Broadview
www.broadview.com.cn

安全技术大系

无线网络安全

中国密码学会 组编
任伟 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

无线网络安全

中国密码学会 组编
任伟 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书全面系统地论述了各种形态无线网络中的关键安全问题及典型的解决方案和协议。内容翔实（涵盖了无线网络的各种形态）、注重跟踪国内外最新发展动态（如无线体域网、物联网等），选材新颖（如 6LoWPAN、4G、无线 Mesh 网络等）、突出重点问题和典型方法（如 WSN 密钥管理、MANET 安全路由等），强调论述的逻辑性（先全貌后重点、先网络架构后安全架构）、系统性及选材的合理性，叙述语言通俗易懂，文字流畅。为提高启发性，该书注重对原理的归纳和总结，注重对安全设计方法的归纳和分析。

全书内容主要包括无线局域网安全、无线城域网安全（含 WiMAX 和无线 Mesh 网络）、无线广域网（如 2G、3G、4G 通信网络）安全、无线个域网安全、无线 VoIP 安全、无线体域网安全、RFID 安全、无线传感器网络安全、移动自组织网络安全、车载自组织网络安全，以及无线物联网安全。每个章节给出进一步的阅读建议和参考文献，指导读者进一步研究学习。

本书适合无线网络安全研究者、安全技术爱好者、无线网络开发人员参考学习。

图书在版编目（CIP）数据

无线网络安全 / 中国密码学会组编，任伟编著. —北京：电子工业出版社，2011.9
（安全技术大系）
ISBN 978-7-121-14104-1

Ⅰ. ①无… Ⅱ. ①中… ②任… Ⅲ. ①无线网－安全技术 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字（2011）第 138976 号

策划编辑：毕　宁　bn@phei.com.cn
责任编辑：许　艳
特约编辑：赵树刚
印　　刷：北京东光印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：14.5　字数：312 千字
印　　次：2011 年 9 月第 1 次印刷
印　　数：3000 册　定价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

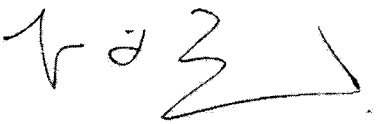
服务热线：（010）88258888。

序　言

任伟博士编著的《无线网络安全》一书系统归纳了各种无线网络中的安全问题及其基本对策，内容全面，包括无线局域网、无线城域网、无线广域网、无线个域网、无线自组网、无线传感网、无线车载网等。部分主题具有前瞻性，如无线体域网、4G、无线物联网的安全问题等。

该书注重区别不同无线网络的个性安全问题，并根据该类无线网络的特征归纳了相应的典型解决方案，如 3G 的 AKA 协议、无线传感网的密钥管理、无线自组网的安全路由问题、无线车载网的隐私保护等，启发读者体会无线网络安全问题，以及解决这些问题的思路。书中提出的解决无线网络安全问题的一般思路，以及对物联网安全架构的构想等具有一定的理论和实践意义。

本书取材独具一格，论述简明扼要、突出重点，内容翔实，组织结构合理，分析透彻，可读性强。该书的出版改变了目前尚无全面论述各种形态无线网络的安全问题与对策书籍的现状，必将有助于推动我国无线网络安全的科研及教学工作。



灵创团队带头人
北京邮电大学信息安全中心主任
灾备技术国家重点实验室主任
国家级教学名师、博士生导师、长江学者

前　言

本书是中国密码学会组织编写的年度信息安全书目，同时也是国内第一本全面介绍各种形态无线网络安全的关键问题及其典型解决方案的研究参考书。

随着无线网络的飞速发展和应用剧增，以及计算机网络和无线通信网络的融合，传统网络安全书籍已经不再满足当前网络实际应用状况的需求，研究者和信息安全从业人员急需一本全面讲解无线网络安全的书籍。目前国内外针对各种形态的无线网络安全原理与协议的参考书尚不多见，因此编写全面论述这一主题的书迫在眉睫。

本书在写作的过程中遵循了以下思路。

（1）内容编排循序渐进、由浅入深、兼顾广度和深度。整书的编排先给出无线网络安全的全貌，便于读者了解无线网络安全问题的共性之处和一般解决思路。然后每章依次探讨了特定无线网络的安全问题。同时每章中首先给出本章无线网络的基本架构、网络特征、安全威胁与需求的全貌，然后针对几个典型安全论题深入分析解释。

（2）选材新颖、理论联系实际。理论的论述突出共性和一般原理（如对接入网围绕 AKA 机制来论述），实践部分强调新颖性（如对最新协议栈 802.16d、802.11s 等的解释）。理论与实际结合时，突出无线网络安全设计方案的一般规律，便于指导将来的安全设计。论述了当前无线网络安全中的几个典型的实际问题与解决方案，如 3G 网络安全、无线局域网安全、WiMAX 安全。

（3）注重启发性，包括原理的总结和归纳、协议设计方法的比较和分析。指出了各种形态无线网络安全问题的相似性，注重问题本质的提炼，启发思考解决未来的无线网络安全问题。

（4）部分高级论题归纳了无线网络安全研究的新进展，如无线体域网安全、车载自组织网络安全，以及无线物联网安全。特别是讨论了几个比较新的课题，如 VANET 隐私保护问题、无线 Mesh 网络安全、体域网安全机制，以及物联网安全问题。对从事该方面研究的研究人员及安全技术研发人员具有一定参考价值。

全书共分 12 章：第 1 章是无线网络安全的概述；第 2 章介绍无线局域网（WLAN）安全；第 3 章介绍无线城域网（WMAN）安全；第 4 章介绍无线广域网（WWAN，如 2.5G、3G 通信网络）安全。第 5 章介绍无线个域网（WPAN）安全；第 6 章介绍无线 VoIP 安全；第 7 章介绍无线体域网（WBAN）安全；第 8 章介绍 RFID 网络安全；第 9 章介绍无线传感器网络（WSN）安全；第 10 章介绍移动自组网（MANET）安全；第 11 章介绍车载自组网（VANET）安全；第 12 章介绍无线物联网（IOT）安全。

本书面向的主要对象包括从事无线网络安全研究的研究人员，学习无线网络安全相关课程

的高等院校信息安全类、密码学类、计算机类、信息工程类专业本科高年级学生和研究生，以及从事无线网络安全技术研发、应用和管理的工程技术人员。

本书得到了中国密码学会的大力支持和推荐，受到了中国科协学会学术部 2010 年项目资助（JXJY2010005-B2），在此表示感谢。成书的过程中，得到了中国密码学会办公室及北京邮电大学杨义先教授的大力支持，也得到了电子工业出版社信息安全项目总监毕宁编辑的大力帮助，在此表示衷心的感谢。感谢研究生叶敏协助绘制了部分插图。由于作者水平有限，不足之处在所难免，在此衷心希望读者提出意见和建议。笔者的 E-mail 是 weirencs@cug.edu.cn。

任　伟

2011 年 2 月于武汉南望山

任伟： 博士，博士后，副教授，中国密码学会会员，CCF 高级会员，ACM 会员，IEEE 会员，中国人工智能学会数字内容安全专委会委员，CCF YOCSEF 武汉学术委员。取得华中科技大学计算机软件与理论博士学位，2004—2008 年先后在香港科技大学计算机系、美国内华达大学（UNLV）计算机学院、美国伊利诺理工大学（IIT）电子与计算机工程系从事信息安全方面的研究。2009 年进入中国地质大学（武汉）信息安全系，现为系主任。曾获得香港科技大学研究资助、UNLV 博士后研究奖金和 IIT 研究生院长奖金。参与包括香港高科技发展基金、NSF、863、973 等多个项目。在国内外期刊如《中国科学》等发表学术论文 30 余篇，其中第一作者被 EI 或 SCI 检索 20 多篇。已出版专（译）著 3 部。并担任多个国际期刊的编委和国际学术会议程序委员会委员。

目　录

第 1 章　无线网络安全概述

1.1　无线网络概述

1. 无线网络的分类

总的来说，由于覆盖范围、传输速率和用途的不同，无线网络可以分为无线广域网、无线城域网、无线局域网、无线个域网和无线体域网。

（1）无线广域网（Wierless Wide Area Network，WWAN）：主要是指通过移动通信卫星进行的数据通信，其覆盖范围最大。代表技术有3G及未来的4G等，一般数据传输速率在2Mb/s以上。由于3GPP和3GPP2的标准化工作日趋成熟，一些国际标准化组织（如国际电信联盟ITU）将目光瞄准了能提供更大无线传输速率和灵活统一的全IP网络平台的下一代移动通信系统，也称为后3G、增强型IMT-2000（Enhanceed IMT-2000）、后IMT-2000（system Beyond IMT-2000）或4G。

（2）无线城域网（Wierless Metorpolitan Area Network，WMAN）：主要是通过移动电话或车载装置进行的移动数据通信，可以覆盖城市中大部分的地区。代表技术是2002年提出的IEEE 802.20标准，主要针对移动宽带无线接入（Mobile Broadband Wireless Access，MBWA）技术。该标准强调移动性，它是由IEEE 802.16的宽带无线接入（Broadband Wireless Access，BWA）发展而来的。另外一个代表技术是IEEE 802.16标准体系，主要有802.16、802.16a、802.16e等。其中802.16是一点对多点的视距条件下的标准，802.16a是它的补充版本，增加了对非视距和网状结构（Mesh Mode）的支持，802.16e是对802.16d的增强，支持在2-11GHz频段下的固定和车速移动业务，并支持基站和扇区间的切换。802.16a/e也称为WiMAX。

（3）无线局域网（Wireless Local Area Netwok，WLAN）：一般用于区域间的无线通信，其覆盖范围较小。代表技术是IEEE 802.11系列，以及HomeRF技术。数据传输速率为11～56Mb/s之间，甚至更高。无线连接距离在50～100m。802.11标准系列包含由IEEE制订的802.11b/a/g3个WLAN标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入。其中，802.11b的工作频段为2.4~2.4835GHz，数据传输速率达到11Mb/s，传输距离控制

在100~300m。802.11a的工作频段为5.15~5.825GHz，数据传输速率达到54Mb/s，传输距离控制在10~100m，但由于技术成本过高，802.11a缺乏价格竞争力。而802.11g标准拥有802.11a的传输速率，安全性较802.11b好，且与802.11a和802.11b的兼容。

（4）无线个域网（Wierless Personal Area Network，WPAN）：无线传输距离一般在10m左右，典型的技术是IEEE 802.15（WPAN）、Bluetooth、ZigBee技术，数据传输速率在10Mb/s以上，无线连接距离在10m左右。例如，Bluetooth工作在全球统一开放的2.4GHz频段，实现低成本短距无线通信，在10m范围内可提供721Kb/s的异步最大通信速率，并可最多同时和7个其他蓝牙设备进行通信，从而组成一个无线个域网。

（5）无线体域网（WBAN）：以无线医疗监控和娱乐、军事应用为代表，主要指附着在人体身上或植入人体内部的传感器之间的通信。从定义来看，WBAN和WPAN有很大关系，但是它的通信距离更短，通常来说为0～2m。因此无线体域网具有传输距离非常短的物理层特征。

图1.1所示为从传输距离角度给出各种网络间的比较。

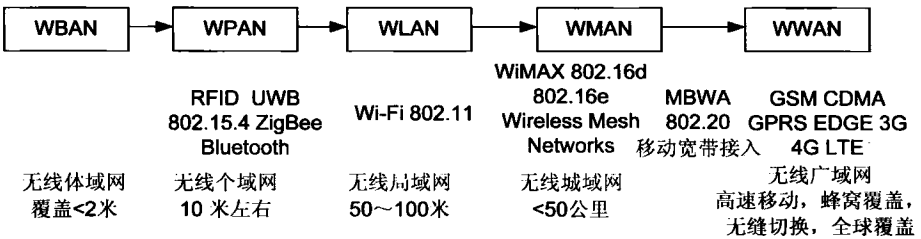


图 1.1　从传输距离进行无线网络的分类

从网络拓扑结构角度，无线网络又可分为有中心网络和无中心、自组织网络。有中心网络以蜂窝移动通信为代表，基站作为一个中央基础设施，网络中所有的终端要通信时，都要通过中央基础设施进行转发；无中心网络以移动自组织网络（Moblie Ad Hoc Networks）、无线传感器网络（Wireless Sensor Networks，WSNs）、移动车载自组织网络（Vehicular Ad Hoc Network，VANET）为代表，采用分布式、自组织的思想形成网络，网络中每个节点都兼具路由功能，可以随时为其他节点的数据传输提供路由和中继服务，而不仅仅依赖单独的中心节点。这种网络具有一些通用特征，如无中心基础设施和自组织、动态拓扑变化（Dynamic或者Static）、有限的传输带宽等。从网络拓扑结构角度对无线网络的分类，如图1.2所示。

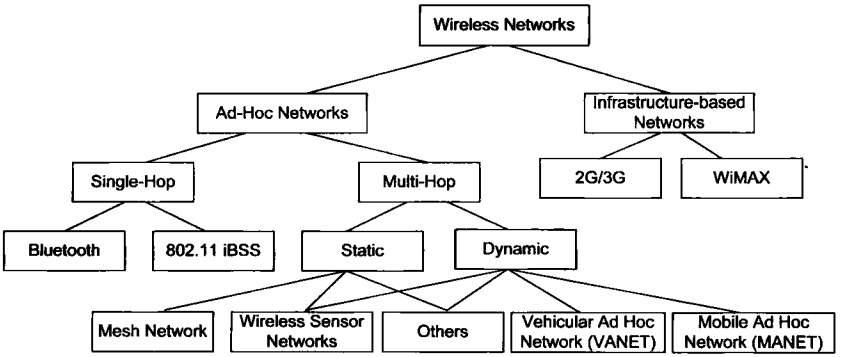


图 1.2　基于网络拓扑结构的无线网络分类

本书的组织便根据这两种分类方法，对各种形态无线网络的安全进行了逐一介绍。

2. 网络节点设备的特点

在进行安全威胁分析和安全方案设计的时候，同时需要考虑网络节点设备的特点。目前，网络终端设备按性能可分为智能手机、平板电脑（笔记本电脑）、具有通信能力的PDA、无线传感器节点、RFID标签和读卡器等。这些网络节点设备通常具有以下特点。

（1）网络终端设备的计算能力一般较弱（可能跟设备价格相关）。

（2）网络终端设备的存储空间有限。

（3）网络终端设备的能源是由电池提供的，持续时间短。

（4）网络终端设备比固定设备更容易发生被窃、丢失、损坏。

因此，在考虑安全威胁的时候，需要注意网络终端设备存在的安全隐患。在设计无线网络安全方案时要充分考虑网络终端设备的能力和特点。

1.2　无线网络安全概述

1.2.1　无线网络安全与有线网络安全的区别

无线网络提高了用户访问网络的自由度，具有网络容易安装，增加用户或更改网络结构方便灵活、费用低廉，可以提供（无线覆盖范围内的）移动接入服务等优势。然而，这种方便和自由也带来了安全问题。由于无线网络通过无线电波在空中传输数据，在信号传递区域

内的无线网络用户，只要具有相同接收频率就可能获取所传递的信息，要将无线网络环境中传递的数据仅仅传送给一个目标接收者是不可能的。另一方面，由于无线移动设备在存储能力、计算能力和电源供电时间方面的局限性，使得原来在有线环境下的许多安全方案和安全技术不能直接应用于无线环境，例如防火墙对通过无线电波进行的网络通信起不了作用，任何人在区域范围之内都可以截获和插入数据；计算量大的加密/解密算法不适用于移动设备等。

与有线网络相比，无线网络所面临的安全威胁更加严重。所有常规有线网络中存在的安全威胁和隐患通常都依然存在于无线网络中，同时无线网络传输的信息更容易被窃取、篡改和插入；无线网络容易受到拒绝服务攻击（Denail of Service，DoS）和干扰等。由于无线网络在移动设备和传输介质方面的特殊性，使得一些攻击更容易实施，同时，解决无线网络安全问题比有线网络的限制更多、难度更大。

无线网络在信息安全方面有着与有线网络不同的特点，具体表现在以下几个方面。

（1）无线网络的开放性使得网络更容易受到恶意攻击：无线链路使得网络更容易受到被动窃听或主动干扰的各种攻击。有线网络的网络连接是相对固定的，具有确定的边界，攻击者必须物理接入网络或经过物理边界（防线），如防火墙和网关，才能进入有线网络。这样通过对接入端口的管理可以有效地控制非法用户的接入。而无线网络则没有一个明确的防御边界，攻击者可能来自四面八方和任意节点，每个节点必须面对攻击者直接或间接的攻击。无线网络的这种开放性带来了非法信息截取、未授权使用服务等一系列信息安全问题。

（2）无线网络的移动性使得安全管理难度更大。有线网络的用户终端与接入设备之间通过线缆连接，终端不能在大范围内移动，对用户的管理比较容易。而无线网络终端不仅可以在较大范围内移动，而且还可以跨区域漫游，这意味着移动节点没有足够的物理防护，从而易被窃听、破坏和劫持。攻击者可能在任何位置通过移动设备实施攻击，而在较大范围内跟踪一个特定的移动节点是很难做到的；另一方面，通过网络内部已经被入侵的节点（也称为妥协节点、攻陷节点）实施攻击而造成的破坏更大，更难检测到。因此，对无线网络移动终端的管理要困难得多。

（3）无线网络动态变化的拓扑结构使得安全方案的实施难度更大。有线网络具有固定的拓扑结构，安全技术和方案容易实现；而在无线网络环境中，动态的、变化的拓扑结构缺乏集中管理机制，使得安全技术更加复杂。另一方面，无线网络环境中做出的许多决策是分

散的，而许多网络算法必须依赖所有节点的共同参与和协作。缺乏集中管理机制意味着攻击者可能利用这一弱点实施新的攻击来破坏协作机制。

（4）无线网络传输信号的不稳定性带来无线通信网络的鲁棒性问题。有线网络的传输环境是确定的，信号质量稳定，而无线网络随着用户的移动其信道特性是变化的，会受到干扰、衰落、多径、多普勒频移等多方面的影响，造成信号质量波动较大，甚至无法进行通信。因此，无线网络传输信道的不稳定性产生了无线通信网络的鲁棒性问题。

此外，移动计算引入了新的计算和通信行为，这些行为在固定或有线网络中很少出现。例如，节点间的协作、数据包的转发、节点间的信任和协作机制、贪心节点的可能性与不合作行为、节点因缺电造成的系统可靠性问题等。因此，有线网络中的安全措施不能应对新的攻击，需要重新审视无线网络的安全威胁及其对策。

总之，无线网络的脆弱性是由于其传输介质的开放性、终端的移动性、动态变化的网络拓扑结构、传输信号的不稳定性、缺乏集中的监视和管理点及没有明确的网络边界防线造成的。因此，在无线网络环境中，在设计实现一个完善的无线网络系统时，必须首先分析网络中存在的各种安全威胁。针对这些威胁提炼必需的安全需求，从而设计相应的安全方案，通常包括用户接入控制设计、用户身份认证方案设计、密钥协商及密钥管理方案的设计等。其中通信的保密性和认证技术是无线网络安全的需求解决的首要问题。

1.2.2 无线网络安全威胁与对策

1. 安全威胁及其具体表现

从信息安全角度来说，安全威胁是指某个人、物或事件对某一资源的保密性、完整性、可用性或合法使用性所造成的危险。安全威胁可以分为故意的和偶然的，故意的威胁又可以进一步分为主动的和被动的。偶然的威胁通常从可靠性、容错性、鲁棒性角度进行分析；故意的威胁通常是安全分析中的主要内容。被动威胁包括只对信息进行监听，而不对其进行修改。主动威胁包括对信息进行故意的篡改（包含插入、删减、添加）、伪造虚假信息等。对每一种可能的攻击行为都要从攻击方法、攻击可能导致的后果、攻击者的数量和实施这种攻击的可能性4个方面进行分析，以便采取相应的安全对策。