第3章 无线城域网安全

由于日常的生产生活中，人们对于各种随时随地地使用网络资源的需求不断增加，因此无线局域网、无线城域网等各种无线通信网络应运而生，并且发展非常迅速。而无线城域网作为有可能与 3G 相匹敌的新型无线网络，将会有很大的发展前途。所以，研究无线城域网的安全性具有十分迫切的现实意义。

3.1 无线城域网简介

3.1.1 无线城域网概述

无线城域网是继无线局域网之后的又一种无线网络，它能够提供更大的传输范围和更快的传输速度，是城市无线接入的一种新型手段。由于互联网技术的不断普及和发展，人们对通过无线手段接入互联网提出了越来越高的带宽和距离要求，目前的众多无线通信技术都难以满足人类对信息的需求，存在着接入速率太低、覆盖范围太小、移动速度慢等种种缺陷。

无线城域网的出现打破了这种局面，此标准最初目的是为了解决“最后一公里”接入问题而提出的，能够完成无线城域网的构造。但是截至目前为止，许多无线网络设备提供商和用户都错误地认为此标准的最主要安全缺陷是使用了 56bit 的 DES。事实上密码的长度与标准的安全缺陷没有太大关系。

IEEE 802.16 标准工作组通过寻找 IEEE 802.11 标准的缺陷并通过相关技术解决了这些缺陷，在这些工作的基础上把现存标准重新组织修订形成了现在的 IEEE 802.16 安全标准。现在的标准包括基于线缆连接的数据服务接口规范，此标准是为了解决“最后一公里”线缆连接的接入问题。因为电缆是有线技术而 IEEE 802.11 是无线技术，二者面临着不同的安全威胁，所以目前的 IEEE 802.16 安全标准对于保护 IEEE 802.16 链路传输是完全失败的。

因此对这些技术的研究有利于我国信息技术的发展、运营竞争力的上升、建设投资费用的降低、无线通信设备制造工艺的改进、我国信息化建设进程的加快、军队科技强军的建设等。

3.1.2 IEEE 802.16 分析

为了让无线城域网技术拥有更好的发展环境从而取得更好的发展，IEEE 先后制定了一系列的无线城域网标准，主要包括 802.16a、802.16c、802.16e、802.16f、802.16g 等。其中最为重要的是 IEEE 802.16 标准，又被称为 WIMAX，它描述了一项无线城域网技术，主

要针对微波以及毫米波频段，提出了一种新的空中接口标准。

IEEE 802.16 工作组成立于 1999 年，工作组被称为 Broadband Wireless Access Standards(宽带无线接入标准)，工作组的主要工作就是负责研究固定宽带的无线接入技术规范，主要是为了解决“最后一公里”的无线宽带城域网的接入问题，其中主要包括 IEEE 802.16 的发展规划、IEEE 802.16 的空中接口标准以及寻求解决共存性问题的建议方案这样的 3 个部分。

目前，IEEE 802.16 标准是最为先进的宽带无线接入规范，它为“最后一公里”或“最初一公里”的无线宽带城域网的接入问题提供了一个廉价的解决方案。它为用户站点与核心网络之间的连接提供了一个通用的连接方式，比如在商务大楼、飞机场、停车场、展览中心、家庭等常见区域都可以通过使用 IEEE 802.16 来连接到 Internet 网络，方便地访问 Internet 网络上的各种资源。可以这样说，IEEE 802.16 工作组的所有工作为宽带无线接入技术的发展和普及作出了巨大贡献。

IEEE 802.16 系列标准如表 3-1 所示。

表 3-1　IEEE 802.16 系列标准

类别	标准编号	标 准 名 称	通过时间	目前状态
空中接口	IEEE 802.16-2001	局域网和城域网 IEEE 标准第 16 部分：固定宽带无线接入系统的空中接口	2001 年 12 月	已被取代
	IEEE 802.16a	局域网和城域网 IEEE 修正标准第 16 部分：固定宽带无线接入系统的空中接口——媒体接入控制(MAC)更改和 211GHz 的附加物理层(PHY)规范	2003 年 1 月	已被取代
	IEEE 802.16d-2004	局域网和城域网第 16 部分：固定宽带无线接入系统的空中接口	2004 年 7 月	在用
	IEEE 802.16e-2005	局域网和城域网 IEEE 标准第 16 部分：许可频段中固定和移动组合运行的物理和媒体接入控制层的固定和移动宽带无线接入系统修正的空中接口	2005 年 12 月	在用

2002 年 4 月，IEEE 802 标准委员会颁布了 IEEE 802.16-2001 标准，该标准为宽带无线接入定义了无线城域网的空中接口规范。但是该标准的工作频段为 10～60GHz，由于在这一频段的信号实际上对建筑物这样的常见障碍物的穿透性能不是很好，这就限制了基站的覆盖范围，无法满足一些用户的需要。另外，一般情况下用户站的天线安装位置都很高，因此系统受到风霜雪雨的影响会比较大，这在一定程度上也阻碍了它的市场应用。

2002 年 7 月，在加拿大温哥华市召开的 Session 2.0 会议上讨论了提交的 IEEE 802.16a 第五版草案。IEEE 802.16a 标准在原来 IEEE 802.16-2001 标准上进行了扩展和修改。IEEE 802.16a 标准于 2003 年 4 月正式颁布。这一标准所规定的信号工作频段是 2～10GHz，其中包含了免牌照的频段以及需要发放牌照的频段。和 IEEE 802.16-2001 标准相比，这一频段的信号可以以更低的成本提供更加广泛的覆盖范围，并且系统受到自然环境的影响更小，系统可以在非视距传输的环境下运行，极大地降低了用户站安装的成本，具有更强的市场竞争力。在 IEEE 802.16a 标准颁布一年之后的 2004 年 7 月，IEEE 802.16d-

2004 标准得到了 IEEE 802 标准委员会的一致通过，该标准对 IEEE 802.16-2001 标准与 IEEE 802.16a 这两个标准进行了修改和补充，虽然它依然是对固定宽带无线接入规定的标准，但是它已经越来越成熟、越来越实用，很好地解决了之前两个标准的很多问题。IEEE 802.16d-2004 规定的频段很宽，主要包括了 10～66GHz 频段、小于 11GHz 许可以及免许可频段。在不同频段下的物理特性各不相同，主要包括以下内容：

(1) 10～66GHz 许可频段，这一频段的信号波长比较短，因此它只能够实现视距传播。常见的信道带宽一般为 25MHz 或者 28MHz，当使用多进制调制方式时，数据的传输速率可以达到 120Mbps。

(2) 11GHz 以下许可频段和免许可频段的波长较长，所以它们能够支持非视距传播，但是，这时系统会存在比较强烈的多径效应，必须采取一些增强的物理层技术，例如功率控制、ARQ、智能天线或者空时编码技术等。另外在免许可频段的信号可能会受到较大的干扰，影响效果，这时需要采用 DFS 等技术来处理干扰。

为了可以为用户提供既具有移动性又能够高速便携访问的宽带无线接入解决方案，2005 年 12 月，IEEE 802 标准委员会正式通过了 IEEE 802.16e-2005 标准。IEEE 802.16e-2005 标准能够向下兼容 IEEE 802.16d-2004 标准，所以它的标准化工作是建立在 IEEE 802.16d 标准基础之上的。IEEE 802.16e-2005 在物理层的实现方式实际上和 IEEE 802.16d-2004 的实现方式几乎是相同的，它们的主要差别在于，IEEE 802.16e-2005 进行了 OFDMA 方面的扩展，并且提供了针对移动性的支持。

通过上面的介绍，从 IEEE 802.16-2001 标准到 IEEE 802.16e-2005 标准，可以看到宽带无线接入技术的发展趋势是向着更高容量、更大覆盖、具有更好的移动性的方向发展的。IEEE 802.16e-2005 标准已经可以在 2～6GHz 的特许频段范围内为高速移动的终端提供网络接入服务，很好地支持了移动性和高速性两种用户最为追求的特性。正是由于它的这些性能使得 IEEE 802.16e-2005 从问世的那天起就备受关注。

实际上，IEEE 802.16e-2005 标准已经演变成为一种针对固定和移动运营商的基于全 IP 的、下一代的、已经标准化的移动解决方案，它的出现对于解决数字鸿沟、固网的“最后一公里”接入和移动的三重播放都有很好的促进作用。

3.2 IEEE 802.16 标准的安全机制分析

通过上面的介绍很容易了解到无线城域网的核心是 IEEE 802.16 标准，为有助于将 IEEE 802.16 定义的广义标准变成更加具体的标准，以满足特定服务提供商的需求，英特尔、诺基亚、AT&T 等 100 家生产、运营商成立了一个非盈利工业贸易联盟组织——WIMAX 论坛，全名是微波接入的全球互通，目标是对以 IEEE 802.16 系列宽带无线接入标准为基础的产品互通性进行测试和认证，以保证市场上设备的部件是标准化的。

3.2.1 安全风险及保护协议

1. IEEE 802.16 标准的安全风险

当一种标准被广泛运用的时候，那么针对它的各种漏洞攻击也会随之而来。总的来说，

IEEE 802.16 标准的安全风险可概括为以下两个方面。

1）物理攻击

IEEE 802.16 的物理层和 MAC 层都很容易遭受到安全攻击，但实际上，IEEE 802.16 标准的所有安全操作都是在 MAC 层完成的，所以，这样看来 IEEE 802.16 的物理层基本上没有任何的防范措施。最为常见的一种攻击方式是“水刑攻击”，在这种攻击中，恶意的攻击者会不停地向接收设备发送数据帧，一直到接收设备的电源耗尽为止。另外针对无线网络来说，最为常见的物理攻击就是对无线电波频谱进行干扰，这样可以极大地影响合法用户的使用质量，甚至在某些情况下使得合法用户无法使用网络资源，这样就可以造成类似于拒绝服务的攻击。IEEE 802.16 标准中没有讨论关于物理层的安全手段的主要原因就是因为物理层的攻击方式并不适合通过标准化的方式来处理。

2）无线信道带来的安全问题

由于无线电信号传播是完全开放的，甚至无法被周围的建筑物之类的障碍物所阻断，这样就使得信号极其容易地被一些恶意的攻击者窃听。这个窃听过程十分容易，其原理和人们使用收音机收听广播的方式是一样的，听众在广播信号的覆盖范围内都可以用收音机收听到广播。当然无线城域网的无线信号的接收并不像收音机那么简单，但是所有在信号覆盖范围内的用户只要有相应的设备，并且处于合适的位置，都可以接收到无线城域网的信号，之后可以根据信号的封装格式对数据进行分析处理。相似的，任何人在适当的位置都可以通过设备向无线网络中发送数据，这样就为恶意的攻击者伪造身份发送伪造数据或者截获从已授权的站点发出的数据帧，然后篡改、重放攻击等提供了方便条件。

2. IEEE 802.16 标准的保护协议

为了解决以上安全问题，IEEE 802.16 主要采取的是在 MAC 层中定义一个保密子层的方式来为通信提供安全保障。保密子层主要包括两个协议：数据加密封装协议和密钥管理协议。

1）数据加密封装协议

数据加密封装协议主要定义了一系列的加密算法，例如公钥密码体制的 RSA 算法、数据加密标准 DES 等；在定义这些加密算法的同时还定义了这些算法的使用规则，它主要依靠 MAC 层的具体机制来实现。

加密服务主要定义在标准定义的 MAC 层的加密子层中。标识加密服务的 MAC 层头信息一般和正常信息的存储格式相同，存储在头信息中，它是通过明文的形式来传输的。在一般情况下，进行加密的只有 MAC 的净负载，普通的 MAC 头信息是不会被加密的。MAC 控制信息一样也是采用明文的方式进行发送，采用这样的发送方式主要是为了便于注册、响应等操作。MAC 净负载加密后的格式如图 3-1 所示。

图 3-1　MAC 净负载的格式

2) 密钥管理协议

密钥管理协议(PKM)提供了安全的密钥交换机制,支持周期性的再认证和密钥更新,是加密子层的核心内容。其中两个重要概念就是授权密钥(AK)和传输加密密钥(TEK)。它们都是由 BS 产生的随机数或伪随机数,前者是认证过程中在 SS 和 BS 之间传输的,而后者用于认证之后传输数据的加密。密钥管理协议在安全机制中往往处于核心位置,是许多研究的重点。

SS 利用 PKM 协议来获得 BS 的认证、流量加密信息和周期性的重认证和密钥更新。PKM 协议使用 X.509 电子证书、RSA 公钥加密算法和强加密算法来进行 SS 和 BS 之间的密钥更新。PKM 协议仍旧使用客户机/服务器模式。SS 作为 PKM 中的"客户机",请求一些与加密相关的信息;BS 作为 PKM 中的"服务器",对这些请求做出应答,以保证每个 SS 客户机只能得到与其已获得认证相关的加密信息。PKM 协议利用 MAC 管理消息,比如 PKM-REQ 和 PKM-RSP 等消息来实现这些功能。

PKM 协议利用公钥加密算法来确认 SS 和 BS 之间的共享密钥,然后共享密钥再用来加密随后的 TEK 交换更新过程。这种双层的密钥分配机制既保证了 TEKs 的及时更新,同时又不增加因为频繁进行公钥算法运算操作的负担。

一个 BS 通过初始授权交换过程来验证一个 SS。每个 SS 拥有一张由其制造商发布的唯一的不重复的 X.509 电子证书。此证书包含 SS 的公钥和 SS 的 MAC 地址。当需要一个 AK 时,SS 把它的电子证书发给 BS。BS 确认此电子证书,然后通过此电子证书包含的公钥加密一个 AK,再返回给请求的 SS。

因为 BS 验证了 SS,这样可以避免攻击者利用一个克隆的 SS 来发动攻击,也就是假冒成合法的 SS 来发动攻击。X.509 电子证书的使用避免了克隆的 SS 们通过假的证书来欺骗 BS。

所有的 SS 都要有一个出厂商预定的 RSA 私/公密钥对或者内置一个能够动态产生此密钥对的算法。如果 SS 是利用内置的算法来产生它的 RSA 密钥对,那么此 SS 应该在它的第一个 AK 交换前产生此 RSA 密钥对。所有有预定的 RSA 密钥对的 SS 也必须要有一个预定的 X.509 证书。所有依靠内置算法来产生 RSA 密钥对的 SS 应该要支持一种机制,以支持通过厂商发布的 X.509 电子证书来产生 RSA 密钥对的能力。

一个安全关联(SA)是一个 BS 和一个或多个与之相连的 SS 为在 IEEE 802.16 网络中进行安全通信而支持的一系列安全资料。IEEE 802.16 标准中定义了 3 种安全关联:初始、静态、动态。每个可管理的 SS 在其初始化过程中建立一个初始 SA。静态 SA 是在 BS 内部预置的;动态 SA 是根据每种特定的服务流的初始化或终止过程而动态地创建或结束的;静态 SA 与动态 SA 都可以被多个 SS 共享。

一个 SA 的可共享信息要包括它所支持的加密套件。同时可共享信息一般也包含 TEK 和初始化向量。SA 包含的其他内容则根据其所支持的加密套件而不同。SA 利用 SAID 来进行定义与区分。每个可管理的 SS 必须和它的 BS 建立一个唯一的与其他 SS 不重复的初始 SA。任何 SS 的初始 SA 的 SAID 都和它的基本 CID 相同。利用 PKM 协议,每个 SS 从它的 BS 那里得到 SA 的加密资料。而 BS 必须保证每个 SS 只能获得其已被授权的获得的 SA 的加密资料。

一个 SA 的加密资料(比如 DES 密钥和 CBC 初始向量)是有生命周期的。当 BS 把 SA

加密资料发给 SS 时，它同时也告诉了 SS 此 SA 的这些加密资料所剩下的生存时间。而 SS 负责当它目前在用的加密资料失效之前重新从 BS 那里申请新的加密资料。如果 SS 目前正在用的加密资料在获得一套新的加密资料之前已经失效，则 SS 必须重新进行入网注册等操作。同时 PKM 协议具体提出了 SS 和 BS 如何保持密钥之间的同步。

3.2.2　密钥的分配更新方法

IEEE 802.16 协议使用 X.509 公钥证书、RSA 公钥算法和三重 DES(数据加密标准)来保护 SS 与 BS 之间的密钥交换。其密钥交换过程如下所述：

(1) 首先，BS 对 SS 进行认证。这个过程是在初始认证期间进行的。每个 SS 都有一个由厂家分配的唯一的 X.509 数字证书，包括 SS 的公钥和 MAC 地址等。当 SS 请求一个 AK 时，SS 将自己的数字证书传给 BS，BS 验证证书的有效性，如果通过，则用证书提供的公钥加密 AK，然后传给 SS。SS 用自己的私钥解密便可以获得 AK。至此，认证过程结束。

这是一种利用公钥密码体制来进行密钥分配的方案，特别适用于大型网络中的密钥管理。公钥的分配无须机密性保护，公钥密码体制的安全性已经得到了实践的证实。

完整的 BS 认证 SS 并分发、更新 AK 的过程如图 3-2 所示。

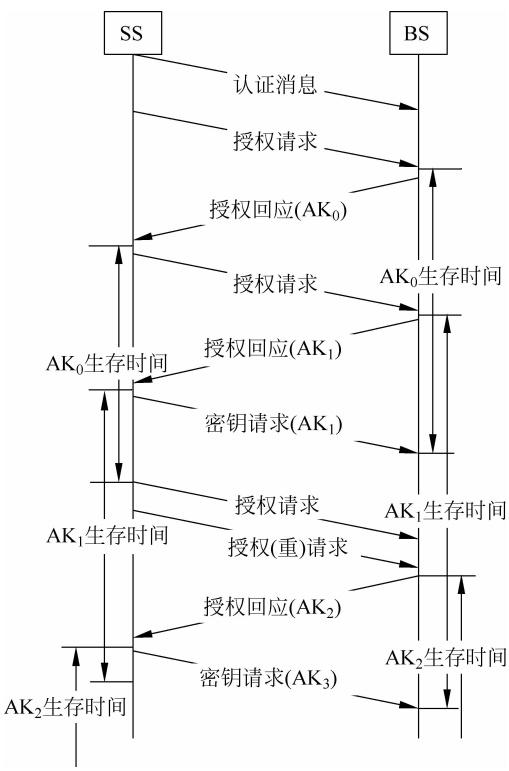

图 3-2　完整的 BS 认证 SS 并分发、更新 AK 的过程

(2) 接下来，SS 向 BS 提出传输加密密钥(TEK)的请求。BS 在接到请求后，用 KEK(由 AK 计算出来的)和三重 DES 算法加密 TEK 并传给 SS。SS 便能利用 KEK 从中解密得到 TEK，至此，密钥交换过程完毕。

同时，安全机制还支持周期性的再认证和传输加密密钥的更新。以周期性的更新 TEK 为例，为了简化分析，假设 BS 同时产生两个序号不一样的 TEK_0 和 TEK_1。其中 TEK_0 的生存时间（设其为 t_0）刚好是 TEK_1 的一半，这样在 t_0 时刻 TEK_0 就会失效，TEK_1 则生效。而这时 SS 就会提出 TEK 密钥请求，BS 再分配一个 TEK_2 给 SS。再过 t_0，TEK_1 也将失效，同时，SS 将申请新的 TEK。就这样 TEK_{n-1} 和 TEK_n 的生存期相互交错，从而实现了 TEK 的周期性更新并保证了它的连续性，具体过程如图 3-3 所示。

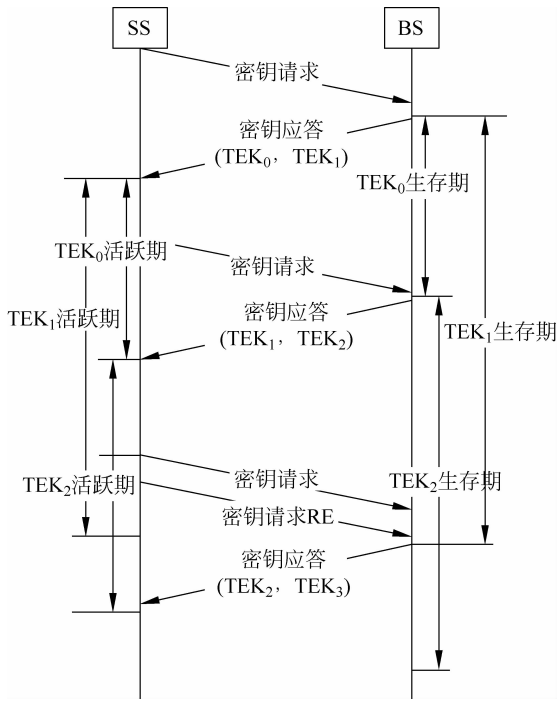

图 3-3　TEK 的周期性更新

3.2.3　加密方法分析

IEEE 802.16 采用 AES-CCM 作为资料传输加/解密算法，但除了 AES-CCM 外，IEEE 802.16 针对一般资料的传输，还可选择复杂度较低的 DES-CBC 加密算法，而针对 Broadcast/Multicast 的需求，IEEE 802.16e 亦采用较合适于群组广播使用的 AES-CTR 加密算法。本小节只简单介绍一下 DES-CBC 算法。

在 IEEE 802.16 支持的资料传输加密算法 DES-CBC 中，通过 KEY-Request/Reply 阶段所产生的 64bit TEK Key 与 TEK Parameters 中的 64bit CBC-IV 值，可经由 DES 算法进行加密，如图 3-4 所示，在资料传输时，将资料分为 64bits 的区块（最后若不足 64bit 也算成一个区块），并将 64bit CBC-IV 与第一个区块的 64bit 资料进行 XOR 运算，之后以 TEK 前 54bit 值为 Key 通过 DES 加密算法产生 64bit 加密后的数据，并存储到数据加密后的暂存位置，在处理下一个 64bit 区块时，便把前一个加密后的 64bit 区块与目前尚未加密过的 64bit 区块进行 XOR 运算，并以 TEK 前 54bit 值为 Key 透过 DES 加密算法同样产生 64bit 加密后的数据，依此类推直到把整个封包依序加密为止。而接收端，只要拥有相同的 64bit

CBC-IV 与 64bit TEK 值就可以依序把封包解密了。

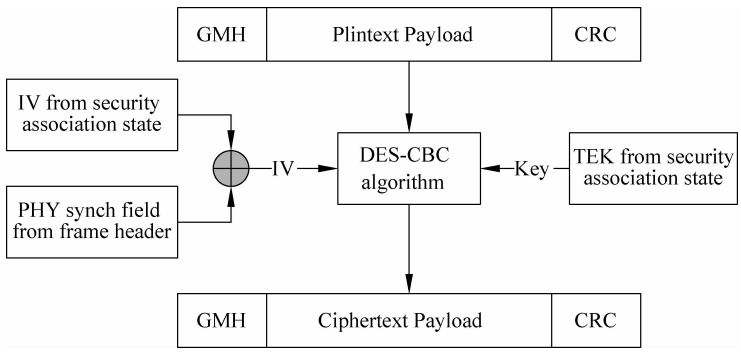

图 3-4　IEEE 802.16 DES-CBC 加密算法

使用 DES-CBC 加密方式是 IEEE 802.16 的安全问题之一，因为长久以来人们一直对 DES 的安全性持怀疑态度。现在发现的 DES 的问题至少有弱密钥问题、密钥长度不够、S-盒的设计问题等。同时加密初始向量 IV 也是可预知的，这也容易遭受伪造攻击。授权密钥 AK 是 IEEE 802.16 中重要的一个密钥，KEK 和 HMAC_key 都是直接或者间接由它产生的，SS 再认证时也需要获得更新的 AK。AK 由 BS 负责产生与分发，如果 BS 产生的 AK 的随机性不够强的话，AK 包括以后的 TEK 都是不安全的。PKM 协议中的一个严重问题是 TEK 的密钥序号。PKM 协议中使用 2bit 的密钥序号来区分每一个 TEK，只需要进行 4 次密钥更新就使得密钥序号从 0 至 3 循环一次。使用这样的密钥序号来区分消息使得协议易受到重放攻击。由于协议本身不包含用于检测重放攻击的信息，如果发生重放攻击，当用户站再次使用以前用过的会话密钥和初始向量时，就可能会导致会话密钥和用户数据的泄露。要解决这个问题，只需简单地增加会话密钥序号的取值空间即可。当然不是盲目地增加，可以依据一个授权密钥的生命期内需要进行会话密钥更新的次数，一般使用 12bit 就足够了。

3.3　WiMAX 两种典型标准的安全机制分析

从 WiMAX 自身安全机制角度来看，WiMAX 分为 IEEE 802.16d 和 IEEE 802.16e 两个版本。前者为固定版本，后者为移动版本。固定版本在实现原理上可能会存在单向认证和加密算法方面的安全隐患，IEEE 802.16e 版本对这些问题做了改进，引入了一些最新的认证和密钥管理技术。这里主要对 IEEE 802.16d 和 IEEE 802.16e 这两个版本进行具体的分析。

3.3.1　IEEE 802.16d 标准

1. IEEE 802.16d 协议栈概述

IEEE 802.16d 的协议栈的空中接口由物理层和 MAC 层组成，如图 3-5 所示。为了支持多种物理层和各种关键技术在宽带无线接入中的应用，IEEE 802.16d 协议定义了较为复

杂的 MAC 层协议。

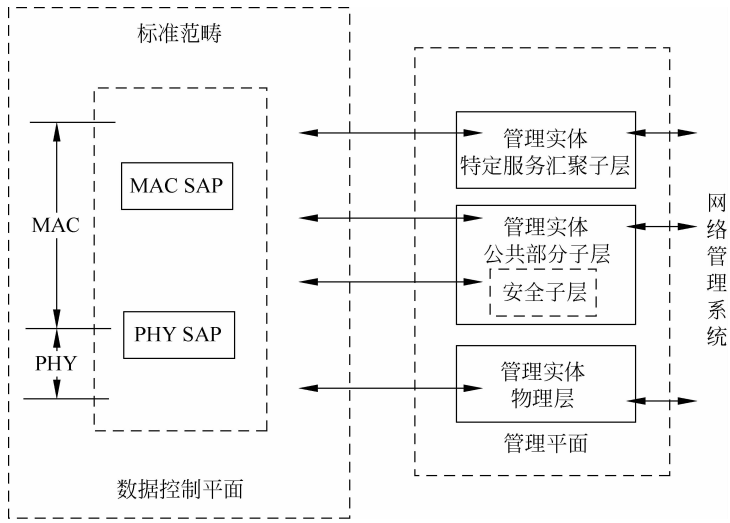

图 3-5 IEEE 802.16d 空中接口的协议栈

1) 安全子层

MAC 层包含一个单独可选的安全子层来提供认证、密钥交换及加密，这是 IEEE 802.16d 协议为了突出安全的重要性，专门在 MAC 中增加的一层。IEEE 802.16d 通过加密 SS 和 BS 之间的连接给用户提供具有保密性的接入无线网络的能力，此外 BS 通过加密相关的业务流禁止未经授权的访问。

IEEE 802.16d 标准的安全子层定义了两部分内容：

(1) 数据加密封装协议。该协议负责加密接入固定 BWA 网络的分组数据，定义了 IEEE 802.16d 支持的加密和鉴权算法，以及这些算法在 MAC PDU(Protocol Data Unit) payload 中的应用规则(加密只针对 MAC PDU 中的 payload 部分，MAC header 不被加密)。

(2) 密钥管理协议 PKM。PKM 负责从 BS 到 SS 之间密钥的安全分发、SS 和 BS 之间密钥数据的同步、对接入网络的限制。

2) MAC 公共子层 CPS

CPS 子层提供了 MAC 层的核心功能，包括系统接入、宽带分配、连接建立和维护等。

3) 特定服务汇聚子层 CS

CS 子层主要负责完成外部网络数据与 CPS 子层数据之间的映射。它将所有从汇聚层服务接入点(Convergence Sublayer Service Access Point，CS SAP)接收到的外部网络数据转化并且映射成 MAC SDU(MAC Service Data Unit)，并通过 MAC 服务接入点(MAC SAP)发送给 CPS 子层。

2. IEEE 802.16d 安全机制

身份认证是消除非法接入网络这种安全威胁的重要手段，是系统安全机制中的第一道屏障，它与密钥管理协议共同作为其他安全机制(如接入控制和数据加密)的前提。

IEEE 802.16d 协议的身份认证与密钥管理由 PKM 协议负责。PKM 协议采用公钥密

码技术实现 BS 对 SS 的身份认证、接入授权以及会话密钥的发放和更新。

安全关联 SA 是 BS 和一个或多个 SS 间共享的一组安全信息，目的是为了支持 IEEE 802.16d 网络间的安全通信。在 IEEE 802.16d 中实际上使用了两种安全关联，即数据安全关联(Data SA)和授权安全关联(Authorization SA)，但只明确地定义了数据安全关联。

1) 数据安全关联

数据安全关联分为初级、静态和动态三类。每个 SS 在初始化过程中都要建立一个初级安全关联，这是该 SS 与 BS 之间专有的；静态安全关联由 BS 提供；动态安全关联在数据传输过程中动态建立和消除，以响应特定服务流的发起和结束。

数据安全关联包含以下内容：

(1) 16bit 的 SAID(Security Association Identifier)标识，初级安全关联的 SAID 与用户站的基本 CID 相同。

(2) 加密模式：CBC(Cipher Block Chaining)模式中的 DES(Data Encryption Standard)。

(3) 加密密钥：两个 TEK(Traffic Encryption Key)用于加密数据。

(4) 两个 2bit 的密钥标识符，对应以上的两个 TEK。

(5) TEK 生命期：最小 30 分钟，最大 7 天。

(6) 64bit 的 TEK 初始化向量。

2) 授权安全关联

授权安全关联包含以下几项内容：

(1) 标识此 SS 的 X.509 数字证书。

(2) 160bit 的 AK(Authorization Key，授权密钥或授权码)。

(3) AK 的生命期：1～70 天，默认为 7 天。

(4) 下行链路的 HMAC(Hash function-based Message Authentication Code)密钥。

(5) 上行链路的 HMAC 密钥。

(6) 用于分发会话密钥的加密密钥 KEK(Key Encryption Key)。

(7) 一个已授权的数据安全关联的列表。

3. PKM 协议

PKM 协议采用客户机/服务器模型，SS 作为客户端来请求密钥，BS 作为服务器端响应 SS 的请求并授权给 SS 唯一的密钥；使用 CPS 子层中定义的 MAC 管理消息来完成上述功能；支持周期性地重新授权及密钥更新机制；使用 X.509 数字证书、RSA 公钥加密算法和强对称算法进行 BS 与 SS 之间的密钥交换。基于数字证书的认证方式进一步加强了 PKM 协议的安全性能。

1) PKM 协议的完整流程

PKM 协议的完整流程包括 6 条消息，分成两个阶段。

(1) 通知和授权。包含 3 条消息。SS 把设备制造商的公钥证书传给 BS，然后 SS 把自己的公钥证书传给 BS，BS 产生一个授权密钥，用 SS 的公钥加密后发给 SS。此过程完成了 BS 向 SS 传递 AK。随着 AK 的交换，BS 建立了 SS 的身份认证以及 SS 的授权接入服务，亦即在 BS 和 SS 之间建立了某种 SA。

具体地，通知和授权阶段的流程如图 3-6 所示。

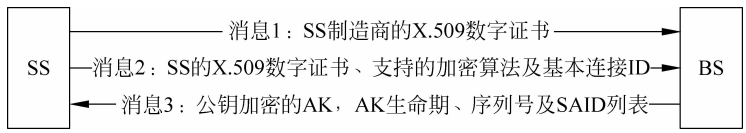

图 3-6　BS 和 SS 认证的第一阶段

SS 向 BS 发送一个认证消息（消息 1），该消息包含 SS 制造商的 X.509 数字证书；SS 向 BS 发送授权请求消息（消息 2），该消息包含生产商针对该设备发布的 X.509 数字证书、SS 支持的加密算法及 SS 的基本连接 ID；BS 验证 SS 的身份，决定加密算法，并为 SS 激活一个 AK，BS 将 AK 用 SS 的公钥加密后返回给 SS（消息 3）。SS 定时发送授权请求消息给 BS 来更新 AK。

（2）密钥协商。包含 3 条消息。BS 将会话密钥 TEK 安全分发给 SS。PKM 协议至少达到 4 个目标：BS 对 SS 的身份认证；BS 对 SS 的接入控制（通过 AK）；密码算法的协商；TEK 的分发。

在获得授权以后，在密钥协商阶段，SS 向 BS 请求 TEK，流程如图 3-7 所示。

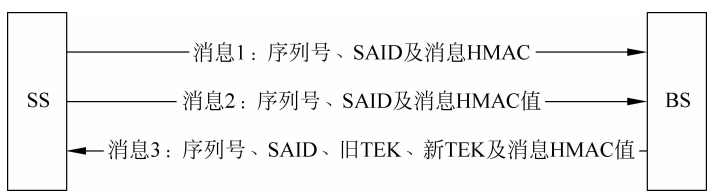

图 3-7　BS 和 SS 认证的第二阶段

BS 向 SS 发送 TEK 更新消息（消息 3，此消息是可选的）；SS 向 BS 发送 TEK 请求消息（消息 1）；BS 在收到请求消息后，生成 TEK，并通过响应消息发送给 SS（消息 2）。SS 定时发送密钥请求消息给 BS 来更新 TEK。

2）密码算法

PKM 协议中 3 种常用的密码算法：

（1）RSA 公钥算法，实现授权密钥的保密传送。

（2）DES 加密算法，实现会话密钥的安全分发。

（3）SHA-1 消息摘要算法，实现报文的完整性保护。

协议过程中，授权密钥是采用 SS 的公钥通过 RSA 算法加密的，保证了只有期望的用户可以解密得到此密钥。会话密钥采用 SS 公钥加密，或者由授权密钥推导的 KEK 采用 3-DES或 AES 加密传送，可有效抵抗攻击者的窃听。协议最后两条报文用 SHA-1 算法提供完整性保护。消息认证密钥同样也是由授权密钥推导得出的。

4. IEEE 802.16d 安全缺陷

PKM 协议具有报文少、效率高和安全算法易于实现的优点，但由于 PKM 协议是参考电缆接入系统的安全协议并结合 WMAN 网络的特点剪裁得到的，采用了共同的安全假设，使得基于 PKM 协议的 IEEE 802.16d 协议存在如下几个方面的缺陷。

1）单向认证

PKM 协议的前提是网络可信，因此只需网络认证用户，而无须用户认证网络，这样可能带来伪网络和伪基站攻击等形式的中间人攻击。

2）未明确定义授权安全关联

IEEE 802.16d 未明确定义授权安全关联，这会引起许多安全问题。例如，安全关联状态无法区分不同的授权安全关联实例，使得协议易受重放攻击，而不辨别 BS 身份也会受到重放或伪造攻击。

3）认证机制缺乏扩展性

SS 中的公钥证书是其设备证书，证书持有者字段为设备的 MAC 地址，缺少对其他认证机制的考虑。

IEEE 802.16d 还假定数字证书的发布是明确的，即没有两个不同的公钥/私钥使用方使用同一个 MAC 地址，但如果不能满足此假设，则攻击者可以伪装成另一方。

4）与 AK 相关的问题

所有的密钥协商以及数据加密密钥的产生依赖于 AK 的保密性，但是 IEEE 802.16d 协议没有具体描述认证和授权中 AK 是如何产生的。

另外，由于 AK 的生存时限较长（最长达到 70 天），而协议只使用一个 2bit 的密钥标识符作为密钥序列空间，即一个 AK 时限内最多只能使用 4 个 TEK，这使得攻击者可以使用已过期的 TEK 进行加密，然后重放数据，因此极易造成重放攻击。建议使用 4bit 或者 8bit 的密钥标识符作为密钥序列空间，或者缩短 AK 的生存时限以防止重放攻击。

5）PKI 部署困难

PKM 协议需要 PKI（Public Key Infrastructure，公钥基础设施）的支持，目前单纯的公钥证书验证合法即可信的方法无法面对今后大规模应用的安全需求。同时，解决不同制造商设备之间的互信问题也是一个不小的挑战。

PKM 中的密钥协商适合单播密钥，并不适于组播密钥，组播密钥必须采用网络统一分配的方式来发放和更新。

6）其他方面

密钥管理协议问题，如没有 TEK 有效性的保证；密码算法协商缺乏保护，可能造成降级攻击；TEK 授权和密钥协商请求由 SS 发起，可能带来拒绝服务攻击隐患；重认证机制不够有效，由 SS 发起的重认证并不能抵御会话劫持攻击。

3.3.2　IEEE 802.16e 标准

1. IEEE 802.16e 协议栈概述

IEEE 802.16e 物理层的实现方式与 IEEE 802.16d 的基本一致，主要差别在于 IEEE 802.16e 对 OFDMA 进行了扩展，可以支持 2048-Point、1024-Point、512-Point 和 128-Point，以适应不同载波带宽的需要。

IEEE 802.16e 标准主要规范了数据控制平面。数据控制平面由物理层（PHY）和媒体接入控制层（MAC）组成。MAC 层又分成了 3 个子层：特定服务汇聚子层（Service Specific Convergence Sublayer，SSCS）、公共部分子层（Common Part Sublayer，CPS）和安全子层

(Security Sublayer,SS)。其移动用户站 MAC 层的协议栈和 IEEE 802.16d 的相同。IEEE 802.16e 移动用户站的协议栈模型如图 3-8 所示。

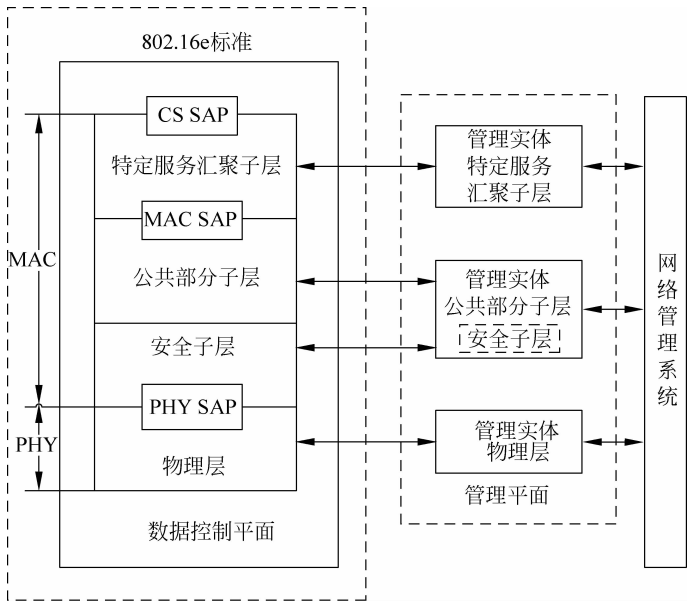

图 3-8 IEEE 802.16e 移动用户站的协议栈模型

汇聚子层的主要功能是负责将其业务接入点(SAP)接收到的外部网络数据进行转化和映射到 MAC 业务数据单元(SDU),并传递到 MAC 层的 SAP。公共部分子层是 MAC 层的核心部分,主要功能包括系统接入、宽带分配、连接建立和连接维护、移动和切换等。它通过 MAC SAP 接收来自汇聚子层的数据并分发到特定的 MAC 连接,同时对物理层上传输和调度的数据实施 QoS 控制。安全子层的主要功能是提供对通信实体和业务数据的认证、密钥交换和加解密处理等。

为了支持移动性,IEEE 802.16e 基站的协议栈和移动用户站有所不同,如图 3-9 所示。

它基于 IEEE 802.16d,针对移动性又定义了切换支持、省电的睡眠模式以及 EAP 支持的增强性安全机制等附加功能。此外,协议栈还增加了移动代理(Mobile Agent,MA)层。

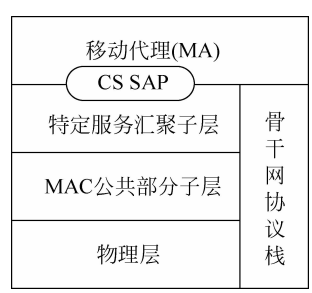

图 3-9 IEEE 802.16e 基站的协议栈模型

2. 帧结构的改进

为了使移动用户与固定用户共同工作和共享媒质,IEEE 802.16e 中采用了“固定”帧与“移动”帧交织的方式。TDD 模式下的 IEEE 802.16e 帧结构如图 3-10 所示。

时间轴被分为许多固定长度的超帧,每个超帧包括固定子帧和移动子帧。每个超帧以固定子帧的前导码起始,紧跟着下行链路前缀及携带着 DL-MAP 和 UL-MAP 消息的突发。

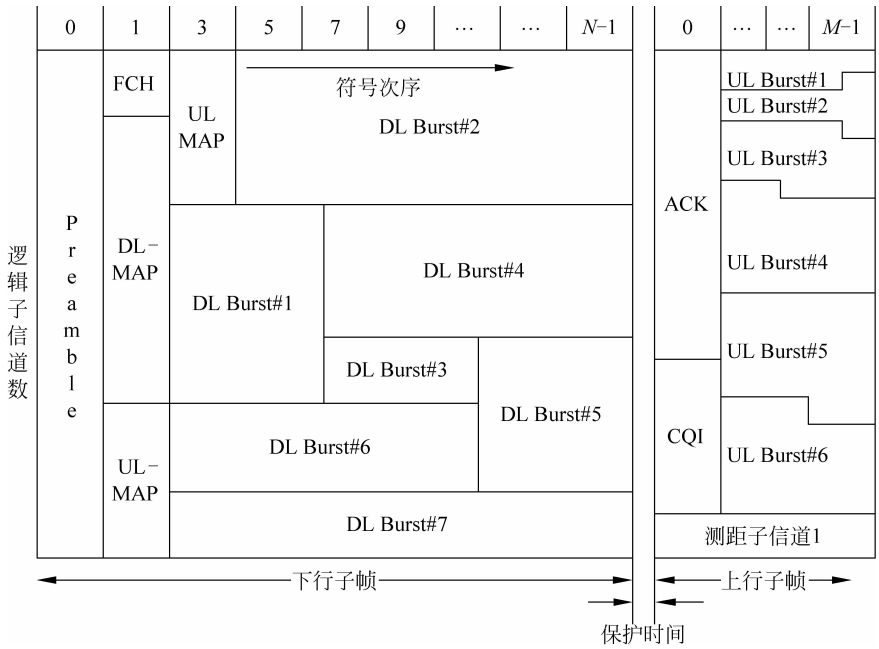

图 3-10　IEEE 802.16e 帧结构

固定子帧之间插入了移动子帧。每个移动子帧包含其自己的 DL-MAP 和 UL-MAP，以便上下行链路的带宽划分。超帧中固定子帧和移动子帧的划分十分灵活，在不同的超帧中会有所不同，因而移动子帧的长度是可变的。为了进行初同步，固定下行帧前缀或固定的 DL-MAP 都将包含最近的移动帧的起始位置信息。

3. IEEE 802.16e 对 IEEE 802.16d 安全机制的完善

IEEE 802.16e 是 IEEE 802.16 工作组正在制定的一个标准，它是对 IEEE 802.16d 的增强，因此保留了 IEEE 802.16d 的安全机制。为了解决 IEEE 802.16d 中存在的安全问题，IEEE 802.16e 将原来在 IEEE 802.16d 中 PKM 定义为 PKM version1，增加了 PKMv2，同时将 SS 变为移动站。IEEE 802.16e 在安全方面做了以下改进：

1）双向认证

IEEE 802.16 现行认证机制中最大的问题就是实行单向认证，因此有必要用双向认证代替单向认证，即增加基站数字证书，用 X.509 标识基站的身份，并用它对基站的公/私钥对进行数字签名。同时在传递证书的消息里增加了随机数字段，防止重放攻击。

2）可扩展认证框架

为了满足移动性带来的新安全的需求，IEEE 802.16e 中提出了新的 EAP 认证框架。EAP 是 IETF 制定的可扩展认证协议，最初用于点到点连接建立过程中的身份认证。EAP 协议的优点在于它只提供了一个认证框架，通过在其中填充各种现有或新设计的认证协议而适合不同的应用场景，不仅降低了链路层运算资源在安全上的开销，而且可以方便地支持现有的和未来的认证协议，从而使得整个接入认证系统具有高可扩展性和强安全性。常见 EAP 认证机制包括 EAP-MD5、EAP-TTLS、PEAP 和 LEAP 等，具体采用哪种机制可以在

认证时选定。

3）组播密钥管理

IEEE 802.16e 中考虑增加多播/组播业务的支持，因此设计了组播密钥的管理系统。MS 第一次向 BS 请求 TEK 时，密钥请求和密钥回应消息通过主管理连接来装载，而以后在更新 TEK 时，由 BS 在 TEK 过渡时间内周期性地进行。BS 将通过广播连接来向所有用户发送密钥回应消息，MS 不再需要向 BS 发送密钥请求消息。除非由于网络堵塞或其他原因，MS 在需要更新时没收到新的密钥才会主动发起密钥请求。

4）切换和漫游

支持切换是 IEEE 802.16e 针对移动接入做的修正中另外一个关键补充，能够在跨越不同边缘时保持连接不中断，是满足移动性的一个先决条件。支持硬切换和软切换两种类型。硬切换使用的是一种先打断后接通的方法，在任何时候用户设备连接到一个基站，比软切换要简单许多，但是反应时间较长一些。软切换可类比蜂窝网络中的切换技术，保证用户设备能保持切换足以支持数据业务。当然，切换过程中密钥的及时更新是关键。

另外，为了支持快速切换，安全部分增加了预认证部分。在 IEEE 802.11 中，预认证具有完备的前向安全性，但是要求切换小区之间有较大的重叠区域。由于需要重新进行全部的认证和密钥分发过程，在时间上有可能会有较大的延时。但在 IEEE 802.16e，预认证并不需要完整的认证过程，只是进行一个简单的消息交换，由认证服务器完成密钥预分发的过程。这种方式的好处是在切换前无须进行耗时的 EAP 认证过程，从而加快了切换的速度。

4. IEEE 802.16e 安全缺陷

（1）IEEE 802.16e 的保密子层还有很多地方没有定义完毕，例如，对于认证的体系结构没有给出说明或事例参考，只是罗列了一堆可以使用的认证方式。

（2）支持宏分集，用户可以从不同的基站接收信息，因此基站间密钥和数据的同步显得尤其重要。

（3）相对于端到端的单播，组播通信的安全问题更为复杂。IEEE 802.16e 的组播密钥管理并没有解决 implosion（信息爆炸问题），即由于一些原因，组播内所有 MS 的密钥没有及时更新，会同时向 BS 发起请求，这样会造成网络拥塞或 BS 来不及处理等问题。

3.4 WLAN Mesh 快速切换与漫游接入认证协议

通过上节的介绍已经知道，无线 Mesh 网络不同于传统 WLAN，无线 Mesh 网络的 AP 是通过无线链路连接形成骨干网络，而不是连接到有线网络基础设施。无线 Mesh 网络的 AP 不仅具有为覆盖范围内的终端用户提供接入服务的功能（即传统 WLAN 中的 AP 功能），而且具备路由转发其他 AP 数据的功能。对于用户终端设备而言，整个网络可看作是传统 WLAN 在更大区域范围内的扩展，用户仍以标准的 IEEE 802.11 方式无线接入 AP，保证了与现有协议标准以及终端设备的兼容性。对于 AP 而言，无线 Mesh 网络可看作一个无线多跳网络，每个 AP 节点均可与其临近 AP 节点直接通信。

当移动用户在无线 Mesh 网络中移动时，无线接入点的改变会导致数据链路层切换，进而触发网络中的路由更新（即网络层切换）。如果无线 Mesh 网络要为用户提供高质量的服

务，必须解决快速切换和漫游接入问题。

3.4.1　WLAN Mesh 切换

切换是一种重要的移动性管理功能，它是蜂窝系统所特有的功能，也是移动通信系统的关键特征之一。切换是移动用户在蜂窝间移动时为了保证业务的连续性而进行的改变业务信道的无线资源管理操作。

切换发生在一次通信过程中，当终端不通信时就不需要切换。从移动用户的角度来看，切换是将正在进行的呼叫或会话从一个物理信道转换到另一个物理信道的过程。也就是说，当一个移动用户正在进行通信时，此用户通过无线链路与一个基站建立连接；如果该用户移动到另一个基站的覆盖区域，则需断开到原基站的无线链路连接，且需建立一条到新基站的链路，以保持通信的连续性。

典型的切换过程分为 4 个阶段：测量控制、测量报告、切换判决和切换执行。测量控制阶段，网络通过发送测量控制消息通知移动用户进行参数测量；测量报告阶段，移动用户向网络发送测量报告消息，此消息中包含了移动用户检测得到的与切换判决相关的数据信息；切换判决阶段，网络根据移动用户测量报告中的相关信息（例如接收信号强度或其他准则）判决是否需要进行切换；切换执行阶段，移动用户和网络执行相应的信令流程，并根据信令做出相应的动作。

下面介绍无线 Mesh 网络用到的切换机制。

1. 数据链路层切换机制

1）WLAN 硬切换机制

在第三代移动通信系统中，移动节点可同时维持多条无线连接（软切换）以实现无缝切换。而 IEEE 802.11 标准规定网络中的移动节点任意时刻只能与一个 AP 关联，这就使得 IEEE 802.11 移动节点仅使用一条无线连接（硬切换）来实现链路层的切换过程。也就是说，IEEE 802.11 标准主要使用基本的硬切换方法，即没有采取什么措施，直接断开与旧 AP 的连接，再与新 AP 建立连接。根据 IEEE 802.11 协议规范，整个切换过程分为 3 个阶段，即 AP 的发现（Probe）阶段、认证（Authentication）阶段和重关联（Reassociation）阶段。WLAN 硬切换过程如图 3-11 所示。

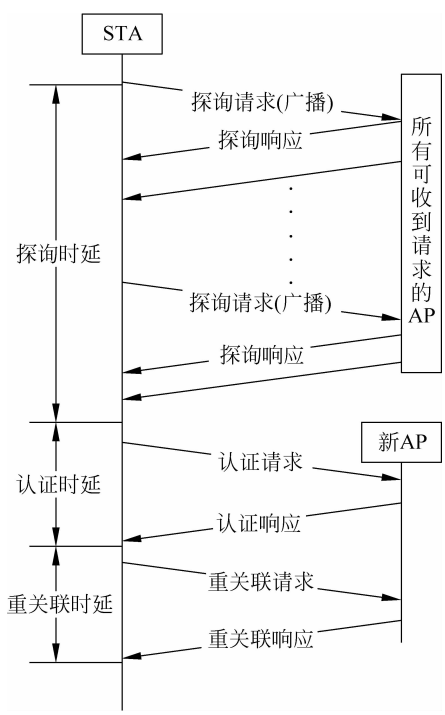

图 3-11　WLAN 硬切换

在移动过程中，STA 的无线链路质量如信号强度、信噪比等参数可能会下降，当其下降到某一特定阈值时，STA 就发起切换，并搜索新 AP。AP 信息的搜索是通过 MAC 层的扫描机制完成的，可分为被动搜索和主动搜索两种方式。在被动搜索方式下，AP 定期发送信标帧（Beacon）信号表明自

己的存在，该信标帧中包含与 AP 有关的信息，包括时间戳、容量、信标间隔、ESSID、业务指示表等。在主动搜索方式下，STA 通过发送探询请求帧主动搜索周围 AP。如果同时收到多个 AP 发来的探询响应帧或信标帧，则选择其中无线链路质量最好的 AP 作为目的 AP。

在认证阶段，STA 和 AP 之间交互认证信息，只有通过认证的 STA 才可以使用网络资源。IEEE 802.11 标准定义了两种认证方式：开放系统认证(Open System Authentication)和共享密钥认证(Shared Key Authentication)。开放系统认证是 IEEE 802.11 标准的默认认证机制，整个认证过程用明文进行认证请求和应答消息的交互，在认证请求中不包含与 STA 相关的认证信息，因而对 STA 不进行实际的认证。一般 STA 都能被认证成功，除非在 AP 中定义了访问控制列表、MAC 地址过滤等控制方式。共享密钥认证是可选的，它根据当前发送认证请求的 STA 是否拥有合法的密钥来决定是否允许接入，与开放认证相比，该方式花费时间比较多，安全性较好。无论采用何种认证方式，必要的步骤是 STA 先向 AP 发送认证请求信息，AP 经过认证后向 STA 发送认证成功或失败的响应。

认证过程完成后，STA 向 AP 发出重连接请求，若 AP 接受重连接请求，就会向 STA 做出重连接响应，于是 STA 可以通过新建立连接的 AP 进行通信，至此链路层切换完成。

2) WLAN 平滑切换机制

从上述硬切换过程可以看出，STA 并没有考虑切换过程中旧 AP 链路上的数据帧，这些数据帧有可能丢失。硬切换机制将丢包问题交给上层处理，从而对整个系统的性能造成影响。为了解决切换所引起的丢包问题，一些文献或标准草案提出了基于 WLAN 的平滑切换机制，也称为转发机制，如由 Lucent 带头起草的 IAPP 协议(IEEE 802.11f 协议)。IAPP 协议主要解决了 STA 移动带来的链路层通信问题，指定了 AP 之间及 IAPP 和高层网络管理实体之间信息如何交互。为了实现 STA 在同一网段上多 AP 之间的漫游功能，还规定了 AP 之间进行通信和交换切换相关信息的协议。WLAN 平滑切换步骤如图 3-12 所示。

从图 3-12 中可以看出，平滑切换机制与硬切换机制的大部分步骤是相似的，不同的是，平滑切换机制中新 AP 收到重关联请求帧后，新旧 AP 之间有一个交互过程，即新 AP 采用有线分布式网络(DS)中的 UDP 传输信息告知旧 AP 越区切换的发生，以及旧 AP 将与 STA 相关的信息和数据转发给新 AP 的过程。此时，STA 与新 AP 连接成功以后并不能立即接收数据，需要等到旧 AP 把数据转发到新 AP 以后才能收到数据，因而增加了切换时延。这种切换机制相对于硬切换而言，是以增加切换时延来换取低丢包率的。

2. 网络层切换机制

1) 移动 IP 切换机制

如图 3-13 所示，移动 IP 引入了三种新的功能实体：

(1) 移动节点(Mobile Node，MN)：每一个移动节点都有一个唯一的本地地址，当移动节点移动时其本地地址不变。

(2) 本地代理(Home Agent，HA)：位于移动节点本地网络上的一个路由器，当移动节点不在本地网络时，该路由器为数据包创建隧道以便把数据包传送到移动节点，并负责维护移动节点的当前位置信息。

(3) 外地代理(Foreign Agent，FA)：位于移动节点外地访问网络上的一个路由器，该路由器为注册节点提供路由服务。外地代理把本地代理通过隧道传送过来的数据包进行解

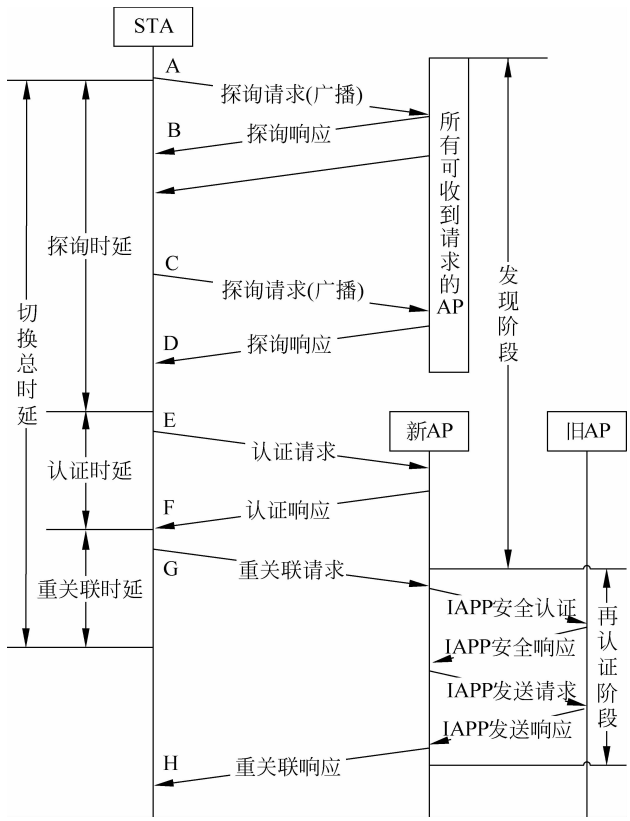

图 3-12　WLAN 平滑切换

封并把这些数据包传送到移动节点。对于从移动节点传送过来的数据包，外地代理作为该注册移动节点的默认路由器。

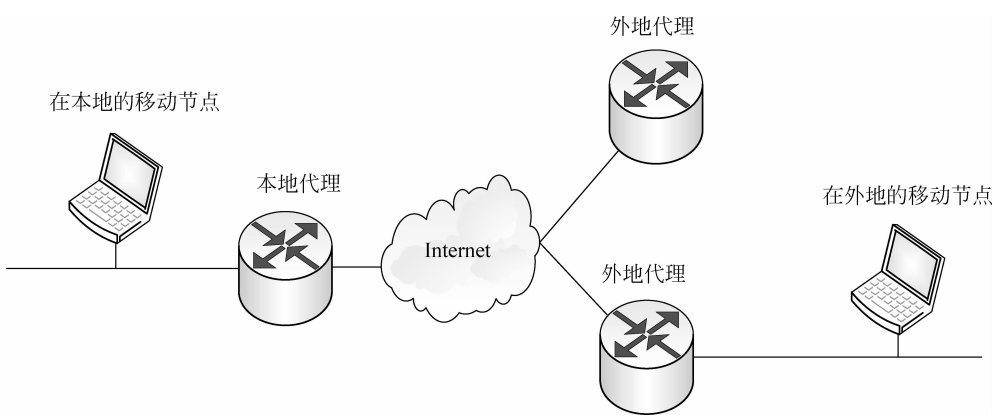

图 3-13　移动 IP 功能实体

移动 IP 的切换过程可分为两个阶段：代理发现阶段和注册阶段。本地代理和外地代理周期性地在它们作为移动代理的一条或多条链路上组播或广播称为代理通告的消息，通告它们与相应链路的连接关系。移动节点根据收到的代理通告消息，判断其是在本地链路

上或是在外地链路上。当连接在本地链路上，移动节点就像固定节点一样工作，不再利用移动 IP 的其他功能。当移动节点检测到从本地链路移动到外地链路，或从一个外地链路移动到新的外地链路时（也即发生切换），就需要一个代表其当前所在位置的转交地址。移动节点可以从外地代理通告消息中获得外地代理转交地址，或通过动态配置协议（DHCP）、手工配置等方法获得配置转交地址。移动主机在获得转交地址后，通过移动 IP 定义的消息向本地代理请求注册。本地代理确认后，将本地地址和相应的转交地址存放在绑定缓存中，并向移动节点发送注册应答。

本地代理和本地链路上的其他路由器通过与外地链路上的路由器交换路由信息，使得发送给移动节点本地地址的分组被正确转发到本地链路上。本地代理截取发往移动节点本地地址的分组，并根据分组的目的 IP 地址查找绑定缓存，获得移动节点的转交地址，然后通过隧道发送分组到移动节点的转交地址。最后，移动节点使用外地网络的路由器作为默认路由器，它发送的分组采用标准的路由机制通过外地网络的路由器直接发送给通信对端，无须采用隧道机制。

移动 IPv6 的切换过程与上述移动 IPv4 的切换过程基本相似，主要的区别是，移动 IPv6 中取消了外地代理的概念，移动主机可通过自动配置的方式获得转交地址，将转交地址向本地代理进行注册的同时，也向通信对端节点进行转交地址的注册，从而可避免移动 IPv4 中存在的“三角路由”问题。

2）微移动性切换机制

从上述基本移动 IP 的切换机制可以看出，移动 IP 切换过程包括移动检测过程和注册过程，切换时延相应分成两个部分：移动检测时延和移动注册时延。在一个频繁移动的环境中，注册产生的大量报文不仅会增加切换的时延，也会浪费较多的网络资源。因此，研究人员提出了微移动性解决方案。在微移动解决方案中，网络以层次结构的方式来划分，当移动节点在一个较小的、处于低层次的区域移动时，位置管理则可以本地处理。这种方案致力于减少因注册产生的往返时间，适用于移动节点当前访问的网络与其本地网络相距很远的情况。

3. 基于移动 IPv6 的改进切换机制

1）移动 IPv6 快速切换机制

IETF 工作组提出的移动 IPv6 快速切换技术是对移动 IPv6 协议的改进，可以加快 IPv6 移动节点的切换过程，减少已有通信连接的中断时间，保证通信流的实时传输。该技术通过提前注册，以及在新的外地网络切换未完成时通过前一个网络保持通信的方法，实现快速切换，以对实时业务提供支持。

移动 IPv6 快速切换可分为预先切换和基于隧道的切换两种机制。预先切换是指当 MN 和原接入路由器（PAR）还保持着第二层的连接时，就发起第三层的切换。基于隧道的切换是指 MN 与新接入路由器（NAR）建立起第二层的连接后，还不启动第三层的切换，而是在两个网络的接入路由器（AR）间建立隧道，PAR 将数据通过隧道转发到 MN。

2）层次移动 IPv6 切换机制

虽然在移动 IPv6 中没有外地代理，但是仍然需要有本地实体来协助移动 IP 切换。按照标准移动 IPv6 的要求，移动节点在外地网络中每移动到一个新的位置就要发送一个绑定

更新消息到本地代理或通信对端节点，而这个位置的变化可能相对来说很小，这个绑定更新的消息其实可以忽略，但按照要求却必须发送出去，这样很多冗余的绑定更新消息占据了有限的带宽，浪费了宝贵的网络资源，还会引发网络冲突，减少有效数据的传输。对此，IETF工作组又提出了 HMIPv6(Hierarchical Mobile IPv6)管理机制，引入了一个新的实体，称为移动锚接点(Mobility Anchor Point，MAP)，从微观移动性方面来解决这些问题，其核心是层次移动性管理，减少冗余信息，并将本地代理的移动性管理的能力下放一部分到区域代理中。

MAP 的引入仅仅是对移动 IPv6 协议的扩展，因此移动节点可根据情况选择是否使用 MAP，并且在任何无须使用 MAP 的时候，移动节点均可以停止对它的使用。这就给移动节点和移动网络带来了极大的灵活性。MAP 的加入使得 HMIPv6 解决方案独立于底层接入技术，允许在不同的接入网之间和内部实现数据的快速转发，大大提高了网络的吞吐量，降低了丢包率，增强了无线接口的实时业务能力。

3) 透明移动 IP 切换机制

上述所有基于移动 IP 的切换机制中，所有移动用户都具有本地地址和转交地址两个 IP 地址，并且所有机制都不能保证用户端的完全透明，也就是说，移动用户终端设备都需要额外实现一些支持移动性的协议(例如移动 IP、蜂窝 IP)。透明移动 IP(TMIP)机制的提出，旨在为移动用户提供跨网移动性支持的同时，无须对用户终端进行任何配置。这种机制的优点是，移动用户在切换过程中始终保持其 IP 地址不变，从而能够继续维持所有切换过程中正在进行的 TCP 会话。TMIP 与标准移动 IP 的主要区别是，用户终端无须额外实现任何特定的协议、配置或者对 IP 协议栈进行改进。

TMIP 最初是针对 WLAN 提出的。在使用 TMIP 机制的网络中，每个移动用户都拥有一个唯一的本地网络或者本地 AP，构成 DS 的网络能够跟踪移动用户的运动状况，这是由 TMIP 中定义的一个称为移动位置寄存器(MLR)的中心服务器来实现的。每个网络中只有一个 MLR，MLR 主要用于保存所有移动用户本地 AP 的相关信息以及移动用户的 MAC 地址、IP 地址与当前位置的映射表。当移动用户切换到外地 AP 时，外地 AP 向 MLR 发送一条查询请求报文，用于查找移动用户本地 AP 的相关信息。在获得本地 AP 信息之后，外地 AP 通过握手消息告知本地 AP 此时移动用户的新接入点，收到本地 AP 的握手应答消息后，外地 AP 增加一条新的到移动用户的单跳路由。同时，外地 AP 还向移动用户发送一条免费 ARP 响应消息，移动用户据此消息将其默认网关的 MAC 地址更新为外地 AP 的 MAC 地址。除此之外，发往移动用户的数据包首先被本地 AP 截获，然后由本地 AP 通过隧道转发到外地 AP；另一方面，若移动用户需要发送数据，则是通过常规的路由方式进行传输，并不需要本地 AP 的参与。值得注意的是，TMIP 使得移动用户即使在外地网络也可以使用其初始的 IP 地址并保持不变。但是，TMIP 与移动 IP 机制一样，仍存在着三角路由问题。

3.4.2　WLAN Mesh 漫游接入

目前公共无线局域网已经广泛部署，但这些局域网往往属于不同的管理者。用户在某个无线网管理中心注册后，可以在该无线网管理中心所属的区域(本地域)使用网络资源。当用户移动到一个他没有注册的区域(拜访域)时，如果拜访域和用户的本地域有相应的合约，用户就可以使用拜访域的网络资源，这种情况称为漫游。当移动设备漫游时，需要重新

进行认证。这要求无线 Mesh 网络的漫游接入协议必须能以较低的时延完成认证，建立共享会话密钥。

1. WLAN Mesh 客户端漫游接入认证协议的提出

目前 IEEE 802.11s 定义的 WLAN Mesh 不支持客户端的漫游，并且初始认证协议中，申请者和认证者的认证密钥是通过认证服务器产生的，导致申请者和认证者之后的所有通信完全可以被认证服务器获取；同时该协议中的基于共享密钥的认证方式不能保证前向保密性，一旦长期密钥丢失，由其保护的所有通信内容都将被泄露。在 EMSA 的基础上，利用三方 Diffie-Hellman 密钥交换和单独认证载荷技术提出了客户端漫游接入认证协议 WMR。该协议不但克服了上述缺陷，而且只需要 4 轮的协议交互便可以实现上述三者之间的相互认证和密钥确认，不需要四次握手进行密钥确认。并且新的协议将基于签名的认证方式和基于共享密钥的认证方式统一于单独的认证载荷，这样认证方式的改变并不影响认证协议的结构。

2. 漫游接入认证协议 WMR

WLAN Mesh 网络中的漫游涉及多个实体，包括移动节点(STA)、Mesh 接入点(MP/MAP)、外部认证服务器(F-AS)和本地认证服务器(H-AS)。STA 和 MP 具有预先定义的网络接入标识，并与 H-AS 共享安全关联；拜访域中提供接入服务的 MP/MAP 与 F-AS 间存在安全信道且相互信任；F-AS 和 H-AS 也存在安全信道。

对于漫游于不同区域的移动设备来说，攻击者更感兴趣的是发起者当前的身份信息及其访问历史，所以要对发起者提供身份保护。同时对于漫游认证协议而言，最大时延一般产生于 F-AS 和 H-AS 之间，故要求它们间的交互轮数尽量少。

1) 系统假定

认证者 A 是认证服务器 AS 管理的安全网络的合法实体，因此 A 和 AS 已经建立安全信道。拜访域中提供接入服务的 MP/MAP 与 F-AS 之间存在安全信道；F-AS 与 H-AS 之间存在安全信道；漫游设备 MP 与其 H-AS 之间存在共享密钥 HMK，该密钥由初始接入认证协议产生。

2) AS 的行为与能力

AS 是整个系统的控制者，控制整个系统中所有成员的加入和离开。申请者 S 只有通过某个认证者 A 被 AS 成功地认证和授权之后才能使用该认证者的服务。AS 的行为是可信的，它收到认证者通过安全信道传递来的认证请求之后会诚实地返回正确的应答。同时为了保证应答的真实性，AS 对应答消息进行签名(用公钥进行签名或者用共享密钥计算 MAC)，S 和 A 均相信具有正确签名的应答消息的权威性。

3) 协议设计思想

将申请者 S 的身份标识信息采用其与 H-AS 的共享密钥加密，实现对申请者的身份保护；申请者 S 与其拜访域内的邻居 MP 进行 DH 密钥交换，保证会话密钥的独立性，从而保证之后传输的数据不为任何第三方(甚至 H-AS 和 F-AS)获取；S 与 H-AS 之间采用基于共享密钥(或者签名认证方式)的认证模式，认证结果由安全信道发送给 F-AS，大大降低了认证开销。

漫游接入认证协议 WMR 如图 3-14 所示。

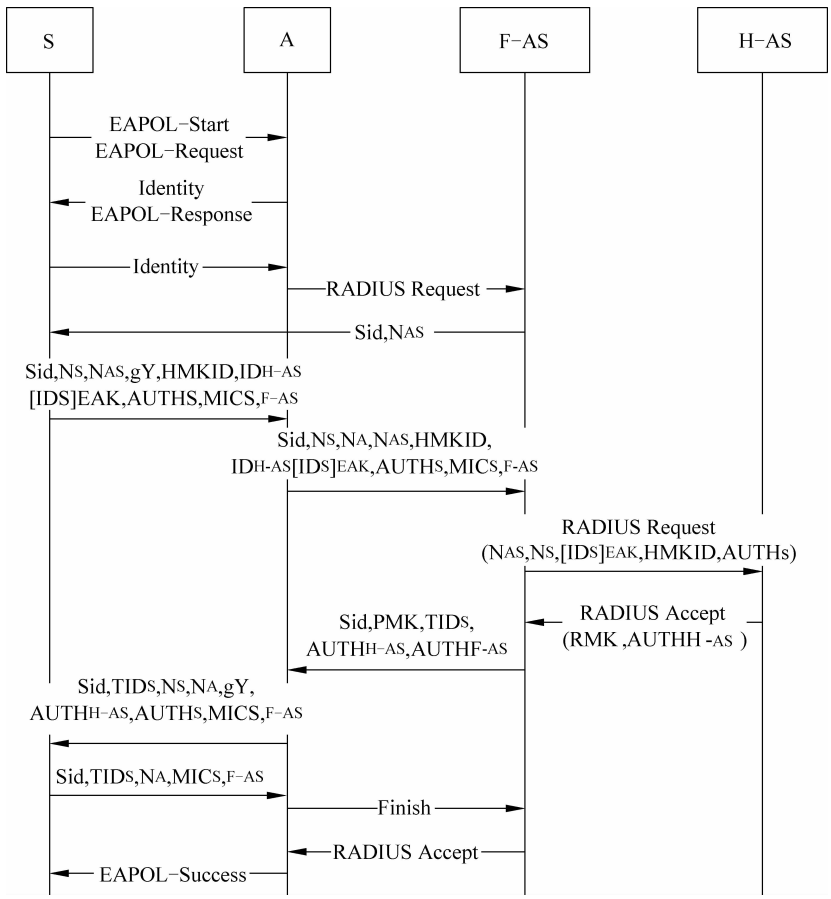

图 3-14　漫游接入认证协议 WMR

其中，Sid 为当前会话的标识符，由认证服务器产生，也可以由三方共同产生；gx、gy 分别为 S、A 用于 DH 密钥交换的临时公钥值；IDs、TIDs 分别为 S 的身份和 F-AS 临时分配给 S 的身份信息；$ID_{H\text{-}AS}$ 为 AS 的标识信息；SKs、$SKH_{\text{-}AS}$、$SKF_{\text{-}AS}$ 分别为 S、$H_{\text{-}AS}$ 和F-AS的长期私钥；HMK 为 S 和 H-AS 之间的共享密钥；HKD 为密钥推导函数；HMIC 为消息认证码计算函数；AUTHs、$AUTHH_{\text{-}AS}$、$AUTHF_{\text{-}AS}$ 分别为 S、H-AS 和 F-AS 的认证信息；MICs. H-AS、MICS. A、MICA. S 分别为 S 和 A 产生的消息认证码。

协议中的关键消息描述如下：

(1) F-AS 以 Sid、NAS 作为 WMR 协议的 Start 消息，该消息由 A 转发给 S。

(2) S 收到 WMR 协议的 Start 消息后，产生用于 DH 交换的临时私钥 x、临时公钥 gx，以及随机数 NS。然后计算漫游主密钥 RMK 和身份加密与认证密钥 EAK：

```
RMK|EAK = HKD(HMK, IDF-AS|NAS|NS)
```

同时利用 EAK 加密身份标识信息[IDS]EAK，产生身份认证信息 $AUTH_S$ 和消息认证码 MICS. F-AS，计算方式如下：

```
AUTHs = HMIC(EAK,M1)        (共享密钥认证);
AUTHs = SIGs(SKs,M1)        (签名认证模式);
MICs.F-AS = HMIC(RMK,M1|AUTHs);
M1 = Sid | Ns | NAS | gx | HMKID | IDH-AS | IDF-AS | IDA | [IDs]EAK
```

最后把消息(Sid | Ns | N_{AS} | gx | HMKID | IDH_{-AS} | [IDs]EAK | AUTHs | MICs.F-AS)发送给 A。

(3) A 收到上述消息后,首先验证 Sid 的有效性,验证通过后产生随机数 NA。然后 NA 和收到的 S 的消息通过安全信道一起发送给 F-AS。

(4) F-AS 收到 A 发送来的消息后,验证 Sid 和 N_{AS}的有效性,验证通过后把消息(N_{AS} | N_S | [IDS]EAK | HMKID | $AUTH_S$)通过安全信道发送给 H-AS。

(5) H-AS 收到 F-AS 发送来的消息后,根据 HMKID 检索相应的密钥 HMK,然后按与 S 同样的方式计算 RMK 和 EAK,并且解密 S 的身份标识信息,验证 $AUTH_S$ 的有效性。验证通过后产生计算:

```
AUTHH-AS.S = HMIC (EAK,M2) (共享密钥认证);
AUTHH-AS.S = SIG(SKH-AS,EAK,M2)(签名认证);
M2 = HMKID | NS | NAS | IDH-AS | IDF-AS
```

最后把消息(RMK | $AUTHH_{-AS}$)通过安全信道发送给 F—AS。

(6) F-AS 收到 H-AS 发送来的消息后,利用 RMK 验证之前收到的 MICS.F-AS 的有效性。验证通过后,产生 S 的临时访问标识 TIDS,计算会话主密钥 PMK 和消息认证码 $AUTHF_{-AS}$.S,计算方式如下:

```
PMK = HKD (RMK,Sid | NS | NA | TIDS | IDA);
AUTHF-AS = HMIC (RMK,M3) (共享密钥认证);
AUTHF-AS = SIG(SKF-AS,RMK,M3)(签名认证模式);
M3 = Sid | HMKID | NS | NA | NAS | TIDS | IDA | IDF-AS | MICH-AC.S
```

最后把消息(Sid | PMK | TID_S | $AUTHH_{-AS}$ | $AUTHF_{-AS}$)通过安全信道发送给 A。

(7) A 收到 F-AS 发送来的消息后,产生用于 DH 交换的临时私钥 y、临时公钥 gy,并且计算会话密钥 PTK 和消息认证码 MICA.S:

```
PTK = HKD (PMK,Sid | gxy | NS | NA | NAS | TIDS | IDA | IDF-AS);
MICA.S = HMIC (PTK,M4);
M4 = Sid | HMKID | NS | NA | NAS | gx | gy | TIDS | IDA | IDF-AS | MICH-AS.S | MICF-AS.S
```

最后把消息(Sid | TID_S | N_S | N_A | gy | $AUTHH_{-AS}$ | $AUTHF_{-AS}$ | MICA.S)发送给 S。

(8) S 收到 A 发送的消息后,先后验证 Sid、Ns、$AUTHH_{-AS}$和 $AUTHF_{-AS}$的有效性,验证通过后按与 A 相同的方式计算 PTK,并验证 MICA.S 的有效性。然后计算消息认证码 MICS.A:

```
MICA.S = HMIC (PTK,M5);
M5 = Sid | HMKID | NS | NA | NAS | gx | gy | TIDS | IDA | IDF-AS
```

最后把消息(Sid | TID_S | MICA.S)发送给 A。

3.5　本章小结

为了满足日益增长的宽带无线接入市场，无线城域网应用而生，随着其应用范围和影响力的不断扩大，其安全问题也得到了越来越多的关注。

本章从无线城域网的发展现状入手，在此基础上分别对 IEEE 802.16d 和 IEEE 802.16e 两种标准的无线城域网安全服务进行了分析，从协议分析的角度描述了无线城域网的发展趋势。之后又对 IEEE 802.16 系列标准与 IEEE 802.11 无线局域网标准进行了比较分析，并着重介绍了无线 Mesh 网络的体系结构及安全性分析。最后对 WLAN Mesh 的快速切换与漫游接入认证协议进行了介绍。

思考题

1. IEEE 802.16 保护子层的两个协议是什么？请分别叙述其工作原理。
2. 简述 IEEE 802.16d 安全机制的基本思想及特点。
3. IEEE 802.16d 有哪些安全缺陷？导致这些安全缺陷的原因分别是什么？
4. IEEE 802.16e 对 IEEE 802.16d 做出了哪些改进？请简述每个改进方面。
5. 针对无线 Mesh 网络的攻击有哪些？针对无线 Mesh 网络路由协议的攻击有哪些？
6. 无线 Mesh 网络的切换机制有哪些？请分别简述其原理。

参考文献

[1] 刘振华. 无线 Mesh 网络安全机制研究(博士学位论文). 安徽：中国科学技术大学，2011.

[2] 袁丽玲. 无线 Mesh 网络的无缝切换技术研究(硕士学位论文). 湖北：华中科技大学，2007.

[3] 张牧，严军荣. 802.11s 无线 mesh 网络研究进展与挑战. 计算机工程与应用，2010，46(22)：75-79.

[4] 孙炳龙. IEEE 802.16 无线城域网安全研究(硕士学位论文). 湖南：中南大学，2006.

[5] 严军荣. 无线 Mesh 网络信道资源分配关键技术研究(博士学位论文). 江苏：南京邮电大学，2009.

[6] 姜一川，王雪平，荆一楠，于建华. 无线城域网 IEEE 802.16 标准的安全性研究. 计算机应用与软件，2008，25(11)：253-255.

[7] 曹春杰，杨超，马建峰，朱建明. WLAN Mesh 漫游接入认证协议. 计算机研究与发展，2009，46(7)：1102-1109.

[8] 曹春杰. 可证明安全的认证及密钥交换协议设计与分析(博士学位论文). 陕西：西安电子科技大学，2008.

[9] 王育刚. 无线城域网的安全性分析(硕士学位论文). 北京：北京邮电大学，2007.

[10] 张子彬. WiMAX 无线网络安全接入技术的研究(硕士学位论文). 甘肃：兰州理工大学，2010.

[11] David Johnston, Jesse Walker. Overview of IEEE 802.16 Security. IEEE Security and Privacy, 2004, 2(3): 40-48.

[12] Thomas Hardjono. Security In Wireless LANS And MANS. London: arthch house, 2003.

[13] Ian F. Akyildiz, X. Wang, W. Wang. Wireless mesh networks: a survey. Computer Networks, 2005, 47(4): 445-487.

[14] FA Zdarsky, S Robitzsch, A Banchs. Security analysis of wireless mesh backhauls for mobile networks. Network Comput Appl, 2011.3, 34(2): 432-442.

[15] Rakesh Kumar Jha. A Journey on Wimax and its Security Issues. International Journal of Computer Science and Information Technologies, 2010, 1(4): 256-263.

[16] S. S. Dwivedi, S. Mishra, V.K. Mishra. Security Issues on Wimax Netwok. International Journal of Advanced Research in Computer Engineering and Technology, 2012, 1(6): 45-47.

[17] N Kahya-Abbaci, N Ghoualmi. Analysis of Security Weaknesses in IEEE 802.16. Signals and Telecommunication Journal, 2012.3, 1(1): 31-40.

[18] 802.16. (2001) IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[19] Nasreldin, M., Aslam, H., El-Hennawy. Wimax Security. In: 22h international conference on advanced information networking and application, IEEE.