

网络空间安全专业规划教材

总主编◎杨义先

执行主编◎李小勇



无线通信安全

Security of Wireless Communication

主编 李晖



北京邮电大学出版社
www.buptpress.com

划教材

总主编 杨义先 执行主编 李小勇

无线通信安全

主编 李 晖



北京邮电大学出版社
www.buptpress.com

内 容 简 介

本教材全面深入地介绍了无线通信安全的相关基础理论,重点讨论了第二代到第四代移动通信系统及无线局域网中的各项关键安全技术。全书共分为3个部分:第1部分是入门篇,介绍了无线通信及无线通信安全的历史和基本概念;第2部分是理论篇,介绍了无线通信安全的理论基础,包括密码学概述、序列密码、分组密码、公钥密码、数字签名、认证理论基础和密钥管理等;第3部分是实例篇,介绍了各种无线通信网络(如GSM、GPRS、窄带CDMA、WCDMA、LTE、TETRA、WLAN、WiMax和蓝牙等)的安全技术,包括认证、加密和密钥管理等。每章最后给出了习题,便于读者巩固、总结和运用书中的知识。

本教材适合作为高校网络空间安全相关专业的本科及研究生教材,也可以作为对无线通信安全、密码学应用、信息安全等内容感兴趣的技术人员或科研人员的参考读物。

图书在版编目(CIP)数据

无线通信安全 / 李晖主编. -- 北京:北京邮电大学出版社, 2018.10
ISBN 978-7-5635-5500-0

I. ①无… II. ①李… III. ①无线电通信—安全技术 IV. ①TN92

中国版本图书馆CIP数据核字(2018)第159119号

书 名:无线通信安全
作 者:李 晖
责任编辑:刘 颖
出版发行:北京邮电大学出版社
社 址:北京市海淀区西土城路10号(邮编:100876)
发 行 部:电话:010-62282185 传真:010-62283578
E-mail: publish@bupt.edu.cn
经 销:各地新华书店
印 刷:北京博图彩色印刷有限公司印刷
开 本:787 mm×1 092 mm 1/16
印 张:21.75
字 数:560千字
版 次:2018年10月第1版 2018年10月第1次印刷



ISBN 978-7-5635-5500-0

定 价: 52.00 元

• 如有印装质量问题,请与北京邮电大学出版社发行部联系 •

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段，来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况，并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向 2, 密码学及应用, 为后三个方向 (系统安全、网络安全和应用安全) 提供密码机制; 它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向 3, 系统安全, 保证网络空间中单元计算系统的安全; 它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向 4, 网络安全, 保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全; 它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御 (攻防与对抗)、端到端的安全通信等内容。

方向 5, 应用安全, 保证网络空间中大型应用系统的安全, 也是安全机制在互联网应用或服务领域中的综合应用; 它主要研究关键应用系统安全、社会网络安全 (包括内容安全)、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看, 网络空间安全一级学科主要由五个模块组成: 网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块 1, 网络空间安全基础知识模块, 包括: 数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块 2, 密码学基础理论知识模块, 包括: 对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块 3, 系统安全理论与技术知识模块, 包括: 芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块 4, 网络安全理论与技术知识模块, 包括: 通信网络安全、无线通信安全、IPv6 安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块 5, 应用安全理论与技术知识模块, 包括: Web 安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心理学、安全控制论、安全系统论等。不过值得庆幸的是，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平，从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据服务与安全隐私技术》《数字内容安全》《量子计算与后量子密码》《无线通信安全》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理（第3版）》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科提供更有力的支撑。

杨义先

教授、长江学者

国家杰出青年科学基金获得者

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

Foreword 前言

Foreword

自 20 世纪 70 年代末第一代通信系统问世以来，移动通信技术发展迅速，特别是与有线因特网连接起来后，移动通信网络为用户提供“永远在线”、高速率的网络服务，用户不仅可以使⽤移动终端随时、随地与人交流，还可以使⽤移动终端浏览新闻、查询信息、网上购物、导航及进⽣移动支付等。

与此同时，移动通信系统普遍采⽤的无线通信技术本身固有的开放性使得它更容易受到监听、滥⽤等安全威胁，导致手机用户的通信记录（语音、短信、通话人、通话时间等信息）以及存储的机密信息（如银行账号、密码等重要资料）等的泄露，虚假基站也使得用户容易收到垃圾短信等。这些由于使⽤无线设备或技术带来的安全问题使⽤户的隐私和通信安全受到了极大的威胁，不仅破坏了社会的和谐与稳定，而且还威胁到了国家安全。因此，研究无线通信安全技术的理论、设计和完善无线通信网络安全是无线通信技术飞速发展的前提，是保障通信安全的关键，是国家信息安全建设的重点。

本教材深入地介绍了无线通信安全的相关基础理论与各项关键技术，主要围绕无线通信网络安全展开讨论。我们将从认识无线通信技术开始，逐步介绍无线通信网络所面临的安全威胁、要达到的安全要求和采⽤的安全措施。正如密码学理论是信息安全的基础一样，大部分的无线通信网络的安全措施依赖于密码学的基本理论，如加解密理论和认证理论。因此，本教材将密码学的基本理论作为无线通信安全的理论基础，进⽣较为详细的介绍，并在此基础上介绍目前主要的无线通信网络（包括第二代移动通信系统、第三代移动通信系统、LTE 系统、无线集群通信系统、无线局域网、无线城域网等）采⽤的安全技术。

本教材共分为 3 个部分：第 1 部分是入门篇，由第 1 章和第 2 章组成，分别介绍无线通信和无线通信安全的历史、分类和基本概念；第 2 部分是理论篇，由第 3~11 章组成，主要介绍无线通信安全的理论基础——密码学的基础知识，包括密码学概述、序列密码、分组密码、公钥密码、数字签名、认证理论基础和密钥管理等；第 3 部分是实例篇，由第 12~21 章组成，包括 GSM、GPRS、窄带 CDMA、WCDMA、LTE、TETRA、WLAN、WiMax 和蓝⽣等的安全技术，主要介绍这些实际通信系统如何进⽣认证及管理密钥，如何保证传输的信息不被非法破译和篡改等。

本教材较完整地描述了无线通信系统中的信息安全基本理论与技术，读者既可以按顺序阅读本教材，也可以先跳过理论篇，直接阅读实例篇，而在理解某类无线通信系统安全技术遇到困难时再翻看前面的理论知识。本教材可以作为本科高年级学生和研究生专业教材，参考学时为68学时。此外，本教材也可以供从事相关领域研究的科研人员阅读参考。相信本教材的深度和广度，可以方便不同层次的读者从书中的理论及技术论述中找到感兴趣的知识或答案。

本教材的策划以及主要章节的撰写、统稿和修改工作由李晖负责，特别要说明的是，本教材的完成是在作者2010年编写的《无线通信安全理论与技术》一书的基础上进行的，相关章节的内容保留了该书的部分内容，因此对参加编写该书的相关人员的辛勤工作表示感谢！另外，潘雪松、陈泽、马倩华、王鑫添、范立岩、陈泽伦、冯皓楠和韩明哲参与了全书的校对工作，北京邮电大学出版社的马晓仟为本教材的出版付出了辛勤而有效的劳动，在此一并表示感谢。

本教材在编写过程中还参阅了国内外同行的大量文献，在此向这些文献的作者表示由衷的感谢！

鉴于无线通信及信息安全的理论与技术处在不断发展和完善之中，加之作者水平所限，本教材难免出现疏漏，甚至错误，恳请各位专家、学者和热心读者指正，并提出宝贵意见。我的电子邮箱是 lihuill@bupt.edu.cn。

李 晖

2018年6月于北京邮电大学

Contents 目录

Contents

第 1 部分 入门篇

第 1 章 无线通信入门	3
1.1 无线通信的历史	3
1.2 无线通信基本技术	6
1.2.1 射频基础	6
1.2.2 无线传输介质	7
1.2.3 传统无线技术	8
1.3 无线通信网络分类	10
1.4 无线通信的研究机构和组织	12
1.4.1 国际电信联盟	12
1.4.2 美国联邦通信委员会	13
1.4.3 欧洲邮电通信管理协会	13
1.4.4 电气和电子工程师协会	14
1.4.5 Wi-Fi 联盟	15
1.4.6 中国通信标准化协会	15
1.5 本章小结	16
1.6 习题	17
第 2 章 无线通信安全入门	18
2.1 无线通信安全历史	18
2.2 无线通信网的主要安全威胁	20
2.2.1 对传递信息的威胁	21
2.2.2 对用户的威胁	22
2.2.3 对通信系统的威胁	23
2.3 移动通信系统的安全要求	23
2.4 移动通信系统的安全体系	24
2.4.1 安全服务	25
2.4.2 安全需求	27

2.4.3 安全域	27
2.5 本章小结	28
2.6 习题	28

第 2 部分 理论篇

第 3 章 密码学概述	31
3.1 密码学的基本概念	31
3.2 密码体制的分类	33
3.3 古典密码简介	34
3.3.1 单码加密法	34
3.3.2 多码加密法	35
3.3.3 经典多图加密法	36
3.3.4 经典换位加密法	36
3.4 密码体制安全性	37
3.5 本章小结	38
3.6 习题	39
第 4 章 序列密码概述	40
4.1 序列密码的基本概念	40
4.1.1 序列密码的起源	40
4.1.2 序列密码的概念	41
4.1.3 序列密码与分组密码	42
4.2 序列密码的分类	42
4.2.1 同步序列密码	42
4.2.2 自同步序列密码	44
4.3 密钥流生成器的结构	44
4.4 本章小结	46
4.5 习题	46
第 5 章 序列密码的设计与分析	47
5.1 序列的随机性概念	47
5.2 线性移位寄存器的结构与设计	49
5.2.1 移位寄存器与移位寄存器序列	49
5.2.2 n 阶反馈移位寄存器	50
5.2.3 m 序列及其随机性	52
5.2.4 LFSR 的软件实现	55
5.3 线性反馈移位寄存器的分析方法	56
5.3.1 m 序列密码的破译	57
5.3.2 序列的线性复杂度	58

5.3.3 B-M 算法	59
5.4 非线性序列	61
5.4.1 非线性反馈移位寄存器序列	61
5.4.2 利用进位的反馈移位寄存器	61
5.4.3 非线性前馈序列	63
5.5 本章小结	66
5.6 习题	66
第 6 章 典型序列密码	68
6.1 A5 算法	68
6.2 RC4 算法	70
6.3 PKZIP 算法	72
6.4 SNOW 2.0 算法	74
6.5 WAKE 算法	76
6.6 SEAL 算法	77
6.7 本章小结	79
6.8 习题	80
第 7 章 分组密码	81
7.1 分组密码理论	81
7.1.1 分组密码概述	81
7.1.2 分组密码算法的设计原则	82
7.1.3 SPN 结构简介	83
7.1.4 密钥扩展算法的设计原则	84
7.2 典型分组密码算法	85
7.2.1 DES 算法	85
7.2.2 AES 算法	93
7.2.3 国际数据加密算法	100
7.3 密码运行模式	103
7.3.1 电子密码本模式	103
7.3.2 密码分组链接模式	105
7.3.3 密码反馈模式	106
7.3.4 输出反馈模式	108
7.3.5 计数器模式	109
7.3.6 最后分组的填充	110
7.3.7 选择密码模式	110
7.4 本章小结	112
7.5 习题	112

第 8 章 公钥密码	114
8.1 公钥密码的基本概念	114
8.1.1 问题的复杂性理论	114
8.1.2 公钥密码的原理	115
8.1.3 公钥密码的使用	116
8.2 RSA 密码体制	117
8.2.1 RSA 算法描述	117
8.2.2 RSA 算法举例	118
8.2.3 RSA 算法实现	118
8.2.4 RSA 算法的常见攻击	118
8.3 椭圆曲线密码体制	119
8.3.1 椭圆曲线概念	119
8.3.2 椭圆曲线密码算法	121
8.3.3 椭圆曲线密码算法实例	122
8.3.4 椭圆曲线密码算法的安全性	123
8.4 NTRU 公钥密码	124
8.4.1 NTRU 基于的困难问题	124
8.4.2 NTRU 算法描述	125
8.4.3 NTRU 算法举例	126
8.5 本章小结	127
8.6 习题	127
第 9 章 数字签名	128
9.1 数字签名的基本概念	128
9.2 常用数字签名技术简介	129
9.2.1 RSA 数字签名方案	129
9.2.2 DSS 数字签名标准	130
9.3 特殊数字签名	132
9.3.1 一次性数字签名	132
9.3.2 群签名	132
9.3.3 代理签名	133
9.3.4 盲签名	134
9.3.5 多重数字签名	134
9.4 本章小结	136
9.5 习题	136
第 10 章 认证理论基础	137
10.1 认证的基本概念和认证系统的模型	137
10.2 认证函数	138

10.2.1	信息加密函数	138
10.2.2	信息认证码	140
10.3	杂凑函数	142
10.3.1	杂凑函数的定义	142
10.3.2	杂凑函数的基本用法	143
10.3.3	杂凑函数的通用模型	143
10.3.4	构造杂凑函数	145
10.3.5	对杂凑函数的攻击	145
10.4	MD4 算法和 MD5 算法	146
10.4.1	算法简介	146
10.4.2	MD5 算法描述	147
10.4.3	MD5 算法的安全性	148
10.5	安全杂凑算法	149
10.5.1	SHA-1 算法描述	149
10.5.2	SHA-1 算法安全性	150
10.6	安全协议	151
10.6.1	安全协议的概念	151
10.6.2	安全协议的安全性	153
10.6.3	安全协议的设计规范	154
10.6.4	协议的形式化证明	155
10.6.5	安全协议的常见攻击和相应对策	156
10.7	身份认证协议	158
10.7.1	身份认证的概念	158
10.7.2	零知识身份认证协议	159
10.7.3	询问应答协议	160
10.7.4	认证协议向数字签名方案的转换	161
10.8	本章小结	161
10.9	习题	162
第 11 章	密钥管理	163
11.1	密钥管理的基本概念	163
11.1.1	密钥的组织结构	163
11.1.2	密钥的种类	165
11.1.3	密钥的长度与安全性	165
11.1.4	穷举攻击的效率与代价	166
11.1.5	软件破译机	167
11.2	密钥生成	167
11.3	密钥分配与协商	169
11.3.1	密钥分配	169
11.3.2	密钥协商	172

11.4	密钥更新	174
11.5	密钥的保护、存储与备份	174
11.5.1	密钥的保护	174
11.5.2	密钥的存储	175
11.5.3	密钥的备份	176
11.6	单钥体制下的密钥管理系统	176
11.7	本章小结	178
11.8	习题	178

第3部分 实例篇

第12章	GSM 安全	181
12.1	数字保密通信	181
12.1.1	数字保密通信的概述	181
12.1.2	保密数字通信系统的组成	182
12.2	GSM 简介	183
12.3	GSM 的安全目标和安全实体	184
12.3.1	GSM 的安全目标	184
12.3.2	GSM 的安全实体	185
12.4	GSM 的鉴权机制	186
12.4.1	GSM 标识码	186
12.4.2	GSM 的鉴权过程	187
12.5	GSM 的加密机制	188
12.6	GSM 的匿名机制	189
12.7	GSM 的安全性分析	189
12.8	本章小结	190
12.9	习题	190
第13章	GPRS 安全	191
13.1	GPRS 简介	191
13.2	GPRS 系统的鉴权	193
13.3	GPRS 系统的加密机制	193
13.4	GPRS 系统的匿名机制	194
13.5	安全性分析	194
13.6	本章小结	195
13.7	习题	195
第14章	窄带 CDMA 安全	196
14.1	CDMA 系统简介	196
14.2	CDMA 系统的鉴权	197

14.2.1	CDMA 系统标识码与安全参数	197
14.2.2	CDMA 系统的鉴权	198
14.3	CDMA 系统的空口加密	200
14.4	CDMA 中的密钥管理	202
14.4.1	A-Key 的分配和更新	202
14.4.2	SSD 的更新	202
14.5	本章小结	203
14.6	习题	204
第 15 章	WCDMA 安全	205
15.1	3G 系统概述	205
15.2	3G 系统的安全结构	206
15.3	认证与密钥协商机制	207
15.3.1	认证与密钥协商协议	207
15.3.2	认证和密钥协商算法	209
15.3.3	AKA 的安全性分析	211
15.4	空中接口安全机制	211
15.4.1	f_8 算法概述	212
15.4.2	f_8 算法的构造方式	213
15.4.3	f_9 算法概述	214
15.4.4	f_9 算法的构造方式	215
15.4.5	KASUMI 算法	216
15.5	核心网安全	221
15.5.1	安全域的划分	221
15.5.2	MAP 安全	222
15.5.3	IPsec 安全	224
15.6	应用层安全	227
15.6.1	WAP 概述	227
15.6.2	WAP 安全	229
15.7	WPKI 介绍	232
15.7.1	WPKI 组成	232
15.7.2	WPKI 中的证书	233
15.7.3	WPKI 的模式	233
15.8	本章小结	235
15.9	习题	235
第 16 章	LTE 安全	236
16.1	LTE 概述	236
16.2	安全威胁及要求	238
16.3	安全架构	239

16.4	用户身份标识与鉴权	240
16.5	密钥管理	241
16.6	传输安全机制	244
16.6.1	机密性保护算法	244
16.6.2	完整性保护算法	245
16.7	本章小结	246
16.8	习题	247
第 17 章	TETRA 安全	248
17.1	数字集群系统及其标准简介	248
17.2	TETRA 标准及网络结构	249
17.2.1	TETRA 标准	249
17.2.2	TETRA 系统结构	250
17.2.3	TETRA 标准中定义的接口	251
17.2.4	TETRA 帧结构	252
17.3	TETRA 系统的基本鉴权过程	253
17.3.1	SwMI 对 MS 的单向鉴权	253
17.3.2	MS 对 SwMI 的单向鉴权	254
17.3.3	MS 与 SwMI 的双向鉴权	255
17.4	空中接口加密	257
17.4.1	空中接口加密在 TETRA 中的层次	257
17.4.2	安全类别	257
17.4.3	空中接口加密的主要算法	258
17.4.4	空中接口加密中的密钥	260
17.5	TETRA 系统端到端安全	261
17.5.1	端到端安全的总体架构	261
17.5.2	加密算法	262
17.5.3	语音加/解密与同步	263
17.5.4	短消息加密	264
17.5.5	密钥管理	265
17.5.6	具体实施的建议	266
17.6	本章小结	266
17.7	习题	266
第 18 章	WLAN 安全	268
18.1	无线局域网及安全简述	268
18.1.1	无线局域网结构	268
18.1.2	无线局域网安全标准现状	269
18.2	IEEE 802.11 中的安全	270
18.2.1	WEP 的工作原理	270

18.2.2 针对 WEP 的分析	273
18.3 IEEE 802.1x 认证	275
18.3.1 IEEE 4802.1x 认证简介	275
18.3.2 EAP 协议	276
18.4 IEEE 802.11i 中的安全	278
18.4.1 密钥管理	278
18.4.2 TKIP 加密机制	280
18.4.3 CCMP 加密机制	281
18.4.4 WRAP 加密机制	283
18.5 本章小结	285
18.6 习题	286
第 19 章 WiMax 安全	287
19.1 WiMax 简介	287
19.1.1 WiMax 技术优势	287
19.1.2 WiMax 安全威胁	288
19.2 WiMax 安全框架	289
19.2.1 WiMax 协议模型	289
19.2.2 WiMax 安全框架	289
19.3 WiMax 安全机制	290
19.3.1 IEEE 802.16 固定接入系统的安全机制	290
19.3.2 IEEE 802.16 移动接入系统的安全机制	292
19.3.3 IEEE 802.16-2004 和 IEEE 802.16-2005 的比较	296
19.4 本章小结	297
19.5 习题	297
第 20 章 蓝牙安全	298
20.1 蓝牙技术简介	298
20.2 蓝牙安全概述	299
20.3 密钥生成	300
20.4 认证	300
20.5 加密	301
20.6 本章小结	305
20.7 习题	305
第 21 章 传感器网络安全	306
21.1 无线传感器网络概述	306
21.1.1 无线传感器网络的体系结构	306
21.1.2 无线传感器网络的特征	307
21.2 无线传感器网络安全挑战与措施	309