摘 要

随着计算机网络、通信技术的发展，移动设备和无线技术也快速的发展起来。由于无线局域网(Wireless Local Area Network)具有有线局域网所无法比拟的灵活性和便利性，它被广泛的应用于许多热点场所，如校园、机场、宾馆、医院、商场等。在给人们带来便利的同时，无线局域网由于其固有的物理特性，带来了一系列安全问题：无线局域网中的数据通过高频无线电波传输，极易遭到窃听，而且在无线网络环境中，难以应用有线网络的物理访问控制手段。于是要求它较之有线局域网应具有更高的安全机制。

1997 年 10 月，IEEE 批准了关于无线局域网的标准 IEEE 802.11，这标志着无线局域网技术开始由实验室走向市场。随后 IEEE 先后批准了 IEEE 802.11b, IEEE802.11a 和 IEEE 802.11g 标准，符合这些标准的产品已经开始大量涌向市场，无线局域网技术由新兴转向成熟，成为世界各大 IT 厂商关注的焦点之一。

本文在重庆市教委科技研究项目（编号：050301）的资助下，对 WLAN 进行了深入的分析和研究。本文首先分析了无线局域网已有安全协议的工作原理，说明了其设计优缺点并指出了一些利用协议设计缺陷进行攻击的方法；接着讨论了 IEEE 802.11 i 的主要内容，包括密钥管理、认证体系和数据保密协议 TKIP、CCMP，分析了它们的设计思想和特点；然后分析比较了现有的无线局域网认证方法，指出了他们存在的缺陷和容易遭受的攻击，并在此基础上，提出了 EAP-SPEKE 密钥交换和认证方法。EAP-SPEKE 协议改进了 SPEKE，不仅支持密钥交换和双向认证，还能够抵御中间人攻击和离线的字典攻击。EAP-SPEKE 方法增强了 IEEE 802.1X 标准和 EAP 协议安全性能而无需更改它们的基础结构。

关键词：IEEE802.11，有线等价保密，认证协议，SPEKE

Abstract

With the development of Computer Network and Communication Technology,mobile devices and wireless technology are evolving at a rapid speed. Owing to its mobility and convenience, wireless LAN is becoming popular in hot spot regions,such as campus, hotels, airports, shopping malls, and so on. With the flourish of WLAN market, people are concerned about the WLAN security more than ever. Data transmitted in WLAN over high frequency radio is subject to eavesdropping, furthermore, physical media access control measures don't adapt to WLAN.

IEEE ratified the WLAN 802.11 standard in Oct 1997, which was a landmark that WLAN technology went from the laboratory into the market. As the 802.11b, 802.11a and 802.11g standards were ratified by IEEE, products consistent with these standards became popular in the market.

By sustentation fund from ChongQing ministry of education grant No: 050301, we do an in-depth study on the security in WLAN. In this paper, we first analyze the mechanism of the present security protocols. We point out their merits and flaws, and present some attacking ways by means of the design flaws in the protocols. Secondly, we analysis the major elements in IEEE 802.11i, including key management, authentication system and data privacy protocols.In the end,wo compares the current authentication methods of Wireless LAN and analyzes their weakness,and amend a password authentication key exchange protocol named EAP-SPEKE(Extensible Authentication Protocol-Simple Password Encrypted Key Exchange) which improves the SPEKE(Simple Password Encrypted Key Exchange). The improved protocol supports mutual authentication and key derivation based on Diffie-Hellman Encrypted Key Exchange and password verification.It can protect the network from the Man-in-the-Middle and the offiine dictionary attacks while does not require any modification to the IEEE 802.1X and EAP.

Key words: IEEE802.11，WEP，Authentication Protocol，SPEKE

独 创 性 声 明

本人声明所呈交的学位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。据我所知，除了文中特别加以标注和致谢的地方外，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 重庆邮电大学 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谢意。

学位论文作者签名：[signature] 签字日期：2006 年 5 月 20 日

学位论文版权使用授权书

本学位论文作者完全了解 重庆邮电大学 有关保留、使用学位论文的规定，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，允许论文被查阅和借阅。本人授权 重庆邮电大学 可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：[signature] 导师签名：[signature]

签字日期：2006 年 5 月 20 日　　签字日期：2006 年 5 月 20 日

第一章 绪论

1.1 研究背景及意义

20世纪90年代以来，移动通信和Internet是信息产业发展最快的两个领域。移动通信使人们可以在任何时间地点与他人进行通信，Internet使人们可以获得丰富的信息。而WLAN则成功的将移动通信和Internet的优势结合起来，以无线信道为传输介质，实现在短距离内的无线网络通信。主要用于传输速率大于1 Mbit/s的局域和室内数据通信，同时为多媒体应用(语音、数据和图像)提供了一种潜在的手段。

WLAN[1]是在有线局域网的基础之上，通过添加无线访问点、无线网桥、无线网卡等硬件设备实现对有线网络的扩充。与有线网络相比，无线网络具有可移动性，可以做到随时上网；同时，无须布线节约了建网时间，而且能够实现即插即用，组网灵活，网络管理人员可以迅速将其加入到现有网络中。越来越多的企业利用WLAN的优势实现移动通信，应用WLAN已成为新一代无线电子商务的发展趋势。目前WLAN的应用主要集中在公众服务、交通旅游服务、货场管理、移动办公系统、智能小区、政府机构及个人用户等领域，随着应用的逐渐深入，市场重心会从公众服务应用渐渐过渡到企业应用及家庭应用上。按照国外的发展经验，WLAN应用最初的重点是高层商务人士，但最终的方向是逐渐趋于大众化，所以企业用户及家庭用户是未来两年WLAN最大的潜在用户群。可以预见，随着开放办公的流行和手持设备的普及，人们对移动性访问和存储信息的需求愈来愈多，因而WLAN将会在办公、生产和家庭等领域不断获得更广泛应用，WLAN的市场已日趋成熟。

安全始终是网络通信的重要问题。然而，WLAN在安全方面存在固有弱点。与有线网络不同，WLAN不需要任何物理连接，而是在开放的环境下以空气为介质进行数据的传输。在无线数据传输的范围内，如果没有采取任何安全措施，任何人只需借助一台简单的接收器就能够收听到在无线信道上的所有对话，未授权的用户可以轻易的截获传输数据，而恶意攻击者可以通过伪装合法身份进入WLAN窃取网络信息。因此，在WLAN上实施窃听更加简单。据美国Gartner发表的有关企业WLAN的安全方面的调查报告表明，由于企业在部署WLAN系统时没有采取适当的安全对策，到2002年底，30%的企业被数据泄漏等安全问题所困扰。据介绍，目前大约50%以上的企业已采用或计划采用WLAN。但据推测至少20%的企业内部网络的WLAN存在问题。RSA安全公司在英国伦敦进

行的一项调查也表明，67%的 WLAN 毫无安全可言。无线网络的安全问题已经引起了国外不少公司或组织的重视，各公司或组织已纷纷投入人力物力开始了无线安全方面的研究，其中，作为基本安全措施的 WLAN 安全协议成为当前安全研究领域的热点之一，无论从理论角度还是从应用角度来看，开展 WLAN 安全的研究，不但具有重要的学术价值，而且对 WLAN 的发展与应用具有极为重要的意义。

1.2 无线局域网的系统模型

- STA 与 AP

无线站点(STA[1])，有时候也叫做无线终端、移动终端等，比如插入无线网卡的笔记本电脑或者 PDA。无线接入点(AP)为 STA 提供服务，作用类似以太网中的集线器。

- BSS 和 ESS，以及 WLAN 的工作模式

基本服务集(BSS[1])类似于移动通信中“小区”的概念。扩展服务集(ESS)是由若干个 BSS 通过 AP 连接而成，有时连入有线网络。ESS 类似于有线局域网中工作组的概念。

如果一个 BSS 是孤立的，不在任何 ESS 中，则称这个 BSS 是独立 BSS(IBSS)。我们很多时候也称 IBSS 内的 STA 工作在特别(Ad hoc)模式，或自组网模式、对等网模式等。

与特别模式相对的工作模式叫做基础结构(Infrastructure)模式。在基础结构模式中，多个 BSS 共同构成 ESS，并连接在有线网路上。这是一种更加普遍的应用模式，因为在大部分时候人们采用 WLAN 是将它作为一种宽带接入手段，接入已有的有线网络。

简单来说，IBSS 概念对应特别模式，ESS 概念对应基础结构模式。

1.3 无线局域网的技术标准

尽管 802.11 b[2]目前得到了广泛的应用，但无线局域网仍存在多种标准。

1997 年设立的 802.11 工作组旨在为 WLAN 制订标准。由于必须与以太网相一致，所以 802.11 需要 PHY[16](物理层)和 MAC[16](介质访问控制层)规范。有线以太网的 PHY 涉及电压和引脚布局，而无线以太网的 PHY 涉及射频和调制。同样，表示 OSI 数据链路层下半层的 MAC 定义了收发以太网无线电信号的介质访问协议。

目前 802.11 共有九种扩展名，从 a 到 i(a、b、c、d、e、f、g、h 和 i)。其中

802.11（a、b 和 g）是与 PHY 有关的标准，其余几个标准见表 1.1。

标准名称	主要内容
802.11d	旨在制订在其他频率工作的多个 802.11b 版本，使之适合于世界上现在还未开放使用 2.4GHz 频段的国家。
802.11e	该标准将对 802.11 网络增加 QoS 能力，它将用时分多址（TDMA）方案取代类似以太网的 MAC 层，并对重要的业务增加额外的纠错功能。
802.11f	该标准旨在改变 802.11 的切换机制，以使用户能在两个不同的交换分区（无线信道）之间，或在两个不同的网络接入点之间漫游的同时还保持连接。
802.11h	该标准旨在对 802.11a 的传输功率和无线信道选择增加更好的控制功能，它与 802.11e 相结合，适用于欧洲地区。
802.11i	该标准旨在消除 802.11 最明显的缺陷：安全问题。
802.11j	该标准将使 802.11a 和 HiperLAN2 这两个标准在同一频率共存。

表 1.1 IEEE802.11 系列部分标准

802.11b

往回推最早应该是 IEEE 在 1997 年发表了第一个 WLAN 的标准 802.11，而现在很多媒体屡屡提到的 802.11 b 是 IEEE 在 1999 年 9 月批准的。802.11 b 也被称为 Wi-Fi，其最高通讯速率为 11 Mbps，室内传送距离为 50 到 150 英尺，室外可达 1000 英尺。

不过随着时间推移以及需要不断适应新的需求，IEEE 又提出了 802.11a 和 802.11g，其它的短距离无线通信标准还有 HomeRF 和 Bluetooth 等。在这些标准中，802.11g、BlueTooth、HomeRF 都和 802.11b 一样共享 2.4GHz 的频段。

802.11g

这个标准是要为 802.11b 提速的，即从原来的 11Mbps 跃升到 54Mbps。

无线设备都是通过分频(spread-spectrum)技术传送数据的，这之中有两种分频技术，一种是 HomeRF 和 Bluetooth 使用的跳频(frequency hopping)技术，另外一种是 802.11b 和 802.11g 使用的直接序列(direct sequence)技术。

802.11a

最后就是 802.11 a[2]了，这个标准便用 5GHz 的频段，其速率可达 54Mbps，该频段在美国又被称为 U-NII(Unlicensed National Information Infrastructure)，分频采用 OFDM（Orthogonal Frequency Division Multiplex）技术。尽管和 802.11b 工作在不同的频段，但它们可以共享介质访问控制 MAC，而 802.11a 更多的是

物理层 PHY 上不同的标准描述。

Bluetooth

Bluetooth[2]可能是更为我们所熟知的技术了，它是一种低带宽、短距离、低功耗的数据传送技术，主要用在 PDA、手机、笔记本电脑等设备。

但是 Bluetooth 事实上是个迟到者，802.11b 现在已经到了大规模生产以降低成本的时候了，而 Bluetooth 产品才刚刚开始进入市场。虽然都在 2.4GHz 频段上工作，但是 2004 年 4 月份 IEEE 的 PAN(Personal Area Network)，即 802.15 工作组提出一项议案，其目的是使 Bluetooth 和 802.11b 可以同时工作。

HomeRF

HomeRF[3]主要为家庭网络设计，是 IEEE802.11 与数字无绳电话技术(EDCT，Digital Enhanced Cordless Telecoimnunications)的结合，目的在于降低语音数据成本。HomeRF 采用了扩频技术，工作在 2.4GHz 频段，能同步支持 4 条高质量语音信道。目前 HomeRF 的最高传输速率可达 10 Mbps。

HiperLAN

HiperLAN[3]是欧洲通信标准协会 ETSI(European Telecommunications Standards Institute)主推的标准，有 HiperLAN/1 和 HiperLAN/2 两套标准，它们都同样运行在 5GHz 上，但 HiperLAN/2 的传送速率更高，和 802.11a 一样，也是 54Mbps，并且兼容 3G WLAN 系统，可以收发数据、图形及语音数据。但是在频率选择上欧洲和美国没有协调一致，这就造成双方的产品未来都成为在欧洲范围内或美国范围内使用的“本地”技术了。标准不一致也可能会使得未来的产品成本在长期内不能降低。

1.4 无线局域网的安全研究现状

自 IEEE802.11 标准设计阶段起，安全问题就成为了无线局域网技术的一个重要方面。IEE802.11 协议的安全措施包括：

（1）采用扩频技术确保无线电波的安全传输，使得监听者难以捕捉到有用的数据。

（2）采取网络隔离及网络认证措施。

（3）设置严密的用户口令及认证措施，防止非法用户入侵。

（4）设置附加的第三方数据加密方案，即使信号被监听也难以理解其中的内容。

然而研究表明，这些措施只是攻击者攻击道路上的一道很容易突破的屏障，攻击者可以利用认证的缺陷轻易地对网络进行非授权访问，可以篡改在无线局域网中的数据，甚至分析足够数据包得到各网络设备中共享的密钥，对数据进行解

密。为此，国内外学者和研究人员对无线局域网的安全认证做了深入的分析和研究，包括对各种现有的网络安全措施的分析，提出相应改进措施以及改进方案。我国也推出了自己的无线局域网的安全标准 WAPI，IEEE 在 2004 年 6 月 25 号推出新一代无线局域网的安全标准 IEEE802.11i。

1.5 本论文的主要工作

本文深入分析了 IEEE 802.11 WLAN 的安全，结合目前的解决方法，具体进行了以下几点工作：

- 分析了目前 802.11 WLAN 的安全措施；
- 讨论了目前主要的 802.11 WLAN 安全解决方案 802.11i，给出了其设计思想；
- 针对 802.11i 认证协议的开放性，本文分析了目前主要的认证协议及其不足；
- 对于目前认证协议的不足，本文分析并提出了 EAP-SPEKE 认证方案；
- 对于 EAP-SPEKE 认证协议，本文不仅从理论上进行分析，而且进行了仿真，直观地表明的协议性能。

第二章 IEEE802.11WLAN 的安全机制分析

IEEE 802.11 标准定义了一系列安全机制(IEEE 802.11b 和 IEEE 802.11a 采用的安全机制与 IEEE802.11 完全相同)，为在无线局域网中的数据传送提供安全保障，这些安全机制包括：

1)服务群标识符 SSID (Service Set Indentifier)访问控制；

2) MAC 地址过滤(MAC Address Filtering)控制；

3)有线等价保密 WEP (Wired Equivalent Privacy)机制。

2.1 服务群标识符（SSID）访问控制

SSID[2][3]访问控制技术对一个或多个 AP 组成的无线局域网都适用，它提供了把大型的无线局域网分割成多个接入子网(可包含一个或多个 AP)的功能。在同一无线子网中，所有 AP 具有相同的 SSID。只有配置相同 SSID 的无线工作站才能接入该网络，即无线工作站必需出示正确的 SSID，才能访问 AP。因此可以认为 SSID 是一个简单的口令，从而提供一定的安全。

但是，应该注意到 SSID 访问控制机制是非常初级的，它存在如下的安全缺陷：

（1）如果把 AP 配置成向外广播其 SSID，那么这种安全机制将不起任何作用。因为任何没有配置指定 SSID 的无线工作站也都可以收到 AP 的 SSID。

（2）由于在一般情况下，用户自己配置客户端无线工作站系统，因此每个站点的用户都知道该 SSID，很容易被非法用户获得。

（3）在几个管理帧中都包含网络名称和 SSID，因此攻击者很容易通过嗅探软件来获得 SSID，即使激活了 WEP，这个缺陷仍然存在。

2.2 MAC 地址过滤控制

每个无线工作站网卡都具有唯一的物理地址标识，因此可以通过手工维护 AP 中的一组允许访问的 MAC[3]地址列表，实现物理地址过滤。只有无线工作站网卡的 MAC 地址存在于允许访问的地址列表中，该工作站才允许接入网络。物理地址过滤属于硬件认证，而不是用户认证。如果增加接入网络的无线工作站，就需要在所有允许接入的 AP 的 MAC 地址列表中手工添加该站点无线网卡的 MAC 地址。

从表面上看，MAC 机制提供了强大的安全性能，然而从实质上却不难发现，该控制方法也存在着许多弱点：

（1）AP 中的 MAC 地址列表需要随时更新，而且目前都是手工维护，因此这种方式的扩展能力很差，只适合于小型无线网络。

（2）由于 MAC 地址过滤控制是基于设备的认证，因此无线工作站的遗失或失窃都会造成该机制失效。

（3）MAC 地址很容易被攻击者获得，通过嗅探软件获得并修改无线网卡的 MAC 地址，攻击者就可以伪装成有效的用户接入到“受保护”的网络上。

2.3 有线等价保密（WEP）机制

由于无线传输比有线传输更容易被窃听，为了保障无线通信信号的安全性，IEEE 802.11 标准定义了 WEP[6][7][8]用于无线工作站和 AP 之间的通讯加密，使窃听者即使窃听到数据包也无法解开数据。WEP 的第二个作用是防止对网络的非授权访问，通过对密钥的保护使没有密钥的非授权者无法访问网络。WEP 机制采用了一种对称密钥加密算法——RSA 数据保密公司的 RC4 算法。

2.3.1 WEP 工作原理

WEP 算法是明文与其等长的伪随机密钥序列按位模二相加的一种算法。加密原理见图 2.1。

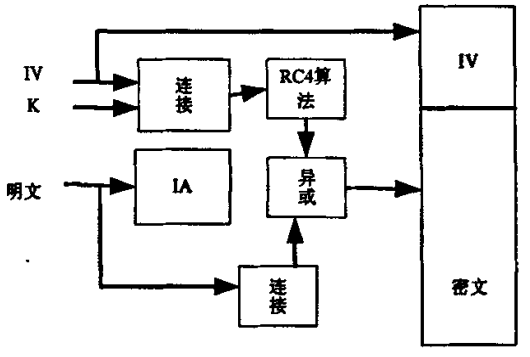

图 2.1　WEP 机制加密原理

WEP 机制加密工作过程如下：

1) 接入点 AP 用共享密钥初始化基本服务集 BSS 的每个工作站点；

2) 根据消息的原文(Plaintext)，发送站点运用 CRC-32 算法产生一个完整性校验向量 ICV (Integrity Check Vector)，并将 ICV 附加到消息原文后面；

3) 发送站点随机选择一个 24 位初始向量 IV (Initialization Vector)，将之与

一个 40 位或 104 位共享密钥(Secret Key)连接在一起产生种子密钥(SEED)，送入到一个伪随机序列发生器 PRNG（Pseudorandom Number Generator)，产生一个与最大可能长度消息加 ICV 等长的伪随机序列；

4) 将 Plaintext +ICV 和伪随机序列按位进行异或运算，产生密文(Ciphertext)；

5）将 IV 放在加密数据前，产生实际传送的数据。

WEP PRNG 是该过程的重要部分，因为它将一个相对短的密钥变换成一个绝对长的密钥序列 IV，以明文的形式传输。它有效地扩展了密钥使用寿命，在密钥保持为常数的条件下通过周期性改变 IV，每一个新的 IV 就产生一个新的种子密钥和密钥序列。

当加密的消息序列到达接收站点时，接收机就开始解密，解密工作原理如图 2.2 所示。

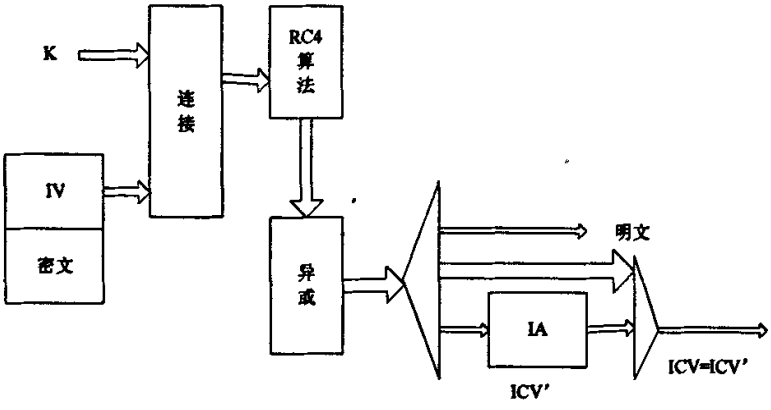

图 2.2　WEP 机制解密原理

1) 把收到消息中的 IV 与密钥号所对应的密钥链接产生种子密钥，然后把其输入到伪随机序列产生器(WEP PRNG)，产生与加密时相同的伪随机密钥序列；

2) 将密文和伪随机密钥序列按位模二相加产生原始明文和原始的完整性校验向量 ICV；

3) 把恢复的明文利用 CRC-32 算法进行完整性校验，输出一个完整性校验向量 ICV'，接着判断 ICV'与 ICV 是否相等，如果相等则说明收到的消息是正确的，如果不相等则说明收到的消息是错误的。

2.3.2 WEP 访问控制（共享密钥认证）

WEP 除了提供数据加密外，第二个作用就是提供了共享密钥认证。共享密

钥认证的步骤如图 2.3 所示。

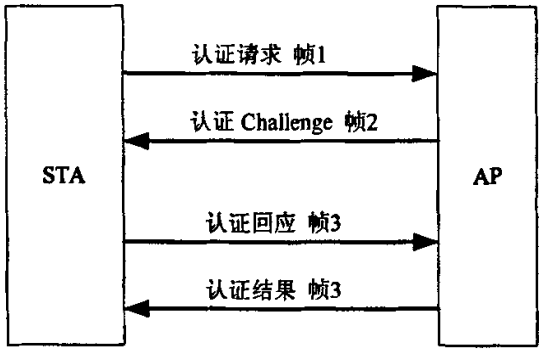

图 2.3　共享密钥认证

1) 无线工作站向接入点 AP 发送“认证请求”数据帧；

2) AP 收到“认证请求”帧后，向工作站发送一个随机口令消息(r)，同时 AP 利用共享密钥和 WEP 算法产生口令的加密信息(y)；

3) 无线工作站点收到口令消息(r)后，运用与 AP 相同的共享密钥和 WEP 算法产生口令的加密响应(y')，并发送给 AP；

4) AP 验证 y 和 y'的关系，如果 y= y'， AP 发送认证成功消息给无线工作站，允许无线工作站点接入该基本服务集 BSS；如果 y≠y'，则接入失败，AP 向无线工作站发送一个不同随机消息的新口令，重新进行身份验证。

2.3.3 WEP 机制缺陷

1、WEP 加密算法存在的漏洞和不安全因素

WEP 算法采用的 RC4 加密算法，其安全的关键在于使用了加密密钥流对明文进行异或操作。因此加密密钥流的重用是 WEP 一个固有的安全问题。以下围绕产生密钥流的两个因素：WEP 密钥和 IV 来分析 WEP 算法的安全问题。

（1）WEP 密钥重用[6]。在 WEP 中，将 IV 和密钥 K 经过伪随机序列发生器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：通过 IV 和密钥产生相同的密钥流，再将密钥流与密文信息相异或。众所周知，对于流密码算法的一个明显缺陷是：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。如：

$C1=P1 \oplus RC4(v, k)$

$C2=P2 \oplus RC4(v, k)$

则有：

$C1 \oplus C2=(P1 \oplus RC4(v, k)) \oplus (P2 \oplus RC4(v, k))=P1 \oplus P2$　　(2.1) [6]

从式(2.1)中可以看出 C1 和 C2 是接收到的 2 个不同的密文信息，将它们进行异或运算后就能将密钥流的加密效果去掉，运算的结果就是 2 个明文信息 P1 和 P2 的异或值。因此，假如一个消息的明文已知（比如已知 P1），不论另外一个消息是否可知（比如 P2），则它的明文可以立即得到（因为已知 C1⊕C2 的结果）。即便是不知道其中一个明文，不能马上恢复出明文，但明文的恢复难度已经大大降低了，并且目前有比较成熟的算法可以完成这项工作。如果使用同一密钥流的包越多，那么破解的难度就越小。

（2）IV 在传输过程中没有加密，攻击者可以轻松的得到 IV。在使用 WEP 进行数据传输时，源端将 IV 及加密后的密文一起传送出去，而对于 IV 并没有使用任何加密保护手段，也没有采用任何的安全保护措施。因此对于攻击者而言，他可以轻松地截获数据分组，从中获取 IV 的明文，并且通过比较 AP 或 STA 发送的数据分组，来发现 IV 的重复使用，从而有效地破解数据或对数据进行篡改。

（3）IV 空间过小，造成其很快就可能重复使用。802.11 存在一个隐蔽的结构问题：IV 数据空间只有 24 位。WEP 使用一次性密码本形式的 RC4，如果不改变 WEP 共享密钥，则最多每 2^{24} 个包就会重复这个一次性密码本。在 11 Mbp 流量的 AP 上，这只需 $1500*8*2^{24}/(11*10^6)$ =约 17500s，即 5 小时左右。由于封装的包往往不足 1500B，所需时间可能还会更短。这使得攻击者可以很快搜集到两段被同一密钥流加密的密文，并通过静态攻击解析出消息。而如果 WLAN 中所有的 STA 与 AP 之间都使用同样密钥的话，IV 重用的概率将大大增加。另外，虽然 WEP 标准建议在每个信息包之后更改 IV，但它并不要求必须如此，因此截获使用了相同 IV 的数据分组可能性也近一步加大。

（4）攻击者可以构建一个与密钥相关的解密流(24GB)，用于解密数据。实际上，即便 IV 随机产生，当发送包数量超过 4823 个时，IV 重复使用的概率将会超过 1/2，这使得字典攻击成为可能。由于当前所使用的密钥流决定于 IV 和密钥，虽然不知道密钥，但是使用的是哪一个密钥是传输包中明确指出的，这样由这些信息就可以唯一确定一个密钥流。用这些密钥流建立一个字典所需要的存储空间为：$1500*2^{24}$=24 GB，这对于攻击者而言并不困难。

（5）IV 弱密钥攻击。WEP 采用的 RC4 方案中存在弱密钥。具有弱密钥意味着密钥与加密结果之间存在超过一般密码所应具有的相关性。在 WLAN 中确定用弱密钥加密的数据包很容易，因为 IV 是明文传输的。被攻击者可以利用 IV 的这个弱点展开攻击。在 1600 多万个 IV 值中，有 9000 多个弱 IV。攻击者收集到足够的用弱 IV 加密的数据分组后，可以更快地分析出 WEP 的加密密钥，从而展开攻击。

2、WEP 协议关于数据完整性的漏洞

如上所述，WEP 使用了 40 位的流密码 RC4 算法。RC4 流密码是一种一次将 1 Byte 明文变化为 1 Byte 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而产生。在解密时把相同的密钥流与密文异或即可得到明文。由于流加密具有这样的特点，因此它对消息的完整性要求很高。为了保证数据的完整性，在 WEP 中的数据报文加入了完整性校验域，以保证数据包在传输过程中不会被篡改。完整性校验和采用的是 CRC-32 校验和，并将它作为整个数据报文的一部分，即 CRC-32 校验和也要经过 WEP 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篡改的要求。这是因为 CRC-32 校验本身并不是一种基于密码学的安全认证代码计算方法。CRC-32 校验和作为一种完整性校验方式，主要用于检测数据在传输过程中引起的随机错码。它能够检查出非恶意性质的突发性错误，如由于传输信道噪声而导致的错误。但它在抵抗蓄谋的、恶意的攻击时就显得软弱无力。而且，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，也更加加剧了它自身在防止人为篡改数据上的弱点。

WEP 的 CRC-32 检验和是一种线性检验和，即它有如下的性质：

$$CRC\text{-}32(X \oplus Y) = CRC\text{-}32(X) \oplus CRC\text{-}32(Y) \qquad (2.2)$$ [6]

由式（2.2）可以推导出以下结论：假设 C 为加密后的密文，M 为明文，C' 为篡改后的密文，M'为篡改后的明文，Δ 为攻击者使用的破坏信息，则有：

$$C' = C \oplus (\Delta, CRC\text{-}32(\Delta))$$

$$= RC4(v, k) \oplus (M, CRC\text{-}32(M)) \oplus (\Delta, CRC\text{-}32(\Delta))$$

$$= RC4(v, k) \oplus (M \oplus \Delta, CRC\text{-}32(M) \oplus CRC(\Delta))$$

$$= RC4(v, k) \oplus (M', CRC\text{-}32(M \oplus \Delta))$$

$$= RC4(v, k) \oplus (M', CRC\text{-}32(M'))$$

因此，只要将 $\Delta \| CRC\text{-}32(\Delta)$ 与合法密文 C 进行异或，就可以得到篡改的密文 C'，而在接收端却无法发现数据已经被篡改。因此可以知道，攻击者可以轻易地破坏数据。另外，由上述 RC4 加密算法本身的加密流重用可知，攻击者可以通过已知明文的攻击，来得到加密密钥流和 IV，从而向网络发送虚假报文。该过程原理如下：

$$P \oplus C = P \oplus (P \oplus RC4(v, k)) = RC4(v, k)$$

$$C' = (M', CBC\text{-}32(M')) \oplus RC4(v, k)$$

攻击者利用截获的明文 P 及其密文 C，可得到加密密钥流 RC4(v，k)。利用该密钥流就可以伪造密文 C'。这将导致对共享密钥认证控制措施的欺骗。

3、WEP 协议关于共享密钥认证的不安全因素

如图 2.3 所示，由于被认证者 STA 向认证者 AP 发送的 Challenge 信息是以明文形式传送的，非法用户可以监听到帧 2，进而得到 Challenge 报文的明文信息 P，以及帧 3 中由认证者使用共享密钥加密后返回的密文 C。因此只需计算出 P 的校验值 ICV（P）就可以得到 P ‖ ICV(P)，然后把这个结果与监听到的密文 C 进行简单的异或运算就可以得到加密时使用的密钥流 S，
S=P ‖ ICV(P) ⊕ C=(P ‖ ICV) ⊕ ((P ‖ ICV) ⊕ S)。由于 BSS 中的各个 STA 以及 AP 是共享密钥 K 的，而且 K 在一定的时间内是不变的。因此，攻击者一旦得到某个 IV 对应的密钥流 S，那么他就可以监听数据包的 IV 值。当相同的 IV 出现时，他就能够解密得到对应的明文。以此类推，攻击者可以利用这个漏洞建立起每一个 IV 与其对应密钥流 S 的码表，这样他就能够伪装成合法用户，用相应的加密密钥流正确加密 AP 送出的任意的 Challenge 信息，从而获取 AP 的信任。

另外，从理论上讲，对于一个好的身份认证机制而言，认证首先应该是双向的，即通讯双方建立关联时既要有 AP 对 STA 的认证，同时又要有 STA 对 AP 的认证。前者保证了 STA 的合法性，后者则保证了 AP 的真实性。而在 WEP 共享密钥认证中，AP 对 STA 进行了认证，而 STA 并没有对 AP 进行认证，即其认证是一种单向的认证。其次，身份认证应该基于被认证方的多个特征，如：MAC 地址、SSID、共享密钥、用户口令等等。这样不仅能够增加非法用户攻击的难度，而且能够进一步保护被认证用户。而在原有的认证机制中都是基于用户单一特征的（MAC 地址或者共享密钥）。这降低了攻击者非法认证成功的难度。再者，STA 与 AP 的认证密钥与会话密钥相同，而且在相当长的时间周期内保持不变，攻击者有足够的时间和数据去破解密钥。这也加大了攻击者攻击 WLAN 成功的可能性。

总之，通过上述对 WEP 协议的数据加密原理、数据完整性保护机制及共享密钥认证的分析可以得知，WEP 协议并不能很好地达到其设计时的安全目标，其安全性和完整性都存在严重的不足。

2.4 无线局域网的常见攻击

由于无线通信固有特性和 IEEE 802.11 标准的安全机制的缺陷（WEP 算法的缺陷、SSID 和 MAC 地址过滤接入控制的弱点），严重影响了系统的安全性能，由此引发的无线局域网可能遭受的攻击有以下几类：

1) 拒绝服务(DOS)攻击[3][9]

无线局域网非常容易受到拒绝服务攻击，只要攻击者有足够功率的设备或工具就可以对 2.4GHz 的频段实施泛洪(flooding)，破坏信道特性直至导致无线

网络完全停止工作。另外，无绳电话、微波炉和其它工作在 2.4GHz 频段上的设备都会扰乱网络的正常运行，从而导致合法用户无法使用网络。不过这类攻击的攻击源比较容易确定。

2）被动攻击，对通信信号解密

由于无线通信采用广播的方式，每个用户端都可以监听到所有的无线通信的信号，因此我们在设计网络的安全措施时必须假定攻击者可以窃听到所有的通信信号。如前面对 WEP 机制缺陷分析，由于 IV 只有 24 比特，攻击者在较短的时间内就可以窃听到使用相同密钥流加密的两个数据报，然后对这两个数据报进行异或运算，就可以得到两段明文的异或值。由于 IP 数据报文中含有很多可以预知的冗余信息，攻击者就可以分析出部分明文的内容，通过足够的累积后，就可将完整的明文分析出来。而且如果多个数据报都是由同一密钥流加密，则会大大提高统计学分析方法的成功率。

3）主动攻击

由于 CRC-32 算法的弱点，对数据的篡改十分容易，攻击者只要知道一条加密消息确切明文就可以构造正确的密文，然后把这个数据报发送给 AP 或其它工作站，这样就把非法的业务流注入到网络中从而增加网络的负荷，如果非法业务流的数量很大就会使得网络负荷过重，并出现严重的拥塞问题。

4）对 IP 地址发起的主动攻击

针对 IP 地址的攻击可以不关心消息的具体内容，只要能够破解数据报的头字节—IP 地址。在破解了 IP 地址后，攻击者就可以对其进行修改，使 IP 地址指向已被控制的机器(比如位于 Internet 上的某主机)。由于大多数无线局域网都可以同 Internet 互联，接入点成功地对移动端发来的数据解密后，就会经由一系列的网关和路由器把明文发向受控制的主机。

5）字典攻击

由于初始化向量 IV 字节空间太小，因此建立字典比较简单，只要攻击者获得了部分明文和对应的密文数据报，那么该次所使用的 RC4 密钥流就可以得到，这一密钥流可以将所有使用同一 IV 的数据包解密。采用此方法，经过一段时间的分析和统计，攻击者就可以建立一个 IV 与密钥流的对应的字典。由于 IV 为 24 位，因此这个字典不会很大(约 10G)。该字典一旦建立，攻击者就可以把无线局域网上的所有加密的数据包解密。

6）置信攻击

攻击者可以将其设备伪造成基站，因为无线工作站通常将自己切换到信号最强的网络，如果失败然后才尝试下一个网络。如果攻击者拥有一个很强的发送设备，就可以让无线工作站尝试登录到他的网络，记录下所有的登录信息，

然后分析这些信息获得密钥和口令。这类攻击非常难于被发现，因为无线工作站点通常不报告失败的登录尝试，因为登录尝试失败在正常的环境下也会发生。要想防止这来攻击，只能通过采用有效的认证机制来避免口令和密钥被攻击者破解。

除此之外，无线局域网还很容易受到一些针对系统缺点的攻击，如配置错误、硬件失败等等。

2.5 本章小结

本章对 802.11 标准自身定义的三种安全机制—SSID、MAC 地址过滤控制、WEP 机制的原理和方法进行了详细的分析，指出了它们在设计中的缺陷以及由此引发的各种安全问题。SSID 是一种非常初级的口令控制；MAC 地址过滤控制是基于设备的接入控制机制，不但管理任务复杂，不适合大型网络，而且通过伪造 MAC 地址或者设备的遗失都会造成该机制失效；WEP 机制提供了数据加密和共享密钥接入的功能，但其在设计中的不足也非常明显。WEP 采用了 RC4 对称密钥加密方法，将 1 Byte 明文和密钥流进行模二相加转换成 1 Byte 密文的一种算法。这种方法对数据的完整性和密钥的非重复性要求很高，而 WEP 在这两方面的存在严重的缺陷。另外，802.11 标准也没有规定安全的密钥发布和管理方法。

虽然我们分别讨论了 802.11 安全的各个方面，但它们是互相影响的，单独解决某一点是无济于事的。随着 WLAN 的发展，802.11 是不适合 WLAN 的各种应用的。我们需要一种更健壮的安全方案。

第三章 IEEE802.11i 的增强安全解决方案

从前一章的分析，我们看到了 802.11 的许多安全缺陷及其实质所在，各国研究者都给予了充分的重视。2004 年 6 月 25 号，IEEE802.11 工作组以表决的方式通过了 IEEE802.11i[5][29]，这一章我们将介绍这一标准。

3.1 802.11i 简述

在媒体大量报道 WLAN 入侵事件和互联网出现使用的 WEP 攻击脚本以后，WLAN 设备商推出了一些私有的解决方案。思科开发了增强接入控制的 802.1X/LEAP 认证方案；一些企业采用了基于 AES[12]（Advanced Encryption Standard）算法的加密方案取代脆弱的 WEP 协议；还有一些专家建议企业采用上层的保护手段，例如 IPSec VPN。但私有的解决方案会给产品的互通带来很大的障碍，需要有统一的标准来保证各个厂家产品之间的兼容性。IEEE802 工程组成立了安全任务组来解决 802.11 中的安全问题，推出的新安全标准为 802.11i。802.11i 使 802.11 的 MAC 层安全增强，其中提出的最终安全解决方案叫做“强健安全网络”（RSN[14]，Robust Security Network）。

RSN 是一个具有以下安全特性的 BSS/ESS：

- 基于 802.1X 的、对于 AP 和 STA 的双向增强认证机制；
- 具有密钥管理算法；
- 动态的会话密钥；
- 加强的加密算法 AES 或 TKIP，其中必须实现基于 AES 的 CCMP ；
- 支持快速漫游和预认证；
- 支持 IBSS。

3.2 数据保密协议

前面我们已经分析了 802.11 中的 WEP 协议存在的安全漏洞，802.11i 为了兼容性考虑保留了 WEP 协议，同时为了增强链路层数据保护，新增两种数据保密协议—TKIP[18]和 CCMP[12]。TKIP 对 WEP 进行了外围重封装，经过软件升级实现。CCMP 是 RSN 的长期解决方案，它采用新的加密算法 AES，需要硬件升级才可以支持。对于兼容 RSN 的设备而言，CCMP 是强制实现的，而 TKIP 是可选的。

3.2.1 TKIP（Temporal key Integrity Protocol）安全性分析

TKIP 协议设计的出发点在于基于现有的硬件环境，通过软件升级消除 WEP 脆弱性，达到可以接受的安全程度。因此 TKIP 采取了对 WEP 协议进行外封装的方式，这样可以继续使用旧的 RC4 加密芯片设备。TKIP 添加了四个算法到 WEP：密码学上的消息完整码(MIC)来防止数据被篡改；新的 IV 序列规则来防止重放攻击；新的 per-packet Key 生成算法以防止弱密钥的出现；一个 Rekeying 机制，以生成新鲜的加密和完整性密钥，防止 IV 重用。

- TKIP 的加密过程如下，参见图 3.1。

a) TKIP 根据 MSDU(MAC 服务数据单元)的源地址(SA)、目标地址(DA)、优先级和数据计算 MIC，把 MIC 添加到 MSDU 后面；

b) TKIP 根据需要把 MSDU 分段为一个或多个 MPDU(MAC 协议数据单元)，并给每个 MPDU 一个单调增加的 TSC（TKIP Sequence Counter)；

c) 对于每个 MPDU，TKIP 计算出 WEP seed，也就是 Per-Packet Key (RC4Key)；

d) TKIP 把 WEP seed 分解成 WEP IV 和 RC4 Base Key 的形式，把他们和 MPDU 一起送入 WEP 加密器进行加密，并将所用 Temporal Key(TK)对应的 Key ID 编入 WEP IV 域中。

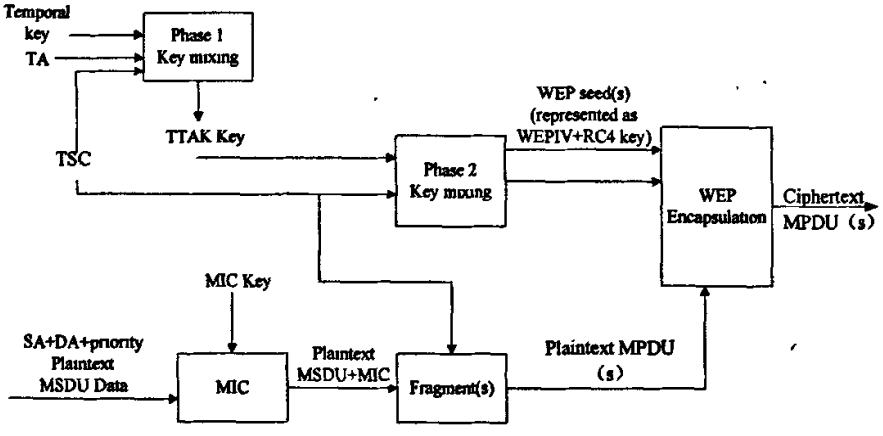

图 3.1　TKIP 加密方块图

TKIP 使用 RC4 加密 MIC，减少了将 MIC 的信息泄漏给攻击者的危险。同时 MPDU 使用 ICV 和 802.11 的 FCS（帧校验序列）来检测随机位错误，那么 ICV 和 FCS 正确而 MSDU 的 MIC 错误就意味着几乎肯定是遭到了包篡改攻击。而且，MIC 保护 SA 和 DA 不被改变，这样，数据包就不能被发送到非法目的地址或源地址进行欺诈。

- TKIP 的解密过程如下，参见图 3.2。

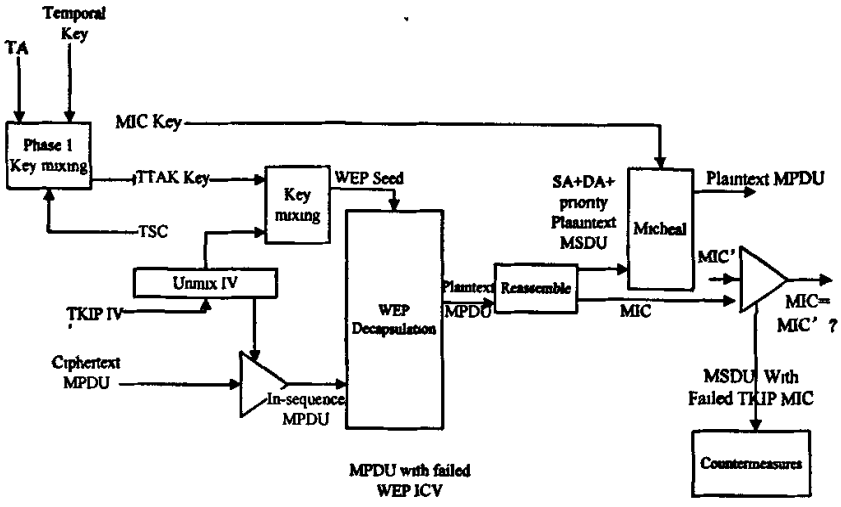

图 3.2　TKIP 解密方块图

a）在 WEP 解封一个收到的 MPDU 前，TKIP 从 WEP IV 域中得到 TSC 和 Key ID，如果 TSC 超出了重放窗口，则该 MPDU 被丢弃。否则，根据 Key ID 定位 Temporal Key(TK)，计算出 WEP seed，也就是 Per-Packet Key(RC4Key)；

b）TKIP 把 WEP seed 分解成 WEP IV 和 RC4 Base Key 的形式，把他们和 MPDU 一起送入 WEP 解密器进行解密；

c）如果 WEP ICV 检查正确，该 MPDU 被组装入 MSDU。如果 MSDU 重组完毕，则检查 MIC；

d）如果 MIC 检查正确，TKIP 把 MSDU 送交上一层，否则，MSDU 被丢弃，并触发重放攻击对策。

TKIP 包裹在 WEP 外面，主要用来改进 WEP 的安全性，但它并不是一个理想的安全协议设计。MIC 的安全性能很弱，必须采用一定的对策才能保证安全。TKIP 复杂的 Per-Packet Key 生成方法是为了适应 WEP 使用的 RC4 算法。虽然扩展了 IV 的长度，将 IV 冲突的几率减少到几乎没有，但 Rekey 机制从理论上还是要认真考虑。

3.2.2 CCMP（Count Mode/CBC-MAC Protocol）安全性分析

由于在 802.11 的环境下，作为流密码的 RC4 算法并不适应，因此应当采用分组密码算法。而 AES 不论是反馈还是非反馈模式，都非常适合于各种计算环境下的软硬件实现。AES 具有如下优点：优秀的密钥扩展方案；灵活的密钥生成算法；分组和密钥被设计成可以在三种长度中自由选择的形式；执行的轮数是变化的，并且内部结构的设计使其在指令级上可以并行执行。所以在 802.11i 标准中，已将 AES 作为数据保密的算法。

CCMP 就是基于 AES 的 CCM 模式。即使用计数器模式（CTR 模式）实现数据保密，使用 Cipher Block Chaining Message Authentication Code (CBC-MAC) 模式实现数据认证。CCMP 使用同一个密钥进行 CTR 模式加密和 CBC-MAC 计算。通常在一个以上的函数中使用同一密钥会导致安全缺陷，但 RSA Labs 的 Jakob Jonsson 已经证明在 CCMP 这种特殊情况下不会出现安全缺陷。因为 CTR 模式和 CBC-MAC 模式分别构造出不同的 IV，消除了该安全缺陷。

CCMP 是操作在 MPDU 上的，它使用了 48 位的 Packet Number (PN)。PN 被用来构建 CTR 模式的 Counter 和 CBC-MAC 的 IV ，同时也是为了减少 Rekey，从而简化密钥管理。CCMP 的加密过程，参见图 3.3。

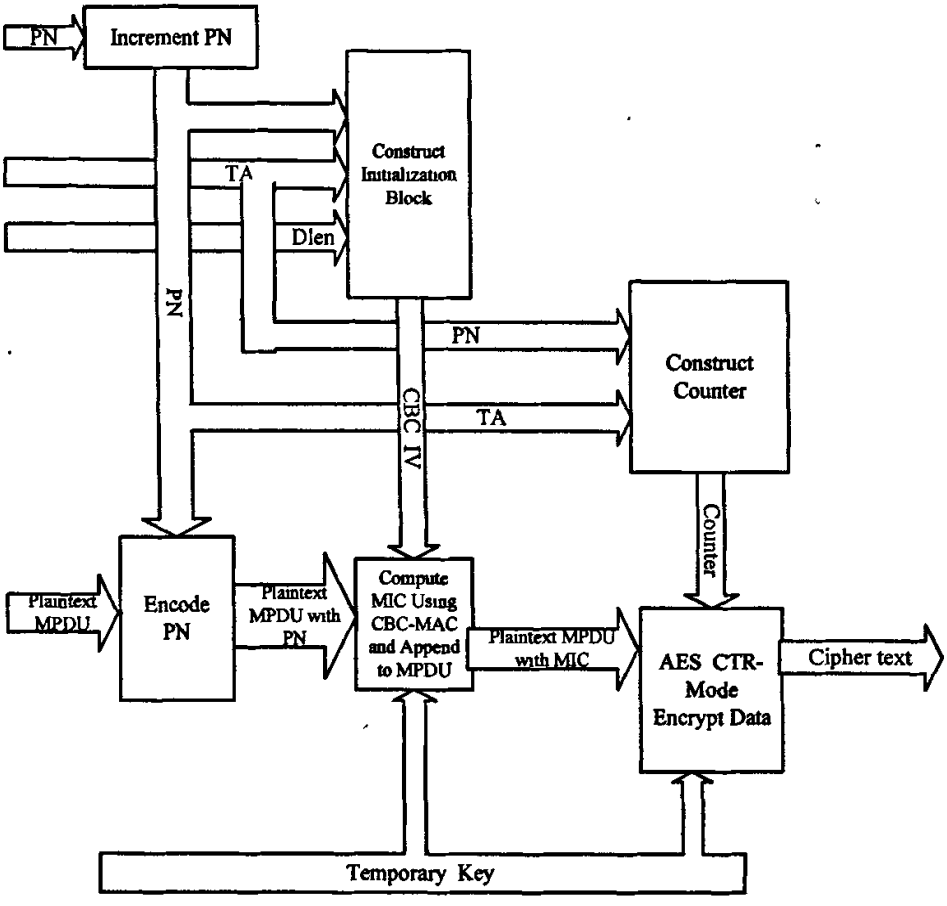

图 3.3　CCMP 加密方块图

a) 增加 PN，保证对每个 MPDU 有一个新鲜的 PN，把 PN 编入 MPDU；

b) 利用 MPDU 的 TA(发送地址)、MPDU 数据长度(Dlen)和 PN 构造 CCM-MAC 的 IV ；

c) 使用该 IV，CCMP 在 CCM-MAC 下使用 AES 计算出 MIC，将 MIC 截为 64 位，添加在 MPDU 数据后面；

d) 利用 PN 和 MPDU TA 构造 CTR 模式的 Counter；

e) 使用该 Counter，CCMP 在 CTR 模式下使用 AES 加密 MPDU 数据和 MIC。

CCMP 的解密过程如下图 3.4 所示。

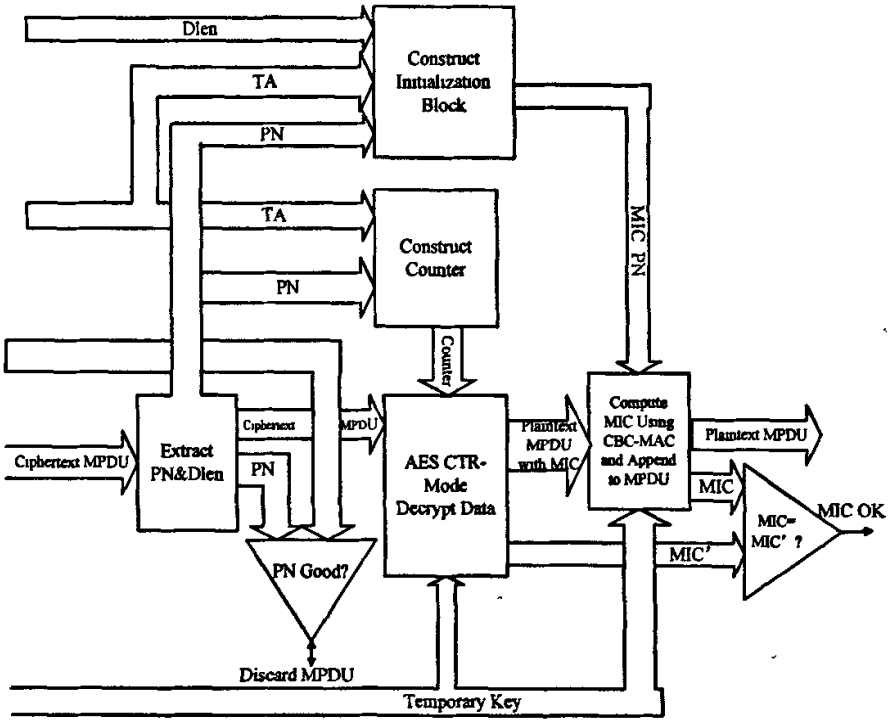

图 3.4　CCMP 解密验证方块图

a）从接收包中解出 PN 和 Dlen，Dlen 至少有 16 个字节用以包括 MIC 和 PN；

b）进行重放检测，如果 PN 在重放窗口之外，丢弃该 MPDU；

c）利用 PN 和 MPDU 的 TA 构造 CTR 模式的 Counter；

d）利用该 Counter，进行 CTR 模式解密，操作同加密一样；

e）利用 MPDU 的 TA，MPDU 数据长度(Dlen)和 PN 构造 CCM-MAC 的 IV，Dlen 要减去 16，以排除 MIC 和 SN；

f）使用该 IV，CCMP 在 CCM-MAC 下使用 AES 重新计算出解密过 MPDU 的 MIC'，比较 MIC'和收到的 MIC，如不匹配，丢弃该 MPDU。

CCMP 同样要和密钥管理结合，才能成为一个安全的协议。MIC 保护了源和目的地址、QoS、Replay Counter 免受篡改或伪造攻击；包序列号检查防止了重放攻击；CCMP 保证了在同一密钥下不会重用 Counter 或 IV；最后，CCMP 对下一层的分组密码原语减少为 1，实现效率很高。

3.3 认证和接入控制

IEEE 802.11i 中的认证、授权与接入控制主要是由三个部分配合完成的，分别是 IEEE 802.1 X 标准、EAP 协议和 RADIUS 协议。

3.3.1 IEEE802.1X 协议

IEEE 802.1X[30]协议，称为基于端口的访问控制协议。主要目的是为了解决无线局域网用户的接入认证问题。IEEE 802.1X 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 802.1X 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 IEEE 802.1X 客户端软件，无需要另外安装客户端软件。

3.3.1.1 802.1X 的体系结构

IEEE 802.1X 协议的体系结构包括三个重要的部分：客户端(Supplicant System)、认证系统(Authenticator System)、认证服务器（Authentication Server System)。802.1X 体系结构如图 3.5 所示。

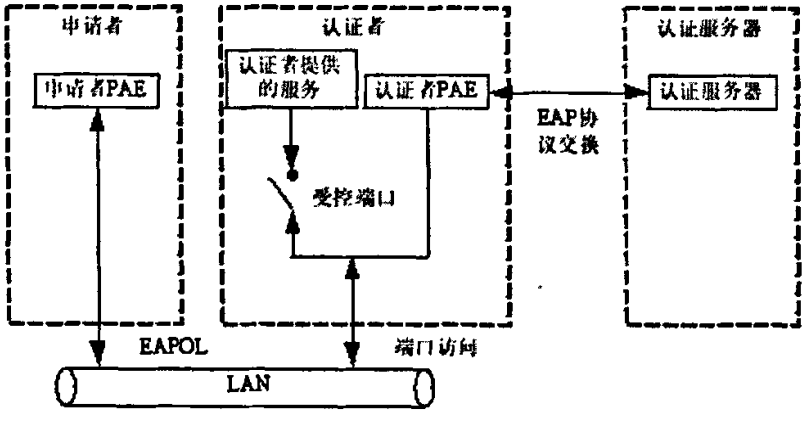

图 3.5　802.1X 体系结构

客户端系统，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，当用户有上网需求时，通过启动这个客户端软件发起 IEEE 802.1X 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(Remote Authentication Dial-In Service，RADIUS)的服务器。该服务器可以存储有关用户的信息，通过检验客户端发送来的信息来判别用户是否有权使用网络系统提供的网络服务。

其中 PAE（Port Access Entity）为端口接入实体，用来执行与认证机制相关的算法和协议。

3.3.1.2 端口控制原理

认证者对于不同用户的端口(可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等)有两个逻辑端口：控制端口(controlled port)和非控制端口(uncontrolled port)。如下图 3.6 所示，非控制端口始终处于双向连通的状态，不管是否处于授权状态都允许申请者和局域网中的其他机器进行数据交换。主要用来传递 EAPOL 协议帧，可保证随时接受客户端发出的认证 EAPOL 报文；控制端口只有在认证通过的状态下才打开，用于传递网络资源和服务。控制端口可配置为双向受控和仅输入受控两种方式，以适应不同的应用环境。

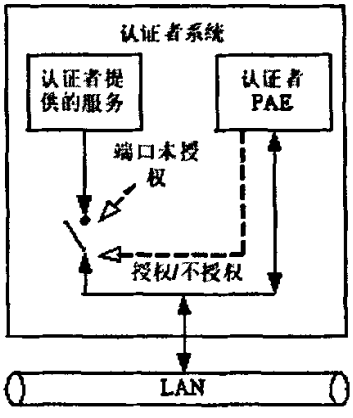

图 3.6　受控和非受控端口

逻辑端口有三种控制状态，端口的控制状态决定了客户端是否能接入网络：

1) Force Authorized：强开，端口一直维持授权状态；

2) Force Unauthorized：强关，端口一直维持未授权状态；

3) Auto：激活 802.1X，初始设置端口为未授权状态，并通知设备管理模块需要进行端口认证。这也是缺省值，后面的讨论都默认是该状态。

当客户机尝试连接至 AP 时，控制端口被强制进入非授权状态，在该状态下，除了 802.1X 报文外不允许任何业务输入、输出。当客户通过认证后，端口状态切换到授权状态，允许客户端通过端口进行正常通信。可以进行如 DHCP、HTTP、FTP、SMTP、POP3 等协议数据的传输。

3.3.1.3 802.1X 认证过程

进行 802.1X 认证前，客户端和认证者（接入点）之间先要建立物理层连接，完成 MAC 层开放认证和关联，并进行安全参数的协商，如下图 3.7 所示。

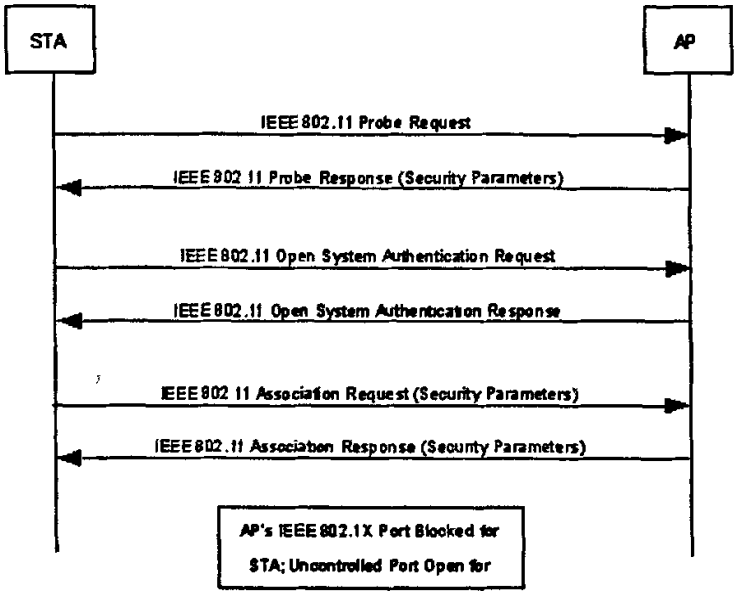

图 3.7　802.1X 认证前接入过程

在 MAC 层关联完成后，才开始进行 802.1X 认证。一个完整的 802.1X 的认证过程如图 3.8 所示。

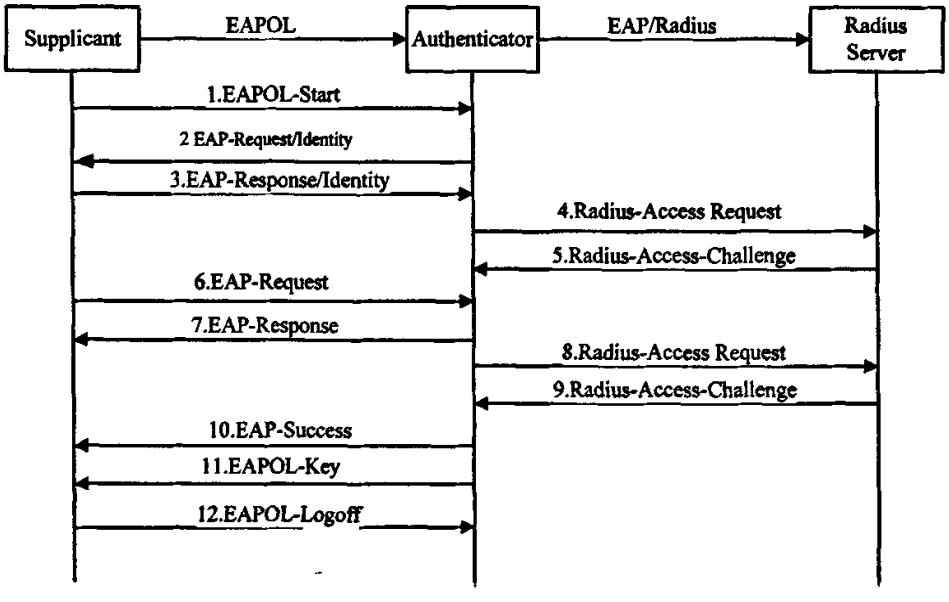

图 3.8　802.1X 认证过程

（1）客户端发起认证过程（如果客户端连续发送多次都没有收到来自认证方的

EAP-Request/Identity 消息，就可以认为认证通过，这是因为可能认证方并不支持 802.1X）。认证过程同样可以由认证方发起，但是它直接发送 EAP-Request/Identity 而不是 EAPOL-Start 消息；

（2）当认证方不知道用户身份时就发送该消息。如果知道，第 2 步和第 3 步也可省略，以加速认证过程；

（3）客户端收到 EAP-Request/Identity 消息，就用其用户名响应，发送 EAP-Response/Identity 消息给认证方；

（4）认证方把包含有用户身份的 EAP 响应包重新以 RADIUS 协议格式封装，并把重新封装后的包由 RADIUS 客户端发送至 RADIUS 服务器；

（5）RADIUS 服务器在收到该包后将选择具体的认证机制，并发送相应的 EAP 请求包到认证方；

（6）认证方并不解释来自 RADIUS 的 EAP 包的具体内容，而只是检查 RADIUS 协议包的类型，由于是质询包，因此认证方将其毫不改变的转发给客户端；

（7）客户端收到上述请求包后，如果支持 RADIUS 服务器选择的认证机制，就根据认证机制的要求作出响应，并通过 EAP 封装后发送给认证方；如果不支持 RADIUS 服务器选择的认证机制，则发送 NAK 包，这样 RADIUS 服务器将重新选择认证机制，并从第 5 步重新开始；

（8）认证方把来自客户端的 EAP 响应包中继到 RADIUS 服务器；

（9）如果 RADIUS 认证服务器通过了对客户端的认证，则向认证方发送 RADIUS-Access-Accept 消息；否则就向其发送 RADIUS-Access-Reject 消息；

（10）如果认证方收到 RADIUS-Access-Accept 消息，则认为认证成功，于是打开受控端口，并向客户端发送 EAP-Success 消息，此后客户端就可以进行授权的正常通信过程；如果认证方收到 RADIUS-Access-Reject 消息，则认为认证失败，于是关闭受控端口，并向客户端发送 EAP-Failure 消息；

（11）当客户端通过认证之后，无线接入点 AP 将向客户端发送用来加密广播帧的广播密钥 EAPOL-Key。广播密钥的发送保证了客户端用于单播时会话密钥的保密性。而会话密钥的派生与发送与认证服务器选择的具体的认证机制有关；

（12）当客户端离线时，向认证方发送离线通知 EAPOL-Logoff，认证方收到消息后重新关闭受控端口。

至此，802.1X 就完成了一次认证过程。

3.3.2 EAP 协议

可扩展认证协议 EAP[24]是 PPP（Point-to-Point Protocol)认证中的一个通用协议。EAP 在链路控制阶段(Link Control Protocol， LCP)没有选定一种认证机

制，而把这一步推迟到认证阶段。顾名思义，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实现的继续使用。

3.3.2.1 EAP 认证过程

EAP 认证过程如图 3.9 所示。

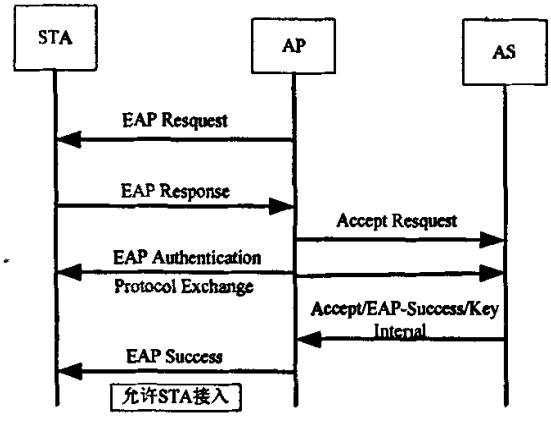

图 3.9　EAP 认证过程简图

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。响应包中的类型域与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。

3.3.2.2 基于 WLAN 的 EAP 的数据封装格式

802.1X 的核心是可扩展认证协议 EAP，EAP 信息被包含在 802.1X 信息中，称作 EAPOL。

（1）EAPOL 消息的封装

- EAPOL 数据包的格式

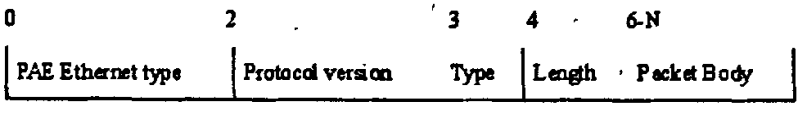

图 3.10　EAPOL 数据包格式

EAPOL 数据包格式如上图 3.10 所示。其中，PAE 以太类型（PAE Ehernet Type）字段占用两个字节，用于存放 PAE 所使用的类型值。目前，802.1X 规定它为 0X888E；协议版本（Protocol Vertion）字段占用一个字节，用于存放 EAPOL 协议的版本信息。目前，版本号为 0000 0001；数据包类型（Packet Type）字段占用一个字节，用于存放所传输数据包的类型，它共定义了下面几种类型：

EAP-Packet，用 00H 表示，认证信息帧，用于承载认真信息；

EAPOL-Start，用 01H 表示，认证发起帧；

EAPOL-Logoff，用 02H 表示，退出请求帧；

EAPOL-Key，用 03H 表示，密钥信息帧；

EAPOL-Encapsulated-ASF-Alert，用 04H 表示。该数据包类型由报警标准提出，用作通过非授权端口发送报警信号的一种方式。

数据长度（Length）字段由两个字节构成，用来定义数据帧的长度，也就是 EAP 包的长度；Packet Body：根据不同的类型有不同的格式。

- EAP 数据包的格式

当 EAPOL 数据包 Type 域为 EAP-Packet 时，Packet Body 为 EAP 数据包结构。其帧结构如图 3.11 所示。

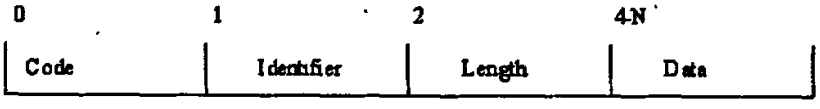

图 3.11　EAP 数据帧格式

其中，码字（Code）字段占用一字节的数据长度，用来指明 EAP 消息的类型，它有请求、应答、成功和失败四种类型，类型号分别为 1、2、3 和 4。标识符（Identifier）字段占用一字节的数据长度，用来提供与请求相匹配的应答。标识符和系统端口号一起标识一组认证交换，也正是由于标识符字段的使用限制了每一个系统端口最多只能同时接入 256 组认证。长度（Length）字段由 2 字节数据长度构成，用来指示 EAP 数据帧的长度。数据（Data）字段的长度不定，其格式由码字字段确定。

（2）EAPOL-Key 消息的封装

当 EAPOL 数据包 Type 域为 EAPOL-Key 时，Packet Body 为 EAPOL-Key 数据包结构，即下面介绍的密钥描述符，主要用于密钥管理的四步握手协议及组密钥更新。

密钥描述符格式如表 3.1 所示。

Descriptor Type 1 octet	
Key Information 2 octet	Key Length 2 octet
Replay Counter 8 octet	Key Nonce 32 octet
EAPOL-KeyIV 16 octet	Key RSC 8 octet
Key ID 8 octet	Key MIC 16 octet
Key Data Length 2 octet	Key Data N octet

表 3.1　密钥描述符格式

Descriptor Type：一个字节，指明密钥的类型，对于 RSN，值为 254（十进制）。

Key Information：2 个字节。具体说明如下：0-2 位表示密钥描述版本号：值为 1，表示 EAPOL-Key MIC 采用 HMAC-MD5 进行计算，组密钥采用 RC4 来加密；值为 2，表示 EAPOL-Key MIC 采用 HAMC-MD5 进行计算，采用 AES-CBC 加密。第 3 位是密钥类型标志位。1 表示对等密钥；0 表示组密钥。第 4、5 位包含了用于生成临时密钥的初始密钥。第 6 位为密钥的 Tx/Rx 标志位。第 7 位为 Ack 标志位，如果认证者发出的消息需要回应，则置位。第 8 位为 MIC 标志位。第 9 位为 Secure 位，如果初始的密钥交换已经完成，置位。第 10 位 Error 标志位，如果申请者对数据的整体性校验出错，置位。第 11 位 Request 标志位，在申请者向认证者发送请求四步握手开始的消息中置位。第 12-15 位保留。

Key Length：2 个字节，表示加密/整体性校验机制所使用的密钥长度。

Replay Counter：8 个字节，使用无符号二进制数表示。申请者端，回应认证者的 EAPOL-Key 消息时，使用收到的认证者端发送包中的计数器；认证者端，则以此来判断是否是发送者端的重发包。

Key Nonce：32 个字节，内容为 ANonce(认证者)或者 SNonce(申请者)，如果无需 Nonce 其值为零。

Key IV：16 个字节，包含了用于产生加密组密钥的 IV。如果无需 IV 置为零。

Key RSC：8 个字节，表示接收序列计数器，用于四步握手的第三条消息及组密钥更新的第一条消息。其他消息中，置零。

Key ID：目前保留，置零。

Key MIC：16 个字节，对 EAPOL 包计算 MIC。

Key Data Length：表示密钥数据长度。对于组密钥，其值和 Key Length 相同；对于对等密钥，第二、三条消息数据为 RSN 的 IE（信息元素，包含了认证和单播、多播密码套件的选择以及是否支持单播密钥等信息），数据长度即为 IE 的长度。对第一、四条消息数据域为空，长度即为零。

Key Data：对于对等密钥，这个域在四步握手的第二、三条消息中包含了 RSN

的 IE，第一、四条消息则为空。

3.3.3 RADIUS 协议

在 IEEE 802.1X 协议体系中，当认证服务器得到认证客户端的身份信息后，便采用 RADIUS[19]认证技术对认证客户端的身份进行识别。因此，RADIUS 认证技术也是 802.1X 标准的关键技术之一。

3.3.3.1 RADIUS 协议概述

远程拨入用户认证服务 RADIUS (Remote Authentication Dial-In User Service)是一个提供标准验证服务的 AAA 协议。AAA 是验证、授权和记账(Authentication，Authorization， Accounting)协议的简称。RADIUS 通过建立一个唯一的用户数据库来存储用户名、用户密码等信息来识别用户，并通过存储传递给用户的服务类型以及相应的配置信息来完成对用户的授权。

RADIUS 协议主要分为两部分，一是认证，另一个是计费。它将接入服务器（NAS ）作为客户端，将运行 RADIUS 服务软件的机器称为服务器端。服务器上存放客户的资料，因此无论用户从哪台服务器连接都可以正常的认证计费。RADIUS 支持代理((proxy)功能，即一方面 RADIUS 可以转发由 NAS 发来的 RADIUS 的请求报文，另一方面可以转发其它 RADIUS 的回应报文给 NAS。其通讯过程如下图 3.12 所示。

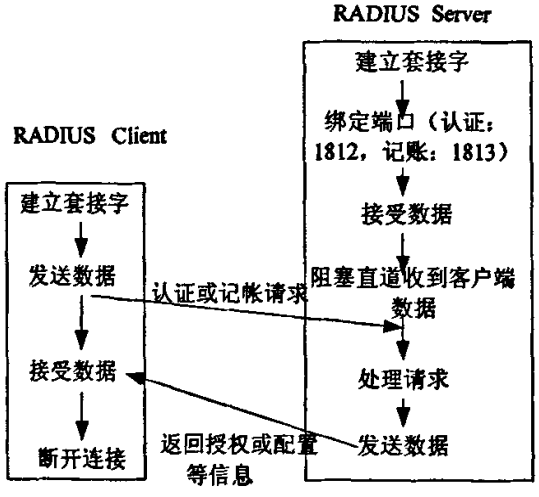

图 3.12　RADIUS 协议通讯过程

3.3.3.2 RADIUS 报文结构

RADIUS 协议是 TCP/IP 应用层的协议，在传输层它被封装到 UDP 协议的报文中，其报文格式如下图 3.13 所示。

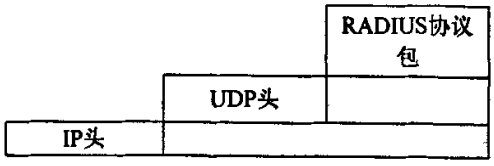

图 3.13　RADIUS 报文格式

其中 UDP 协议的目标端口可以为 1812、1813。其中 1812 为认证端口，1813 为计费端口。

RADIUS 数据报文的格式如下图 3.14 所示。

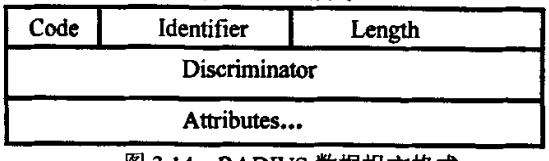

图 3.14　RADIUS 数据报文格式

编码(Code)：编码域占一个字节，该值决定了 RADIUS 数据包的类型。在接收到一个无效编码域的协议包后，RADIUS 服务器会直接丢弃该数据包。

标识符(Identifier)：标识符域占一个字节，用于辅助鉴别请求包与响应包。如果在一个很短的时间片内，不同请求有相同的源 IP 地址、源 UDP 端口号和标识符，则 RADIUS 服务器会认为这是上一个请求的重复。

长度(Length)：长度域占两个字节，它指包括编码、标识符、长度、鉴别码和属性域在内的数据包的总长度。如果数据包的长度比这个长度要短，则此数据包会被直接丢弃。数据包最小的长度是 20 个字节，最大的长度是 4096 个字节。

鉴别码(Discriminator)：鉴别码域占十六个字节，其中最重要的字节最先被传输。这个值是用来鉴别 RADIUS 通信的数据源和隐藏用户密码。根据所在数据包的不同，可将它分为请求鉴别码和响应鉴别码两大类。

属性(Attributes)：RADIUS 属性在请求和响应协议包中携带详细的认证、授权、信息和配置细节。所有的属性在数据包中均以变长的类型、长度和值域这样的三元组的形式出现。

3.3.3.3 RADIUS 的工作流程

RADIUS 工作流程具体如下图 3.15 所示。

步骤 1：用户通过拨号或其它方式向网络接入服务器(NAS)发出连接请求，并把相应的用户名、密码等信息传送给 NAS（1）；

步骤 2：NAS 生成请求接入(Access-Request)包，并发送到 RADIUS 服务器（2）；

步骤 3：RADIUS 服务器对该用户进行认证（3）；

步骤 4：若认证成功，RADIUS 服务器向 NAS 发送允许接入包（4），否则，RADIUS 服务器向 NAS 发送拒绝接入包(4')；

步骤 5：若 NAS 接收到允许接入包，则为用户建立连接，并对用户进行授权和提供服务（5），并转步骤 6；否则，若收到拒绝接入包，则拒绝用户的连接请求(有时回送拒绝信息)，结束认证过程；

步骤 6：NAS 发送请求记帐包给 RADIUS 服务器（6）；

步骤 7：RADIUS 服务器接收到该请求记帐包后开始记帐（7），并向 NAS 回送记帐响应包（8）；

步骤 8：如果用户断开与 NAS 的连接（9），NAS 就会向 RADIUS 服务器发送“停止记帐”包（10）；

步骤 9：RADIUS 服务器收到停止记帐的请求后停止记帐(11)，并向 NAS 发送停止记帐响应（12）。

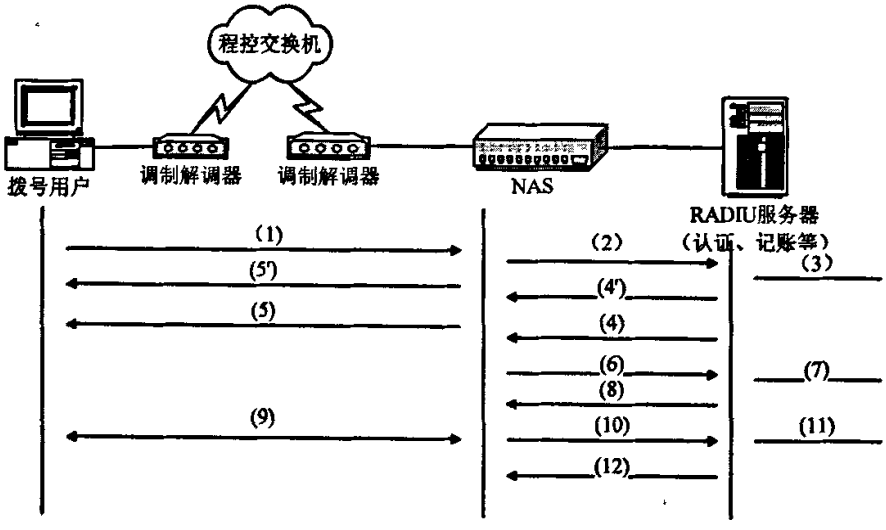

图 3.15　RADIUS 工作流程图

在 RADIUS 的典型应用中，用户以一定的方式，如通过登录程序或 PPP 协议等把认证信息发送到客户端。客户端一旦收到用户端的认证信息，就会产生包含像用户名、密码、客户端标识符等属性的请求接入包，发送到 RADIUS 服务器端。如果客户端在一定的时间间隔内没有收到服务器端的响应，客户端会重新发送该数据包或在重发失败了若干次后把该数据包发送到指定的备用服务

器上。服务器端在收到来自客户端的请求接入包后，根据用户名查找相应的配置文件或数据库以验证用户的密码等信息，判断是否认证通过。

3.3.3.4 RADIUS 系统特征

（1）客户端/服务器模型

由一个网络接入服务器作为 RADIUS 的客户端。客户端负责将用户的信息传给指定的 RADIUS 服务器，然后根据 RADIUS 服务器返回的信息进行后续的操作。RADIUS 服务器负责接收用户连接请求，对用户进行认证，然后向客户端返回必要的配置信息来为用户提供服务。RADIUS 服务器也可以作为其它的 RADIUS 服务器或其它种类认证服务器的代理客户端。

（2）网络安全

在客户端和 RADIUS 服务器之间的数据传输通过共享密钥进行加密，这个密钥不会在网络上传输。另外，在用户端和 RADIUS 服务器之间传输的用户密码也经过了加密，从而避免有人在不安全的网络上进行探听以获得用户的密码。

（3）灵活的认证机制

RADIUS 服务器可以支持各种方法来对用户进行认证。当它得到了用户的用户名和初始密码以后，它可以支持 PAP，CHAP，MSCHAP，EAP 以及其它的认证机制。

（4）可扩展的协议

在 RADIUS 系统中，所有的处理都由可变长度的“属性-长度-值”三元组实现。因此可以加入新的属性来对协议进行扩展，却不会对已有的应用产生任何的影响。

（5）对证书的支持

在 RADIUS 中可以通过 EAP 协议来提供对证书的支持。从信息安全的角度来看，基于公共密钥基础设施 PKI 的安全认证体系是未来信息安全的发展方向。借助 EAP 协议，RADIUS 能够提供对证书的支持从而实现和 PKI 的结合，最终为系统提供安全灵活的安全结构。

3.4 密钥管理

缺乏自动有效的密钥管理是 802.11 的一大安全缺陷，人工配置密钥的方法烦琐而低效，并且以口令作为密钥还容易受到字典攻击。因此密钥发放和更新机制的设计也是 802.11i 的一个重点。802.11i 设计的密钥管理协议包括四步握手和组密钥更新等。

WLAN 网络中，单播密钥是在某个 STA 和 AP 对之间使用的，因此在 802.11i 中叫成对临时密钥(PTK[9])。多播密钥是在同一个 AP 覆盖的小区内使用的，在 802.11i 中叫作组临时密钥(GTK)。PTK 是由 802.1X/EAP 认证过程得到的成对主密钥（PMK）推导得到的，而组密钥也是在 AP 上产生以后，由 PMK 推导的密钥保护分发的。因此，PMK 是处于密钥层次最高级的母钥。

3.4.1 四步握手密钥协商机制

四步握手[1][9]的目的在于由 STA 和 AP 共享的 PMK 推导单播通信密钥 PTK。四步握手以 PMK 为信任基础，双方分别提供了随机数，可以保证握手报文的现场性以及协商所得会话密钥的新鲜性。握手报文带有验证码 MIC，可防攻击者篡改。四步握手中的组密钥分发报文带有序列号，可防攻击者重放旧的组密钥。四步握手中还考虑了对无线链路连接探寻阶段协商的密码算法进行有保护的确认，防止算法降级攻击(bidding down attack)。总体而言，四步握手具有较好的安全性和较高的效率。

3.4.1.1 密钥初始化

如果 IEEE 802.1X 认证成功，AP 向客户端转发 EAP-Success ，AP 然后初始化两种密钥交换：四步握手和组密钥更新。密钥初始化如图 3.16 所示。

图中的 EAPOL-Key (S，M，A，T，N，K，KeyRSC，ANonce/SNonce，GNonce，MIC，GTK)中的各个参数的含义如下：

S 对应 EAPOL-Key 消息的 Key Information 的 Secure 位；

M 对应 EAPOL-Key 消息的 Information 的 MIC 位；

A 对应 EAPOL-Key 消息的 Information 的 Ack 位；

T 对应 EAPOL-Key 消息的 Information 的 Tx/Rx 标志位；

N 对应 EAPOL-Key 消息的 Information 的 Key index 位；

K 对应 EAPOL-Key 消息的 Information 的 Key Type 位；

KeyRSC 对应 EAPOL-Key 消息的 Key RSC 域；

ANonce/Snonce 对应 EAPOL-Key 消息的 Key Nonce 域；

GNonce 对应组密钥的 Nonce；

MIC 对应 EAPOL-Key 消息的 MIC 域；

GTK 对应 EAPOL-Key 消息的 Key Data 域。

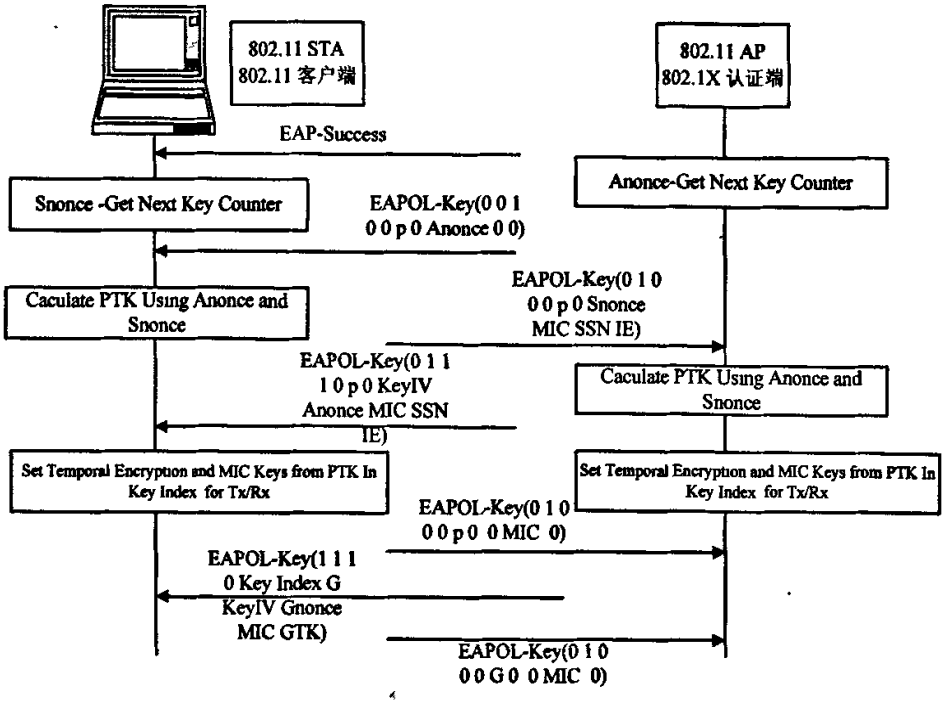

图 3.16　密钥初始化

3.4.1.2 四步握手过程

四步握手过程流程如下：

（1）认证者发送 EAPOL-Key 消息，其中包含 ANonce；

（2）申请者由收到的 ANonce 和本身的 SNonce 产生 PTK；

（3）申请者发送 EAPOL-Key 消息，包含 SNonce 和 MIC；

（4）认证者由 ANonce 和收到的 SNonce 产生 PTK，并且对 MIC 做校验；

（5）认证者发送 EAPOL-Key 消息，其中包含 ANonce、MIC 及是否安装加密/整体性密钥；

（6）申请者发送 EAPOL-Key 消息，确认密钥已经安装。

3.4.2 组密钥更新

组密钥更新[31]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；

（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；

（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。

3.5 完整接入流程

完整的 802.11i 接入流程包括探寻、开放系统认证、关联、802.1X/EAP 认证、四步握手等几个阶段。探寻、开放系统认证和关联是为了建立 STA 和 AP 之间的二层连接，真正的身份认证是二层连接建立后的 802.1X 过程。四步握手完成单播和组播密钥的分发。四步握手完成以后 AP 上的 802.1X 受控端口才真正打开，允许用户数据通过。在保密通信过程中，通过四步握手和组密钥更新来更新密钥。802.11i 中保留了 802.11 的开放系统认证是出于兼容性考虑。完整接入流程如图 3.17 所示。

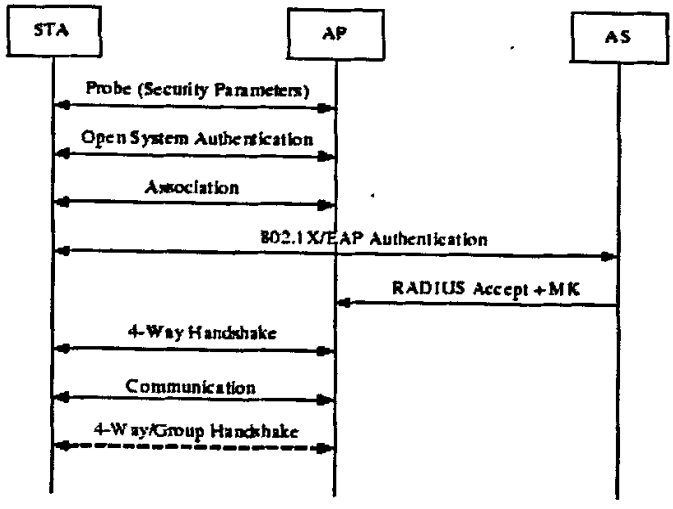

图 3.17　802.11i 完整接入流程

3.6 其他安全机制

802.11i 中还定义了其他一些安全机制，包括预共享密钥认证机制(采用四步握手)，加速切换时认证速度的预认证机制和 PMK 缓冲机制，保护 STA 之间直接通信的 STA 密钥握手协议，还有 IBSS 环境中的安全机制等。

3.7 本章小结

IEEE 802.11i 是针对 IEEE 802.11 中的安全漏洞进行修补的 MAC 层安全增

强标准。它提出了强健安全网络的概念，并考虑了对遗留设备最大限度的向下兼容。

在数据保护方面，IEEE 802.11i 设计了两种新的保密方法 TKIP 和 CCMP 。TKIP 是在 WEP 的基础上重新封装得到的一个保密协议。对于大部分的 WLAN 产品，只需经过固件或者软件的升级就可以实现。CCMP 保密协议是 RSN 的默认保密协议，具有更高的安全性，但由于采用新的 AES 算法而需要硬件上的更新支持。

针对 802.11 缺乏自动有效的密钥管理的缺陷，802.11i 设计了密钥协商的四步握手和组播密钥更新协议。四步握手可以用于单播和组播密钥协商，以及单播密钥更新；组播密钥更新协议专门用于组播密钥更新。有了这两个协议，WLAN 可以支持动态的密钥更新。

802.11i 利用 802.1X 和 EAP 进行认证，但是 802.11i 没有规定 EAP 上承载的认证协议，只是要求双向认证。因为无线环境中移动设备具有比较少的资源，如何使认证协议既安全又需要比较少的资源是很重要的，同时又应该具有良好的扩展性。我们在下一章分析 WLAN 目前的几个认证协议。

第四章 无线网络认证协议的分析和比较

认证协议[25][26]为开放网络中两个或多个通信参与者提供一个共享的会话密钥，该密钥用于保护后续的通信。本章将重点讨论 WLAN 的一系列认证协议。

4.1 无线网络认证需要满足的条件

一个好的适用于无线局域网的认证方法需要具备那些特性呢？这一节就认证方法必须具有的特性、应当具有的特性和可能具有的特性这三个方面分别给出这个问题的答案。

4.1.1 必须具备的特性

（1）相互认证。认证方法必须提供相互认证，即不仅认证服务器要认证用户，而且用户也要对认证服务器进行认证。在无线网络环境下，相互认证非常重要，否则攻击者将很容易建立一个欺诈的无线接入点 AP，从而对用户进行两类攻击。一类是欺诈的 AP 并未连接到目标网络，它通过欺骗用户达到获取用户认证密码的目的；另一类是欺诈 AP 已经连接到目标网络，它可能不考虑用户的密码而“授权”用户让其使用网络，从而插入用户和网络的数据传输路径，达到记录或者更改用户会话的目的。

（2）自我保护。由于无线局域网的物理介质不是很安全，因此认证方法必须能够保护自己不被窃听。这个条件指的是，认证方法必须能够在认证过程中起到这样的作用：即使偷听者窃听到会话过程也得不到他们期望得到的，并且可以作为日后用来冒充合法用户的有用的信息。

（3）抵御字典攻击。认证方法必须不受联机或是脱机状态下字典攻击的影响。联机状态的字典攻击是指，攻击者冒充用户向认证服务器重复发送试图连接网络的请求，可以通过限制一个用户可以拥有的最多失败认证次数来阻止这种攻击；脱机状态的字典攻击指的是，攻击者在自己的机器上向认证服务器重复发送试图连接网络的请求，如果他们获得一对简单的“挑战/响应(Challenge/Response)”对，他们就可以在字典中尝试所有的口令看哪一个口令产生“挑战”想要的“响应”，从而获得用户的口令，因此简单的“挑战/响应”方法对脱机状态的字典攻击很敏感。

（4）产生会话密钥。认证方法必须可以产生会话密钥用以提供消息鉴权、机密

性并保护用户所建立会话的完整性。这些密钥将传递给用户的设备驱动程序在下一个会话中作为 WEP 或 TKIP 密钥。

4.1.2 应当具有的特性

（1）认证用户。认证方法应当对用户而不是对用户的设备进行认证，这样就可以增加那些对用户设备进行攻击的难度。为满足这个条件可以根据用户容易记忆的秘密而制订认证方法，或是将这个秘密加载到一个便于用户携带智能卡上，从而将用户和用户设备分离。

（2）先前的保密。认证方法应当能够进行先前的保密。先前保密意思是说，用户的秘密，不论是口令还是密钥，都不能在将来某个时候受到威胁。假设攻击者记录了用户的会话，但这段会话被用户认证过程中所产生的密钥加密，即使攻击者具有用户的知识，他也不能解密这段会话。

（3）访问接入点。认证方法应当能与支持采用 EAP、802.1X 协议的无线接入点 AP 协同工作。

（4）快速有效。认证方法应当在最小数量的协议回合内完成，而且只需要最少的计算资源就能完成认证过程所需要的计算量。

（5）低维护成本。认证方法应当易于网络管理员管理。例如，一个需要在每个用户设备上都安装证书的认证方法不利于管理员管理，仅对证书撤销单的维护就是一项昂贵的管理负担。

（6）便于用户使用。认证方法应当便与用户使用。例如，使用证书的认证方法，虽然给管理员带来不便却方便了用户；使用智能卡，虽然给用户带来不便却易于管理员管理。用户不会介意使用一个短小的易于记忆的口令。

4.1.3 可能具有的特性

（1）扩充传统方法。认证方法可以将无线认证方法和传统的认证方法相结合，从而增强一个不太安全传统方法的安全性。这种特性特别适合那些传统方法不能很快被新方法替代的环境。

（2）快速的重认证。认证方法可以提供比传统的方法更快速更精确的重认证机制。

4.2 WLAN 的认证协议

RSN 的认证基于 802.1X/EAP，目前提出和使用的认证方案有 EAP-TLS、

EAP-TTLS、PEAP、LEAP、EAP-MD5、EAP-SRP，结合移动通信系统中的 SIM 卡，还有一种类型 EAP-SIM。下面讨论这几种认证方案。

4.2.1 EAP-TLS 协议

EAP-TLS[13][17]（传输层安全）认证协议是由微软公司开发出来的一种基于证书的双向认证方案，通过采用 EAP 支持的 TLS 公钥证书认证机制，从而提供客户端与服务器之间的相互认证。该方法要求客户端和服务器双方都持有由他们彼此皆信赖的第三方所发放的数字证书，这里的第三方就是 CA(Certificate Authority)。

EAP-TLS 认证流程大致如下：

（1）通过探询和验证，建立终端和 AP 之间的无线连接；

（2）开始 TLS 认证，终端与认证服务器交互证书，协商会话加密密钥；

（3）建立传输层安全信道，认证服务器通知 AP 允许该客户端访问无线网络，终端发送的信息加密后在 TLS 上传送。

EAP-TLS 方法的特点如下：

（1）提供了客户端与服务器之间的相互认证；

（2）动态生成基于用户的和基于会话的 WEP 密钥，以保护 WLAN 客户端和接入点之间随后进行的通信；

（3）支持分装和重组机制（对于那些很长的 EAP 消息包，比如证书）；

（4）重新链接速度快(通过 TLS 会话重新开始)；

（5）证书管理任务繁重。

EAP-TLS 方法的安全性能与其它方法相比较是最高的，缺点就是对大型的 WLAN 实现起来不太容易，尤其是在证书管理方面。该协议不对用户身份进行保护，协议交换轮数为 5 轮。

4.2.2 EAP-TTLS 协议

EAP-TTLS[27]（隧道传输层安全)方法由 Funk Software 和 Certicom 公司开发，它扩展了 EAP-TLS 方法。此方法提供了一种基于证书的认证方法，并通过加密的通道(或“隧道”)进行客户端和服务器之间的相互认证。该方法还提供了一种根据每个用户、每个会话动态派生 WEP 密钥的方法。与 EAP-TLS 不同的是，EAP-TTLS 只需要服务器端的证书而不需要客户端的证书。该方法由于是 Funk 提出，因此使用客户端和服务器端软件需要收费。

EAP-TTLS 认证流程大致如下：

（1）在客户端和 AP 之间建立数据通信安全隧道(采用 EAPOL 协议)，在客户端和 TTLS 认证服务器之间建立传递认证信息的安全隧道，其中 AP 和认证服务器之间采用 RADIUS 协议进行通信；

（2）利用建立好的隧道传送后续 EAP 认证包，实现 TTLS 认证。

EAP-TTLS 认证支持多种认证包，包括 CHAP、PAP、MS—CHAP 和 MS—CHAPv2 等。并且通过定义新的属性，TTLS 还可方便地支持更多新的协议包。

4.2.3 EAP-PEAP 协议

EAP-PEAP[1]（保护可扩展身份验证协议）是由微软、Cisco 和 RSA 共同提出的一种通过 TLS 来进一步增强其他 EAP 身份验证方法安全性的身份验证机制。PEAP 只需要服务器端的证书而不需要客户端的证书，从而简化了 WLAN 的安全结构。PEAP 以与 EAP-TTLS 同样的形式在 EAP 之上添加了 TLS 层，不同的是 PEAP 将 TLS 会话的结果作为载体保护其他传统的 EAP 方法。PEAP 使用 TLS 提供服务器到客户端的认证，但不提供客户端到服务器的认证，这也就是在该方法中只要求服务器持有公共密钥证书的原因。客户端和服务器交换一系列以 TLS 报文格式封装的 EAP 报文，这些 TLS 报文通过使用客户端和服务器协商的 TLS 会话密钥进行确认和加密。

PEAP 提供以下服务从而保护 EAP：

（1）报文证明。冒充者既不能伪造也不能插入 EAP 报文；

（2）报文加密。冒充者既不能阅读也不能解密受保护的 EAP 报文；

（3）服务器端到客户端的认证；

（4）密钥交换(建立动态的 WEP 或 TKIP 密钥)；

（5）分装和重组(对于那些较长的 EAP 报文)；

（6）快速重连接(通过 TLS 会话恢复)。

PEAP 方法有效地扩充了那些缺少以上一个或多个特性的传统的 EAP 方法。对请求者的认证是在 TLS 加密信道的保护下进行的，因此请求者的身份得到保护；PEAP 具备显式密钥认证但不具备向前保密性和密钥泄露伪装。

4.2.4 EAP-LEAP 协议

EAP-LEAP[1]（轻量级扩展身份认证协议）是由思科公司提出的一种基于 802.1X 的扩展认证协议。该协议基于双向相互认证，意思是客户端和 AP 双方必须在允许客户端访问网络前进行相互认证。相互认证阻止了非法(未授权)AP

接入受保护的网络。Cisco LEAP 基于用户名/口令方法。

使用 LEAP，安全密钥会随着每一个通信会话而动态的改变，从而阻止攻击者搜集用来破译数据的报文。通过 LEAP 产生的新密钥在用户和 AP 之间使用共享密钥方法。LEAP 同时为无线网络提供了另一种级别的安全措施，就是在允许流量通过无线设备前对所有到网络的链接都进行认证。

LEAP 方法不能抵御字典攻击，而且由于 LEAP 为 Cisco 公司所私有，因此它不能用在其他厂商生产的 AP 设备上。

4.2.5 EAP-MD5 协议

EAP-MD5[1]功能通过 RADIUS 服务器提供简单的集中用户认证。在这种方式下，RADIUS 服务器不需要证书或者安装在无线工作站中的其他安全信息。用户注册时，RADIUS 服务器只是检查用户名和口令，如果匹配，就通知无线访问点允许该客户端访问网络。EAP-MD5 是一种单向认证机制，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。

EAP-MD5 认证流程大致如下（设 AP 为认证点）：

（1）通过探询和验证，建立终端和 AP 之间的无线连接；

（2）开始 EAPOL 验证流程，终端将用户名信息发送给 AP，AP 利用“Access—Request”报文将用户名发送给 RADIUS 认证服务器，并在报文中附加相关的 RADIUS 属性；

（3）RADIUS 认证服务器发送质询文本，通过 AP 转发给用户终端；

（4）客户端将密码和质询文本做 MD5 算法后回送给 RADIUS 认证服务器。由 RADIUS 认证服务器判断用户信息是否合法，并回送认证成功/认证失败报文；

（5）如果认证成功，用户将获得 IP 地址以接入网络，此时将启动计费流程。

由于在 WLAN 中进行非法监听非常容易，而 EAP-MD5 认证方式的安全性较差，因此不适用于 Wi-Fi 网络。

4.2.6 EAP-SIM 协议

EAP-SIM[1][15]主要将 WLAN 与现有 GSM 系统联系起来，通过 SIM 卡实现客户端和认证服务器之间的相互认证。SIM 用户接入流程包括认证、DHCP 地址分配、强制 Portal、页面推送和计费等。接入认证点通过接入网络和 GSM(GPRS) 信令网络间的网关来中继对认证服务器的请求。认证服务器从归属位置寄存器(HLR)查询认证数据，并根据这一数据对用户进行认证。

EAP-SIM 是一种对称钥认证方式，它使用了改进的 GSM 认证方式来支持

双向认证。该协议是共享密钥认证，在用户和 AAA 认证的过程中，会话密钥始终没有在无线链路上出现，而且采用了 N=2 或 3 个三元组增强会话密钥的安全性，双方都采用了随机数来保证会话的新鲜性。所以，对于攻击者而言，不知道共享密钥 Ki，将无法成功认证。EAP-SIM 协议完成了隐式密钥认证。和 EAP-TLS 一样，Ki 的泄漏将导致以前会话密钥的泄漏，不具有前向保密性。另外，服务器端 Ki 的保密非常重要，因为服务器需要以明文形式使用 Ki，所以如何防止服务器操作人员窃取 Ki 变得非常复杂。

4.2.7 EAP-SRP 协议

EAP-SRP[1][22]（远程安全口令认证协议），属于双向认证。支持动态密钥的生成，对现有 802.1X 和 WEP 不用做任何修改。与 TLS 认证方式不同的是，SRP 是通过口令来进行认证的，不需要在客户端和服务器安装证书。

EAP-SRP 认证流程大致如下：

（1）服务器以固定格式存储用户信用信息（信息包括用户名、口令识别符等。口令识别符是对原始口令进行运算后的值）；

（2）服务器和客户端计算并交换公共密钥（服务器根据口令识别符计算密钥，密钥的交换需要遵循哈希算法）。

这种认证方式不够灵活。需要为每个新用户存储用户信用信息，且容易遭受“字典攻击”。

上述几个协议的关系如下表 4.1 所示。在这个表中，下层的协议表示较底层的协议。

<table>
<tr><td>EAP-MD5</td><td>LEAP</td><td>TLS</td><td>TTLS</td><td>其他协议</td></tr>
<tr><td colspan="5">EAP</td></tr>
<tr><td colspan="5">802.1X</td></tr>
<tr><td colspan="3">PPP</td><td colspan="2">802.11</td></tr>
</table>

表 4.1　协议之间的关系

4.3 基于证书方法的不足

上述讨论的一系列 EAP 认证方法，像 EAP-TLS、EAP-TTLS、EAP-PEAP 等都是基于证书的认证方法。它们使用了基于公共密钥的证书和传输层安全协议，为无线局域网提供了强大的安全保证，然而这些方法也存在一些问题：

1、管理开销大。基于证书方法最大的不足就是管理证书工作量大。这一系列方

法都要求认证方持有客户端（用户设备）认可的权威机构所发放的公共密钥证书。这就要求网络管理员要么从商业证书管理局购买服务器证书，要么自己编写专业软件。不仅如此，接下来，网络管理员还要配置各个接入网络的设备，使其识别认证方和 CA 的证书。例如，EAP-TLS 方法要求所有用户设备都持有证书，这就大大增加了管理的开销。同时，证书的分发也是一个大问题，因为必须安全的在用户设备上安装证书。同样的，维护证书撤销清单也比较困难，认证方要知道那种证书好或那种不好。

2、协议交换次数多。这是基于证书的 EAP 认证方法的另一个不足，即完成一次认证所需要在客户端和服务器端进行多次连续的协议信息交换（来回行程）。例如，使用受 PEAP 保护的传统的 EAP-MD5 方法完成对一个单一用户的认证在客户端和认证方之间就需要进行六次来回行程。这样会导致一些问题，特别当移动用户进行无缝漫游时。

3、不是对用户而是对用户设备进行认证。这个不足表现在用户要么必须将证书存储在用户的设备上，要么携带一块智能卡。前一种方法只是认证用户设备而起不到认证用户个体的作用，如果在用户设备不是很安全或是多个用户使用一个设备的情况下，就失去了作用；在后一种方法中，虽然用户可以随处携带证书，但是用户设备和智能卡之间需要一个转换接口，明显给用户带来不便。

4.4 本章小结

通过以上对 WLAN 基于证书认证协议的分析，本文认为，在无线局域网环境下采用基于口令的认证方法比基于证书的认证方法更加方便和经济实用。显然，此时对基于口令的认证方法有了新的要求，因为它也不可避免的存在着弱点，比如它们特别容易遭受离线的字典攻击，攻击者采用这种方法可以从解密高手的“字典”中推测用户可能的口令。为了解决这个问题，使基于口令的认证方法更加适用于无线网络环境，本文在下一章改进了基于 SPEKE （Simple Password-authenticated Exponential Key Exchange）算法的 EAP 认证方法。

第五章 EAP-SPEKE 认证方案及性能仿真

为回应昂贵的和不方便的基于证书的认证方法，研究安全的工作人员已经开发了一系列完整的基于口令的认证方法，但是需要特别指出的是，这里提到的基于口令的认证方法有别于传统的有缺陷（在无线网络环境下）的口令方法，我们用术语“强壮的口令（Strong Password）[23]”认证方法来特指这一类基于口令的方法。

使用强壮口令方法的主要益处在于，通信的双方可以证明彼此都互相知道一个秘密而不会向第三方（可能正在监听他们的会话）揭示这个秘密。事实上，这类方法既不会揭示秘密也不会使攻击者很容易就发现这个秘密，它们通过使用一个小的、易于记忆的口令来达到强壮的认证目的。这类方法的核心是 Diffie-Hellman 密钥交换算法。通信的双方使用 Diffie-Hellman 密钥交换算法产生加密密钥，即使观察者观看了他们的整个会话过程也无从得知这些密钥。

5.1 SPEKE 算法及安全性分析

5.1.1 SPEKE 算法

SPEKE（Simple Password-authenticated Exponential Key Exchange）算法[4][12]由 David Jablon 于 1996 年提出，该算法基于口令和 DH-EKE（Diffie-Hellman Encrypted Key Exchange）。与 DH-EKE 不同的是，SPEKE 将用户的口令作为密钥交换的底数或是产生元，而在 DH-EKE 中通常选取一个固定的公开的数作为密钥交换的底数。SPEKE 旨在用小口令就能在不安全的信道上建立安全的认证并产生密钥而不受离线的字典攻击。

SPEKE 是已知的强壮的密钥交换和认证协议中最简单的一种协议，该协议的工作机制分为两个阶段：密钥交换阶段和密钥认证阶段。在密钥交换阶段，客户端和服务器经过协商，建立 Diffie-Hellman 密钥 K；在密钥认证阶段，客户端和服务器要彼此确认对方的确知道密钥 K，然后再将 K 做为它们的会话密钥。下面以客户端/服务器为例详细说明 SPEKE 的密钥交换和密钥认证过程。

首先定义几个数学符号，如下表 5.1 所示。

数学符号	代表意义
pwd	客户端和服务器的共享口令，该口令不长

p	适合用于 Diffie-Hellman 密钥交换的大素数
q	（p-1）的一个质因子
g	合适的 DH 底数，素数或是一个素数集合
f（pwd）	将 pwd 转换成合适的 DH 底数的函数，本例中选取 $f(pwd)=pwd^2 \bmod p$
X_A，X_B	客户端和服务器分别秘密选取的随机数
Q_A，Q_B	客户端和服务器分别计算出的幂运算值
E_K（M）	用 K 作为密钥加密 M 的对称加密函数
H（M）	关于 M 的单向散列函数
K	生成的会话密钥

表 5.1　SPEKE 认证过程中的数学符号

第一阶段，通信的双方首先采用函数 f（pwd）将口令 pwd 转换成求幂运算的底数，然后根据 DH 密钥交换建立共享密钥 K，接下来就是一个纯粹的 Diffie-Hellman 密钥交换过程：

1、客户端计算 $Q_A=f(pwd)^{2XA} \bmod p$，并将 Q_A 发送给服务器；

2、服务器计算 $Q_B=f(pwd)^{2XB} \bmod p$，并将 Q_B 发送给客户端；

3、客户端计算 $K=H(Q_B^{XA} \bmod p)$；

4、服务器计算 $K=H(Q_A^{XB} \bmod p)$。

第二阶段，客户端和服务器在将 K 做为会话密钥前，要证实彼此的确都知道 K。可以采用如下方法验证密钥 K：

5、客户端选取随机数 X_A，并将 $E_K(X_A)$ 发送给服务器；

6、服务器选取随机数 X_B，并将 $E_K(X_B, X_A)$ 发送给客户端；

7、客户端证实 X_A 正确，则将 $E_K(X_B)$ 发送给客户端；

8、服务器收到 $E_K(X_B)$，则证实 X_B 正确。

事实上，上述两个阶段可以同时进行，以减少传送信息的轮回、减少通信量、加快执行过程，简化后的过程如下：

首先在会话开始前，客户端和服务器先设置几个参数。客户端首先选择一个口令 pwd 和一个秘密的随机数 X_A，接着计算 $Q_A=f(pwd)^{XA} \bmod p$。服务器同样也选择 pwd 和一个秘密的随机数 X_B，并计算 $Q_B=f(pwd)^{XB} \bmod p$。接下来：客户端计算将 Q_A 和哈希函数 $H(ID_A, RAND_A)$ 的计算结果发送给服务器；服务器收到 Q_A 和哈希函数值后，用它选取的秘密随机数 X_B 计算会话密钥 $K=H(Q_A^{XB} \bmod p)$。接着，服务器选取随机数 $RAND_B$，并用 K 加密 $RAND_A$ 和 $RAND_B$，然后将加密后的值 $E_K(RAND_A, RAND_B)$ 和 Q_B 一起发送给客户端；客户端收到 Q_B，如果它的确知道随机数 X_A（即它就是 X_A 的发送者），那么它

就能够根据 K=H（Q_B^{XA} mod p）计算出 K 从而解密 E_K ($RAND_A$，$RAND_B$)。于是客户端可以向服务器发送 M=E_K ($RAND_B$)。如果服务器用它的密钥 K 解密 E_K ($RAND_B$)得到 $RAND_B$，则验证了客户端，从而完成了一次双向认证过程。

5.1.2 SPEKE 安全性分析

1、最直接的攻击方法是攻击者在信道上窃听通信的报文，可以获得 Q_A、Q_B。但是由于离散对数计算困难性以及 Diffie-Hellman 体制安全性，它们无法得到 X_A，X_B，故也无法获得会话密钥 K，也不能猜测出 pwd，满足 4.1.1 节中无线网络认证方法必须满足的特性的第一和第二条件。

2、假设攻击者通过某种途径获取了会话密钥 K，但是它不会像 EKE 协议那样直接受到 Deinng-sacco 攻击，即通过 K 以及字典猜测 pwd，以获得正确的口令 pwd。主要原因是 SPEKE 协议是由双方共同确定会话密钥，不需要在通信信道上加密传送，又因基于离散对数问题，攻击者无法从 K 直接推出 Q_A、Q_B，因此，也就不能从中得到 pwd。但是如果攻击者既知道了 K，又知道了 X_A，则他可以猜测到口令 pwd。为防止这种情况，双方一定要及时销毁临时参数 X_A，X_B。

3、假设攻击者攻破了服务器方，获取了用户口令 pwd，他可以冒充合法用户，但是其不能获取以前通信的会话密钥。知道口令 pwd，可以计算出 Q_A、Q_B，但是基于 Diffie-Hellman 的安全性，由 Q_A、Q_B 不能算出 K=H（Q_A^{XB} mod p)。这一点即满足了安全准则 forward secrecy。为了防止攻击者攻破服务器直接得到 pwd，我们可以在服务器方存放验证口令的散列函数 H（pwd)，此时即使攻击者知道了 H（pwd）也不能立即获得 pwd。当然这样做，会影响协议执行的性能。

4、为了防止离散对数攻击，底数和模数必须满足一定的条件。在 SPEKE 中，底数不能是模数的本原元。如果 f (pwd)是有限群 Z_P 的本原元时，因为所计算的指数结果没有加密，攻击者可以在子群空间中测试其结果。一旦结果是 p 的一个本原元，就可推测底数也是质数。对于一个本身安全的模数 p 来说，这一情况泄漏了有关口令 pwd 的信息，容易引起对 pwd 的部分攻击。但是对任何 pwd，如果底数是一个大质数 p 的生成元（generator）时，则 $f(pwd)^{XA}$ mod p 不会泄漏有关口令 p 的任何信息。例如在本例中定义的 $f(pwd)=pwd^2$ mod p。虽然 Q_A、Q_B 没有加密，但是基于 Diffie-Hellman 安全性，攻击者是不能得到会话密钥 K 的有关信息或是猜测 pwd。

综上所述，SPEKE 算法具有强大的功能使它适用于无线局域网络的认证，表现在：

1、SPEKE 算法采用一系列貌似随机数的报文在通信的设备间交换，SPEKE 模块用这些报文执行计算，然后判断通信的另一方是否使用了正确的口令。如果双方的口令相匹配，SPEKE 则为通信的双方产生一个共享密钥。在第三方看来，SPEKE 报文看起来就像随机数，不能用于确认任何对口令的可能的猜测；

2、SPEKE 算法的中心是公钥计算。除了口令之外，SPEKE 不需要其它公钥、私钥或是其他敏感数据参与计算；

3、SPEKE 使用“零知识证明”（Zero Knowledge Password Proof ，ZKPP）认证方法来安全的传输密码，因此参与会话的任何一方不会得到任何信息，除非他们在会话过程中使用了准确的口令；

4、SPEKE 提供可以协商的、强壮的、长度不受限制的密钥；

5、保护基于 Hash 函数的挑战/响应方法不受离线字典攻击的破坏；

6、客户端和服务器端同时进行认证；

7、不需要额外的安全基础结构；

8、不需要客户端和服务器端证书；

9、使用普通的口令就能实现完全的现代加密术；

10、使用方便，要实现 SPEKE，用户只需要在设备上完成一次性安装或是第一次和 AP 联系时安装程序即可。SPEKE 不像 TLS 等方法需要额外的基础结构就能达到与之相当级别的安全认证，而且可以嵌入到 AP 设备中。

基于上述原因，SPEKE 算法使得基于口令的认证更加强大、更加安全。采用 SPEKE 算法，即使是用很小的口令也能很好地防范攻击。但是在 SPEKE 中，并没有提供验证机制，即验证用户方是否为真正的 pwd 持有者，而且用户的口令存放于认证服务器中，如果某个攻击者攻破了服务器截获了用户口令，那么他就可以轻而易举的直接冒充合法的用户。因此，如果对 SPEKE 加以改进，将它扩展为可认证的密钥交换协议，并结合 EAP，则可以更好的发挥它在无线局域网中的安全认证作用。

5.2 EAP-SPEKE 认证方案

5.2.1 改进的 SPEKE

假设认证服务器端的验证口令由散列函数 S=H（pwd）确定，$V=g^{pwd}$，V 和 S 都存储在认证服务器中；客户端拥有口令 pwd，a 和 b 都是随机数，客户端向认证服务器请求通信。

1. 客户端计算：S=H（pwd），$Q_A=S^{2a} \bmod p$。将计算结果 Q_A 发送给认证服务器；
2. 认证服务器计算：$Q_B=S^{2b} \bmod p$，　$K_1=Q_A{}^b \bmod p$，
   $PROOF_{BK1}=H(H(K_1))$。将 Q_B 和 $PROOF_{BK1}$ 发送给客户端；
3. 客户端计算：$K_1'=Q_B{}^a \bmod p$，$TEST_{BK1}=H(H(K_1'))$，
   $PROOF_{AK1}=H(H(K_1'))$。检验 $TEST_{BK1}$ 与收到的 $PROOF_{BK1}$ 是否相等，若相等则将计算出的 $PROOF_{AK1}$ 发送给认证服务器；
4. 认证服务器检验 $PROOF_{AK1}$ 的正确性，如果 $PROOF_{AK1}=PROOF_{BK1}$，则认证服务器产生一个随机数 x，并计算：$U=g^x \bmod p$，将计算结果 U 发送给客户端；
5. 客户端计算：$K_2=U^{pwd} \bmod p$，$PROOF_{AK2}=H(K_2)$。将结果发送给认证服务器；
6. 认证服务器收到 $H(K_2)$后计算 $K_2=V^x \bmod p$，并验证 $H(K_2)$的正确性。如果 $H(K_1)$和 $H(K_2)$都正确，则完成会话密钥 K_1 的建立过程，否则中止会话。

前三步同 SPEKE 协议一样，完成会话密钥的建立，其安全性同 SPEKE 协议一样。后三步主要是验证客户端是否是口令 pwd 的真正持有者。如果攻击者不知道 pwd，则他只能靠猜测 pwd 来计算 K_2。由于一次性猜对 pwd 的概率是很小的，故即使他知道了 H(pwd)也不能冒充合法用户。如果攻击者知道了 V，由于计算离散对数的困难性，他是计算不出 pwd 的。因此改进后的 SPEKE 协议相对于以前的协议，安全性更好。在系统认证过程中，即使服务器方被攻破，也能保证一定程度的安全性。

5.2.2 EAP-SPEKE 认证流程

在无线局域网环境下，将改进后的 SPEKE 协议和 EAP 协议结合起来，即把 SPEKE 协议加到 EAP 会话过程中，以 EAP 用户—User 和 EAP 认证方—Authentication Sever（实际应用中，通常有一个后置认证服务器和 AP 进行协商，但在本讨论中我们仅以 Authenticator 作为认证方为例来说明认证过程，以下简称 AS）为例说明协议流程。

首先先定义几个数学符号，如表 5.2 所示（重复的符号如表 5.1 中的定义）。

数学符号	代表意义
S	User 和 AS 共享密钥的散列值
V=f（pwd）	将 pwd 转换成合适的 DH 底数的函数，验证 User 的确是 pwd 和合法持有者

$Proof_{XK}$	Hash 函数值，证明 X 知道 K
$Test_{XK}$	Hash 函数值，检验 X 知道 K

表 5.2　EAP-SPEKE 认证过程中的数学符号

EAP-SPEKE 的协议流程如下图 5.1 所示。

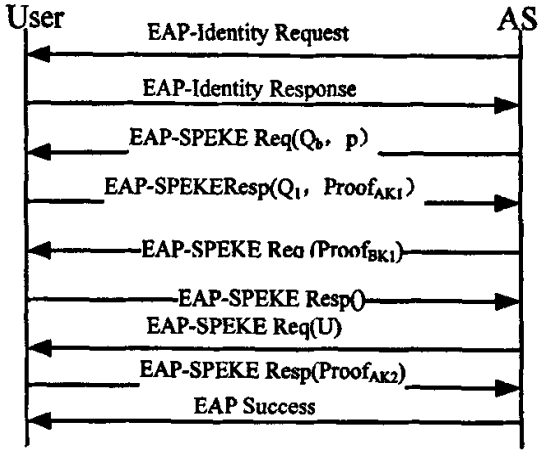

图 5.1　EAP-SPEKE 协议流程

AS 存放了合法用户 User 的 ID、S 和 V。

（1）AS 发起 EAP 对话，它向 User 发送一个 EAP-Identity Request 请求，接着 User 回应 AS，向它发送一个 EAP-Identity Response 响应；

（2）当 AS 收到 User 发来的 EAP-Identity Response 响应包后，就在其数据库中检索到用户的口令的散列值 S，然后产生一个临时随机数 b，并计算：$Q_B = S^b \bmod p$，其中 p 是一个大素数。然后将该计算结果 Q_B 和 p 以 EAP-SPEKE-Request 报文的形式发送给 User；

（3）User 产生一个临时随机数 a 并计算：$Q_A = S^a \bmod p$，$K_1 = Q_B^a \bmod p$，$Proof_{AK1} = H(Q_A, K_1)$，将计算结果 Q_A 和 $Proof_{AK1}$ 以 EAP-SPEKE-Response 报文的形式发送给 AS；

（4）当 AS 收到对应它第一次发送的 EAP-SPEKE-Request 包的 EAP-SPEKE-Response 包后，计算：$K_1 = Q_A^b \bmod p$，$Test_{AK1} = H(Q_A, K_1)$，$Proof_{BK1} = H(Q_B, K_1)$，将其计算的 $Test_{AK1}$ 结果和从 User 那儿收到的 $Proof_{AK1}$ 值相比较，如果不相等则发送认证失败信号；如果相等，AS 则向 User 发送第二个 EAP-SPEKE-Request 包，并将 $Proof_{BK1}$ 值封装在该包中；

（5）当 User 收到来自 AS 的第二个 EAP-SPEKE-Request 包，就用之前收到的 Q_B 和自己计算出的 K_1，计算：$Test_{BK1} = H(Q_B, K_1)$，将其计算出的 $Test_{BK1}$ 结果和从 AS 处收到的 $Proof_{BK1}$ 值相比较，如果不相等，则异常中止与 AS

的对话：如果相等，则返回一个空值的 EAP-SPEKE-Response 包给 AS，表明它满意这一认证结果；

（6）当 AS 收到这个空的响应包后，它计算：$U=g^x \bmod p$，并将结果以 EAP-SPEKE-Request 包格式封装发送给 User；

（7）User 收到该 EAP-Request 包后计算：$K_2=U^{pwd} \bmod p$，$Proof_{AK2}=H(K_2)$，将 $Proof_{AK2}$ 以 EAP-SPEKE-Response 格式法送给 AS；

（8）AS 收到 $H(K_2)$后计算：$K_2=V^x \bmod p$，并验证 $Proof_{AK2}$ 的正确性。如果 $Proof_{AK1}$ 和 $Proof_{AK2}$ 都正确，则完成会话密钥 K_1 的建立过程，AS 返回一个 EAP-Success 包给 User，表明认证成功并结束本次对话。

5.3 EAP-SPEKE 性能理论分析

具体实现协议时，要考虑多方面因素，例如双方通信的来回次数、报文的长度以及协议的执行时间等。SPEKE 和 EAP-SPEKE 协议均是基于离散对数密码体制的，协议执行的时间主要花费在指数计算及模运算的时间上，其他诸如报文的传递时间相对离散对数计算来说比较少。如设：Tg：当底数 g 很小时，计算指数值所需时间；Te：当指数 e 很小时，计算指数值所需时间；Tb：当底数 g 和指数 e 都不小时，计算所需的时间。由下表 5.3 可以看出，EAP-SPEKE 协议执行时间相对来说比较长，因为它有两个 DH 交换过程。

协议	客户端	服务器
SPEKE	2*Tb	2*Tb
EAP-SPEKE	3*Tb	3*Tb

表 5.3　协议执行时间比较

因此，为了加快 EAP-SPEKE 协议执行时间，可以采取以下措施：

（1）尽量减小模数 p，但是一定要满足 DH 的安全性要求。此时，我们可以经常更换 p，攻击者一般也不会花很大的代价来计算一个特定的 p；

（2）双方同时并行计算，如图 5.1 所示，在 SPEKE 执行中，上述客户端的 Q_A、K_1、K_2 可以分别与认证服务器端的 Q_B、K_1、K_2 同时进行。原来 K_1 与 K_2 是分开验证的，现在只需一起验证即可。这样做，一方面减少了通信报文的传递次数，另一方面也使得整个协议执行的时间（忽略通信报文的传送时间）由原来的 7T 降为 4T，如果认证服务器方的 U 值提前计算并存储，则执行时间降为 3T。

需要指出的是，在本例说明中，协议初期用来求幂运算的底数的选取采

用了一个将用户口令转换成合适 DH 底数的函数，在实际应用中也可以采用其他函数建立底数，比如椭圆曲线算法 ECC。

5.4 EAP-SPEKE 协议和其他协议的比较

1、EAP-SPEKE 和 LEAP 相比：

Cisco LEAP 是 Cisco 私有的协议并且只能用于自己生产的无线接入点 AP 上，它是 EAP 的衍生物，在客户端和服务器端之间提供双向认证，在网络的 AP 级别上享有专有权。

EAP-SPEKE 独立于 AP 并且可以和任何与 802.IX 协议兼容的 AP 协同工作。这就使它具有很大的灵活性，可以应用于混和的网络和那些不是全部采用 Cisco 无线局域网设备的网络。

2、EAP-SPEKE 和 PEAP 相比：

PEAP 提供一次性令牌认证，支持密钥交换和中止，并且数据库可扩展支持 LDAP/NDS 目录。PEAP 加密 EAP 客户端和服务器间的对话，并通过使用 TLS 信道保障其安全性，同时提供客户端和服务器端之间的双向认证。

EAP-SPEKE 虽然不要求客户端和服务器使用证书或令牌，却能够提供它们同时认证。口令可以安全的交换而不会向第三方泄露任何信息，也不需要增加 TLS 信道。

3、EAP-SPEKE 和 SRP 相比：

EAP-SPEKE 比 SRP 计算简单，信息交换次数少，SRP 要进行两次取模和求幂运算。

表 5.4 给出了各个认证协议之间的比较。

	传统的方法 EAP-MD5	基于证书的方法(TLS、TTLS、PEAP)	基于口令的方法 SRP	基于强壮口令 EAP-SPEKE
必须具备的特性				
相互认证	否	是	是	是
自我保护	是	是	是	是
抵御字典攻击		是	否	是
产生会话密钥	否	是	是	是
安全性	无	强大	弱	强大
应该具备的特性				

认证用户		否，如果证书存在磁盘上	是	是
向前保密	N/A	无	是	是
快速有效	是	否	是	是
低维护成本	是	否	是	是
便于用户使用	是	否，除非证书存在磁盘上	是	是
应用于广泛的 AP	是	否	否	是
可以具备的特性				
扩充传统方法	N/A	是	否	否
快速的重认证	否	是	否	否

表 5.4　各个认证协议之间的比较

5.5 EAP-SPEKE 性能仿真分析

虽然我们通过对认证协议的过程进行分析，比较了各个认证协议的性能，但是很不直观，同时也不能看出协议对网络的影响。我们通过对认证协议的性能进行仿真，可以使我们直观地看出协议性能的好坏和协议对网络的影响。

5.5.1 仿真平台

由于协议运行在网络上，所以我们需要一个与操作系统无关的平台，它可以屏蔽对操作系统的实际的访问，且能近乎真实地模拟各种网络环境，让我们可以在各个层次上模拟网络的运行。事实上，已有许多研究机构对此作出努力，并开发出自己的网络仿真器。比如，Columbia 大学的 Alex Dupuy 开发的 NEST，California 大学的 S.Keshav 在 NEST 的基础上，开发了 REAL 网络仿真器。Lawrece Berkeley 国家实验室的网络研究小组对 REAL 做了进一步的改进，得到 LNBL Network Simulator，即 ns-1。UC Berkeley 的 MASH 研究组对 LNBL 继续改进，提出 NS-2.26，这是一个很优秀的软件，它可以在一台计算机上动态仿真多种网络的运行。

我们采用 NS-2.26 作为仿真平台，工作在一台 PC 机上(C1.7G，256M RAM)，操作系统为 Red Hat Linux 8.0。

5.5.2 仿真环境和过程

我们的协议使用在无线局域网的环境，而 NS-2.26 对该环境的支持不够完全，主要有以下几个方面：物理层只支持 802.11，不支持 802.11b，802.11a，802.11g；只支持 802.11 IBSS 模式，不支持 802.11 BSS 模式；不支持 AP 的 802.1X 认证方式。所以我们需要对 NS-2.26 进行扩展以支持我们的仿真需要。

我们通过 NS 的邮件列表，获得一个补丁 ns-AP-patch。该补丁支持：不同的物理层（802.11，802.11b，802.11a，802.11g）；802.11g 物理层的保护；802.11g 短时隙；AP 转发（BSS 模式）；AP 可以和不同的工作站 STA 以不同的速率通信；改善的 CCA 仿真；EDCA 优先级访问。利用该补丁，我们解决了 802.11b，802.11a，802.11g 和 BSS 模式的支持问题。

我们仿真的无线环境包括 1 个 BSS，BSS 由 1 个 AP 和 20 个 STA 构成。其物理层采用了 802.11g，RTS 门限为 3500。在 AP 和 STA 之间建立认证协议的通信，以观察认证协议对正常通信的影响。

5.5.3 仿真结果及分析

认证协议对正常数据流的影响如图 5.2 所示。图中横坐标为数据包的序列号，纵坐标为相邻两个数据包到达目的地的时间差，单位为秒。图中的突出部分是认证协议引入的时延。我们把 EAP-SPEKE 和 EAP-TLS、EAP-LEAP 这两个典型的认证协议相比较，EAP-TLS 是基于证书的认证方案，EAP-LEAP 是基于口令的认证方案。

仿真结果表明，协议 EAP-SPEKE 引入的时延明显小于 EAP-TLS 和 EAP-LEAP 引入的时延，即 EAP-SPEKE 协议的性能明显优于这两个认证协议。

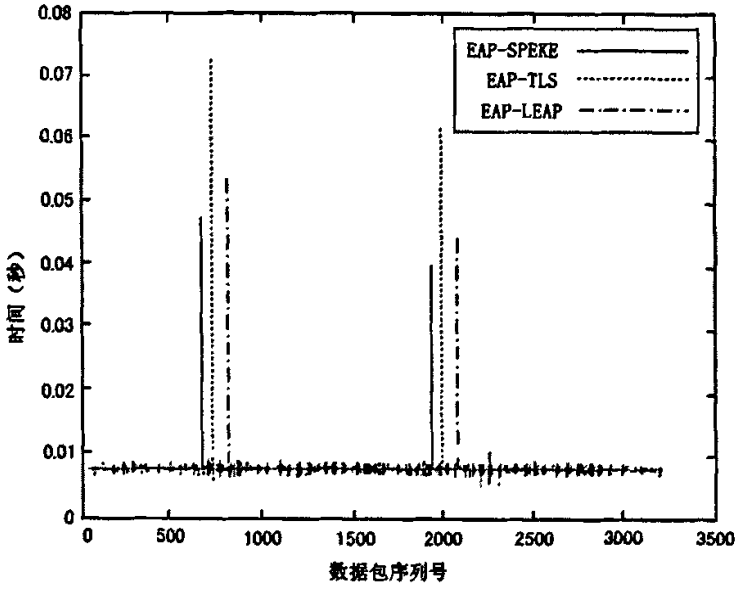

图 5.2　仿真结果

5.6 本章小结

由于 EAP 是可扩展的认证协议，支持多种算法，因此完全可以把它与一种适用于无线局域网的算法相结合，为之提供安全的认证机制。本章提出了一种改进的、强壮的、基于口令的密钥交换和认证协议 EAP-SPEKE，能够为无线局域网提供安全性很好的认证机制，并将其与现有的诸多方法进行了比较，如表 5.4 所示。该方法不需改动现有的 IEEE802.1X 标准及 EAP 协议，有利的补充了 EAP 协议，增强了 IEEE802.1X 标准的安全性能。

结束语

本文主要对无线局域网已有安全协议的工作原理进行了分析，指出了其安全问题的实质所在。在此基础上，介绍了目前的主流解决方案，详细讨论了其设计思想。然后我们重点分析了解决方案中的认证协议，讨论了适用于 WLAN 环境的安全认证协议应满足的条件。最后，提出在无线局域网中采用 SPEKE 算法与 EAP 相结合的方式，来提供客户端和认证服务器的密钥交换和相互认证。并对 SPEKE 算法加以改进，让认证服务器确定客户端是否为口令的真实持有者。并且将 EAP-SPEKE 方法与现有的认证方法相比较，进行了仿真分析，达到了预期的性能。

下一步要进行的工作有：

（1）各类无线网融合时带来的安全问题；

（2）认证协议分析与证明的进一步研究。

致 谢

首先感谢我的导师何方白教授三年来对我的培养、关心和教育。在我的研究生学习期间，她不仅教会了我一套行之有效的科学研究方法，而且她严谨的治学态度、深厚的学术造诣、高度的责任感和虚怀若谷的为人品格给了我很大的影响。在此，我向她表示由衷的谢意！

接下来，我要感谢信科 907 实验室的师兄师弟同门们给予我的帮助！在每一次的研讨会上，大家集思广益，交流学习心得，这些都给予我学习和研究中极大的启发。尤其感谢方飞、冉伟、李蔚蔚、陈华、王小平、张威等给予我的关心、支持和帮助！

此外，我还要感谢杨纪、章殷、范白謇、董佳松、李永强、俞星玉、唐丽娟、吴大鹏等在学习和生活上给予我的鼓励和帮助！

特别要感谢我的父母！他们对我的无私关爱和殷切期望是我前进的动力；他们的谆谆教诲让我学会了以乐观开朗的态度去迎接学习和生活中的各种挑战！

最后感谢重庆邮电大学所有的老师！感谢所有关心、爱护和帮助过我的人们！

攻硕期间从事的科研工作及取得的研究成果

从 2003.10-2005.10，参与了题目为“无线网络安全论证”课题的研究。该课题受到重庆市教委科技研究项目资助，编号：050301。个人工作：对当前无线局域网的安全漏洞进行了深入研究；并且在无线环境下，实现虚拟专用网以改善网络的安全性能。

[1] 宋娜娜、何方白，“无线局域网的安全性探讨”，信息安全与通信保密杂志社，2005 年第 11 期

参考文献

[1] 刘乃安著. 无线局域网（WLAN）——原理、技术与应用. 西安. 西安电子科技大学出版社. 2004

[2] Tara M.Swaminatha，Charlea R.Elden 著. 王超译. 无线安全与保密. 北京. 清华大学出版社. 2003

[3] Christian Barnes 等著. 无线网络安全防护. 北京. 机械工业出版社. 2003

[4] 董小燕，许勇，吴国新，翟明玉著. 基于用户口令的认证密钥交换技术. 数据通信-2003 年第一期. 35-39

[5] 叶永涛，益晓新，王庭昌著. 802. 11 协议族及最新进展. 解放军理工大学学报(自然科学版). 第 3 卷第 4 期. 2002 年 8 月. 10-13

[6] J. Walker. Unsafe at any key size: an analysis of the WEP encapsulation. Tech. Rep.03628E. IEEE 802.11 committee. March 2000. 1-9

[7] Borisov Nikita, Goldgerg Ian, Wanger David. Security of the WEP algorithm. ISAAC, Berkeley,2001，36(3):3-6

[8] Arbaugh, William A. An Inductive Chosen Plaintext Attack Against WEP/WEP2. IEEE801.11 Task group on Security(Tgi).Orlando. IEEE802.11-01 /230. May 2001. 1-18

[9] Tom Karygiannis，Les Owens .NIST Special Publication 800-48 Wireless Network Security

[10] IEEE Standards for local and metropolitan based network access control. IEEE Draft area networks: Standard for port P802.1X/D11.March 2001

[11]SultanWeatherspoon.Overview of IEEE 802.11b Security.Network Communications Group, Intel Corporation, 2002.3

[12] Aydos, M., Yantk, T., Koc, C.K., A high-speed ECC-based wireless authentication on an ARM microprocessor Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference，11-15 Dec. 2000，Pages:401-409

[13] T. Dierks, and C. Allen, The TLS Protocol Version 1.0, IETF RFC 2246, Jan 1999.

[14] Jui-HungYeh,Jyh-ChengChen,Chi-Chen Lee,WLAN Standards, Potentials,IEEE Volume 22,Issue 4,Oct-Nov 2003 Page(s):16-22

[15] Koien，G.M.，Haslestad, T.，Security aspects of 3G-WLAN interworking，Communications Magazine，IEEE Volume 41，Issue11，Nov.2003 Page(s):82-88

[16] L.M.S.C. OF THE IEEE COMPUTER SOCIETY. Wireless LAN Medium

Access Control(MAC) and Physical Layer (PHY) Specifications，ANSI/IEEE std 802.11 .1999 edition.

[17] B.Aboba，PPP EAP-TLS Authentication Protocol，IEFT RFC 2716

[18] Jesse Walker. 802.11 Security Series Part II ： TKIP. http://cedar.intel.com/

[19] C. Rigney，Remote authentication dial In Supplicant Service (RADIUS)，IEFT RFC2865

[20] G Meredith，Securing The Wireless LAN，CISCO SYSTEMS SUPPLICANTS MAGAZINE，Third Quarter 2001

[21] Sponsor，IEEE standard for Local and etropolitan are networks-Port-Based Network Access Control，June 14，2001，IEEE Std 802.IX-2001

[22] D.Taylor，Using SRP for TLS Authentication，IETF draft-ietf-tls-srp-0l.txt(work in progress)，2001

[23] David P.Jablon，Strong Password-Only Authenticated Key Exchange，ACM Computer Communications Review，October 1996.

[24] Interlink Networks，Inc. EAP Methods for Wireless Authentication,2003.04

[25] Wireless LAN Security Interoperability Lab，What are Your EAP Authentication Options，www.opusl.com/www/whitepapers

[26] Mihir Bellare，Phillip Rogaway，The Authentication Protocol for Password—Based Authenticated Key Exchange，Contribution to IEEE P1363，2000.03

[27] P.Funk，S.Blake-Wilson.EAP Tunneled TLS Authentication Protocol. http://www.ietforg/Internet-drafts/draft-haverinen-pppext-eap-ttls-02.txt，Novermber 2002

[28] Analysis of 802.11(Wireless LAN) security，http://www. engr. smu. edu

[29] IEEE P802.11i D3.0，Specification for Enhanced Security http://www.cs.umd.edu/mhshin/doc/802.11 /802.11 i-D3.0.pdf，November 2002

[30] Arunesh Mishre，Willian A.Arbangh. An Initial Security Analysis of the IEEE 802.1X Standard

[31] Uri Blumental，Milind M. Buddhikot，Juan A. Garay，etal.A Scheme for Authentication and Dynamic Key exchange in wireless networks[J]. Bell Labs Technical Journal，2002，7(2):37-48