基于IEEE802.16d的WiMAX安全研究思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_9F_BA_E4_BA_8EIEEE_c101_644137.htm 1、概述 IEEE 802.16d安全子层，提供鉴权、安全密钥交换和加密并定义了加密封装协议、密钥管理（PKM）协议，提供多种管理信息和业务的加密密钥和算法，并提供用户认证和设备认证两种认证方式。 2、体系结构 在802.16d版本中主要是通过在MAC（媒体接入控制）层中定义了一个安全子层来提供安全保障，如图1所示。安全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。其中数据加密封装协议定义了IEEE 802.16 d支持的加密套件，即数据加密与完整性验证算法，以及对MAC PDU载荷应用这些算法的规则。而密钥管理协议则定义了从基站向用户工作站分发密钥数据的安全方式，两者之间密钥数据的同步以及对接入网络服务的限制。 2.1 MAC层 IEEE 802.16d的安全规范主要存在于MAC层上。MAC层通过安全子层来实现安全策略，它提供了安全认证、安全密钥交换和加密，其目标是提供接入控制和保证数据链路的机密性。 在WiMAX网络中，当两个节点建立一个链接时，它们通过一系列协议来确保两者之间的机密性和惟一连接。基站（BS）和用户站（SS）之间的握手机制是通过MAC层中的安全子层完成的，其中包含5个实体：安全联盟（SA）、X.509证书、PKM认证、机密性密钥管理和加密。 根据WiMAX的最初草案文件，通过安全子层提供机密性、校验和加密，然而为了达到更好的安全保障，在无线协作骨干网中需要一种端到端的安全策略，它能提升最初草案中的安全机制。 2.2 物理层 IEEE 802.16d的

安全机制主要位于MAC层的安全子层，大部分运算法则和安全机制也都工作于此。物理层和MAC层是紧密联系在一起的，物理层上的安全策略主要以密钥交换、编码、解码的形式存在，用于对入侵者隐藏数据信息。另外一个与物理层相关的方面就是传输功率。未经授权频段的WiMAX与已获授权频段的 WiMAX的功率水平相比较低，其目的是减少干扰半径。 由于调制也是在物理层上完成的，基于这种考虑，其他安全措施也可以安置于物理层上。因为数据对应一个特定的接收者，不可能被其他接收者解码，所以扩频也可以作为一种安全措施。这意味着如果某个接收者不知道扩频码，即使拥有对数据的物理接入，也无法解码该数据包。 2.3 安全层 WiMAX安全规范的核心基于MAC层协议栈的安全子层，大部分的算法和安全机制都以MAC控制信息的形式存在于此。所以，WiMAX可以自由地选取工作在7层模型中更高层（如网络层、传输层、会话层等）上的安全机制，这些机制包括IP安全（IPSec）协议、传输层安全（TLS）协议和无线传输层安全（WTLS）协议。该子层提供接入控制，通过电子签名认证用户和设备，并且应用密钥变换进行加密以保证数据传输的机密性。当两个设备建立连接，协议发挥了确保机密性和认证接入设备的作用。BS和CPE（用户端设备）之间的协调通信通过MAC层的安全子层实现。 3、802.16d的安全关键技术 3.1 包数据加密 包数据加密有3种方式：3-DES EDE（encrypt-decrypt-encrypt）、AES ECB（electronic codebook）、RSA 1 024 bit，密钥在认证过程中分发，且动态更新。 3.2 密钥管理协议 PKM使用X.509数字证书、RSA公钥算法以及强壮的加密算法来实现BS和SS之间的密钥交换。 PKM协议使用

了C/S模型，在这个模型中，SS作为PKM的“ Client ”，向BS请求密钥资源，而BS作为PKM的“ Server ”，对这些请求进行响应，确保了每个SS只收到向它授权的密钥资源。PKM协议使用PKM-REQ和PKM-RSP等MAC管理消息完成这个过程。PKM协议用公钥加密机制在BS和SS之间建立共享密钥（AK），确保后续TEK（数据加密密钥）的安全交换。这种密钥分发的两层机制使得TEK的更新不再需要公钥操作的计算代价。 3.3 安全联盟 一个SA是BS和Client SS（一个或多个）之间为了支持在IEEE 802.16网络上的安全通信而共享的一个安全信息集合。定义了3种SA：基本SA、静态SA、动态SA。每个可管理的SS在初始化过程中都会建立一个基本SA。静态SA由BS提供。动态SA根据特定服务流的初始化和终止而建立和删除。静态SA和动态SA都能被多个SS共享。 一个SA的共享信息应该包括在该SA上使用的cryptographic suite，还可能包括TEK和初始化向量。SA的具体内容取决于SA的cryptographic suite，SA由SAID惟一标识。 每个可管理的SS应该与BS之间建立一个惟一的基本SA，该SA的SAID应该等于该SS的Basic CID。 一个SA的密钥资源（如DES密钥和CBC初始化向量）都有一个有限的生命周期。当BS将SA密钥资源发给SS时，它同时也提供了该密钥资源的剩余生存时间。在SS当前持有的密钥资源失效时，SS就会向BS请求新的密钥资源。如果在新的密钥收到之前，当前密钥失效，SS就会重新进行网络登录。 PKM协议规定了如何使BS和SS之间保持密钥同步。 3.3.1 SA与连接之间的映射 下列规则用于连接与SA之间的映射关系。 ◆所有的传输连接应该映射到一个已经存在的SA。 ◆多播传输连接可能映射到任意一个静态或动态SA。 ◆Secondary Management

连接应该映射到基本SA。 ◆Basic和Primary Managemnet连接不应该映射到任何SA。 在实际应用中，上述这些映射关系的实现是通过在DSA-XXX消息中包含SA的SAID和相应的CID来实现的。Secondary Management连接和基本SA之间的映射不必明确指出。 