





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](http://www.gdst.com.cn)  
邮 箱 [wpc\\_gdst@163.com](mailto: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

---

版权所有，翻版必究  
(如有印装错误，请与出版社联系)

# 《中南财经政法大学青年学术文库》

## 编辑委员会

主任：杨灿明

副主任：吴汉东 姚莉

委员：（排名按姓氏笔画）

朱延福 朱新蓉 向书坚 刘可风 刘后振 张志宏

张新国 陈立华 陈景良 金大卫 庞凤喜 胡开忠

胡贤鑫 徐双敏 阎伟 葛翔宇 董邦俊

主编：姚莉

## 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1章 绪 论 .....	003
1.1 WiMAX 概述 .....	003
1.2 认证与认证协议 .....	012
1.3 IEEE 802.16 系列协议安全机制的研究状态 .....	016
1.4 本章总结 .....	022

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

第2章 PKMv2 认证机制及问题概述 .....	025
2.1 IEEE 802.16e 安全子层的框架结构和 PKM 定义 .....	025
2.2 PKMv1 认证协议缺陷及攻击方法 .....	026
2.3 PKMv1& PKMv2 安全关联比较 .....	034
2.4 PKMv2 认证模式 .....	034
2.5 PKMv2 密钥层次 .....	037
2.6 PKMv2 SA TEK 3-Way 握手与 PKMv1 TEK 交换的比较分析 .....	038

2.7	PKMv2 认证协议问题	045
2.8	本章小结	046
<b>第 3 章</b>	<b>PKMv2 EAP 认证方法需求分析与选取</b>	<b>047</b>
3.1	EAP 方法概论	047
3.2	IEEE 802.16e 对 EAP 使用方法的需求	049
3.3	现有的 EAP 方法	054
3.4	基于 16e 需求的 EAP 方法比对和选取	058
3.5	本章小结	063
<b>第 4 章</b>	<b>PKMv2 单一 EAP 及双 EAP 认证模式设计与改进</b>	<b>064</b>
4.1	EAP-based 认证模式：基于改进的 SPEKEY 的 EAP-TTLS 方法	064
4.2	EAP-Authenticated EAP 模式：改进的 AKAY 方法 + 改进的 SPEKEY	085
4.3	本章小结	112
<b>第 5 章</b>	<b>PKMv2 单一 RSA 模式及 RSA、EAP 混合模式认证协议     选取与设计</b>	<b>114</b>
5.1	IEEE 802.16e PKMv2 RSA 的消息类型	114
5.2	初始化接入单一 RSA 双向认证比对分析	116
5.3	RSA - Authenticated EAP 模式：RSA+ 改进的 EAP-SPEKEY 方法	123
5.4	RSA+EAP_Based 认证模式：RSA+ 改进的 EAP-AKAY 方法	131
5.5	本章小结	135
<b>第 6 章</b>	<b>PKMv2 5 种认证模式下的重认证机制设计与优化</b>	<b>137</b>
6.1	关键因素	138
6.2	一般性流程	140
6.3	5 种模式重认证设计	142
6.4	基于认证计数器的 RSA+Authenticated EAP 模式的重认证流程设计	144
6.5	基于 EAP-AKAY 方法的双 EAP 模式快速重认证优化设计	155



6.6 本章小结 .....	174
<b>第三部分 扩展部分</b>	
<b>第 7 章 IEEE 802.16 Standard Mesh 网络安全机制分析 .....</b>	<b>177</b>
7.1 Mesh 网络的特性 .....	177
7.2 Mesh 模式下的节点入网和同步过程 .....	179
7.3 WiMAX Mesh 网络入网认证和密钥交换过程及安全分析 .....	184
7.4 本章小结 .....	200
<b>第 8 章 总结和展望 .....</b>	<b>201</b>
8.1 全书总结 .....	201
8.2 未来研究的展望 .....	204
<b>附录 A 简略字表 .....</b>	<b>206</b>
<b>参考文献 .....</b>	<b>208</b>

## 图目次

图 1-1	PMP 网络结构 .....	007
图 1-2	Mesh 模式网络结构 .....	009
图 1-3	MMR 模式网络拓扑结构 .....	010
图 1-4	IEEE 802.16 协议框架 .....	010
图 1-5	单向函数的认证协议 .....	012
图 1-6	单钥体制下的认证过程 .....	013
图 1-7	双钥体制下的认证过程 .....	014
图 1-8	中间人攻击 .....	016
图 2-1	802.16e 安全子层 .....	026
图 2-2	PKMv1 RSA 认证流程 .....	026
图 2-3	PKMv2 RSA 认证消息格式 .....	027
图 2-4	PKMv1 TEK 交换消息 .....	027
图 2-5	PKMv1 TEK 交换流程 .....	028
图 2-6	PKMv1 伪冒 BS 攻击方法 .....	033
图 2-7	PKMv2 密钥层次 .....	037
图 2-8	IEEE 802.16e PKMv2 AK 生成办法 .....	038
图 2-9	PKMv2 SA TEK 3-Way 握手消息 .....	040
图 2-10	文献 [58] 简化的 PKMv2 SA TEK-3Way 握手 .....	042
图 2-11	客户端 SS 计算开销比对 .....	044
图 2-12	BS 端计算开销比对 .....	044

图 3-1 EAP 过程简图 .....	049
图 3-2 EAP-TLS 认证流程 .....	055
图 3-3 EAP-PEAP 简要流程图 .....	056
图 3-4 EAP-SIM 简要流程图 .....	058
图 3-5 用户认证 EAP 方法安全值比对 .....	059
图 3-6 设备认证方法安全值比对 .....	060
图 4-1 TTLS 的实体协议栈 .....	065
图 4-2 AVP 封装格式 .....	066
图 4-3 TTLS EAP 包的多层封装方式 .....	066
图 4-4 EAP-TTLS 的伪冒者(中间人)攻击 .....	068
图 4-5 针对文献[108]的伪冒者攻击 .....	073
图 4-6 本书提出的改进 EAP-SPEKE 方法 .....	074
图 4-7 改进 TTLS-SPEKE 方法下的伪冒者攻击 .....	076
图 4-8 改进 SPEKEY 与原有 SPEKE 的性能比对 .....	077
图 4-9 EAP-TTLS-SPEKEY 方法的 TLS 握手 .....	078
图 4-10 第二阶段 EAP-SPEKEY 方法 .....	080
图 4-11 AK 来源于 PMK(基于单一 EAP 授权) .....	081
图 4-12 EAP-TLS-MD5、EAP-TTLS-SPEKE、EAP-TTLS-SPEKEY 的认证消息比较 .....	083
图 4-13 识别伪冒者攻击消息轮回数比较 .....	084
图 4-14 客户端(服务器端)三种方法的计算开销比对 .....	085
图 4-15 IEEE 802.16e EAP-EAP 模式 .....	087
图 4-16 EAP-AKA 常用参数生成结构图 .....	089
图 4-17 EAP-EAP 模式 EAP-AKA 方法 .....	090
图 4-18 EAP-AKA 中间人攻击 .....	092
图 4-19 已有 EAP-AKA 改进的主密钥更新机制 .....	094
图 4-20 文献[115]改进前后客户端计算开销比对 .....	097
图 4-21 文献[115]改进前后服务器端计算开销比对 .....	097
图 4-22 EAP-AKAY 改进的密钥更新机制 .....	098
图 4-23 EAP-AKAY 和文献[115]客户端计算开销比对 .....	102

图 4-24	EAP_AKAY 和改进前 EAP_AKA 客户端计算开销比对 .....	103
图 4-25	EAP-AKAY 和改进前 EAP-AKA 服务器端计算开销比对 .....	103
图 4-26	EAP-AKAY 和文献 [115] 服务器端计算开销比对 .....	103
图 4-27	EAP-Authenticated EAP 的第一轮 EAP-AKAY 方法 .....	105
图 4-28	EAP-EAP 中的 EAP-SPEKE 方法 .....	107
图 4-29	源于 EIK 的 CMAC/HMAC .....	108
图 4-30	源于 PMK 和 PMK2 的 AK(双 EAP 认证) .....	108
图 4-31	总消息和认证交互消息数比对 .....	110
图 4-32	识别伪装攻击消息回数比对 .....	110
图 4-33	两种认证模式设计方法的客户端计算开销比对 .....	111
图 4-34	两种认证模式设计方法的服务器端计算开销比对 .....	112
图 5-1	双向 RSA 认证流程 .....	116
图 5-2	AK 仅来源于 PAK (基于 RSA 的授权密钥层次) .....	117
图 5-3	PKMv1/PKMv2 RSA 对应消息 .....	118
图 5-4	PKMv1 伪装 BS 攻击 .....	120
图 5-5	PKMv2 中间人侦听 .....	120
图 5-6	PKMv1&PKMv2 消息与交互轮回数比对 .....	121
图 5-7	PKMv1&PKMv2 客户端计算开销比对 .....	122
图 5-8	PKMv1&PKMv2 服务器端计算开销比对 .....	122
图 5-9	RSA+Authenticated eap 中 RSA 认证流程 .....	124
图 5-10	本书提出的改进 EAP-SPEKEY 方法认证流程 .....	125
图 5-11	RSA+Authenticated EAP 模式下产生 AK 的密钥层次 .....	126
图 5-12	EAP-AKAY+EAP-SPEKEY、RSA+EAP-SPEKEY 消息和交互轮回数 比对 .....	129
图 5-13	EAP-AKAY+EAP-SPEKEY、RSA+EAP-SPEKEY 发现伪装者回数 比对 .....	129
图 5-14	EAP-AKAY 和 PKMv2 RSA 客户端计算开销比对 .....	130
图 5-15	EAP-AKAY 和 PKMv2 RSA 服务器端计算开销比对 .....	130
图 5-16	仅使用 RSA 认证的 PKMv2 AK 产生层次 .....	134
图 5-17	仅使用 EAP Based 方法认证的 PKMv2 AK 产生层次 .....	135

图 6-1	PKMv2 重认证的一般性流程	141
图 6-2	双向 RSA 重认证流程	142
图 6-3	单一 EAP_Based 重认证流程	143
图 6-4	PAK 缓存	146
图 6-5	PMK 缓存	146
图 6-6	基于认证计数器的重认证流程	147
图 6-7	基于认证计数器的双向 RSA 重认证流程 (1)	148
图 6-8	基于认证计数器的双向 RSA 重认证流程 (2)	149
图 6-9	基于认证计数器的双向 EAP 重认证流程 (1)	150
图 6-10	基于认证计数器的双向 EAP 重认证流程 (2)	151
图 6-11	理想状态下基于计数器机制的认证交替	153
图 6-12	理想状态下的计数器机制与全认证机制	153
图 6-13	理想状态下的非计数器单一重认证	154
图 6-14	理想状态下的计数器 / 非计数器单一重认证比对	154
图 6-15	采用改进 EAP-AKAY 方法的快速重认证流程	158
图 6-16	时间 T 内的 FA 和 FSA 认证	160
图 6-17	总认证次数 E (n) 变化曲线组 1	164
图 6-18	总认证次数 E (n) 变化曲线组 2	164
图 6-19	总认证次数 E (n) 变化曲线组 3	165
图 6-20	总认证次数 E (n) 变化曲线组 4	166
图 6-21	总认证消耗 C (n) 随 AV 向量个数 K 变化曲线图	167
图 6-22	总认证消耗 C (n) 随 AV 向量个数 K 变化曲线图	168
图 6-23	总认证消耗 C (n) 随 AV 向量个数 K 变化曲线图	169
图 6-24	自适应机制和固定 K 值机制性能比较图	171
图 6-25	网络环境震荡时的 K 值选择	172
图 6-26	网络环境震荡时认证消耗比对	173
图 7-1	PMP 结构下新节点入网认证	184
图 7-2	Mesh 模式下新节点入网认证	185
图 7-3	EAP-TTLS-SPEKE 方法的握手阶段	186
图 7-4	EAP-TTLS-SPEKEY 方法隧道阶段	189

图 7-5 EAP-Authenticated EAP 的第一轮 EAP-AKAY 方法 .....	190
图 7-6 第二轮 EAP-AKAY 方法 .....	191
图 7-7 Mesh 模式下 PKMv1 TEK 交换流程 .....	193
图 7-8 Mesh 模式下 PKMv2 TEK 交换流程 .....	194
图 7-9 Mesh 模式下 PKMv3 TEK 交换流程 .....	196
图 7-10 Mesh 模式下相邻节点 TEK 交换流程 .....	197
图 7-11 Mesh 模式下改进后的相邻节点 TEK 交换流程 .....	198

## 表目次

表 1-1	IEEE 802.16 的系列标准	005
表 1-2	IEEE 802.16 主要标准特性	006
表 2-1	PKMv1 允许的加密套件	030
表 2-2	授权策略域字段含义	035
表 2-3	MS 在 SBC-REQ 和 PKMv2 SA-TEK-Request 中授权组合含义	036
表 2-4	SBC-RSP 取值组合含义	036
表 2-5	PKMv2 SA TEK Challenge 消息	038
表 2-6	PKMv2 SA TEK Request 消息	039
表 2-7	PKMv2 SA TEK Response 消息	039
表 2-8	客户端 SS 计算开销比对	043
表 2-9	BS 端计算开销比对	043
表 3-1	EAP Code 数据包格式	048
表 3-2	EAP Code 定义	048
表 3-3	EAP 数据包类型	048
表 3-4	EAP 认证方法的取值组合	050
表 3-5	PKMv2 EAP_Start 消息	052
表 3-6	PKMv2 EAP Transfer 消息	053
表 3-7	PKMv2 Authenticated EAP Transfer 消息	053
表 3-8	PKMv2 EAP Complete 消息	053
表 3-9	PKMv2 Authenticated EAP_Start 消息	054

表 3-10	EAP 方法比对 .....	059
表 4-1	EAP-TTLS 常用方法缺陷 .....	070
表 4-2	SPEKE 方法中的数学符号 .....	070
表 4-3	客户端计算开销比对 .....	084
表 4-4	服务器端计算开销比对 .....	084
表 4-5	EAP-AKA 方法中的数学符号 .....	088
表 4-6	改进前后客户端计算内容 .....	096
表 4-7	改进前后服务器端计算内容 .....	096
表 4-8	改进前后客户端计算开销比对 .....	096
表 4-9	改进前后服务器端计算开销比对 .....	096
表 4-10	客户端计算内容比对 .....	101
表 4-11	服务器端计算内容比对 .....	101
表 4-12	客户端计算开销比对 .....	102
表 4-13	服务器端计算开销比对 .....	102
表 4-14	客户端计算开销比对 .....	111
表 4-15	服务器端计算开销比对 .....	111
表 5-1	PKMv2 RSA Request 消息 .....	114
表 5-2	PKMv2 EAP Reply 消息 .....	115
表 5-3	PKMv2 RSA-Reject 消息 .....	115
表 5-4	PKMv2 RSA-Acknowledge 消息 .....	115
表 5-5	客户端计算开销比对 .....	121
表 5-6	服务器端计算开销比对 .....	121
表 5-7	客户端计算开销比对 .....	129
表 5-8	服务器端计算开销比对 .....	130
表 5-9	各种认证方法比对 .....	132
表 6-1	PMK 生存周期 .....	139
表 6-2	理想状态参数设计 .....	152
表 7-1	Key Request 消息 .....	193
表 7-2	PKMv3 Key_Agreement-MSG#1 消息 .....	195
表 7-3	PKMv3 Key_Agreement-MSG#2 消息 .....	195
表 7-4	PKMv3 Key_Agreement-MSG#3 消息 .....	195



# 第一部分 背景知识

