摘要

随着无线局域网的不断普及，无线局域网的安全成为了目前计算机网络方面的热门话题。确保无线局域网的安全，主要从两个方面进行考虑：一方面是加强认证的技术，另一方面是加密。本文主要是从加强 IEEE802.1x 认证的角度对此技术进行探讨，结合了 Radius 服务器技术，EAP-TLS 认证等一起来确保无线网络的安全。

本文在总结前人对无线局域网的安全问题研究的基础上，对如何通过加强 IEEE802.1x 协议的安全性来加强无线局域网的安全做了细致的探讨，提出了 WLAN 安全认证和密钥管理的软件方案，实现了包括安全认证、密钥管理、数据保护等安全功能，支持用户通过认证登陆网络，并有效保证了无线局域网中数据访问的安全性和可靠性。

本文首先对本课题进行概述和研究的范围进行定位，接着介绍了无线局域网的相关知识，并对 IEEE 802.11 协议做了重点的介绍，同时总结了前人对无线局域网的安全问题的研究成果，分析了无线局域网移动通信系统的存在的各种安全威胁，并对无线局域网的主要安全措施的缺陷及改进做了重点的介绍，提出了解决无线局域网安全的主要思路。

本文重点是分析了 IEEE802.1x 协议及 EAP-TLS 认证的技术，描述了 EAP 协议，和 TLS 传输层安全协议，为后面的模型和软件方案的建立做了深入的准备，并进一步论述了无线局域网的密钥管理，包括密钥管理的目的和密钥的种类以及提出了无线局域网的密钥管理和安全认证的模型，包括认证者端和 STA 端的两个子模型。文章的最后是展望了无线局域网的未来-IEEE802.11i 协议。

关键词： 无线局域网；网络安全；IEEE802.1x；EAP-TLS 认证；IEEE802.11

ABSTRACT

With the further popularization of WLAN, the security of WLAN has been becoming a hot topic in the research field of computer networks. There are two ways to insure the security of WLAN, one is to improve the technology of Authentication, the other is to use the Encryption. In this article, we discuss the security of WLAN from the angle of enhancing the IEEE802.1x Authentication by combining with the technology of Radius Server and the Authentication of EAP-TLS to improve the security in WLAN.

This article makes a further exploration on the security of WLAN by enhancing the security of IEEE802.1x protocol, basing on the summarization of the former researcher's hard work in this field. And it puts forward to a software solution on security authentication and key management of WLAN, including the functions of security authentication, key management and data protection, and it supports the clients to log in the networks by authentication, which effectively improves the security and reliability of data access in WLAN.

First of all, this article makes the summarization and positioning of the research topic. Then it introduces the related knowledge of WLAN and the IEEE 802.11 protocol, which provides an important basis for our research of security in WLAN. Furthermore, it summarizes the former research on the security of WLAN, analyzes various of intimidations which lie in the mobile communication systems of WLAN, introduces the bugs and improvement of the major secure measures in WLAN and puts forward to the major solutions to solve the security in WLAN.

Moreover, the emphasis of this article analyzes IEEE802.1x protocol and the authentication of EAP-TLS, mainly describes the protocol of EAP and TLS, which provide a further preparation of the model and software solutions in the later chapters. Then it summarizes the key management in WLAN, including the intention of key management and the styles of key, puts forward to the key management system of WLAN. And it also puts forward to the model of secure authentication system of WLAN, including the implementation of authenticator and STA, at the end of this article, we describe the future of security in WLAN, focusing on the IEEE802.11i protocol.

Keywords:WLAN, Network security,IEEE802.1x, EAP-TLS Authentication IEEE802.11.

第一章 绪论

1.1 研究背景及意义

通信技术发展的最终目标是任何人（Whoever），在任何时候（Whenever）、与任何地方（Wherever）的任何人（Whomever），进行任何形式（Whatever）的通信。这就是所谓的 5W 通信[1][2][3]。为此，人类正在不断地致力于个人通信业务 PCS（Personal Communication System）的研究与开发，特别是在移动环境下的多媒体通信是未来的重要通信服务。随着无线局域网技术上的成熟，产品种类的不断增加和产品成本下降，未来几年，无线局域网的应用将越来越广。可以预期，在未来信息无处不在的时代，无线网将依靠其灵活性、可移动性和良好的扩容性，能够使人们享受到简单、方便、快捷的网络连接服务。

任何网络，包括有线网络都受到大量安全问题的困扰，包括来自网络用户的攻击、未认证用户的存取权以及来自公司或者工作组外部的窃听[4][5][6][7]。由于无线媒体的开放性，窃听是无线通信常见的问题，所以无线网络的安全性比有线网络更受到关注，对接入 WLAN 的用户必须进行接入控制和消息加密。

无线局域网是一种灵活、方便的连网方案，其概念早已经出现，但由于受带宽和信号范围的约束，始终没有走出实验室，直到 IEEE802.11 工作小组针对无线局域网的 11Mbit/s 规范进行了最后的标准化，无线局域网才得到商用。该小组先后出台过一系列标准，主要有 IEEE 802.11a 和 IEEE 802.11b 和 IEEE 802.11g。这些标准在传输带宽上有很大的区别，但它们所采用的安全机制则是完全相同的。

随着 IEEE 802.11 标准的发布，无线局域网的设计和应用得到了迅速的发展，满足了人们在一定区域内实现不间断移动办公的需求，安全问题也随之产生。

IEEE802.11 系列标准所定义的规范也提供了一些安全的解决手段，如 SSID，MAC 技术和 WEP 加密等。但随着人们对无线局域网技术的逐渐熟悉与了解，特别是在这场网络安全 “道高一尺，魔高一丈”的这场对抗战中，黑客

的水平也不断地上涨，上述的技术都在一定程度上不能够有效地确保无线局域网的安全。而且就整个形势而言，无线网络的安全只是一个旅程，它的昨天并不是一个结果。因此，如何研究出安全的，有效的无线网络的安全解决方案以确保一定时期内无线局域网的安全就成为了当务之急，特别是在当前的日益普及的这种无线局域网时代的到来就更加的紧迫。

1.2 国内外研究现状[8][9][10][11][12][13][14][15]

无线局域网中，安全的概念主要体现为访问控制和信息保密两部分，前者由服务识别号 SSID 机制保障，但 SSID 本身很不安全，服务区号完全可以通过窃听或其它简单手段来获得，因此，这种访问控制机是非常初级的。虽然，IEEE802.11 标准定义了 WEP，使数据无法被监听和修改，另外也提供接入控制。但是，据加州伯克立分校的研究学者的实验的发现，WEP 协议存在严重的缺陷，可导致信息被破译和修改。

无线局域网中存在如下几种安全隐患。

（1）拒绝服务攻击 无线局域网存在一种比较特殊的拒绝服务攻击，攻击者可以发送与无线局域网相同频率的干扰信号来干扰网络的正常运行，从而导致正常的用户无法使用网络。如果攻击者有足够功率的无线电收发器，就能够很容易地产生干扰信号，以致于无线局域网无法使用这个无线电信道。

（2）无线窃听 无线局域网中，网络的安全尤其面临挑战，无线电信号可能传播到办公室外面，利用这点，入侵者就可以在建筑物外面来访问无线局域网，也就可以窃听网络中传输的数据。

（3）其他问题 在局域网中还有一种比较特别的置信攻击，攻击者可以将自己伪造成为基站。如果攻击者拥有一个很强的发送设备，就可以让移动设备尝试登录到攻击者的网络，通过分析找出密钥和口令。除此之外，无线局域网也很容易受到一些针对系统缺点的攻击，例如软件 BUG、配置错误和硬件失败等。

目前无线局域网的安全机制主要体现在 3 个方面。

- 加密算法：IEEE802.11 标准采用 RC4 算法，它是一种流密码算法。
- 认证：IEEE802.11 标准采用了两种认证方法，共享密钥认证和开发系

统认证。

- 密钥管理：采用了挑战应答传送和接收密钥的方式。

目前，针对 IEEE802.11 的无线局域网的安全机制所存在的缺陷，国内外的研究主要体现在两个方面：首先是针对目前的安全缺陷提出一些改进的方案。综合起来有：

1) 修正 WEP 机制，通过对 RC4 算法进行改进以提高 WEP 机制的安全。
2) 采用 IPSec 技术，即由 WLAN 用户建立专用的 VPN 通道来提高网络的安全性。
3) 配合其他的安全机制。除了 WEP 外，WLAN 也可配合 SSH 或 SSL 等网络安全机制。

其次，为了进一步加强无线网络的安全性，IEEE802.11 工作组正在开发新的安全标准 IEEE802.11i。标准的草案主要包含 TKIP（临时密钥完整性协议）、AES（先进的加密标准）加密技术和 IEEE802.1x 认证协议。

IEEE 802.11TGi(任务组 I)委员会已经制订了临时密钥完整性协议(TKIP)，作为过渡解决方案。TKIP 像 WEP 一样基于 RC4 加密，但以另一种方式实施，解决了 WEP 目前存在的脆弱性。它提供了快速更新密钥的功能。利用 TKIP，随着各个厂商计划推出 TKIP 固件补丁，消费者在无线局域网硬件上的投资将得到保护。

IEEE 802.11TGi 在正开发一个使用 AES（高级加密标准）的新协议，以实施更强大的加密和信息完整性检查。IEEE 802.11i 预计将采用 IEEE 802.1x 鉴权。

IEEE 802.11i 将包括增强的加密格式和鉴权机制，如 RADIUS、Kerberos 和 IEEEE 802.1x。IEEE 802.11i 的许多安全增强特性都可以通过固件升级来完成，而有些必须通过硬件来完成。

无线局域网的安全技术研究比较领先的主要是美国和欧洲的组织，特别是大学。如美国的 Carnegie Mellon University, Johns Hopkins University, Suny Buffalo, University of Maryland, Auburn University,英国的 Manchester University 等在此课题上都有比较领先的优势。

我国的无线局域网的安全技术研究起步较晚，研究不是很系统，但我国对这个领域也很重视，最近的几年也集中了不少的人力和物力对此进行研究，搞得比较好的有北京邮电大学，东南大学等高校。目前，我国已经颁布了自己的

两项国家标准。但鉴于无线局域网应用的不断普及，我国还是应该花更多的时间对此问题进行研究，这不管对商业利益来说，还是对国家利益来说，都有巨大的重要性。

1.3 前期工作

在确定此题目之前，在导师李振坤教授的指导下，本人做了大量的调查工作，主要集中在国内外的研究现状的分析以及课题的可行性分析。并且在总结前人的基础上和导师一起联合发表了论文“无线局域网的安全性分析”等相关的论文[16]，从中也积累了一定的经验。

另外一点是参加了广东工业大学计算机工程研发中心的“基于无线局域网的广东大厦餐饮管理系统”的研发工作，对无线局域网的实践应用方面有着一定的认识。同时，本人也利用一些网络仿真软件，如 OPNET，COMNET，数学软件 Mathematica 等做了一些实验，虽然不尽成功，但也略有收获。

此外，本人在三年的研究生学习中，也很重视网络安全的技术的研究，如 Ddos 技术和防火墙技术等，在这些小话题上也做了一定的调查和总结，并在此基础上发表了几个相关的论文[17][18][19]。

在前期研究工作中，我重点在无线网络和网络安全这两个课题上做了大量工作，本文在此基础上，无线局域网的安全的相关问题做进一步深入研究。

1.4 本文内容及论文组织

在本文的工作中，探讨了建立无线局域网安全认证系统的模型。主要内容包括：一、提出无线局域网的安全认证系统的模型。认证机制采用了 EAP-TLS，认证服务器采用目前比较成熟的 RADIUS 服务器。二、本文提出 WLAN 安全认证和密钥管理的软件方案，实现了包括安全认证、密钥管理、数据保护等安全功能，支持用户通过认证登陆网络，并有效保证了无线局域网中数据交换的安全性和可靠性。三、总结了前人关于无线局域网安全的最新研究成果。

本文第二章介绍了无线局域网的发展历史，无线局域网的优势，无线局域网的标准，以及无线局域网的主要应用领域，接着本章的重点对无线局域网的安全问题进行总结和论述。首先在总结前人的基础上对无线局域网的安全问题

进行综述，列举了无线局域网移动通信系统的安全威胁，包括无线链路威胁、服务网络威胁和终端威胁等，接着从 OSI 模型的角度，重点介绍了无线局域网与有线局域网的安全的区别的三个主要层次，包括物理层、数据链路层和网络层等三层的无线安全问题。接着本章对无线局域网的主要安全措施的缺陷及改进做了重点的介绍，主要介绍了三项技术，即 SSID 技术、MAC 地址过滤和基于 WEP 的安全机制。最后，本章重点论述了解决无线局域网安全的主要思路，主要是对 VPN 方案和 802.1x 做了总结。

第三章对 IEEE802.1x 协议及 EAP-TLS 认证的技术进行介绍，首先是介绍了 IEEE802.1x 的提出背景，IEEE802.1x 的体系结构、IEEE 802.1x 的认证过程和 IEEE 802.1x 协议的优点等。接着介绍了 EAP 协议，主要是介绍了 EAP 的认证类型、EAP 的认证过程、EAP 协议的主要特点和 EAP 在 IEEE802.1X 中的应用等，最后是介绍了 TLS 传输层安全协议，主要论述了握手协议的机制、记录协议、TLS 的认证过程、EAP-TLS 数据包格式、EAP-TLS 认证过程和 EAPOL 消息的交互过程等，为后面的模型的建立做了很好的准备。

第四章提出了无线局域网安全认证系统的模型，包括认证者端和 STA 端的构建。认证者端的实现及主函数流程设计、认证模块的实现等。在认证模块的实现这里提出了认证模块的协议流程和认证模块的程序设计，最后是提出了四步握手密钥协商机制的实现，包括工作流程、程序模块设计。STA 端的实现主要包括了软件流程图和四步握手密钥管理的实现。在此章中，还对无线局域网的密钥管理进行了论述，包括密钥管理的目的和密钥的种类以及提出了无线局域网的密钥管理模型。此模型的主要内容包括强安全网络 RSN 的安全性能协商、认证和密钥管理系统、密钥层次、TKIP 密钥层次和 AES 密钥层次等。本章最后是展望了无线局域网安全的未来，对 IEEE802.11i 的做了重点的描述。

第二章　无线局域网及其安全机制

2.1 无线局域网的发展历史

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[20]，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，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。

2.2　无线局域网的优势

	无线局域网	有线局域网
传输距离	根据天线增益可远达 10 公里	双绞线网段距离较短，几百米
建网时间	时间短，甚至几分钟就可以解决问题	施工时间比较长
工作站移动性	可以无线覆盖的范围内自由移动	无法自由移动
对建筑物的影响	影响很小	影响较大，可能破坏建筑物的原貌

表 2-1　　无线局域网与有线局域网的比较

从表 2-1 的对比可看出，无线局域网主要具有以下优势[21][22][23]：

(1)安装便捷

一般在网络建设中，施工周期最长、对周边环境影响最大的，就是网络布线施工工程。在施工过程中，往往需要破墙掘地、穿线架管。而 WLAN 最大的优势就是免去或减少了网络布线的工作量，一般只要安装一个或多个接入点(Access Point) 设备，就可建立覆盖整个建筑或地区的局域网络。

（2）使用灵活

在有线网络中，网络设备的安放位置受网络信息点位置的限制。而一旦WLAN 建成后，在无线网的信号覆盖区域内任何一个位置都可以接入网络。

（3）经济节约

由于有线网络缺少灵活性，这就要求网络规划者尽可能地考虑未来发展的需要，这就往往导致预设大量利用率较低的信息点。而一旦网络的发展超出了设计规划，又要花费较多费用进行网络改造。而 WLAN 可以避免或减少以上情况的发生。

（4）易于扩展

WLAN 有多种配置方式，能够根据需要灵活选择。这样，WLAN 就能胜任从只有几个用户的小型局域网到上千用户的大型网络。

2.3 无线局域网的标准

1、IEEE802.11 系列

1990 年，IEEE802 标准化委员会成立 IEEE802.11 无线局域网（WLAN）标准工作组[24][25]。IEEE802.11 无线局域网标准工作组的任务为研究 1Mbit/s 和 2Mbit/s 数据速率、工作在 2.4GHz 开放频段的无线设备和网络发展的全球标准，并于 1997 年 6 月公布了该标准，它是第一代无线局域网标准之一。该标准定义物理层和媒体访问控制（MAC）规范，允许无线局域网及无线设备制造商建立互操作网络设备。802.11 标准中物理层定义了数据传输的信号特征和调制。在物理层中，定义了两个 RF 传输方法和一个红外线传输方法，RF 传输方法采用扩频调制技术来满足绝大多数国家工作规范。在该标准中 RF 传输标准是跳频扩频和直接序列扩频，工作在 2.4000GHz～2.4835GHz 频段。直接序列扩频采用 BPSK 和 DQPSK 调制技术，支持 1Mbit/s 和 2Mbit/s 数据传输速率。跳频扩频采用 2～4 电平 GFSK 调制技术，支持 1Mbit/s 数据传输速率，共有 22 组跳频图案，包括 79 个信道。红外线传输方法工作在 850nm～950nm 段，峰值功率为 2W，支持的数据传输速率为 1Mbit/s 和 2Mbit/s。

IEEE 802.11 是 IEEE 最初制订的一个 WLAN 标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入，业务主要限于数据访问，速率最高只能达到 2Mbit/s。由于它在速率和传输距离上都不能满足人们的需要，所以 802.11 标准很快被 802.11b 所取代。1999 年 9 月，802.11b 被正式批准。该标准规定 WLAN 工作频段为 2.4GHz～2.4835GHz，数据传输速率达到 11Mbit/s，传输距离控制在 50～150 英尺。该标准是对 802.11 的一个补充，采用补偿编码键控调制方式，采用点对点模式和基本模式两种运作模式，在数据传输速率方面可以根据实际情况在 11Mbit/s、5.5Mbit/s、2Mbit/s、1Mbit/s 的不同速率间自动切换，它改变了 WLAN 的设计状况，扩大了 WLAN 的应用领域。

802.11b 已成为当前主流的 WLAN 标准，被多数厂商所采用，所推出的产品广泛应用于办公室、家庭、宾馆、车站、机场等众多场合。然而随着网络应用中视频、语音等关键数据传输需求越来越多，速率问题将会成为 802.11b 进一步发展的主要障碍。此外 802.11b 使用的是 ISM2.4GHz 波段，而家用微波炉、蓝牙芯片和无绳电话（在北美）也都使用这个波段，所以相对 802.11a 而言，802.11b 还面临着更多的干扰源。此外 802.11b 存在的安全问题也不容忽视，目前主要通过 WEP 加密协议来弥补这一缺陷，IEEE 也正在开发另外一个标准 802.11i 来专门解决 WLAN 中的安全问题。

1999 年 802.11a 标准制订完成，该标准规定 WLAN 工作频段为 5.15GHz～5.825GHz，数据传输速率达到54Mbit/s或72Mbit/s，传输距离控制在10～100m。该标准也是 802.11 的一个补充，扩充了标准的物理层，采用正交频分复用的独特扩频技术和 QPSK 调制方式，可提供 25Mbit/s 的无线 ATM 接口和 10Mbit/s 的以太网无线帧结构接口，支持多种业务如话音、数据和图像等，一个扇区可以接入多个用户，每个用户可带多个用户终端。

虽然 802.11a 在技术上和出台时间上都占有优势，但由于技术成本过高，缺乏价格竞争力，经济规模始终无法扩大，加上 5GHz 并非免费频段，在部分地区面临频谱管制的问题，市场销售情况一直不理想。除了成本问题，802.11a 最大的缺陷就是无法与 802.11b 兼容，使它在市场上的扩展大受限制，802.11g 的出现也给它带来极大的压力。

2003 年 6 月 12 日，IEEE 正式推出 802.11g 标准，7 月 28 日，通过 Wi－Fi 认证的 802.11g 产品上市。该标准提出拥有 802.11a 的传输速率，安全性较 802.11b 好，采用两种调制方式：802.11a 中采用的 OFDM 与 802.11b 中采用的 CCK，做到了与 802.11a 和 802.11b 的兼容。802.11g 的兼容性和高数据速率弥补了 802.11a 和 802.11b 各自的缺陷，一方面使得 802.11b 产品可以平稳地向高数据速率升级，满足日益增加的带宽需求；另一方面使得 802.11a 实现与 802.11b 的互通，克服了 802.11a 一直难以进入市场主流的尴尬，因此 802.11g 一出现就得到众多厂商的支持。

802.11i 标准结合 802.1x 中的用户端口身份验证和设备验证，对 WLAN 的 MAC 层进行修改与整合，定义了严格的加密格式和鉴权机制，改善 WLAN 的安全性。据 Wi－Fi 联盟预测，该标准预计将于 2004 年 6 月核准推出。

2、HiperLAN 系列

HiperLAN 是欧盟在 1992 年提出的一个 WLAN 标准[26][27]。2000 年，HiperLAN2 标准制订完成。HiperLAN2 部分建立在 GSM 基础上，使用频段为 5GHz。在物理层上 HiperLAN2 和 802.11a 几乎完全相同：采用 OFDM 技术，最大数据传输速率为 54Mbit/s。HiperLAN2 标准详细定义了 WLAN 的检测功能和转换信令，用以支持更多无线网络，并支持动态频率选择、无线信元转换、链路自适应、多束天线和功率控制等。它和 802.11a 最大的不同是 HiperLAN2 不是建立在以太网基础上的，而是采用 TDMA 结构，形成一个面向连接的网络。HiperLAN2 的面向连接的特性使它很容易满足 QoS 要求，可以为每个连接分配一个指定的 QoS，确定这个连接在带宽、延迟、拥塞、比特错误率等方面的要求。这种 QoS 支持与高传输速率一起保证了不同的数据序列（如视频、话音和数据等）可以同时进行高速传输。

HiperLAN 对应 802.11b，HiperLAN2 与 802.11a 具有相同的物理层，它们可以采用相同的部件。另外，HiperLAN2 强调与 3G 的整合。HiperLAN2 标准也是目前较完善的 WLAN 协议，支持 HiperLAN2 标准的厂商主要集中在欧洲地区。

3、HomeRF 系列

HomeRF 工作组是由美国家用射频委员会领导、于 1997 年成立的[28]，其主要工作任务是为家庭用户建立具有互操作性的话音和数据通信网。它于 2001 年 8 月推出 HomeRF2 标准，该标准集成了语音和数据传送技术，工作频段为 10GHz，数据传输速率达到 100Mbit/s，在 WLAN 的安全性方面主要考虑访问控制和加密技术。

HomeRF 是对现有无线通信标准的综合和改进：当进行数据通信时，采用 IEEE802.11 规范中的 TCP/IP 传输协议；当进行语音通信时，则采用数字增强型无绳通信标准。但是，该标准与 802.11b 不兼容，并占据了与 802.11b 和 Bluetooth 相同的 2.4GHz 频率段，所以在应用范围上会有很大的局限性，更多的是在家庭网络中使用。

4、蓝牙技术

蓝牙（IEEE 802.15）是一项最新标准，对于 802.11 来说，它的出现不是为了竞争而是相互补充。蓝牙比 802.11 更具移动性，比如，802.11 限制在办公室和校园内，蓝牙能把一个设备连接到 LAN 和 WAN，甚至支持全球漫游。此外，蓝牙成本低、体积小，可用于更多的设备。但是，蓝牙主要是点对点的短距离无线发送技术，本质上要么是 RF 要么是红外线[29]。而且，蓝牙被设计成低功耗、短距离、低带宽的应用，严格来讲，不算是真正的局域网技术。

以上几种无线局域网标准的简要比较见表 2-2。

	802.11	802.11b	802.11a	Bluetooth	HomeRF
频率	2.4GHz	2.4GHz	5GHz	2.4GHz	2.4GHz
带宽	1~2Mbps	可达 11Mbps	可达 54 Mbps	1Mbps	1~2Mbps 可增至 11Mbps
距离	100m 功率增加可扩展	100m	5~10km	10m~100m	100m
业务	数据	数据 图像	语音 数据 图像	语音 数据	语音 数据

表 2-2　无线局域网几种标准的比较

2.4 无线局域网的应用领域

无线局域网的主要应用领域如下：

接入网络信息系统：电子邮件、文件传输和终端仿真[30]；

难以布线的环境：老建筑、布线困难或昂贵的露天区域、城市建筑群、校园和工厂；

频繁变化的环境：频繁更换工作地点和改变位置的零售商、生产商，以及野外勘测、试验、军事、公安和银行等；

使用便携式计算机等可移动设备进行快速网络连接；

用于远距离信息的传输：如在林区进行火灾、病虫害等信息的传输；公安交通管理部门进行交通管理等；

专门工程或高峰时间所需的暂时局域网：学校、商业展览、建设地点等人员流动较强的地方利用无线局域网进行信息的交流；零售商、空运和航运公司高峰时间所需的额外工作站等；

流动工作者可得到信息的区域：需要在医院、零售商店或办公室区域流动时得到信息的医生、护士、零售商、白领工作者；

办公室和家庭办公室（SOHO）用户，以及需要方便快捷地安装小型网络的用户。

2.5 无线局域网的安全综述

无线局域网移动通信系统的安全威胁，根据攻击的位置可分为以下几类：无线链路威胁、服务网络威胁和终端威胁。

（1）无线链路威胁　终端设备与服务网之间的无线接口可能受到以下攻击威胁[31]。

- 非授权访问数据：入侵者可以窃听无线链路上的用户数据、信令数据和控制数据，甚至可以进行被动或主动流量分析。
- 对完整性的威胁：入侵者可以修改、插入、重放和删除无线链路上的合法用户的数据或信令数据。
- 拒绝服务攻击：入侵者通过在物理上或协议上干扰用户数据、信令数据和控制数据在无线链路上的正确传输，来实现无线链路上的拒绝服务攻击。

（2）服务网络威胁　在服务网络内的攻击可分为以下几类。

- 非授权访问数据：入侵者在服务网内窃听用户数据、信令数据和控制数据，非授权访问存储在系统网络单元内的数据，甚至可以进行被动或主动流量分析[32]。
- 对完整性的威胁：入侵者可以修改、插入、重放或删除用户的业务数据、信令数据或控制数据；还可以假冒通信的某一方对通信的数据进行修改，甚至可以修改存储在网络单元中的数据。
- 拒绝服务攻击：入侵者通过在物理上或协议上干扰用户数据、信令数据或控制数据在网络中的正确传输，来实现网络中的拒绝服务攻击；还可以通过假冒某一网络单元阻止合法用户的业务数据、信令信息或控制数据，从而使合法用户无法接受正常的网络服务。
- 否认：用户可能对业务费用、业务数据来源或对接收到其他用户的数据进行否认；网络单元否认发出信令或控制数据或否认接收到其他网络单元发出的信令或控制数据。
- 非授权访问服务：入侵者可能模仿合法用户使用网络服务，也可能假冒服务网，当有合法用户接入时就有可能获得网络服务；入侵者还可假冒归属网，以获取使其他假冒某一用户所需的信息；用户滥用其权限以获取对非授权服务的访问；服务网滥用其权限以获取对非授权服务的访问。

（3）终端威胁　与终端相关的安全威胁如下[33]。

- 攻击者利用终端的终端设备访问系统资源；
- 对系统内部工作有足够了解的攻击者可能获取更多的访问权限；
- 攻击者利用借来的终端超出允许的范围访问系统；
- 通过修改、插入或删除终端中的数据以破坏终端数据的完整性；
- 通过修改、插入或删除 USIM 卡中的数据以破坏 USIM 卡数据的完整性。

无线局域网和传统有线局域网，均符合现有的网络协议。网络系统的安全涉及到平台的各个方面。按照网络 OSI 的七层模型，网络安全贯穿于整个七层模型。针对网络系统实际运行的 TCP/IP 协议，网络安全贯穿于信息系统的 4 个层次。对应网络系统的安全体系层次模型，如表 2-3 所示。

应用层	应用系统	应用层	应用系统安全
	应用平台		应用平台安全
会话层		会话安全	
网络层		安全路由/访问控制	
数据链路层		链路安全	
物理层		物理层信息安全	

表 2-3　网络系统的安全体系层次模型

（1）物理层 物理层信息安全，主要防止物理通路的损坏、物理通道的窃听、对物理通路的攻击（干扰等）。

（2）数据链路层 保证链路层的网络安全，保证通过网络链路传送的数据不被窃听。主要采用加密通信（远程网）等手段。

（3）网络层 网络层的安全需要保证网络只给授权的客户使用授权的段务，保证网络路由正确，避免被拦截或监听。

（4）操作系统　操作系统安全要求保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

（5）应用平台　应用平台指建立在网络系统之上的应用软件服务，加数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术（如 SSL 等）来增强应用平台的安全性。

（6）应用系统 应用系统的最终目的是为用户服务。应用系统的安全与系统设计和实现关系密切。应用系统促使应用平台提供的安全服务来保证基本安全，如通信内容安全，通信双方的认证，审计等手段。

由于无线局域网是采用射频技术进行网络连接及传输的开放式物理系统，其安全性要表现在物理层、链路层和网络层，其他几个方面的安全性与有线网类似。

网络的安全策略从具体上也是与 TCP/IP 协议相符合的。如果原先的安全策略是为一个封闭的有线局域网而制定的，如果引入了一个或多个无线局域网应用，假定在无线局域网自身能提供良好的安全保障情况下（即无线局域网可以提供良好的安全保障，以弥补其传输方式的改变所带来的在物理层、链路层和网路层上的安全变化），完全可以把新增的无线局域网当作一个或多个子网来对待，无须对现有安全策略做根本性调整。

无线局域网与有线局域网在物理层、链路层和网络层的主要差别如下[34]。

2.5.1 物理层的安全

目前，无线局域网使用的扩频技术主要有直接序列扩频和跳频技术。直扩和跳频技术的抗干扰机理不同，直扩系统靠伪随机码的相关处理，降低进入解调器的干扰功率来达到抗干扰的目的；而跳频系统是靠载频的随机跳变，躲避干扰，将干扰排斥在接收通道以外来达到抗干扰的目的。因此，这两者仍具有很强的抗干扰的能力，各有特点，也各有不足。

（1）抗强的定频干扰　由直扩抗干扰的机理可知，直扩抗干扰是通过相干解扩取得处理增益来达到抗干扰的目的，但超过了干扰容限的定额干扰将会导致直扩系统的通信中断或性能急剧恶化。而跳频系统是采用躲避的方法抗干扰，强的定额干扰只能干扰跳频系统的一个或几个频率，若跳频系统的频道数很大，则对系统性能的影响是不严重的。

（2）抗衰落　特别是频率选择性衰落，这是室内通信环境下必须解决的问题。由于直扩系统的射频带宽很宽，小部分频谱衰落不会使信号频谱产生严重的畸变，而对跳频系统而言，频率选择性衰落将导致若干个频率受到影响，导致系统性能的恶化。跳频系统要抗这种选择性衰落，可采用快速跳频的方法，使每一个频率的驻留时间非常短，平均衰落就非常低。

（3）抗多径干扰 多径问题是在移动通信、室内通信等系统中必须考虑的问题。多径干扰是由于无线电在传播过程中遇到的各种反射体（如高山、建筑物、墙壁、天花板等）引起的反射或放射。在接收端的直接传播路径和反射信号产生的群反射之间的随机干涉形成的。多径干扰信号的频率选择衰落和路径差引起的传播时延，会使信号产生严重的失真和波形展宽，导致码间干扰，不但能引起噪声增加和误码率上升，使通信质量降低，甚至使某些通信系统无法工作。由于直扩系统采用伪随机码的相干解扩，只要多径时延大于一个伪随机码的频谱宽度，这种多径就可能对直扩系统形成干扰，直扩系统甚至可以利用这些干扰能量来提高系统的性能。而跳频系统则不然，跳频系统要抗多径干扰，则要求每一跳的驻留时间很短，即要求快跳频。在多径信号没有到来之间接收机已开始接收一下跳信号。从实现上看，实现伪随机码速率大于 1Mchop/s 的直扩系统比跳频速率 1Mhop/s 要容易得多。

（4）抗窃听性　由于扩频系统将传送的信息扩展到很宽的频带上去，其功率密度随频谱的展宽而降低，甚至可以将信号掩没在噪声中。因此，其保密性

很强，要截获或窃听、侦察这样的信号是非常困难的，除非采用与发送端所用的扩频码与之同步后进行相关检测，否则对扩频信号是无能为力的。由于扩频信号功率谱密度很低，在许多国家，如美、日、欧洲等国家对专用频段，如 ISM 频段，只要功率谱密度能够满足一定的要求，就可以不经批准使用该频段[35]。

2.5.2 链路层的安全

IEEE802.11b 标准规定了一种称为有线等效保密 WEP[36]（Wired Eequivalent Protocol）的可选加密方案，提供了确保无线局域网数据流的机制。WEP 采用的加密算法是由 Ron Rivets of RSA Data Security Inc 在 1987 年设计的 40 位的 RC4 算法。RC4 加密算法属于对称流密码，支持可变长度密钥。WEP 采用 RC4 对数据进行加密，它将初始化向量 IV（Initialization Vector ）和共享密钥 k 两部分经过“异或 XOR”运算形成密钥，并扩展成为任意长度的伪随机位“密钥流”。加密过程就是将产生的密钥流与明文信息进行“异或 XOR”运算；解密过程为基于 IV 和 k 产生相同的密钥流，将它与密文信息相“异或 XOR”运算，WEP 中 IV 长度为 24 位。

WEP 能够为无线局域网提供与有线网络相同级别的安全保护，用于保障无线通信信号的安全性（保密性与完整性）；以防止无线网络的非授权访问（通过对密钥的保护，使没有密钥的非授权者无法访问网络）。

因此，采用 IEEE 802.11 标准的无线局域网是否安全，很大程度上是由 WEP 的安全性来决定的。

在 WEP 中，通信的报文加入了完整性校验 IC （Integrity Check）以保证通信信息的完整性。为了避免使用重复的密钥流，WEP 则使用了初始化向量 IV，用于对不同的数据包产生不同的 RC4 密钥。每个数据包使用不同的初始化向量 IV，最简单的做法就是 IV 从 0 算起，每一次接收或发送一个数据包，IV 就加 1，而 IV 就包含在通信的数据包文中。

在 WEP 的设计中期望达到 3 个主要目标[37]。

（1）机密性（Confidentiality） WEP 最基本的目标就是为了防止偶尔窃取无线局域网中的数据行为；

（2）访问控制（Access control） WEP 的第 2 个目标是对无线网络设备询问的控制。在 IEEE 802.11 中设计了一个可选的功能，它可以使无线网络设备

丢弃没有采用 WEP 正确加密的所有数据包。

（3）数据完整性（Data integrity） 第 3 个目标是阻止对传输数据的篡改。在 WEP 数据帧结构中完整性校验和段的设置就是为了保证这个目的。

IEEE802.11 标准提供了两个方案来对 WLAN 中的 WEP 密钥进行定义。第一种方案中，无线子系统中所有的工作站（包括客户机和访问点）共享一套 4 个缺省的密钥。当一个客户机得到缺省的密钥后，它可以安全地和系统中其他所有的工作站进行通信。这种缺省密钥的问题在于它们越是广泛地进行分配，就越有可能暴露。第二种方案中，每个客户机建立和其他工作站“密钥映射”关系。这种方案工作起来更为安全，因为拥有密钥的工作站更少。但当工作站的数量不断增加时，分配这样一个独一无二的密钥会变得很困难。

尽管 WEP 是可选的，但无线以太网兼容性联盟 WECA（Wireless Ethernet Compatibility Alliance）要求无线相容性认证 Wi-Fi （Wireless Fidelity），认证的产品支持 WEP 的 40 位密钥，因此，WECA 成员都支持 WEP。有的厂家利用软件实现加密和解密过程的大量计算，也有的厂家，如 Cisco，利用硬件加速器来保证数据流加密和解密过程中的性能损失最小。

2.5.3 网络层的安全

IEEE 802.11b 标准定义了 3 种机理来提供 WLAN 的访问控制和保密：服务配置标识符 SSID（Service Setup Identifier）；身份认证（Authentication）；虚拟专用网 VPN（Virtual Private Network）[38]。下面进行简单介绍。

（1）服务配置标识符 SSID WLAN 中经常用到的一个特性是称为 SSID 的命名编号，它提供低级别上的访问控制。SSID 通常是 WLAN 子系统中设备的网络名称，它利用于在本地分割子系统。SSID 作为编号来允许/拒绝访问是危险的，因为 SSID 的安全性并不好。把无线客户机连接到有线网络的设备称为访问点，它通常在自己的信标中广播 SSID。

（2）身份认证 一个客户机在进行身份验证之前不能接入到 WLAN 中。IEEE 802.11b 标准定义了两种身份验证的方法：开放式和共享密钥式。身份验证必须在每台客户机上进行设置，并且这些设置应该能够与打算和客户机通信的所有访问点相匹配。

开放式身份验证为缺省的方法，整个验证过程以明码电文的方式完成，即

使客户机没有提供正确的 WEP 密钥也能和访问点进行通信。在共享密钥的方法中，访问点发送给客户机一个访问文本信息包，客户机必须使用正确的 WEP 密钥对它进行编码，并且把它返回访问点。如果客户机提供的密钥错误或者根本没有提供密钥，说明身份验证失效，它将不会允许和访问点进行通信。

一些 WLAN 厂商支持基于客户机物理地址，或者说基于介质访问控制 MAC（Media Access Control）地址的身份验证方法。只有当客户机的 MAC 地址与访问点所使用的验证表中的地址相匹配时，访问点才允许客户机与它进行通信。

（3）虚拟专用网 VPN　虚拟专用网 VPN 加密机制是透明运行在 WLAN 上的，它的使用独立于任何本地 WLAN 安全方案，这在后文简要论述。

2.6 无线局域网的主要安全措施的缺陷及改进

1、SSID 技术

SSID 用来区别不同的局域网[39]，但人们常采用一些有意义的名称以便记忆，如厂商名、地点或部门名称。这些默认的 SSID 很容易被非法用户猜到，使得黑客很轻易进入网络。因此，SSID 应该像密码一样，使用长而有意义的字符，包括字母、数字和符号。

另外，AP 的默认设置为定时广播 SSID，以便于相关用户更容易找到正确的网络，但也使得未经认证的用户可以轻易地发现可用的 SSID。这也是大多数无线局域网侦测软件的工作方式，使其没有 SSID 仍可以找到网络。

因此，在把 SSID 作为保护无线局域网的基本措施时，应将 SSID 当做密码来设定，不使用容易猜到的字串，而且禁用 AP 的广播功能。

但是，这也并不是一种根本的解决方案，因为如果用户设置的密码过长的话，会给使用过程带来很多不必要的麻烦，太短的话，黑客仍然可以使用穷举法之类的破解方法以软件的形式去破解。

2、MAC 地址过滤

如同 AP 可以用 SSID 来区别，每一个网络终端的 WLAN 网卡都有一个唯一的 MAC 地址。每个 AP 都存有一个合法的 MAC 地址列表，只有在该表中的

设备才能进入网络。但这种机制有两个问题。

第一个问题是数据管理的问题[40]。使用这项技术，无线局域网管理员就必须持续维护这个 MAC 数据库，实时更新数据库。这个数据库要么保存在每一个 AP 上，要么保存在 AP 都“可见”的服务器上。一旦有终端的 MAC 地址改变，管理员就必须更新所有的数据库以适应目前的情况。在拥有成百台设备的企业应用环境中，这就不是一个小问题，可能需要一个专职人员进行数据库实时管理。

第二个问题是 MAC 地址过滤并不是 100%的安全。攻击者可以通过无线嗅探器来监听无线通信，可以轻易从用户的数据中得到认可的 MAC 地址，即使是加密过的用户数据，接下来攻击者就可以使用合法的 MAC 地址来实现入侵。

因此，MAC 地址过滤适用与规模较小、安全级别不是很高的网络。

3、基于 WEP 的安全机制

WEP 安全性的分析主要从以下几个方面考虑。

1）密钥流复用

WEP采用流密码算法RC4对数据进行加密[41]，它将密钥（在WEP中为公共初始向量IV和密钥Key两部分）扩展成为任意长度的伪随机位“密钥流”。加密过程就是将产生的密钥流与明文信息进行异或运算；解密过程包括：基于IV和密钥产生相同的密钥流，将它与密文信息相异或。

众所周知，流密码算法的缺陷是：如果对2个不同的消息使用相同的IV和密钥进行加密，则可以把2个消息的信息都破解出来。

2） 完整性校验

WEP使用了40位的流密码RC4算法。RC4流密码是一种一次将1Byte明文变化为1Byte密文的对称密码，密文通过把明文与密钥流（伪随机序列）进行异或运算产生，解密时把相同的密钥流与密文异或即可。由于流密码具有这样的特点，它对消息的完整性要求很高。

为了保证通信信息的完整性，在WEP中的通信报文加入了完整性校验IC域，以保证数据包在传输过程中不被篡改。完整性校验和采用CRC-32校验和，作为通信报文的一部分，CRC-32校验和也要经过加密。但事实上，CRC-32校验和并不能胜任保证攻击方不对信息数据的修改。这是因为CRC-32校验和不是一种基于密码学的安全认证代码。CRC-32校验和作为一种完整性校验方式，主要设计用于检测

信息数据中的随机错码。CRC-32校验和一般用于检查非恶意的突发性错误（如由于传输信道噪声而导致的错误），但它对于抵抗蓄谋恶意的攻击显然就显得软弱无力。另外，CRC-32校验和作为信息数据的一部分和信息数据一起采用流密码进行加密，更加加剧了它自身的弱点。

出现这种问题的主要原因是CRC-32的算法是线性的，就是说CRC-32校验和具有强烈的数据关联性，这一点与密码学要求的随机性相反。并且，CRC-32 算法本身就十分简单，所以，恶意的攻击方完全可以做到在信息数据流中插入比特位后调整CRC-32校验和与其相符，使数据看起来没有发生变化，从而轻松地实施攻击。

通过对WEP的分析，发现WEP存在许多明显的致命缺陷。无论WEP采用的密钥长度如何，这些缺陷使得经WEP保护的数据保密性毫无意义。将WEP的密钥长度从40位增加到104位，或者128位对于增加WEP的抵抗攻击能力没有任何帮助。这主要是与WEP采用怎样的保密机制有关，而与采用的密钥长度无关。因此，对于其使用者来说结果是悲剧性的。所以，为了达到有线等价保密性（WEP）的目标，必须对WEP进行明显的改进。

1） 密码和运行模式的改进

当今对称密钥加密算法的研究必须依据AES块密码的方法进行研究。高级加密系统AES（advanced encryption system）被公认为与许多流行的对称密钥加密算法一样，是优秀的加密算法。具有实现效率高，应用范围广泛（从8位处理器到超级计算机均可适用）的特点。建议未来的WEP应该强制采用128位的AES加密算法作为加密机制。

WEP采用AES，的偏移代码本运行模式OCB（offset codebook mode），同样，它也是流密码，产生一个消息认证代码，用于阻止攻击者进行消息伪造。OCB模式下被加密数据的长度与明文数据的长度相同，单独一个密钥用于加密和认证。OCB模式仅需要AES，加密引擎，不需要解密引擎，它是一种并行工作方式。OCB模式对密码学的起始要求较低，可以在一次传递中同时完成一个消息的加密/解密和标记/校验。

在OCB模式中的密钥实际是步长，即偏移量（这也是OCB模式的得名）和。步长和的大小决定了密码块的大小（在AES，中为128 位）。在每一节中，步长只计算一次。OCB 的每个帧超帧头中128位用于OCB认证标志。

2 ）节密钥产生

这里提出一个节密钥产生算法， 用于现在WEP正在使用的手动配置基本密钥的情况。而对于动态密钥分配则无需引入节密钥产生算法。

节密钥产生算法生成2个节密钥：一个用于发送,一个用于接收。

A）将（a）BSSID，（b）发送方的MAC地址，（c）接收方的MAC地址连接起来组成一个序列串。每个地址的顺序十分重要，特别是发送方地址和接收方地址不能颠倒。

B）使用基本密钥（手动配置的密钥）和1个128位全零的IV， 对A)中产生的序列串运行OCB-AES算法。

OCB-AES算法的作用是：（1）将基本密钥从直接攻击中消除；（2）将节密钥与特殊使用它的部分进行弱连接。在这种算法下，虽然所有的BSS成员都共享同样的基本密钥，而相同级别的不同终端设备使用的节密钥是不同的。但是，当基本密钥是一个密码，或者采用相关技术从密码中得出基本密钥时，这种算法就不能抵抗字典攻击。假如，基本密钥被攻击者破获，则所有的密钥就会被欺骗。这个缺陷是该算法无法避免的。

3 ） 随机数

建议采用的随机数产生是安全的和真正随机的，这一点在密码学中至关重要。

4） 数据分装

建议WEP采用的新的数据分装技术，包括：

a）采用128位的IV 在每节开始初始化时，加密方随即选择。对于连续帧，译码方则从前1个被加密的数据帧中选用最后的128位被加密的数据作为密钥；

b）采用32位的序列数 这个32位的序列数会被首先量化加密。它表示在当前密钥已经发送的数据帧的数目。当使用手动配置密钥时，这个序列数将停止使用，设置为全零；当采用动态密钥时，在密钥建立起来的时候，这个序列数被初始化为零；

c）采用LLC数据载荷，这个数据也要加密；

d）采用128位的OCB数据认证标志这种数据封装方法将增加36字节到数据帧中。这是当今网络安全必须付出的代价。

当WEP开始封装数据的时候，加密方首先检查计数器是否已经计满（计到最

大值）。如果计数器已经计满，则停止使用当前密钥对数据流进行加密，直到密钥管理系统更换了基本密钥。假如计数器还没有计满，并且使用动态密钥，则加密方将计数器加1，并将这个新的计数器值插入到帧的适当位置。加密方选择当前值，采用OCB对计数器和数据进行加密和标识。它将OCB认证标志加在数据帧尾。现在，数据帧就可以传输了。

当WEP要对接收到的数据进行拆包的时候，译码方根据到达的MAC地址确定正确的位置。译码方使用数据帧中的IV与OCB中的IV进行比较，将数据包解密，并验证它的认证特性。假如，采用了动态的密钥，最终还要验证计数器的值是否比以往接收到的值大，即WEP接收方始终保持一个为1的接收窗口。这一点可以防止当前密钥是动态分配时的重放攻击，重放不采用动态密钥分配是不可行的。

2.7 解决无线局域网安全的主要思路

无线传输的媒质是共享的，也正是这个原因，相对有线网络来说，通过无线局域网发送和接收数据时更容易被窃听。设计一个完善的无线局域网系统，加密和认证是需要考虑的两个必不可少的安全因素。无线局域网中应用加密和认证技术的最根本的目的就是使无线业务能达到有线业务同样的安全等级。在任何系统中实现加密和认证都必须考虑以下 3 个方面[42]。

（1）用户对保密的需求程度　用户对保密需求的不断膨胀以及对保密要求的不断提高是促进加密和认证需求发展的源动力。在很大程度上，加密和认证技术的设计思路是综合分析用户对保密的需求程度的结晶。

（2）实现过程的易操作性　如果安全机制实现过于复杂，那么就很难被普通的用户群接受。所以，安全机制必须具有易操作性。

（3）政府的有关规定　许多政府（如美国政府等）都认为加密技术是涉及国家安全的核心技术之一，许多专门的加密技术仅限应用于国家军事领域中。因此，几乎所有的加密技术都是禁止或者限制出口的。

无线局域网安全解决措施主要有以下几种思路：

1. 有线等价保密协议 WEP[43][44][45]

这在前一小节已经提到过，其中最重要的思路就是对 RC4 算法进行改进。

2. VPN 的解决方案[46][47][48]

对于较大规模和安全等级高的商业网络来说，VPN 是替代 WEP 和 MAC

地址过滤的较为理想的无线接入的安全方案。在 VPN 安全方案中，VPN 为接入用户提供一条专用的安全接入隧道到内部网络，常用的隧道有 PPTP 和 L2PP，网络结构为标准的集中认证结构，如 RADIUS 服务器认证。客户端与内部网络被 AP 和 VPN 服务器之间的局域网和 VPN 服务器隔开。VPN 服务器负责客户端的认证和传输加密，同时作为内部网络的网关。

VPN 方案的优点有：1）适用于用户众多的大规模网络；2）对 AP 和客户端的管理需求小，而 VPN 服务器可集中管理；3）客户端与内部网络隔离，通信前必须经过 VPN 认证；4）WEP 密钥和 MAC 地址列表的管理成为可选项；5）统一的用户界面。

VPN 使用起来也有一些缺点：1）现阶段 WLAN 的 VPN 安全方案不支持广播功能。大规模网络通过广播功能从信息源向多用户传送视频、音频等信息，如果通过多个点对点传送来实现，将占用网络的很多带宽，而广播能更有效地利用网络带宽在骨干线路上传输这些信息。2）当移动终端从一个 VPN 服务器所在的子网漫游到另一个子网，用户需重新登陆。同样，当客户端从待机模式重新激活时也需要重新登陆。

3.802.1x

这也是本论文研究的重点，在后面的几章中论述。

第三章 IEEE802.1x 协议及 EAP-TLS 认证

3.1 IEEE802.1x 认证协议

3.1.1 IEEE802.1x 的提出背景

有线局域网通过固定线路连接组建，计算机终端通过网络接入固定位置物理端口，实现局域网接入，数据传输直接送到目的地，这里没有直接控制到端口的方法，也不需要控制到端口，这些固定位置的物理端口构成有线局域网的封闭物理空间。但是，由于无线局域网的网络空间具有开放性和终端可移动性，因此很难通过网络物理空间来界定终端是否属于该网络。随着无线局域网的广泛应用，如何通过端口认证来实现用户级的接入控制就成为一项非常现实的问题。IEEE802.1x 正是基于这一需求而出现的一种认证技术[49]。

IEEE802.1x 协议，称为基于端口的访问控制协议，是由 IEEE 于 2001 年 6 月提出的，符合 IEEE802 协议集的局域网接入控制协议，主要目的是为了解决无线局域网用户的接入认证问题，能够在利用 IEEE802 局域网优势的基础上提供一种对连接到局域网用户的认证和授权手段，达到接受合法用户接入，保护网络安全的目的。

目前，IEEE802.1x 认证协议作为业界最新的标准已经得到了很多网络设备制造商的重视，Cisco,3Com,Avaya,D-Link 等纷纷组织研发力量进行基于 IEEE802.1x 协议相关产品的开发。作为软件厂商，微软在 Windows XP 中已经整合了 IEEE802.1x 客户端软件，无须另外安装客户端软件。

3.1.2 IEEE802.1x 的体系结构

协议的体系结构包括三个重要的部分：客户端、认证系统和认证服务器[50][51]。

客户端称作申请者，一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，当用户有上网的需求时，通过启动这个客户端软件发起

IEEE802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端系统需支持 EAPOL 协议。

认证系统，称作认证者，在 WLAN 中就是无线接入点，在认证过程中只起到“透传”的功能，所有的认证工作在申请者和认证服务器上完成。

认证服务器，通常采用远程接入用户认证服务的服务器，该服务器可以存储有关用户的信息，通过检验用户端发送来的信息判别用户是否有权使用网络系统提供的网络服务。

IEEE802.1x 标准采用现有的认证协议，即 IETF 提出的 PPP 协议的扩展—EAP（可扩展认证协议），EAP 消息包含在 IEEE802.1x 消息中，被称为 EAPOL，即 EAP over LAN（在无线局域网中称作 EAPOW，也就是 EAP over Wireless），在 Supplicant 和 Authenticator 之间传输；Authenticator 与 Authentication Server 间同样运行 EAP 协议，EAP 帧中封装了认证数据，将该协议承载在其他高层次协议中，如 Radius，以便穿越复杂的网络到达认证服务器，称为 EAP over RADIUS。

认证系统和认证服务器之间的通信可以通过网络实体进行，也可以使用其它的通信通道，例如认证系统和认证服务器集成在一起，两个实体之间的通信就可以不采用 EAP 协议。

3.1.3 IEEE 802.1x 的认证过程

（1）当用户有上网需求时，用户打开 IEEE 802.1x 客户端程度，输入用户和口令发起连接。此时，申请者将发出“请求认证”报文给 AP，开始启动一次认证过程。

（2）AP 收到“请求认证”数据帧后，发出请求帧，要求用户的客户端程序将输入的用户名送上来。

（3）客户端程序响应请求，将“用户名”信息通过数据帧送给 AP，AP 将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

（4）认证服务器收到 AP 转发上来的“用户名”信息后，将该信息与数据库中的“用户名”表项相比较，找到该“用户名”对应的“口令”信息，用随即生成的加密字对其进行加密处理（MD5 算法），同时将此加密字传给 AP，并

通过 AP 转传给客户端的程序。

（5）客户端程序收到 AP 转传来的加密字后，用该加密字对“口令”部分进行加密处理，并通过 AP 转传给认证服务器。

(6)认证服务器将送上来的加密后的口令信息和之前自己经过加密运算后的口令信息进行对比。如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向 AP 发出打开控制端口指令，允许用户的业务流通过控制端口访问网络；否则，把反馈认证失败的消息，并保持 AP 的端口关闭的状态，只允许认证信息数据通过而不允许非认证数据通过。

（7）认证成功后，认证服务器通过有线 LAN 向 AP 发送会话密钥。

3.1.4　IEEE 802.1x 协议的优点

与传统的 PPPoE 和 Web/Portal 认证方式相比，IEEE 802.1x 认证协议具有以下优点，能更好地适应现代网络用户数量急剧增加和业务多样性的要求。

1. 协议实现简单[52]

IEEE 802.1x 协议为二层协议，不需要达到三层，对设备的整体性能要求不高，可以有效降低建网成本。

采用 IEEE 802.1x 方式，用户可以以有线网络的速度进行工作，一台服务器能够在多个接入点之间处理多达 20000 个用户的认证。

2. 认证和业务分离，易于运营

IEEE 802.1x 的认证体系结构中采用了“控制端口”和“非控制端口”的逻辑功能，仅仅关注端口的打开与关闭。当合法用户接入时，该端口打开；当非法用户接入或没有用户接入时，该端口处于关闭状态。认证的结果在于端口状态的变化，而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题，是各种认证技术中最简化的方案。

接入认证通过以后，IP 数据包在二层普通 MAC 帧上传送，认证后的数据流和没有认证的数据流完全一样，这是由于认证行为仅在用户接入的时刻进行，认证通过后不再进行合法性检查。业务流和认证流实现分离，对后续的数据包处理没有特殊要求，所有业务都不受认证方式限制，易于实现多业务运营。

3. 安全可靠

（1）用户身份识别取决于用户名，而不是 MAC 地址，从而可以实现基于用户的认证、授权和计费。

（2）支持可扩展的认证，主要地无口令认证，如公钥证书和智能卡、互联网密钥交换协议（IKE）、生物测定学、信用卡等，同时也支持口令认证，如一次性口令认证、通用安全服务应用编程接口（GSS_API）方法（包括 Kerberos）。

（3）动态密钥生成保证每次会话密钥各不相同，并且不必存储于 NIC 和 AP 中。

（4）全局密钥（Global Key）可以在会话密钥的加密下安全地从接入点传给用户。

（5）相互认证有效防止了中间人攻击和假冒接入点 AP，还可以防范地址欺骗攻击、目标识别和拒绝服务攻击等，并支持针对每个数据包的认证和完整性保护。

（6）可以在不改变网络接口卡的情况下，插入新的认证和密钥管理方法。

3.2 EAP 协议

3.2.1 EAP 的认证类型

通过使用 EAP，可以支持智能卡（Smart Card）、kerberos、公钥、一次性口令（OTP）等多种认证机制。请求/应答包中的类型域规定了 EAP 的各种类型，最初有以下几种类型[53]。

（1）Identity——用来查询对方的身份。

（2）Notification——由认证者用来向对方传递一条可显示的消息。

（3）Nak（Response only）——仅对应答包有效，作为不接受请求认证类型时的响应。

（4）MD5-Challenge——类似于 PPP CHAP 协议，包含质询消息。

（5）One-Time Password——请求包中含有一个 OTP 质询消息，应答类型为 OTP 或 Nak。

（6）Generic Token Card——用于要求用户输入各种类型的令牌卡。

除了以上的几种基本类型，为了提供更高的级别安全，逐渐增加了更多的

类型定义，比如 EAP-TLS 协议中请求/应答包的类型域相应为 EAP-TLS。传输层安全（TLS）协议提供相互认证、整体性保护加密套件协商及两端的密钥交换。使用 EAP-TLS，可以允许一个 PPP 端点吸收 TLS 协议中的优点来支持更多的认证机制。

3.2.2　EAP 的认证过程

可扩展认证协议 EAP 是 PPP（Point-to-Point Protocol）认证中的一个通用协议，其特点是 EAP 在链路控制协议（Link Control Protocol , LCP）阶段没有选定一种认证机制，而把这一步推迟到认证阶段。也就是说，EAP 可以支持多种认证机制，允许使用一个“后端”服务器来实际实现各种认证机制，认证者仅需要传送认证信息。EAP 协议本身具有良好的可扩展性，这使得在添加新的认证机制时丝毫不会影响现有协议的继续使用。1998 年，IETF 对 EAP 进行了标准化，即 RFC2284，“PPP Extensible Authentication Protocol（EAP）”。

EAP 认证过程简述如下[54]：

（1）在链路建立阶段完成后，认证者发送一个或多个请求（Request）数据包来对对方进行认证，该数据包中有一个类型域表明请求的类型。

（2）对方发送一个响应（Response）数据包对每一个请求做出应答。响应包中的类型域请求包中的类型域对应。

（3）认证者发送一个成功（Success）或失败（Failure）数据包结束认证阶段。

3.2.3 EAP 协议的主要特点

可扩展认证协议 EAP 提供了灵活的链路层安全结构，主要特点如下[55]。

（1）简单封装协议；不依赖于 IP、ACK/NAK 无滑动窗结构，不采用分组，因此操作简单。

（2）可以运行在任何链路层之上（PPP，IEEE 802.3，IEEE 802.5，IEEE 802.11 等），具有良好的适用性。

（3）EAP 采用高层认证技术，并且支持多种 IETF 安全协议标准（TLS，IKE，GSS-API 等），从而降低了链路层运算资源在安全上的开销。

（4）可方便地扩展支持未来的认证协议（如 DIAMETER），具有良好的可扩展性。

（5）可以运行于有损或无损媒体之上，包括无线媒体。

EAP 可以用就用于以下几个地方：EAP/PPP，EAPOL，EAP/RADIUS，EAP/Diameter，COPS 访问 PIB。

3.2.4 EAP 在 IEEE802.1X 中的应用

1、EAP 协议在 IEEE 802.1x 中应用的层次结构如图 3-1 所示

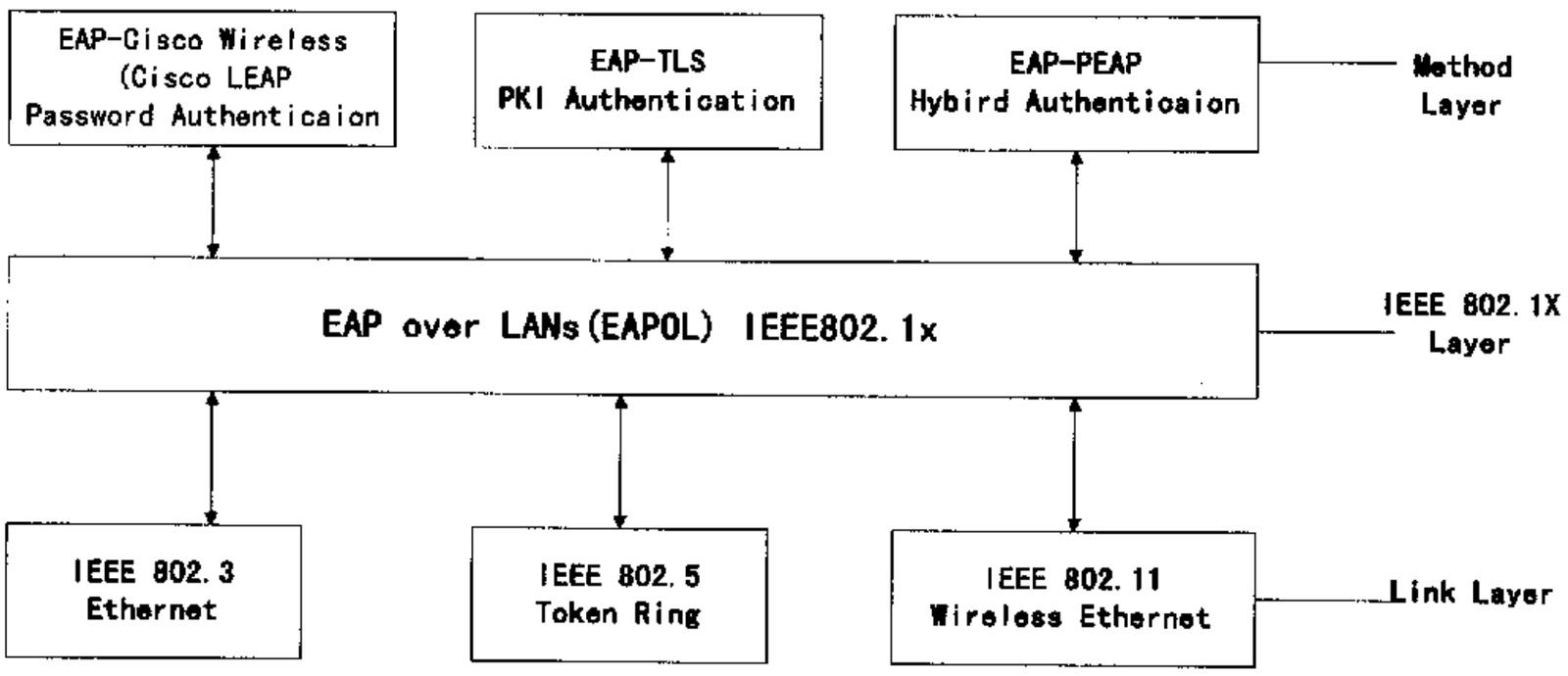


图 3-1 EAP 协议在 IEEE 802.1x 中应用的层次结构

2、EAPOL 消息的交互过程

EAP 消息被封装在 IEEE 802.1x 消息中，称做 EAPOL.

EAPOL 并没有一个固定的交互模式。下面以申请者发起的一次性口令认证为例，说明大多数情况采用的 EAPOL 消息的交互过程。

如图 3-2 所示，在申请者和认证者之间传输的 EAPOL 消息实线表示，承载于高层协议的 EAP 消息用虚线表示，认证者完成 EAP 消息的重新封装（re-packaging）来传输认证消息。根据采取的不同认证方法，质询（challenge）消息的数量和内容会有所不同。认证服务器把认证结果以 RADIUS-ACCEPT 或 RADIUS-REJECT 包形式传给接入点，接入点再重新封装 EAP-Success 或 EAP-Failure 消息给申请者。当申请者收到 EAP-Success 消息，说明认证成功可以接入 LAN 了。

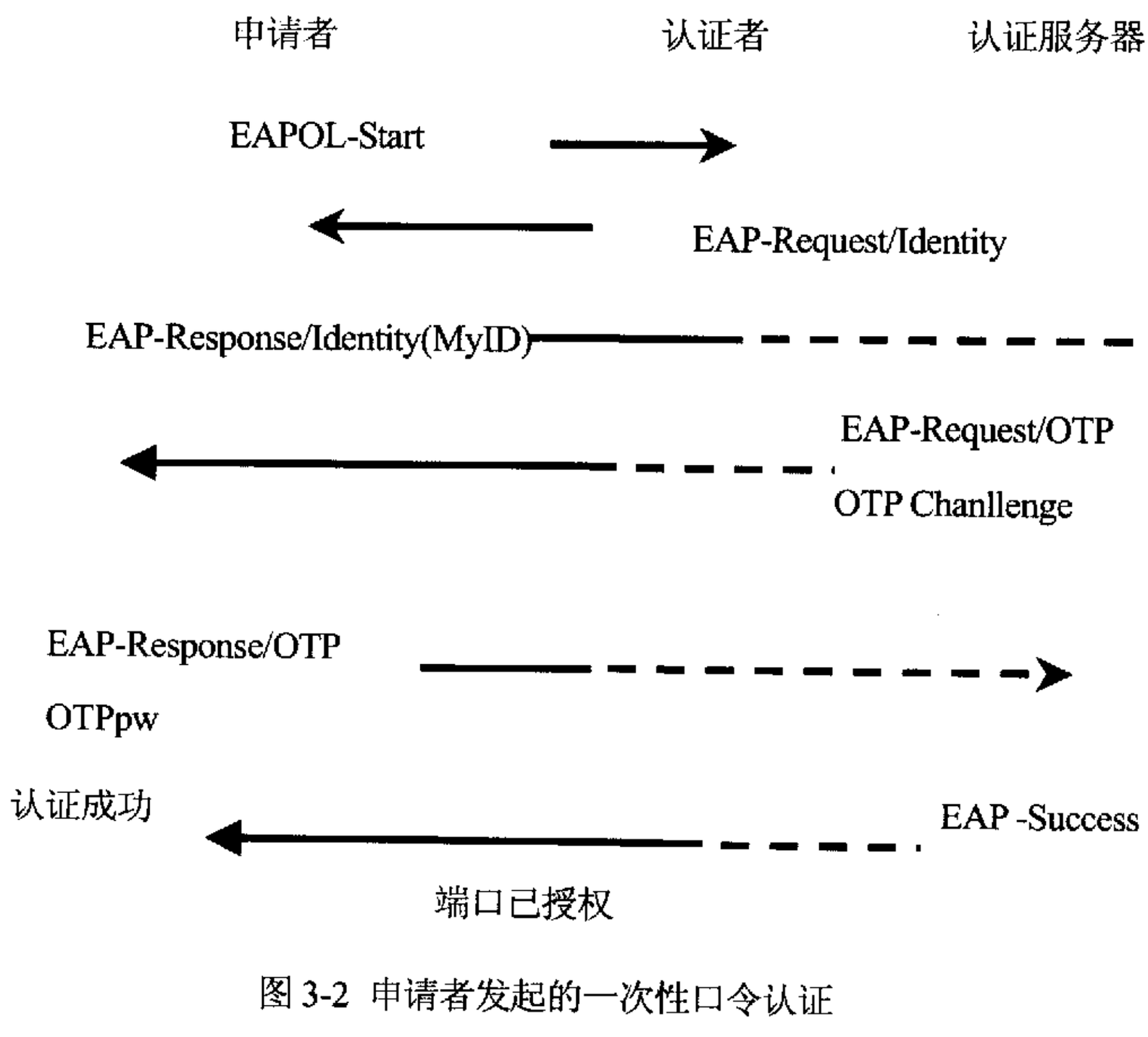


图 3-2 申请者发起的一次性口令认证

3.3 TLS 传输层安全协议

SSL（Secure Socket Layer，安全套接字层协议）是 Netscape 公司设计的主要应用于 Web 的安全传输协议[56]，是用于在客户机和服务器之间构建安全的通信通道的协议，它在 Web 上获得广泛应用，目前有 2.0 和 3.0 两个版本。1999 年，IETF 将 SSL 进行标准化，即 RFC2246，称其为 TLS（Transport Layer Security，传输层安全）。从技术上讲，TLSI.0 与 SST3.0 的差别非常微小。

TLS 现已被业界广泛认可，在 OSI 分层结构图中位于 TCP 和应用层协议（HTTP，SMTP，FTP）之间。它既可以为客户机认证服务器（server-side authentication），也可以为服务器认证客户机（client-side authentication），二者都是基于公钥机制（Public Key Infrastructure, PKI）的，其中 client-side authentication 是可选的（EAP-TLS 中要求使用）。

TLS 协议分为两部分：握手协议（Handshake Protocol）和记录协议（Record Protocol）。其中 Handshake Protocol 在内容是通信双方如何利用它来安全地协商

出一份密钥。Record Protocol 则定义了传输的格式。

3.3.1 握手协议

这是 TLS 中最复杂的一部分，协商协议版本、加密和 MAC 算法以及用来保护在 TLS 记录中发送的数据的加密密钥，使得服务器和客户机能够相互鉴别对方的身份。其中又包括三个子协议（sub-protocols）：握手协议、修改密文规约协议和告警协议[57]。

1、握手协议

握手协议由一系列在客户机和服务器之间交换的报文组成，其报文格式如下。

Type	Length	Data

Type 一共有 10 种类型。

0	hello_request
1	client_hello
2	server_hello
11	Certificate
12	server_key_exchange
13	certificate_request
14	server_hello_done
15	certificate_verify
16	client_key_exchange
20	Finished

客户机与服务器之间建立逻辑连接所需的交换有 4 个阶段（常用的密钥交换方法有 RSA、固定的 Diffe-Hellman、短暂的 Diffe-Hellman、匿名的 Diffe-Hellman 和 Fortezza）。下面以 RSA 密钥交换来说明。

阶段 1：建立安全能力。

这个阶段用于开始逻辑连接并且建立和这个连接关联的安全能力。客户机发起这个交换，发送 client_hello 报文，包含版本、随机数、会话 ID、密文族和压缩方法等参数，其中随机数是客户机生成的随机结构，由 32 位的时间戳和安全随机数生成器生成的 28 字节的随机数，一共是 32 字节，记做

client_hello.random 。密文族选择 TLS_RSA_WITH_RC4_128_MD5 和 TLS_RSA_WITH_RC4_128_SHA。同时，在这个阶段产生 48 字节的预先主密码 pre_master_secret；发送之后，客户机等待与 client_hello 报文具有同样参数的 server_hello 报文。随机数字字段是服务器生成的独立于客户机的随机数字段，记做 server_hello.random。密文族字段包含服务器从客户建立密文族列表中选择的一个密文族，压缩字段包含了服务器从客户建立压缩列表中选择的一个压缩算法。

阶段 2：服务器鉴别和密钥交换。

服务器通过发送自己的证书 certificate 开始这个阶段，报文中包含一个或一个链的 x.509 证书。服务器创建临时的 RSA 公开/私有密钥对，并且使用 server_key_exchange 报文来发送这个公开密钥，报文内容包括了这个临时 RSA 密钥的两个参数，加上这些参数的签名。下一步向客户请求证书，certificate_request 报文包括了两个参数：certificate_type 和 certificate_authorities，证书类型指出了公开密钥算法和它的使用，第二个参数是可接受的证书管理机构名字的列表。本阶段的最后一个报文是 server_hello_done，由服务器发送，指示服务器的 hello 和相关报文的结束，在这之后，服务器将等待客户的响应，该报文没有任何参数。

阶段 3：客户鉴别和密钥交换

一旦收到了服务器的 done 报文，客户机验证服务器是否已提供了合法的证书，检查服务器 hello 参数是否是可接受的。如果这些条件满足，客户机就把一个或多个报文发送给服务器。客户机通过发送 certificate 报文来开始这个阶段，如果没有合适的证书可用，客户机发送 no_alert 告警作为替代。接下来是 client_key_exchange 报文，使用来自 server_key_exchange 报文的临时 RSA 密钥对 pre_master_secret 进行加密。在这个阶段最后，客户机发送 certificate_verify 报文来对客户证书提供明确的验证，在 handshake_message 上计算 MD5 和 SHA-1 散列，并用 RSA 私钥对散列数据的连接进行加密。握手报文指的是从客户 hello 开始的所有发送和接收的握手协议报文，但不包括客户 hello 报文。该报文的目的是为了验证客户对于客户证书私有密钥的所有权，即使有人误用了该客户的证书，也不能发送这个报文。

阶段 4：结束

这个阶段完成安全连接的建立。客户发送 change_cipher_spec 报文并且将挂起的 Cipher_spec 复制到当前的 Cipher_spec，注意这个报文不是握手协议的一部分，而是使用修改密文规约协议来发送的。然后，客户发送 finished 报文。计算方法如下。

PRF(master_secret,finished_label,MD5(handshake_messages)+SHA-1(handshake_messages))[0...11],其中主密码 master_secret 是根据 pre_ master_secret 计算的。

master_secret=PRF（pre_master_secret，“master secret”，ClientHello.random+ServerHello.random）[0...47];

结束标号 finished_label 对于客户机是“客户结束（client finished）”，对于服务器是“服务器结束（server finished）”。握手报文是目前为止来自握手报文但不包括该报文的所有数据。作为对这个两个报文的响应，服务器发送它自己的 change_cipher_spec 报文，将挂起状态迁移到当前的 Cipher_Spec，并且发送它的结束报文，这时握手过程完成。

共享的主密码是通过密钥交换的方式为这个会话生成性的 48 字节值。创建过程分两个步骤：第一，交换预先主密码；第二，双方计算出主密码。对于 RSA 密交换方法，客户机生成 48 字节的预先主密码，使用服务器的公开 RSA 密钥进行加密，然后发送给服务器。服务器使用自己的私有密钥对密文进行解密以恢复预先密码。接着双方用同样的公式计算主密码 master_secret 以及会话密钥。

PRF(master_secret,

“clientEAPencryptionClientHello.random+ServerHello.random)[0...127];主会话密 Master_Session_key 取上述结果的前 32 字节用于后的密钥管理过程。

说明：这里的伪随机函数 PRF 是采用 RFC2246“The TLS Protocol Vesrsion 1.0”中的定义。

PRF（secret,label,seed）=P_MD5(S1,label+seed)XOP R SHA-1(S2,label+seed)

这里的 S1，S2 是通过将 secret 分为两半得到的。

2. 修改密文规约协议

修改密文规约协议是最简单的，协议内容由单个报文组成，该报文由值为 1 的单个字节组成，目的是使得挂起状态被复制到当前状态，改变了这个连接将要使用的密文族。

3. 告警协议

用来将 TLS 有关的告警传给对方实体。这个协议的每个报文由 2 字节组成。

级别	告警

第一字节值是警告（1）或致命的（2）用来传送报文的严重级别。如果级别是致命的，TLS 立刻中止该连接。第二字节包含了指出特定告警的代码。

3.3.2　记录协议

记录协议完整的操作是接收传输的应用报文，将数据分片可管理的块，进行可选的压缩数据，应用 MAC，加密，增加首部，在 TCP 报文段传输结果单元。在无线局域网的认证中采用 TLS 协议，记录协议并没有用到全部操作，只是定义传输格式，附加一个首部，称做 Record Header.

0	1	2	3,4
Type	Major Version	Minor Version	Length

Type：内容类型，指明处理这个包装的数据片的高层协议。

20　change_cipher_spec 修改密文规约协议

21　Alert 告警协议

22　Handshake 握手协议

23　application_data

Major Version：主要版本，对 TLSv3.0 字段值为 3。

Minor Version：次要版本，对 TLSv2.0 字段值为 1。

Length：数据片以字节为单位的长度。

3.3.3　TLS 认证过程

TLS 认证过程从握手阶段开始：

（1）客户机连接到服务器请求认证；

（2）服务器发送自己的数字证书给客户机；

（3）客户机通过已安装的公共 CA 证书来验证服务器的身份；

（4）服务器请求验证客户身份；

（5）客户机发送数字证书到服务器；

（6）服务器验证客户身份；

（7）客户机和服务器协商确定加密和消息完整性机制；

（8）上述过程完成后，可以安全地进行通信，数据采用记录协议封装。

3.3.4 TLS 协议的安全性

握手协议使客户机的服务器之间相互进行认证，并协商加密算法和密钥，握手协议提供的连接安全性具有以下三个基本特点。

（1）身份验证：对等方实体可以使用非对称密码算法（例如 RSA，DSS）进行认证。

（2）共享密钥的协商是保密的，即使攻击者能发起中间人攻击，协商的密钥也不可能被窃听者获得。

（3）协商是可靠的，攻击者不能在不被发现的情况下篡改协商通信消息。

3.3.5 EAP-TLS 数据包格式

RFC2716 PPP EAP TLS Authentication Protocol 中定义了 EAP 支持 TLS 认证的方式。EAP TLS Request/Response 的格式如图 3-3 所示。

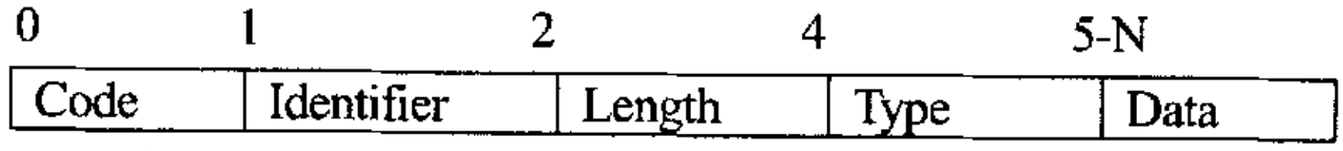


图 3-3 EAP TLS 数据包格式

Code：1——Request；

2——Response.

Identifier：辅助进行 Response 和 Request 的匹配。

Length：EAP 包的长度，包含 Code, Identifier, Length 和 Data 域的全部内容。以上三个域的内容共 4 字节，称做 EAP Header。

Type：13，指明是 EAP-TLS 认证。

Data：0 1 5-N

Flags	TLS Message Length	TLS Data

Flags：0 1 2 3 4 5 6 7 8 bit。

+-+-+-+-+-+-+-+-+

|L M S R R R R R|

+-+-+-+-+-+-+-+-+-+-+-+

L=Length included，置位表示包含后面的 TLS message Length 域

M=More fragments，除了最后一个分帧，其余都要置位

S=EAP-TLS start，EAP-TLS Start message 中置位

R=Reserved

TLS Message Length：4 字节，指明 TLS Data 的长度。

TLS Data：根据记录协议封装的 TLS 包，一个 TLS 记录的最大长度是 16384 字节，但是一个 TLS 消息可能包含多个 TLS 记录，为了避免一次传送的 EAP-TLS 消息超出 PPP MTU 长度或是最大 RADIUS 包长度等，设置 TLS 消息的最大长度为 1398 字节。

3.3.6　EAP-TLS 认证过程

EAP-TLS 认证过程如图 3-4 所示。

（1）客户机发出 EAP start 消息请求认证；

（2）AP 发出请求帧，要求客户输入用户名；

（3）客户机响应请求，将自己的用户名信息通过数据帧发送给 AP；

（4）AP 将客户的用户名信息重新装成 RADIUS Access Request 包发送服务器；

（5）RADIUS 服务器验证用户名合法后客户机发送自己的数字证书；

（6）客户机通过证书验证服务器的身份；

（7）客户机给服务器发送自己的数字证书；

（8）服务器通过证书验证客户的身份，这里完成了相互认证；

（9）在相互认证的过程中，客户机和服务器也获得了主会话密钥 Master_Session_Key；

（10）认证成功，RADIUS 服务器向 AP 发送 RADIUS ACCEPT 消息，其中包含密钥信息；

（11）AP 向客户机转发 EAP Success 消息，认证成功。

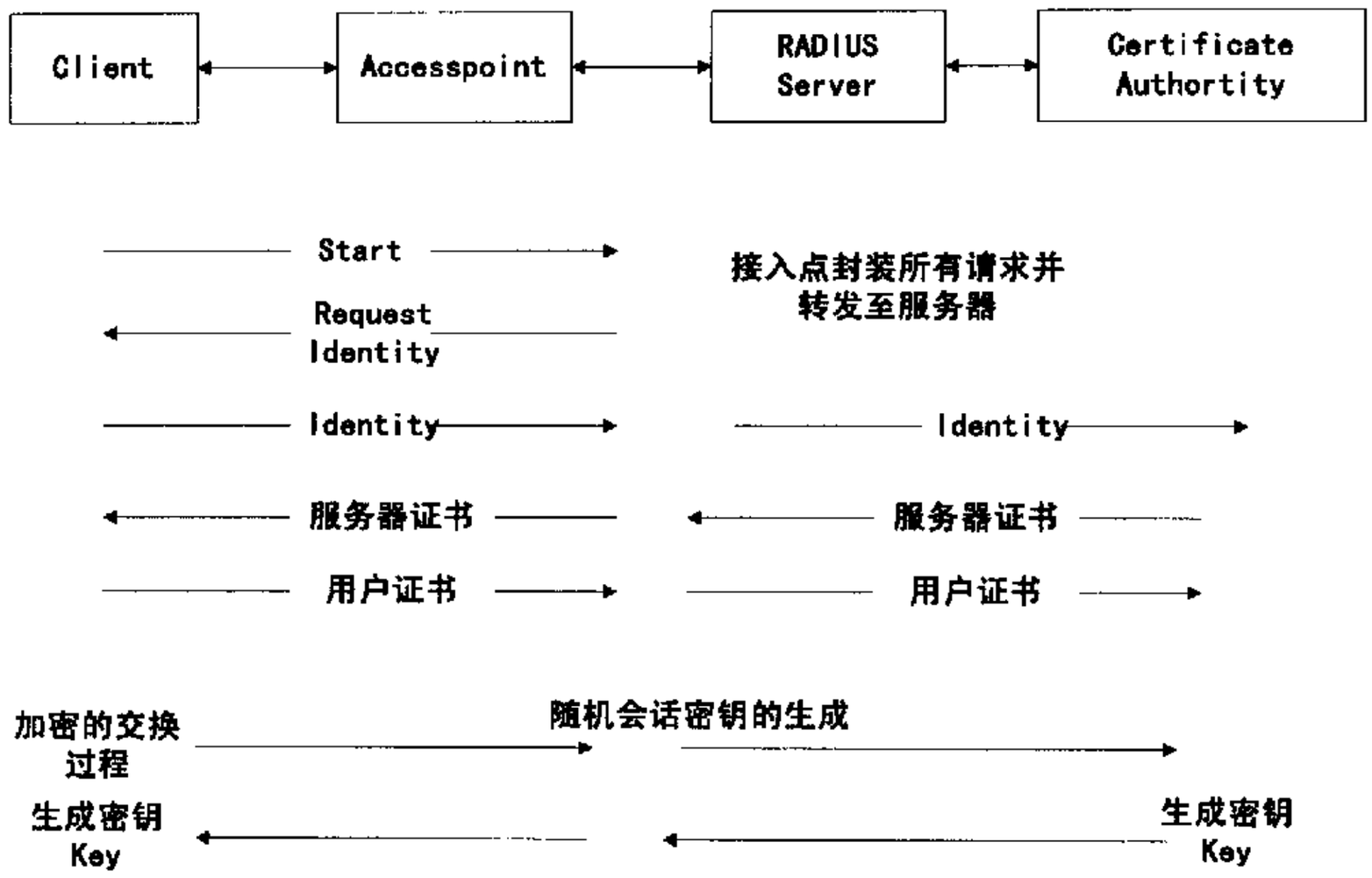


图 3-4　EAP-TLS 的认证过程

3.3.7　EAPOL 消息的交互过程

引入 TLS 认证机制后的 EAPOL 消息的交互过程可以用图 3-5 来表示。

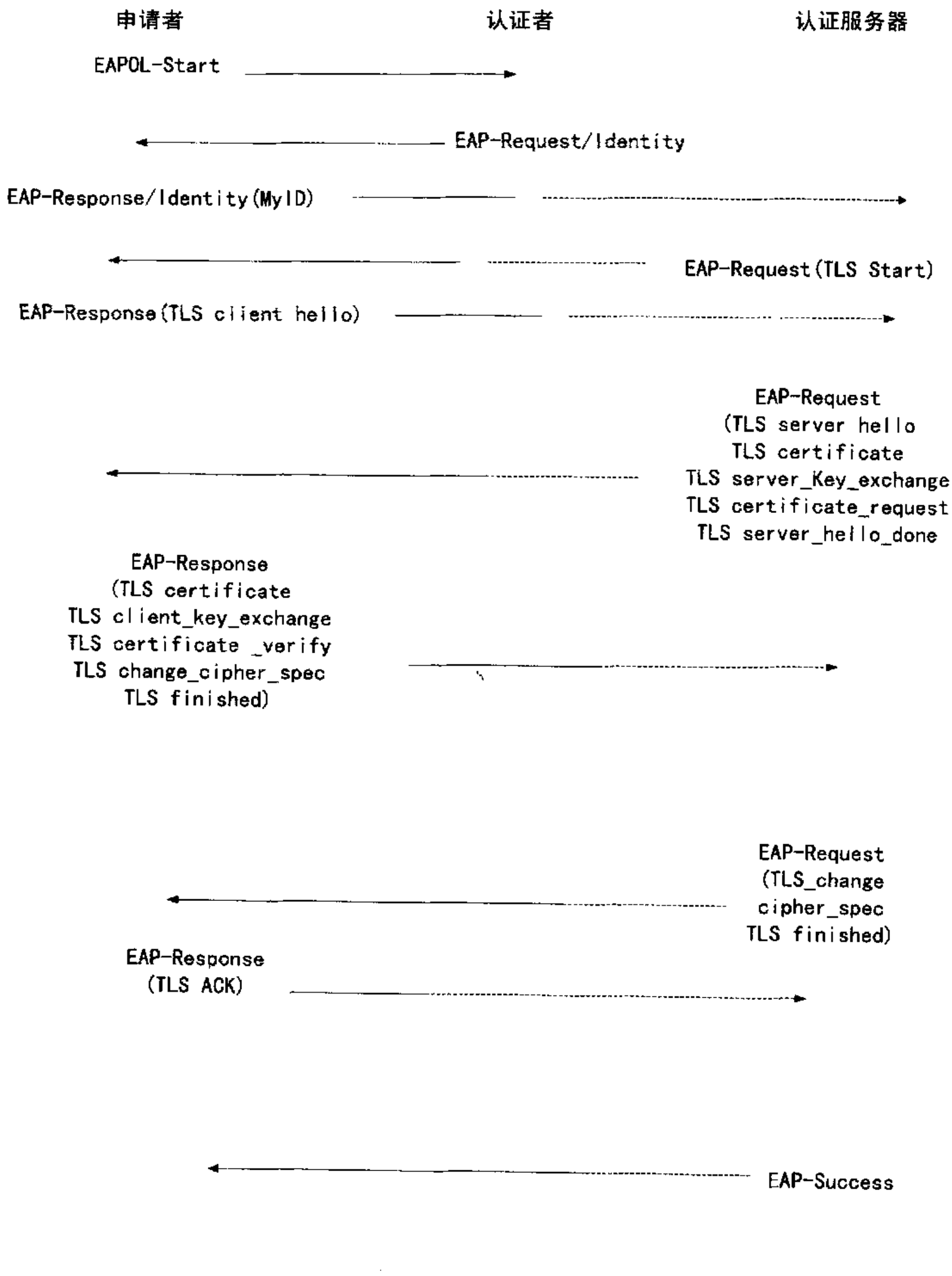


图 3-5　EAP-TLS 认证 EAPOL 消息的交互过程

第四章 无线局域网安全认证模型的构建

4.1 无线局域网安全认证模型概述

4.1.1 IEEE802.1x 安全认证的特点

传统的认证方案是 在IEEE802.11 WLAN环境下采用IEEE802.1x的认证体系的结构（具体过程参考第三章），存在以下安全隐患：

（1）802.1x 是一个不对称协议，它只允许网络鉴别用户，而不允许用户鉴别网络。因而，攻击者能够窃听用户和访问点之间的通信；扮演“中间人”的角色在移动用户和合法访问点之间传递虚假信息，实施中间人攻击。

（2）移动用户和访问点之间传送的低层信号不具备安全性，一个攻击者可能冒充移动用户而哄骗访问点。比如，攻击者可能伪造一个“断开连接”的802.11管理帧，并以 AP 身份发送至工作站，使得移动用户的网络连接断开；其次，攻击者可能进而“劫持”先前用户的网络连接，使用移动用户的 MAC 而取得网络通信的权利。

（3）存在多种拒绝服务（Ddos）攻击方式使合法连接掉线，或使网络陷入拥塞状态而无法提供正常服务。

4.1.2 无线局域网安全认证模型的提出

在本课题的研究中，提出的无线局域网的安全认证模型的思路如下，采用IEEE802.1x基于端口的接入控制协议，整个认证系统包括AS（认证服务器），认证者(AC)和客户端(STA)3个部分（网络拓扑结构见图4-1），整个安全过程对于接入点是透明的，AC将参数通过AP的接口控制模块配置AP。认证机制采用了EAP-TLS，认证服务器采用目前比较成熟的RADIUS服务器，并支持EAP-TLS认证。

密钥管理模块参考了IEEE802.11工作组关于RSN（强安全网络）的草案，采用四步握手的密钥协商机制，动态地产生和分配密钥。

其实现方案模型的框架如图 4—2 所示。

图 4-1 安全无线局域网构成图

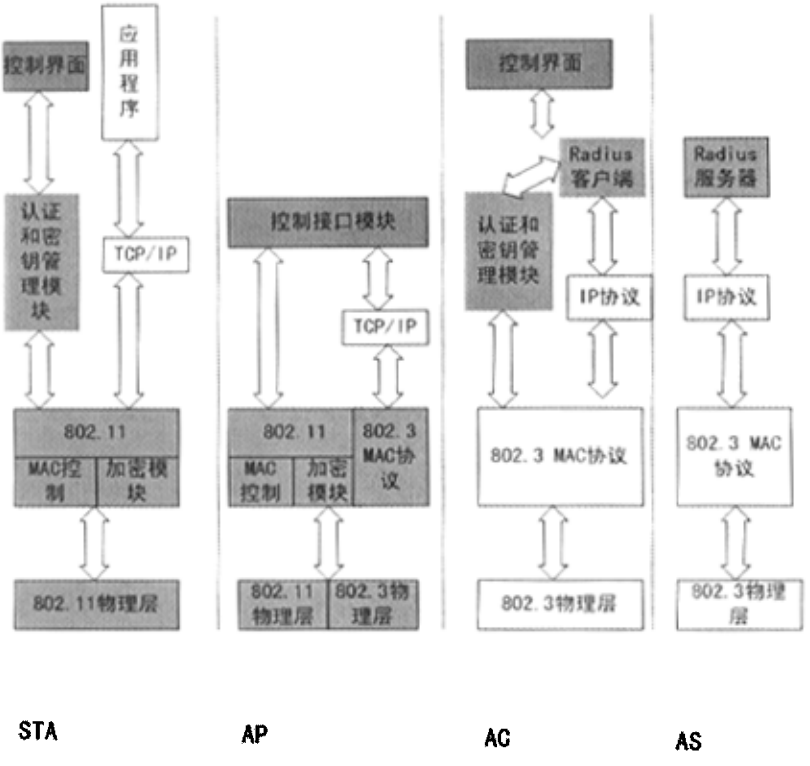


图 4—2 无线局域网安全认证模型图

采用本方案的优点：

首先：我们在 EAP 的上层协议增加相互认证机制，本文提出了使用 TLS 协议，组成 EAP-TLS 能够有效地防止假冒身份的攻击。因为 EAP 协议本身缺少对自身信息的完整性和保密性的保护措施。通过 TLS 协议，特别是 TLS 协议中的四步握手的协商机制，能够有效地实现安全的双向认证。在单纯的 EAP 协议中，通信的双方缺乏有效的双向认证。我们采用的 TLS 协议能够保证请求

者和认证这之间传输的 EAP 报文的完整性和保密性，减少被攻击者截获或假冒真实数据报的机会。事实证明，本文采用的 EAP-TLS 的结构能够很有效地在两个端点之间提供双向认证、加密协商和密钥交换等服务。这样也同时有效地防止了前文所提到的中间人攻击，因为攻击者没有被 STA 或 AP 的任何一方确证，就不可能拥有会话密钥。所以，即使他能够截获工作站与访问点之间的报文，也没有可能被破译数据。

其次：本模型中提出的密钥管理模块可提供数据完整性服务、数据源认证服务和数据保密服务等。这在原先的单纯的 802.1x 的机制中是做不到的，802.1x 采用的是 SNMPv2 的端口管理方法存在着缺陷，即在利用 SNMPv2 实施管理的环境中，网管工作站与受管理设备间的通信报文没有任何完整性和保密性的保护，管理者只需要提供一个密码，就能进入管理系统进行所有的配置操作，例如把某个端口设置成非认证端口，让所有数据流通过。由于一般设备的 SNMP community 出厂值都会设置成 public,而 SNMPv2 没有密码统一管理与分发的机制，因此很多管理员甚至不去修改默认的内容，而造成很大的安全漏洞。而通过我们提出的密钥管理的思路就能有效地防止类似的漏洞。另外，强安全网络（RSN）机制的嵌入，也更有效的为 AP 和 STA 提供增强的认证机制、合理的密钥管理方案、动态分配密钥等，同时 RSN 也能够更有效地增强数据加密和封装机制和管理和控制帧的保护。

4.2 无线局域网的密钥管理

4.2.1 密钥管理的目的及种类

密钥管理处理密钥自产生到最终销毁的整个过程中的有关问题，包括系统的初始化，密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁等内容。密钥是保密系统中最脆弱也是最重要的环节。

密钥管理的目的是维持系统中各实体之间的密钥关系，以抗击各种可能的威胁，如下所述。

（1）秘密钥的泄漏。

（2）秘密钥和公开钥的确认性的丧失，确认性包括共享或有关一个密钥的

实体身份和知识或可证实性。

（3）秘密钥或公开钥未经授权使用。

密钥管理系统中还常常依靠可信赖的第三方参与的公证系统，如 CA（证书授权机构）。

密钥的种类很多，但从通信网的一般应用来看，有以下几种。

（1）基本密钥（Base Key）或初始密钥（Primary Key）。

由用户选定或由系统分配，可在较长时间（相对于会话密钥）内由一对用户所专用的秘密钥，故又称做用户密钥（User Key），要求它既安全又便于更换，和会话密钥起去启动和控制某种算法所构造的密钥产生器，来产生用于加密数据的密钥流。

（2）会话密钥（Session Key）。

会话密钥即两个通信终端用户在一次通话或交换数据时所使用的密钥。当它用做对传输的数据进行保护时称为数据加密密钥（Data Encrypting Key），当用于保护文件时称为文件密钥（File Key）。会话密钥的作用是使我们可以不必频繁地更换基本密钥，有利于密钥的安全和管理。这类密钥可以由用户双方预先约定，也可由系统的密钥建立协议动态地产生并赋予通信双方，它为通信双方使用，又称做专用密钥（Private Key）。

（3）密钥加密密钥（Key Encrypting Key）

用于对传送的会话或文件进行加密时采用的密钥，通信网每一个结点都分配一个这类密钥。

除了以上几种类型，还可根据需要产生加密过程中所需的各种密钥。

4.2.2 强安全网络 RSN 的安全性能协商[58]

强安全网络（Robust Securit Network, RSN）是 IEEE802.11 工作组 TGi 任务组提出的改进安全无线局域网模型。RSN 提供了许多在基本的 IEEE802.11 体系中没有提供的安全措施。主要包括：

（1）安全性能协商；

（2）为 AP 和 STA 提供增强的认证机制；

（3）合理的密钥管理方案；

（4）动态分配的密钥；

（5）增强的数据加密和封装机制；

（6）管理和控制帧的保护。

为兼容不支持 RSN（non-RSN）的设备，TGi 规定了安全性能协商的机制。安全协商机制用于协调不同类型的 STA 之间安全业务内容的配置，包括认证协议、密钥管理协议和单播/组播的加密套件等。

根据是否支持 RSN，AP 分为两类：RSN AP 和 WEP AP。RSN AP 支持 IEEE 802.1x 认证的密钥管理协议，并且单播加密套件采用 TKIP 和 AES；WEP AP 支持现有标准规定 AP 所具有的认证业务，单播加密套件采用 40 比特或 104 比特的 WEP 算法。

根据是否支持 RSN 和是否支持 IEEE802.1x 认证协议，STA 可以分为三类：RSN STA、不支持 IEEE802.1x 认证协议但支持 IEEE802.1x 密钥管理协议的 WEP STA。RSN STA 支持 IEEE802.1x 认证的密钥管理协议，并且单播加密套件采用 TKIP 和 AES；WEPSTA 无论是否支持 1EEE802.1x 密钥管理协议，其单播加密套件采用 40 比特或 104 比特的 WEP 算法。

AP 根据配置支持的 STA 类型中单播加密套件最低的级别来决定组播加密套件。加密套件的级别由低到高依次为 WEP，TKIP，AES。

TGi 在 IEEE802.11 标准原有的管理帧帧体中加入了 RSN 信息单元（Information Element， IE）以协商各 AP 和 STA 的类型等安全性能的配置情况。STA 从来自 AP 的信标帧（Beacon）的探询帧（Probe）中得到 RSN IE，以决定将使用 AP 的安全性能。来自 STA 的关联（Association）和重新关联（Re-association）请求消息中的 RSN IE 包含了 STA，根据 AP 的配置确定用于关联的安全性能。由此，STA 和 AP 完成了安全性能的协商。此外，在 IBSS 中的 STA 同样通过 Beacon 和 Probe 应答消息中的 RSN IE，确定将与之建立关联的 STA 的安全性能。

4.2.3 密钥层次

认证成功之后，申请者和认证服务器各自生 32 字节的对等主密钥（Pairwise Master Key，PMK）。生成的方法与认证方式相关，通常 EAP 认证都是由认证

过程中得到主密钥，再派生出对等主密钥。如果采用 RADIUS 作为服务器的协议，则通过使用 Vendor-Specific 中的子属性 MS-MPPE-Recv-Key(vendor-id=17)将 PMK 传送给认证者。

申请者和认证者都得到 32 字节的 PMK，又称主会话密钥（Master Session Key），处于密钥层次的第一级；根据 PMK 计算对等传输密钥（Pairwise Transient Key, PTK），继而得到加密所需的各种密钥。

无线局域网中支持的加密算法包括 TKIP（ Temporal Key Integrity Protocol）和 AES（Advanced Encryption Standard）两种。

4.2.3.1 TKIP 密钥层次

TKIP 的密钥导出层次如图 4-3 所示。在认证成功后，通信双方将获得 PMK，然后根据此 PMK 以及图中所示的其他参数，应用输出为 512 比特的 PRF-512 函数导出 PTK，取 PTK 的第 1~128 比特作为 EAPOL-Key MIC Key，第 129~256 比特作为 EAPOL-Key Encr.Key，第 257-384 比特作为临时加密密钥（Temporal Encryption Key），第 385-448 比特作为 Temporal Key Owner TX MIC Key（用来做校验），第 449-512 比特作到为 Temporal Key Owner RX MIC Key（用来做校验）。最后，Temporal Encryption Key 经过两级密钥混合函数导出 RC4 加密密钥。

说明：

图 4-3 中计算 PTK 的参数 AA（Authenticator Address）和 SA（Supplicant Address）分别是认证者和申请者的 MAC 地址；SNonce 和 ANonce 分别是申请者和认证者发出的现时。计算方法如下：PRF-256（Random-number, “Init Counter”，Local Mac Address||Time），对于申请者和认证者，Local Mac Address 分别是 SA 和 AA；Random number 是长度为 32 字节的尽可能随机的数；Time 是系统当前时间。

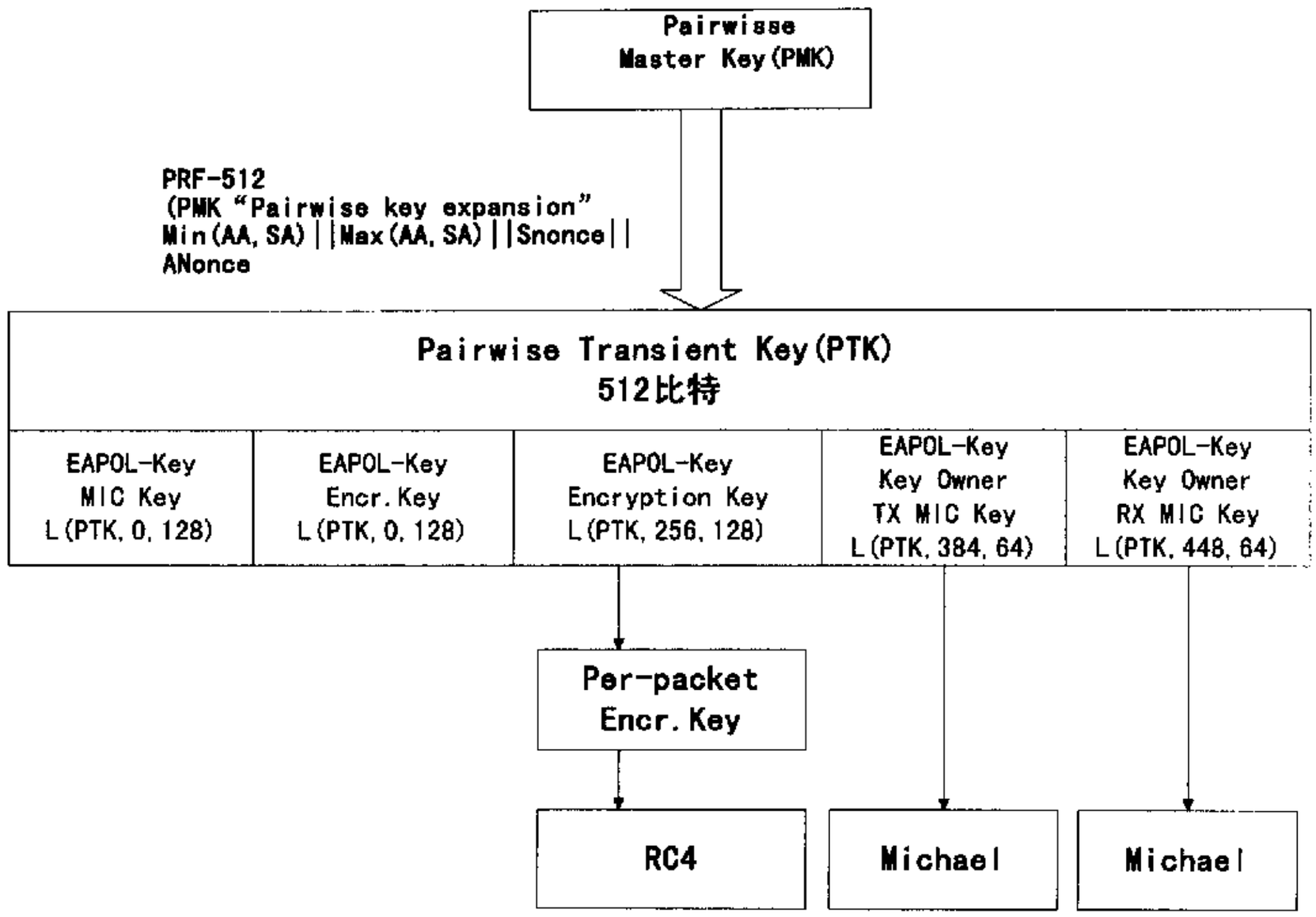


图 4-3　TKIP 的对等密钥层次

‖为连接符号，Min 函数和 Max 函数按照值的大小对圆括号内的两地址（以字节序列表示）分别选出其中较小者和较大者。

L 函数 L（I，F，L）是取比特序列 1 从第 F 个比特开始的 L 个比特。

TGi 草案中的 PRF 函数是基于 SHA1 哈希算法的 HMAC 算法的，其定义为：

H-SHA-1（K，A，B，X）=HMAC-SHA-1（K，A‖Y‖B‖X）

PRF-128（K，A，B）=PRF（K，A，B，128）

PRF-256（K，A，B）=PRF（K，A，B，256）

PRF-384（K，A，B）=PRF（K，A，B，384）

PRF-512（K，A，B）=PRF（K，A，B，512）

```
PRF(K,A,B,Len)
{
octet i;
for(I=0;I<(Len+159)/160;I++) {
        R=R||H-SHA-1(K,A,B,I)
```

}

L(R,0,Len)

}

其中：||为连接符号，A 为对应不同应用的 PRF 函数的标识符，Y 为一个值为 0 的字节，X 为一个包含参数的字节。

PRF 函数的输出即其导出比特序列的长度（该长度的值为 128，192，256，384，512，单位为比特，TGi 草案将对应的函数分别命名为 PRF-128，PRF-192，PRF-256，PRF-384，PRF-512）有不同的值。

4.2.3.2 AES 密钥层次

AES 的密钥导出层次如图 4-4 所示。在认证成功后，通信双方将获得 PMK（Pairwise Master Key），然后根据此 PMK 以及图中所示的其他参数，应用 PRF-384 函数（输出为 384 比特）导出 PTK（Pairwise transient Key），取 PTK 的第 1~128 比特作为 EAPOL-Key MIC Key，第 129~256 比特作为 EAPOL-Key Encr. Key，第 257~384 比特作为临时加密密钥（Temporal Encryption Key），最后，由临时加密密钥（Temporal Encryption Key）根据 CBC-MAC 等法导出 AES 加密密钥。

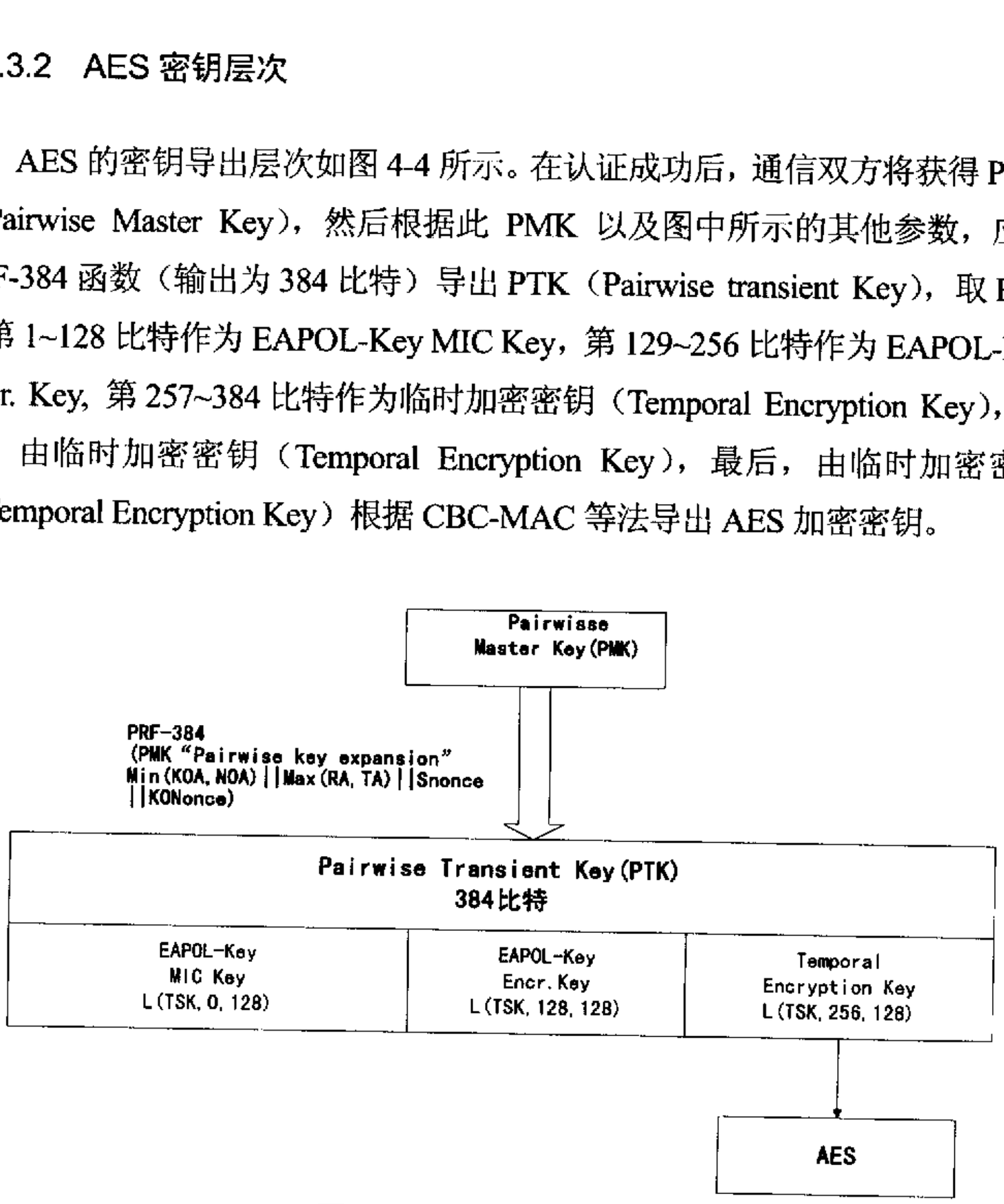


图 4-4 AES 的密钥导出层次

4.3 四步握手密钥协商机制

四步握手的协商机制，能够有效地实现安全的双向认证。在单纯的 EAP 协议中，通信的双方缺乏有效的双向认证。我们采用的 TLS 协议中的四步握手的协商机制能够保证请求者和认证这之间传输的 EAP 报文的完整性和保密性，减少被攻击者截获或假冒真实数据报的机会。同时，能够很有效地在两个端点之间提供双向认证、加密协商和密钥交换等服务。

作为密钥管理系统中最主要的步骤，目的是确定申请者和认证者得到的 PMK 是相同的，并且是最新的，以保证可以获得最新 PTK。同时，通过四步握手的结果通知申请者是否可以加载加密/整体性校验机制[59] [60]。

4.3.1 四步握手密钥初始化

如果 IEEE802.1x 认证成功，认证者向申请者转发 EAP-Success，然后认证者初始化两途中密钥交换；四步握手和组密钥更新。

图4-5 中 EAPOL-Key(S,M,A,T, N,K,KeyRSC, ANonce/SNonce,GNonce,MIC,GTK) 的各个参数的含义如下。

- S：对应 EAPOL-Key Information 的 Secure 位。
- M：对应 EAPOL-Key Information 的 MIC 位。
- A：对应 EAPOL-Key Information 的 Ack 位。
- T：对应 EAPOL-Key Information 的 Key usage 标志位。
- N：对应 EAPOL-Key Information 的 Key index 位。
- K：对应 EAPOL-Key Information 的 Key Type 位。
- KeyRSC：对应 EAPOL-Key 的 Key RSC 域。
- ANonce/SNonce：对应 EAPOL-Key Key Nonce 域。
- GNonce：组密钥的 Nonce。
- MIC：对应 EAPOL-Key MIC 域。

GTK：对应 EAPOL-Key Data 域。

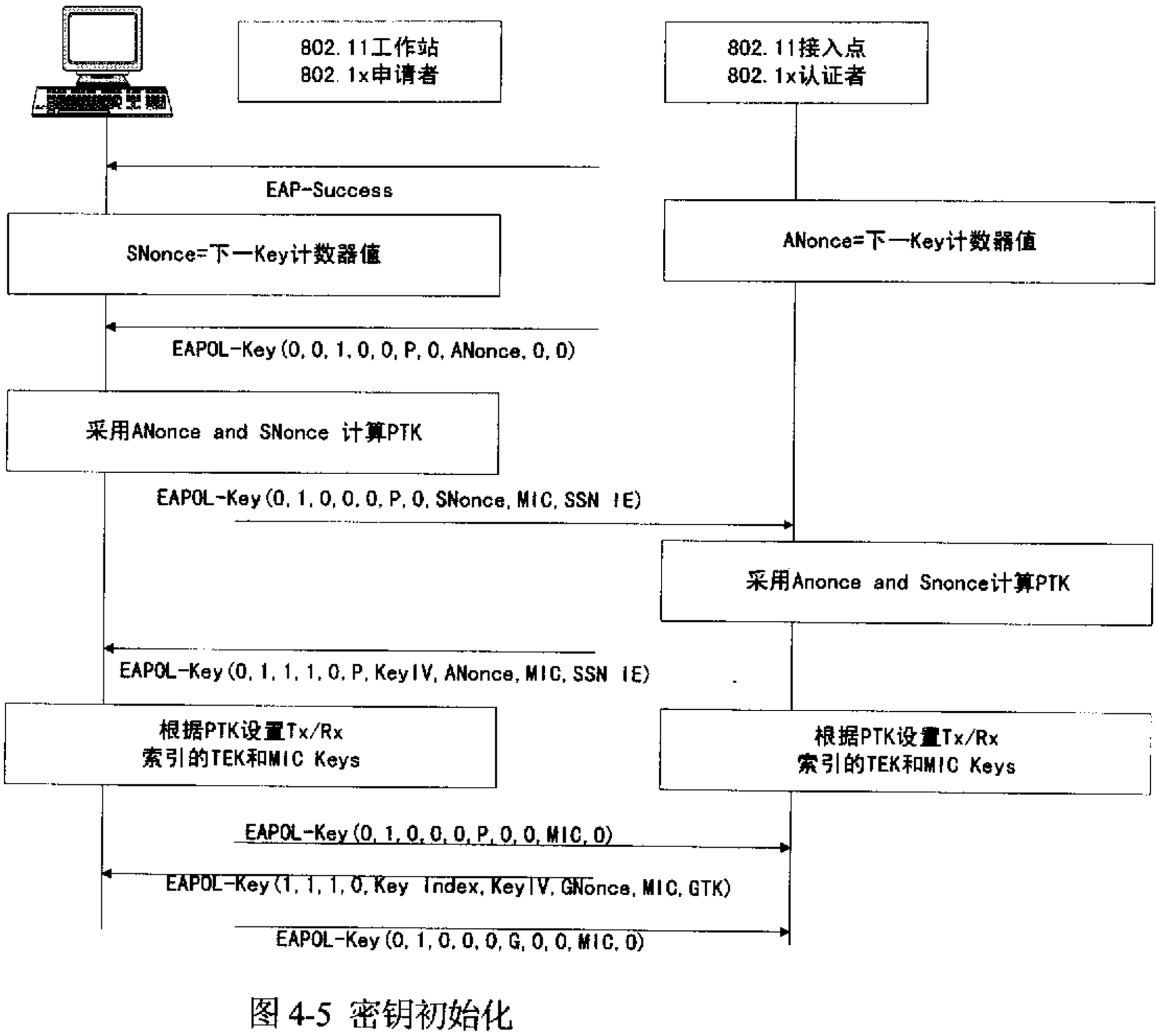


图 4-5 密钥初始化

4.3.2 四步握手过程

四步握手用来确认认证者和申请者使用相同的 PMK，产生新的 PTK，同时也用来通知申请者端加载加密/整体性校验机制。流程如下。

（1）认证者发送 EAPOL-Key 消息，其中包含 ANonce。

Authenticator->Supplicant: ANonce

（2）申请者由 ANonce 和 SNonce 产生 PTK，发送 EAPOL-Key 消息，包含 SNonce 和 MIC。

Supplicant->Authenticator: SNonce, RSN IE,

MIC (EAPOL-Key MIC Key(PTK (ANonce, SNonce)), EAPOL-Key message)

（3）认证者由 ANonce 和 SNonce 产生 PTK，并且对 MIC 校做验，发送

EAPOL-Key 消息，其中包含 ANonce，MIC 及是否安装加密/整体性密钥。

Authenticator->Supplicant: Install, KeyRSC, ANonce, RSN IE,

MIC（EAPOL-Key MIC Key （PTK （ANonce, SNonce)), EAPOL-Key message）

（4）申请者发送 EAPOL-Key 消息，确认密钥已经安装。

Supplicant->Authenticator:

MIC（EAPOL-Key MIC Key（PTK （ANonce SNonce)), EAPOL-Key message）

说明：

- 上述消息都是用 EAPOL-Key 消息封装。
- MIC 是消息完整性检查（Message Integrity Check）, MIC(X,Y)中，X 是密钥，Y 是做完整性校验的数据。Y 是 EAPOL-Key 消息， X 是 EAPOL-Key MIC Key，由 PTK 产生。
- ANonce 是认证者产生的现时,在认证者发出的两条消息中相同，申请者只有收到第三条消息才能判断 ANonce 是否正确。
- SNonce 是申请者产生的现时。
- Key RSC 是对等密钥的当前序列计数器，通常为 0。
- 申请者通过发送 EAPOL-Key 消息，Request 位置 1 发起四步握手过程。
- 认证者发出的消息 ACK 位置 1，申请者发出的消息 ACK 不置位
- 认证者忽略不是对发送 EAPOL-Key 消息的期望响应的消息，也忽略 ACK 置位的 EAPOL-Key 消息。
- 认证者收到四步握手的第二条消息，将其中的 RSN IE 和收到的 associate 请求中的 RSN IE 相比较，申请者收到四步握手的第三条消息，将其中的 RSN IE 和收到的 Beacon 或者 probe response 帧中的 REN IE 相比较，如果发现不同，则报错，同时客户机断开连接。

4.3.3 组密钥更新

组密钥更新用来向申请者发送新组密钥，只有当第一次四步握手成功了才能进行组密钥初始化，流程如下。

（1）认证者产生新的 GTK，并对其加密，包含在 EAPOL-Key 消息中发送。

Authenticator->Supplicant; Key Index, KeyRSC, Enc (GTK).

MIC(EAPOL-Key MIC Key (PTK (ANonce, SNonce)), EAPOL-Key message)

（2）申请者对收到的消息做 MIC 校验，解密 GTK 并安装到加密/整体性机制中[61]。

Supplicant->Authenticator:

MIC （EAPOL-Key MIC Key （PTK（ANonce, SNonce)), EAPOL-Key message）

（3）申请者发送 EAPOL-Key 消息，对认证者进行确认。

（4）认证者对收到的消息做 MIC 校验，并且将 GTK 安装到加密/整体性机制中。

说明：

- Key Index 是认证者要求申请者加载的加密/完整性机制的索引。
- KeyRSC 是组密钥的当前序列计数器，如果工作站使用了组密钥并且关联，那么值不为零。
- Enc(GTK)：组密钥 GTK 用由四步握手过程产生的 PTK 产生的 EAPOL-Key encryption key 加密。
- MIC（X，Y）跟前面介绍的相同。
- 申请者通过发送 EAPOL-Key 消息，Request 位置 1 发起组密钥更新过程。
- 当认证者既要完成四步握手又要完成组密钥更新时，必须先进行四步握手过程。

配置组密钥后，secure 位置位，然后才能进行数据传输。

4.3.4 四步握手机制的状态机

1、申请者状态机

如图 4-6 所示，申请者认证结束后，收到 EAPOL-Key 消息，进入

STAKEYSTAT 状态，对收到的消息进行处理，四步握手的第一条消息无须 MIC 校验，其它消息需要校验。StaProcessEAPOL-Key 函数根据需要对接收到的 EAPOL-Key 消息进行 MIC 校验，封装新的 EAPOL-Key 消息并发送。

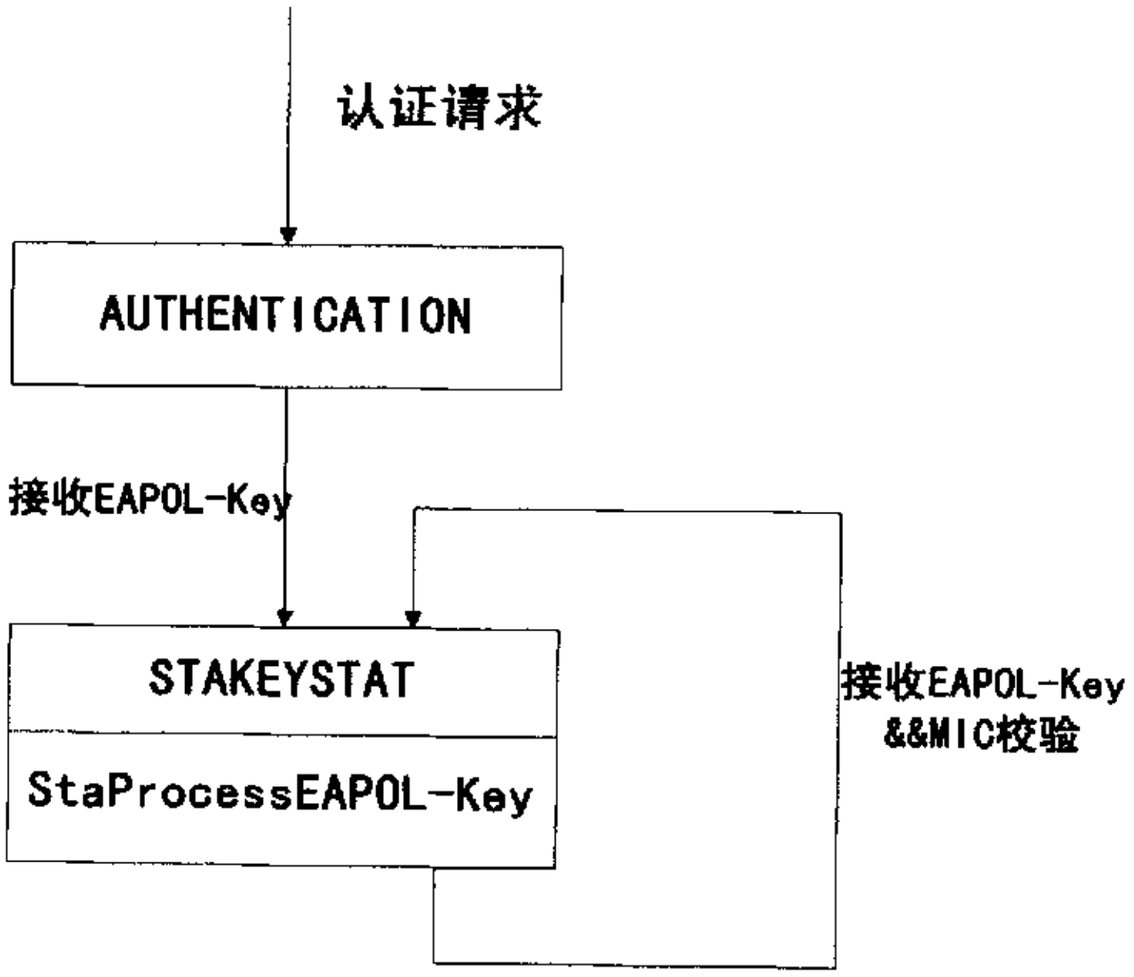


图 4-6　申请者状态机

2、认证者状态机

此状态机实现了认证者端四步握手机制的主要过程，包括发送和接收 EAPOL-Key 消息，从而完成密钥的初始化。共计以下 8 个状态：DISCONNECT，AUTHENTICATION.INITPMK, INITPSK, PTKSTART, PTKINITNEGOTIATING, PTKINITDONE，INTEGRITYFAILURE。

认证者在 IEEE 802.1x 认证之后，PMK 或者预先分配的 PSK（Pre-shared Key）作为密钥的第一层次，转入 PTKSTART 状态，向申请者发送第一条 EAPOL-Key 消息，收到申请者的回应之后，进入 PTKINITNEGOTIATING 状态，计算 PTK，并封装和发送下一条 EAPOL-Key 消息，收到申请者的应答之后，进入 PTKINITDONE，至此 PTK 的协商已经完成，如果整体性校验出错，则转入 PTKSTART 重新进行协商。

在此过程中，如果在预定时间内未收到申请者的响应，可以重发数次。超过和重发机制可以根据实际的应用情况进行设定。

4.3.5 工作流程

四步握手的密钥管理机制属于密钥初始化的一部分，用来确认认证者和申请者使用相同的 PMK，产生新的 PTK；同时也用来通知申请者端加载加密/整体性校验机制[62]。

如图 4-7 所示，在四步握手的密钥协商机制中，申请者和认证者之间在数据链路层发送和接收 4 条 EAPOL-Key 消息，这也正是四步握手名称的由来。通过认证，双方得到 PMK，再通过协商，各自产生相同的 PTK，得到加密所需的各种密钥。

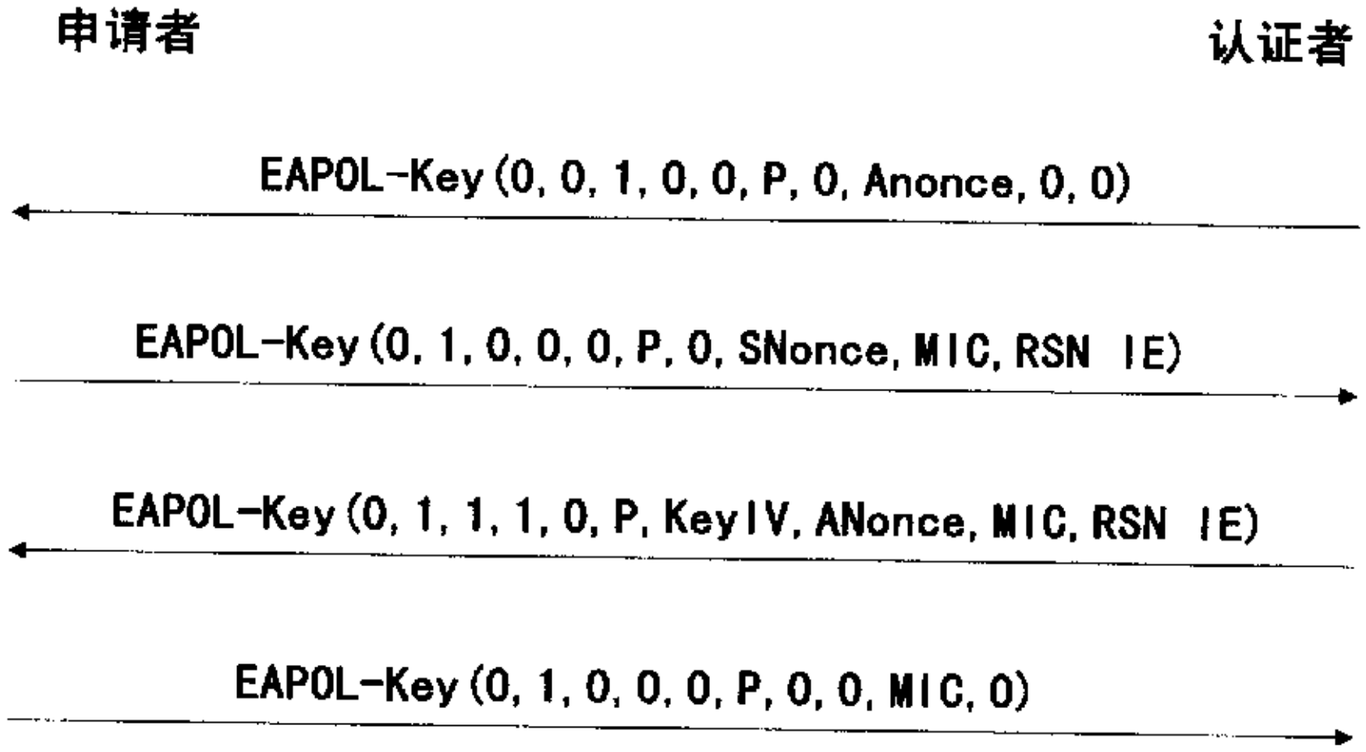


图 4-7 四步握手密钥协商机制

4.4 认证者端的模型

在本文中提出的 WLAN 安全认证和密钥管理的软件方案，实现了包括安全认证、密钥管理、数据保护等安全功能，支持用户通过认证登陆网络，并保证了无线局域网中数据交换的安全性和可靠性。

4.4.1 主函数流程设计

主函数流程(见图 4-8)如下：程序初始从用户界面读入认证信息，然后等待请求，并同时打开链路层收包线程。根据收到的数据包做如下的处理：如果是未经认证的用户发送的请求 EAP-Start，并且 AP 处于空闲状态，则进入用户认证和密钥管理模块，否则如果 AP 处于忙状态（有用户正在进行认证），则回

发 Logoff，提示用户过一段时间再进行登陆；如果收到的数据包是 EAP-Logoff 类型，表示用户想退出网络，则在用户列表中删去此用户，用户可安全退出；如果是已认证的用户，则密钥管理程序可通过查找用户列表使其正常与外部网络连接。如果用户通过认证并完成密钥协商，就可以成功登陆网络，与外部分布式网络相连。否则，将无法与外部网络相连。在程序的设计中建立了用户列表来支持多用户登陆。对于已认证用户，用户列表中加入该用户的信息包括分配的密钥；用户如果要求退出网络，则在用户列表中删去此用户。这样密钥管理模块可以通过查找用户列表，支持多个用户同时上网。这样做的好处还在于程序进行某个用户认证的过程中，同时也可以支持其他已认证用户的安全上网。

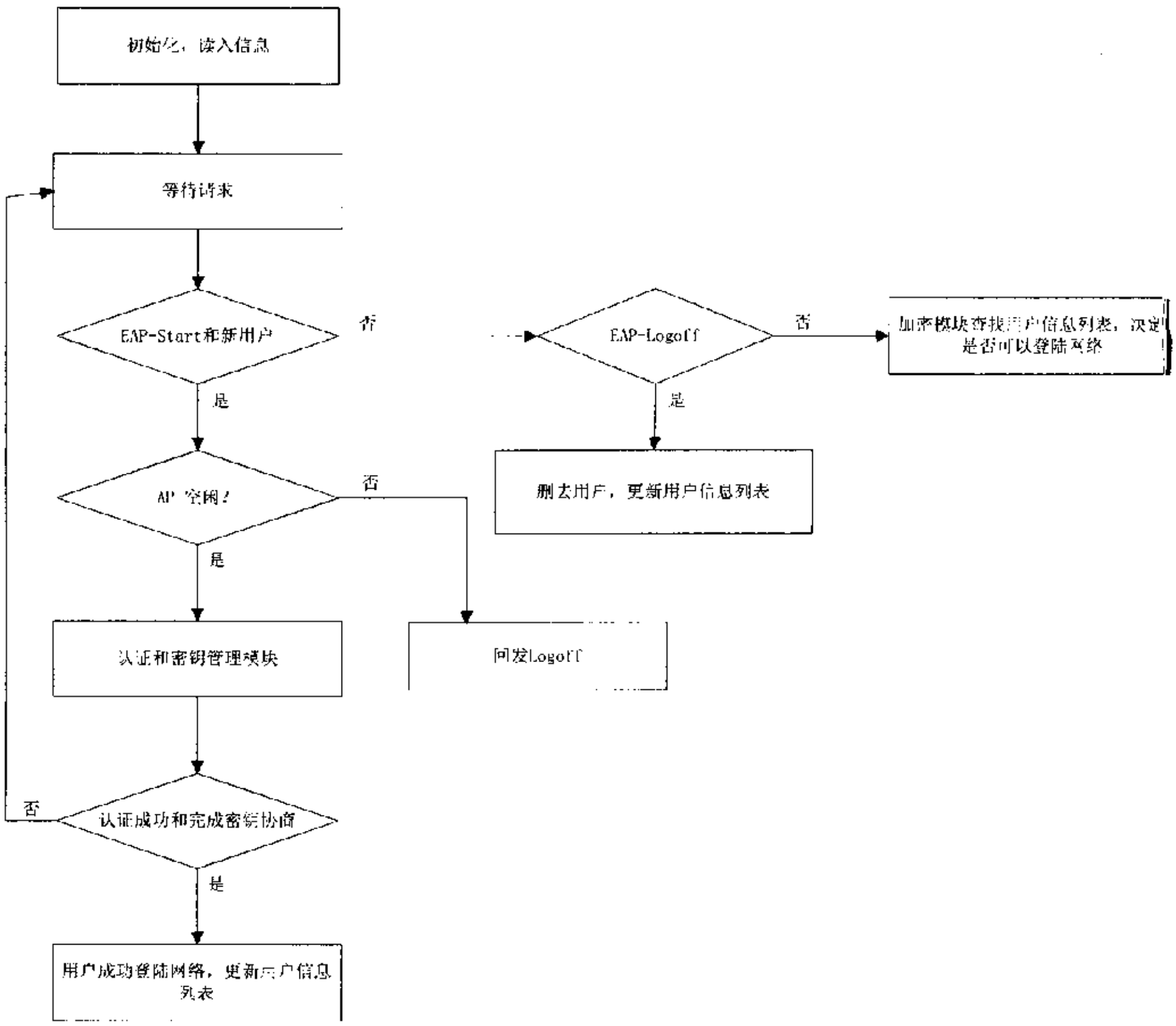


图 4-8　主函数流程

4.4.2 认证模块的实现

4.4.2.1 认证模块的协议流程

采用 EAP 认证方式时，AP 一般并不翻译或是修改 EAP 信息，无须理解 EAP 认证协议，只需简单作为后端服务器的透明传输代理，将数据包传递给 RADIUS 服务器。协议的流程如图 4-9 所示。

4.4.2.2 认证模块的程序设计

对于认证者，参照 IEEE802.1x 协议中认证者状态机和后端服务器状态机来进行程序设计。

考虑到整个程序的结构，认证者状态机中的循环处理在主程序中实现，程序流程如图 4-9 所示。初始化之后，进入 Disconnect，在 Connecting 状态下收到数据包如果是 EAP-Start，则表示用户请求进行 EAP 认证，这里的认证总是由申请者发起。收到用户回应的 ID 之后，进入认证阶段，同时启动后端服务器线程，与 RADIUS 服务器进行认证。在收到认证结果数据包之后，认证成功则继续进行四步握手的密钥协商，否则直接进入 End，结束此进程。

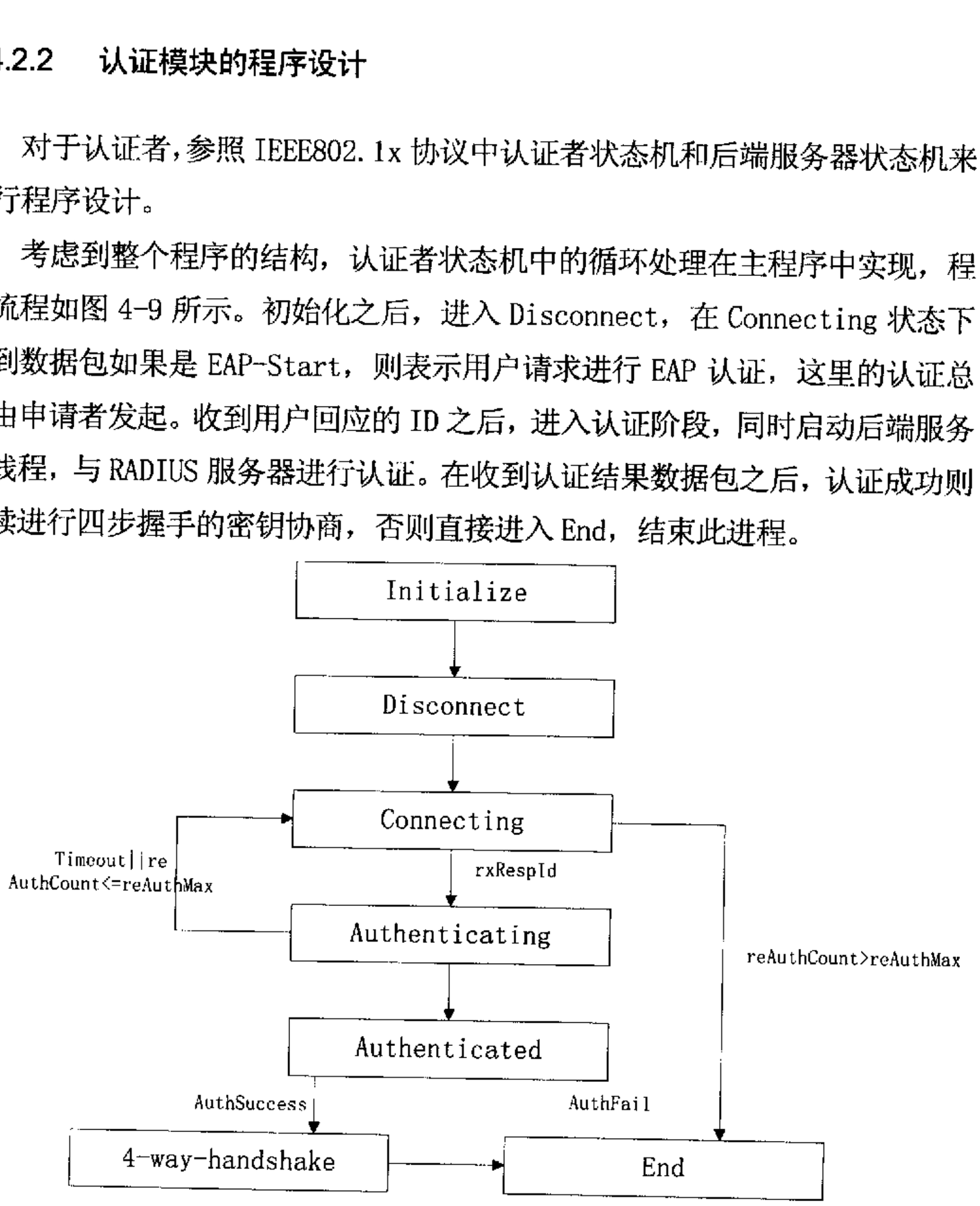


图 4-9 认证者程序流程

如果在一定的时间内没有收到响应，根据重发机制等待一段时间，如果超过重发次数，则结束此次认证。

如图 4-10 所示，此程序实现了后端服务器的状态机，认证者将申请者的认证数据包重新封装并转发给 RADIUS 服务器，同时将收到的 RADIUS 服务器的数据包解封转发给申请者。

开始认证之后进入 RESPONSE（响应）状态，认证者将申请者发送来的链路层数据包重新封装成 RADIUS 格式，向服务器转发。如果从服务器收到的响应是 aReq，表示质询，继续进行认证，进入 REQUEST（请求）状态，向申请者转发该数据包，并等待申请者的回应，如果收到的是响应是接受或者拒绝，则向申请者转发认证结果，进入 SUCCESS（成功）或 FAIL（失败）状态，认证过程结束。如果在一定的时间内未收到服务器的响应（aWhile= =0）或经过数次重发未收到客户端的响应，则进入 TIMEOUT（超时）状态。服务器回到 IDLE（空闲）状态，再次等待认证。

RADIUS 协议使用 UDP 作为传输层协议，采用 Socket 编程来实现。认证者和申请者在链路层进行数据包的发送和接收，支持 EAPOL 协议。用户界面模块与底层通信模块采用进程进行消息传递，认证者和后端服务器的程序之间采用线程进行相互调用。

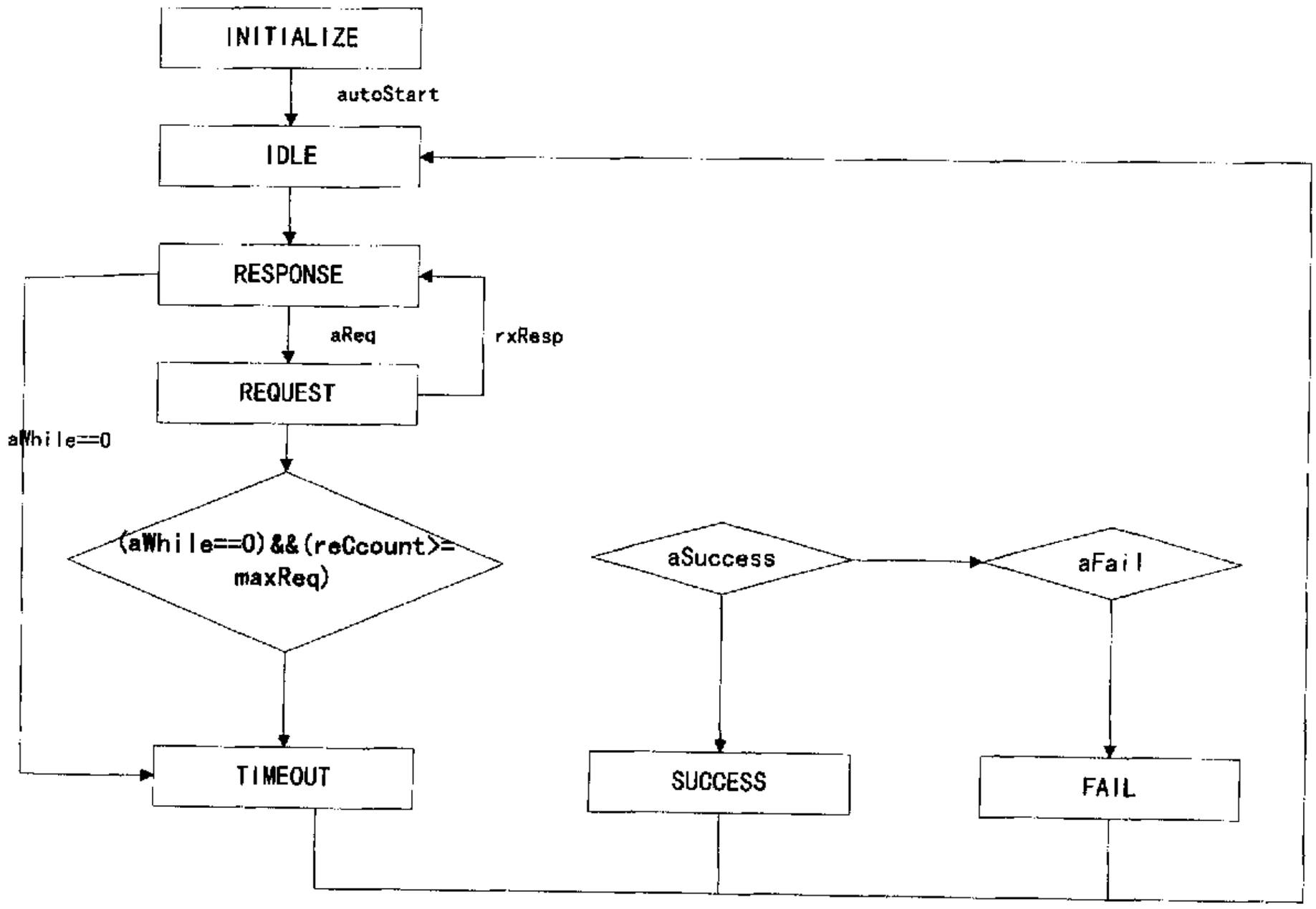


图 4-10 后端服务器的程序流程

4.5 STA 端的模型

客户端实现 IEEE802.1x 中的状态机以及密钥管理中的状态机，软件流程图如图 4-11 所示。

4.5.1 软件流程图

实现对 IEEE802.1x 做了改进，协议中的状态机原本只支持单用户的认证，有很大的局限性，因此在实现时进行了处理以支持多用户认证。AP 空闲时，如果有用户发起认证请求，就开始一次认证；AP 正在认证一个用户时，若有新的用户请求认证，那么回复该用户 Logoff，用户收到该条信息后，等待一段时间后重新发起认证请求，这一时间根据实际中一次认证时间暂设为 20s，可以根据不同的状况更改这一设置。这样，采用先来先到的方式对用户认证请求进行处理，认证者可以支持多个用户通过认证，并和外部的公众网进行通信。

程序主要包括3个主要部分：IEEE802.1x认证、TLS认证和密钥管理。主控模块进行模式选择，参数设置；接着调用认证模块，实现IEEE802.1x的状态机，EXIT 其中对应状态机中的各个状态的功能分别用函数实现，Authenticating函数调用TLS认证模块，过程包含了收包线程的关闭，返回认证结果给主控模块；认证成功，则调用密钥管理模块，进行四步握手密钥协商过程，四步握手成功后可以加载加密/整体性校验机制，然后进行数据传输，调用加密模块；认证失败或者四步握手失败，退出认证，客户端可以重新发起下一次认证。

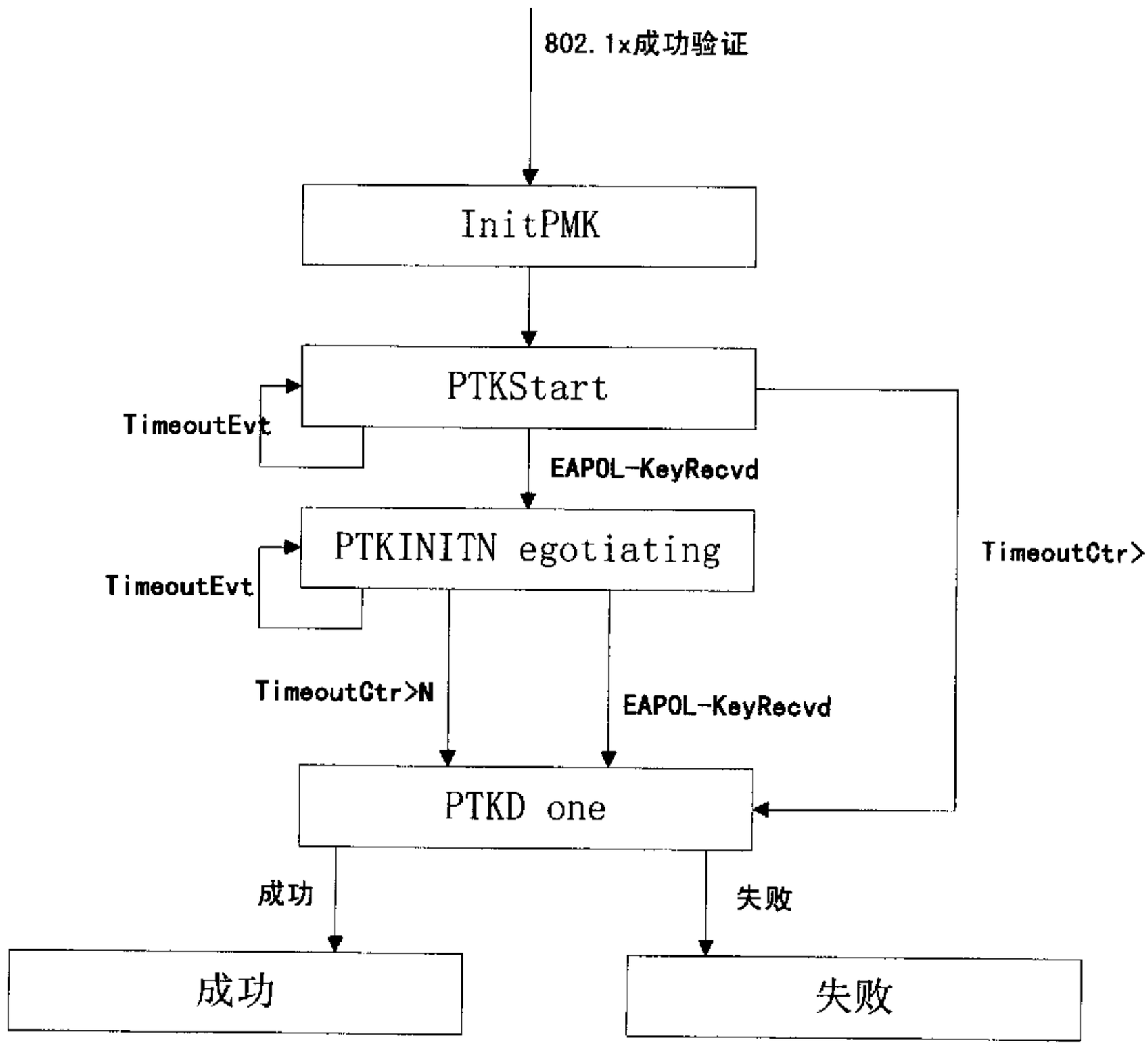


图4-11 四步握手的程序流程图

4.5.2 四步握手密钥管理的实现

四步握手的密钥管理机制属于密钥初始化的一部分，用来确认认证者和申

请者使用相同的 PMK，产生新的 PTK；同时也用来通知申请者端加载加密/整体性校验机制。它实现的关键在于四条 EAPOL-Key 消息的发送和接收。认证者向申请者发送第一、三条消息，申请者向认证者发送第二、四条消息。

以下是对各条消息内容的简要说明。

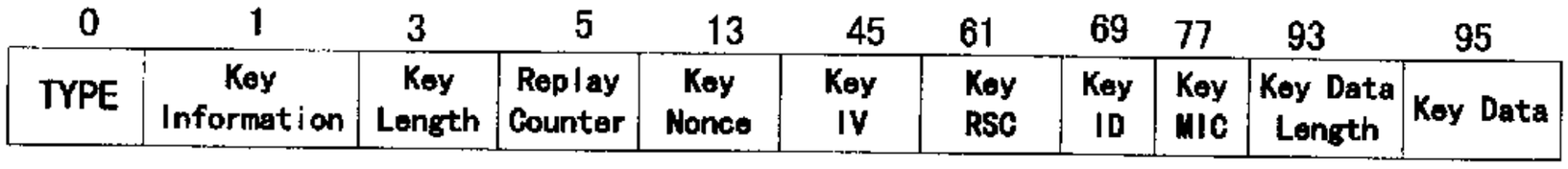


图 4-12 EAPOL-Key 消息内容

（1）认证者向申请者发送第一条消息，包括了 ANonce，没有进行整体性校验。

EAPOL-Key（0，0，1，0，0，P，0，Anonce，0,0）

Descriptor Type: 0xFE

Key Information: 0x0089

Key Length: 0x0040

Replay Counter: 0x00 (8 字节)

Key Nonce: 由 PRF-256（Random number，“Init Counter”，Local Mac Address ‖Time）计算得到

Key IV: 0x00 (16 字节)

Key RSC: 0x00 (8 字节)

Key ID: 0x00 (8 字节)

Key MIC: 0x00 (16 字节)

Key Data Length: 0x000

Key Data: NULL

(2) 申请者发送第二条消息，包含了 SNonce 和 MIC，并由 SNonce 和 ANonce 产生 PTK。

EAPOL-Key（0，1，0，0，0，P，0，Snonce，MIC,RSNIE）

Descriptor: 0xFE

Key Information: 0109(Ack 置 0，MIC 置 1，其余同第一条消息)

Key Length: 0x40

Replay Counter: 从第一条消息中得到

Key Nonce: 依据第一条消息中的计算方法得到 SNonce

EAPOL-Key IV:0x00(16 字节)

Key RSC: 0x00 (8 字节)

Key ID: 0x00 (8 字节)

Key MIC: 从 EAPOL-Key 的 Protocol Version 域开始一直到 EAPOL-Key 包结束计算出的 MIC 值。注意，计算时先置 Key MIC 域为 0，计算完毕后再将结果填充该域。MIC 的计算使用 EAPOL-Key MIC Key 作为参数，从前面的密钥层次可以看出 EAPOL-Key MIC Key 就是 PTK 的前 16 字节内容。

Key Data Length: 0x0004

Key Data: 0x25 0x02 0x01 0x00(这里选取了最简单的一种 RSN IE 格式)

（3）认证者由 SNonce 和 ANonce 产生 PTK，并且对 MIC 做校验，发送第三条消息，其中包括 ANonce，MIC 及是否安装加密/整体性密钥等信息。

EAPOL-Key（0，1，1，1，0，P，KeyIV，MIC，RSNIE）

Descriptor Type: 0xFE

Key Information: 0x01c9

Key Length: 0x0020

Replay Counter: increase 1

Key Nonce: ANonce

Key IV: 0x00 (16 字节)

Key RSC: 仅用于第三条消息

Key ID: 0x00 (8 字节)

Key MIC: 计算同上

Key Data Length: 0x0004

Key Data: 0x25 0x02 0x01 0x00

(4)申请者发送第四条消息，确认密钥已经安装。

EAPOL-Key（0，1，0，0，0，P，0，0，MIC，0）

Descriptor Type: 0xFE

Key Information: Ack 置 0，MIC 置 1，其余同第三条消息

Key Length: 0x0040

Replay Counter: 从第三条消息中得到

Key Nonce: SNonce

EAPOL-Key IV: 0x00 (16 字节)

Key RSC: 0x00 (8 字节)

Key ID: 0x00 (8 字节)

Key MIC: 计算同上

Key Data Length: 0x0000

Key Data: NULL

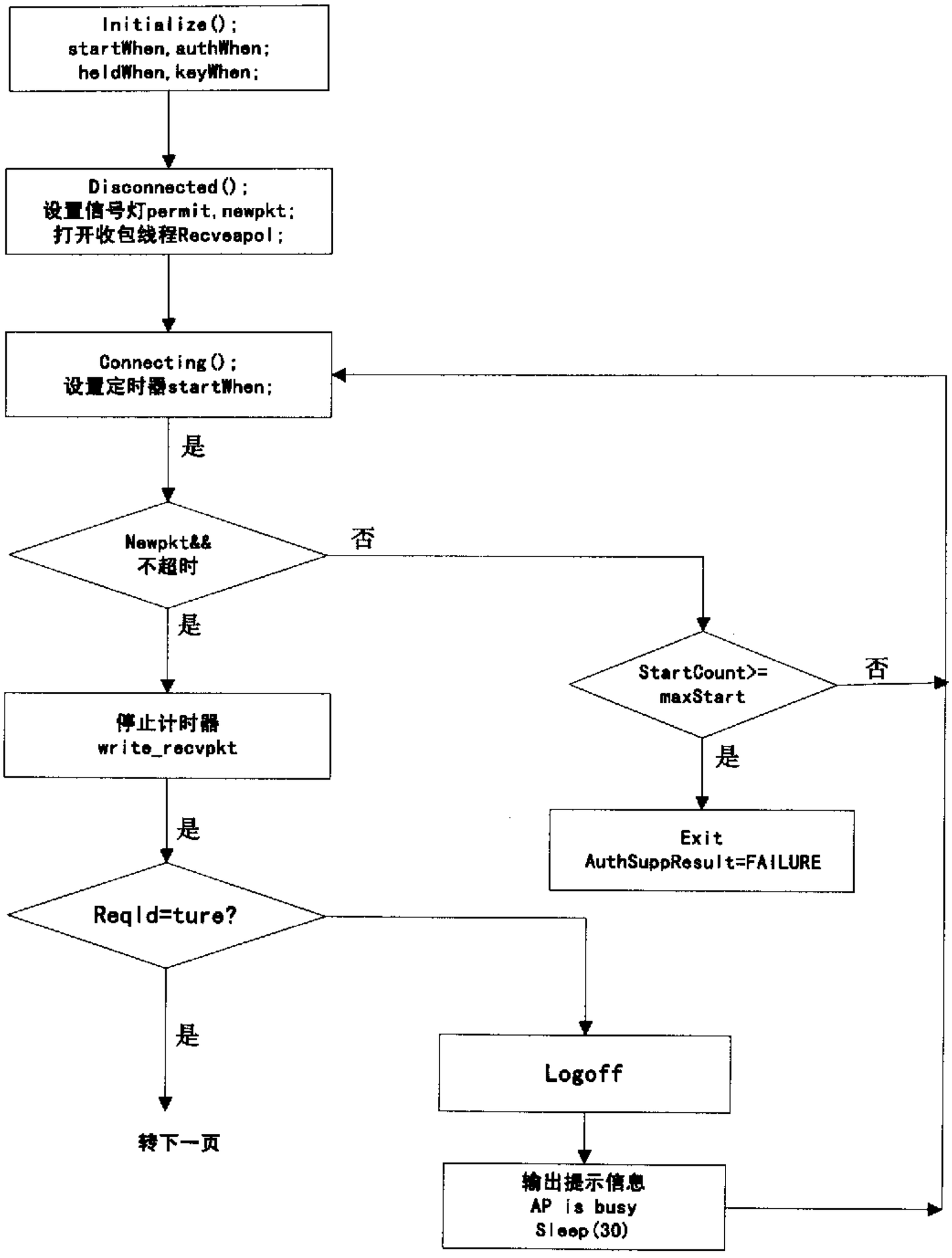
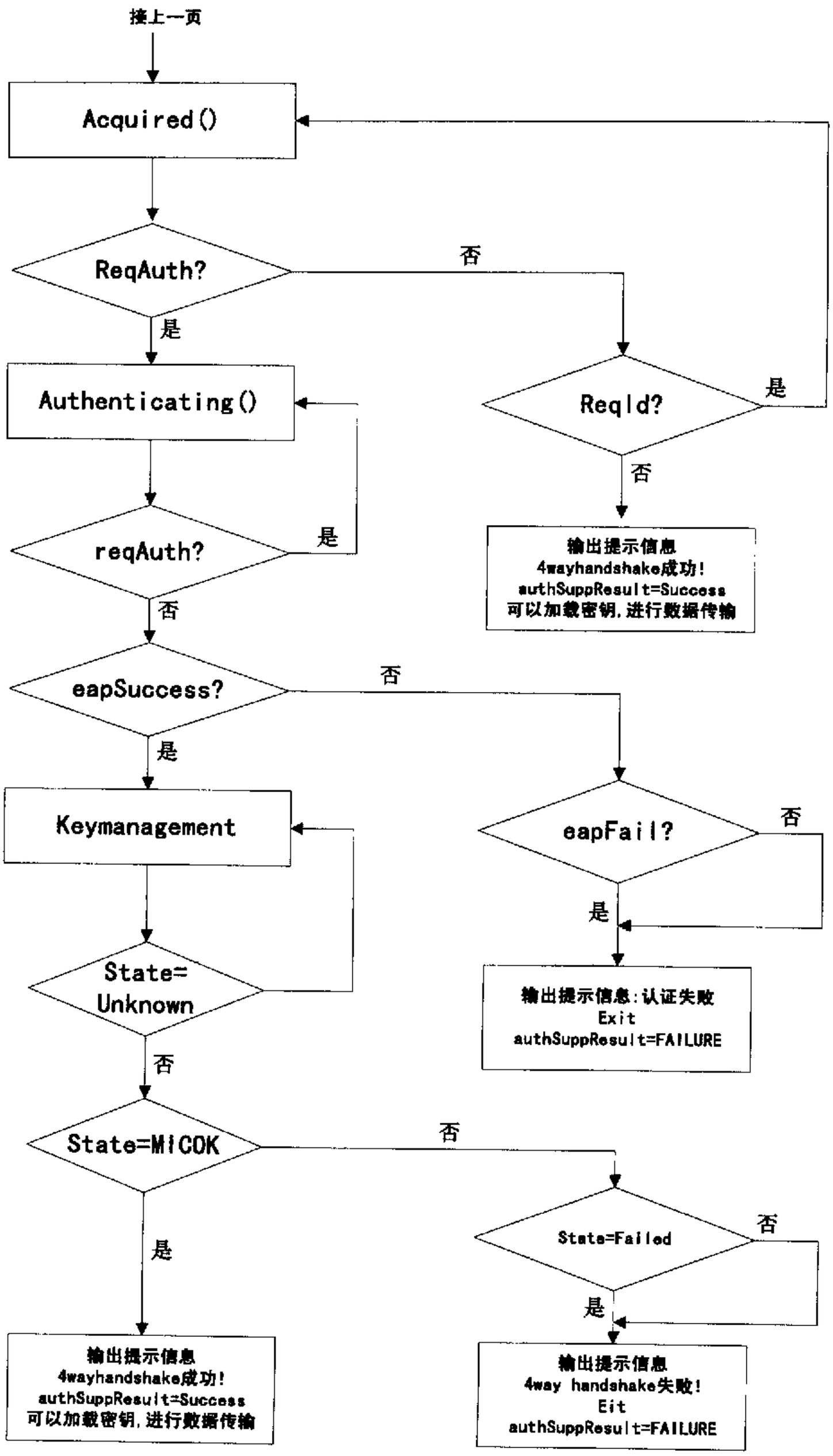


图 4-13　客户端的软件流程



续图 4-13　　客户端的软件流程

4.6 无线局域网安全的未来——IEEE802.11i

为了进一步加强无线网络的安全性，IEEE802.11 工作组正在开发新的安全标准 IEEE802.11i。标准的草案主要包含 TKIP（临时密钥完整性协议）、AES（先进的加密标准）加密技术和 IEEE802.1x 认证协议。

IEEE 802.11TGi(任务组 I)委员会已经制订了临时密钥完整性协议(TKIP)，作为过渡解决方案。TKIP 像 WEP 一样基于 RC4 加密，但以另一种方式实施，解决了 WEP 目前存在的脆弱性。它提供了快速更新密钥的功能。利用 TKIP，随着各个厂商计划推出 TKIP 固件补丁，消费者在无线局域网硬件上的投资将得到保护。

IEEE 802.11TGi 在正开发一个使用 AES（高级加密标准）的新协议，以实施更强大的加密和信息完整性检查。IEEE 802.11i 预计将采用 IEEE 802.1x 鉴权。

IEEE 802.11i 将包括增强的加密格式和鉴权机制，如 RADIUS、Kerberos 和 IEEEE 802.1x。IEEE 802.11i 的许多安全增强特性都可以通过固件升级来完成，而有些必须通过硬件来完成。

802.11i 将解决无线安全问题。大多数制造商都将在这些标准制订完毕时进行实施。此外，他们还必须提供不同厂商的无线局域网产品之间的互操作性，并确保他们的产品符合 802.11i 标准。

结论

本课题主要对 IEEE802.11 系列标准的无线局域网的安全性做了一定程度上的探讨。论文中主要做了以下的工作：

1、提出无线局域网的安全认证系统的模型。认证机制采用了 EAP-TLS，认证服务器采用目前比较成熟的 RADIUS 服务器，并支持 EAP-TLS 认证。

2、本文提出 WLAN 安全认证和密钥管理的软件方案，实现了包括安全认证、密钥管理、数据保护等安全功能，支持用户通过认证登陆网络，并保证了无线局域网中数据交换的安全性和可靠性。

3、总结了前人关于无线局域网安全的最新研究成果。

本文的研究结果表明，采用 IEEE802.1x 结合 RADIUS 服务器等能够更有效地确保无线局域网的安全性，在一定程度上能够弥补和防止 IEEE802.1x 本身所隐含的缺陷带来的攻击。本文提出的 WLAN 安全认证和密钥管理的软件方案是在总结前人的基础上提出的模型，具有一定的创新性。

本课题的进一步的研究工作是采用网络访真软件 OPNET，COMNET、UC Berkerley ns 和数学软件 Mathematica 等对实际的效果进行模拟和测试。在这场网络安全，特别是无线局域网的安全的对抗战中，永远都不会有一个结果，它只是一个旅程。正如孙子兵法所讲的“兵无常势，水无常形”，在这个艰苦的攻防战中，攻防双方的水平和档次都在不断的上升，需要我们不断地花很多时间去研究。

今后作者将继续致力与无线局域网的安全性方面的研究，并密切关注当今无线网络和网络安全方面的最新发展。

参考文献

[1] Matthew S.Gast. 802.11 Wireless Networks. O'Relly & Associates,Inc,Nov. 2002.

[2] 王欣靖, 李星等. 通信与网络新技术点评.北京：人民邮电出版社,2003 年 11 月.

[3] 唐岗. 无线局域网综述. 现代通信, 2002 年 8 月.P12-14.

[4] 崔玉文. 无线局域网安全问题的研究.哈尔滨学院学报,2002 年 6 月.P118-119.

[5] 徐玉.国外 WLAN 发展和面临的信息安全问题,2002 年 4 月.

[6] 黄炜. 探讨无线局域网安全性. 计算机时代, 2001 年第 11 期. P33-34.

[7] John Boladian.构建安全的无线局域网.通信世界,2003 年 1 月.

[8] 张伟. 无线局域网安全性研究.计算机工程,2002 年 1 月.P180-182.

[9] 孙树峰等. 无线局域网安全技术研究.计算机工程与应用,2003 年 7 月.P40-42.

[10] Kevin Regan.Wireless LAN Security:Things You Should Know about WLAN Security.

[11] David Pollino. How to Secure An Office Wireless Network.

[12] Dr.S.A.Vanstone. Next generation security for wireless:elliptic curve cryptography.

[13] Roy Szweda. Where is the future in wireless. http://www.three-fives.com .

[14] Bruce Potter. Tends in Wireless Security-The Big Picture.

[15] Bruce Potter. Wireless Authentication options for up and down the Stack.

[16] 沈芳阳,李振坤,林志.无线局域网安全机制探讨.广东工业大学学报,2004 年 9 月.

[17] 沈芳阳, 陈耀溪, 黄毅, 李振坤. 防火墙选购标准和技术前景展望.计算机应用研究, 2003 年第 20 卷. P155-156.

[18] 沈芳阳、李振坤、柳正青. DDos 攻击及其防范策略.微机发展,2003 年第 13

卷第 91 期. P46-48.

[19] 沈芳阳, 阮洁珊, 李振坤. 防火墙选购、配置实例及前景.广东工业大学学报,2003 年第 20 卷第 3 期, P40-44.

[20] 尹桂杰等. 无线局域网关键技术和发展综述.电视技术,2002 年第 2 期.P134-139.

[21] 杨志军. 浅谈无线局域网的优势和标准, 网络科技时代, 2002.

[22] 董火民等.无线与有线网络解决方案的比较与分析,计算机应用研究.2000 年第 9 期.P54-57.

[23] 曹常义等. 无线局域网的标准及前景.移动通信, 2002 年第 1 期. P44-47.

[24] 陈如明.蓝牙、无线局域网及其相关发展策略考虑.信息技术与应用,2002 年第 7 期.P3-11.

[25] 无线局域网的标准选择.北京电子, 2002 年.

[26] 曹常义等. 无线局域网的标准及比较.电信技术, 2002 年 6 月. P78-80.

[27] 熊静等. 无线局域网标准之分析及其解决方案.2002 年.

[28] Mark Ciampa. 无线局域网的设计与实现.科学出版社.2003 年 7 月.

[29] 刘昆等.基于 802.11 协议的无线局域网应用.自动化与仪器仪表,2003 年第 2 期.P54-56.

[30] 金纯等.IEEE802.11 无线局域网.电子工业出版社,2004 年 1 月.

[31] Bernard Sklar. Digital Communication. Publishing House of Electronics Industry,2002 年 9 月.

[32] Juha Heiskala. OFDM Wireless LANs: A Theoretical and Practical Guide. Publishing House of Electronics Industry,2003 年 3 月.

[33] GIL HELD. Deplying Wireless LANs. Post&Telecommunications Press. 2002 年 12 月.

[34] 周斌.保障 802.11 网络的安全.数据通信,2003 年第 2 期.P28-33.

[35] 赵丹. 无线局域网安全机制分析.信息安全与通信保密,2002 年 9 月.P37-40.

[36] 蒲洁. 无线局域网络的安全性.电力系统通信,2002 年第 9 期.P7-10.

[37] 曹秀英等. 无线局域网安全系统.电子工业出版社,2004 年 3 月.

[38] 陈曦等. 无线局域网的安全机制及安全性分析.计算机应用,2003 年 3 月.P30-32.

[39] 何礼. 无线局域网及其安全机制.四川通信技术,2000 年 10 月,P10-14.

[40] 谷大武等. 无线局域网络中的安全技术.电信快报,2002 年.

[41] 陈平等. 无线局域网的关键技术及其安全性分析.西南科技大学学报,2002 年 12 月.P1-5.

[42] 李强等. 增强无线局域网的安全性能.通讯世界,2003 年 4 月.P24-26.

[43] 王磊等.WEP 算法安全性浅析.西安联合大学学报,2003 年 10 月.P78-80.

[44] 沈基明等.802.11 WLAN 安全漏洞分析和改进方案.通信技术,2002 年第 7 期.P67-69.

[45] 吴越等.IEEE802.11 标准无线局域网安全缺陷分析及其解决方案研究.计算机工程与应用,2003 年 5 月.P31-34.

[46] 崔晓斐. 无线局域网及安全.丹东纺专学报,2002 年 12 月.P50-51.

[47] AVAYA Inc. Configuration and employment of IPSec VPN Security for 802.11 wireless LANs.2002.

[48] Intel. Wireless Security and VPN.2001.

[49] Arunesh Mishra. An Initial Security Analysis of the IEEE 802.1x Standard. University of Maryland,Feb.2002.

[50] 张永德等.对 IEEE802.1X 协议的安全性分析.东北电力学院学报,2003 年 4 月.P75-78.

[51] 张杰. 无线局域网标准及安全性研究.Modern Science&Technology of Telecommunications,2002 年 11 月.P4-8.

[52] 郭立群. IEEE802.1x 认证技术的原理与应用.太原科技,2003 年第 6 期.P72-73.

[53] L.Blunk,J.Vollbrecht.PPP Extensible Authentication Protocol(EAP).RFC2284,March1998.

[54] 王璐，曹秀英.EAP 协议及其应用.通信技术,2002 年 7 月.

[55] B.Aboba,D.Simon, PPP EAP TLS Authentication Protocol,RFC2716,Oct.1999.

[56] T.Dierks,Certicom,C.Allen,Cericom. The TLS Protocol Version 1.0,RFC2246,Jan.1999.

[57] 周学广等.信息安全学.机械工业出版社,2003 年 3 月.

[58] Tim Moore. “Suggested Changes to Robust Security Network(RSN) for

IEEE802.11”,doc:IEEE 802.11-02/178R0,March 2002.

[59] Bernard Aboba.IEEE802.1X Pre-Authentication,IEEE802.22-02/389R0,July 2002.

[60] 石兴方等.802.11 无线局域网的认证机制研究. 计算机工程,2003 年 6 月.P131-133.

[61] Jerome Swartz. Security Systems for a mobile world.Technology in Society. 2003.5.

[62] Wassim Itani etc. J2ME application-layer end-to-end security for m-commence.Journal of Network and Computer Applications.2004.

攻读学位期间发表的学术论文

[1] 沈芳阳, 陈耀溪, 黄毅, 李振坤. 防火墙选购标准和技术前景展望.计算机应用研究, 2003 年第 20 卷. P155-156

[2] 沈芳阳、李振坤、柳正青. DDos 攻击及其防范策略.微机发展,2003 年第 13 卷第 91 期. P46-48

[3] 沈芳阳, 阮洁珊, 李振坤. 防火墙选购、配置实例及前景.广东工业大学学报,2003 年第 20 卷第 3 期，P40-44

[4] 陈耀溪，沈芳阳，蔡治. 宽带 IP 城域网组网技术及技术进展研究.广东自动化与信息工程,2003 年第 24 卷第 2 期.P32-34

[5] 徐建哲，沈芳阳，邓静. 三层结构及其应用实例研究.广东工业大学学报,2003 年第 20 卷第 4 期，P78-82

[6] 柳正青，刘怀亮，李振坤，沈芳阳. XML 编程接口的研究与一个应用模型. 微机发展, 2003 年第 13 卷第 6-2 期，P61-63

[7] 韩贵来，李卫华，卢方国，沈芳阳.面向 Agent 的网格中间件模型.广东工业大学学报,已录用

[8] 沈芳阳, 李振坤, 林志.无线局域网安全机制探讨.广东工业大学学报,2004 年 9 月

[9] 郭庚麒, 沈芳阳. Jini 技术及其应用实例.微机发展,2004 年 6 月

致谢

首先，衷心感谢我的导师李振坤教授对我的指导和帮助。李教授以其渊博的知识、丰富的阅历、耐心的教导和宽厚的为人令我受益匪浅。过去的三年，无论在学习上、生活上、还是在思想上，李教授都给了我无微不至的教导和关怀，同时在我最困难的时刻也给了我最重要的指导和支持，在此，谨向李教授致以我最衷心的感谢和崇高的敬意！同时衷心祝愿李教授快乐幸福！

衷心感谢计算机学院的杜秋虹书记、何振炎书记、曾庆尚书记、区益善教授、汤庸教授、傅秀芬教授、徐海水副教授、吴伟民副教授、杨文伟副教授、余永权教授、张立臣教授、凌捷教授、曾文曲教授、何瑞麟副教授、李立希副教授、唐平副教授、张益新教授、张梅副教授以及计算机学院的其他老师对我的关心和培养。衷心感谢研究生处的潘玲老师、梁丽华老师、张应春老师、刘怡军老师等多位老师的支持和鼓励。同时，衷心感谢计算机工程研发中心的李怀香副教授、陈平华老师、王文彦老师、刘广聪老师、黄益民老师、陈靖宇老师等各位老师在学习上和生活上给予我的诸多帮助。你们的帮助使我得以顺利完成学业。

衷心感谢我的师兄刘怡俊、刘少涛、孙炜、崔洪刚，王帮海、徐建哲、马传松、师姐王秋杰、边晓燕、杨桂华、张晶，师弟许兴鹃、朱兵章、李科景、梁海健、孙延海、聂小东、谭石强、刘竹松，师妹何佳嘉、张喆、宋静静、陈作霞、蓝芳华，我的室友韩贵来、张信一、张华、许伟权、刘冬宁。正是你们陪我度过了这个三年的岁月，与你们的交流使我解决了研究中的诸多困难。谢谢你们！

衷心感谢我同在工程中心的好朋友柳正青、刘怀亮，邓静，和你们共同学习的三年令我今生难忘；衷心感谢我的研究生同学陈建伟、崔振兵、卢方国、刘浩钊、钟迅科、陈贤初、钟祥睿、谢新屋、凌小君、陈其明、王竑、陈志、李文志、何东风、申健、曹咏春、黄红梅、何玉菁等，你们给予我很多的帮助和快乐，祝你们幸福、快乐！

衷心感谢广东省燃料公司的黄致惠总经理，正是你的支持、鼓励和帮助使