数 N_{UE}、随机数 N_{AP}、AP 的证书 $Cert_{AP}$ 和验证结果 Res_{AP}、UE 证书 $Cert_{UE}$ 和验证结果 Res_{UE} 及 ASU 对消息各字段的签名 Sig_{ASU}.

(5) AP 收到证书认证响应消息后,检查随机数 N_{AP} 和签名 Sig_{ASU} 的有效性. 验证通过后,生成用于 ECDH 交换的临时私钥 y 和临时公钥 yP,使用自己的临时私钥 y 和 UE 的临时公钥 xP 进行 ECDH 计算,得到密钥种子 xyP,利用密钥导出算法 KD-HMACSHA256 对其进行扩展,生成基密钥然后设定接入结果为成功. AP 向 UE 发送接入认证响应消息,包括标记信息 $flag5$、随机数 N_{UE}、随机数 N_{AP}、临时公钥 xP、临时公钥 yP、AP 的身份标识 ID_{AP}、UE 的身份标识 ID_{UE}、AP 的证书 $Cert_{AP}$ 和验证结果 Res_{AP}、UE 证书 $Cert_{UE}$ 和验证结果 Res_{UE}、ASU 对证书认证响应消息各字段的签名 Sig_{ASU} 及 AP 对消息各字段的签名 Sig_{AP}.

(6) UE 验证随机数 N_{UE}、签名 Sig_{ASU} 及 Sig_{AP} 和证书验证结果 Res_{AP} 的有效性. 验证通过后,使用自己的临时私钥 x 和 AP 的临时公钥 yP 进行 ECDH 计算,得到密钥种子 xyP,利用密钥导出算法 KD-HMAC-SHA256 对其进行扩展,生成基密钥. 至此,AP 与 UE 建立了基密钥安全关联.

3 3G-WLAN 融合网络体系结构

我们设定 UE 为 3G 网络签约用户,UE 可以是 3G-WLAN 双模手机、PDA 及笔记本等. WLAN UE,即 WLAN 单模 UE,可以通过 WLAN 接口卡在热区,如机场、图书馆等,访问高速率数据服务. 而 3G-WLAN 双模 UE,还可以通过 3G 接口卡实现无缝连接. 目前 WLAN 存在两种不同的安全接入体系 IEEE 802.11i 和 WAPI. 在此,设定 WLAN AN 采用 WAPI 安全接入机制.

为了实现基于 WAPI 的 UE 接入,我们提出了 3G-WLAN 融合网络的体系结构. 图 2 为漫游场景下的网络体系. 该体系扩展了 3GPP I-WLAN,使得 3G 用户可以在 WAPI 机制下漫游接入,由 AN、3G 受访公共陆地移动通信网络域(3G VPLMN)和 3G 归属公共陆地移动通信网络域(3G HPLMN)三部分组成.

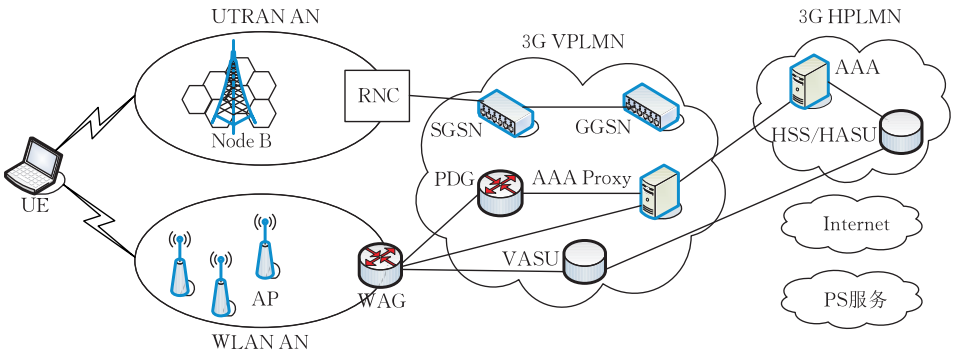


图 2　安全体系结构

AN 定义了网络元素：WLAN AN 和全球陆上无线接入 AN(UTRAN AN). WLAN AN 为 UE 提供无线 IP 连接，以便 UE 的请求能够被 3G 网络中的服务器认证和授权. UTRAN AN 是 UMTS 最重要的一种接入方式，为 UE 提供无缝连接服务.

在 3G VPLMN 中，SGSN、GGSN 是 UMTS 的核心网络元素. 3GPP AAA 代理(3GPP AAA Proxy)完成 AAA 的代理和过滤功能. WLAN 接入网关(WLAN Access Gateway，WAG)完成数据转发功能，目的是为 UE 提供 3G PS 域服务和 Internet 访问服务. 分组数据网关(Packet Data Gateway，PDG)可能位于受访网络，也能位于归属网络，通过 PDG 可以访问 3G PS 域的服务，是用户建立隧道传输数据的重要关卡. VASU 是受访域 ASU，为了支持 WAPI 所扩展的网络元素，主要完成用户证书管理和用户身份的认证等. VASU 是一个逻辑实体，其既可以与其它网络元素共存于一个物理实体，也可以独立存在.

3G HPLMN 主要有两种网络元素：3GPP AAA 服务器(3GPP AAA Server)和归属用户服务器(HSS). AAA 服务器完成 AAA 功能以及必要时为 PDG、WAG 和 WLAN AN 提供授权、策略实施以及路由信息. HSS 存储用户访问互联服务时需要的认证信息和服务订阅信息，其本质上是一个信息数据库. HASU，归属域 ASU，是为了支持 WAPI 所扩展的网络元素，主要完成用户证书管理和用户身份的认证等. HASU 是一个逻辑实体，其既可以与其它网络元素共存于一个物理实体，也可以独立存在. 在此，我们假设 HASU 与 HSS 共用一个物理实体.

4　安全融合方案

我们提出了基于 USIM 的证书分发方案，UE 通过该方案向 HSS 申请临时证书. 结合证书分发方案，提出了两种具体的安全融合方案. 两种方案的区别在于证书分发与 WAPI 之间的耦合度. 第 1 种是松耦合，证书分发与 WAPI 相对独立，UE 先使用 3G 接口卡采用证书分发机制申请证书，然后，使用 WLAN 接口卡在 WAPI 机制下接入 WLAN AN，适用于 3G-WLAN 双模 UE. 第 2 种是紧耦合，证书分发叠加到 WAPI 机制中，适用于 WLAN 单模 UE. 两种方案互为补充，实现了安全融合. 下面我们首先给出系统假设，然后详细介绍两种方案.

4.1　系统假设

WAPI 系列标准未提供漫游安全解决方案，即未解决漫游 UE 与受访域 ASU 信任关系建立问题. 同时，也未规定 ASU 证书管理方法. 因此，各 ASU 的证书可能由同一个证书权威(CA)颁发，也可能不同. ASU 可以通过多种可能途径获取并验证对方的证书的有效性，如在线 CA、证书链和交叉证书[23]等. 本文假定 HSS/HASU 拥有证书 $Cert_{\mathrm{HASU}}$，VASU 拥有证书 $Cert_{\mathrm{VASU}}$. 为了简化 ASU 证书的获取和验证过程，我们假设运营商在签订漫游协议时预先验证并存储了漫游伙伴的 ASU 证书. 此外，我们假设 UICC 卡上存储了 UE 与 HSS/HASU 之间的共享主密钥 K_{UH} 和 $Cert_{\mathrm{HASU}}$.

4.2　松耦合安全融合方案

松耦合包括两个阶段：证书分发阶段和 WAPI-XG1 安全接入阶段. 在证书分发阶段，UE 向 HSS/HASU 请求临时证书，HSS/HASU 颁发临时证书给 UE，并将 VASU 的证书发送给 UE，以方便 UE 建立与 VASU 的信任关系. 证书分发过程完成之后，UE 在 WAPI-XG1 机制下接入 WLAN AN. 详细过程如下：

(1) 当 UE 探测到 WLAN 信号并希望通过 WLAN 接入，UE 随机选择私钥 SK_{UE}，并计算相应的公钥 PK_{UE}，将(PK_{UE}，SK_{UE})作为临时证书的公

钥与私钥对. UE 向 HSS/HASU 发送证书请求消息 *CertReq*:

$$\{N, PK_{UE}, E_{PK_{HASU}}(ID_{VASU}, IMSI, TMSI, s, COUNT_{UE}, MAC_{K_{UH}}(ID_{VASU}, IMSI, TMSI, s, PK_{UE}, COUNT_{UE}, ID_{HASU}))\},$$

其中,ID_{VASU}是 VASU 的身份标识,ID_{HASU}是 HSS/HASU 的身份标识,*IMSI* 是 UE 国际移动签约用户标识,*TMSI* 是 UE 随机选择的临时身份. s 是会话标识符,$COUNT_{UE}$是计数器,目的是防止重放攻击,N 是随机数挑战,$MAC_{K_{UH}}$是使用 UE 的主密钥 K_{UH}计算的消息认证码.

(2)接收到证书请求消息 *CertReq* 之后,HSS/HASU 首先解密

$$D_{SK_H}(E_{PK_{HASU}}(ID_{VASU}, IMSI, TMSI, s, COUNT_{UE}, MAC_{K_{UH}}(ID_{VASU}, IMSI, TMSI, s, PK_{UE}, COUNT_{UE}, ID_{HASU})))$$

得到 *IMSI*;根据 *IMSI*,从签约用户数据库获取 UE 的主密钥 K_{UH},并利用 K_{UH}验证 $MAC_{K_{UH}}(ID_{VASU}, IMSI, TMSI, s, PK_{UE}, COUNT_{UE}, ID_{HASU})$的有效性. 若验证通过,HSS/HASU 构造 UE 的临时证书 $Cert_{UE}$:

$$\{PK_{HASU}, TMSI, PK_{UE}, T, Sig_{HASU}(TMSI, PK_{UE}, T)\},$$

其中 T 是临时证书的有效期. 根据受访网络标识 ID_{VASU},检索相应证书 $Cert_{VASU}$. HSS 发送证书响应消息 *CertRep*:

$$\{TMSI, Cert_{UE}, Cert_{VASU}, Sig_{HASU}(N, Cert_{VASU}, TMSI)\}.$$

(3)UE 在接收到证书响应消息之后,首先验证临时证书和签名的有效性. 若验证通过,将 VASU 加入 UE 信任的 ASU 列表,UE 成功与 VASU 建立了信任关系,解决了 WAPI-XG1 漫游信任关系建立问题.

(4)UE 利用 $Cert_{UE}$ 在 WAPI 机制下接入 Internet,具体过程如 2.2 节所述. 至此,UE 实现了基于 WAPI 机制的漫游接入.

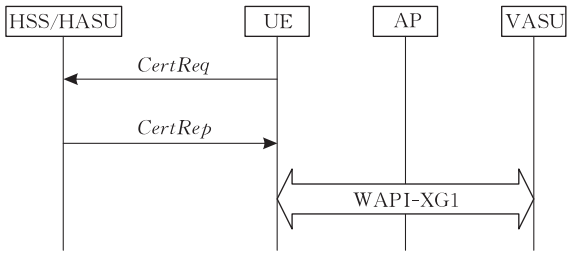


图 3 松耦合方案

4.3 紧耦合安全融合方案

该方案与上述方案的不同之处在于,证书分发过程被叠加到 WAPI 认证过程中. 具体而言,将证书请求消息 *CertReq* 叠加到接入认证请求消息和证书认证请求消息中,替换 UE 证书字段. VASU 接收到 *CertReq* 之后,将 *CertReq* 转发给 HSS. HSS 发送 *CertRep* 给 ASU 作为响应. 下面我们给出详细过程,如图 4 所示,着重指出其与 WAPI-XG1 不同之处.

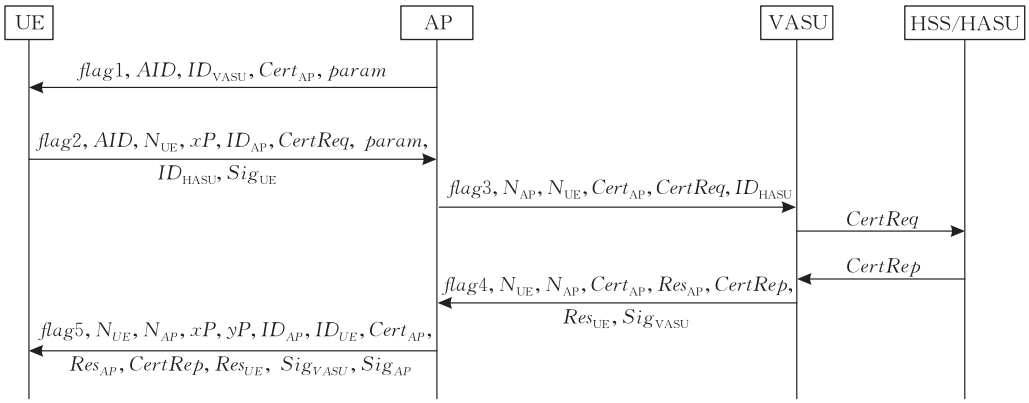


图 4 紧耦合方案

(1)AP 向 UE 发送认证激活消息.

(2)UE 发送接入认证请求消息给 AP,与 WAPI-XG1 的区别在于,将 $Cert_{UE}$ 字段替换为 *CertReq*.

(3)AP 接收到接入认证请求消息后,从 *CertReq* 字段获取 PK_{UE}并验证 Sig_{UE},验证通过后,发送证书认证请求消息给 VASU,与 WAPI-XG1 的区别在于,将 $Cert_{UE}$字段替换为 *CertReq*.

(4)VASU 首先从证书认证请求消息中解析出证书请求消息 *CertReq*,之后,将 *CertReq* 转发给 HSS/HASU.

(5)HSS/HASU 执行 4.2 节中步(2)的操作,并发送证书响应消息 *CertRep* 给 VASU.

(6)接收到 *CertRep* 后,VASU 根据归属网络

标识 ID_{HASU}，检索相应证书 $Cert_{HASU}$，并利用 $Cert_{HASU}$ 验证 $Cert_{UE}$. 验证通过后，发送证书认证响应消息给 AP，与 WAPI-XG1 的区别在于，将证书认证响应消息中 $Cert_{UE}$ 字段替换为 $CertRep$.

(7) AP 发送接入认证响应消息给 UE，与 WAPI-XG1 的区别在于，将 $Cert_{UE}$ 字段替换为 $CertRep$.

(8) UE 验证 $CertRep$，验证通过后，将 VASU 加入 UE 信任的 ASU 列表. 至此，UE 成功接入受访域 WLAN AN，同时，与 VASU 建立了信任关系，从而解决了 WAPI-XG1 漫游信任关系建立问题.

5　安全性分析

5.1　CK 模型

Bellare、Canetti 和 Krawczyk 于 1998 年引入了模块化思想来分析安全协议[13]，为利用可重用的模块构造新的可证安全的密钥交换协议提供了理论基础. 之后，Canetti 和 Krawczyk 进一步扩展了该方法[14]，称之为 Canetti-Krawczyk 模型，简称 CK 模型. CK 模型在安全协议设计方面的作用日趋明显，目前已应用于不同安全需求的安全协议设计[17,19,24-25].

在 CK 模型中定义了两种攻击模型，即理想模型 AM 和现实模型 UM[14]. AM 是认证的链路模型，在该模型中，攻击者是被动的，能够调用协议运行、攻陷协议参与者(Party corruption)、查询会话密钥(session key query)、暴露会话密钥(session key reveal)以及测试会话密钥(test session query). 但是，只能忠实地传递同一消息一次，不能伪造、篡改或重放来自未被攻陷的参与者的消息. UM 模型是未认证链路模型，攻击者除了能够执行 AM 模型中的所有攻击外，还可以伪造、篡改和重放消息.

认证器是模块化方法中一个非常重要的机制，它可以确保将 AM 中安全的协议转化为 UM 中安全的协议.

定义 1[13]. 设 π 和 π' 是 n 方消息驱动协议，π 运行在 AM 中，π' 运行在 UM 中. 如果对于任何 UM 敌手 U，存在一个 AM 敌手 A 使得 $AUTH_{A,\pi}$ 和 $UNAUTH_{U,\pi'}$ 是计算不可区分的，则称 π' 在 UM 中仿真 π.

定义 2[13]. 编译器 C 是一个算法，它的输入是协议的描述，输出也是协议的描述. 若一个编译器 C 对于任何的协议 π，协议 $C(\pi)$ 在 UM 中仿真 π，则这个编译器称为认证器.

定理 1[13]. 假设 λ 是一个 MT-认证器，也就是说 λ 在 UM 中仿真了简单消息传输(MT)协议，假设 C_λ 是在 λ 的基础上定义的一个编译器，那么可以说 C_λ 是一个认证器.

MT 协议即将一条消息由一个参与者发送给另一个参与者. 一个协议的认证器 C_λ 是若干个 MT 认证器 λ 的组合. 如果 AM 中协议只有一个消息流的话，那么一个 MT 认证器 λ 就可以作为认证器 C_λ，否则为 AM 中协议的每个消息流进行仿真的 MT 认证器 λ 组合在一起才能作为认证器 C_λ.

CK 模型首先在理想模型中证明协议的安全性，再利用认证器将协议转换到现实模型中. 基于 CK 模型设计认证和密钥协商(AKE)协议的基本方法一般可以分为以下 4 步[26]：

(1) 设计基本协议，并证明在 AM 下是安全的；

(2) 构造认证器，并证明是一个有效的认证器；

(3) 通过认证器将基本协议转换成 UM 下的安全协议；

(4) 进行必要的重新排序、重用消息组合以优化结果协议.

5.2　认证安全性分析

唐强已对 WAPI-XG1 进行了分析，指出其在 CK 模型下是可证明安全的[22]. 本节我们分析证书分发协议的认证安全性，将在 5.3 节中分析匿名性. 我们首先设计 AM 中的证书分发协议，然后，在现有的认证器基础上构造我们所需要的认证器，最后，应用所构造的认证器得到 UM 中的证书分发协议.

5.2.1　AM 中的证书分发协议

UE 和 HSS/HASU 需要经过一轮消息交互，实现证书的分发. 在 AM 中，由于敌手不能对消息进行伪造、篡改和重放，只能真实地转发合法参与者产生的消息，所以协议是安全的. 下面我们给出 AM 中的证书分发过程：

(1) UE 随机选择私钥 SK_{UE} 并计算相应的公钥 PK_{UE}，将 (PK_{UE}, SK_{UE}) 作为临时证书的公钥与私钥对，发送消息 $\{ID_{VASU}, IMSI, TMSI, s, PK_{UE}\}$ 给 HSS/HASU；

(2) HSS/HASU 收到消息后，构造 UE 的临时证书 $Cert_{UE} = \{PK_{HASU}, TMSI, PK_{UE}, T, Sig_{HASU}(TMSI, PK_{UE}, T)\}$，其中 T 是临时证书的有效期. 根据受访网络标识 ID_{VASU}，获取相应证书 $Cert_{VASU}$. 发送消息 $\{TMSI, Cert_{UE}, Cert_{VASU}\}$ 给 UE；

(3) UE 收到消息后，将 VASU 加入 UE 信任

的 ASU 列表.

5.2.2 证书分发协议认证器构造

在 CK 模型中,需要仿真 AM 协议的每个消息流,所采用的 MT 认证器组合在一起就构成了完整的协议认证器.本文采用了两种 MT 认证器:基于计数器的 MT 认证器[24]和基于数字签名的 MT 认证器[13],分别如图 5 和图 6 所示.采用基于计数器的 MT 认证器仿真 UE 向 HSS/HASU 发送的消息,采用基于数字签名的 MT 认证器仿真 HSS/HASU 向 UE 发送证书 $Cert_{\mathrm{VASU}}$,而发送 $Cert_{\mathrm{UE}}$ 则无需再仿真,因为 $Cert_{\mathrm{UE}}$ 本身已包含有 HSS/HASU 的签名和 UE 临时身份,可以理解为应用基于数字签名的 MT 认证器仿真的结果.

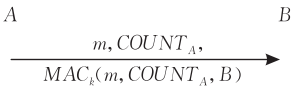


图 5 基于计数器的 MT 认证器

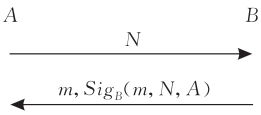


图 6 基于数字签名的 MT 认证器

完整的认证器由若干 MT 认证器组合而成.由于我们采用的认证器是可证安全的,基于计数器的 MT 认证器的安全性证明见文献[24],基于数字签名的 MT 认证器的安全证明见文献[13].因此,由定理 1 可知,所构造的认证器也是安全的.

5.2.3 UM 中的证书分发协议

将上述两种 MT 认证器分别应用于 AM 中协议的消息流仿真得到 UM 中的协议,如图 7 所示.由于所构造的证书分发协议认证器是可证安全的,从而,根据 CK 模型方法自动编译得到的如图 7 所示的 UM 协议也是可证安全的.然后应用文献[26]的方法优化 UM 中的协议,将图 7 中第一、二条消息合并,最后得到图 8 所示协议.文献[26]在 CK 模型下已证明该优化过程不影响协议的安全性.因此,图 8 所示的 UM 中证书分发协议是可证安全的.

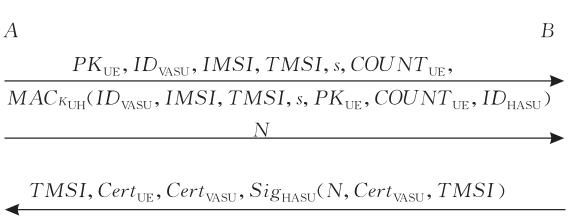


图 7 UM 中证书分发协议

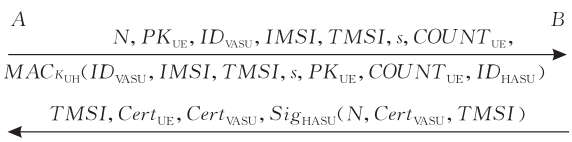


图 8 优化的 UM 中证书分发协议

5.3 匿名性和不可跟踪性

我们首先给出匿名性和不可追踪性的定义,然后对证书分发方案进行分析.

5.3.1 匿名性和不可跟踪性定义

为了描述方便,设 k 为系统安全参数,$UE(k)=\{UE_1, UE_2, \cdots, UE_{Q1}(k)\}$ 为所有 UE 的集合,$HASU(k)=\{HASU_1, HASU_2, \cdots, HASU_{Q2}(k)\}$ 为所有 HSS/HASU 的集合,其中 $Q_1(k)$、$Q_2(k)$ 为多项式.UE_i,$HASU_j$ 是参与方的身份,$1\leq i\leq Q_1(k)$,$1\leq j\leq Q_2(k)$.

在我们的分析过程中,匿名性攻击者模型采用 UM 模型.为了分析协议的匿名性,我们参考文献[24]设计了一个匿名游戏,该游戏的执行者是仿真器 S,S 将敌手 A 作为子程序激活运行.该游戏详细过程如下.

1. S 建立系统,其中的参与方为 $UE(k)$ 中的 UE 和 $HASU(k)$ 中的 HSS/HASU;

2. S 运行 A 并回答 A 的所有询问;

3. A 可以激活系统中的任意参与方和进行询问,从而在这些参与方之上运行证书分发协议;

4. A 从所有的系统参与方中选择两个 UE($UE_i, UE_j\in UE(k)$)和一个 HSS/HASU($HASU\in HASU(k)$);

5. A 向 S 发送测试询问,输入为($UE_i, UE_j, HASU$);

6. S 仿真证书分发协议的两个运行过程,一个的参与方是 UE_i 和 $HASU$;另一个是 UE_j 和 $HASU$.同时,S 更新每个参与方的状态信息.S 随机选择 $b\xleftarrow{R}\{0,1\}$,如果 $b=0$,返回 UE_i 的仿真脚本给 A,否则,返回 UE_j 的仿真脚本.

7. 接收到测试询问的响应后,A 还可以继续发起所有允许的攻击以及激活参与方来运行协议.

8. A 输出一个比特 b',作为对 b 的猜测,运行终止.

在上述游戏中,如果 UE_i、UE_j 和 $HASU$ 均未被攻陷,并且 A 输出了正确的比特 b' 使得 $b'=b$,则称攻击者 A 获胜,攻击者 A 获胜的优势定义为 $Adv_{\pi,A}(k)=|Pr[A\text{ 游戏获胜}]-1/2|$.

定义 3 如果在安全参数足够大的情况下,对任意多项式时间攻击者 A,其优势 $Adv_{\pi,A}(k)$ 都是可忽略的,那么称协议满足匿名性和不可追踪性.

5.3.2 匿名性和不可跟踪性分析

定理 2. 如果 $E_{PK_{\mathrm{HASU}}}$ 是 CCA 安全的,那么 $Adv_{\pi,A}(k)$ 是可忽略的.

证明.　如果协议不满足匿名性，也就是说攻击者 A 能以不可忽略 $v(k)$ 的优势获胜，那么我们可以构造加密方案 $E_{PK_{\mathrm{HASU}}}$ 的攻击者 D，使得 D 能以不可忽略的概率攻破 $E_{PK_{\mathrm{HASU}}}$.

我们简单描述一下 D 攻击过程：首先，D 适应性地选择密文以询问解密预言机. 然后，D 选择两个不同的消息 msg_0 和 msg_1，并向游戏仿真者询问密文. 仿真器随机选择 $b \xleftarrow{R} \{0,1\}$，并返回密文 $c = E_{PK_{\mathrm{HASU}}}(msg_b)$. 接收到密文 c 后，D 适应性地选择除 c 之外的密文询问解密预言机，最后输出 b' 作为对 b 的猜测.

现在构造该攻击者 D 来仿真游戏 Game 0，其中 D 扮演 A 的仿真器. (1)首先，D 选择并创建 UE 集合 $UE(k)$ 和 HSS/HASU 集合 $HASU(k)$. 然后，D 对 $UE(k)$ 中 UE 和 $HASU(k)$ 中的 HSS/HASU 进行初始化，为每个 UE 分配随机选自 $\{0,1\}^k$ 的认证密钥，并将计数器置为 0，为每个 HSS/HASU 分配随机选择的公钥与私钥对用于加密和签名. 之后，D 随机从 $HASU(k)$ 中选择 $HASU$，并将其加密密钥设置为 PK_{HASU}. (2) D 将 A 作为子程序激活运行，回答 A 的所有询问，仿真协议运行中参与方激活的所有响应.

如果 A 在测试询问中未选择 $HASU$，D 随机选择 $b' \xleftarrow{R} \{0,1\}$ 作为输出结果，并终止.

在测试询问中，如果 A 选择 $HASU$，D 构造并返回协议运行脚本，构造过程为：首先，D 随机选择 SK，计算相应的 PK，构造两个等长的消息 $msg_0 = \{ID_V, UE_i, TMSI, s, COUNT_i + 1, MAC_i\}$，$msg_1 = \{ID_V, UE_j, TMSI, s, COUNT_j + 1, MAC_j\}$. 将 msg_0、msg_1 作为输入询问 CCA 安全仿真器，该仿真器返回密文 c. 然后，D 构造 $message_1 = \{N, PK_{\mathrm{UE}}, c\}$，$message_2 = \{TMSI, Cert_{\mathrm{UE}}, Cert_{\mathrm{VASU}}, Sig_{\mathrm{HASU}}(N, Cert_{\mathrm{VASU}}, TMSI)\}$，其中 N 是随机数. 同时，D 更新 UE_i、UE_j 和 $HASU$ 的内部状态计数器的值.

D 将 $message_1$ 和 $message_2$ 作为测试询问的应答. 之后，D 继续执行游戏，回答 A 的所有询问并仿真协议运行中参与方激活的所有响应. 当 A 输出 b' 作为对 b 的猜测，D 输出 b' 并终止.

设 E 为 A 在测试询问中选择 $HASU$ 的事件. 由于 $HASU$ 是从 $HASU(k)$ 中均匀地随机选择而来，因而，$Pr[E] = \dfrac{1}{Q_2(k)}$. 因此，我们可以得到

$$\begin{aligned} &Pr[A \text{ 正确猜测 } b] \\ &= \left(\frac{1}{2} + v(k)\right) Pr[E] + \frac{1}{2}(1 - Pr[E]) \\ &= \frac{1}{2} + \frac{v(k)}{Q_2(k)}, \end{aligned}$$

并且不可忽略，得证.　　证毕.

6　结束语

本文研究了 3G 与基于 WAPI 的 WLAN 之间的安全融合问题. 我们提出了新的基于 USIM 的证书分发协议，结合证书分发协议和 WAPI-XG1，给出了两种安全融合方案. 第 1 种称为松耦合，证书分发与 WAPI 相对独立，UE 先使用 3G 接口卡采用证书分发机制申请证书，然后，使用 WLAN 接口卡在 WAPI 机制下接入 WLAN AN. 第 2 种称为紧耦合，即将证书分发叠加到 WAPI 接入认证机制中. 两种方案互为补充，实现了 3G 与 WLAN 用户统一管理及 3G 签约用户基于 WAPI 安全机制的 WLAN 接入，并且保护了用户隐私. 所提出的安全融合方案的身份认证和匿名性在 CK 模型下是可证明安全的. 但是，椭圆曲线密码学(ECC)在理论及工程实践中并不完善，容易遭受边信道攻击，如能量分析和时间分析. 我们下一步将研究 ECC 抵抗能量分析和时间分析攻击的强度. 此外，我们下一步还将通过仿真和测试床等手段分析对比两种安全融合方案的性能，主要包括计算开销和通信开销等指标.

参　考　文　献

[1] Gustafsson E, Johnson A. Always best connected. IEEE Wireless Communications, 2003, 10(1): 49-55

[2] 3GPP TS 23.234. 3GPP system to Wireless Local Area Network (WLAN) interworking; System description. 2008

[3] 3GPP TS 23.402. Architecture enhancements for non-3GPP accesses. 2010

[4] Shin M, Ma J, Mishra A, Arbaugh W. Wireless network security and interworking. Proceedings of the IEEE, 2006, 94(2): 455-466

[5] 3GPP TS 33.102. 3G security; Security architecture. 2009

[6] IEEE 802.11i. IEEE standard for Information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements—part 11: Wireless LAN medium access control and physical layer specifications amendment 6: Medium access control security enhancements. 2004

[7] National Standard of the People's Republic of China. GB15629.11-2003/XG1-2006 (Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications). 2006 (in Chinese)
(中华人民共和国国家标准. GB 15629.11-2003/XG1-2006 (信息技术—系统间远程通信和信息交换—局域网和城域网—特定要求第 11 部分：无线局域网媒体访问控制和物理层规范). 2006)

[8] 3GPP TS 33.234. 3G Security; Wireless Local Area Network (WLAN) interworking security. 2008

[9] Arkko J, Haverinen H. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). The Internet Society RFC 4187, 2006

[10] Tseng Y-M, Yang C-C, Su J-H. Authentication and billing protocols for the integration of WLAN and 3G networks. Wireless Personal Communications, 2004, 29(3): 351-366

[11] Tseng Y-M. GPRS/UMTS-aided authentication protocol for wireless LANs. IEE Proceedings Communications, 2006, 153(6): 810-817

[12] Tseng Y-M. USIM-based EAP-TLS authentication protocol for wireless local area networks. Computer Standards & Interfaces, 2009, 31(1): 128-136

[13] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols//Proceedings of the 30th ACM Symposium on Theory of Computing, Dallas, 1998: 419-428

[14] Canetti R, Krawczyk H. Analysis of key exchange protocols and their use for building secure channels//Proceedings of the Eurocrypt. Springer-Verlag, 2001: 453-474

[15] Arbaugh W, Shankar N, Wan Y, Zhang K. Your 802.11 wireless network has no clothes. IEEE Wireless Communications, 2002, 9(6): 44-51

[16] Kambourakis G, Rouskas A, Kormentzas G, Gritzalis S. Advanced SSL/TLS-based authentication for secure WLAN-3G interworking. IEE Proceedings Communications, 2004, 151(5): 501-506

[17] Hou Hui-Fang, Liu Guang-Qiang, Ji Xin-Sheng, Zhang Qiu-Wen. Provably security authentication scheme based on public key for heterogeneous wireless network. Journal of Electronics & Information Technology, 2009, 31(10): 2385-2391(in Chinese)
(侯惠芳，刘光强，季新生，张秋闻. 基于公钥的可证明安全的异构无线网络认证方案. 电子与信息学报，2009，31(10)：2385-2391)

[18] Prasithsangaree P, Krishnamurthy P. A new authentication mechanism for loosely coupled 3G-WLAN integrated networks//Proceedings of the 59th IEEE Vehicular Technology Conference(VTC 2004-Spring). 2004: 2998-3003

[19] Li Ya-Hui, Li Feng-Hua, Yang Wei-Dong, Ma Jian-Feng. Provably secure authentication protocols for heterogeneous wireless networks. Journal on Communications, 2007, 28(11): 21-29(in Chinese)
(李亚晖，李凤华，杨卫东，马建峰. 可证明安全的异构无线网络认证协议. 通信学报，2007，28(11)：21-29)

[20] Lin P, Lin Y-B, Feng V, Lai Y-C. GPRS-based WLAN authentication and auto-configuration. Computer Communications, 2004, 27(8): 739-742

[21] Lee J-S, Lin P-Y, Chang C-C. Lightweight secure roaming mechanism between GPRS/UMTS and wireless LANs. Wireless Personal Communications, 2009, 53(4): 569-580

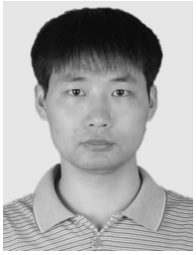
[22] Tang Q. On the security of three versions of WAI protocol in Chinese WLAN implementation plan//Proceedings of the Communications and Networking in China. IEEE Press, 2007: 333-339

[23] Long M, Wu C-H, Irwin J D. Localized authentication for inter-networking roaming across wireless LANs. IEE Proceedings Communications, 2004, 151(5): 496-500

[24] Yang G, Wong D S, Deng X. Formal security definition and efficient construction for roaming with a privacy-preserving extension. Journal of Universal Computer Science, 2008, 14(3): 441-462

[25] Peng Hua-Xi. An identity-based authentication model for multi-domain. Chinese Journal of Computers, 2006, 29(8): 1271-1281(in Chinese)
(彭华熹. 一种基于身份的多信任域认证模型. 计算机学报，2006，29(8)：1271-1281)

[26] Tin Y S T, Boyd C, Nieto J G. Provably secure key exchange: An engineering approach//Proceedings of the Australasian Information Security Workshop(AISW2003). Australasian, 2003: 97-104



JIANG Qi, born in 1983, Ph. D. candidate. His research interests include security protocols and wireless network security.

MA Jian-Feng, born in 1963, Ph. D., professor, Ph. D. supervisor. His research interests include information security and cryptography.

LI Guang-Song, born in 1977, Ph. D., lecturer. His research interests include wireless network security and cryptographic algorithms.

MA Zhuo, born in 1980, Ph. D., lecturer. His research interests include trusted computing and network security.

Background

This research is supported by the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z429, National Natural Science Foundation of China under grant Nos. 60633020, 60702059, 60872041.

The integration of heterogeneous wireless network is an inevitable trend. 3G and WLAN, two important technologies for providing wireless access services, possess complementary properties in terms of coverage and data rate. Therefore, the integration of 3G and WLAN is the most promising one and the focus of both industry and academia.

Security is one of the major challenges which heterogeneous wireless network integration faces. 3G and WLAN face distinct security challenges, each has addressed security in different ways. UMTS achieves network access security using the Authentication and Key Agreement (AKA) protocol, while WLAN has two different security architectures, i. e., IEEE 802. 11i and WAPI. How to integrate the vastly different security architectures used in each access network and unify user management is to be solved in urgent need.

3GPP TS 33. 234 has defined the security architecture of 3GPP I-WLAN, which adopts the AAA and EAP technologies as the two glue components of the interworking solution. The EAP AKA allows the UMTS AKA to be performed between the WLAN terminals and 3GPP system. Tseng has proposed two USIM based certificate distribution mechanism to achieve unified user management for 3G and WLAN. However, the existing schemes are for the security integration of 3G and IEEE 802. 11i based WLAN, the security integration of 3G and WAPI based WLAN remains to be solved.

To achieve the security integration of 3G and WAPI based WLAN, this paper proposes a USIM based certificate distribution protocol. Two security integration schemes, i. e., loosely coupled and tightly coupled, are presented, which unify user management of 3G security architecture and WAPI, and realize WAPI based network access for 3G subscribers and identity privacy protection. The entity authentication and anonymity of the certificate distribution protocol is analyzed in CK model, and the results show that the protocol is provably secure.