一种改进的 WLAN-3G 融合网络认证协议

刘 云[1],范科峰[2],张素兵[3],莫 玮[1],沈玉龙[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,陕西西安 710071;
2;北京邮电大学网络与交换国家重点实验室信息安全中心,北京 100876;3. 中国电子技术标准化研究所,北京 100007)

摘 要: 本文在分析了现有 3GPP WLAN-3G 融合网络接入认证协议 EAP-AKA 的优势和不足的基础上,引入 WAPI 证书鉴别机制,提出 WAPI-3G 互联结构模型,并针对该互联模型设计了一种接入认证协议 EAP-WAPI.本文提议的 WLAN-3G 互联结构模型及接入认证机制解决了融合组网环境下 WLAN 终端统一接入认证的问题.分析和仿真结果表明,相比于原有的 WAPI 认证协议 WAPI-XG1,本文所提议的协议具有较高的安全性和执行效率.

关键词: 无线通信; 无线局域网(WLAN); 第三代移动通信系统(3G); 融合网络;
可扩展认证协议(EAP); 无线局域网鉴别和保密基础结构(WAPI); 接入认证
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2010) 02-0399-06

Improved Authentication Protocol for WLAN-3G Interworking Networks

LIU Yun[1], FAN Ke-feng[2], ZHANG Su-bing[3], MO Wei[1], SHEN Yu-long[1]
(1. *Key Lab of CNIS, MOE, Xidian University, Xi'an, Shaanxi* 710071, *China*; 2. *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*; 3. *China Electronics Standardization Institute, Beijing* 100007, *China*)

Abstract: Based on analyzes the available WLAN-3G interworking protocol EAP-AKA proposed by 3GPP, introducing the certificate authentication mechanism, an improved architecture and a novel authentication protocol EAP-WAPI are proposed in order to achieve authentication for the users using WLAN access network, which solves the problem of integrated access authentication. The analysis and simulation results show that compared to the formal WAPI authentication protocol WAPI-XG1, the protocol EAP-WAPI improves the process of authentication interaction and the implementation efficiency.

Key words: wireless communication; wireless local area Networks(WLAN); 3rd-generation(3G); integrated Networks; extensible authentication protocol(EAP); authentication and key agreement(AKA); access authentication

1 引言

随着全球通信业的发展和普及,3G 无线网络已逐渐成为移动通信市场的新技术主流,其特点是网络覆盖范围广,能够提供语音,数据和多媒体等业务,具有很强的漫游功能,安全性较高,但是传输速率较低.无线局域网(WLAN)作为局部热点范围内的应用网络,特点是能够为用户提供较高的传输速率和方便的接入服务,因此,将 WLAN 网络和 3G 网络进行互连,会使两种技术的优势得到充分的发挥,起到优势互补的作用.第三代合作伙伴计划(3GPP)组织针对 3G 与 WLAN 网络融合提出了一套互联方案[1]和三种互联结构[2],描述了互联需求[3],并为互联的安全接入设计了可扩展认证和密钥协商协议(EAP-AKA)[4].由于 EAP-AKA 协议存在以下漏洞和不足:认证流程需要多次请求和相应交互,使得认证时延较大,当 UE(user equipment)连续在不同无线局域网中切换时,这些延迟会成为瓶颈;不支持加密套件协商和认证协议版本的协商;加密密钥和加解密算法固定等,使得有必要设计一种新的 WLAN-3G 融合网络认证接入协议.基于此,引入 WAPI 证书鉴别机制,提出 WAPI-3G 互联结构模型作为现有模型的补充,并针对该互联模型设计了一种接入认证协议 EAP-WAPI.该协议利用更高安全性的证书鉴别机制,有效地解决了上述不足之处.

2 现有 WLAN-3G 融合网络接入认证协议 EAP-AKA 的分析

EAP-AKA 协议首先进行 WLAN UE 和 WLAN AN(access Network)之间的 WLAN 网络接入,主要在 WLAN 网络空中接口建立安全通道和开启链路层的通信端口;然后 WLAN AN 要求 WLAN UE 发送身份信息,并传输 WLAN UE 信息给移动用户的归属网,获取移动用户的

收稿日期:2009-07-03;修回日期:2009-12-02
基金项目:国家自然科学基金委员会—广东联合基金资助项目(No.U0835004);中国博士后科学基金(No.20080550333,No.200902073);国家自然科学区(No.60672112)

授权信息;归属网络的 HSS(home subscriber server)/HLR(heme location register)生成关于移动用户的认证向量,并发送给 3G AAA(authentication authorization and accounting)服务器,用于完成对移动用户的接入认证、授权和计费;3G AAA 服务器发送身份认证的质询消息,并由 WLAN AN 转发给 WLAN UE;WLAN UE 利用 USIM(universal mobile telecommunication system)卡中的密码密法验证收到的质询信息的正确性,并计算会话密钥材料和身份响应消息,然后发送响应消息组 WLAN AN;3G AAA 服务器收到由 WLAN AN 转发的身份响应消息后,验证消息的正确性,然后发送认证成功消息和会话密钥材料给 WLAN AN,完成 WLAN UE 的接入认证.

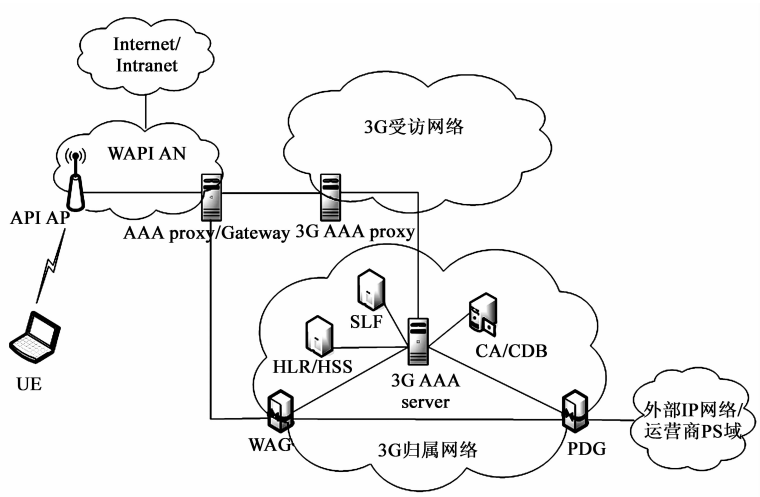


图1 WAPI-3G互联体系结构模型

经过大量的实践和研究,EAP-AKA 认证存在以下一些漏洞和不足:

(1)认证流程需要多次请求和响应交互,造成认证时延较大.

(2)由于不同的运营商可能拥有不同无线接入设备,这就要求额外的信任管理功能.

(3)网络侧不需要认证,接入点始终被信任.

(4)在一些情况下,系统允许通过使用在明文中传输 IMSI 来认证用户,存在安全漏洞..

(5)EAP-AKA 不支持加密套件协商和认证协议版本的协商.

(6)EAP-AKA 基于对称加密体制,不支持非对称加密体制及基于证书鉴别的接入认证.

3 基于 WAPI 的 WLAN 和 3G 融合网络体系结构设计

3GPP WLAN-3G 互通规范主要针对采用 802.11i 安全机制的 WLAN 和 3G 互联.由于 3G 网络的安全性高于 802.11i WLAN,因此 WLAN-3G 融合网络安全体系以 3G 安全体系为模型,融合网络的接入认证借助于 UMTS AKA 协议.但是大量地研究和实践表明 EAP-AKA 存在一些不足之处,主要表现在无线链路易受攻击和对称密码体制的脆弱性.为此 3GPP 开展了采用具有更高安全性的证书鉴别机制完成接入认证的研究[5,6].

WAPI 的接入认证过程采用证书鉴别方式[7,8],无线链路上采用椭圆曲线 DH 协商保护通话内容,安全性远远高于 UMTS AKA,因此可考虑采用 WAPI 安全标准实现 WLAN-3G 融合网络用户的安全接入.

针对 WLAN-3G 融合组网证书鉴别接入认证机制,结合我国 WLAN 安全标准 WAPI,提出一种基于 WAPI 的 WLAN 与 3G 融合组网体系结构(即 WAPI-3G 互联结构模型),该结构的安全体系以 WAPI 安全体系为模型,采用 WAPI-WAI(WLAN authentication infrastructure)认证过程实现 WLAN 用户的安全接入认证.

图 1 给出了一种 WAPI-3G 融合组网互联体系结构模型.

WAPI 用户访问 WAPI 网络或 3G 核心域中的数据域(PS-packet switch)业务时都必须先经过 3G AAA 服务器的身份认证,即在 3G 核心网络统一完成认证功能.当用户设备接入 WAPI AN 时,需要在 3G 核心网中进行身份认证和获取访问权限.一旦接入认证通过,用户获得接入权限,WAPI 用户就可以获得以下两种数据访问方式:

(1)用户直接通过 WAPI AN 访问 Internet/Intranet,用户数据直接从 WAPI AN 路由到 Internet/Intranet;

(2)如果用户访问的是 3G 的 PS 域业务,经 3G AAA 服务器认证并授权后,WAPI 用户设备和 PDG(packet data gateway)之间先建立端到端的数据隧道,用户数据通过 WAPI AN,再经由核心网内的 WAG(WLAN access gateway)和 PDG 网关路由到外部 IP 网络,获得 3G 提供的 PS 域业务.

4 基于 WAPI 的 WLAN-3G 融合网络认证协议 EAP-WAPI

针对 WLAN-3G 融合组网证书鉴别接入认证机制,结合我国 WLAN 安全标准 WAPI,提出一种基于 WAPI 的 WLAN 与 3G 融合网络认证协议 EAP-WAPI.

4.1 设计思想

EAP-WAPI 提供了一种使用 EAP 协议封装 WAPI 客户端与 3G AAA 服务器间认证消息交互的过程,具体封装了 WAI 中的两个阶段:

(1)证书鉴别过程:从 AP(access point)向 UE 发出认证激活请求开始,直至 AP 和 UE 接收到 AS(authentica-

tion server)的证书鉴别结果并决定是否打开受控端口为止.

(2)单播密钥协商:UE 与 AP 完成单播密钥协商,产生协商会话密钥.会话密钥将用于加密后面的通信数据,如 UE 和 AP 间组播密钥通告/响应以及业务数据传输.

EAP-WAPI 思想既保留了 WAPI 安全协议中接入认证协议 WAI 机制不变,同时又保证了 UE 通过 WAPI AN 安全的接入 3G 网络.

4.2　认证流程设计

WAI 证书鉴别采用的是双向认证机制:认证请求者 STA(station)通过认证者 AP 向认证服务器 AS 进行认证时,AP 决定访问网络,并在认证请求者和认证服务器之间完成 EAP 路径的桥接,使两者能够进行交互;AS 对 STA 和 AP 的身份进行认证,并将认证结果传递给 AP,AP 根据 AS 的认证结果决定是否允许该 STA 接入,然后将认证结果转交给 STA,STA 根据 AS 的认证结果决定是否接入该 AP.

一次成功的 EAP-WAPI 接入认证流程如图 2 所示.

以下是 EAP-WAPI 协议的认证流程:

STA、AP 安全关联及 EAP 认证启动阶段:

(1)STA 与 AP 建立安全关联后,STA 向 AP 发送 EAP 开始消息 EAPOL-Start,启动 EAP 认证.

(2)AP 向 STA 发送“EAP 请求/Identity”,请求用户身份.

(3)STA 向 AP 发送“EAP 响应/Identity”,AP 收到后转发给 AAA Server.

(4)AAA Server 根据 HLR/HSS 中的注册信息检查用户身份的合法性.检查通过后,AAA Server 发送“EAP 请求/WAPI-身份证书”,请求 STA 与 AP 的证书.证书鉴别及单播会话密钥协商阶段:

(5)AP 接收到“EAP 请求/WAPI-身份证书”后,向

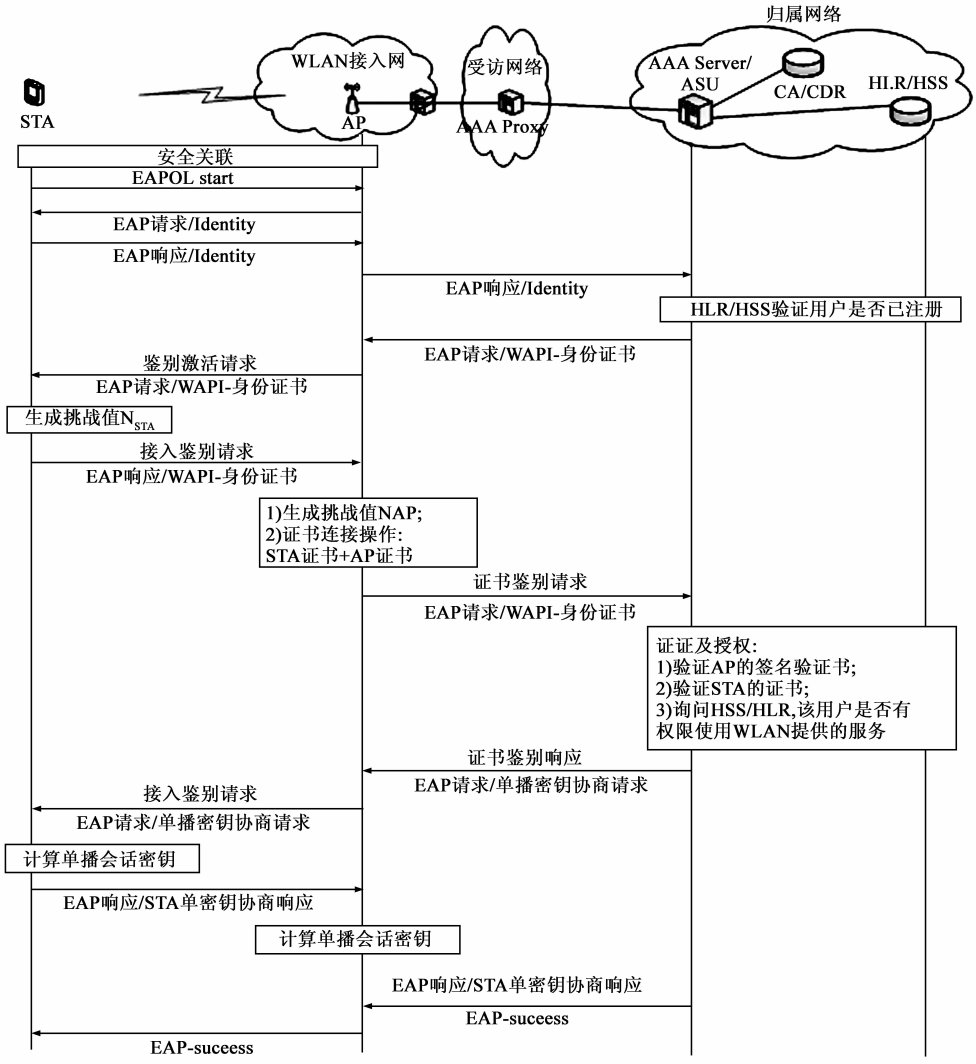


图2　EAP-WAPI认证流程

STA 发送“EAP 请求/WAPI-身份证书”(即鉴别激活分组),请求 STA 的身份证书.该消息封装了 WAI 中的鉴别激活分组消息,消息内容主要包括 AP 的证书 CertAP,AP 信任的认证服务器的身份,采用椭圆曲线非对称加密算法进行 D-H(Diffie-Hellman)协商的 ECDH(the elliptic curve Diffie-Hellman)参数.

(6)STA 接收到由 AP 发送的“EAP 请求/WAPI-身份证书”(即鉴别激活分组)后,根据鉴别激活发组中 AP 信任的 AAA Server 身份,选择由该 AAA Server 颁发的证书;产生用于 ECDH 交换的临时私钥 x、临时公钥 $x\cdot P$ 和 STA 的质询 NSTA;生成“EAP 响应/WAPI-身份证书”(即接入鉴别请求分组),消息内容主要包括(NSTA,x,CertSTA)和对消息的签名 SigSTA.

(7)AP 收到 STA 发来的“EAP 响应/WAPI-身份证书”(即接入鉴别请求分组)后,验证消息中 STA 的签名 SigSTA 和 STA 身份证书 CertSTA;若验证成功,本地生成 AP 的挑战 NAP;构造“EAP 响应/WAPI-身份证书”(即证书鉴别请求分组),消息主要内容包括(ADDID,NAP,NSTA,Cert AP, Cert STA).其中,ADDID 为 STA 和 AP 的 MAC 地址.

(8)AAA Server 收到 AP 发来的“EAP 响应/WAPI-身份证书”(即证书鉴别请求分组)后,验证 AP 证书 Cert AP 和 STA 证书 Cert STA;如果验证成功,询问 HSS/HLR,该用户是否有权限使用 WAPI 无线局域网提供的服务.如果有权限,则 HSS/HLR 根据 AP 和 STA 的证书的验证结果,构造“EAP 请求/单播密钥协商请求”(即证书鉴别响应分组),消息内容主要包括证书验证结果 Res 和 AAA Server 的签名 SigAS.注意该消息功能上包括两部分:证书鉴别响应和单播密钥协商请求.

(9)AP 收到 AAA Server 发来的“EAP 请求/单播密钥协商请求”(即证书鉴别响应分组)后,检查消息中的 NAP 与自己在证书鉴别请求分组中的 NAP 是否相同,若相同,继续执行操作;否则丢弃该证书鉴别响应分组;本地再次生成用于 ECDH 交换的临时私钥 y 和临时公钥 $y\cdot P$;使用自己的临时私钥 y 和 STA 的临时公钥 $x\cdot P$ 进行 ECDH 计算,得到密钥种子$(x\cdot y\cdot P)$abscissa,并对其进行扩展 KD-HMAC-SHA256$(x\cdot y\cdot P)_{abscissa}$, $N_{AP}\parallel N_{STA}\parallel$"key expansion"生成长度为 16 个八位位组的基密钥 BK 和用于下一次证书鉴别过程的鉴别标识种子,并对该鉴别标识种子进行 SHA-256 运算,得到下一次证书鉴别过程的鉴别标识;重新构造“EAP 请求/单播密钥协商请求”(即接入鉴别响应分组),消息内容主要包括(基密钥标识 BKID,STA 和 AP 的 MAC 地址 ADDID,NAP,NSTA,AP 临时公钥 $y\cdot P$,STA 临时公钥 $x\cdot P$,证书验证结果 Res).该消息功能上包括两部分:接入鉴别响应和单播密钥协商请求.

(10)STA 收到“EAP 请求/单播密钥协商请求”(即接入鉴别响应分组)后,检查消息中的 NSTA 与自己在证书鉴别请求分组中的 NSTA 是否相同,若相同,继续执行操作;否则丢弃该接入鉴别响应分组;在接入鉴别响应分组中查找接入认证结果 Res;若允许 STA 接入,STA 使用自己的临时私钥 x 和 AP 的临时公钥 $y\cdot P$ 进行 ECDH 计算,得到密钥种子$(x\cdot y\cdot P)$abscissa,并对其进行扩展 KD-HMAC-SHA256$(x\cdot y\cdot P)_{abscissa}$, $N_{AP}\parallel N_{STA}\parallel$"key expansion"生成长度为 16 个八位位组的基密钥 BK 和用于下一次证书鉴别过程的鉴别标识种子,并对该鉴别标识种子进行 SHA-256 运算,得到下一次证书鉴别过程的鉴别标识.计算单播会话密钥:KD-HMAC-SHA256(BK, $ADDID\parallel N_{AP}\parallel N_{STA}\parallel$"key expansion")生成 96 个八位位组,前 64 个八位位组为单播会话主密钥 UMK(第一个 16 个八位位组为单播数据的加密密钥 UEK,第二个 16 个八位位组为单播完整性校验密钥 UCK,第三个 16 个八位位组为 WAI 协议消息鉴别密钥 MAK,第四个 16 个八位位组为组播密钥的加密密钥 KEK).利用 MAK 计算消息鉴别码 MIC_{STA} = KD-HMAC-SHA256(MAK, $BKID\parallel ADDID\parallel N_{AP}\parallel N_{STA}\parallel$).构造“EAP 响应/STA 单播密钥协商响应”,消息主要内容包括(NSTA,NAP,MICSTA).

(11)AP 收到“EAP 响应/STA 单播密钥协商响应”,检查收到的 NAP 与本地存储的 NAP 是否相同,如果相同,继续下面处理;否则丢弃.计算单播会话密钥:KD-HMAC-SHA256(BK, $ADDID\parallel N_{AP}\parallel N_{STA}\parallel$"key expansion")生成 96 个八位位组,前 64 个八位位组为单播会话主密钥 UMK(第一个 16 个八位位组为单播数据的加密密钥 UEK,第二个 16 个八位位组为单播完整性校验密钥 UCK,第三个 16 个八位位组为 WAI 协议消息鉴别密钥 MAK,第四个 16 个八位位组为组播密钥的加密密钥 KEK).利用 MAK 计算消息鉴别码 MIC_{AP} = KD-HMAC-SHA256(MAK, $BKID\parallel ADDID\parallel N_{AP}\parallel N_{STA}$).构造“EAP 响应/AP 单播密钥协商响应”,消息主要内容包括(NSTA,NAP,MICSTA).

EAP 认证结束:

(12)AAA Server 收到“EAP 响应/AP 单播密钥协商响应”后,向 AP 发送 EAP-Success 消息.

(13)AP 收到 EAP-Success 消息后,转发给 STA.至此,接入认证过程结束.

5 EAP-WAPI 协议的分析

5.1 安全性分析

EAP-WAPI 是一个 WAPI UE、AP 和 AS 三方联合认证的过程,它的安全性主要体现如下:

(1)EAP-WAPI 在功能上由 EAP 的“请求/响应”与 DH密钥交换协议复合而成,其中 EAP 协议封装了 WAPI 双向身份认证机制,DH 协议实现了 WAPI 证书鉴别协议的基密钥 BK 协商;

(2)EAP-WAPI 证书鉴别属于强认证类型.

(3)用户终端 UE 和接入点 AP 之间的双向认证机制有效防止了中间人攻击;

(4)接入网空中接口数据机密性保护采用椭圆曲线加密算法.UE 与 AP 之间的通过基于椭圆曲线非对称加密算法的 D-H 协商(ECDH)来保护通话内容基密钥 BK.即使线路被窃听,窃听者也无法计算出 D-H 协商密钥,也就无法破译通话的内容.

(5)终端设备 UE、接入点 AP 和后台认证服务器 AS 之间的消息通过 MAC-SHA 算法完成数据完整性保护;消息来源可靠性由数字签名来实现.

与 EAP-AKA 协议相比,EAP-WAPI 具有如表 1 所示安全特点:

表 1　EAP-AKA 与 EAP-WAPI 的安全性比较

安全特性	EAP-AKA	EAP-WAPI
认证机制	单向认证	双向认证
IMSI 安全性	易截获攻击	加密传输不易被截获和攻击
加密密钥及算法	固定	可协商(安全性和灵活性高)
支持加密体制	仅对称加密	支持非对称加密方式

同原 WAPI 认证协议 WAPI-XG1 相比,在一次成功地 WAI 证书鉴别和单播密钥协商过程中,用户终端设备需完成两次签名和三次验签工作,AP 需要完成三次签名和四次验签工作,带来相当大的运算开销.

为了提高效率,我们通过减少认证交互轮数和非对称密码算法签名/验签次数来提高协议的执行效率.EAP-WAPI 在设计上减少了一轮 STA、AP 和 AS 的接入认证交互次数,将“AS(AP:证书鉴别响应”和“AS→AP:单播密钥协商请求”合为一条消息,相应地将“AP→STA:接入鉴别响应”和“AP→STA:单播密钥协商请求”也合为一条消息.与 WAPI-XG1 协议相比较,用户终端 STA 和接入点 AP 各减少了一次签名和验签过程.

5.2　仿真性能分析

为进一步分析采用 EAP 封装 WAI 并改进了 WAI 认证交互过程后的 EAP-WAPI 的效能,我们在 OPNET 的环境下对 EAP-WAPI 进行了仿真.

仿真场景为一个 7000m × 7000m 的开阔环境,如图 3,共有 7 个移动终端 STA,2 个 AP 通过 Internet 连接到后台认证服务器 AS 上,AP 与服务器 AS 之间为有线连接,STA1 进行延时统计并分析统计量 delay.

测试中使用两个子场景(scenarios),网络拓扑结构完全一样,只是配置不同,以便对测试结果进行对比.

子场景 1:场景中网络节点采用国标 WAPI-XG1 安全协议完成 STA 的接入认证和单播会话密钥协商;

子场景 2:场景中网络节点采用自主设计的 EAP-WAPI 接入认证协议完成 STA 的接入认证和单播会话密钥协商.

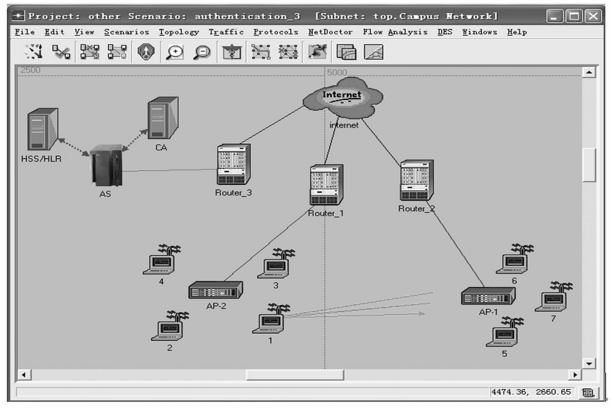


图3　EAP-WAPI仿真测试场景

测试场景中无线网络节点参数设置为:所有无线节点采用 802.11g,数据传输速率为 1Mbps,传输功率为 0.005W,无线信道 MAC 层 CSMA/CD 协议采用二进制指数退避算法.预设网络节点计算耗时如表表 1 所示.

表 2　网络节点计算耗时表

	STA	AP	AS
签名/验签	0.5s	0.5s	0.01s
计算 BK	2.0s	1.0s	—
计算单播会话密钥	2.0s	1.0s	—
证书鉴别	1.5s	1.0s	0.3s

仿真时间为 5 分钟,两个子场景下 STA1 ~ STA7 重复执行接入认证过程.仿真后收集到两个子场景下 STA1 每次的认证时延,对比结果如图 4 所示.

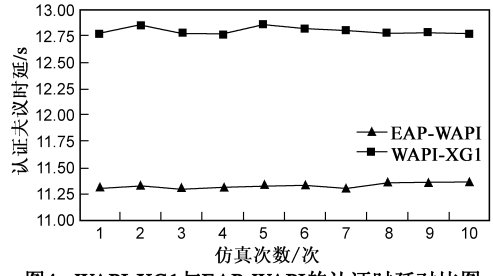


图4　WAPI-XG1与EAP-WAPI的认证时延对比图

认证时延对比图 4 中横坐标为认证次数,纵坐标为认证协议的执行时间,上半部分为子场景 1(执行 WAPI-XG1 协议)的延时范围,下半部分为子场景 2(执行 EAP-WAPI 协议)的延时范围.

从图中可以看出,在认证次数为 10 次的情况下:子场景 1 下 STA1 的认证延时范围集中在[12.75,13.00],平均认证时延为 12.81s;子场景 2 下 STA1 的认证延时范围集中在[11.20,11.35],平均认证时延为 11.28s.

仿真结果表明,子场景 2 下 STA 认证时延降低了

11.84%.

对于当前的无线网络,影响协议性能的最主要因素是消息传输延时,EAP-WAPI 虽然增加了一些 EAP 封装带来的传输负担,但是由于 EAP-WAPI 改进了 WAPI-XG1 认证交互过程,减少了一轮认证交互,STA、AP 各自减少一次签名/验签和一次抢占无线信道耗时,因此协议执行效率显著提高.

6 结束语

针对 3GPP 提出的 WLAN-3G 互联结构模型中的认证协议 EAP-AKA,提出了一种适合 WAPI-3G 互联的网络体系结构.为解决 WAPI 用户安全接入认证问题,本文设计了一种新的接入认证协议 EAP-WAPI,利用 EAP 封装 WAPI 中的证书鉴别和单播密钥协商过程,实现用户终端与后台认证服务器的认证交互.为提高用户接入效率,EAP-WAPI 改进了原 WAPI-XG1 标准,减少了交互轮数,缩短了证书鉴别和单播密钥协商的时间.本文最后在 OPNET 环境下对 EAP-WAPI 进行了性能仿真.仿真结果表明,EAP-WAPI 协议的执行效率优于 WAPI-XG1.本文所提出的 EAP-WAPI 协议改进了 WLAN-3G 互联网络安全接入协议,具有一定的应用价值.

参考文献:

[1] TR 22.934 V6.2.0,3GPP. Technical Specification GroupServices and System Aspects;Feasibility study on 3GPP system to Wireless Local AreaNetwork(WLAN) interworking (Release 6)[S].

[2] TS 23.234 V7.2.0, 3GPP.3GPP system to Wireless Local Area Network(WLAN) interworking;System Description (Release 7)[S].

[3] TS 22.234 V7.4.0. September 2006,3GPP. Technical Specification GroupServices and System Aspects; Requirements on 3GPP system to Wireless Local Area Network(WLAN) interworking (Release 7)[S].

[4] TS 33.234 V7.5.0. June 2007, 3GPP. Universal Mobile Telecommunications System (UMTS);3G security; Wireless Local Area Network (WLAN) interworking security (Release 7)[S].

[5] TS 33.102 V7.4.0,3GPP. Technical Specification GroupServices and System Aspects; 3G. Security Architecture(Release 7)[S].

[6] TS 24.109 V6.9.0,3GPP. Technical Specification Group Core Network and Terminals; Bootstapping interface(Ub) and network application function interface(Ua)(Release 6)[S].

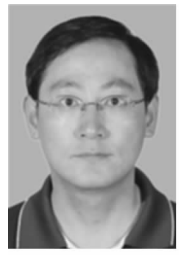
[7] 李兴华,马建峰.WAPI 实施方案中的密钥协商协议的安全性分析[J].计算机学报,2006,29 (04):576 - 580.
Li Xin-hua,Ma Jian-feng. On the security of the key-agreement protocol of chinese WLAN standard implementation plan[J]. Chinese Journal of Computers,2006,29 (04):576 - 580.(in Chinese)

[8] 张帆,马建峰.WAPI 认证机制的性能和安全性分析[J].西安电子科技大学学报,2005,32(02):210 - 216.
Zhang Fan,Ma Jian-feng. On the security and performance of WAPI[J]. Journal of Xidian University,2005,32(02):210 - 216.(in Chinese)

作者简介:

刘 云 男,1981 年出生于重庆市忠县,2003 本科和 2006 硕士毕业于电子科技大学通信学院,2006 年就读西安电子科技大学博士.主要研究方向:无线网络及信息安全.
E-mail:cloud_ly@163.com

范科峰 男,1978 年出生于陕西礼泉,博士后,中国电子学会高级会员,IEC TC100 DRM 及 JTC1 DCMP 专家.主要研究方向:内容保护;无线网络.
E-mail:fankf@cesi.ac.cn



张素兵 男,1973 年出生于山西阳泉,博士后.中国电子学会高级会员.主要研究方向:无线网络.

莫 玮 男,1956 年出生于广西南宁,教授,博士生导师,IEEE 高级会员.目前的研究方向:智能信息处理与测试技术等.

沈玉龙 男,1978 年出生于江苏泗洪,西安电子科技大学,讲师,博士,ACM 会员,IEEE 会员,电子学会会员.主要研究:无线网络安全技术.