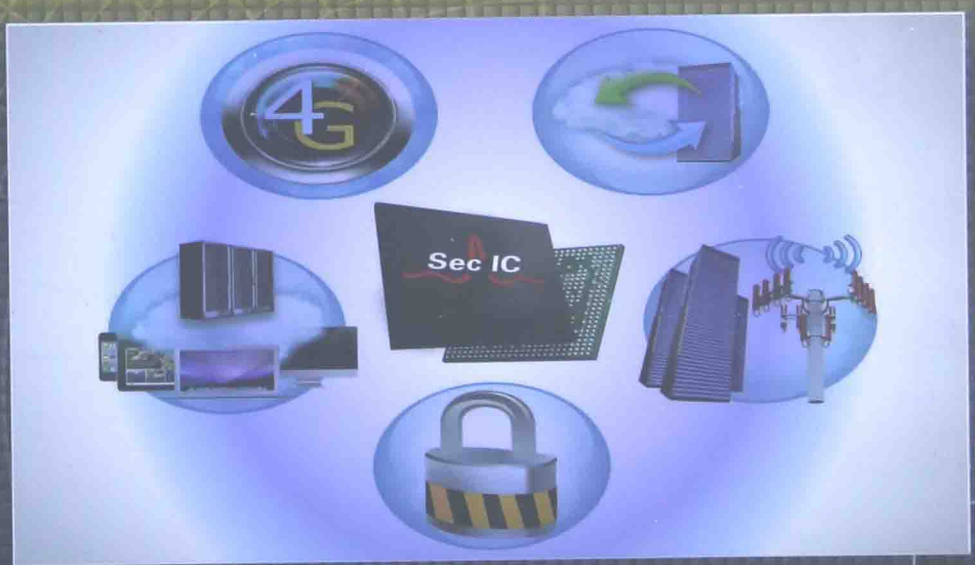
国防科技图书出版基金

网络与信息安全前沿技术丛书

无线通信网络安全技术

祝世雄 罗长远 安红章 郁滨 编著

Security Technology of Wireless Communication Networks



国防工业出版社
National Defense Industry Press

国防科技图书出版基金

网络与信息安全前沿技术丛书

祝世雄　罗长远　安红章　郁滨　编著

无线通信网络安全技术

Security Technology of Wireless Communication Networks

如果您想了解无线通信网络安全技术发展历程，领略其设计之美，从而启发自己的系统设计思维，那么本书是您最佳的选择之一。全书涵盖主流无线通信网络安全技术，从基本原理、详细方案、安全效能和演进关系等方面进行全方位剖析，内容全面翔实，描述深入浅出，既可作为系统性学习的教材，也可作为按需查阅的工具书。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

无线通信网络安全技术 / 祝世雄等编著. —北京：国防工业出版社,2014.9
(网络与信息安全前沿技术丛书)
ISBN 978-7-118-09548-7

Ⅰ.①无… Ⅱ.①祝… Ⅲ.①无线电通信-通信网-安全技术 Ⅳ.①TN92

中国版本图书馆 CIP 数据核字(2014)第 203058 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　印张 25　字数 475 千字
2014 年 9 月第 1 版第 1 次印刷　印数 1—3000 册　定价 129.00 元

致　读　者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需

要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	王　峰			
副主任委员	吴有生	蔡　镭	杨崇新	
秘　书　长	杨崇新			
副秘书长	邢海鹰	贺　明		
委　　员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	陆　军	芮筱亭
	李言荣	李德仁	李德毅	杨　伟
	肖志力	吴宏鑫	张文栋	张信威
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

在过去的十余年内，无线通信技术经历了巨大的变化，无线网络越来越融入人们的生活，在日常生活、办公及抢险救灾等应用中发挥着极其重要的作用，对人类的生产力产生了前所未有的推动力。但是，无线网络在给我们带来便利的同时，它的安全问题也日益突显。由于无线传输介质的开放性，无线通信网络面临网络、终端、信息等多个层面的安全威胁，如何基于无线通信设备计算能力、储存能力受限和用户移动等特点，实现无线通信网络及其应用的安全，是当前无线通信系统快速发展的基础和关键所在。

无线通信技术虽日新月异，但其演进路线日渐清晰，系统梳理无线网络体系结构，分析各种无线通信安全防护技术特点，从工程应用角度介绍无线通信网络安全技术及其发展趋势，已成为学习和掌握无线通信网络安全内涵的重要途径。本书立足顶层，从体系、系统、技术三个层面对无线通信网络安全技术进行论述，既介绍了传统无线通信系统的安全防护方案，又针对未来发展趋势对多个关键技术和领域进行了重点介绍和分析。全书涉及个人移动通信系统、宽带无线接入网络、无线自组织网络、无线个域网络、移动 IP 和异构无线网络等方面，内容全面翔实、体系结构清晰、偏重实际应用，有利于全面掌握技术动态和发展趋势。

全书共分 7 章，第 1 章为无线通信网络安全基础，介绍无线通信网络组成、面临主要威胁及主要安全防护措施；第 2 章为个人移动通信系统安全，介绍 2G、3G 和 4G(LTE)等无线通信系统安全技术；第 3 章为宽带无线接入网络安全，介绍 WLAN、WiMAX、无线 Mesh 等无线网络安全技术；第 4 章为无线自组织网络安全，介绍 Ad hoc 网络、WSN 网络密钥管理、路由安全等技术；第 5 章为无线个域网络安全，重点介绍蓝牙、ZigBee 安全技术及其实现机制；第 6、7 章分别对移动 IP 安全技术和异构无线网络安全技术的基本原理、关键技术和发展趋势进行介绍。本书由祝世雄组织编写与统

稿，并主笔第1、3章编写，罗长远主笔第2、4、7章编写，安红章主笔第6章及部分第2章内容编写，郁滨主笔第5章编写。

本书是由保密通信重点实验室和解放军信息工程大学在相关科研项目和教学实践的基础上，通过系统地分析、总结和整理而编著。电子科技大学李乐民院士、西安电子科技大学王育民教授在本书的编写过程中提出了宝贵的建议，保密通信重点实验室田波、曾兵、张文政、刘义铭和中国电子科技集团公司第三十研究所谢上明、李毅、王运兵、陈浩在本书编写过程中给予了大力支持，重点实验室汤殿华、吴颖、吴开均、董新峰，及解放军信息工程大学研究生李伟、邢洪智、霍士伟、王利涛等先后参加了资料搜集、文字整理等工作，谨在此向他们表示衷心的感谢。同时还要感谢所有直接或间接为本书做出贡献的同事和朋友，以及国防工业出版社的领导和编辑为本书付出的辛勤劳动。

本书可作为研究生和高年级本科生的教材，也可供科学技术界和产业界从事无线通信网络安全技术研究和开发的科研人员、工程技术人员阅读参考。在撰写过程中，虽已尽最大努力将所引用的资料名称列入参考文献条目，但是由于本书的资料内容不仅来源丰富，而且数量较大，难免出现疏漏或错误，故在此向相关作者表示深深的歉意。由于作者水平有限，本书存在诸多不足之处，恳请读者予以批评指正。

目　录

Contents