重点大学信息安全专业规划系列教材

无线网络攻防原理与实践

易 平 主编

清华大学出版社

重点大学信息安全专业规划系列教材

无线网络攻防原理与实践

易 平 主编

清华大学出版社
北京

内 容 简 介

本书详细阐述了无线网络安全的基本原理和安全攻防技术。作为一本原理与实践相结合的教材，本书系统、全面地介绍了无线网络原理和安全攻防技术。在理论基础上，设计了多个相关实验，由基本攻防实验、综合攻防实验，到最后完成创新实验。全书分为6章，分别讲述：无线自组织网络发展现状、无线自组织网络安全技术、无线自组织网络攻防原理、无线自组织网络攻防网络仿真实验、无线自组织网络硬件平台攻防实验、无线局域网攻防实验。

本书融合多个全国大学生创新项目的成果，特别适合无线通信、网络安全的创新实验课程与创新实验项目的指导教材。同时，适于作为通信与信息系统、电子与信息工程、计算机应用、计算机网络等相关专业的大学本科和研究生教材，也适合以上相关专业的应用开发人员、工程技术人员参考。

图书在版编目(CIP)数据

无线网络攻防原理与实践/易平主编. —北京：清华大学出版社，2012.1
(重点大学信息安全专业规划系列教材)
ISBN 978-7-302-25477-5

Ⅰ. ①无… Ⅱ. ①易… 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(2011)第084389号

责任编辑：魏江江　顾　冰
责任校对：时翠兰
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京市清华园胶印厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：18.75　**字　数**：462千字
版　　次：2012年1月第1版　　**印　　次**：2012年1月第1次印刷
印　　数：1～3000
定　　价：29.50元

产品编号：039142-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

进入20世纪90年代后，没有固定基础设施支撑、由若干移动节点组成的无线自组织网络，简称为移动Ad Hoc网络(Mobile Ad Hoc Networks)，逐渐成为分组无线网中的一个研究热点。无线自组织网络是一种不同于传统无线通信网络的技术。传统的无线蜂窝通信网络，需要固定的网络设备如基地站的支持，进行数据的转发和用户服务控制。而无线自组织网络不需要固定设备支持，各节点即用户终端自行组网，通信时，由其他用户节点进行数据的转发。这种网络形式突破了传统无线蜂窝网络的地理局限性，能够更加快速、便捷、高效地部署，适合于一些紧急场合的通信需要，如战场的单兵通信系统。它主要应用在抢险、抗灾、救援、探险、军事行动、应急任务和临时重大活动等，需要快速建立、移动、灵活的通信系统的场合中。它无论是在民用还是在军事上都有着显著的意义，而为了达到连续和无缝的通信要求，无线自组织网络将起着至关重要的作用，因为现有的任何系统并不能支持更为广泛的、完全意义上的连续、无缝通信。在这一方面，无线自组织网络将是未来通信中关键而又现实的延伸，它可以灵活地扩展到任意的地域。

有感于无线自组织网络安全技术的迅速发展，许多大学已经开设了有关无线网络安全方面的课程，但是仅仅在理论上讲述已经不能满足教学和实践的需求，作者在自身研究工作积累的基础上精心编写了本书，让读者分享我们学习与研究工作的经验和成果。本书不仅可以使初学者能够了解无线网络安全原理和技术，还可以通过循序渐进的实验过程，完全掌握无线网络前沿的攻防技术。

本书有几大特色：

(1) 理论与实践相结合。首先论述无线安全和攻防的相关理论，再动手进行实践，网络仿真和平台实验。全面的攻防实践，实验设计从攻击入手，到检测和防护，每一步都有详细的实验教程。实验设计由浅入深，由基本攻防实验、综合攻防实验，到创新实验。逐步加大难度与深度，便于读者学习掌握。

(2) 软件与硬件结合。不仅设计了大量的NS2仿真实验，而且引入了新一代仿真工具NS3，设计了在NS3环境下的仿真实验。不仅进行攻防的网络仿真实验，而且专门设计了硬件平台攻防实验，在嵌入式开发平台上进行设计开发，更有助于锻炼提高网络攻防的实践能力。

(3) 融入最新科研成果。本书融合了项目组多年来的研究成果，包括自然科学基金和863计划等多个项目，一些实验案例直接取自于国家大学生创新实验项目，其中包

括“移动自组织网络安全模块设计与实现”、“基于 NS2 无线 Mesh 网络仿真实验床的设计与实现”、“面向世博会场馆的无线 Mesh 网络安全防护技术”等。其中许多无线网络攻防技术，包括泛洪攻击、黑洞攻击、虫洞攻击、移动防火墙等一些原先只是在理论界探讨的前沿研究成果，已经由本书设计成可行的实验案例，直接进行具体实验操作，可以进一步掌握无线攻防的前沿技术。

本书共分 6 章，第 1 章介绍了无线自组织网络的起源和发展。首先对无线自组织网络的概念和特点进行了一个简要叙述。然后介绍了无线自组织网络的起源、发展历程和应用领域。其次着重阐述了无线自组织网络领域中关键技术的研究现状及相关研究机构。

第 2 章介绍了无线自组织网络的安全研究进展。由于无线自组织网络的独特结构，使得常规的安全方案无法应用，必须针对其特点设计专门的安全解决方案。本章从密钥管理、路由安全、入侵检测、增强合作几个方面介绍了应用于无线自组织网络的安全解决方案。首先讨论了密钥管理，主要介绍了自组织的密钥管理和分布式的密钥管理两类算法，指出了其优点和缺点。然后分析了 5 种典型的路由安全协议，对它们进行了综合比较并指出其存在问题及改进方法。接下来说明了基于 agent 的分布式监视合作检测的入侵检测体系结构。最后讨论了基于激励和基于惩罚的两种增强合作的机制。

第 3 章首先对无线自组织网络的安全缺陷和两种经典的路由协议，然后介绍了针对路由协议攻击的一些方法，其中重点分析了两只攻击方式：泛洪攻击和黑洞攻击。详细讨论了其攻击原理，并设计了检测和响应方法。最后，设计了一种适用于无线自组织网络的主动防护方法—— 移动防火墙，对其原理进行了详细的分析讨论。

第 4 章首先介绍了 NS2 一些基本概念、安装使用和实验数据的分析方法。为了便于读者掌握 NS2，专门设计了三个 NS2 基础仿真实验。然后，设计了泛洪攻击与检测实验、黑洞攻击与检测实验、虫洞攻击实验、移动防火墙实验。此外还介绍了全新的 NS3 软件仿真平台，并设计出相应的仿真实验。

第 5 章首先介绍了硬件实验平台的软件系统配置，介绍了基于 Linux 内核的开源无线路由器操作系统——OpenWrt，分析了其结构和组成，论述了基于 Click 的路由机制，详细分析了路由报文处理过程，设计了编译安装硬件平台的流程。然后基于嵌入式开发的硬件平台，设计了两种基本攻防实验，即泛洪攻击和检测实验、黑洞攻击和检测实验；两种综合实验，即泛洪和黑洞攻击、检测与防护综合实验。最后，讲述了安全加密与认证实验。通过在此平台上设计一整套的攻击、检测及响应的软件解决方案，来加深对无线网络以及其上的安全问题的理解。

第 6 章，无线局域网(WLAN)是近年来发展迅速的无线数据通信网，但在发展同时，它又面临着许多安全问题。本章首先对无线局域网进行了概述，然后对无线局域网的安全风险和安全需求进行了分析，最后重点阐述了无线局域网的安全技术、安全协议。最后，设计了几个安全攻防实验。

易平撰写了本书第 1～4 章与第 5 章前 7 节内容，吴越撰写了第 5 章第 8 节，邹福泰撰写了第 6 章，全书最后由易平统稿。许多学生参与了本书的案例设计，其中包括杜尚鑫、王翔宇、杨浩等。本书在编写过程中得到上海交通大学信息安全工程学院有关专家教授的关心与支持，在此向他们表示衷心的感谢。

作者衷心感谢清华大学出版社的大力支持，尤其感谢本书的编辑为本书付出的辛勤劳

动和汗水。

无线网络涉及领域宽、内容多、发展快，本书的取材有些为学术界和工程技术界的研究成果，也包括本书作者的一些成果和观点。相关研究成果属于设计原作者，我们在书中均作了引用标识。我们尽量以客观的态度对待任何一项研究方法和成果，对于其中的争议甚至错误，希望留待读者去进一步甄别与探究。尽管我们力求完美，但作者水平有限，疏漏、不当与错误之处在所难免，欢迎读者批评指正。

本书得到国家自然科学基金重点项目“无线自组织网络安全特性研究”(No. 60932003)；国家高计划研究发展计划 863 资助项目“无线自组网实时入侵检测与主动防护机制研究”(2007AA01Z452)；上海市自然科学基金资助项目“无线 Mesh 网络主动安全防护模型研究”(09ZR1414900)等项目的资助。

编　者

于上海交通大学

目　录

第1章　无线自组织网络概述

无线自组织网络技术是支持普适计算及未来移动通信系统的重要技术基础，对无线自组织网络相关技术的研究已经成为计算机网络和通信领域中的一个热点。本章首先对无线自组织网络的概念和特点进行简要叙述。然后介绍无线自组织网络的起源、发展历程和应用领域。最后重点介绍无线自组织网络领域中关键技术的研究现状及相关研究机构。

1.1　研究背景

随着21世纪的到来，人类社会已进入一个崭新的发展阶段——信息社会。通信和网络技术的迅猛发展加速了信息交流，极大地促进了人类社会的“全球化”，深刻改变了社会的经济、政治与生活面貌。全球化的发展又进一步刺激了通信与网络技术的发展，人们追求任何人在任何时间、任何地点与任何人进行任何种类的信息交换。

在20世纪的大部分时间里，以固定电话网为代表的有线网络一直是信息的主要载体。然而在近二十年时间里，随着微电子技术与无线通信理论的迅速发展，无线通信网络获得了跨越式的发展，已成为全球通信网络的主要组成部分，最根本的原因在于无线通信网络使人们摆脱了通信线路的束缚，更接近于个人通信的需要。

近些年来，无线通信网络的发展非常迅速，这主要是由于个人通信的需求，无论是在支持范围上，还是种类、质量要求上都大大增加的缘故，而连接世界各地、可共享现有信息资源的Internet(因特网)的崛起更是极大地刺激了无线通信的发展。无线通信网络由于能快速、灵活、方便地支持用户的移动性而使它成为个人通信和Internet发展的方向，目前几乎所有的通信系统都与无线通信方式有关，如蜂窝系统、无绳电路系统、卫星通信系统、无线局域网与无线广域网(WLAN/WAN)[1]、移动IP[2]、无线ATM[3]、分组无线网(PRNET)[4]、无线自组织网络[5]等，而对无线和移动的相关研究成为这些通信系统中的最主要的部分。

传统意义上对无线通信网络的研究仅限于一跳无线网络，如蜂窝系统和无线局域网，它们都属于有基础设施的移动无线网络。在这些系统中，移动用户(或节点)在有限的区域里(即小区)移动，借助于固定的具有多部收发信机、可全双工方式工作的基站和可以大容量传输的有线骨干网络系统而与其他用户通信。当移动用户移出一个基站的覆盖范围而进入到另一个基站的覆盖范围内时由基站实现越区切换，这样移动用户就可以在整个通信网络中连续、无缝地通信。

在20世纪90年代，没有固定基础设施支撑、由若干移动节点组成的移动自组织网络——无线自组织网络(Mobile Ad Hoc Networks)逐渐成为分组无线网中的一个研究热点。无线自组织网络独立于任何静态的基础设施，可即时建立。它主要应用在抢险、抗灾、救援、探险、军事行动、应急任务和临时重大活动等，需要快速建立、移动、灵活的通信系统的场合中。它无论是在民用还是在军事上都有着显著的意义，而为了完成连续和无缝的通信要求，无线自组织网络将会起着至关重要的作用，因为仅仅基于现有的任何系统并不能支持

更为广泛的、完全意义上的连续、无缝通信。在这一方面，无线自组织网络将是未来通信中关键而又现实的延伸，它可以灵活地扩展到任意的地域。

无线自组织网络是一个复杂系统，所涉及的研究内容非常广泛，目前对它的研究和应用已发展成为通信领域的一个独立分支，存在一些需要彻底研究的问题。

本书内容很多来源于政府资助项目，它们分别是国家高技术研究发展 863 计划资助项目“无线自组网实时入侵检测和主动防护机制研究”(2007AA01Z452)，国家自然科学基金重点项目“无线自组织网络安全特性基础理论研究”(No. 60932003)，上海市自然科学基金“无线 Mesh 网络主动安全防护模型研究”(09ZR1414900)。

1.1.1 无线自组织网络的概念及特点

无线自组织网络是由具有无线通信能力移动节点组成的、具有任意和临时性网络拓扑的动态自组织网络系统，其中每个节点既可作为主机也可作为路由器使用。Ad Hoc 的意思是 for this 引申为 for this purpose only，即“为某种目的设置的，特别的”意思，即 Ad Hoc 网络是一种有特殊用途的网络。移动终端具有路由功能，可以通过无线连接构成任意的网络拓扑，这种网络可以独立工作，也可以与 Internet 或蜂窝无线网络连接。在后一种情况中，无线自组织网络通常是以末端子网的形式接入现有网络。考虑到带宽和功率的限制，无线自组织网络一般不适于作为中间传输网络，它只允许产生于或目的地是网络内部节点的信息进出，而不让其他信息穿越本网络，从而大大减少了与现存 Internet 互操作的路由开销。无线自组织网络中，每个移动终端兼备路由器和主机两种功能：作为主机，终端需要运行面向用户的应用程序；作为路由器，终端需要运行相应的路由协议，根据路由策略和路由表参与分组转发和路由维护工作。在无线自组织网络中，节点间的路由通常由多个网段(跳)组成，由于终端的无线传输范围有限，两个无法直接通信的终端节点往往要通过多个中间节点的转发来实现通信。所以，它又被称为多跳无线网、自组织网络、无固定设施的网络或对等网络。无线自组织网络同时具备移动通信和计算机网络的特点，可以看做是一种特殊类型的移动计算机通信网络。

图 1-1 描述了一个由 5 个主机组成的简单的无线自组织网络。主机 D 不在主机 A 的无线覆盖范围之内(用环绕主机 A 的圆环表示)，同时主机 A 也不在主机 D 的无线覆盖范围内。如果主机 A 和 D 之间需要交换信息，就需要主机 B、C 为它们转发分组，因为主机 B、C 在主机 A 和 D 的无线覆盖范围之内。

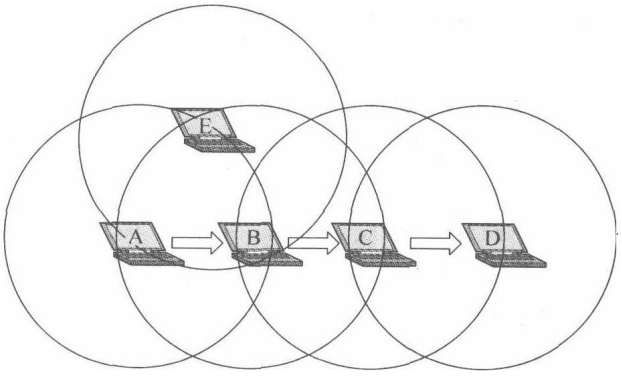

图 1-1 一个简单的无线自组织网络

与通常的网络相比，无线自组织网络具有以下特点[4]。

(1) 网络的自组织性：无线自组织网络相对常规通信网络而言，最大的区别就是可以在任何时刻、任何地点不需要硬件基础网络设施的支持，快速构建起一个移动通信网络。它的建立不依赖于现有的固定网络通信设施，由网络本身节点自组织形成网络。无线自组织网络的这种特点很适合灾难救助、偏远地区通信等应用。

(2) 动态的网络拓扑结构：在无线自组织网络中，移动主机可以在网中以任意速度和任意方式移动，主机的移动会导致主机之间的链路增加或消失，主机之间的关系不断发生变化。加上无线发送装置发送功率的变化、无线信道间的互相干扰及地形及地物等综合因素影响，各移动节点间的连接关系将时刻发生变化，因此，造成网络拓扑结构不断发生变化，而且变化的方式和速度都是不可预测的。对于常规网络而言，网络拓扑结构则相对较为稳定。

(3) 多跳的通信路由：由于节点无线发射功率的限制，节点的覆盖范围有限。当它要与其覆盖范围之外的节点进行通信时，需要中间节点的进行转发。此外，无线自组织网络中的多跳路由是由普通节点协作完成的，而不是由专用的路由设备(如路由器)完成的。网络中每一个节点可充当多个角色，它们可以是服务器、终端、路由器。

(4) 有限的无线通信带宽：在无线自组织网络中没有固定基础设施的支持，因此，主机之间的通信均通过无线传输来完成。由于无线信道本身的物理特性，它提供的网络带宽相对有线信道要低得多。除此以外，考虑到竞争共享无线信道产生的碰撞、信号衰减、噪音干扰等多种因素，移动终端可得到的实际带宽远远小于理论中的最大带宽值。

(5) 有限的主机能源：在无线自组织网络中，主机均是一些移动设备，如 PDA、便携计算机或掌上电脑。由于主机可能处在不停的移动状态下，主机的能源主要由电池提供，因此，网络具有能源有限的特点。

(6) 网络的分布式特性：在无线自组织网络的各节点都具备独立的路由能力，没有中心控制节点对各节点网络操作进行控制，节点通过分布式协议互联。一旦网络的某个或某些节点发生故障，其余的节点仍然能够正常工作。

(7) 生存周期短：无线自组织网络主要用于临时的通信需求，相对于有线网络，它的生存时间一般比较短。

(8) 安全性较差：无线自组织网络是一种特殊的无线移动网络，由于采用无线信道、有限电源、分布式控制等技术，它更加容易受到被动窃听、主动入侵、拒绝服务、剥夺“睡眠”等网络攻击。信道加密、抗干扰、用户认证和其他安全措施都需要特别考虑。

(9) 移动节点的局限性：无线自组织网络中，移动节点具有携带方便、轻便灵巧等好处，但是也存在固有缺陷，例如能源受限、内存较小、CPU 性能较低等，从而给应用程序设计开发带来一定的难度，同时屏幕等外设较小，不利于开展功能较复杂的业务。

1.1.2　无线自组织网络的发展历程

无线自组织网络技术起源于 20 世纪 70 年代，它是在美国国防部高级研究计划局(DARPA)资助研究的战地无线分组数据网(PRNET)[5]项目中产生的一种新型网络技术。DARPA 当时所提出的是一种军用无线分组数据通信网络。在此之后，DARPA 于 1983 年启动了高残存性自适应网络项目 SURAN(Survivable Adaptive Network)[6]，研究如何将 PRNET 的研究成果加以扩展，以支持更大规模的网络。1994 年，DARPA 又启动了全球移