中南财经政法大学
青年学术文库

新型无线网络的安全策略
——WiMAX网络安全

Security Strategy for New-style Wireless Network
—WiMAX Security

杨　璠◎著

世界图书出版公司

中南财经政法大学
青年学术文库

新型无线网络的安全策略
——WiMAX网络安全

Security Strategy for New-style Wireless Network
—WiMAX Security

杨　璠 ◎著

中国出版集团公司
世界图书出版公司
广州·上海·西安·北京

图书在版编目（CIP）数据

新型无线网络的安全策略：WiMAX 网络安全 / 杨璠著 . —广州：世界图书出版广东有限公司，2016.12
ISBN 978-7-5192-2313-7

Ⅰ . ①新… Ⅱ . ①杨… Ⅲ . ①宽带接入网—安全技术
Ⅳ . ① TN915.6

中国版本图书馆 CIP 数据核字（2017）第 001933 号

书　　名	新型无线网络的安全策略——WiMAX 网络安全 XINXING WUXIAN WANGLUO DE ANQUAN CELUE WiMAX WANGLUO ANQUAN
著　　者	杨　璠
策划编辑	孔令钢
责任编辑	黄　琼
装帧设计	黑眼圈工作室
出版发行	世界图书出版广东有限公司
地　　址	广州市新港西路大江冲 25 号
邮　　编	510300
电　　话	020-84460408
网　　址	http:// www.gdst.com.cn
邮　　箱	wpc_gdst@163.com
经　　销	新华书店
印　　刷	北京振兴源印务有限公司
开　　本	710mm × 1000mm　1/16
印　　张	14.75
字　　数	255 千
版　　次	2017年2月第1版　2017年2月第1次印刷
国际书号	ISBN　978-7-5192-2313-7
定　　价	46.00 元

《中南财经政法大学青年学术文库》

编辑委员会

前　言

计算机网络自从1969年于美国诞生，经过一系列的演变和发展，渗透到人类生活的每一个毛孔，成为人类生活不可缺少的组成部分。计算机网络发展之迅猛，网络技术的不断推陈出新，无论是从网民的增长速度还是网络覆盖的范围，无不展示着计算机网络强有力的生命力，并在人类面前多方位刷着存在感。

如果说网络的出现是由于二战后美苏对峙而进行的军事竞赛所需，那么现在人类对网络的迫切需求则是立足于现代生活。为了适应人类的需求，提供更灵活、更广范围覆盖、更高通信质量的服务，计算机网络朝着无线、移动、自组织方向发展。并逐步涌现出一批新型的网络，如能够实现完全自组织，且网络拓扑结构非常灵活的Ad hoc网络和Ad hoc类似的无线传感器网络wireless Sensor Network，以及通过分层既拥有控制节点又有自组织特性的Mesh网络等。作为更高传输速率、更大覆盖范围、号称最后一公里的无线技术标准，WiMAX网络既可以部署在传统的点到多点的无线网络结构上，也可以支持Mesh网络结构。

无线网络的应用扩展了网络用户的自由，然而，这种自由同时也带来了安全性问题。与传统有线网络不同，无线环境下的安全威胁更加复杂、多变，安全防御的困难更为突出。由于无线网络发展较晚，新近使用的许多技术还不够成熟，技术缺陷和安全漏洞在所难免。

在网络通信中，身份认证及密钥协商是网络系统安全的基础。IEEE 802.16系列标准的密钥管理协议PKM（Privacy Key Management）也主要分为身份认证和密钥协商两个部分，其发展也体现了安全性的演变：从最初单向认证，不能抵抗重放攻击、中间人攻击的PKMv1到IEEE 802.16e中可实现双向认证并引入了EAP（Extensible Authentication Protocol）认证协议的PKMv2，再到最新的IEEE 802.16M的PKMv3。

为了弥补 IEEE 802.16 系列标准认证机制中存在的缺陷和不足，美国电气电子工程师协会 IEEE 不断地做出改进。在 PKMv2 中通过 EAP 和 RSA 的组合，PKMv2 定义了 5 种认证模式。多种认证模式结合 EAP 的灵活性，使得 PKMv2 的认证机制具有良好的扩充性，但同时也带来了认证流程的多样化和复杂化。在 PKMv3 中对 PKMv2 做了一些改进，如通过添加消息验证码增加了管理消息完整性与一致性验证，同时保留并仅支持 EAP 认证方法。

但无论是 PKMv2 还是 PKMv3 都没有完整地定义如何进行认证模式下的 EAP 方法选取，因此从设备商的角度看，认证机制可以自行设计和优化，这无疑又将带来设备难以兼容的弊端。因此从商业化进程需求看，认证机制的进一步标准化迫在眉睫。

同时，除 IEEE 802.16 系列标准一直支持的 PMP 网络模式外，IEEE 802.16d 增加和开启了对 Mesh 网络模式的支持。Mesh 模式的引入有效地提高了网络的健壮性和网络通信的有效性及灵活性。然而，遗憾的是，IEEE 802.16 的系列标准中并未就 Mesh 模式下的新节点认证与密钥交换进行详细的定义。

为了解决该无线通信标准中存在的一些问题，本书从认证机制、密钥交换机制的设计、改进、优化角度出发，重点研究 WiMax 网络在初始化入网时，PMP 网络结构下单播初始化认证、重认证机制和密钥交换机制。在此基础上，还探讨了基于 Mesh 模式下的新节点入网认证和密钥交换流程的安全性，结合 IEEE 802.16 标准的相关定义设计了一套完整的基于 EAP 的入网认证方法和密钥交换策略。

研究的意义在于为 IEEE 802.16 标准的密钥管理协议的设计与实际应用提出可供参考的解决方案。由于作者的水平有限，写作中难免出现错误和纰漏，恳请广大读者们批评指正，感谢！

目　录

第一部分　背景知识

第二部分　基于 IEEE 802.16 standard 的 PMP 模式安全机制分析

第三部分 扩展部分

图目次

表目次

第一部分　背景知识