清华
科技大讲堂

入门 • 综合 • 创新

无线网络攻防原理与实践

WU XIAN WANG LUO GONG FANG YUAN LI YU SHI JIAN

（第2版）

易 平 ◉ 主编

- 注重理论与实践相结合。
- 注重软件与硬件相结合。
- 注重网络攻防的前沿技术。
- 提供泛洪攻击、黑洞攻击、虫洞攻击、移动防火墙等实验案例。

清华大学出版社

清华科技大讲堂

无线网络攻防原理与实践（第2版）

易 平 主 编

清华大学出版社
北 京

内 容 简 介

本书详细阐述无线网络安全的基本原理和安全攻防技术。作为原理与实践相结合的教材，本书首先系统、全面地介绍无线网络原理和安全攻防技术。然后在理论基础上，设计多个相关实验，由基本攻防实验到综合攻防实验，最后完成创新实验，由浅入深、循序渐进。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、网络仿真实验、无线局域网的攻防原理与安全实践、无线局域网的攻防实践。

本书特色是：①设计了大量 NS2 的仿真实验，引入新一代仿真工具 NS3，设计了在 NS3 环境下的仿真实验。②基于新一代网络渗透测试系统 Kali Linux，设计了 WiFi 网络攻防实验，包括无线扫描、无线破解、无线 DoS 攻击、无线监听等攻防实验，有助于锻炼提高网络攻防的实践能力。

本书融合了多个全国大学生创新项目的成果，特别适合作为无线通信、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，可以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，也适合作为以上相关专业的应用开发人员、工程技术人员的参考书。

图书在版编目(CIP)数据

无线网络攻防原理与实践/易平主编. —2 版. —北京：清华大学出版社，2017
(清华科技大讲堂)
ISBN 978-7-302-46904-9

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(2017)第 063957 号

责任编辑：魏江江　梅栾芳
封面设计：杨　兮
责任校对：焦丽丽
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20　　**字　　数**：480 千字
版　　次：2012 年 1 月第 1 版　2017 年 7 月第 2 版　　**印　　次**：2017 年 7 月第1 次印刷
印　　数：1～2000
定　　价：49.00 元

产品编号：071249-01

易平　博士

上海交通大学网络空间安全学院副教授。多年来一直从事无线网络和信息安全的教学和研究工作，主编了《无线网络攻防原理与实践》《无线网络攻防教程》等教材，研发无线网络攻防创新实验系统。先后主持和参加了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”，国家863计划“无线自组网实时入侵检测和主动防护机制研究”“无线网状网络WMN安全关键技术研究”，上海市自然基金“无线Mesh网络主动安全防护模型研究”，上海科委重点项目“无线移动网络安全接入管控系统关键技术研究及港务应用”等多项国家和地方项目。

前　言

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，简称为移动自组织网络(Mobile Ad Hoc Networks)，逐渐成为分组无线网中的研究热点。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。无论是在民用还是在军事上它都有着显著的意义，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地域。

随着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了解无线网络安全原理和技术，还可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，进行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 WiFi 网络攻防实验，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，包括国家自然科学基金和 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来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;最后着重阐述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 章介绍无线自组织网络安全技术。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应用于无线自组织网络的安全解决方案。首先讨论密钥管理,主要介绍自组织的密钥管理和分布式的密钥管理两类算法,指出其优点和缺点。然后分 5 种典型的路由安全协议,对它们进行综合比较并指出其存在的问题及改进方法;接下来说明基于 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进行介绍,然后介绍针对路由协议攻击的一些方法,其中重点分析两种攻击方式:泛洪攻击和黑洞攻击;详细讨论其攻击原理,并设计检测和响应方法;最后,设计一种适用于无线自组织网络的主动防护方法——移动防火墙,对其原理进行详细的分析讨论。

第 4 章首先介绍 NS2 的一些基本概念、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 3 个 NS2 基础仿真实验;然后,设计泛洪攻击与检测实验、黑洞攻击与检测实验、虫洞攻击实验,以及移动防火墙实验;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 章介绍无线局域网的攻防原理与安全实践。无线局域网是近年来发展迅速的无线数据通信网,但在发展的同时,它又面临着许多安全问题。本章首先对无线局域网进行概述,然后对无线局域网的安全风险和安全需求进行分析,最后重点阐述无线局域网的安全技术和安全协议。

第 6 章介绍了无线局域网的攻防实践。为了增强对无线局域网安全协议的理解,基于新一代网络渗透测试系统 Kali Linux 设计了 WiFi 网络攻防实验,包括无线扫描、无线破解、无线 DoS 攻击、无线监听等 15 个攻防实验,通过攻防实验提高网络攻防的实践能力。

易平撰写了本书第 1～4 章和第 6 章,邹福泰撰写了第 5 章,全书最后由易平统稿。许多同学参与了本书的案例设计,包括夏之阳、王翔宇、杨浩等同学。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。

无线网络涉及领域宽、内容多、发展快,本书大部分内容来自作者自己的成果和观点,也参考了学术界和工程技术界的研究成果,相关研究成果属于设计原作者的,在书中均做了引用标识。我们尽量客观地对待书中所有研究方法和成果,对于其中的争议或错误,留待读者

进一步甄别与探究。由于作者水平有限，疏漏、不当之处在所难免，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”(60932003)、国家高计划研究发展计划(863 计划)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)等的资助。

编　者

于上海交通大学

2017 年 1 日

目　录

第 1 章　无线自组织网络概述 …… 1

1.1　研究背景 …… 1
1.1.1　无线自组织网络的概念及特点 …… 2
1.1.2　无线自组织网络的发展历程 …… 3
1.1.3　无线自组织网络的应用领域 …… 4
1.2　无线自组织网络的主要研究领域 …… 6
1.2.1　MAC 层协议 …… 6
1.2.2　路由协议 …… 7
1.2.3　组播路由协议 …… 11
1.2.4　服务质量保证 …… 11
1.2.5　网络管理 …… 12
1.2.6　网络安全 …… 13
1.3　无线自组织网络的研究机构及其研究方向 …… 13
参考文献 …… 14

第 2 章　无线自组织网络安全技术 …… 18

2.1　引言 …… 18
2.2　无线自组织网络的安全弱点和安全目标 …… 18
2.2.1　安全弱点 …… 18
2.2.2　安全目标 …… 20
2.3　密钥管理 …… 20
2.3.1　自组织密钥管理 …… 21
2.3.2　分布式密钥管理 …… 22
2.3.3　两种密钥管理方案的比较和分析 …… 22
2.3.4　其他密钥管理方案 …… 23
2.4　路由安全 …… 24
2.4.1　路由安全威胁 …… 25
2.4.2　路由安全协议 …… 26

2.4.3 路由安全协议的比较与分析 …… 29
2.5 入侵检测 …… 31
2.5.1 入侵检测方案 …… 31
2.5.2 入侵检测方案比较与分析 …… 32
2.6 增强合作的机制 …… 32
2.6.1 基于激励机制 …… 33
2.6.2 基于惩罚机制 …… 34
2.6.3 两类算法的比较与分析 …… 35
2.7 总结与展望 …… 35
参考文献 …… 37

第3章 无线自组织网络攻防原理 …… 40

3.1 无线自组织网络的安全缺陷 …… 40
3.1.1 传输信道方面 …… 40
3.1.2 移动节点方面 …… 41
3.1.3 动态拓扑 …… 41
3.1.4 安全机制方面 …… 41
3.1.5 路由协议方面 …… 41
3.2 两种经典路由协议 …… 41
3.2.1 DSR 路由协议 …… 41
3.2.2 AODV 路由协议 …… 43
3.3 无线自组织网络的路由攻击方法 …… 47
3.3.1 篡改 …… 47
3.3.2 冒充 …… 47
3.3.3 伪造 …… 47
3.3.4 拓扑结构与通信量分析 …… 47
3.3.5 资源消耗攻击 …… 47
3.3.6 虫洞攻击 …… 48
3.3.7 黑洞攻击 …… 48
3.3.8 Rushing 攻击 …… 48
3.4 泛洪攻击 …… 48
3.5 泛洪攻击检测及响应 …… 50
3.6 黑洞攻击 …… 50
3.6.1 被动黑洞攻击 …… 51
3.6.2 主动黑洞攻击 …… 51
3.7 黑洞攻击检测及响应 …… 53
3.8 基于移动防火墙的无线自组织网络主动防护机制 …… 53
3.8.1 主动防护算法概述 …… 53
3.8.2 簇形成机制 …… 54

3.8.3 信号强度检测 …… 55
3.8.4 入侵响应策略 …… 55
3.8.5 移动防火墙设计 …… 56
参考文献 …… 59

第4章 网络仿真实验 …… 60

4.1 NS2网络仿真工具概述 …… 60
4.1.1 NS2简介 …… 60
4.1.2 NS2的基本结构 …… 61
4.1.3 NS2中C++和OTcl的关系 …… 61
4.1.4 NS2使用流程 …… 62
4.1.5 模拟结果分析 …… 63
4.1.6 NS2的下载和安装 …… 66
4.2 NS2实验数据分析处理 …… 68
4.2.1 trace文件 …… 68
4.2.2 trace文件的处理 …… 69
4.2.3 数据合成 …… 72
4.2.4 实验数据的批量绘图 …… 74
4.2.5 数据批处理 …… 75
4.3 NS2仿真基础实验 …… 77
4.3.1 使用Tcl语言配置一个简单的网络环境 …… 77
4.3.2 使用CMU工具配置一个随机场景 …… 82
4.3.3 在NS2中移植实现MFlood协议 …… 85
4.4 NS2仿真攻击与检测实验 …… 92
4.4.1 黑洞攻击实验 …… 92
4.4.2 黑洞检测实验 …… 98
4.4.3 泛洪攻击实验 …… 107
4.4.4 泛洪检测实验 …… 114
4.4.5 信道抢占攻击实验 …… 117
4.4.6 虫洞攻击实验 …… 124
4.4.7 移动防火墙实验 …… 135
4.5 NS3网络仿真工具概述 …… 143
4.5.1 NS3简介 …… 143
4.5.2 NS3基本结构 …… 143
4.5.3 NS3模拟流程 …… 146
4.5.4 模拟结果分析 …… 146
4.6 NS3仿真实验 …… 151
4.6.1 实验一：两个节点间简单通信的模拟实现 …… 151
4.6.2 实验二：使用可视化组件模拟一个星型拓扑结构网络 …… 153

4.6.3 实验三：AODV协议简单场景模拟 …… 156
4.6.4 实验四：简单无线Mesh网络场景模拟 …… 165
参考文献 …… 172

第5章 无线局域网的攻防原理与安全实践 …… 173

5.1 概述 …… 173
5.1.1 无线局域网协议栈 …… 173
5.1.2 无线局域网组成 …… 177
5.1.3 无线局域网的拓扑结构 …… 177
5.1.4 无线局域网的应用及发展趋势 …… 179
5.2 安全风险与安全需求 …… 180
5.2.1 无线局域网的安全风险分析 …… 180
5.2.2 无线局域网安全需求分析 …… 184
5.3 安全技术 …… 187
5.3.1 服务装置标识符 …… 187
5.3.2 物理地址过滤 …… 187
5.3.3 直接序列扩频技术 …… 187
5.3.4 扩展服务集标识符 …… 188
5.3.5 开放系统认证 …… 188
5.3.6 共享密钥认证 …… 188
5.3.7 封闭网络访问控制 …… 189
5.3.8 访问控制列表 …… 189
5.3.9 密钥管理 …… 189
5.3.10 虚拟专用网 …… 189
5.3.11 RADIUS服务 …… 190
5.3.12 入侵检测系统 …… 191
5.3.13 个人防火墙 …… 191
5.3.14 基于生物特征识别 …… 192
5.3.15 双因素认证 …… 192
5.3.16 智能卡 …… 192
5.4 安全协议 …… 192
5.4.1 WEP协议 …… 192
5.4.2 WEP的改进方案TKIP …… 195
5.4.3 认证端口访问控制技术IEEE 802.1x …… 195
5.4.4 IEEE 802.11i …… 196
5.4.5 WPA …… 196
5.4.6 WAPI协议 …… 199
5.5 安全实践 …… 200
5.5.1 WEP安全风险 …… 200

5.5.2 WPA 安全风险 …… 203
5.5.3 常用攻击工具 …… 206
5.5.4 攻击实验 …… 207
参考文献 …… 216

第 6 章 无线局域网的攻防实践 …… 217

6.1 基础实验 …… 217
6.1.1 VMware Workstation 的基本使用 …… 217
6.1.2 Mac OS 中虚拟机安装与使用 …… 222
6.1.3 Kali 安装 …… 224
6.2 无线扫描 …… 236
6.2.1 使用 airodump-ng 进行无线扫描 …… 236
6.2.2 使用 Kismet 进行无线扫描 …… 241
6.2.3 扫描隐藏 SSID …… 248
6.3 无线破解 …… 250
6.3.1 暴力破解字典生成方式 …… 250
6.3.2 使用 fern 工具进行 WPA 破解 …… 251
6.3.3 使用 Gerix 工具进行 WPA 破解 …… 254
6.3.4 使用 WiFite 工具进行 WPA 破解 …… 258
6.3.5 使用 aircrack-ng 进行 WPA 破解 …… 261
6.3.6 利用 WPS 破解 …… 263
6.4 无线 DoS 攻击 …… 270
6.5 无线监听 …… 275
6.5.1 ARP 欺骗与消息监听 …… 275
6.5.2 使用 Wireshark 进行监听与解析 …… 280

附录 A Analist 代码 …… 286

附录 B FileMixer 代码 …… 292

附录 C MFlood 协议的描述代码 …… 296

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计划(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"(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,可以看作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。

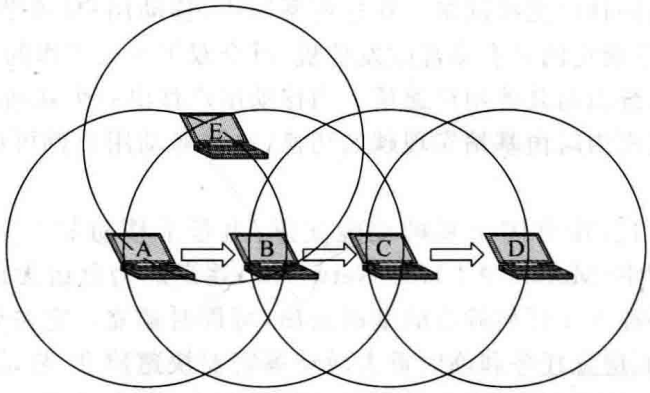

图1-1 一个简单的无线自组织网络

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、任何地点不需要固定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、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，需要中间节点来进行转发。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)资助研究的战地分组无线网(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(Survivable Adaptive Network，SURAN)[6]项目，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

动信息系统(Globle Mobile Information Systems,GloMo)项目[7],旨在对能够满足军事应用需要的、可快速展开、高抗毁性的移动信息系统进行全面深入的研究,以便能够建立某些特殊环境或紧急情况下的无线通信网络。无线自组织技术就是吸取了 PRNET、SURAN 以及 GloMo 等项目的组网思想而产生的一种新型的网络结构技术。美国军方一直在研究适用于军方的无线自组织网络技术,后来又陆续资助了联合战术无线系统(JTRS)[8]等项目。成立于 1991 年 5 月的 IEEE 802.11 标准委员会[9]采用了"Ad Hoc 网络"一词来描述这种特殊的自组织对等式多跳移动通信网络,无线自组织网络就此诞生。Internet 任务工作组(IETF)也将无线自组织网络称为 MANET(Mobile Ad Hoc Networks)[10]。

随着移动通信和移动终端技术的高速发展,无线自组织网络技术不仅在军事领域中得到了充分的发展,而且也在民用移动通信中得到了应用。典型的系统有加拿大最早研究的业余分组无线网(TAPR)[11],图书馆自动化无线电网络[12]等。IETF 于 1996 年成立了 MANET 工作组,专门研究 Ad Hoc 网络环境下基于 IP 协议的路由协议规范和接口设计[10]。这使得无线自组织网络的设计思路也由传统的单一技术体系过渡到基于 IP 的多技术体系,从而导致该网络更具有开放型、适应性、灵活性,提高了开发和应用速度。随着配备有无线收发设备的高性能移动终端的降价和随之而来的普及性,加上人们对于个人通信需求的日益增长,无线自组织网络的研究重新开始得到国内外研究人员的重视。特别是 1998 年以来,无论是国内还是国外,各科研团体对无线 Hd Hoc 网络的研究不断升温,尤其是在网络层的路由协议方面的研究工作已经取得了很大的进展。

1.1.3 无线自组织网络的应用领域

无线自组织网络的许多优良特性为它在民用和军事通信领域占据一席之地提供了有力的支持。首先,网络的自组织性提供了廉价而且快速部署网络的可能。其次,多跳和中间节点的转发特性可以在不降低网络覆盖范围的条件下减少每个终端的发射范围,从而降低设计天线和相关发射/接收部件的难度,也降低了设备的功耗,从而为移动终端的小型化、低功耗提供了可能。从共享无线信道的角度看,无线自组织网络降低了信号冲突的概率,提高了信道利用率。从对使用者的保护来看,高功率的无线电波产生的电磁辐射对用户的身体健康也有影响。另外,网络的鲁棒性、抗毁性满足了某些特定应用需求。它的应用场合可以归纳为以下几类。

1. 军事应用

军事应用是无线自组织网络技术的主要应用领域。在现代化的战场上,由于没有基站等基础设施,装备了移动通信装置的军事人员、军事车辆以及各种军事设备之间可以借助无线自组织网络进行信息交换,以保持密切联系、协作完成作战任务。装备音频传感器和摄像头的军事车辆和设备也能够组成无线自组织网络将在目标区域收集重要的位置和环境信息传送到处理节点。另外,需要通信的舰队战斗群之间也可以通过无线自组织网络建立通信而不必依赖陆地或卫星通信系统。无线自组织网络因其特有的无须架设网络设施、可快速展开、抗毁性强等特点,它是数字化战场通信的首选技术,并已经成为战术互联网的核心技术。为了满足信息战和数字化战场的需要,美军研制了大量的无线自组织网络设备,用于单兵、车载、指挥所等不同的场合,并大量装备部队。美军的数字电台 NTDR 和无线互联网控制器等通信装备都使用了无线自组织网络技术。

2. 移动会议

目前，越来越多的人携带手提电脑、PDA 等便携式设备参加各种会议。如果与会者不借助路由器、集线器或基站就能将各种移动终端快速地组织成无线网络从而完成提问、交流以及资料的分发，这无疑具有重要的意义，而无线自组织网络就具有这样的功能。当一些移动用户聚集在办公室外的某个环境时，他们也可以借助无线自组织网络来协同工作。此外，借助无线自组织网络还可以实现分布式会议。

3. 紧急和突发场合

在自然灾害或其他各种原因导致网络基础设施出现故障或无法使用时，快速恢复通信是非常重要的。借助于无线自组织网络技术和协议，可以快速地建立临时网络，延伸网络基础设施，从而为营救赢得时间，降低灾难所带来的危害。例如，在因发生了地震、水灾、火灾或遭受其他灾难后而使得基站、通信干线等基础通信设施无法使用时，可以形成无线自组织网络来快速地建立联系，组织营救。此外当刑警或消防队员紧急执行任务时，可以通过无线自组织网络来保障通信指挥的顺利进行。

4. 偏远野外地区

当处于边远或野外地区时，无法依赖固定或预设的网络设施进行通信。无线自组织网络技术具有单独组网能力和自组织特点，是这些场合通信的最佳选择。

5. 临时场合

无线自组织网络的快速、简单组网能力使得它可以用于临时场合的通信。例如庆典、展览等场合，可以免去布线和部署网络设备的工作。

6. 动态场合和分布式系统

通过无线连接远端的设备、传感节点和激励器，无线自组织网络可以方便地用于分布式控制，特别适合于调度和协调远端设备的工作，降低分布式控制系统的维护和重配置成本。无线自组织无线网络还可以用于在自动高速公路系统(AHS)中协调和控制车辆[12]，对工业处理过程进行远程控制等。

7. 个人通信

个人局域网(PAN)是无线自组织网络技术的又一应用领域，用于实现 PDA、手机、掌上电脑等个人电子通信设备之间的通信，并可以构建虚拟教室和讨论组等崭新的移动对等应用(MP2P)。考虑到电磁波的辐射问题，个人局域网通信设备的无线发射功率应尽量小，这样无线自组织网络的多跳通信能力将再次展现它的独特优势。

8. 商业应用

可组建家庭无线网络、无线数据网络、移动医疗监护系统和无线设备网络，开展移动和可携带计算以及无所不在的通信业务等。

9. 其他应用

考虑到无线自组织网络具有很多优良特性，它的应用领域还有很多，这需要进一步去挖掘。例如它可以用来扩展现有蜂窝移动通信系统的覆盖范围[13]，实现地铁和隧道等场合的无线覆盖，实现汽车和飞机等交通工具之间的通信，用于辅助教学和构建未来的移动无线城