北京邮电大学

硕士学位论文

WLAN安全解决方案设计与实现

姓名：李煜

申请学位级别：硕士

专业：计算机科学与技术

指导教师：漆涛

20070420

WLAN 安全解决方案设计与实现

摘 要

无线局域网(WLAN)是计算机网络与无线通信技术相结合的产物，由于无线网络所特有的开放性，其安全问题一直是业界研究的重点。本论文对 WLAN 安全协议进行了深入的研究，提出了无线接入点(AP) 中安全认证模块的具体实现，并且对实现过程中的一些关键问题提出了切实有效的解决方案。最后对 WAPI 协议提出了一点改进意见。

本论文主要分为五个部分。

第一部分概述了 WLAN 网络的应用现状以及本论文的项目背景。

第二部分介绍了 WLAN 的基本概念、标准演进及 WLAN 网络中存在的安全风险。并介绍了 WLAN 网络在大型运动会中应用的历史以及为了使 WLAN 网络能顺利服务于大型运动会，所采取主要安全措施。

第三部分深入分析了现有 WLAN 安全协议的原理和机制。包括对 WEP 安全缺陷的研究以及 IEEE 802.11i 协议的原理和 WAPI 的安全机制分析。

第四部分详细讨论了 AP 中安全认证模块的总体设计，并实现了 IEEE 802.11i 和 WAPI 协议。最后，结合当前应用的实际情况，对 WAPI 提出了一点改进意见，使其更好的应用于运营级网络。

第五部分对本论文进行了概要的总结。

关键词

WLAN，AP，IEEE 802.1X，IEEE 802.11i，WEP，WAPI

WLAN SECURITY SOLUTION DESIGN AND IMPLEMENTATION

ABSTRACT

WLAN is a combination of computer networks and wireless communications technology. As unique to the open wireless network, the security problem has been the focus of the industry. This thesis lucubrate WLAN security protocol and realize the Security Authentication Module in AP(access point),then put forward an improved solution for application of WAPI in operation-level network.

This thesis is divided into five sections.

The first part outlines the WLAN network and the project background of this thesis.

The second part introduces the basic concepts, standards for the WLAN and WLAN network security risks .

The third part analyzes the existing WLAN security protocols in detail, including WEP, IEEE 802.11i and WAPI security mechanism.

The fourth part discusses security authentication module design in AP, and realize the IEEE 802.11i and WAPI protocol. First,designs the overall structure of the system. Second,defines the interface between modules.Then design the program flow of the module. Finally, gives an improved solution of WAPI in operation-level network.

The fifth part is a brief summary.

KEY WORDS

WLAN, AP, IEEE 802.1X, IEEE 802.11i, WEP, WAPI

图目录

表目录

独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：李煜 日期：07.4.27

关于论文使用授权的说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密在 年解密后适用本授权书。非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：李煜 日期：07.4.27

导师签名：李伟 日期：07.4.27

第一章 绪论

1.1 研究背景

在互联网领域，一直都是有线线缆和光纤的天下。无线技术的出现，为用户提供了一种崭新的互联网接入方式，使我们摆脱了网线的束缚，而且由于采用无线接入方式，使无线局域网不仅建网成本要低于传统有线局域网，还更加灵活，可以根据需要快速建网。同时，无线局域网把局域网的高数据传输速率与移动通信系统的移动功能有机地融为一体，使我们距离随时随地与任何人进行任何内容通信的人类通信终极梦想又进了一步。

基于上述优点，目前无线局域网在全球的发展势头非常好。应用范围已经非常广泛。按照其应用的空间范围来划分可分为室内应用和室外应用。室内应用包括大型办公室、车间、智能仓库、临时办公室、会议室、证券市场、会展中心、酒店、飞机场、医院、酒吧、咖啡屋、体育场馆等；室外应用包括城市建筑群间通信、学校校园网络、工矿企业厂区自动化控制与管理网络、银行金融证券城区网、税务、矿山、水利、油田、港口、码头、江河湖坝区、野外勘测实验、军事流动网、公安流动网等。按照其应用的行业来划分可大致分为大众应用市场、医疗行业、教育行业、金融服务行业等等。

无线局域网在大型运动会中的应用是一个崭新的课题。首先在 2002 年韩日世界杯上无线局域网有了一定规模的应用；而在国内的大型运动会上无线局域网的应用则始于 2001 年世界大学生运动会和第九届全运会。但以上无线局域网的应用都仅限于为数不多的比赛场馆或新闻中心等场所，在广东省第十一届运动会中无线局域网得到了前所未有的广泛应用。作为传统布线网络的一种替代方案或延伸，无线网络为移动用户和布线困难的场所提供了方便的网络接入，非常适合于体育场馆。

同时，无线技术最大的优点“随处可收”，也给网络安全带来了巨大的挑战。而无线局域网的最初标准 IEEE 802.11 并没有很好的解决这一由无线技术自身的特点所带来的安全问题。随着无线局域网的大范围应用，其在安全方面的弊端开始逐步暴露出来：在日本，西屋百货公司基于无线局域网的移动 POS 机因为泄漏消费者隐私而被曝光；在韩国，许多准备部署无线局域网的公司发现一些公司员工已经私自安装了无线局域网接入点设备，使得公司针对有线互联网设计的安全方案形同虚设；在英国，年轻的黑客驾车沿街扫描(war driving)周围建筑物中的无线局域网信号，随手截取保密信息,无线局域网黑客文化已经略具雏形；在美国，负责研究核武器以及其他国家防御技术的 Lawrence Livermore 国家实验室

关闭了已有的两个无线计算机网络并宣布禁止使用无线局域网，原因在于这些设备的系统中存在的安全隐患容易遭受到黑客的攻击而丢失机密信息。而雅典正是因为无线局域网的安全问题，使 Wi-Fi 网络无缘 04 年奥运会...

由此，我们看到安全问题已经成为无线局域网发展的一个瓶颈。为了更好的保护无线局域网的网络安全，促进产业发展，产业链上各大厂商以及 IEEE 和其他相关组织，都在积极寻求解决方案，先后提出了 WPA、WPA2(IEEE 802.11i)等安全标准。我国为了保护国家信息安全，也提出了自己的无线局域网安全标准 WAPI，目标都是解决 IEEE 802.11 中 WEP 安全机制的安全隐患。

1.2 文中涉及的主要概念说明

WLAN(Wireless LAN ，“无线局域网”)、Wi-Fi 和 IEEE 802.11 的区别与联系：

WLAN 只是个一般性术语，用以指短距离、高速的无线网络。Wi-Fi 是 WLAN 的一种，同时也是目前应用得最多最有影响力的 WLAN。

IEEE 802.11 是个正式的 WLAN 技术标准，由它来定义 Wi-Fi 系统如何工作。

Wi-Fi 是由 Wi-Fi 联盟定义的针对产品的基于 IEEE 802.11 的行业标准，所有厂家的 Wi-Fi 产品都经过了互操作性认证[8]。

一般来讲，IEEE 802.11 和 Wi-Fi 其实是一回事。在本文中 WLAN 指的是采用 IEEE 802.11 标准的无线局域网。

1.3 本人所做的工作及论文主要内容

在研究生期间，主要从事了大量网络安全协议开发和应用方面的工作，包括防火墙中 NP 微码的开发和无线局域网接入点(AP)中安全认证协议的设计和开发工作，对网络安全有了一定程度的研究。并在平时的工作和学习中对 TCP/IP 协议族有了深入的了解。并从事了大量的 WLAN 安全方面的开发

本论文主要以 WLAN 安全项目为背景，对 IEEE 802.11 无线局域网现存的安全问题以及国内外现有的安全机制进行了探讨。论证了 WEP 存在着严重的安全漏洞，进而引入 IEEE 802.11i 和我国的无线局域网安全国家标准 WAPI，并在“WLAN 安全项目”中实现了这两个标准，同时对 WAPI 在实际运营中的应用给出了指导性建议。主要涉及的协议包括 IEEE 802.11、IEEE 802.11i、IEEE 802.1X、RADIUS、WAPI。

全文由五章组成，第二章对无线局域网进行了概要介绍，包括无线局域网的概念，传输方式，网络拓扑结构，以及无线局域网的标准演进和 WLAN 的安全风险。

第三章对现有的安全机制进行了深入分析，包括 802.11 中采用的安全协议

WEP 和 IEEE 最新的安全标准 802.11i 和我国的 WLAN 安全标准 WAPI。

第四章对 AP 中安全认证模块进行了实现，涉及的协议有 IEEE 802.11i、IEEE 802.1X、EAP 和 WAPI，并对 WAPI 提出了一点改进意见，使其能更好的在运营级网络中应用。

第五章对论文进行了总结。

1.4 本章小结

本章先简单介绍了文中所用的基本概念，比较介绍了 WLAN、Wi-Fi 和 IEEE 802.11 在概念上的区别与联系。然后介绍了 WLAN 目前的发展现状，以及目前所面临的安全问题和本论文的项目背景，最后介绍了本论文的章节安排。

第二章 WLAN概述及应用

2.1 WLAN基本概念及标准演进

2.1.1 WLAN基本概念

无线局域网(WLAN)是采用无线传输媒体的计算机局域通信网络。1971年夏威夷大学的学者创造了第一个基于数据包传输的无线网— ALOHANET 3，它实质上就是第一个WLAN。进入20世纪90年代，人们要求在任何时间、任何地点都能使用网络资源，而传统的有线网络很难实现可移动的通信。因此，在这种趋势和要求的推动下，导致了WLAN的发展与进步。IEEE 802.11[2]系列标准是WLAN的主要标准[1]。

2.1.2 WLAN标准演进

(1) IEEE 802.11

1997年IEEE 802标准化委员会IEEE 802.11WLAN标准工作组公布了IEEE 802.11标准，它是第一代无线局域网标准，该标准定义了物理层和媒体访问控制层规范。802.11工作在2.4GHz上，理论传输速率分为1Mbps和2Mbps

(2) IEEE 802.11b

为了更高的数据传输速率，IEEE于1999年9月批准了IEEE 802.11b标准。IEEE 802.11b标准对IEEE 802.11标准进行了修改和补充，其中最重要的改进就是在IEEE 802.11的基础上增加了两种更高通信速率5.5Mbit/s和11 Mbit/s。11b也是工作在2.4GHz频段上，同时对最初的802.11标准保持了兼容。

(3) IEEE 802.11a

802.11a标准是已得到广泛应用的802.11b无线联网标准的后续标准，802.11a的物理层速率可达54Mbit/s，但11a的工作在5.5GHz上，不能兼容以前的标准。

(4) IEEE 802.11g

802.11g标准方案在确保兼容现有使用2.4GHz频带的IEEE 802.11b的同时，实现了54Mbps数据传送速度。既达到了用2.4GHz频带实现IEEE 802.11a水平的数据传送速度，也确保了与装机数量超过1100万台的IEEE 802.11b产品的兼容。

(4) IEEE 802.11 n(草案)

对IEEE 802.11的数据传输速率进行了大幅提高，使用802.11n超过100Mbps的速率不再是梦想，甚至有报道称可以达到320Mbps的最高速率。对

802.11 的数据传输速率进行了大幅提高，使用 802.11n 超过 100Mbps。

目前由于 11n 标准还没有正式出台，IEEE 802.11g 54Mbps 的无线局域网产品仍然是企业部署无线局域网络的主流选择。而增强型的 11g 标准的速度已可以达到 100Mbps，与有线局域网相当，这进一步促进了无线局域网应用的发展。

这些后演进的标准只是对最初的 IEEE 802.11 在物理层上进行了改进，使其有更高的数据传输速率，在 MAC 层上的是一致的，所以它们在安全认证方面采用的都是 802.11 中定义的 WEP 协议。

2.1.3 WLAN 网络建立过程

无线局域网的基本网络连接建立过程是在 IEEE 802.11 中定义的，无论是后续的 IEEE 802.11 系列标准还是 WAPI 都是建立在这个基本连接过程之上的。

在 IEEE 802.11 网络中主要有两个实体：AP 和 STA，AP 就是无线接入点，STA 是无线工作站，最常见的就是带有无线网卡的笔记本。其中 AP 是核心，一个 STA 要想加入到一个无线局域网，首先要与这个无线局域网中的 AP 建立连接，然后通过这个 AP 与其它的 STA 或网络进行通信。网络的基本模式如图 2-1 所示：

图 2-1 IEEE 802.11 网络基本组成

IEEE 802.11 定义了 AP 与 STA 之间从建立连接到发送数据所需要的三种帧类型，分别是：控制帧(类型值是 00)、管理帧(类型值是 01)、数据帧(类型值是 10)。控制帧用来告诉设备什么时候开始和停止发送消息；利用管理帧来建立连接；一旦 STA 和 AP 已经同意建立连接，数据就以数据帧的形式来发送。

重点来介绍一下管理帧，因为 WEP 的认证是通过管理帧来实现的。管理帧有 7 种：

信标帧(Beacon)：信标帧是由 AP 定时发送的广播帧，用来通知本无线局域网的存在和 AP 性能等有用信息；

探询请求/应答帧(Probe Request/Response)：STA 通过发送探询请求帧来寻找 AP，AP 利用探询应答帧来告诉 STA 网络的信息；

链路验证帧(Authentication Request/Response)：AP 和 STA 之间的 WEP 认证就是通过链路验证请求/应答帧来实现的；

关联请求/应答帧(Association Request/Response)：链路验证通过之后，AP和STA之间再建立关联关系，通过关联帧来协商一些网络参数指标；

重新关联请求/应答帧(Reassociation Request/Respons)：当漫游到其他AP时，需要重新建立关联；

解除关联帧(Deassociation)：当断开网络连接时需要解除关联；

解除认证帧(Deauthentication)：解除关联之后再去解除认证。

具体的网络连接流程见图2-2：

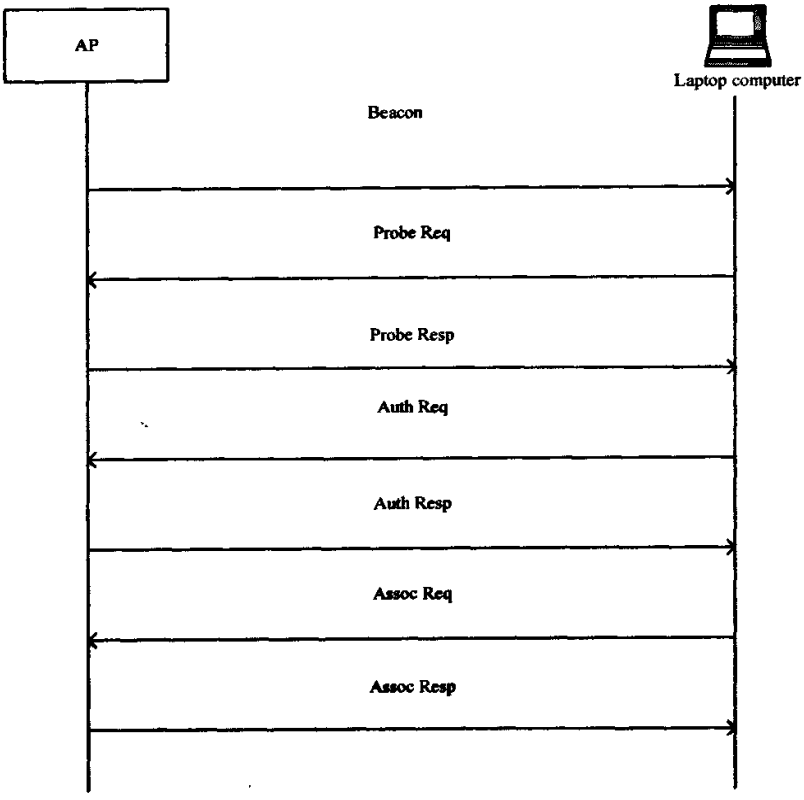

图2-2 IEEE 802.11网络连接建立过程流程图

2.2 WLAN在大型运动会中的应用

自从1964年东京奥运会首次使用了卫星转播技术以来，在每届奥运会中通信技术都发挥着越来越重要的作用，现代奥运会已经不仅仅是运动员竞赛的场所，还是架构在先进通信技术、计算机技术、电子技术等手段之上的高科技赛场。做为一种突发性的通信需求，奥运会的观众、运动员、媒体记者的数量都是惊人的，要求是近乎苛刻的。因此，在传统的有线局域网基础上，无线局域网的科学运用可以很好的补充和完善奥运会的通信要求，更加方便、准确、及时的为会场工作人员、运动员、记者、观众提过网络接入服务，从而满足各用户群的需要。

无线局域网系统服务于大型运动会，必须具备以下特点：

➢ 高可靠性

必须具有高度的安全可靠性，尤其是为体育竞赛的计时记分、成绩处理、信息发布等系统的链路必须做到万无一失。

➢ 高吞吐量

用户数量密集的区域必须有足够的吞吐量，足够的带宽来满足大数据量的网络使用需求。

➢ 高安全性

要有足够的安全机制，可以实现访问控制，实现用户认证，实现用户分级管理。

➢ 安装便捷

WLAN 最大的优势就是免去或减少了网络布线的工作量，只需安装一个或多个无线接入点 (即 AP) 设备，就可建立覆盖整个建筑或地区的局域网络。

➢ 易管理性

可以通过多种方式方便、及时的对无限局域网设备进行管理、设置、维护，可以进行远程控制。

➢ 易扩展性

根据网络容量的需要，能够及时的扩容，增加设备。针对无线局域网系统技术发展的特点，在无线网络系统技术更新换代周期很短的情况下，无线网络系统的基本设备能较容易地升级、扩展。

对于大型运动会中无线局域网的应用，我们建议采用基础构架模式来组网。(如图 2-3)：

图 2-3 基础架构模式示意图

这种模式适合于大型运动会比赛场馆内部、组委会办公区、新闻中心等场所进行组网，是大型运动会无线局域网的主要组网方式。在这种组网方式由无线接入点(AP)、无线工作站(STA)以及分布式系统(DSS)构成。无线接入点 AP 用于 STA 和有线网络之间接收、缓存和转发数据，所有的无线通讯都经过 AP 完成。并通

过外接的增益天线来实现本区域范围的无线信号的覆盖，覆盖半径达上百米。AP 可以连接到有线网络，实现无线网络和有线网络的互联。

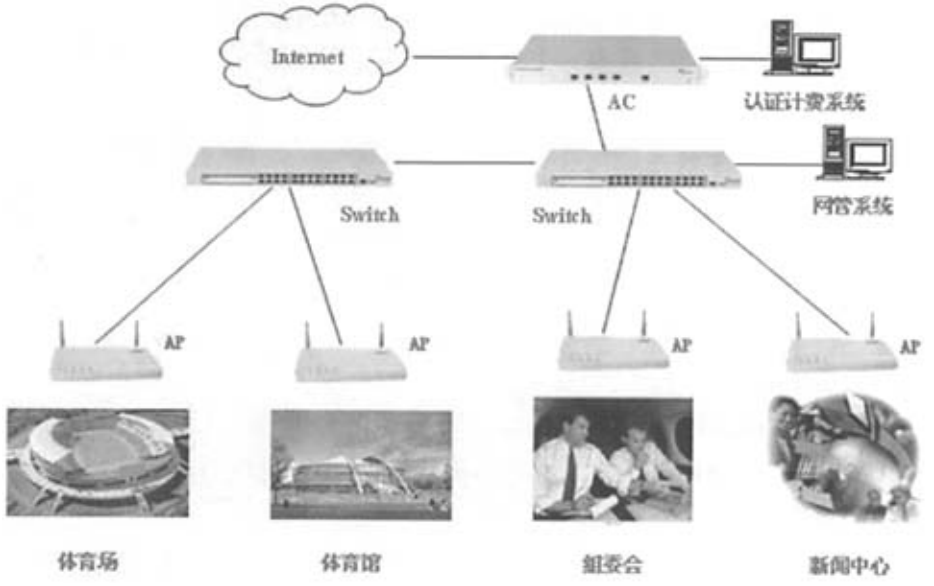

图 2-4 AP 在体育场馆 WLAN 组网中的位置

在体育场、体育馆、组委会办公楼、新闻中心等建筑和区域内，根据用户数、场馆面积安置适当数量的 AP，再通过一定数量的交换机进行汇聚并且接入访问控制器(AC)，通过 AC 来访问外部网络资源，如 Internet。

2.3 WLAN 的安全风险及解决方案

2.3.1 WLAN 中存在的安全风险

无线局域网安全的最大问题在于无线通信设备是在自由空间中进行传输，而不是像有线网络那样是在一定的物理线缆上进行传输，因此无法通过对传输媒介的接入控制来保证数据不会被未经授权的用户获取。 所以，WLAN 就面临一系列的有线网络中并不存在安全问题主要包括：

- 来自网络外部用户的进攻。
- 来自未认证的用户获得存取权。
- 来自网络内部的窃听泄密等。

现阶段针对 WLAN 的攻击主要为了实现两个目的。首先是通过 WLAN 寻找一个进入有线网络的切入点，有线网络经过长时间的发展能够建立完善的安全保护体系，例如通过安装防火墙可以提供对自身的保护，但是在其基础上扩建

WLAN时，如果没有对WLAN的安全防护作出全面的部署，则会危及到原始有线网络的安全，通常可以在防火墙内部安装恶意的无线访问接入点 AP(Access Point)，这种做法相当于给防火墙安装了后门，攻击者通过WLAN进入有线网内部实施恶意访问变得十分简单。

第二，针对无线数据的窃取。目前WLAN使用2.5GHz的无线电波进行网络通信，AP在一定半径内广播信号，无需通过可见的线路即可建立通信，任何攻击者都可以用一台带无线网卡的PC机或者无线扫描器进行窃听并使用某些特殊的网络嗅探工具扫描无线网络信号，一旦定位到信号，就能够截获并收集经过空间传播的数据。

针对 WLAN 的攻击次数不断增加，而攻击的手段也不断更新。目前针对WLAN的攻击方式主要包括嗅探、欺骗、网络劫持等。

(1) 嗅探

这是一种针对计算机网络通信的电子窃听。通过使用嗅探工具，网络监听者能够察看无线网络的所有通信。要想使WLAN不被识别工具发现，必须关闭用

于网络识别的广播以及任何未经授权用户访问资格。然而关闭广播意味着WLAN不能被正常用户发现，因此WLAN用户免受嗅探攻击的唯一方法是保护尽可能使用加密会话。

(2) 欺骗

攻击者冒充合法用户连接到想要入侵的网络，这样就可以避免目标网络对其非法身份的识别。最常用的一种欺骗手段是将自己的无线网络或网卡的MAC地址设定为合法地址，这可以通过在 Windows 平台修改注册表实现。一种新的欺骗攻击方式称为验证欺骗，攻击者通过对WLAN的嗅探累积多个用户验证请求，每个请求都包含原始明文消息及返回的加密过的应答，从这些材料中攻击者可以伪造身份验证信息欺骗AP成为合法用户。

(3) 网络劫持

攻击者将自己的主机伪装成默认网关或特定主机，所有试图进入网络或连接到被攻击者顶替的机器上的用户都会自动连接到伪装机器上。典型的无线网络劫持是使用欺骗性AP。通过构建一个信号强度好的AP,使无线用户忽视正常的AP而连接到欺骗性AP上，攻击者接受到来自其他合法用户的验证请求和信息后就能够将自己伪装成合法用户并进入目标WLAN。

上述三种是针对WLAN的一般攻击方式。从上述攻击方式上我们可以看到，对WLAN的攻击主要有两种渠道，一是直接劫持传输网络数据的无线电波，另一种就是冒充合法用户或AP接入无线网络。所以，WLAN的安全机制业主要包括两部分：一是用户认证，即只允许合法用户接入 WLAN；二是数据加密，即

网络中的数据传输采用密文的形式。以此来保证 WLAN 网络的安全。

2.3.2 WLAN 安全项目采用的安全解决方案

安全问题已经成了 WLAN 应用和发展的重中之重，雅典奥运组委会就因为 WLAN 的安全存在隐患而放弃了在 2004 年雅典奥运会的各个赛场布置 WLAN 网络。但由于针对 WLAN 安全的技术不断更新，如果能够应用最先进的安全技术，同时进行合理的配置，那么就可以解决这个棘手的问题。

所以在本项目中对网络安全方面非常重视，运用了多种手段：

- WEP 加密，支持 64 位和 128 位
- IEEE 802.11i，IEEE 推出的 WLAN 最新安全标准
- 多 SSID，通过 SSID 来限制用户的访问权限
- MAC 过滤、IP 过滤
- 同时支持多种认证方式来检测用户身份
- WAPI，我国推出的 WLAN 安全国家标准

这样，在 WLAN 安全项目中的 AP 就可以支持以下六种安全模式下：

1. 不加密
2. WEP(802.11 中定义的安全方案)
3. 802.1X+动态 WEP 密钥
4. 802.11i(WPA)
5. 802.11i(WPA)+PSK(与共享密钥)
6. WAPI

以上，是本次 WLAN 安全项目对 AP 在安全认证方面的基本要求。

2.4 本章小结

本章先介绍了 WLAN 的基本概念，即什么是 WLAN。然后介绍了 IEEE 802.11 系列的 WLAN 标准的发展情况。之后介绍了 WLAN 在现代大型运动会中的应用。最后介绍了 WLAN 面临的安全威胁，以及为了应对这些安全问题，在“WLAN 安全项目”中要实现的安全认证方案。

第三章 WLAN安全协议解析

3.1 WEP安全体制

3.1.1 WEP认证机制

IEEE 802.11中定义了WEP安全机制，用以保证802.11定义的无线局域网的安全。WEP分为认证阶段和加密阶段，认证阶段用来保证只有合法用户才能接入网络，数据加密用来保证传输过程的安全性。其中认证就是图2-2中的Authentication (链路验证阶段)阶段，有两种方式，一种是开放式认证，另一种是共享密钥认证。

所谓开放式认证其实就是不认证，只要STA发送一个消息请求认证，AP就回应一个成功消息。

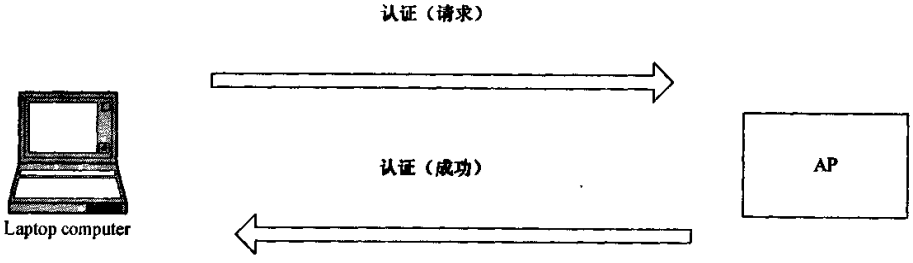

图3-1 开放式认证流程图

共享密钥认证需要AP和STA事先共享一个认证密钥，这时需要交互4个链路验证消息。首先STA向AP发出认证请求，然后AP发出一个128bits的随机数(challenge)，叫做质询文本，STA收到质询文本后，用WEP的加密算法和预先设置的密钥把该数字加密，将密文回复给AP。因为AP存储了先前发出的随机数，它可以检查发回的结果是不是用正确的密钥加密的，如果是就发送认证成功的消息。

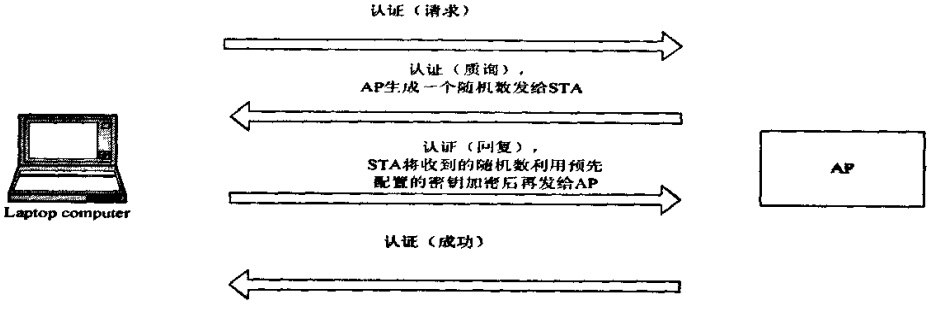

图3-2 WEP认证流程

我们发现在共享密钥认证过程中有两个漏洞。第一，AP没有向STA证明它知道密钥，即认证只是单向的。第二，我们从图3-2中可以看到，认证质询和认证回复消息正好是一对匹配样本，质询中是明文，回复中是密文，如果有攻击者在监听，完全可以利用这对样本来计算出密钥。所以这种方法不但不能进行认证，实际上反而帮助敌人攻击了加密密钥。所以在目前的绝大多数系统中已不再使用这种WEP认证方法，链路验证都采用开放式。

3.1.2 WEP加密机制

在WEP安全机制的加密阶段，采用的是RC4加密算法，RC4是一种字节流加密算法，每次从字节流中读入一个字节，然后与密钥流进行异或，结果作为输出字节。

RC4的使用又分两个阶段，一个是初始阶段，用来形成最终的加密密钥和在明文中加入完整性校验码(ICV)；二是加密阶段，将需要加密的数据与密钥流进行异或。总体来看RC4加密流程如图3-3所示：

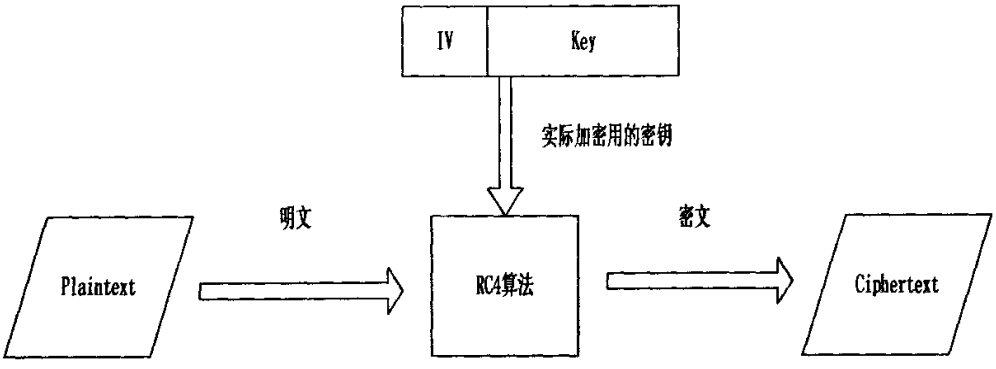

图3-3 RC4加密流程

在初始阶段中，包括对两方面的处理，一方面是对密钥，另一方面是对明文。图3-3中的Key就是前边认证时使用的密钥，这个Key是在初始配置时输入到AP和STA中的，因为在802.11中使用的是静态密钥，如果在加密中只使用这个Key的话，就会使相同的明文产生相同的密文，这在加密网络中传输的数据时是非常不可取的，因为在网络协议中，每个字段的意义都是固定的，比如说源IP总是位于数据包的同一位置，那攻击者如果在这个位置看到了相同的加密字节，就会知道这个报文是来自于同一个IP地址的。

为了解决这个问题就引入了IV(初始化向量)，通过改变IV，来使实际加密每个数据包的密钥都不同，在802.11中IV是24bits的，Key目前多数系统都采用104bits，这样实际加密强度就是128bits。但这个IV需要明文传递给接收方，

以便接收方生成解密密钥。

对明文的处理主要是加上 ICV(完整性校验码)，然后把这个 ICV 和明文一起加密，这样在接受方解密之后可以利用 ICV 来判断是否有任何位在传输中被破坏。

经过初始阶段的处理后，开始利用 RC4 算法进行加密，然后发送出去的数据帧格式是：

表 3-1 利用 WEP 加密后的数据帧格式

MACHeader	IV	Data	ICV	FCS

其中，IV 字段中包含两部分，首先是 3 字节的初始向量值，然后是 6bits 的填充值，一般是 0，最后是 2bits 的 KeyID,告诉对方用的是几号密钥，因为 STA 客户端和 AP 在配置时可以设置 4 个密钥，当然这 4 个密钥是对应相同的，即 STA 中的 1 号密钥与 AP 中的 1 号密钥相同，以此类推。所以需要一个 KeyID 来告诉对方我使用的是哪个密钥，对方好找到自己对应的密钥去解密。Data+ICV 是被加密的，其他字段均为明文。

WEP 加密流程如图 3-4 所示：

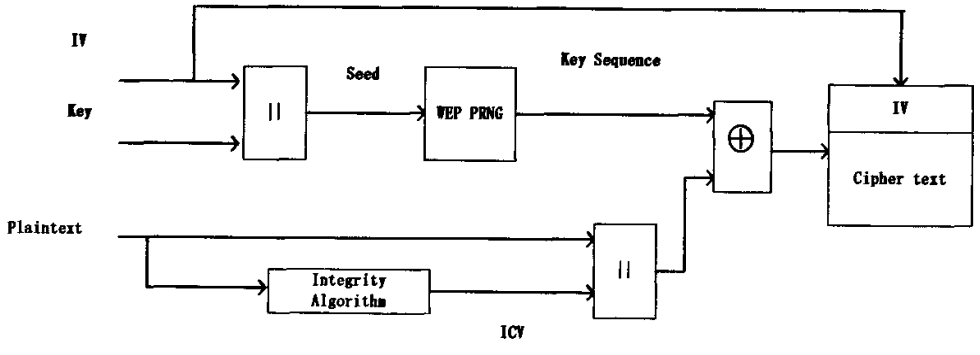

图 3-4 WEP 数据加密流程

这样发送方把加密后的密文和用来生成密钥的 IV 和 KeyID 传给了接收方。接受方收到后，首先生成解密密钥，然后与密文异或就可以得到明文。

3.1.3 WEP 安全机制漏洞分析

一个安全系统需要具备的安全措施包括：

(1)认证

(2)接入控制

(3)重播防护

(4)消息篡改检测

(5)消息加密

(6)密钥保护

而在这六个方面上，WEP 安全机制都没有完成任务。首先在认证方面，前边我们已经提到过，WEP 认证既没有实现相互认证，还泄露了可以攻击密钥的明文、密文匹配的样本；而且认证时没有使用独立密钥，即认证所用密钥与加密数据报文时所用密钥相同；所以目前绝大多数系统已经不使用 WEP 认证。

而在接入控制和重播防护方面，802.11 没有提供任何的防护措施。

对于消息篡改检测，WEP 试图利用 ICV 值来进行保护。ICV 的思想就是基于所有要加密的数据算出一个校验值，把这个校验值附在数据末尾，然后整个加密，如果有人改变了密文中的一位，解密后的数据就不会有相同的校验和，就发现了篡改。但是设计者忽略了，用于计算 ICV 的方法被称为一种线形性方法。这会导致，如果你只改变了消息中的一位，你就可以预测到 ICV 中哪些位将被改变。更主要的是，由于 RC4 通过异或数据得到密文，位反转在加密过程会被保留下来，使得攻击者可以同时篡改加密后的数据和 ICV 中的对应位，而使篡改不被发现。这样我们看到利用 ICV 来实现对消息篡改的检测不能实现它的目标[3]。

在消息加密方面，利用了 RC4 算法，密钥方面利用 IV 和预先配置的 Key 一起作为加密密钥，使用 IV 的目的就是想利用 IV 的变化来使加密每个数据包的密钥不同，避免相同的明文生成相同的密文。但是通过研究 IV 我们发现，实际上很难起到设想的作用，因为 24bits 的 IV 传输了 2^{24}(约 1700 万)帧后就会产生 IV 冲突，而 802.11b 每秒就能够传输 500 个全长帧，而在这样的速率下，IV 的容量 7 个小时内就会用光。实际上冲突可能出现的更加频繁，因为也许会有许多个设备在传输。这样经过一段时间，如果收集到同一 IV 足够多的样本，很可能就能够猜出密钥流的重要部分，此后就会解密的越来越多。可见 IV 并没有很好的解决密钥冲突的问题。

在密钥保护方面，WEP 也没有对 AP 和 STA 上的预设密钥进行任何的保护措施。

所以在上述 6 个方面，WEP 都没能实现安全机制的任务。

3.1.4 小结

本节详细介绍了 WEP 安全机制，包括认证和加密两部分的实现原理。最后详细论证了 WEP 安全机制的缺陷。正是由于 WEP 安全机制的这些缺陷，才针对性的开发了 802.11i 和我国自主知识产权的 WLAN 安全标准 WAPI。

3.2 IEEE 802.11i 协议

为了弥补 IEEE 802.11 标准中 WEP 协议的缺陷，IEEE 802.11 的 i 工作组专门制定了新的 WLAN 安全认证标准，IEEE 802.11i[4]。实际上就是把 1999 年制定的 IEEE 802.1X[5]安全标准引入了 WLAN。

IEEE 802.11i 规定使用 IEEE 802.1X 作为接入认证协议，定义了 TKIP(Temporal Key Integrity Protocol)和 CCMP(Counter-Mode/CBC-MAC Protocol)两种安全机制。其中 TKIP 为了兼容以前的 WEP 设备，依然采用 WEP 机制里的 RC4 作为核心加密算法，这样就可以通过在现有设备上升级固件和驱动程序的方法来使设备演进到 IEEE 802.11i，达到提高 WLAN 安全的目的。相对于 TKIP 这种折中方案，CCMP 机制完全摆脱了 WEP 的束缚，从设计一开始就以安全为前提，完全抛开其他模式，采用了 AES(Advanced Encryption Standard)加密算法，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。由于 AES 对硬件要求比较高，因此 CCMP 无法通过在现有设备的基础上进行升级实现，所以目前使用比较多的还是 TKIP 加密机制[6]。

TKIP 和 CCMP 最大的不同点发生在数据加密和解密的底层，在之前的建立连接、密钥管理等阶段是几乎完全相同的，而系统中加、解密是通过硬件来实现的，并不在软件设计的范围内，所以这里就不将二者进行单独的分析，而统一作为 IEEE 802.11i 协议来探讨。

加入了 IEEE 802.11i 的 IEEE 802.11 无线局域网连接过程分为以下几步：

1、发现阶段；

2、IEEE 802.1X 认证阶段；

3、密钥管理阶段，包括密钥生成、密钥分配；

4、最后对数据进行加密传输。

在发现阶段主要是进行 IEEE 802.11 网络的基本连接过程(如图 2-2)，之后利用 IEEE 802.1X 协议进行用户认证，只有通过了认证的用户才能证明是合法用户，否则虽然建立了网络连接也不能进行数据传输。通过了认证之后，为了能够进行密文通信，需要在密钥管理阶段生成密钥。最后进行数据的加密传输。具体流程如图 3-5：

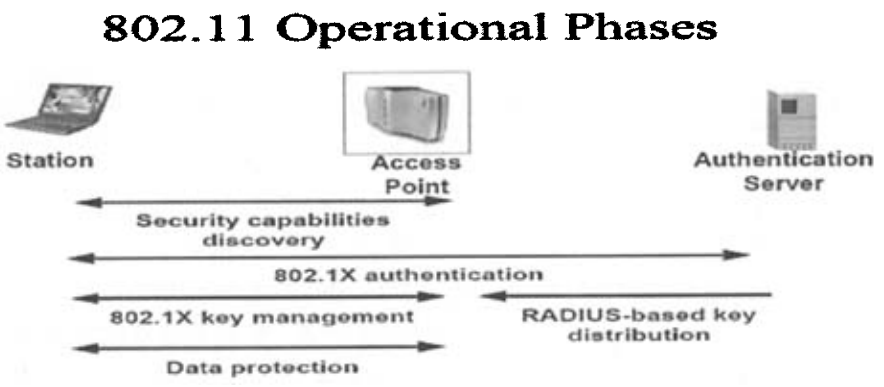

图 3-5 IEEE 802.11i 操作流程

由于发现阶段比较简单没有实现安全认证方面的功能，所以我们从第二阶段802.1X 认证阶段开始介绍。

3.2.1 IEEE 802.1X 及 EAP-SIM 认证

在认证方面，IEEE 802.11i 将 1999 年为有线局域网制定的接入控制协议 IEEE 802.1X 引入到了无线局域网中，利用 IEEE 802.1X 中定义的 EAP[7]协议对用户进行认证。EAP 的全称是可扩展的认证协议，其可扩展性表现在支持多种认证方法，比较常用的是 EAP-MD5、EAP-TLS 等认证协议，在本系统中为了利用现有的移动 2.5G 网络进行认证和计费，我们增加了对 EAP-SIM 认证的支持。

这一阶段的作用就是鉴别了用户的合法身份，并对通过鉴别的用户生成了下一阶段——密钥管理中所使用的主密钥。

3.2.1.1 IEEE 802.1X 体系结构及 EAP 认证流程

IEEE802.1X 的体系结构包括了 Supplicant System 客户端系统，Authenticator System 认证系统，Authentication Server System(简称“AS”) 认证服务器系统三个角色。

Supplicant 客户端是指向认证系统(Authenticator)发起请求，对其身份的合法性进行检验的实体，通常在 STA 中。Authenticator 认证系统实指在 LAN 连接的一端用于认证另一端设备的实体，通常由 AP 充当。Authentication Server 认证服务器是指为认证系统提供服务的实体，这里认证服务器所提供的服务是指通过检验客户端发送过来的身份标识，来判断该请求者是否有权使用认证系统所提供的网络服务，通常为 RADIUS 服务器，该服务器存有用户的信息，例如用户 VLAN ID 和优先级，用户的访问控制列表等等。当用户通过认证后，认证服务器将这些信息发给 Authenticator ，之后由 Authenticator 创建动态用户访问列表，监管用户的通信。

Supplicant 和 Anthenticator 之间传输用 EAPOL 协议，Authenticator 和 Authentication Server 之间传输常用 RADIUS 协议。也就是说，在认证上我们采用的是 802.1X+RADIUS 模式。

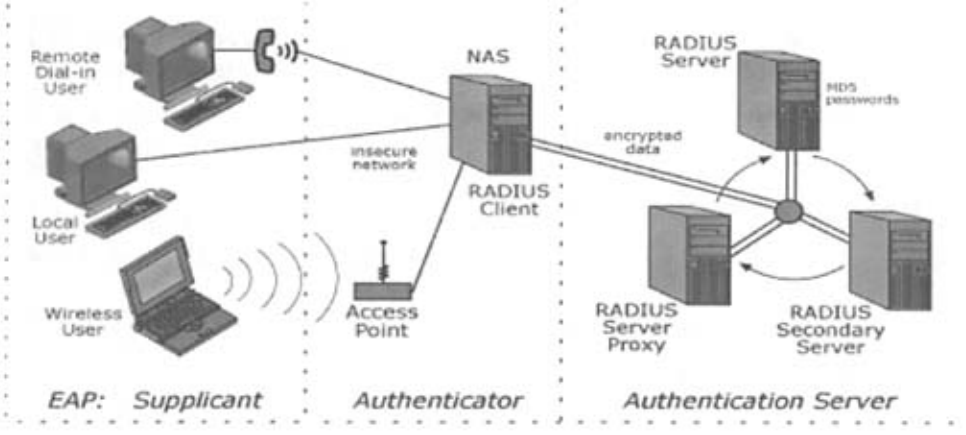

图 3-6 IEEE 802.1X+RADIUS 模型

从图 3-6 中我们看到无线用户通过 EAP 协议向 AP 发送认证信息，AP 再通过 RADIUS Client 与 RADIUS Server 利用 Supplicant 发过来信息进行认证，在实际系统中我们通常将 RADIUS Client 集成到 AP 中。

Supplicant 与 AP 中 Authenticator 模块通信时，采用的主要的报文类型有：

表 3-2 Supplicant 与 Authenticator 进行 EAP 认证所用的报文类型

报文类型	作用
EAPOL-Start	Supplicant 通过这个报文来通知 Authenticator 要进行认证。
EAP-Packet	EAP-Packet 中包括 Request、Response、Success、Failure 四种类型的 EAP 报文，Authenticator 通过 EAP-Request 报文来向 Supplicant 请求认证信息，相反 Supplicant 通过 EAP-Response 来回复 EAP-Request；如果认证成功，Authenticator 向 Supplicant 发送 EAP-Success 通知消息，反之则发送 EAP-Failure。
EAPOL-Logoff	当 Supplicant 要断开连接时，通过这个报文来向 Authenticator 发出申请。

Authenticator 与 Authentication Server 之间的通信所使用的 RADIUS 协议的主要报文类型是：

表 3-3 Authenticator 与 Authentication Server 之间的通信所使用的主要报文类型

报文类型	作用
Access-Request	Authenticator 通过这个报文向认证服务器发出接入认证请求信息
Access-Challenge	认证服务器通过 Access-Challenge 报文向 Authenticator 请求接入认证信息。
Access-Accept	如果认证通过，认证服务器就向 Authenticator 发送这个报文,表示允许接入。
Access-Reject	如果认证没有通过，认证服务器就向 Authenticator 发送这个报文，表示拒绝接入。
Accounting-RequesAccounting-challenge	这两个报文是计费认证时使用的。

认证的具体流程如图 3-7：

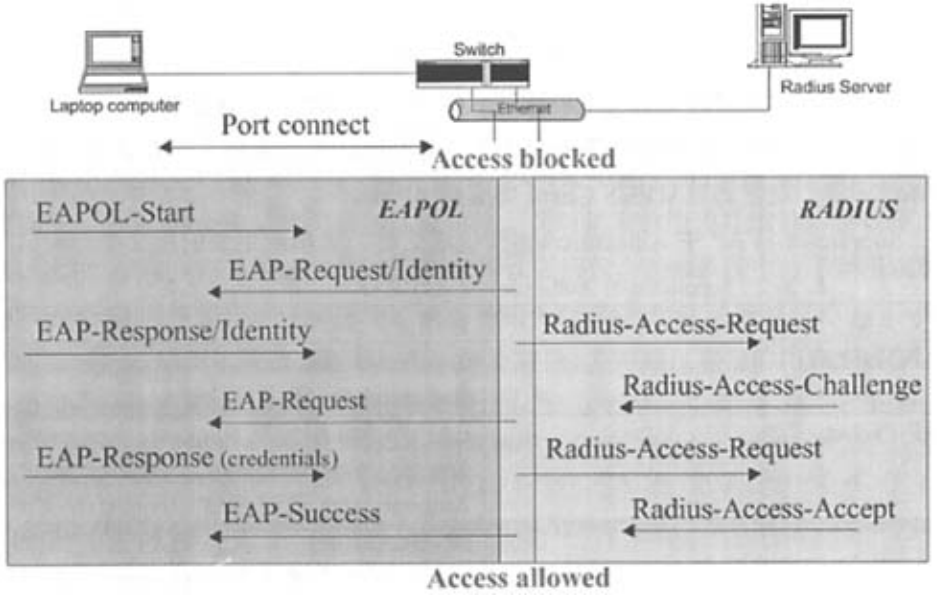

图 3-7 802.1X+RADIUS 认证流程

1、首先 Supplicant 发送 EAPOL-Start 给 Authenticator 来启动认证流程。

2、Supplicant 收到 EAP-Request/Idenitity 报文后，向 Authenticator 发送一个 EAP-Response/Identity，该报文携带了用户的 indentity，即唯一标识符，有这样的 identity，服务器才能提供认证功能。

3、Authenticator 收到 EAP-Response/Identity 报文后封装在 RADIUS 的 Access-Request 报文的 EAP-Message 属性内转发给 RADIUS 服务器。RADIUS 服务器通常将利用 EAP-Response/Identity 来断定将对用户使用何种 EAP 类型(即用户采用的是何种认证方式)。

4、RADIUS 服务器收到携带客户端身份 ID 的 Access-Request 后，将回应一

个 Access-Challenge 报文，并将 EAP-Request 报文、用于用户密码加密的 Challenge(MD5 Challenge 或 OTP Challenge，取决于 EAP 所用的认证机制)封装在 Access-Challenge 报文的 EAP-Message 属性内。

5、Authenticator 收到 Access Challenge 报文后，从 EAP-Message 属性域提取出 MD5 Challenge 或 OTP Challenge 信息，以 EAP-Request 报文发送给 Supplicant。

6、Supplicant 收到 Challenge 信息后，将自己的密码进行加密，以 EAP-Response 报文发送给 Authenticator。

7、Authenticator 将收到的 EAP Response(含有用户密码信息)封装在 EAP-Message 属性域内，以 Access-Request 报文发送到 RADIUS 服务器，进行认证。

8、RADIUS 服务器验证通过后，将 EAP-Success 报文封装在 Access-accept 报文的 EAP-Message 属性域内发送给 Authenticator PAE。如果认证没有通过，则将 EAP- Failure 报文封装在 Access-Reject 报文 EAP-Message 属性域内发送给 Authenticator。Authenticator 将 EAP-Success 或 EAP-Failure 发送给 Supplicant，通知认证通过与否，同时将服务器同时送来的一些显示信息和提示一并传递 Supplicant。

3.2.1.2 EAP-SIM 认证原理

EAP-SIM[9]认证最主要的优点是通过手机 SIM 卡中的信息进行用户认证，并实现计费。这样就利用了现有的 2.5G 移动通信网络，使 WLAN 与现有的移动网络有效的结合起来。所以在“WLAN 安全项目”中，在 AP 中增加了对 EAP-SIM 认证的支持，同时保持原有对 EAP-MD5、EAP-TLS 等认证协议的支持。

因为 EAP-SIM 认证是对 SIM 卡中的信息进行认证，而这个认证需要用到 HLR(归属位置寄存器)中的信息，所以采用这种认证方式后，AS 必须将认证信息利用 SS7(七号信令)传递给 HLR(归属位置寄存器)，所以在这种认证中有四个角色：Supplicant、Authenticator、Authentication Server 和 HLR。

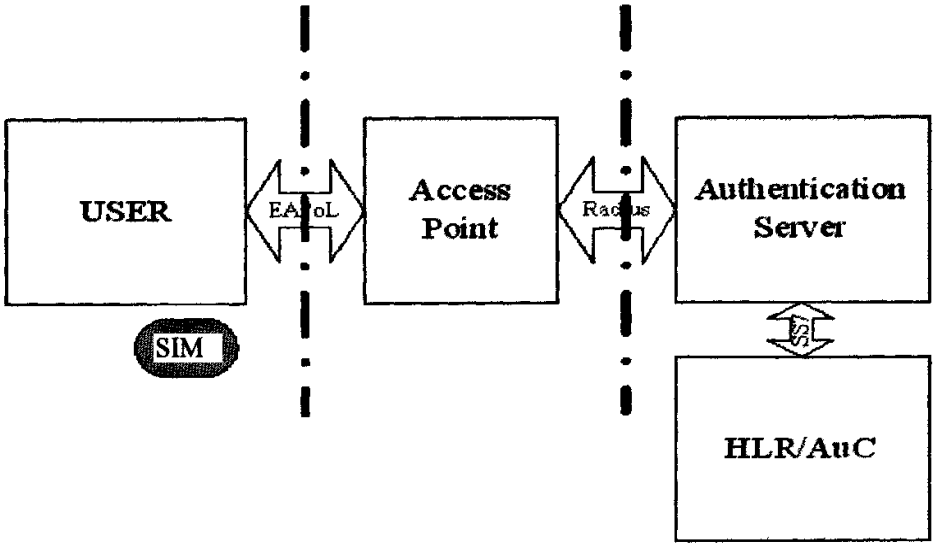

图 3-8 EAP-SIM 体系结构

EAP-SIM 认证基本原理：EAP-SIM 认证所使用的基本安全因素是 SIM 卡和 HLR(归属位置寄存器)中的 IMSI(International Mobile Subscriber Identification 国际移动用户身份)，密钥 Ki 和算法 A3、A8。这 4 个基本要素只有 SIM 卡和 HLR 中掌握。IMSI 相当于用户名的作用，Ki 是作为初始密钥，A3、A8 算法用来生成下一级密钥。只有 SIM 卡中的这些信息与 HLR 中相应的 IMSI 所对应的相同时，才能通过认证。而这 4 个基本安全要素是不会通过网络传输的，确保了它们的安全性。

具体认证流程及原理如图 3-9 所示：

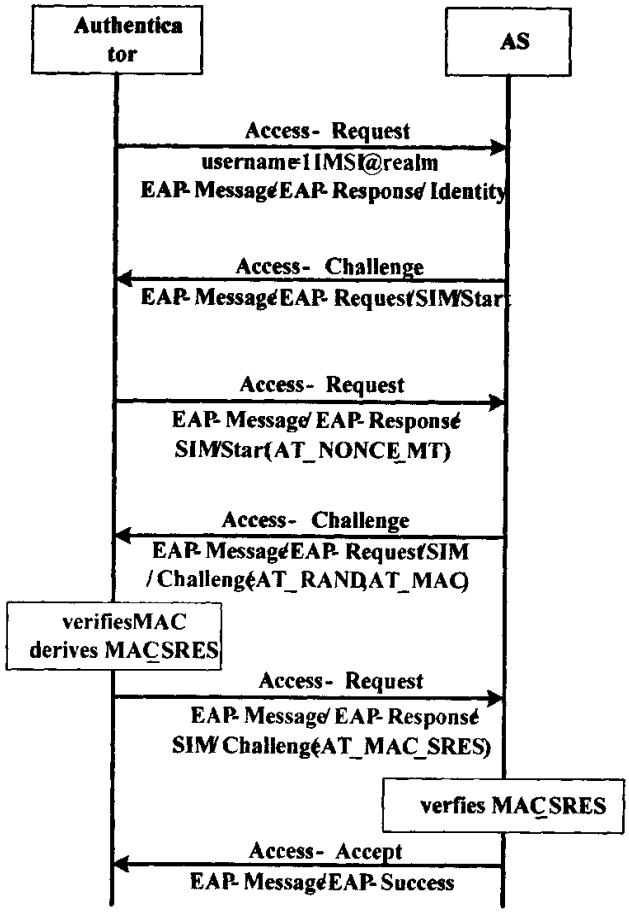

图 3-9 EAP-SIM 认证流程图

1、Authenticator 向 AS 发一个 Access-Request 报文，在这个报文中携带用户的 IMSI 信息。

2、AS 收到带有 IMSI 的 Access-Request 报文后，发现这个用户使用的是 EAP-SIM 认证，就向 Authenticator 发送启动 EAP-SIM 认证流程的 Access-Request/EAP-Message/EAP-Responses/SIM/Start 报文。

3、Authenticator 收到这个启动 EAP-SIM 认证流程的报文后，向 AS 发送 Access-Request 请求报文，在这个报文的 EAP-Message 属性中带有的信息是：AT-NONCE-MT，这是一个 16Bytes 的随机数，是终端用户生成通过 Authenticator 透传给 AS

4、AS 收到这个 NONCE 后，计算出 AT-RAND 和 AT-MAC 两个值，再将这两个值传回给 Authenticator。其中，AT-RAND 是 HLR 根据 IMSI 生成，通过七号信令传给 AS 的，AT-MAC 的构造方法：

第一步：根据 kc 和 NONCE_MT 构造 4 个密钥：K_{sres}、K_{int} 和 K_{encr}、K_{sess}

其中，Kc=A8(Ki,RAND)，A8、Ki、RAND 都在 HLR 中。得到 Kc 后再去

计算 Master_Key，Master_Key=SHA1(n*Kc|NONCE_MT)，n 表示 HLR 中随机三元组的个数，一般为 3。

再利用函数 PRF(Master_Key)得到一个 160B 的伪随机序列，截取这个序列得到上边的四个密钥。

第二步：先按照 MAC 的值为 0，构造 EAP 报文，用 K_{int} 进行 HMAC-SHA1-128 加密，得到 20 个字节，取前 16 个字节，作为 MAC 值，即：

AT_MAC=HMAC_SHA1_128(K_init,整个 EAP 包)

5、Authenticator 收到 AT-MAC 后，将这个值发给用户，先用同样的方法再计算一次 AT-MAC 值，看结果是否与收到的 AT-MAC 一致，如果一致，说明 HLR 中的 Ki 与自己的一致，同时说明用户生成的随机数在传输的过程中也没有被篡改，再去计算 MAC_SRES：

MAC_SRES=HMAC_SHA1_128(K_sres,n*SRES|Message Subtype)，其中 SRES=A3(Ki,RAND)

然后将这个 MAC_SRES 通过 Authenticator 透传给 AS。

6、AS 收到后再用同样的方法计算一下 MAC_SRES，如果与收到的一致，就说明终端用户的 SIM 卡中的 Ki 与 HLR 中对应 IMSI 中的一致，而且收到的用户生成的随机数也是正确的。这时就向 Authenticator 发送 Access-Accept 报文，表示认证成功。最主要的是 AS 在这个 Access-Accept 中携带了两个密钥：MPPE-SEND-KEY，MPPE-RECV-KEY,而 MPPE-RECV-KEY 就是 802.11i 安全机制中的主密钥。利用这个主密钥开始下边的密钥管理流程。

3.2.2 密钥管理

在 IEEE 802.11i 标准中，在密钥管理方面是对 IEEE 802.11 改动最大的。首先，摒弃了共享密钥这种密钥分配方式。其次，在密钥结构方面，采取分层次的密钥结构。通过密钥管理阶段得到最终数据加密用的单播密钥和组播密钥以及计算完整性校验码的密钥。

下图是 802.11i 在密钥管理上的整体思想：

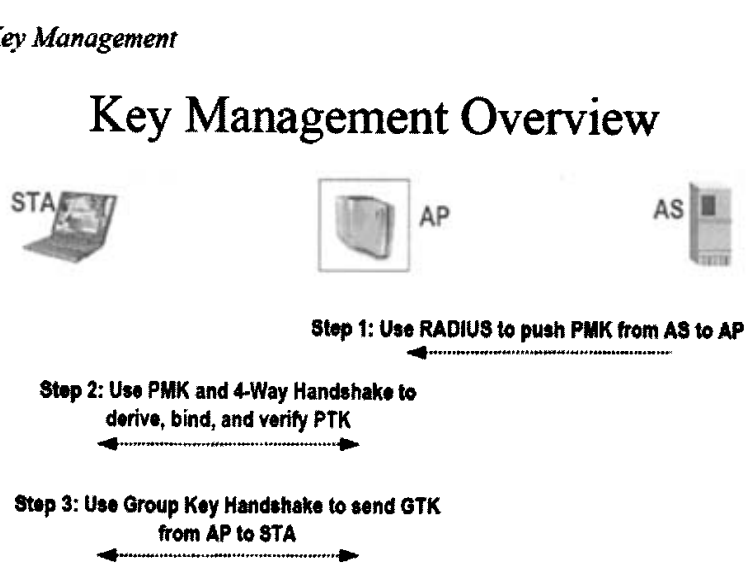

图 3-10 IEEE 802.11i 密钥管理整体结构

第一阶段，就是 AS 把生成的 PMK 利用 RADIUS 协议传给 AP，这是在 EAP 认证成功时，在 Access-accept 报文中携带了 PMK 的值发送给了 AP。

第二阶段，就是由 PMK 生成 PTK(单播临时密钥)。在 IEEE 802.11i 中为了保证安全采用了分层的密钥结构，单播密钥的体系结构见下图。而且还摒弃了共享密钥的密钥分配方式，同时为了不让最后使用的密钥在网上传输，采用了 AP 和 STA 分别生成但播密钥，这是通过“四次握手”实现的。

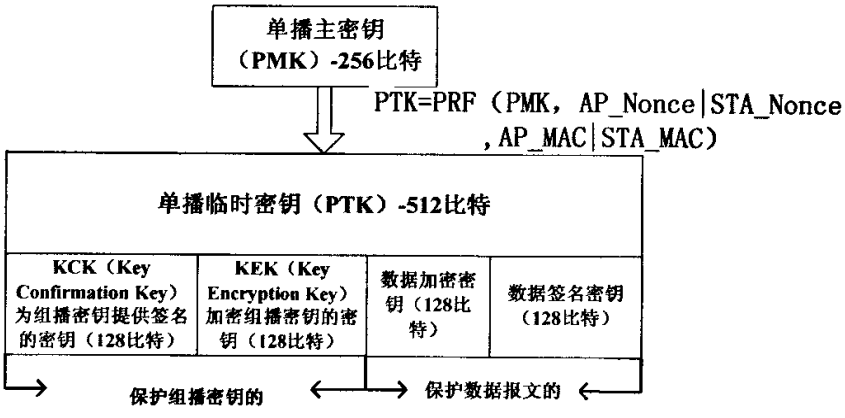

图 3-11 单播密钥体系结构

由上图我们看到，PMK 不是最终的加密密钥，STA 和 AP 要利用 PMK 以及 STA 和 AP 的 MAC 地址还有 STA 和 AP 分别生成的随机数来生成 PTK(Pairwise Transit Key)，PTK=PRF(PMK，AP_NONCE|STA_NONCE,AP_MAC|STA_MAC)，其中，PRF 是伪随机数生成函数。生成的 PTK 的前 128bits 作为以后传递组播密钥的签名密钥，128bit-255bit 作为传递组播密钥的加密密钥。256-383bit 作为加

密数据报文的密钥，后128bits作为数据报文的签名密钥。

下面我们再来看密钥的生成。首先,AP的PMK是在第一阶段由AS传给AP的。然后AP和STA通过交换随机数(NONCE)来生成PTK，因为整个生成过程需要交换4个报文，所以把这个过程叫做“四次握手”，“四次握手”流程如图3-12所示：

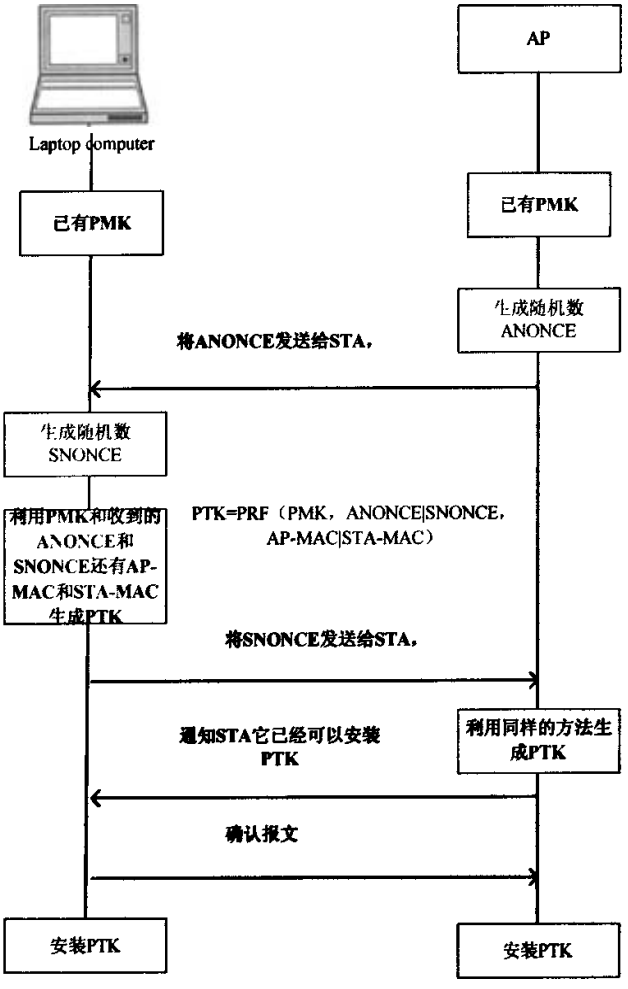

图3-12 四次握手流程

通过四次握手，AP和STA交换了ANONCE和SNONCE，计算了PTK，同时从四次握手的第二个报文开始就利用计算出来的PTK给报文做了签名，这样AP只有计算出同样的PTK才能成功地验证签名，而只有二者的PMK相同，才能计算出同样的PTK，所以就间接核实了双方是否有同样的PMK、PTK。最后又同步了密钥。可以说从四次握手以后，AP和STA之间就可以利用单播密钥加密数据报文了。

因为组播密钥是由AP单方面生成发给STA的，而为了密钥的安全传递，所

以要等到生成PTK之后才能开始建立组播密钥体系。

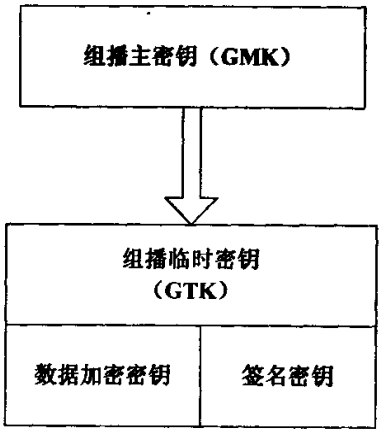

图 3-13 组播密钥层次结构

组播密钥是接入点AP生成后传给STA的，所以不需要向单播密钥生成那样复杂，只需要两次握手就够了，组播密钥生成及发送的两次握手的过程如图3-14：

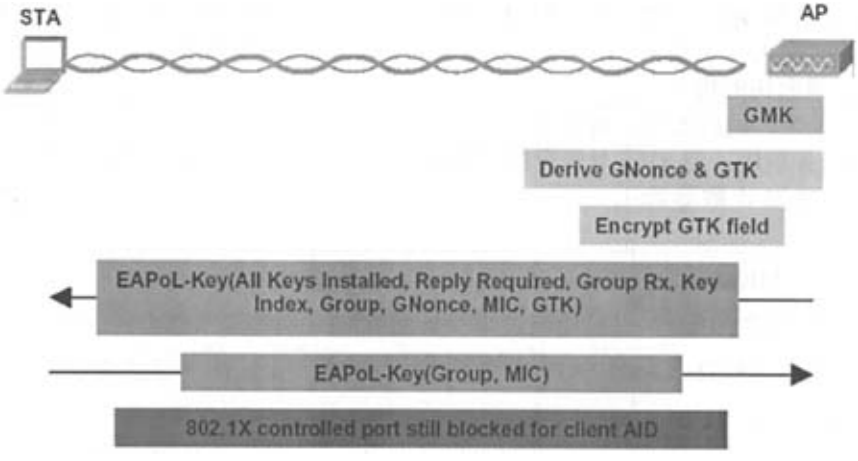

图 3-14 组播密钥“二次握手”流程图

由于一个AP下连接的所有STA都使用相同的组播密钥，所以每当有一个STA断开连接的时候，AP都要更新组播密钥。这是组播密钥在更新上的一个特性。

当单播密钥和组播密钥都生成了之后，就可以对数据报文加密传送了。

3.2.3 数据加密

前边已经介绍过IEEE 802.11i定义了两种安全机制，一个是TKIP，另一个是CCMP。CCMP采用的是迄今为止最先进的分组加密算法AES来对数据进行加密，很好的保护了网络的安全性。而TKIP为了兼容原来的WEP系统，仍然采用了RC4加密算法，只是引入了一些措施来弥补WEP的漏洞，但这只能是一

个折中方案。

TKIP 主要解决的 WEP 加密体系中的问题：

表 3-4 WEP 采用的加密体的缺点

序号	WEP 的缺点
1	IV 值太短，不能有效防止重用
2	对消息篡改没有有效的监测方法
3	直接使用主密钥，并且从不更新密钥
4	没有措施来防止消息重发

TKIP 针对上述每一项不足都采取了补救措施，以此来解决 WEP 的安全漏洞。

表 3-5 从 WEP 到 TKIP 的改动

措施	目的	针对的缺点
对消息的所有字节，利用 Michael 方法生成了消息完整性校验码 MIC	确保消息的完整性	对消息篡改没有有效的监测方法
认证和加密使用不同的密钥，同时加入一个发布和改变广播密钥的机制	引入密钥管理	直接使用主密钥，并且从不更新密钥
加大 IV 长度，同时改变 IV 制的选择规则，将 IV 作为一个重发计数器而再利用	避免 IV 重用，同时加入对消息的重发保护	IV 值太短，不能有效防止重用；没有措施来防止消息重发

1、引入 MIC

在讲 WEP 的缺陷时，已经论述过由于计算 ICV 采用的是线性方法，所以 ICV 不能保证消息不被篡改。在 TKIP 中使用了一种叫做 Michael 的算法来生成消息完整性码(MIC)。

Michael 算法是专门为 TKIP 设计的，在计算 MIC 时，只使用了置换、循环移位和异或操作，没有用到乘法，这样就降低了对硬件的要求。

同时，由于 TKIP 需要兼容 WEP 的硬件结构，所以在 TKIP 中也仍然保留了 ICV。而且 MIC 和 ICV 的区别不仅表现在计算方法上，也表现在它们保护的内容上。这就涉及到一个分段的概念，首先从应用层将要传输的数据向下依次传给网络层、传输层、数据链路层，最后到物理层，而每一层都要加上一个头，而这些数据未必能一次传输，若不能就需要分段，在物理层一次传一个分段，每个分段叫做一个 MPDU(MAC 协议数据单元)，没有分段之前叫做 MSDU(MAC 服务数据单元)，ICV 是对 MPDU 的数据计算的，MIC 是对 MSDU 的数据计算的。就是说当收到一个报文解密之后就可以检验 ICV 是否符合，但必须要等一个 MSDU 收齐了之后才能检验 MIC 值。

2、IV 的选择和使用

在WEP中IV值只有24bit，以至于在一个忙得网络中可能被经常重复使用，在TKIP中，将IV扩展到48bit。而且还赋予了IV第二个任务，作为顺序计数器以避免重发攻击。

由于TKIP需要兼容WEP的硬件设备，而在WEP中是将24bit的IV直接加在密钥前边的，所以在TKIP中不能简单的通过结合密钥和IV来得到一个新的RC4密钥，我们将处理IV和密钥来形成新的RC4密钥的过程叫做密钥混合。密钥混合分为两个阶段，在第一个阶段中利用IV的高32bits和发送方的MAC地址还有四次握手后生成的会话密钥来生成一个 80bits 的输出。然后再利用这80bits值和IV的低16bits还有会话密钥去生成新的128bits的RC4密钥。这两个阶段可以归纳为两个函数：

P1K<——Phase(TA,TSCU,TK)

P2K<——Phase(P1K,TSCL,TK),其中，TA表示发送法方的MAC地址。TSC的意思是TKIP顺序计数器，事实上就是IV值。TSCU表示IV值得高32bis，TSCL表示IV值得低16bits。P1K是第一阶段80bits的输出，P2K作为第二阶段的输出，事实上也就是128bits的RC4密钥。

总结TKIP的加密机制，可以分为三个模块：密钥导出模块、计算MIC模块、RC4加密模块，三个模块的关系如图3-15所示：

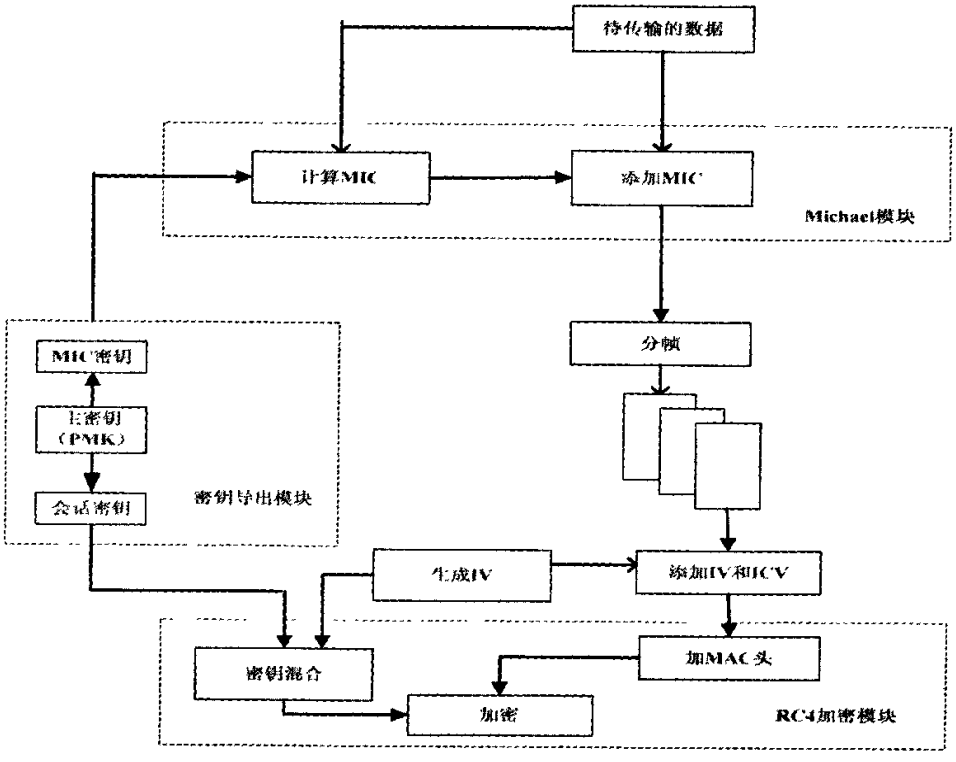

图3-15 TKIP加密模块及流程

3.2.4 小结

本节先详细介绍了802.11i网络建立的流程及其中用到的802.1X认证协议：802.11i网络建立流程分为4个阶段，第一阶段是发现阶段，主要是建立802.11网络关联，流程与802.11网络一致；第二阶段是802.1X认证阶段，主要是利用802.1X标准实现客户端的接入认证，为了与移动现有的网络结合，并且利用现有的计费体系，我们实现的是EAP-SIM认证；第三阶段是密钥管理阶段，这也是802.11i标准的重点，即，采用分层次的密钥管理体系，通过四次握手来生成单播密钥及二次握手来生成组播密钥，以此来避免密钥在网络上直接传输。第四阶段是数据加密阶段，即利用前一阶段生成的密钥来开始数据的加密传输。

3.3 WAPI安全机制

WAPI[11]是无线局域网鉴别与保密基础结构的英文缩写，它由无线局域网鉴别基础结构WAI(WLAN Authentication Infrastructure)和无线局域网保密基础结构WPI(WLAN Privacy Infrastructure)两部份组成。WAI负责接入认证，WPI负责数据加密。

3.3.1 WAI

WAI是鉴别模块，采用公开密钥密码体制，利用证书来对WLAN系统中的STA和AP进行认证，同时采用基于椭圆曲线算法的公钥加密机制，支持192、224、256bit的三种椭圆曲线加密。在这个模块中有三个实体：

鉴别器实体AE(Authenticator Entity)：为鉴别请求者在接入服务之前提供鉴别操作的实体，驻留在AP中。

鉴别请求者实体ASUE(Authentication Supplicant Entity)：需通过鉴别服务单元进行鉴别的实体，驻留在STA中。

鉴别服务实体ASE(Authentication Service Entity)：为鉴别器和鉴别请求者提供相互鉴别的实体，驻留在ASU中。

鉴别服务单元ASU(Authentication Service Unit)是基于公钥密码技术的WAI鉴别基础结构中最为重要的组成部分，它的基本功能是实现对STA用户证书的管理和STA用户身份的鉴别等。ASU作为可信任和具有权威性的第三方，保证公钥体系中证书的合法性。ASU为每个客户颁发公钥数字证书，并为使用该证书的客户提供公钥合法性的证明。ASU的数字签名确保证书不被伪造或篡改。ASU负责管理所有参与网上信息交换的各方所需的数字证书(包括产生、颁发、吊销、更正等)，是实现电子信息安全交换的核心。

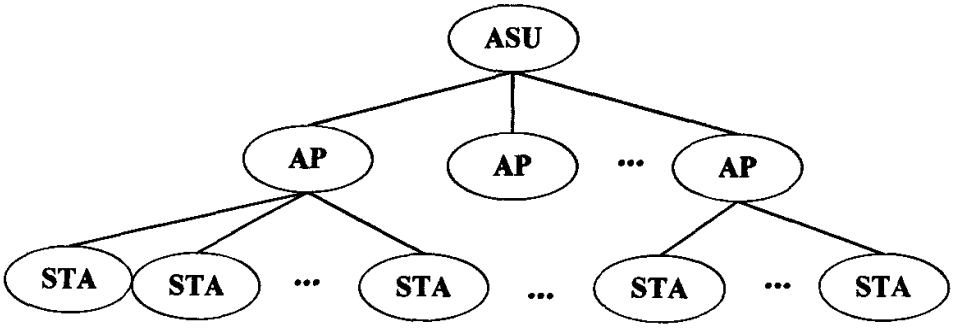

图 3-16 基于 ASU 的 WAI 逻辑拓扑结构示意图

WAI 中 STA 和 AP 的证书采用如下格式：

表 3-6 WAI 中的证书格式

公钥证书的版本号
证书的序列号
证书颁发者采用的签名算法
证书颁发者名称
证书颁发者的公钥信息
证书的有效期
证书持有者名称
证书持有者名称的公钥信息
证书类型
扩展
证书颁发者对证书的签名

其中：

- 公钥证书版本号

该字段指定证书的格式，以使具体的协议能提取该公钥证书的有效数据项

- 证书序列号

每个由 ASU 颁发的证书都需要分配一个唯一的序列号，由证书的序列号和颁发者名称可以唯一的确定一个证书

- 证书颁发者采用的签名算法

该字段指定了证书颁发者所采用的签名算法，包括算法名称、签名长度和签名者所使用的公钥长度

- 证书颁发者名称

该字段指定证书颁发者的公钥信息

- 证书颁发者的公钥信息

该字段指定证书颁发者的公钥信息

- 证书的有效期

该字段指定证书可以使用的有效期，采用 UTC 时间格式

➢ 证书持有者名称

该字段指定证书持用者的身份

➢ 证书持用者的公钥信息

该字段指定证书持用者的公钥信息

➢ 证书类型

该字段标识证书持用者的设备类型，如 STA、AP、ASU

➢ 扩展

保留字段

➢ 证书颁发者对证书的签名

该字段由证书颁发者 ASU 对证书上本字段以前的所有项进行签名得到

WAI 阶段的主要做的工作就是 ASU 利用证书对 AP 和 STA 进行认证，具体的鉴别流程如图 3-17 所示：

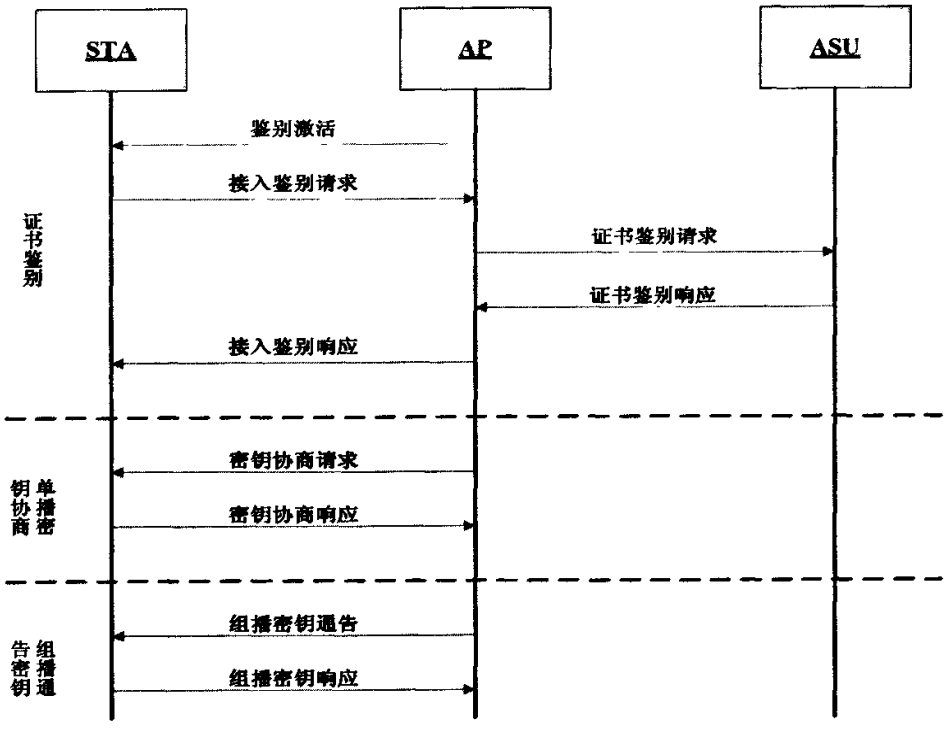

图 3- 17 WAI 鉴别流程图

1、鉴别激活。当 STA 关联或重关联至 AP 时，由 AP 向 STA 发送鉴别激活以启动整个鉴别流程。

2、接入鉴别请求。STA 向 AP 发出接入鉴别请求，即将 STA 证书与 STA 当前系统时间发给 AP。

3、证书鉴别请求。AP 记录鉴别请求时间，然后向 ASU 发出证书鉴别请求，

即将 STA 证书、接入鉴别请求时间、AP 证书及 AP 的私钥对它们的签名构成证书鉴别请求发送给 ASU。

4、证书鉴别响应。ASU 验证 AP 的签名和 AP 证书的有效性，若正确，进一步验证 STA 证书。验证完毕后，ASU 将 STA 证书鉴别结果信息(包括 STA 证书和鉴别结果)、AP 证书鉴别结果信息(包括 AP 证书、鉴别结果及接入鉴别请求时间)和 ASU 对它们的签名构成证书鉴别响应发回给 AP。

5、接入鉴别响应。AP 对 ASU 返回的证书鉴别响应进行签名验证，得到 STA 证书的鉴别结果，根据此结果对 STA 进行接入控制。AP 将收到的证书鉴别响应回送至 STA。STA 验证 ASU 的签名后，得到 AP 证书的鉴别结果，根据该鉴别结果决定是否接入该 AP。

6、密钥协商请求。AP 产生一串随机数据，利用 STA 的公钥加密后，向 STA 发出密钥协商请求。此请求包含请求方所有的备选会话算法信息。

7、密钥协商响应。STA 收到 AP 发来的密钥协商请求后，首先进行会话算法协商，若响应方不支持请求方的所有备选会话算法，则向请求方响应会话算法协商失败，否则在请求方提供的备选算法中选择一种自己支持的算法；再利用本地的私钥解密协商数据，得到 AP 产生的随机数据；然后产生一串随机数据，利用 AP 的公钥加密后，再发送给 AP。

8、组播密钥通告。单播密钥协商成功后，AP 向 STA 发送组播密钥通告分组通告组播密钥。

9、组播密钥响应。STA 接收到组播密钥通告后，检查报文的消息鉴别码，解密组播通告数据得到组播主密钥，并构造组播密钥响应报文发给 AP

密钥协商成功后，STA 与 AP 将自己与对方分别产生的随机数据进行模 2 运算生成会话密钥，就可以利用协商的会话算法通过受控端口进行安全通信了。

3.3.2 WPI

对于单播密钥协商和组播密钥通告后得到的单播和组播密钥，AP 和 STA 利用 KD-HMAC-SHA256 算法进行扩展，将单播主密钥扩展成 48 字节的单播会话密钥，其中第一个 16 字节作为单播加密密钥，第二个 16 字节作为单播完整性校验密钥，后面 16 字节作为 WAI 消息鉴别密钥。将组播密钥通过 KD-HMAC-SHA256 算法扩展为 32 字节的组播会话密钥，其中第一个 16 字节作为组播加密密钥，第二个 16 字节作为组播完整性校验密钥。为了进一步提高通信的保密性，WAPI 还规定，在通信一段时间或者交换一定数量的数据之后，STA 和 AP 之间可以重新协商会话密钥。

采用国家密码管理委员会办公室批准的用于 WLAN 的对称密码算法实现数

据保护，对 MAC 子层的 MSDU 进行加、解密处理。

这个密码算法的具体细节目前还没有公开，而是无偿转让给了包括联想、华为、东软、兴唐等在内的 11 家国内厂商，而其他任何企业要想生产并销售此类设备，必须要先和这 11 家厂商合作。

3.3.3 小结

本节详细解析了 WAPI 的鉴别机制 WAI，接入鉴别流程以及每个实体所要做的工作。

3.4 三种安全机制的比较

IEEE 802.11i 和 WAPI 都是为了弥补最初的 IEEE WLAN 标准 802.11 中的 WEP 安全机制的漏洞而研发的，都解决了 WEP 的遗留问题，而且整体的设计思想也是相近的，但也有很多地方不尽相同，各有优劣：

首先，WAPI 的长处就是不仅认证了 STA，也对 AP 进行了认证。而在 IEEE 802.11i 中我们看到只有对 STA 进行了认证，没有对 AP 的认证

在具体实现中，STA 在关联到 AP 之后，必须与 AP 进行双向身份鉴别。先由 STA 将自己的证书和当前时间提交给 AP，然后 AP 将 STA 的证书、提交时间和自己的证书一起用自己的私钥签名，并将这个签名连同这三部分一起发给 ASU。

所有的证书鉴别都由 ASU 来完成，当其收到 AP 提交来的鉴别请求之后，会先验证 AP 的签名和证书。当鉴别成功之后，进一步验证 STA 的证书。最后，ASU 将 STA 的鉴别结果信息和 AP 的鉴别结果信息用自己的私钥进行签名，并将这个签名连同这两个结果发回给 AP。

AP 对收到的结果进行签名验证，并得到对 STA 的鉴别结果，根据这一结果来决定是否允许该 STA 接入。同时 AP 需要将 ASU 的验证结果转发给 STA，STA 也要对 ASU 的签名进行验证，并得到 AP 的鉴别结果，根据这一结果来决定是否接入 AP。

这样由于 WAI 中对 STA 和 AP 进行了双向认证，因此对于采用“假”AP 的攻击方式具有很强的抵御能力。

但是 IEEE 802.11i 的优点也很明显，就是支持更丰富的认证方式，在 WAPI 中已经明确定义了认证方法，即 WAI。但是由于 IEEE 802.11i 的接入控制采用的是 IEEE 802.1X 协议，而 IEEE 802.1X 利用的是 EAP 协议来进行认证，EAP 的一个最主要特点就是支持多种认证方法，并且很容易扩充，这样，目前 IEEE 802.11i 既支持传统的用户名-密码认证方式(EAP-MD5)，也支持采用证书的认证

方式(EAP-TLS)，而且还可以与现有的移动网络互连，利用 SIM 卡中的信息到 HLR 中去认证(EAP-SIM、EAP-AKA)，然后利用现有的移动系统进行计费，用户使用起来也很方便，而且可以节约网络建设成本。

可以说认证方式的多样灵活是 IEEE 802.11i 相对于 WAPI 最大的优势。

在加密方面，IEEE 802.11i 提供了两种加密机制供选择，一个是 TKIP、另一个是 CCMP。其中 TKIP 是对 WEP 的进一步封装，通过增加 IV 值得范围以及密钥管理方面的改进来解决 WEP 的弱密钥问题。但 TKIP 的某些方面，特别是 Michael 完整性协议公认易受攻击。所以 IEEE 抛开了 WEP，不考虑兼容问题，只关注安全，提出了 CCMP 安全机制。CCMP 机制基于 AES(Advanced Encryption Standard)加密算法和 CCM(Counter－Mode/CBC－MAC)认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。由于 AES 对硬件要求比较高，因此 CCMP 无法通过在现有设备的基础上进行升级实现。所以目前还不是主流应用。

但由于 WAPI 中 WPI 采用的 SSF43 对称加密算法没有公开，所以无从比较 WPI 与 TKIP、CCMP 谁更加安全。

表 3-7 三种安全机制比较

	WEP	IEEE 802.11i	WAPI
认证特征	单向认证	用户和认证服务器之间双向认证，但没有认证 AP	无线用户和接入点(AP)之间的双向公钥证书认证
性能	认证简单，效率高	认证过程复杂	认证过程简单
安全漏洞	认证易于伪造，降低了总体安全性	没有对AP进行认证	无
认证算法	1、开放式认证 2、共享密钥认证	未确定	192/224/256 位的椭圆曲线签名算法
认证安全强度	低	较高	最高
扩展性	低	高	低
加密算法	64 位的 RC4 流加密	1、128 位的 RC4 流加密 2、128 位的 AES 加密	WPI
密钥	静态	动态(基于用户、基于认证、通信过程中动态更新)	动态(基于用户、基于认证、通信过程中动态更新)
密钥安全强度	低	高	高

3.5 本章小结

WLAN 网络的安全已经成为设备厂商和用户共同关注的焦点，也是决定WLAN 发展的主要因素。WEP 作为最初的无线局域网安全机制，已经不能很好的保护无线局域网，IEEE 802.11i 是目前最新的无线局域网安全国际标准。WAPI是我国自主知识产权的无线局域网国家标准，从保护国家信息安全角度来讲，意义深远。

本章，从技术的角度对这三种安全机制进行了深入的比较分析。

第四章 IEEE 802.11i 协议的设计与实现

4.1 AP 中代码总体架构

作为接入设备，AP 必须要有接入认证和安全加密的功能，同时还需具备二/三层转发、网络管理、VLAN 等一系列网络设备的基本功能。

AP 的系统软件结构可以分为驱动、二层转发、TCP/IP 协议栈、功能特性和管理五个部分。驱动部分包括以太网驱动和 WLAN 驱动；二层转发包括二层帧转发、端口隔离、链路完整性、FDB、VLAN、风暴抑制以及端口镜像；功能特性包括 DHCP、路由模块、认证模块、负载均衡等；管理包括命令行、telnet、ftp 上传下载和 SNMP。

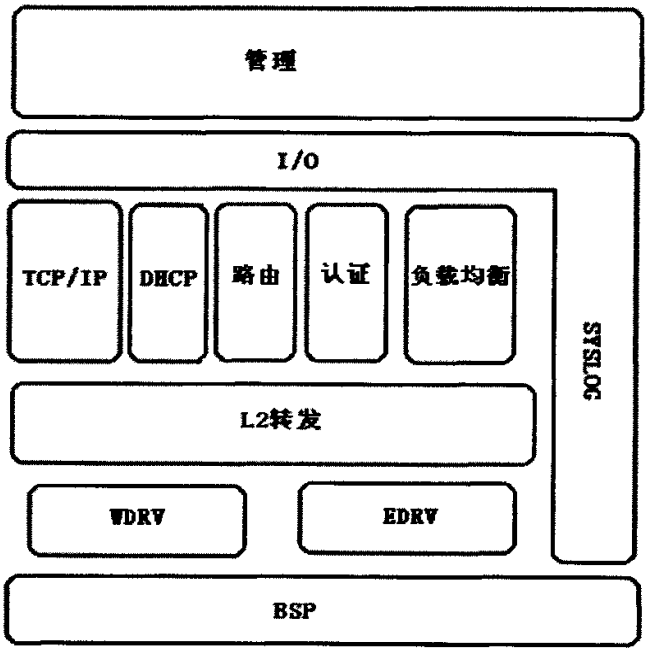

图 4-1 AP 中的系统软件结构

整个系统启动是从 BSP 和驱动开始的，通过 WLAN 驱动使 STA(常见的为带无线网卡的笔记本)与 AP 之间建立起 802.11 连接。在此基础上通过二层转发模块将收到的报文按类型分发到不同的功能模块进行处理。

本论文实现了其中认证模块中 IEEE 802.11i 和 WAPI 协议的功能。

4.2 IEEE 802.11i 软件的总体设计

IEEE 802.11i 在原有的 802.11 标准的基础上定义了加密和认证两方面的内容。加密方面，提出了 TKIP、AES 两种加密标准，为了保证性能我们都用硬件

来实现加密工作。所以软件需要做的工作就是对用户进行身份认证，同时生成并提供正确的密钥给硬件。

4.2.1 系统设计及模块划分

前面我们已经介绍过加入了 IEEE 802.11i 后的 WLAN 连接需要四步。第一步是 802.11 的无线连接建立阶段，这一阶段的作用就相当于建立了一个通道，使 STA 与 AP 之间可以发送认证报文，但是在没有完成认证，生成密钥之前 STA 并不能通过 AP 访问网络，也就是说这个通道只是为认证建立的。第二步就是接入认证阶段，这一阶段的作用是识别合法用户，检验用户是否有权限接入网络；认证通过后进入第三步，第三步的作用就是生成加密密钥，之后进入第四步，就是数据传输阶段，也就是 STA 可以通过 AP 来访问网络了，而且 STA 与 AP 之间传输的数据是利用第三步生成的密钥加密的。

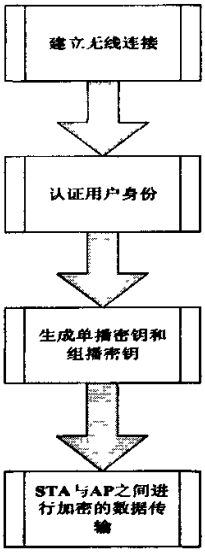

图 4-2 IEEE 802.11i 总体流程

对应于图 4-2 中的四个步骤，我们将 IEEE 802.11i 软件分成主要的四个模块：连接建立模块、接入认证模块、密钥管理模块和加解密模块。其中连接建立模块由无线网卡中自带的 WLAN 驱动模块(WDRV)完成，本系统硬件中我们采用的是 Athero 无线网卡；加解密模块是由硬件完成。所以软件中要完成的主要就是接入认证模块和密钥管理模块以及相关的一些异常处理部分、日志部分和命令行模块。

4.2.2 各功能模块设计

4.2.2.1 接入认证模块

IEEE 802.11i 的接入认证主要是引入了 IEEE 802.1X 协议来实现，所以本模块主要是实现了 802.1X 协议。802.1X 是一个基于端口的访问控制协议，端口可以是物理端口，比如以太口；也可以是逻辑的，比如用户设备的 MAC 地址。在 802.1X 协议中端口分为两类，一类是受控端口，一类是非受控端口，受控端口又分授权和非授权两种状态，默认是非授权状态。我们用非受控端口来传输认证报文，802.1X 中使用的是 EAP(可扩展的认证协议)协议来进行认证，当认证通过且密钥已经协商完成后将受控端口设为授权状态，开始数据传输。

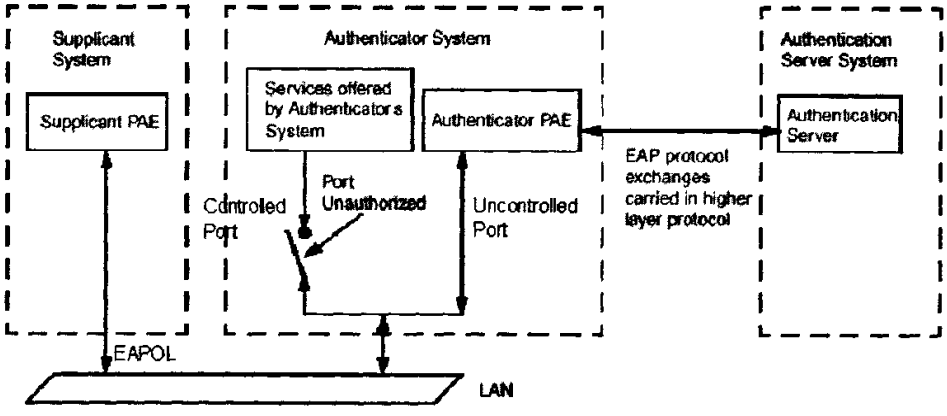

图 4-3 IEEE 802.1X 协议体系结构

由图 4-3 我们看到 802.1X 协议中共有 3 个角色：Supplicant、Authenticator 和 Authentication Server System。其中 Authenticator 是我们在 AP 中要实现的接入认证模块。

从认证的角度来讲 AP 是 STA 和 AS(认证服务期)之间的桥梁，也就是说 AP 既要与 STA 中的 Supplicant 通信也要与 AS 通信，所以我们在认证模块中定义了两个子模块——认证者模块(Authenticator)和认证服务器的客户端模块，前者用来和 STA 通信，后者用来和认证服务器通信。因为通常情况下我们使用的都是 Radius 服务器，因此我们也将认证服务器客户端模块叫做 Radius 客户端模块(Radius Client)。

同时由于 AP 支持多种认证方式，为了便于管理和扩充，在 AP 的认证模块中还有一个子模块——NAS(Network Access System)，用来管理用户数据和统一多种认证方式及计费。同时也作为 Authenticator 模块与 Radius Client 模块之间的一个桥接模块。

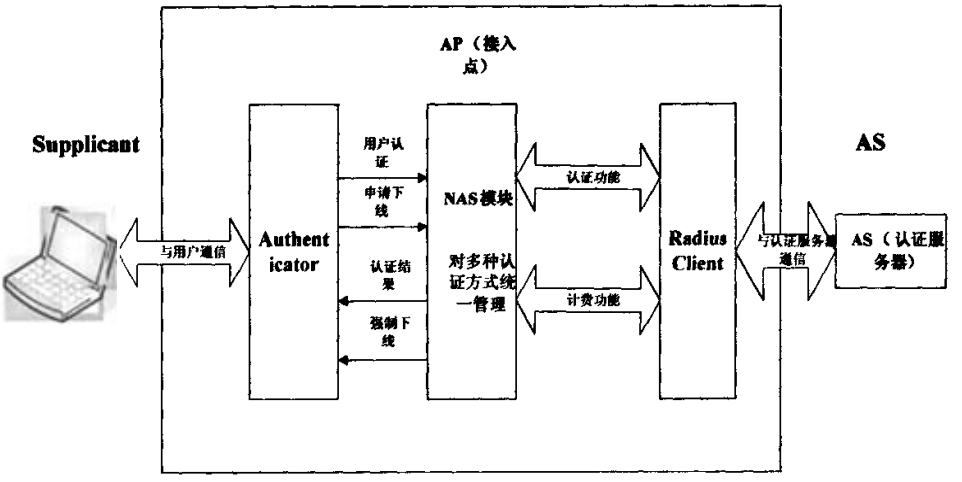

图 4-4 IEEE 802.1X 认证模块结构

这样我们将接入认证模块再次分为 Authenticator、NAS 和 Radius Client 三个子模块。

1.Authenticator 子模块

802.1X 中 Authenticator 与 Supplicant 之间的认证采用的是 EAP 协议，就 EAP 本身而言支持多种认证方法，并且有良好的扩展性，在本系统中我们实现的是 EAP-SIM 认证。因为 EAP-SIM 利用了 SIM 卡中的信息进行认证，这样对用户而言不用再单独申请 WLAN 的帐户，运营商也可以有效利用现有的 2.5G 网络对 WLAN 的用户进行认证和计费。Supplicant 与 Authenticator 之间的 EAP-SIM 认证流程如图 4-5 所示：

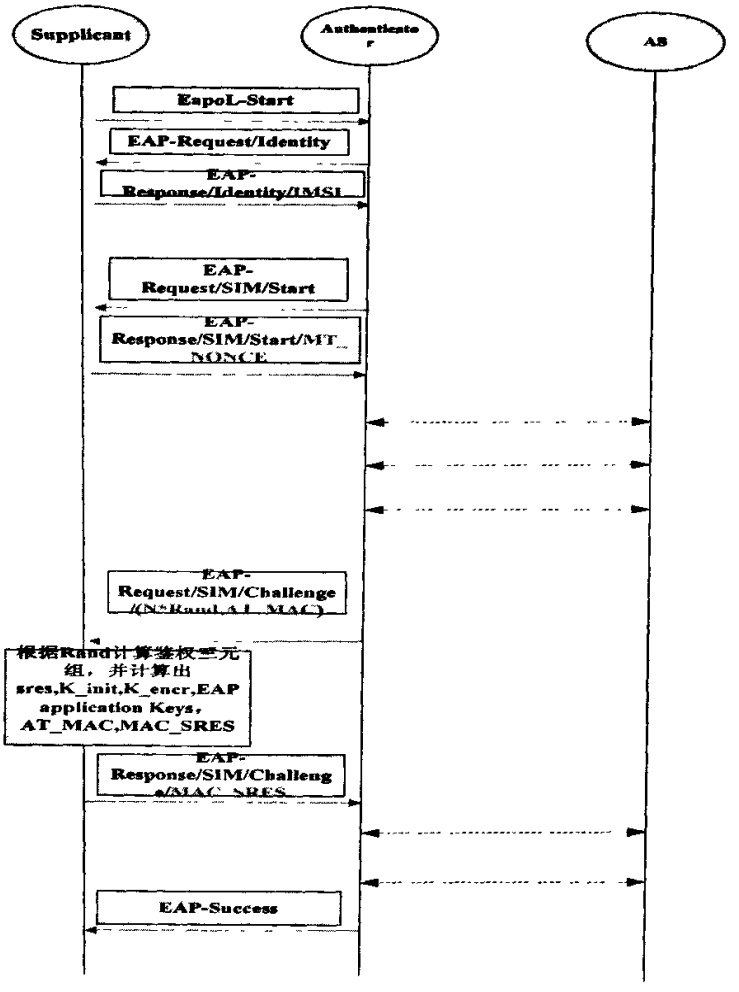

图 4-5 Supplicant 与 Authenticator 之间的 SIM 认证流程

由图 4-5 我们看到 Supplicant 和 Authenticator 之间的通信在流程方面是按照 EAP-SIM 认证协议的要求来进行的，同时发送的报文则利用的是 EAPoL(EAP over LAN)报文，格式如表 4-1 所示：

表 4-1 EAPoL 报文格式

Protocol Version (1B)	Packet Type (1B)	Packet Body Length (2B)	Packet Body

表 4-2 EAPoL 报文各字段取值及含义

EAPoL 字段	取值	含义
Protocol Version	1	当前使用的是 1 版本
Packet Type	0	表示 Packet Body 中是 EAP 报文
	1	表示这个报文是 EAPoL-Start 报文

	2	表示这个报文是 EAPoL-Logoff 报文
	3	表示这个报文是 EAPoL-Key 报文
Packet Body Length		表示 Packet Body 中内容的长度
Packet Body		根据 Packet Type 的不同而不同

当 Packet Type 取值为 1 或 2 时，Packet Body 字段为空。当 Packet Type 字段取值为 0 时，表示 Packet Body 中是 EAP 报文，EAP 报文的格式如表 4-3 所示：

表 4-3 EAP 报文格式

EAP 报文字段	取值	含义
Code(1B)	1	表示这是个 EAP-Request 报文
	2	表示这是个 EAP-Response 报文
	3	表示这是个 EAP-Success 报文
	4	表示这是个 EAP-Failure 报文
Identifier(1B)		每个 EAP 报文的唯一标识号
Length(2B)		表示整个 EAP 报文的长度
Data		这个字段分为两部分一个是 Type,另一个是 Data，Type 表示后边 Data 字段的类型。

在实现流程方面，Authenticator 模块中设计了一个状态机 ASM(Authenticator State Machine)来使图 4-5 中的流程顺利进行，也就是说每收到一个报文或来自其他模块的消息时会使状态机的状态发生轮转，在新进入的状态的处理函数中按照 EAP-SIM 协议中定义的流程发送响应报文。在 ASM 状态机中，为 Authenticator 定义了 7 个状态：

1.INITIALIZE：来做一些初始化工作，给定时器、计数器清零等。

2.DISCONNECTED：在这个状态下发送 EAP-Fail 报文给 Supplicant 报文。

3.CONNCETING：在这个状态下 EAP-Request 报文给 Supplicant 报文。

4.AUTHENTICATING：收到 EAP-Response\Identity 报文后，进入这个状态，并将这个 EAP-Response\Identity 封装成消息发送到 NAS 模块，同时将全局变量 AuthStart 置 1 来启动与 AS 之间的认证。

5.AUTHENTICATED：如果用户通过 AS 认证后，就转到这个状态下，在这个状态下向 Supplicant 发送 EAP-Success 报文。

6.ABORTING：在 AUTHENTICATING 状态下收到了 EAPoL-Start、EAPoL-Logoff 或认证超时时进入这个状态。

7.HELD：认证失败后进入这个状态，在这个状态下需要等待 60s，系统会开始重新认证，在这 60s 内系统不会对任何报文进行回复。

ASM状态机如图4-6所示：

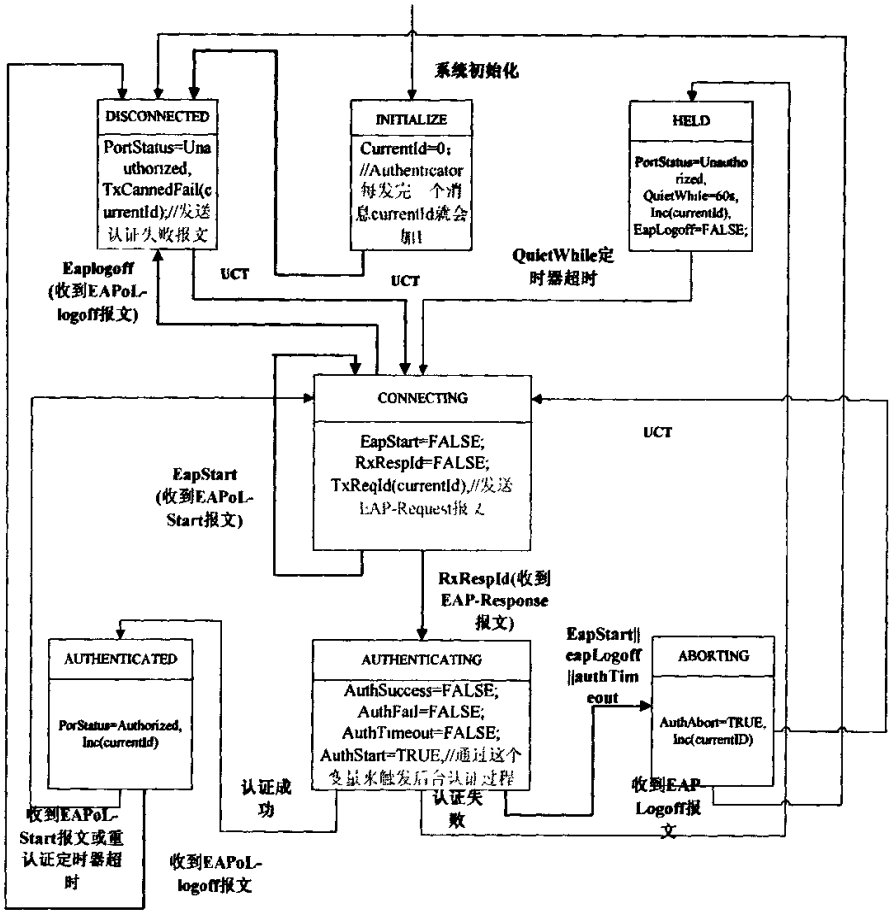

图 4-6 ASM状态机

也就是说在Authenticator模块，每收到一个EAP认证消息，都要首先判断状态机的状态，然后再进行处理。同一个消息，当ASM处于不同状态的时候处理函数是不同的，而具体的处理方法是按照EAP-SIM认证协议中的定义来进行的，即论文用ASM状态机定义了对EAP报文的处理流程。

但从图4-4中看到Authenticator模块连接Supplicant和NAS两个模块，所以Authenticator模块既要处理从Supplicant发送过来的EAP认证报文；又要处理NAS模块以消息的形式转发过来的，AS发送的对用户的认证报文。除了认证报文以外，Authenticator模块还要处理来自时钟模块、命令行模块的消息。因此Authenticator模块主要处理四类消息：

来自Supplicant的认证报文；

来自NAS模块的认证消息，消息中是AS发送过来的认证报文；

来自时钟模块的消息；

来自命令行模块的消息；

所以 Authenticator 模块在收到消息后，首先判断消息类型，如果是来自 Supplicant 模块和 NAS 模块的认证消息就去触发 ASM 状态机，按照状态机的流程进行处理，如果是来自时钟模块或命令行模块的消息，再分别调用各自的处理函数。Authenticator 模块对消息的总体处理流程如下图 4-7 所示：

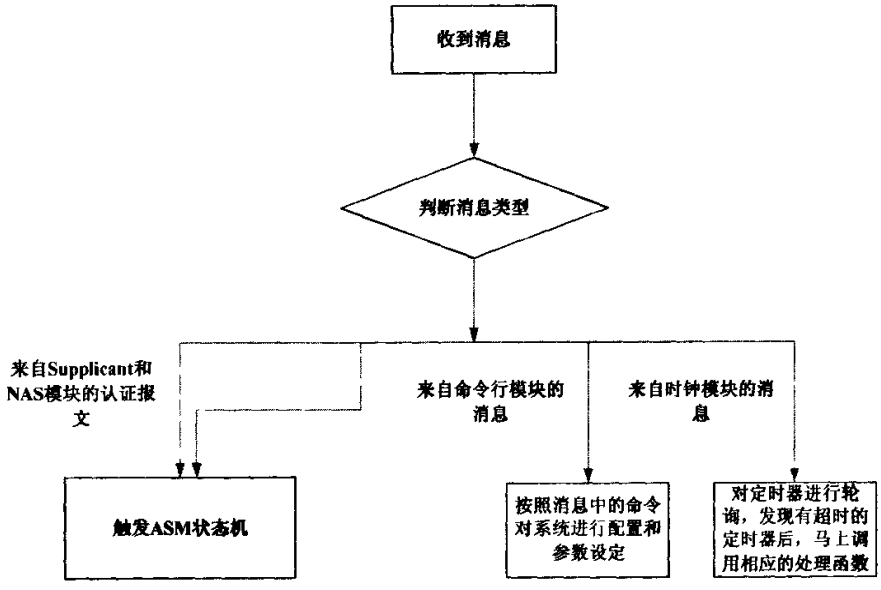

图 4-7 Authenticator 模块消息处理流程

2.Radius Client 子模块

Radius Client 模块是用来和 Authenticator Server 通信的，在 EAP-SIM 认证中，Radius Client 模块和 AS 之间的报文流程如图 4-8 所示：

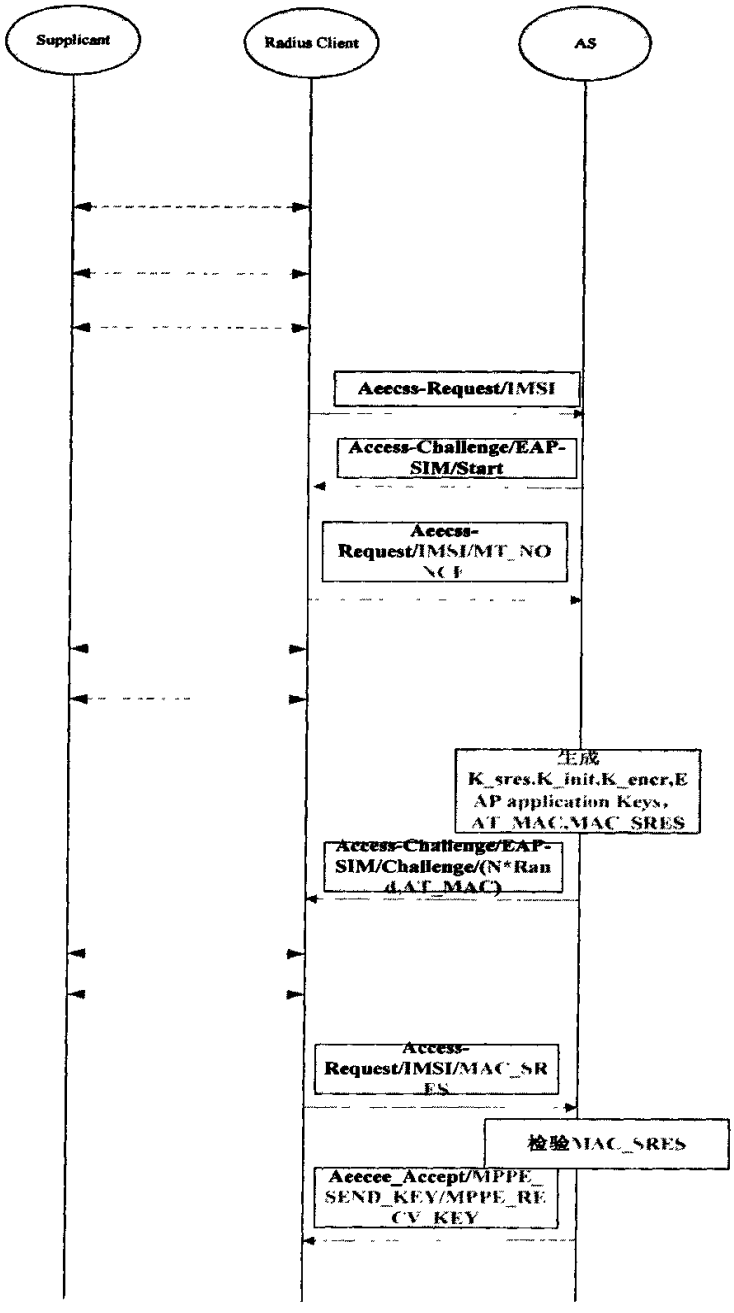

图 4-8 Radius Client 与 AS 之间的认证流程

Radius Client 和 AS 之间的通信利用的是 Radius 协议，Radius 协议的报文格式如表 4-4 所示：

表 4-4 Radius 报文格式

Code (1B)	Identifier (1B)	Length (2B)	Authenticator (16B)	Attributes

表 4-5 Radius报文各字段取值及含义

字段	取值	含义
Code	1	表示报文是 Access-Request 报文
	2	表示报文是 Access-Accept 报文
	3	表示报文是 Access-Reject 报文
	11	表示报文是 Access-Challenge 报文
Identifier		这个字段是用来帮助匹配请求和回复的，如果是重传的包，值不变。
Length		它表示整个 RADIUS 包的长度，如果收到的报文比 length 中说明的值的短，则这个包会被丢弃。Length 的最小值是 20，最大是 4096。
Authenticator		不同的报文类型有不同的 Authenticator。 在 Access-Request 包中，Authenticator 的值是一个 16 字节的随机数，这个值应该是不可预计和唯一的。 在 Access-Accept, Access-Reject, and Access-Challenge 的报文中的 Authenticator 叫做 Response Authenticator。 ResponseAuthenticator=MD5(Code+ID+Length+RequestAuth+ responseAttributes+shareSecret);
Attributes		Radius 协议的属性字段是 Radius 协议最有特色的字段，它使 Radius 协议可以很容易的扩展，具体格式见表 4-6

表 4-6 Radius协议属性字段的格式

Type(1 B)	Length(1 B)	Value

由于篇幅所限，我们这里只介绍两种属性的 Type，也是本系统中最常见的取值，Type=79，表示 Value 中封装的是 EAP 报文，这样 NAS 模块就可以提取出 EAP 报文然后以消息的形式发送给 Authenticator 模块。Type=26 时，表示 Value 域中是 Vendor-Specific 信息，即厂商自己定义的信息，系统用这个属性将认证成功后 AS 为密钥管理阶段生成的主密钥（PMK，Private Master Key）发送给 AP。Length 表示整个属性域的长度。

这个模块主要的作用是将 Authenticator 得到的用户认证信息发送给 AS 进行认证，同时接收 AS 发送的 Radius 认证报文,并发送给 Authenticator 模块。为了

实现这种后台认证功能，与 Authenticator 模块类似，系统中定义了一个状态机 BASM(Backend Authentication State Machine)来实现这一功能。

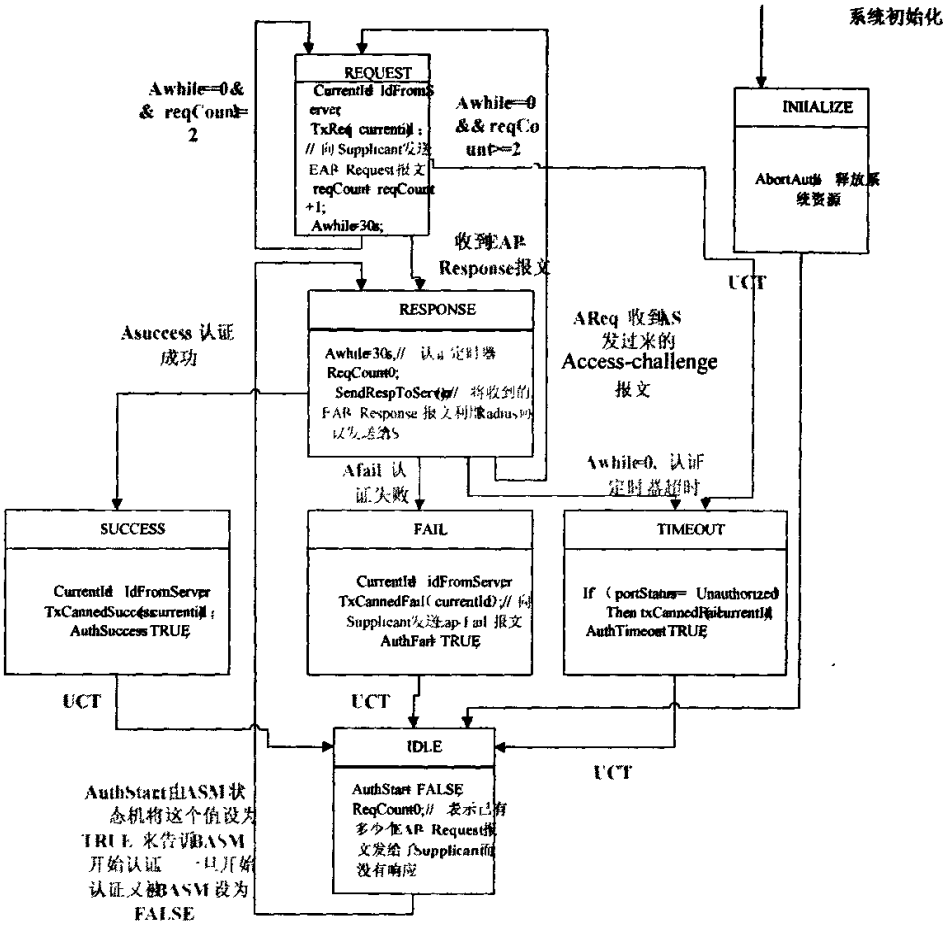

图 4-9 BASM 状态机

这个状态机是由收到 Supplicant 发送过来的 EAP-Response\Identity，即用户名报文后，ASM 状态机进入 AUTHENTING 状态，将全局变量 AuthStart 设为 True 来触发的。但是，这个模块与 Authenticator 之间还有一个 NAS 模块相桥接，也就是说 Radius Client 模块是与 NAS 模块直接通信的，在这里只是为了认证流程的连续所以把这个模块放在了 Authenticator 模块之后来介绍。也就是说 NAS 将要发送给 Radius 服务器的报文封装成 Radius 报文格式以消息的形式发送给 Radius Client 模块，然后由 Radius Client 模块统一处理与 AS 之间的通信，报文处理流程如图 4-10 所示：

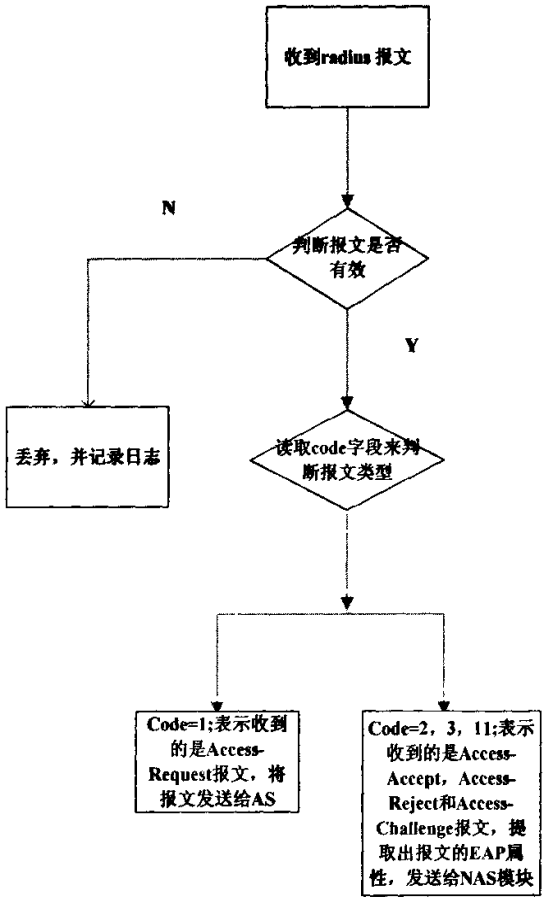

图 4- 10 Radius Client 模块报文处理流程

3.NAS 子模块

作为管理用户数据和统一认证流程的模块，NAS 是整个认证体系里的中枢模块。它主要的工作就是循环从消息队列中取出消息，并对消息进行处理。主要处理的消息有四类：各类认证模块发送过来的消息，Radius Client 模块发送过来的消息，命令行模块发送过来的消息，定时器发送过来的超时消息。其中最主要的就是处理 Authenticator 模块和 Radius Client 模块发送过来的消息。对于 Authenticator 模块发送过来的消息，要把它封装成 Radius 报文格式，然后发送给 AS，对于 Radius Client 发送过来的消息，要提取出 Radius 报文的属性字段，然后发送给 Authenticator 模块。

主要消息处理流程如图 4-11 所示：

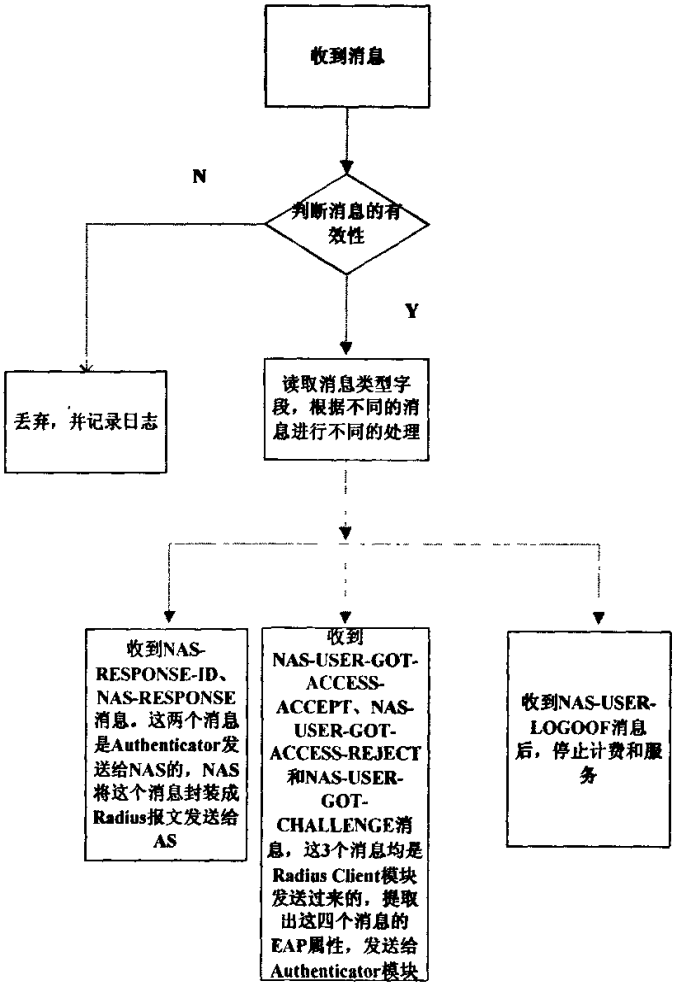

图 4-11 NAS 模块主要消息处理流程

4.2.2.2 密钥管理模块

密钥管理模块的主要功能是生成数据传输阶段所使用的单播加密密钥和组播加密密钥。对应于图 4-2 中的第三个阶段，当接入认证模块收到 AS 发送过来的 Radius-Access-Accept 报文后，即认证成功后会启动密钥协商过程。且在 Radius-Access-Accept 报文的 Attributes 字段中会携带一个 type=26 的属性值，这个属性值中携带的是 AS 发送过来的主密钥信息(PMK，Private Master Key)。而密钥管理模块就是从这个 PMK 开始生成单播密钥和组播密钥的。整个密钥协商过程就是密钥管理模块与 Supplicant 之间通过交互 EAPoL-Key 报文实现的。

在表 4-1 中介绍过 EAPoL 报文的格式，当 EAPoL 报文中的 Packet Type=3 时，表示后边 Packet Body 字段是 EAPoL-Key 报文，EAPoL-Key 报文的格式如表 4-7 所示：

表 4-7 EAPoL-Key报文格式

Descriptor Type(1B)	
Key Information (2B)	Key Length(2B)
Replay Counter(8B)	
Key Nonce(32B)	
EAPoL-Key IV(16B)	
KeyRSC(8B)	
KeyID(8B)	
KeyMIC(16B)	
Key Material Length(2B)	Key Data(nB)

表 4-8 EAPoL-Key报文中各字段的含义

字段	含义
Descriptor Type	表示密钥类型，1 表示 RC4 密钥
Key Information	这个字段包含着各种与握手过程相关的控制位
Key Length	这个字段表示目标密钥的长度，即四次握手时表示 PTK 密钥的长度，二次握手时表示 GTK 密钥的长度。
Replay Counter	由 Authenticator 在发送每个握手报文时加 1(四次握手报文重传不加，二次握手报文重传要加 1，Supplicant 返回同样的值。
Key Nonce	保存四次握手中的 Anonce 或 Snonce，当不需要这两个值时清 0。
EAPoL-Key IV	密钥向量，对于 PMK 无作用，清零；对于 GMK，可以用全局计数器初始化，然后每次加 1。
KeyRSC	被安装的密钥(TK)的 RSC(receive sequence counter)，只在四次握手中的第三个报文中和二次握手中的第一个报文中使用，用于同步重传状态。
KeyID	密钥 ID，置 0。
KeyMIC	对整个报文进行签名，从 Key Descriptor Version 位开始，Key MIC 置 0，Key Data 已经加密。
Key Material Length	Key Data 的长度，对于 PMK，报文 1 和 4 该值为 0，报文 2 和 3 是 Key Data 的长度；对于 GMK，该值与 Key Length 相同。
Key Data	携带密钥传递过程中的一些附加数据，包括 RSN IE、Group Key(s)、STAKey(s)、PMKID(s)或其

	它用户自定义的信息。

密钥管理模块的处理流程图：

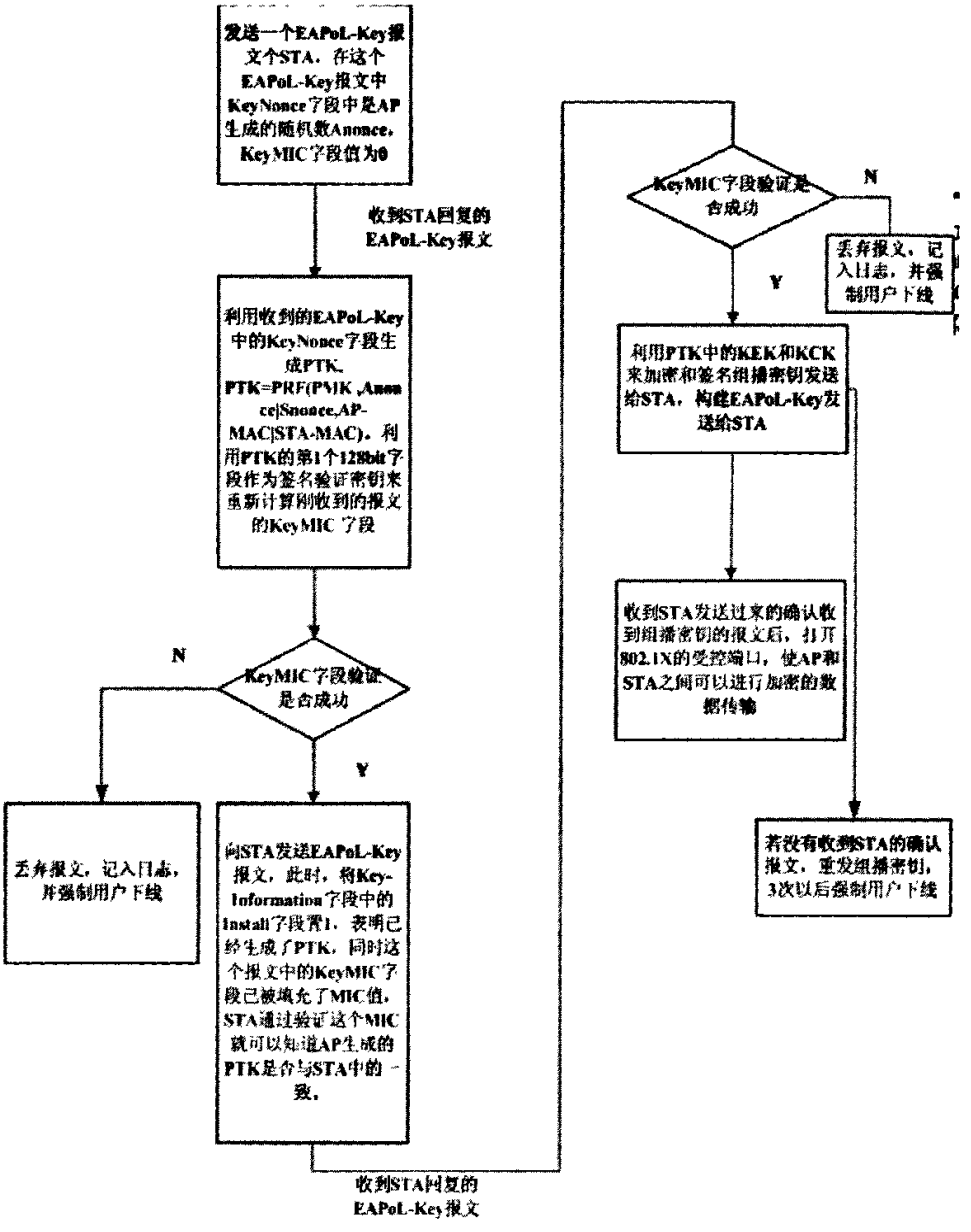

图 4-12 密钥管理模块处理流程图

4.2.2.3 命令行模块

命令行模块主要的功能是通过界面配置，来设置系统参数，关于认证主要设计的命令有：

表 4-9 802.11i系统中的主要配置命令

配置命令	作用
Authtype [NONE||DOT1X|802.11i-PSK|802.11i]	设置认证方式
Ciphertype [WEP|TKIP|AES|AUTO]	设置加密算法
GroupKeyUpdateInterval <0-30>	设置组播密钥更新时间
PassphraseKey [PassphraseKey]	设置共享密钥(十六进制)
Passphrase [Passphrase]	设置共享密钥(ASCII)
Preauth [enable|disable]	启动/关闭预认证功能
Tx-Period	设置 AP 报文重传等待时长
ServerTimeout	设置等待服务器认证时长
Clear	清楚配置命令
setting-enable	执行配置的命令
Show Authtype	显示认证方式
Show Wpaversion	显示支持的 WPA 版本
Show Ciphertype	显示加密算法
Show GroupKeyUpdateInterval	显示组播密钥刷新时间

4.2.2.4 日志模块

在系统运行过程中，需要将收到的每一个报文和状态变化记入日志，以便系统维护。我们可以通过命令 Show Syslog 来查看日志。

4.3 系统实现

本系统是在 VxWorks 下利用 c 语言编写的，满足 IEEE std 802.11i/D 7.0,October 2003 标准

4.3.1 接入认证模块

本系统中接入认证模块主要实现的功能就是对 EAP-SIM 用户进行认证，首先通过与用户进行 EAP 通信来获取用户的认证信息，在将这些信息进行验证和处理后发送到认证服务器。同时接入认证模块也与本系统内部及外部的多个模块有接口，接口之间都是通过消息来进行通信的。在这个过程中主要要处理以下几类消息：

1.来自用户侧(STA)的报文

2.来自认证服务器(AS)的报文

3.来自命令行的消息

4.来自时钟模块的消息

5.来自其他模块的命令，如底层驱动发送的端口控制命令

其中第 1 和 2 类消息我们分别通过接入认证模块的 Authenticator 子模块和 Radius Client 子模块来处理。主要处理函数是 EAPoL_rcv_handle()和 EAPoR_rcv_handle()。

EAPoL_rcv_handle()函数处理得是用户侧发送过来的报文，如 EAPoL-Start、EAP-Response 报文。

EAPoR_rcv_handle()函数处理的是认证服务器发送过来的报文，如 Radius_Access_Challenge、Radius_Access_Reject、Radius_Access_Accept 报文。处理流程在设计中已经有了详细的介绍。

对于来自命令行的消息我们全部都是在文件 cli.c 中实现的。对于每一个命令，都对应一个函数来进行实现，其中主要的有：

表 4-10 与命令行模块的主要接口消息及处理函数

命令行消息	实现函数	功能
DOT1X_CLI_CMD_SetDot1xQuietPeriod	dot1x_SetQuietPeriod()	设置ASM状态机中的Quiet状态的等待时长
DOT1X_CLI_CMD_SetDot1xtxPeriod	dot1x_SettxPeriod()	设置发送报文的时间间隔，即发送一个报文多久没有回复后重发
DOT1X_CLI_CMD_SetDot1xservertimeout	dot1x_Setservertimeout()	设置服务器认证超时时间
DOT1X_CLI_CMD_SetDot1xsupptimeout	dot1x_Setsupptimeout()	设置间隔多久向 Supplicant 重发认证请求信息
DOT1X_CLI_CMD_SetDot1xmaxreq	dot1x_SetmaxReq()	设置向 Supplicant 重发 EAP-Request 报文的最多次数
GroupKeyUpdateInterval	apCfgGroupKeyUpdateIntervalSet()	设置组播密钥更新时间间隔

对于来自时钟模块的消息是通过 timer_check()函数来处理的，这个函数每 1s 被调用一次，然后将接入认证模块中的每一个定时器都减去 1，如果哪个定时器等于 0 了，就说明等待超时，在调用相应的处理函数进行处理。

表 4-11 与时钟模块的主要接口及处理函数

超时的定时器	调用的处理函数
txWhen	Try_Trigger_ASM_ConnectingTimeOutEvent()

quietWhen	Try_Trigger_ASM_HeldQuietTimerEvent()
aWhile	Try_Trigger_BASM_ResponseaWhileTimeoutEvent()
reKeyWhen	groupkeysm_trans()

4.3.2 密钥管理模块

密钥管理模块生成了单播报文的加密密钥和组播报文的加密密钥，并对组播密钥根据配置进行定时更新。

在密钥管理模块中设计了两个状态机 PTKSM 和 GTKSM，分别对应单播密钥的“四次握手”流程和生成组播密钥的“二次握手”。

PTKSM 状态机中主要有 ST_INITIALIZEPTK、ST_INITPMK、ST_PTKSTART、ST_PTKINITNEGOTIATING 和 ST_PTKINITDON 五个状态。

表 4-12 PTK 状态机中主要状态与函数实现的对应关系

状态	对应的函数	功能
ST_INITIALIZEPTK	statePTK_INITIALIZEPTK()	这是一个初始化函数，主要的作用是给所有的定时器和计数器清零，并给一些全局变量赋值。
ST_INITPMK	statePTK_INITPMK()	从收到的 Radius_Access_Accept 报文中提取出 PMK。
ST_PTKSTART	statePTK_PTKSTART()	构建并发送“四次握手”的第一个报文。
	ANonceCalc()	计算四次握手第一个报文中的随机数。
ST_PTKINITNEGOTIATING	PTKGenerate()	生成 PTK

发送组播密钥主要利用的函数是：

stateGROUP_REKEYNEGOTIATING()：构建并发送“二次握手”的第一个报文。

stateGROUPKEY_SETKEYSDONE()：将组播密钥保存在密钥列表中。

4.3.3 命令行模块

命令行模块将用户通过命令行配置的参数和信息下发到配置文件中，或给全

局变量赋值。

利用函数 DEFUN(“命令”,“设置的参数”)得到对应命令的设置参数，之后再根据命令调用函数进行处理。

4.3.4 日志模块

利用函数 HOS_SysLog(CHAR iLog_Type, CHAR iLog_Level, CHAR * szFmt, ...)将要记录的信息写入日志文件。

4.4 系统测试

1. 测试用例 1：

在 AP 下我们进行如下配置：

SSID TEST \\表示本无线局域网的名称叫“TEST”

Authtype 802.11i \\表示 AP 采用的是 IEEE802.11i 作为安全认证协议

CipherType TKIP \\表示 AP 采用的加密算法是 TKIP

GroupKeyUpdateInterval 3600 \\表示组播密钥每 3600s 更新一次

IP 10.23.11.100 \\表示 AP 的 IP 地址

Add server in VLAN 1 serverIP 10.23.11.249 \\表示 IP 地址为 10.23.11.249 的机器是认证服务器

因为目前国内还没有运营商开通基于 EAP-SIM 认证的 WLAN，所以我们只能通过软件来模拟客户端，我们使用的是 linux 下的开源代码 wpa-supplicant-0.3.8 来模拟 SIM 客户端，首先定义配置文件 sim.conf：

```
network={
    ssid = “ TEST ”                          // 认证客户端名称
    key_mgmt = IEEE 80211i                   //认证密钥管理协议类型
    eap = SIM                                //eap 认证类型 eap-sim
    identity = “ 146000932312345@cmcc.com ”  // 用户帐号，即模拟的 IMSI
        }
```

然后在 linux 系统下运行客户端程序 wpa_supplicant-0.3.8，来开始一次基于 EAP-SIM 认证的 WLAN 连接。

测试结果是可以通过 AP 访问 Internet，符合预期结果。我们通过抓包工具可以看到整个报文交互流程：

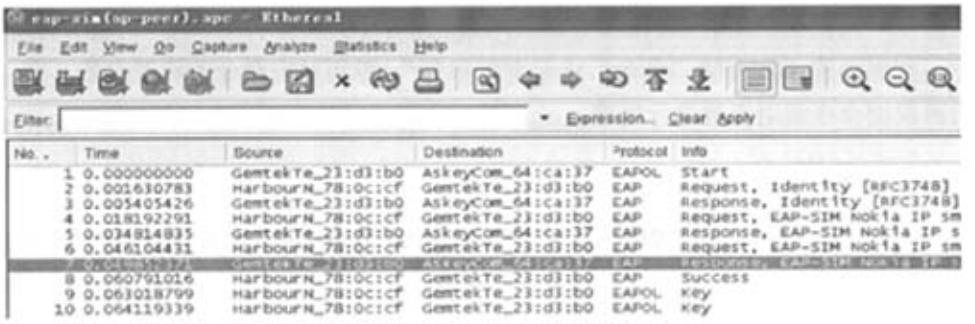

图 4-13 AP 与 STA 间 EAP-SIM 认证抓包结果图

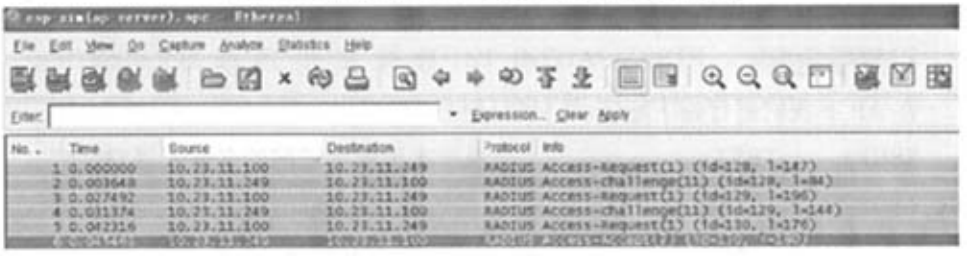

图 4-14 AP 与 AS 间 EAP-SIM 认证抓包结果图

图 4-13 中 Gemteket_23：d3：b0：是客户端的无线网卡的 MAC；AskeyCom_64：ca：37 和 HarbourN_78：0c：cf 均表示 AP 的无线网卡，其中 HarbourN_78：0c：cf 是 AP 的逻辑 MAC， AskeyCom_64：ca：37 是 AP 中真正无线网卡的 MAC。图 4-14 中， 10.23.11.100 是 AP 的 IP 地址，10.23.11.249 是 AS 的 IP 地址，我们看到 AS 向 AP 发送了 Radius_Access_Accept 表示认证成功的报文，AP 也向 STA 发送了 EAP-Success 报文。同时图 4-13 中 EAP-Success 报文后边的 EAPoL-Key 报文就是“四次握手流程”中的前两个报文，因为后两个报文以及“二次握手”均以利用 PTK 中的 KEK 和 KCK 加密签名，所以在空中抓包无法判断出是 EAPoL-Key 报文。

2．测试用例 2：

在测试用例 1 的基础上我们改动一下模拟 SIM 客户端的配置文件，我们将 identity 中的只改动一位，如将第一位改为 2，再进行一次连接测试。

客户端的配置文件 sim.conf：

```
network={
    ssid = " TEST "                          // 认证客户端名称
    key_mgmt = IEEE 80211i                   //认证密钥管理协议类型
    eap = SIM                                //eap 认证类型 eap-sim
    identity = " 246000932356789@cmcc.com "  // 用户帐号，即模拟的 IMSI
        }
```

AP 上的配置不变，我们发现测试结果是认证失败，符合预期结果，这是因

为在 AS 上没有新的 identity 的注册信息。

3.测试用例 3：

在测试用例 1 的基础上，我们改动 AP 的配置，将认证方式改为 PPPoE,这样 AP 的配置如下：

SSID TEST

Authtype PPPoE

CipherType TKIP

GroupKeyUpdateInterval 3600

IP 10.23.11.100

客户端的配置不变，发起连接后提示认证方式不匹配，符合预期结果。

4.5 本章小结

IEEE 802.11i 是目前最新的 WLAN 安全国际标准，有效解决了 WEP 遗留的安全问题，有力的保障了无线局域网的安全。IEEE 802.11i 主要是在两方面对 WEP 进行了改进，一个是引入了 IEEE 802.1X 协议进行接入认证；另一个就是增加了密钥管理部分。本节就这两个部分进行了设计与实现说明。

第五章 WAPI协议的设计与实现

WAPI作为我国自主研发的无线局域网安全认证协议，自诞生之日起就受到了国内外的广泛关注，也得到了国家的大力扶持。但是到目前为止，WAPI在产业化应用方面一直进展缓慢。在本次的“WLAN安全项目”中，要求实现WAPI协议的目的就是推动WAPI应用的发展。本论文在AP中实现了WAPI协议，同时为了测试，也实现了WAPI的客户端和认证服务器的Demo。

但是由于WAPI协议本身还有很多有待完善的地方，在认证方式上还缺乏扩展性，缺少异常下线检测机制以及计费机制等运营级网络所必需的特性，所以系统只是简单的实现了认证的基本功能。

5.1 系统设计及功能模块划分

作为WLAN的安全认证标准WAPI与其他的标准一样，也是分为认证和加密两部分，认证部分是WAI(WLAN Authentication Infrasturcture)，加密部分是WPI(WLAN Privacy Infrastructure)。由于WPI使用的算法是采用我国国家密码管理委员会办公室批准的用于WLAN的对称密钥算法，且这一算法细节目前并没有公开，所以关于WPI的部分我们只能购买相关厂商的加解密芯片或者Lib库。因此软件部分我们实现的是WAI部分，这一部分完成的功能是验证用户的身份，若是合法用户那么还要与用户协商出单播和组播密钥。

WAI认证的总体结构与802.1X非常相似，依然有三个角色，分别是：AE(Authentication Entity)鉴别器实体，通常在AP中实现，用来为鉴别请求者在接入网络之前提供鉴别操作；ASUE(Authentication Supplicant Entity)鉴别请求者实体,通常在STA客户端中，用来请求通过鉴别服务单元的鉴别；ASE(Authentication Service Entity)鉴别服务实体，通常在ASU(鉴别服务单元)中，为AE和ASUE提供相互鉴别。这三个角色共同组成了WAI鉴别系统结构。

从图5-1中我们看到AP提供两种访问LAN的逻辑通道，定义为两类端口，即受控端口和非受控端口。AP提供STA连接到鉴别服务单元（ASU）的端口（非受控端口），确保只有通过鉴别的STA才能使用AP提供的数据端口（受控端口）访问网络。也就是说STA在通过AP访问网络之前，必须先通过AP提供的非受控端口到ASU中的ASE实体去认证，只有ASUE和AE均通过了ASE的认证，AP的受控端口才会得到授权。同时认证成功后AE与ASUE之间还要协商单播和组播密钥，这样可以使AE与ASUE之间的通信是密文的。只有鉴别成功并生成密钥之后，ASUE才可以通过AP的受控端口访问Internet。

根据WAI协议的这种角色划分，我们在代码中也同样按照这个结构来划分

模块：执行 ASUE 功能的 Wapi_asue 模块、执行 AE 功能的 Wapi 模块和执行简单 ASU 功能的 Waiae 模块。

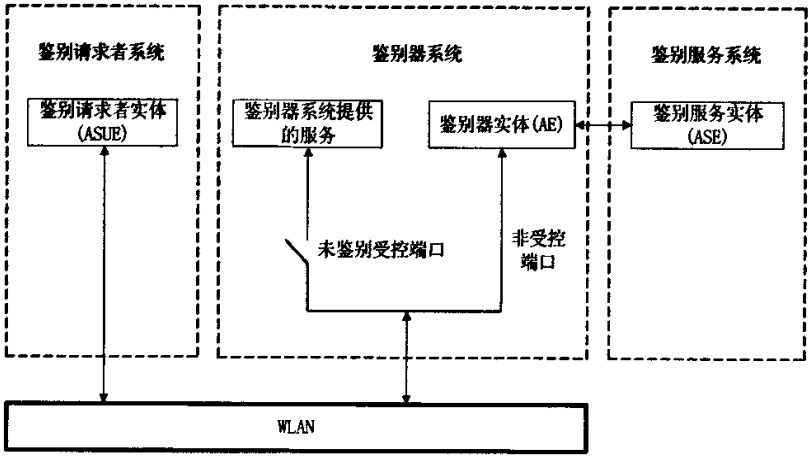

图 5-1 WAI 鉴别系统结构

同时我们也要知道 WAPI 只是安全认证协议，那么在进行认证之前也要建立 IEEE 802.11 的 WLAN 连接，当 AP 与 STA 关联成功之后，AE 将向 STA 中的 ASUE 模块发送鉴别激活报文，以此来启动整个鉴别过程，具体流程如图 5-2 所示。

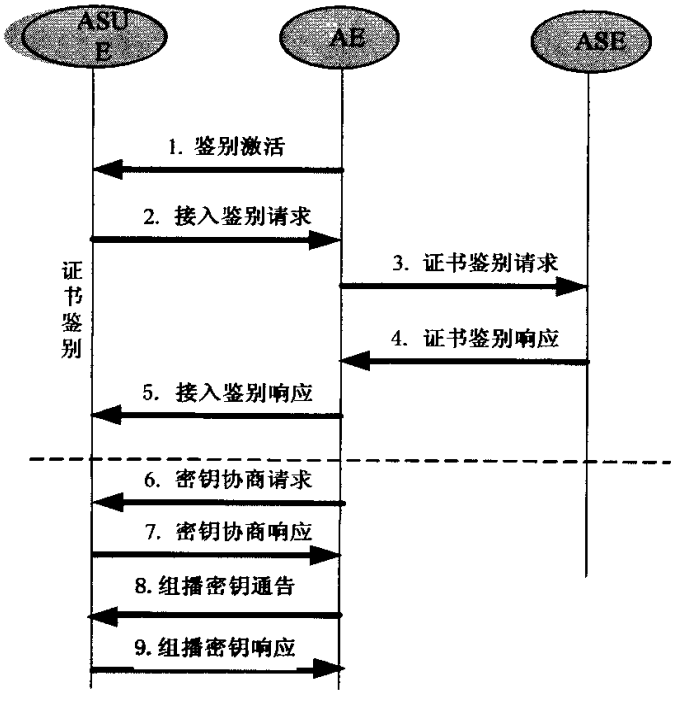

图 5-2 WAI 鉴别流程

5.2 各功能模块设计

在 Wapi_asue、Wapi 和 Wapi_asu 这三个模块中，只有 Wapi 是 AP 中的模块。而 Wapi_asue 和 Wapi_asu 一个是客户端模块，一个是服务器模块，均是为了测试的目的编写的 demo。但由于实现的比较简单，而且也不是主要工作，所以在下面的论述中对于 Wapi_asue 模块和 Wapi_asu 模块的介绍比较简略。重点介绍了 Wapi 模块的设计与实现

5.2.1 Wapi_asue 模块

这个模块要实现的功能是一个小型模拟的 WAPI 客户端，主要目的是为了搭建测试网。如图 5-2 所示，要想具有 WAPI 简单的客户端功能，Wapi_asue 子模块最少要对 4 个报文进行响应：鉴别激活分组、接入鉴别响应、密钥协商请求和组播密钥通告。

1.当收到 AE 发送的鉴别激活分组后，ASUE 将自己的证书和鉴别请求时间封装到接入鉴别请求分组的数据字段中，然后发送给 AE。

2.当收到 AE 发送的接入鉴别响应分组后，先利用 ASU 的公钥来验证 ASU 的签名，通过之后再去取 AP 证书的鉴别结果，根据结果来决定是否接入该 AP。

接入鉴别响应分组的数据字段的格式为：

STA 证书鉴别结果信息	AP 证书鉴别结果信息	ASU 签名

3.当收到密钥协商请求分组后，第一步要去查看 AP 提供的候选算法中是否有自己能支持的，若没有则回复算法协商失败，若有则选一种算法作为与 AP 之间通信的加密算法。之后利用自己的私钥去解密 AP 发送过来的随机数，然后再产生一串随机数，利用 AP 的公钥加密后，封装在密钥协商响应分组中发送给 AP

密钥协商请求分组的数据字段的格式为：

密钥协商数据	备选会话算法个数	备选算法标识

密钥协商响应分组的数据字段的格式为：

会话算法协商响应标识	密钥协商数据

WAI 中 STA 与 AP 之间的鉴别所用的报文格式是统一的，只是数据字段有所不同。

表 5-1 STA 与 AP 之间的鉴别数据格式

STA 与 AP 之间的鉴别数据格式的字段(2B)	取值	含义
鉴别协议类型号(2B)	0x88b4	WAPI 协议的以太网标识号
版本号(2B)	1	

鉴别分组类型(2B)	0	表示鉴别激活分组
	1	表示接入鉴别请求分组
	2	表示接入鉴别响应分组
	3	表示密钥协商请求分组
	4	表示密钥协商响应分组
	7	表示组播密钥通告分组
	8	表示组播密钥响应分组
保留(2B)		
数据长度(2B)		
数据		根据鉴别分组类型的不同而不同

Wapi_asue 子模块在收到报文后先去判断鉴别分组类型字段的取值，这样就可以得到报文类型，然后再进行处理。

5.2.2 Wapi 模块

Wapi 模块对应于 AE 的功能，是整个 WAI 的核心模块，除了要与 ASUE 通信外还要与鉴别服务实体(ASE)通信外，同时还要处理来自底层驱动的消息、来自命令行的消息以及来自时钟模块的消息。

即 Wapi 模块主要处理以下六类消息：

```
enum wapi_msg_type
{
    WAPI_MSG_ASUE,    /* 客户端报文到达消息 */
    WAPI_MSG_ASE,     /* 服务器端通知消息 */
    WAPI_MSG_DRIVER, /* 驱动层发送的消息 */
    WAPI_MSG_CLI,     /* 管理配置消息 */
    WAPI_MSG_TIMER,   /* 时钟超时消息 */
    WAPI_MSG_PORTFLAG_CHANGE,    /* 端口改变消息 */
};
```

所以 Wapi 在从消息队列中取出消息后要根据消息类型来调用不同的函数处理。其中 Wapi 模块对来自 ASUE 和 ASE 模块报文的处理流程是 WAI 中定义的。具体流程如图 5-3 所示。其他四种类型的消息都分别定义了处理函数来处理。

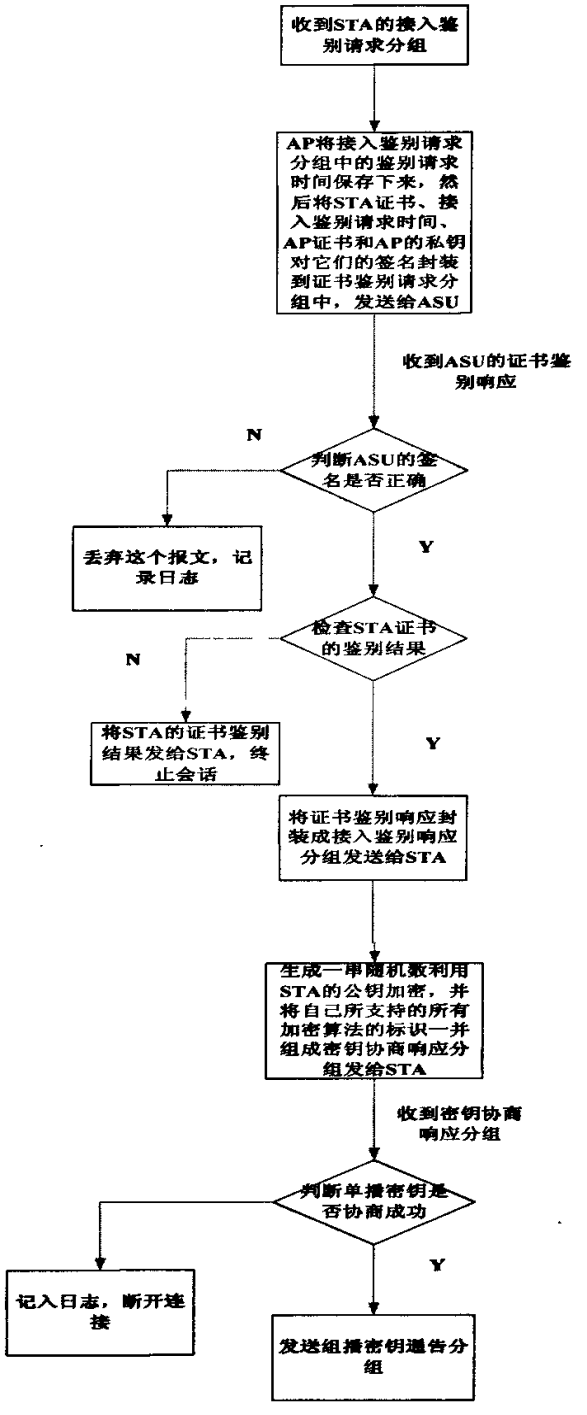

图 5-3 AE 中报文处理流程

5.2.3 Wapi_asu 模块

Wapi_asu 模块执行的一个重要功能就是简单实现了 ASU 的认证功能，也是出于测试目的的考虑。目前由于 WAPI 标准中没有说明证书的颁发、吊销、管理

如何进行，而且目前国内也没有能够商用的 ASU，这也是阻碍 WAPI 商用的一个重要原因，为了能够对我们开发的 AP 中的 Wapi 模块进行测试，就在 Wapi_asu 模块中简单的实现了 ASU 的功能。在这个模块中只有两个个函数：asu_recv_certauthreq()和 asu_tx_certauthreps()，一个用来接收证书鉴别请求，另一个用来发送证书鉴别响应。

5.3 系统实现

本系统是在 VxWorks 下利用 c 语言编写的，满足 GB15629.11-2003 和 GB15629.1102-2003 国家标准。

5.3.1 Wapi_asue 模块

作为一个简单的客户端只实现了与 Wapi 模块的通信，处理了鉴别激活分组、接入鉴别响应分组、密钥协商请求分组和组播密钥通告分组四个报文。分别对应 4 个处理函数：

1.鉴别激活分组报文的处理函数：

wai_asue_authActive_recv()；//在这个函数中主要是实现的功能是向 Ap 发送接入鉴别请求分组

2.接入鉴别响应分组的处理函数：

wai_asue_connectResp_recv()；//这个函数的第一步先验证 ASU 的签名，若通过，再取检查 ASU 对 AP 证书的鉴别结果，若通过则表示 AP 是合法的。

3.密钥协商请求分组的处理函数：

wai_asue_usknegreq_recv()；//这个函数的第一步先检查 AP 支持加密算法中有没有自己可以支持的，若没有，则回复协商失败；若有，再去解密 AP 发送过来的随机数，并同样生成一串随机数利用 AP 的公钥加密后发送给 AP。

4.组播密钥通告分组的处理函数：

wai_asue_mskAnnounce_recv()；//记录组播密钥索引号后发送组播密钥响应报文给 AP。

Wapi_asue 模块的主函数处理流程是：

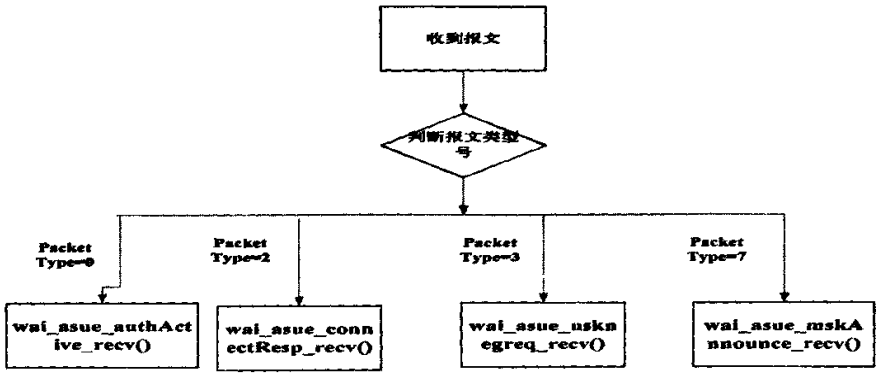

图 5-4 Wapi_asue 模块主函数处理流程

5.3.2 Wapi 模块

Wapi 模块中要处理的消息类型有 5 类：

1.来自用户侧的消息(即来自 Wapi_asue 模块的消息)

2.来自服务器侧的消息(即来自 Wapi_asu 模块的消息)

3.来自底层驱动的消息

4.来自命令行的消息

5.来自时钟模块的消息

Wapi 模块的主函数 Wapi_main()从消息队列中取出一个消息后，首先要判断消息的类型。对于第 1、2 类消息的分别调用了函数 asue_msg_recv_handle()和函数 ase_msg_recv_handle()来处理，处理的流程与图 5-3 一致。

第 3、4、5 类消息属于模块间的接口消息。

来自底层驱动的消息主要有两个，一个是当 STA 与 AP 关联成功后，驱动模块给 Wapi 模块发送 WAPI_MSG_DRIVER_ASSOCIATED 消息，使 Wapi 模块知道有 STA 与本 AP 关联成功，需要向 STA 发送鉴别激活报文；另一个是当用户下线时，驱动模块向 Wapi 模块发送 WAPI_MSG_DRIVER_LOGOFF 消息，来终止认证和计费。

表 5-2 Wapi 与底层驱动模块的接口消息

与底层驱动模块的接口消息	处理函数
WAPI_MSG_DRIVER_ASSOCIATED	wapi_pae_set_associated()
WAPI_MSG_DRIVER_LOGOFF	wapi_pae_set_logoff()

与命令行的接口主要是用户通过命令行配置的参数信息被命令行模块以消息的形式发送到了 Wapi 模块，根据这些参数信息对变量进行赋值。

表 5-3 Wapi 与命令行模块的接口消息

与命令行模块的接口消息	作用	处理
WAPI_MSG_CLI_SetWapitxActivePeriod	设置了鉴别激	全局变量

	活报文的重发间隔	txActivePeriod=命令行模块传过来的参数
WAPI_MSG_CLI_SetWapireAuthPeriod	设置重认证时间间隔	全局变量rxAuthPeriod=命令行模块传过来的参数
WAPI_MSG_CLI_SetWapireUskPeriod	设置担播密钥更新间隔	全局变量txUskPeriod=命令行模块传过来的参数
WAPI_MSG_CLI_ShowClearStatistic	清除Wapi的统计信息	调用函数wapi_statistic_init()

时钟模块的消息每秒钟都会发送一次，收到WAPI_MSG_TIMER消息后，Wapi就调用timer_msg_recv_handle()；来处理，在这个函数中会遍历Wapi模块中的所有定时器，遇有超时，就会马上调用处理函数处理。

Wapi模块主函数的处理流程为：

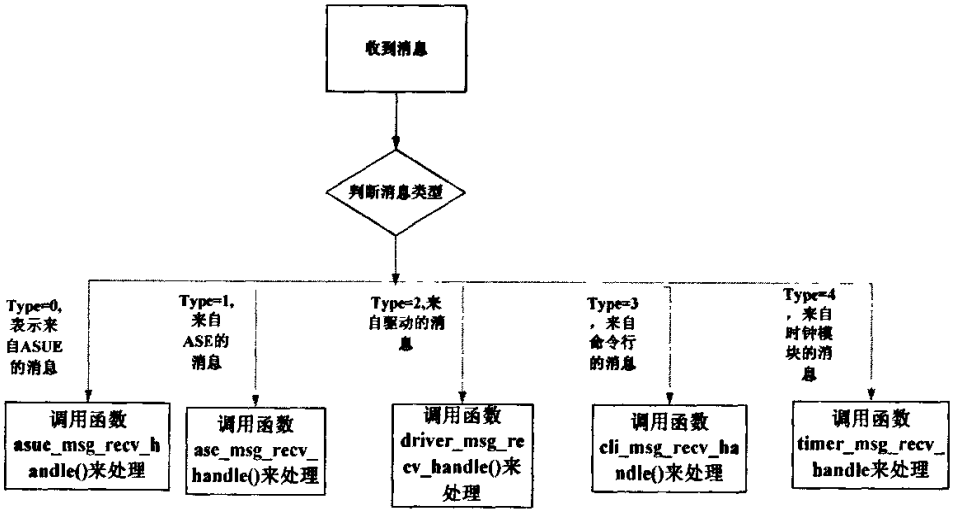

图5-5 Wapi_main函数处理流程

5.4 系统测试

因为目前还没有能够商用的WAPI客户端和服务器，所以我们使用三个AP来搭建测试环境，将其中一个AP的宏CONFIG_WAPI_ASUE打开，利用这个AP来模拟WAPI的客户端，将另一个AP的宏CONFIG_WAIAE_ASU打开，然后将这个AP作为WAPI的服务器，第三个AP担任WAI结构中的AE。这样三个AP就简单模拟了一个STA-〉AP-〉AS的测试网络。

1. 测试用例1

在AP上配置：

AuthType：WAI

CipherType：WPI //表示用WAI认证，WPI加密数据报文

并将WAI的证书以配置文件的形式存放到AP和模拟客户端中。然后在作为客户端的AP上的ASUE的目录下键入命令Start<apMAC>来开始一次基于WAPI认证协议的WLAN连接，apMAC表示AP中无线网卡的MAC地址。测试结果是认证成功，符合预期结果。测试的通过也证明了AP已具备实现WAPI接入的功能。

2.测试用例2

在AP上配置

AuthType：WAI

CipherType：WPI

更改AP上的证书

测试结果是AP证书验证失败，符合预期结果。

3.测试用例3

在AP上配置

AuthType：WAI

CipherType：WPI

更改客户端的证书

测试结果是STA证书验证失败，符合预期结果。

5.5 WAPI协议在应用中的改进

WAPI要想能够在运营级网络中应用，必须要解决计费的问题、证书管理问题、客户端问题等。证书管理问题主要在ASU中实现，客户端和ASU由本项目的其他承办公司来承担研发工作。

那么，为了使WAPI能够在运营级AP中得到应用，我们可以将WAPI的认证机制WAI与EAP-SIM认证结合使用，即对于WAPI用户先进行WAI认证，通过了之后再进行EAP-SIM认证。这样一来首先解决了WAPI没有对计费功能进行定义的不足；其次，从用户的角度来讲也非常方便，因为目前WLAN只是有线网络的一种补充，很多用户不会专门去申请WLAN的账户，而由于目前移动电话已经相当普及，利用SIM卡中的信息进行认证和计费对用户来讲就显得非常方便；再次，从实现角度来讲也非常简单，因为AP设备已经支持了EAP-SIM和WAI认证，这样在认证阶段无需做太多的更改，只是在认证通过了之后要对WAPI用户和IEEE 802.11i用户进行分别管理，因为在发送数据报文时，要使用

不同的加密算法。目前在芯片上已经可以同时支持 WAPI 和 IEEE 802.11i 的加密算法，所以 AP 完全可以同时支持 WAPI 用户和 IEEE 802.11i 用户。

在 WAPI 客户端方面，需要的改动也非常小，只是需要在 WAI 客户端的基础上将 EAP-SIM 认证的客户端集成进来，这样在 WAI 认证成功后，给 EAP-SIM 认证模块发送一个消息，触发客户端发出 EAPoL-Start/SIM 报文，来进行 EAP-SIM 认证。

通过在应用中的这种改进，可以在 AP 侧将 WAPI 与现有的 IEEE 802.11i 系统融合起来，即 AP 可以同时支持 WAPI 用和 IEEE 802.11i 用户，这样将更有利于 WAPI 的推广。

5.6 本章小结

WAPI 是我国 WLAN 安全的国家标准，采用了先进的公钥加密体制来进行认证，并且实现了用户和 AP 之间的双向认证，提高了网络的安全性。为了推动 WAPI 的应用，促进 WAPI 产业链的早日成熟，本章在 AP 中实现了对 WAPI 的支持。

WAPI 模块中主要实现的是 AE(Authenticator Entity)和 ASU(Authentication Service Unit)和 ASUE 功能。这样系统就分为三个模块，分别对应代码中的 Wapi、Wapi_asu、Wapi_asue 模块。同时并定义了与其他模块之间的接口消息。然后对主要函数的功能进行了说明。

最后，提出了 WAPI 协议的一个改进意见。

第六章 总结与展望

在研究生期间，主要从事了大量的网络安全系统的开发和应用方面的工作，尤其是对 WLAN 网络中 AP 的安全认证方面做了一定的开发工作。由于所做的工作是属于接入层设备，所以对目前网络中主要采用的接入认证方法进行了一定的研究，有一些心得，这篇论文就是对我研究生期间的学习，工作和研究的一个总结。

WLAN 作为计算机网络和移动通信技术的结合，近几年得到快速的发展，尤其在无线宽带城市建设方面，WLAN 技术在全球扮演着重要角色，并显示出了强大的发展空间。可以预期随着开放办公的流行和手持设备的普及，在变化频繁的办公环境、临时组建的大型会议或商业场合、及家庭应用等领域，无线局域网将获得更加广泛的应用，因此保障无线局域网安全的认证技术和相关安全机制，也将继续是热点的讨论问题。

但由于 WLAN 中的数据通过射频无线电传输，这对于恶意的攻击者实施窃听是十分有利的。与有线网络相比较，WLAN 难以在物理上采取控制措施，因此保护 WLAN 的安全难度要远大于保护有线网络。目前 IEEE 802.11i 是最新的 WLAN 安全标准，但随着技术的快速发展，以及 WLAN 与未来 3G 网络的融合又将有很多新的安全问题需要我们不断地去研究。

WAPI 作为我国自主开发的 WLAN 安全协议，在业界引起了激烈的争论，它采用了先进的公钥证书体制来从理论上完整的解决了无线局域网安全问题。但由于兼容性等问题，WAPI 要想取得广泛的应用还需要我们不断地对它进行完善和改进。

在本文中，由于作者的知识和能力有限，只对其中很有限的若干问题进行了探讨和研究，其过程中难免会有很多纰漏和不足之处，敬请谅解。

参考文献

[1] Jon Edney,Wiliam A.Araugh 著，周正等译，《无线局域网安全实务——WPA 与 802.11i》，人民邮电出版社， 2006.2

[2] IEEE Std 802.11，Part 11：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications，1999.

[3] 王大虎，杨维等，《WEP 的安全技术分析与对策》，.中国安全科学学报，2004 年 08 期

[4] IEEE Std 802.11i，Part 11： Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)Specifications. Amendment 6：Medium Access Control (MAC) Security Enhancements， 2004.

[5] IEEE Std 802.1X：Port-Based Network Access Control,2001

[6] 李勤，张浩军等，《无线局域网安全协议的研究和实现》，计算机应用，2005

[7]Blunk and Vollbrecht, RFC 2284, March 1998,PPP Extensible Authentication Protocol(EAP), IETF.

[8] 马建峰，朱建明等，《无线局域网安全一方法与技术》，北京机械工业出版社，2005

[9] H.Haverinen，IETF Draft，June 2002 EAP SIM Authentication，Draft-haverinen-pppext-eap-sim-05.txt.，IETF

[10] 朱坤华，王玉芬，李新丽著，《两种无线局域网安全标准 WAPI 与 802.11 i 的比较》，河南科技学院学报，2005 年 3 月第 33 卷第 I 期，84-85.

[11] GB 15629.11，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 MAC 和物理 PHY 层规范，2003

[12] Tim Moore， Suggested Changes to Robust Security Network (RSN) for IEEE 802.11IEEE 802.11-02/298r4.，September 2002.

[13] Neils Ferugson，Michael: an improved MIC for 802.11 WEP IEEE 802.11-02/020r0，Jan 2002.

[14] 《中国移动 WLAN 用户接入流程技术规范》

[15] 杨寅春，张世明等，《WAPI 安全机制分析》，计算机工程，第 31 卷第 10 期，2005

[16] 钱进，《无线局域网技术与应用》，电子工业出版，2004

[17] 金纯，陈林星，杨吉云著，《IEEE 802.11 无线局域网》，电子工业出版社，2004

[18] 刘乃安，李晓辉著，《 无线局域网(WLAN):原理、技术与应用》，西安电子科技大学出版社，2004.10

[19] Dr:CyrusPeikari, SethFogie 著,周靖等译，《无线网络安全》，北京电子工业出版社，2004.7

[20] 吕霞，杨军，《WLAN 标准 GB15629.11 安全机制——WAPI 协议解析》，电子设计应用，2004

[21] 尹传勇，刘寿强，毕雅宁，《营造安全的无限空间——无线局域网新标准 WAPI 解析》，计算机安全，2004

[22] Qu Wei,Srinivas S, IPSec-based Security Wireless Virtual Private Network, IEEE MilCom2002, California, 2002: 7985

[23] Carlton R Davis，周永彬译，《IPSec VPN 的安全实施》，:清华大学出版社，2002

[24] Carlisle Adams, Steve Lloyd，冯登国译，《公开密钥基础设施一概念、标准和实施》，人民邮电出版社，2001

致谢

衷心感谢我的导师漆涛，研究生学习期间，漆老师严谨的治学态度、渊博的专业知识以及开明的思想给我留下了深刻的印象和深远的影响，将使我受益终生。感谢漆老师给我提供了一流的实验室环境，让我可以学习到本专业前沿的知识。

感谢曹首峰和张勇两位师兄在3年来给予我的帮助和指导，师兄精益求精的工作态度给我树立了良好的榜样。

感谢同届的易磊、张珊珊同学在日常学习和工作中对我的帮助和配合，感谢同宿舍的张珊珊、刘芳、路杨同学在生活上对我的关心和照顾，我们一起走过了温馨的三年。

感谢下一届的师弟师妹们在工作和生活上对我的支持。

感谢我的父母为我的成长所付出的一切，没有他们的付出就没有我今天的一切。

感谢北邮给我提供了成长的环境，祝愿母校明天更美好！

WLAN安全解决方案设计与实现

作者： 李煜
学位授予单位： 北京邮电大学

相似文献(10条)

1.学位论文 王鑫 无线局域网环境下认证技术的研究 2007

本文主要围绕无线局域网的安全问题，致力于实现无线局域网的安全和认证，并针对在公用WLAN的应用展开研究。本文首先分析了无线局域网的应用状况和面临的安全威胁，然后以无线局域网的安全技术发展历程为主线，对各种安全技术进行了详细的研究，指出了它们的特点和存在的不足之处，并就目前的一些解决方案进行了分析比较，提出了根据实际应用，建立多层安全保护措施，以最大限度地降低安全风险。接着，论文着重对基于802.1X的无线局域网安全认证的实现进行了研究。802.1 X是基于端口的网络访问控制方案，它和扩展认证协议EAP(ExtensibleAuthentication Protocol)一起来共同实现无线局域网的安全认证。论文主要通过搭建认证环境，来实现EAP-MD5，EAP-TLS认证方法。从中，我们验证了EAP-MD5是一种单向认证机制，通过Radius服务器只能保证客户端到服务器的认证，并不保证服务器到客户端的认证。而EAP-TLS既提供认证，又提供动态会话钥匙分发，在无线客户端和服务器之间提供互相认证。最后，论文给出了研究工作总结，并提出了以后的研究思路。

2.会议论文 王玉峰 计算机无线局域网 1996

无线局域网是实现移动计算机网络和个人通信的基础。该文介绍了无线局域网的发展背景、现状、组成及其应用，说明了无线局域网的体系结构和传输技术。

3.学位论文 王勇 椭圆曲线密码体制在WLAN安全机制中的应用 2006

无线局域网(Wireless Local Area Network，WLAN)是现代无线通信技术在计算机网络中的应用，它为通信的移动化、个人化和多媒体应用提供了实现手段和技术。 无线局域网以其方便、快捷、廉价等诸多优势，在企业内部和公共热点地区等领域的应用中很快取得了长足的发展和巨大的成功，而与此同时用户对无线网络的各种性能，尤其是安全性能的要求变得格外苛刻。无线局域网的安全认证和数据加密问题成为进一步推进其在信息化领域中应用的关键性问题。 为此，IEEE标准委员会于2004年6月批准了802.11i[1]，该安全协议采用AES[1](Advanced Encryption Standard，高级加密标准)算法替代RC4算法，使用802.1x/EAP协议进行用户认证。然而由于802.1x/EAP(Extensible Authentication Protocol，可扩展认证协议)认证方式的不足，使得无线局域网的安全问题在多种攻击手段面前仍然显得十分突出。 本文首先介绍了无线局域网当前存在的安全问题以及研究现状，接着从原理和技术两个方面介绍了当前无线局域网的安全协议IEEE802.11i。 接着对基于802.1x/EAP的认证方式展开了具体的分析，探讨了该认证方式的原理以及优缺点。 针对其存在的缺点，本文提出了基于椭圆曲线的数字签名的认证方式。该认证方式利用证书来对系统中的STA(Station，端站)和AP(Access Point，接入点)进行认证，认证服务器用于管理参与信息交换各方所需要的证书(包括证书的产生、颁发、吊销和更新)。证书中包含有证书颁发者(认证服务器)的公钥和签名以及证书持有者的公钥和签名(这里的签名采用的是椭圆曲线数字签名算法)，是网络设备的数字身份凭证。 本文进一步探讨了该认证系统的结构框架以及实现基于椭圆曲线的数字签名的流程，并给出了实现椭圆曲线的加密算法。 最后，本文提出了今后进一步的工作和该技术的展望。

4.期刊论文 王晓峰.王炳和 无线局域网中的核心技术及其应用 -航空计算技术2003,33(3)

无线局域网对计算机网络技术的进一步发展起到了深刻的影响.该文着重介绍了无线局域网中的关键技术--直序扩频技术的工作原理和系统结构,讨论了无线局域网的协议结构.在此基础上给出了一个无线扩频通信局域网的典型设计方案.此设计方案主要对某大型企业无线局域网的扩频通信部分的各具体参数进行了详细设计,为实际工程应用提供了可行性技术指导.

5.学位论文 李燕 基于网络处理器的千兆防火墙中NAT的设计与实现 2006

随着互联网的飞速发展和网络犯罪案件的急剧上升，网络安全已经作为一个非常严峻的问题摆在了人们面前，受到了越来越多的关注与重视。本文介绍了作者在研究生学习期间就网络安全方面所做的研发工作，主要包括两部分内容，分别是：基于网络处理器的千兆防火墙中NAT子系统的设计与实现；无线局域网监测设备中系统控制与管理功能的设计与实现。在每个部分中，首先介绍课题的相关理论，然后阐述本人对课题的研究和实现。 本论文第一章到第四章将主要讲述NAT技术及其在基于Intel网络处理器IXP2400的千兆包过滤防火墙中的设计与实现，第五章讲述-我在无线局域网监测设备项目中所做的一些工作。具体内容如下： 第一章介绍了网络处理器的相关知识，着重讲述了英特尔公司的IXP2400网络处理器的体系结构及IXA软件框架。 第二章简要介绍了防火墙技术，包括防火墙的概念、分类及其关键技术。 第三章介绍了基于Intel网络处理器IXP2400的千兆包过滤防火墙的总体设计方案，实现的功能及功能模块的划分。 第四章详细阐述了网络地址转换(NAT)子系统的设计方案、具体实现、测试结果和经验体会。 第五章介绍了无线局域网和WindowsSockets网络编程的相关知识，重点讲述无线局域网监测设备中系统控制与管理子系统的详细设计与实现。

6.会议论文 刘刚 无线局域网(WLAN)建设中的关键技术分析 2002

无线局域网(WLAN)具有部署灵活、高带宽、建设速度快、支持局部地区的低速移动性等优点,在国内外有着广阔的市场前景.但是,WLAN技术比较新,无线接入技术,尤其是用户接入管理技术,相对比较复杂.本文针对WLAN建设中的2项关键技术——IEEE802.11b无线接入技术和IEEE802.1x用户接入管理技术——进行了分析,希望对广大从事WLAN建设的同志们有所帮助.

7.学位论文 曾志纯 移动计算机网络中的双向功放与天线技术研究 2004

随着人们对网络通信需求的不断提高,人们希望不论何时、何地、与何人都能够进行包括数据、语音、图像等任何内容的通信,并希望实现主机在网络中的漫游.为了提高工作效率和随时能够交换和处理信息,人们提出了移动计算机网络的概念.为了使无线网络系统不仅支持移动终端之间的通信,而且应允许无线设备接入有线网络,达到宽带通信和全球连接的目标,一个新的领域—无线局域网WLAN(Wireless LocalAreaNetwork)应运而生.随着WLAN的广泛应用,作为增加WLAN通信距离、增大WLAN覆盖范围的重要的高频部件—双向功放和天线的作用越来越重要.该文以双向功放和天线在WLAN中的应用为线索,对双向功放在使用过程中出现的非线性失真问题和组网天线技术进行了理论研究和实验仿真.文章首先介绍了功放中的线性化技术—预失真技术和前馈技术.分析研究了预失真技术和前馈技术的原理、性能及其实现方法,并在深入研究两种技术的基础上,提出了集合两者优点于一体的自适应前馈预失真线性化系统方案.接着对典型WLAN功放进行了电路结构和性能的分析研究,并着重分析了功放电路中线性化技术的应用以及在线性化方面的改进,同时对功放相关的性能进行了测试.最后该文介绍了WLAN中的组网天线技术,分析了常见天线性能指标,对几种不同种类天线进行了性能分析与比较,并以某定向天线为例进行了结构和性能的分析研究.同时也研究了天线在WLAN中的应用技术.由于WLAN的应用日益广泛,人们的需求迅速增长.该课题的研究成果对WLAN的覆盖面积,解决传输接收信号中等面临的问题,改善WLAN的通信性能具有重要的理论指导意义.

8.期刊论文 叶军.宋建军 大型灌区信息化系统计算机网络的建设 -中国农村水利水电2004(10)

在新疆大型灌区信息化系统初步建设的基础上,介绍了计算机网络技术在灌区信息化系统中的应用方式,从网络的组网方式、网络安全性、网络业务种类等多方面进行了说明.并对灌区信息化系统在进一步深入建设后,网络通信系统的建设方式进行探讨.

9.期刊论文 曹东.郑秀文 无线局域网技术在松辽委的应用 -东北水利水电2003,21(11)

本文重点阐述了无线局域网技术原理,以及利用无线局域网技术实现多个计算机网络互联的技术方案和无线局域网在松辽委的实际应用情况及无线局域网的应用前景.

10.学位论文 马金平 基于Web网管设备在NNM网管系统中监管的实现 2004

本文在设计和实现WLAN无线运营网络模型与系统架构的基础上，采用HP NNM网络管理平台，根据网络的实际需要进行二次开发，提供简单、灵活、

完善的网络管理。详细阐述了系统构成的功能模块以及其设计与实现。WLAN网管系统的扩展性使其在保护用户原有资源的前提下，保证网络系统与网管系统同步发展。本系统采用基于三层架构的委托代理模型，同时支持多种网络管理协议，实现对基于Web网管模式的网络设备和多种其他类型的网络设备的集成管理，降低管理成本。在对WBM网管设备的管理中，根据不同设备采用相应XML配置文件动态解析设备管理页面，提取设备MIB信息；代理模型层次架构充分体现了WLAN网管系统扩展性和灵活性，创建设备相应的配置文件即可实现对其监控管理。本系统在NNM的基础上以图形界面跟踪并分析热点AP的性能状况，视图中动态刷新和显示AP运行状态；实时监视热点AP接入的用户数、用户地址列表、用户产生流量；基于热点AP历史数据的可用率、故障发生率、利用率分析以进行故障诊断；网管系统故障自动报警功能将及时告知网管人员网络故障。通过对WLAN无线网络设备的监控数据的分析，管理员可以及时预测网络的通信质量，改善和优化网络性能，确保网络的正常高效运行。