国际信息工程先进技术译丛

WILEY
www.wiley.com

无线自组织网络和传感器网络安全

Security in Wireless Ad Hoc and Sensor Networks

（土耳其） Erdal Çayırcı
（挪威） Chunming Rong 著
李 勇 译

机械工业出版社
CHINA MACHINE PRESS

关于本书

本书为无线自组织网络和传感器网络安全提供深度指南。

本书介绍了与无线自组织网络相关的基础和关键问题，重点是安全问题。本书讨论了无线自组织网络、传感器网络和Mesh网络中的安全攻击和对策，简要介绍了相关标准。作者清晰地阐明该领域各种挑战和解决方案，包括自举、密钥分发和交换、认证问题、隐私、匿名性和容错。

本书为计算机、电子和通信工程专业研究生、学术界和企业界的研究人员、军队中的C4I工程师和军官提供了非常宝贵的资源。互联网服务提供商和移动通信运营商的无线网络设计师也会发现这本书非常有用。

国际信息工程先进技术译丛

无线自组织网络和传感器网络安全

（土耳其）Erdal Çayırcı
（挪威）Chunming Rong 著
李 勇 译

机 械 工 业 出 版 社

本书系统地介绍了与无线自组织网络、传感器网络和 Mesh 网络（WASM）安全相关的问题及对策。全书共分 15 章，内容分为两个部分：第一部分介绍与无线自组织网络相关的基础和关键问题。第二部分详细讨论 WASM 中的安全攻击和对策。另外本书每章后面附有习题，利于读者对书中内容加深理解。

本书可作为高等院校相关专业研究生或高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域工作的科技人员参考。

Security in Wireless Ad Hoc and Sensor Networks/by Erdal Çayırcı, Chunming Rong/ISBN：978－0470027486

本书版权登记号：图字 01-2010-1526 号。

图书在版编目（CIP）数据

无线自组织网络和传感器网络安全/（土）凯伊瑞奇（Çayırcı, E.），（挪）容春明（Rong, C.）著；李勇译. —北京：机械工业出版社，2011.6

（国际信息工程先进技术译丛）

Security in Wireless Ad Hoc and Sensor Networks

ISBN 978-7-111-34574-9

Ⅰ.①无… Ⅱ.①凯… ②容… ③李… Ⅲ.①无线电通信—自组织系统—通信网—安全技术 ②无线电通信—传感器—安全技术 Ⅳ.①TN92 ②TP212

中国版本图书馆 CIP 数据核字（2011）第 084220 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：刘星宁 责任编辑：刘星宁

版式设计：霍永明 责任校对：陈延翔

封面设计：马精明 责任印制：乔 宇

三河市国英印务有限公司印刷

2011 年 7 月第 1 版第 1 次印刷

169mm×239mm · 15.75 印张 · 311 千字

0001-3000 册

标准书号：ISBN 978-7-111-34574-9

定价：68.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社 服 务 中 心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者购书热线：（010）88379203

网络服务

门户网：http://www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

译 者 序

近年来，无线自组织网络和传感器网络引起学术、军事和工业界的广泛关注。无线自组织网络是一种没有固定基础设施的、无中心、多跳的无线移动网络，传感器网络和 Mesh 网络都属于特殊的自组织网络。无线自组织网络和传感器网络目前已广泛应用在军事通信、救灾行动、环境监测、智能交通、医疗保健、民用智能家居等众多领域。特别当传感器网络作为物联网感知层的重要组成部分时，随着物联网在各行各业中的应用和推广，传感器网络将给人们的工作、生活等各个领域带来深远的影响。

然而，无固定基础设施、无线接入、移动性、快速随机部署等特征，使安全问题成为无线自组织网络、传感器网络中非常有挑战性的领域。由于传感器节点和传感器网络自身的限制，如传感器节点的电池能量、内存储器、传输范围、节点容易受损等，加之传感器网络有着与传统网络明显不同的技术要求，使得在传统网络中成熟的安全技术，如传统的公钥基础设施（PKI）等，不能直接应用。

本书作者 Erdal Çayırcı 教授和 Chunming Rong 教授多年致力于传感器网络、计算机与网络和无线通信安全等领域的研究工作，成果显著。Erdal Çayırcı 是北大西洋公约组织联合作战中心 CAX 支撑分部负责人、挪威斯塔万格大学电子和计算机工程学院教授。他是论文《A Survey on Sensor Networks》的合作者之一（该论文于 2002 年 8 月发表在《IEEE Communications》杂志上，根据 2011 年 3 月 21 日 Google 学术搜索结果，目前已被引用 6137 次）。Chunming Rong 现在是挪威斯塔万格大学计算机系终身教授、服务计算研创中心主任、国际云计算协会（www. cloudcom. org）会长、IEEE CloudCom 国际云计算学术会议系列创始人和主席。

本书内容覆盖与无线自组织网络相关的基础和关键问题，重点阐述在无线自组织网络、传感器网络特征和限制下的新的安全挑战及解决方案。本书在内容编排上充分体现了该领域多学科交叉的特点，涵盖通信、网络、信息安全、密码学等相关领域的知识。全书共分 15 章，内容分为两个部分：第一部分介绍与无线自组织网络相关的基础和关键问题，包括无线自组织网络、传感器网络和 Mesh 网络（WASM）及其应用领域，无线媒介基础知识，数据链路层、网络层和传输层的安全挑战和解决方案，WASM 特有的挑战及已有的安全解决方案。第二部分详细讨论 WASM 中的安全攻击和对策，包括 WASM 中的安全攻击、密码学基础、基本问题相关的挑战和方案，保护隐私、匿名性、入侵检测、流量分析、访问控制、容错等

方面的相关挑战和方案，安全路由，WASM 特有的挑战和方案，信息战和电子战，无线网络安全相关标准等。

本书部分章节初译得到研究生陈曦、熊裕聪、张攀的努力协助，在此表示感谢。惠颖、顾斐、段涛、王澍波、李珍、潘亮协助校对了部分初稿。全书由李勇统稿审校。

译者还要感谢英文版原书作者 Erdal Çay₁rc₁ 和 Chunming Rong 教授对本书翻译工作的支持。感谢约翰威立国际出版公司在本书版权引进方面所做的工作。

本书的翻译和出版得到北京交通大学红果园双百人才培育计划、中央高校基本科研业务费专项资金资助（2009JBM004）支持，在此表示感谢。

由于译者水平有限，书中难免有疏漏或错误，敬请广大读者批评指正。

译　者

2011 年春于北京

前　言

由随机部署的自组织无线节点构成的自组织网络有广泛的应用，如用于军事通信、灾难救援行动和人员稀少地区的临时网络等，因此近 20 年自组织网络已被广泛研究。最近，传感器网络吸引了学术界和企业界的兴趣。传感器网络是一种能量受限的、可扩展的自组织网络。另一种形式的自组织网络即 Mesh 网络，针对发展中地区的无基础设施的网络环境、廉价多跳无线回程连接（Wireless Backhaul Connections）和社区无线网络等应用领域。无线接入、移动性、快速随机部署等特征使安全问题成为这类网络非常有挑战性的领域。安全也是使诸多自组织应用实用化的一个关键问题。尽管这类网络的安全已广泛研究了十余年，但仍然存在许多挑战期待提出更佳的解决方案。因此，许多来自学术界和企业界的研究者和工程师们还在继续研究这一领域。

本书为 14～18 周（每周 3 小时）的研究生课程（计算机工程、通信工程、电子工程或计算机科学等专业）设计。需要先修计算机网络相关课程。本书自包含论及无线自组织网络问题，并介绍无线自组织网络、传感器网络、Mesh 网络的安全问题，提供这些领域安全方面的新进展。本书也可作为参考书，读者可能包括来自网络或安全领域、企业或军方的工程师，希望进行无线自组织网络、传感器网络、Mesh 网络的协议、网络和安全系统设计与实现任务。

本书包括两个部分：第一部分介绍与无线自组织网络相关的基础和关键问题。这部分强调了第二部分要讨论的安全问题。第二部分详细讨论无线自组织网络、传感器网络和 Mesh 网络中的安全攻击和对策。有一章非常简要地介绍信息战和电子战及相关术语。最后一章简要介绍了相关标准。

关 于 作 者

Erdal Çayırcı

1986 年毕业于陆军学院，1989 年毕业于位于桑德霍斯特的皇家陆军军官大学。1995 年在中东技术大学获得计算机工程专业硕士学位，2000 年在 Bogazici 大学获得计算机工程专业博士学位。2005 年，他从陆军退役时身为陆军上校。2001 ~ 2005 年，他是伊斯坦布尔技术大学、Yeditepe 大学、海军理工学院副教授。2001 年，他还是乔治亚技术学院宽带无线网络实验室访问研究员、电子和计算机工程学院访问讲师。目前，他是位于挪威斯塔万格的北大西洋公约组织联合作战中心 CAX 支撑分部负责人、斯塔万格大学（University of Stavanger）电子和计算机工程学院教授。他的研究领域包括军事建设性仿真、传感器网络、移动通信、军事战术通信。Çayırcı 教授担任国际期刊《IEEE Transactions on Mobile Computing》、《Ad Hoc Networks》、《Wireless Networks》编委，曾被期刊《Computer Networks》、《Ad Hoc Networks》和《Special Topics in Mobile Networking and Applications（MONET）》特邀主编四辑专刊。

因为 2002 年 8 月在《IEEE Communications》杂志上发表了题为《A Survey on Sensor Networks》的学术论文，他获得 2002 年度 IEEE 通信学会最佳指导论文奖。2003 年获得土耳其总参谋部 Fikri Gayret 奖、2005 年获得土耳其海军年度创新奖、2006 年获 ITEC 优秀奖。

Chunming Rong

分别于 1993 年、1995 年和 1998 年在挪威卑尔根大学（University of Bergen）获得计算机科学专业学士、硕士和博士学位。1995 ~ 1998 年，他是卑尔根大学的 Research Fellow。2001 ~ 2003 年，他在 Simula 研究实验室从事博士后研究工作。目前，他是斯塔万格大学计算机科学系教授和负责人。自 2005 年，担任奥斯陆大学兼职教授。2007 年，容教授获得 ConocoPhilips 通信奖（挪威）。1999 年，他的论文《New Infinite Families of 3-Designs from Preparata Codes

over Z_4》获得《Discrete Mathematics》期刊主编奖。

2003～2006 年，他是国际期刊《International Journal of Computer Science & Applications（IJCSA）》副编辑、《International Journal of Mobile Communications（IJMC）》编委会成员。2007 年，他担任 IEEE 网络和分布式系统安全国际研讨会（SSNDS）程序主席，2008 年担任该会议总主席。2007 年，他担任在香港召开的自治和可信计算国际会议（ATC）的颁奖主席，2008 年担任 ATC 会议总主席（挪威）。2008 年，他还是普适智能和计算国际会议（UIC）总主席。

2005～2007 年，容教授担任挪威计算机科学会议基金委员会主席；2007～2011 年，担任挪威信息安全网络（NISNet）委员会成员、挪威信息学顾问委员会成员。他曾是挪威研究顾问委员会“ICT 安全和脆弱性（IKT-SoS）”项目成员。目前他还为挪威石油工业协会（OLF）集成运营安全工作组服务。

作为项目负责人，他承担过挪威研究顾问委员会资助项目“油气钻井和填充中的数据处理集成”（2008～2010）、“安全和可靠的无线自组织通信（SWACOM）”（2006～2009）、“智能家庭环境中的基于 IP 的综合服务”（2007～2010）。挪威信息安全网络（NISNet）也获得了挪威研究顾问委员会的年度资助。

容教授研究兴趣包括计算机和网络安全、无线通信、密码学、身份管理、电子支付、编码理论和语义网技术。

致　　谢

感谢我们的博士生 Turgay Karlidere、Yan Liang 和 Son Thanh Nguyen。Turgay Karlidere 对第 4 章媒介访问控制内容作了贡献，并提供其中相关的标准。Son Thanh Nguyen 撰写了第 15 章关于数据安全标准的内容。Yan Liang 帮助编辑了两章。

10.3 节摘自一篇 Hegland 等（2006）共同署名的文献，我们要感谢论文的合作者 A. M. Hegland、E. Winjum、S. F. Mjølsnes、Ø Kure 和 P. Spilling，允许我们把这篇论文写进本书。

缩略语表

AAA	Authentication Authorization Accounting	认证、授权、审计
ACQUIRE	Active Query Forwarding in Sensor Network	传感器网络主动查询转发
ADC	Analog-to-Digital Conversion	模-数转换
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	认证头
AKA	Auxiliary Key Agreement	辅助密钥协商
AM	Access Mesh	接入 Mesh
AOA	Angle Of Arrival	到达角度
AODV	Ad hoc On-demand Distance Vector Routing	自组织按需距离矢量路由
ARAN	Authenticated Routing for Ad hoc Networking	自组织网络认证路由
ARIADNE	On-demand Secure Ad hoc Routing	按需安全自组织路由
BACNet	Building Automation and Control Network	楼宇自动化和控制网络
BAN	Body Area Network	体域网
BEC	Backward Error Correction	后向纠错
BGP	Border Gateway Protocol	边界网关协议
BM	Backbone Mesh	骨干 mesh
BWA	Broadband Wireless Access	宽带无线接入
C2	Command and Control	指挥和控制
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance	指挥、控制、通信、计算、情报、监测、侦察
C4ISRT	Command, Control, Communications, Computer, Intelligence, Surveillance, Reconnaissance, Targeting	指挥、控制、通信、计算、情报、监测、侦察、目标捕获
CA	Certificate Authority	证书权威机构
CA	Collision Avoidance	碰撞避免
CBRN	Chemical, Biological, Radiological and Nuclear	化学、生物、放射、核
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	计数器模式密码块链消息认证码协议
CD	Collision Detection	碰撞检测
CDMA	Code Division Multiple Access	码分多址

COMINT	Communications Intelligence	电信侦查
CRC	Cyclic Redundancy Check	循环冗余校验
CRL	Certificate Revocation List	证书撤销表
CRS	Charging and Rewarding Scheme	计费和奖励方案
CSMA	Carrier Sense Multiple Access	载波侦听多址访问
CTS	Clear To Send	消除发送
DADMA	Data Aggregation and Dilution by Modulus Addressing	通过模数寻址的数据聚合和稀疏
DCF	Distributed Coordination Function	分布式协调功能
DCMD	Detecting and Correcting Malicious Data	检测和纠正恶意数据
DES	Data Encryption Standard	数据加密标准
DISN	Defense Information System	国防信息系统
DLL	Data Link Layer	数据链路层
DOS	Denial Of Service	拒绝服务
DS	Direct Sequence	直接序列
DSR	Dynamic Source Routing	动态源路由
EAP	Extensible Authentication Protocol	可扩展的认证协议
ECM	Electronic Counter Measure	电子对策
EGP	Exterior Gateway Protocol	外部网关协议
ELINT	Electronic Intelligence	电子情报
EMP	Electro Magnetic Pulse	电磁脉冲
EPM	Electronic Protection Measure	电子保护手段
ESM	Electronic Support Measure	电子支持手段
ESP	Encapsulated Security Payload	封装安全载荷
ESRT	Event-to-Sink Reliable Transport	事件到汇聚节点的可靠传输
EW	Electronic Warfare	电子战
FDD	Frequency Division Duplexing	频分双工
FDM	Frequency Division Multiplexing	频分复用
FDMA	Frequency Division Multiple Access	频分多址接入
FEC	Forward Error Control	前向错误控制
FH	Frequency Hopping	跳频
GPS	Global Positioning System	全球定位系统
HCI	Human-Computer Interaction	人机交互
HMAC	Hash Message Authentication Code	哈希消息认证码

IBC	Identity-Based Cryptography	基于身份的密码学
IBE	Identity-Based Encryption	基于身份的加密
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IDS	Intrusion Detection System	入侵检测系统
IEEE	International Electrical and Electronics Engineers	国际电气与电子工程师学会
IF	Intermediate Frequency	中频
IGP	Interior Gateway Protocol	内部网关协议
IHL	IP Header Length	IP 头长度
IKA	Initial Key Agreement	初始密钥协商
INSENS	Intrusion-tolerant Routing in Wireless Sensor Networks	无线传感器网络入侵容忍路由
IP	Internet Protocol	互联网协议
IrDA	Infrared Data Association	红外数据协会
IS-IS	Intermediate System-Intermediate System	中间系统-中间系统
ISM	Industrial, Scientific and Medical	工业、科学和医疗
IV	Initialization Vector	初始矢量
LA	Location Area	位置区域
LAS	Local Area Subsystem	局域子系统
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LEACH	Low-Energy Adaptive Clustering Hierarchy	低功耗自适应聚簇分层
MAC	Medium Access Control	媒介访问控制
MAC	Message Authentication Code	消息认证码
MACA	Multiple Access with Collision Avoidance	避免碰撞多址访问
MACAW	Multiple Access with Collision Avoidance, Wireless	MACA 无线
MARQ	Mobility-Assisted Resolution of Queries	移动性辅助查询解析
MD	Message Digest	消息摘要
MIC	Message Integrity Code	消息完整性码
MIMO	Multiple Input, Multiple Output	多输入多输出
MMSE	Minimum Mean Square Estimation	最小均方估计
MPDU	MAC Protocol Data Unit MAC	协议数据单元
MR	Mobile Radio	移动无线电
MS	Mobile Subsystem	移动子系统
MT	Mobile Terminal	移动终端
NATO	North Atlantic Treaty Organization	北大西洋公约组织
NAV	Network Allocation Vector	网络分配矢量

OSI	Open System Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
PAMR	Power-Aware Many-to-many Routing	功耗感知多对多路由
PC	Personal Computer	个人计算机
PCF	Point Coordination Function	点协调功能
PCM	Pulse Code Modulation	脉冲编码调制
PDA	Personal Digital Assistant	个人数字助理
PKC	Public Key Cryptography	公钥密码学
PKG	Private Key Generator	私钥生成器
PKI	Public Key Infrastructure	公钥基础设施
PRMA	Packet Reservation Multiple Access	分组预约多址接入
PSFQ	Pump Slowly, Fetch Quickly	缓发快取
PSK	Preshared Key	预共享密钥
QAM	Quadrature Amplitude Modulation	正交调幅
QoS	Quality of Service	服务质量
QPSK	Quadrature Phase Shift Keying	正交相移键控
QRS	Quarantine Region Scheme	隔离区方案
RADIUS	Remote Authentication Dial In User Service	远程认证拨入用户服务
RAP	Radio Access Point	无线电接入点
RBS	Reference Broadcast Synchronizations	参照广播同步
RC	Rivest Cipher	Rivest 密码
RIP	Routing Information Protocol	路由信息协议
RMST	Reliable Multisegment Transport	可靠多片段传输
RSA	Ron Rivest, Adi Shamir, Len Adleman	Rivest, Shamir, Adleman（姓氏首字母）
RSN	Robust Security Network	鲁棒安全网络
RSS	Received Signal Strength	接收信号强度
RTS	Request To Send	请求发送
SA	Security Association	安全关联
SAODV	Secure Ad hoc On-demand Distance Vector	安全按需自组织距离矢量
SHA	Secure Hash Algorithm	安全哈希算法
SIGINT	Signal Intelligence	信号情报
SLSP	Secure Link State routing Protocol	安全链路状态路由协议
SMCS	System Management and Control Subsystem	系统管理和控制子系统
SN	Sequence Number	序列号
SNDV	Sensor Network Database View	传感器网络数据库视图
SNEP	Sensor Network Encryption Protocol	传感器网络加密协议

SNR	Signal-to-Noise Ratio	信噪比
SOHO	Small Office, Home Office	小办公室，家庭办公室
SPAAR	Secure Position-Aided Ad hoc Routing	安全位置辅助自组织路由
SPI	Sequence Parameter Index	序列参数索引
SPIN	Sensor Protocols for Information via Negotiation	基于信息协商的传感器协议
SPINS	Security Protocols for Sensor Networks	传感器网络安全协议
SQTL	Sensor Query and Tasking Language	传感器查询与任务分配语言
TACOMS	Post-2000 Tactical Communications	2000 年后军事通信
TCP	Transmission Control Protocol	传输控制协议
TDD	Time Division Duplexing	时分双工
TDM	Time Division Multiplexing	时分复用
TDMA	Time Division Multiple Access	时分多址接入
TDOA	Time Difference Of Arrival	到达时间差值
TESLA	Timed Efficient Stream Loss-tolerant Authentication	定时高效流容忍损耗认证
TKIP	Temporal Key Integrity Protocol	临时密钥完整性协议
TOA	Time Of Arrival	到达时间
TPSN	Timing-sync Protocol for Sensor Networks	传感器网络时间同步协议
TRANS	Trust Routing for Location-aware Sensor Networks	位置感知传感器网络可信路由
WAS	Wide Area Subsystem	广域子系统
WASM	Wireless Ad hoc, Sensor and Mesh network	无线自组织网络、传感器网络和 Mesh 网络
WEP	Wired Equivalent Privacy	有线对等保密
Wi-Fi	Wireless Fidelity	无线保真
WiMAX	Worldwide interoperability for Microwave Access	全球微波接入互操作性
WLAN	Wireless Local Area Network	无线局域网
WMAN	Wireless Metropolitan Area Networks	无线城域网
WMN	Wireless Mesh Network	无线 Mesh 网络
WPA	Wi-Fi Protected Access	Wi-Fi 保护接入
WPAN	Wireless Personal Area Network	无线个域网
WSAN	Wireless Sensor and Actuator Network	无线传感器网络和执行器网络

目　　录

第一部分

无线自组织网络、传感器网络和 Mesh 网络

第1章 绪 论

与有线媒介相比，尽管无线媒介有有限的频谱和附加的限制，它为移动通信提供了唯一手段。另外，对有限频谱和高级物理层/数据链路层协议的有效利用，使得在有限的无线频谱上的宽带通信和集成业务成为可能。通过无线自组织网络随机、快速地部署大规模无线节点（Tetherless Node），这种技术还广泛应用在比如军事通信、救灾行动和人口稀少地区的临时网络等领域。可见，无线自组织网络应用已非常普遍。然而，除有线网络已存在的安全问题外，无线自组织网络也带来了新的安全挑战：

1）无线广播媒介比有线媒介更易于被搭线窃听。

2）无线媒介只有有限容量，需要负载更少的高效方案。

3）自组织网络需要自形成、自组织、自愈算法，以及处理隐藏和暴露终端节点等挑战的方案，可能需要设计应对更复杂的安全攻击。

4）无线媒介易于受通信干扰和其他拒绝服务攻击的影响。

无线传感器网络和执行器网络（Wireless Sensor and Actuator Network，WSAN）基于随机部署大规模微型传感器节点和执行器（Actuator）进入或非常接近待观察的事物/现象。无线传感器网络推动了许多应用领域，比如通过军事无人传感器网络的军事侦察、借助体域网（Body Area Network，BAN）进行老年人的健康监测、建立楼宇自动化和控制网络（Building Automation and Control Network，BACNet）实现楼宇自动化。这些本质上都是带有附加的、更严格限制的自组织网络。相比传统自组织网络，这些网络需要高能效并可扩展，带来的安全挑战更严峻。因为传感器节点相比典型自组织网络节点如个人数字助理（Personal Digital Assistant，PDA）和笔记本电脑，是微型的、容量有限的，所以适于 WSAN 的安全方案应该需要较少的计算能耗和存储。

无线 Mesh 网络（Wireless Mesh Network，WMN）是另外一种自组织网络。无线 Mesh 网络可应用于发展中地区的无基础设施网络、价格低廉的多跳无线回程连接（Wireless Backhaul Connections）和社区无线网络。事实上，自组织网络可认为是无线 Mesh 网络的子集。因为无线 Mesh 网络为其他 Mesh、自组织或基于基础设施的网络运转提供无线中枢（Backbone），例如互联网、IEEE 802.11、IEEE 802.15、IEEE 802.16、移动电话、无线传感器、无线保真（Wireless Fidelity，Wi-Fi）、全球微波接入互操作性（Worldwide interoperability for Microwave Access，WiMAX）和 WiMedia 网络。缺少集中的权威机构、可使用各种接入技术访问网络，使得无线

Mesh 网络安全成为一个更有挑战的领域。

1.1　信息安全

为使上述和更多的自组织网络应用更加实际，它们必须可以安全防御各种攻击。安全攻击是破坏他人拥有信息的安全性的尝试（RFC 2828）。在本书第二部分，我们区分并讨论针对自组织网络的所有安全攻击。需要安全服务防御这些攻击，并保证信息的安全；这些服务可以分成两大类：通信安全和计算机安全（见图 1-1）。通信安全防御经由通信链路或无意发射（Unintentional Emanations）的被动攻击或主动攻击。它确保通信业务以必需的质量等级持续，确保秘密数据或信息不能被未授权节点从通信中截获。计算机安全保证计算机硬件和软件的安全。它探测节点或主机的安全威胁，从攻击中恢复特定的节点或主机。

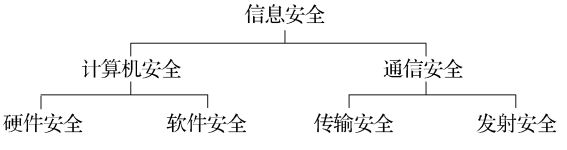


图 1-1　信息安全

1.1.1　计算机安全

宿主计算机或网络节点可被物理攻击，某些硬件组件可能会被替代、损坏或失效。另外，硬件电子元器件会被微生物侵蚀。硬件安全主要是预防、探测和修复这些物理攻击。

对计算机硬件的另一种攻击，特别是在战场上，可能是通过电磁脉冲（ElectroMagnetic Pulse，EMP）武器来进行。可发射电磁脉冲的便携系统目前已经可以使用，可以嵌入关键硬件部件抵抗这类攻击。电磁脉冲不仅损坏软件，也可以烧毁硬件。

病毒、蠕虫和木马是攻击软件的技术的例子。它们是可以感染敌手计算机的代码。病毒可以多次复制自身，一般设计用来给被攻击的软件带来破坏。木马是对被攻击系统进行未授权访问的一种手段。蠕虫可以在网络中从一个节点到另一个节点复制自身并消耗计算能量和内存等资源。有许多软件包可以消除这些威胁。然而，这些软件大多数只能检测已知的病毒、蠕虫和木马。因此，它们完全取决于攻击程序相关特征的可用性。

1.1.2　通信安全

通信安全的一个重要部分是传输安全，即预防传输中的保密数据泄漏给未授权方、抵御通过通信链路对计算机的攻击、确保通信服务不被恶意攻击干扰。注意到一旦计算机被网络病毒感染，相应的对策可归入计算机安全范畴。然而，一个被攻

击的网络节点可从内部攻击网络，使网络安全防御内部攻击也应该在传输安全范畴中考虑。

通信安全的另一个重要部分是发射安全（Emanation Security）。计算机可能会通过 Van Eck 辐射（Van Eck Radiation）或传导发射信号。每一个电子设备（如计算机、复印机、打印机、电话等），发射电磁波，称为 Van Eck 辐射。有可能从远处接收这种电磁泄漏，并结合显示屏截屏、击键和复制文档；也有可能通过靠近传输或存储保密数据设备的介质，如输电线、金属管、水管、电缆等传导保密数据。发射安全旨在预防这类攻击，军方对这个领域已进行广泛的研究。这类系统称为 TEMPEST。TEMPEST 不是一个缩略词，而是用于军事目的的一个词。

1.2 本书范围

本书主要讨论无线自组织网络、传感器网络和 Mesh 网络（Wireless Ad hoc, Sensor and Mesh network, WASM）的传输安全。其他文献中，传输安全也称网络安全或互联网安全，这些术语是同义的，涵盖除了前两节阐述的计算机安全和发射安全之外的所有信息安全问题。尽管本书集中讨论传输安全，由于相关性，并且 Van Eck 辐射和电磁脉冲对军方尤其重要，而且 WASM 的重要应用领域之一是军事领域，本书也涉及计算机安全和发射安全。本书最大限度地不泄漏任何机密信息。本书阐述的是一般意义上的，针对一般需求和设计原则，在公共领域可获得的内容，并不针对任何特定的军事系统。

本书详细阐述 WASM 中的所有已知的安全缺陷，解释可以利用这些缺陷的威胁和攻击。面对这些潜在的威胁和攻击，本书研究如何提高下述安全服务：

1）认证：确保消息来自所声称的消息源；
2）访问控制：预防未授权使用的网络资源；
3）机密性：确保保密数据不能被未授权接收方泄漏；
4）完整性：保证消息在传输中未被篡改；
5）不可否认性：确保消息源和消息目的地与消息中所指定的一样。

其他诸如下列安全相关问题也在本书范围内：

1）防御拒绝服务（Denial Of Service, DOS）攻击；
2）在敌对环境中的可靠的端到端服务；
3）安全路由；
4）预防滥用有限资源的措施；
5）减少安全方案计算、存储、能量消耗等代价的措施。

1.3　本书组织

本书希望编写成面向学术界和企业界的内容自包含的教材。因此，本书包括两个部分：首先介绍与 WASM 相关的基础和关键问题。尽管第一部分的首要目标是为读者提供必需的背景知识，但在本部分中，我们也突出和阐释对信息安全有影响的事实。第二部分，本书提供 WASM 安全的新进展。

包括绪论在内，本书第一部分包括 7 章。第 2 章介绍 WASM 及其应用领域，因为军事通信是 WASM 最重要的应用领域之一，而且有一些对安全产生影响的特性，本章专门有一节介绍军事通信。然后讨论影响网络设计的因素及其如何影响安全方案。

第 3 章阐述与无线媒介相关的基础知识，如物理层方面的知识。本章详细阐述传播环境、调制、无线频道损伤（Wireless Channel Impairments）、干扰以及与这些问题相关的安全考虑。

第 4 ~ 6 章分别解释在数据链路层、网络层和传输层的挑战和解决方案。分层的方法可以提供协议和方案的互操作性和可用性。然而，分层并不总能产生最佳方案。因此，相比跨层设计，在代价更高的协议栈基础上，对底层细节的透明性、协议的互操作性和可重用性可以满足。因为 WASM 引入一些非常严格的限制，所以本书中的跨层协议比较普遍。

第 7 章介绍 WASM 特有的挑战，如节点定位（Node Localization）、时间同步、寻址、覆盖、移动性和资源管理，以及应对这些挑战的文献中已有的安全解决方案。

本书第二部分包含 8 章。首先详细讨论 WASM 中的安全攻击。第 9 章介绍密码学基础。第 10 章讨论与基本问题相关的挑战和方案，如自举（Bootstrapping）、密钥分发和完整性。第 11 章介绍保护隐私、匿名性、入侵检测、流量分析、访问控制、容错（Tamper Resilience）、可用性和合理性（Plausibility）的相关挑战和方案。

自组织网络的自形成、自组织和自愈特性为信息安全带来新的挑战。第 12 章提供与安全路由相关的挑战和方案，接下来一章讨论 WASM 特有的挑战和方案。

第 14 章是关于信息战和电子战及其与 WASM 安全相关性的简要介绍。注意电子战里面包含的内容非常多，本章只对其进行简单介绍。最后一章是关于无线网络安全相关标准的介绍。

1.4　电子资源

本书网址为 http：//www. securityinadhoc. net/，在这个网站可获得下列资源：

1）**幻灯片**：幻灯片用以补充书中内容，是为以本书作为教材或参考书的 14 周课程设计的。幻灯片会保持更新。

2）**更正表**：对本书的所有更正列在此表中。如果你对本书有任何评论或改进建议，请通过网站上的“contact us”发邮件给我们。

3）**兴趣组**：这个链接可为你提供用户名和密码，用来访问与本书内容相关的兴趣组。

4）**有用的链接**：提供有用的网站链接。

1.5 复习题

1.1 什么是信息安全？信息安全如何分类？

1.2 什么是 Van Eck 辐射？

1.3 什么是通过传导的发射攻击？如何预防？

1.4 病毒、蠕虫和木马之间的区别是什么？

1.5 什么是电磁脉冲攻击？

1.6 什么是安全攻击？

1.7 什么是拒绝服务攻击？

1.8 什么是安全服务？

第 2 章　无线自组织网络、传感器网络和 Mesh 网络

广义上，无线网络范式可分为无线自组织网络和蜂窝网络（Cellular Networking）两类。这两类网络间的主要不同是固定基础设施是否存在（见图 2-1）。在无线自组织网络中，没有固定基础设施，数据包通过无线多跳连接传递到目的地。节点的作用通常不只是主机，也可能是路由器，能通过其他节点转发数据包。因为节点可能不是固定的，或者说，它们可能会失败，所以自组织网络的拓扑结构可以改变。在蜂窝网络中，移动终端通过单跳无线链路达到接入点。固定基础设施把不同的接入点链接起来。因此，无线自组织网络和蜂窝网络通常分别被称为无基础设施（Infrastructureless）网络和有基础设施（Infrastructured）网络。无线自组织网络和蜂窝网络的基本特征比较见表 2-1。

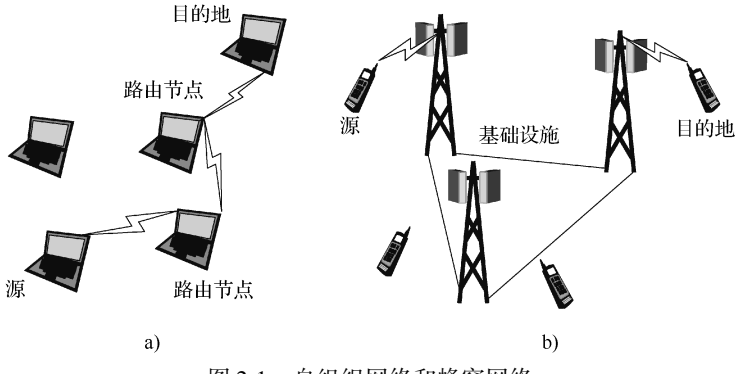


图 2-1　自组织网络和蜂窝网络

a）自组织网络　b）蜂窝网络

表 2-1　自组织网络和蜂窝网络

	自组织网络	蜂 窝 网 络
基础设施	没有基础设施	有固定基础设施
拓扑	骨干节点可能会移动。拓扑可能改变，通常是因为移动和/或节点故障	节点在基础设施中是固定的，终端可能移动，但是基础设施的拓扑很少会改变
节点	用户用的终端节点也可以用来转发其他节点的数据包	在基础设施中的节点在源点和目的地之间传送数据。它们作为终端或主机的用法是不平凡的。终端节点不从其他节点转发数据包
链路	链路大部分是无线的。端到端的连接可以通过无线多跳连接	终端节点通过无线链路接入到基础设施。在基础设施中的链路可以是无线或者有线

2.1 自组织网络和应用

在无线自组织网络中，节点通常是不囿于一定范围的（Tetherless），因而节点可以自由移动。它们可以起到主机或路由器的作用，并且可以转发其他节点的数据包。当有自形成、自配置和自愈算法用于这些节点时，可以开发一个满足各种应用需求的、非常灵活和可迅速部署的网络架构。

军事通信和军事网络是自组织网络的最明显的应用，我们将在一个单独的小节中加以讨论。除了军事通信领域外，还有很多其他的应用领域需要迅速的部署和不受范围约束的通信（Tetherless Communication）。

2.1.1 应用举例

自组织网络最明显的应用领域（但不限于）如下：

1）临时网络部署：当构造一个基础设施不可行或是代价高昂时，自组织网络可以被部署。例如，它们可以被当做集会、不发达地区或人口稀少地区或地形上很难架设基础设施的地方的临时解决方案。

2）救灾行动：当自组织网络用于在大规模灾难，如地震、海啸和洪水后救灾行动管理时，它的迅速部署能力使它成为一项杰出的技术。

3）智能楼宇：大量的传感器和执行器可以在没有架设任何基础设施的情况下部署，进而创造一个智能环境和可感知的计算环境。

4）合作对象（Cooperative Object，CO）：合作对象是实体，它们由传感器、执行器和合作对象组成，并且具有以一种智能和自治的方式与彼此以及环境通信、交互的能力，以实现特定的目标。注意这是一个递归定义。一个合作对象可以由其他合作对象组成。合作对象通常是移动的、可感知的实体，对从大量嵌入在环境中的传感器传来的实时感知数据和从附近其他合作对象传来的请求做出反应。

5）卫生保健：监测病人与老年人健康状况和行踪的系统是自组织网络的另一个明显应用领域。

2.1.2 挑战

自组织网络还有其他很多应用领域。这些应用可以通过解决特定于无线自组织网络中的挑战来实现，对其中的一些挑战简单介绍如下。

2.1.2.1 无线媒介

在自组织网络中，至少有一些通信链路是通过无线媒介建立的。无线媒介和其他媒介的主要区别如下：

1）无线媒介更容易出错。例如，在无线媒介中误码率（Bit Error Rate，BER）比光纤中的 10^7 倍还高。

2）错误比有线媒介中更猛烈（Burstier）。

3）无线媒介的载荷能力有限。在有线媒介中，可以通过铺设新的线路增加传输能力，但是在无线媒介中，频谱有限并且不能扩展。

2.1.2.2　干扰、隐藏终端和裸露终端

在广播媒介中的无约束的传输可能导致两个或更多的接收包在时间上的重叠，称为碰撞或干扰。这也可能在有线媒介中发生，但是碰撞能被检测到。然而，在无线媒介中，隐藏终端现象会阻碍碰撞的检测，即一个终端的传输可能被另一个不能被检测到的终端干扰。一个可能干扰但是不能被检测到的终端称为隐藏终端（Hidden Terminal）。例如，源 a 和源 b 传输的数据在目的地互相干扰，如图 2-2 所示。但是，没有一个源节点可以感知到对方在传输数据，因为它们互相隐藏，即它们在对方能感知的范围之外。

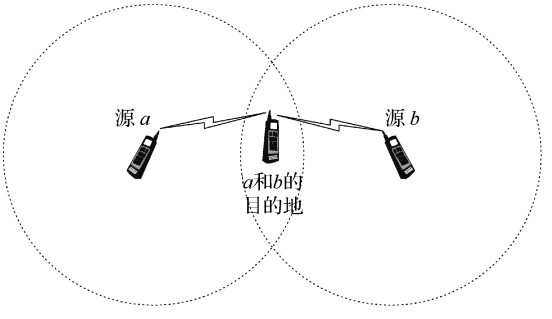


图 2-2　隐藏终端

另一种影响到自组织协议（尤其对于媒介访问控制）的现象称为裸露终端（Exposed Terminal）。为了避免和源 b 传输数据给目的地 d 产生碰撞，源 a 可能不会传输数据给目的地 c，尽管在这种情况下，在各自的目的地两个发送方传输的数据都不会产生干扰。这里，源 a 就是一个裸露终端，如图 2-3 所示。

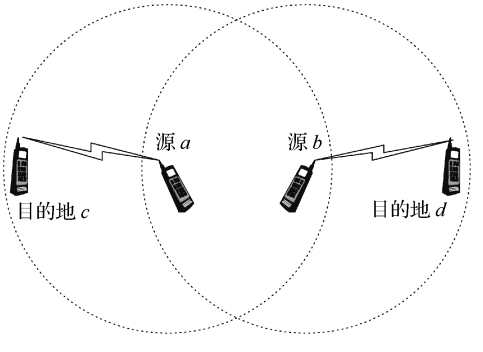


图 2-3　裸露终端

隐藏终端和裸露终端为无线自组织网络带来了挑战，处理这些问题的方案将在第 4 章中加以讨论。

2.1.2.3　移动性、节点故障、自形成、自配置、拓扑维护、路由和自愈

由于节点的移动性，由无线媒介带来的挑战更加严重，这些节点可同时作为终端和路由器。如果移动节点只是终端，在蜂窝网络中的定位管理技术可以满足。然而，在自组织网络中，任何节点既可以是一个终端，又可以是一个路由器。因此，

当节点改变位置或失效时，它们形成的网络拓扑结构就会改变。大部分自组织网络是自形成、自配置和自愈的，这意味着它们可以自主形成一个网络，并且适应网络中的改变。这些自形成和自愈方案的效率与节点拓扑数据的可用性、详细程度和准确性密切相关，这些构成了网络感知（Network Awareness）的层次。网络感知由各个节点的拓扑维护提供，这些节点不是空闲的。

在拓扑维护代价和自形成、自愈算法效率中存在一个权衡。由于拓扑数据的解析和准确性的提高，可以开发更多有效的自形成和自愈算法。但是，这也表明在拓扑维护代价上的增加，即为了拓扑维护而传输数据包的数量增加，数据包数量也取决于拓扑改变的频率。拓扑维护的过程可以根据以下标准分类：

1）为了监测目的而产生的流量：主动或被动；

2）监测频率：按需（事件驱动）或者连续的（时间驱动）；

3）信息的复制：集中或分散。

我们将在第 5 章中更详细地研究关于拓扑维护的问题。

2.1.2.4 节点定位和时钟同步

在一个没有固定基础设施的网络中，节点定位和时钟同步变得更具有挑战性。这两个问题对于很多应用中的安全和网络协议非常重要。因此，我们将在第 7 章中分节对它们进行讨论。

2.1.2.5 端到端可靠性和拥塞控制

因为拓扑改变问题在自组织网络中是十分突出的，并且无线媒介容易出错，所以端到端面向连接的传输控制协议（Transmission Control Protocol，TCP）不太适合自组织网络。TCP 是基于传输中数据包的丢失大部分归因于拥塞的假设。

2.2 传感器网络和执行器网络

一个无线传感器网络和执行器网络（WSAN）是一个部署在被观察的事物里或者在很接近它的地方的自组织网络。不像一些现有的传感技术，传感器网络节点的位置不需要设计或预先确定。这使得在难以接近的地形随机部署成为可能。另一方面，这意味着传感器网络协议和算法必须具有自组织能力。

传感器网络的另一个独特特性是传感器节点的协作。传感器网络节点都配有一个板载处理器（On-board Processor）。并不是传送原始数据给负责融合的节点，传感器网络节点使用其处理能力在本地进行简单的计算，并且只传输必需的部分处理的数据。

在无线传感器网络和执行器网络中，成百上千的传感器节点（Sensor Node，简记 snode）被密集部署在整个传感器区域内。两个相邻的传感器节点的距离通常被限制在几米内。节点通常在传感器区域内通过随机播撒来部署。在某些应用中，控

制各种设备的执行器节点（Actuator Node，简记 anode）也能在传感器网络内定位。如图 2-4 所示，收集节点（Collector Node，简记 cnode）可以位于传感器区域里面或者接近传感器区域，这些收集节点通常比在区域内的其他节点更有能力。收集节点通常也被称做汇聚节点（Sink）或者基站（Base Station），任务是负责从传感器节点收集感知数据，然后把收集的数据传给用户。在许多应用中，它们也负责启动任务分派（Task Dissemination）。通过传感器节点收集的感知数据按照自组织方式在传感器网络多跳转达，在汇聚节点中集中，这可以视为在传感器网络和用户之间的接口。多个传感器网络可以通过因特网或者在汇聚节点和网关之间的直接连接，集成为一个更大的网络。

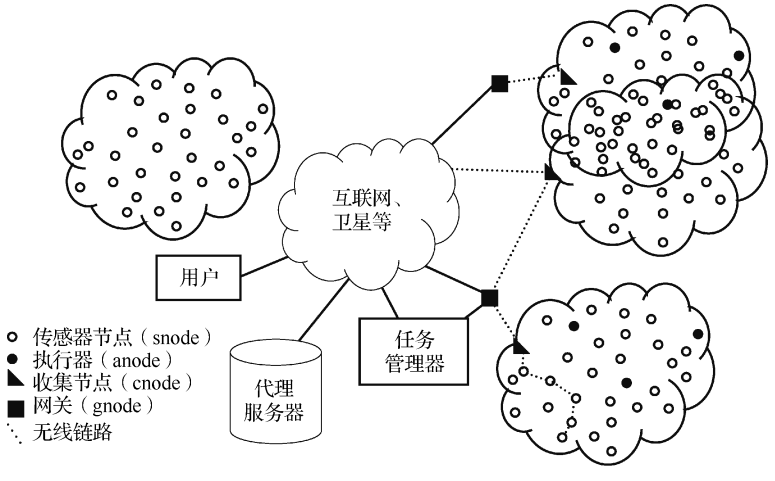


图 2-4　无线传感器网络和执行器网络

2.2.1　应用举例

无线传感器网络和执行器网络有广阔的潜在应用，包括复杂系统的安全和监测、控制、驱动和维护，室内外环境的细粒度监控。这些应用的一些例子解释如下：

1）军事应用：无线传感器网络也许是军事指挥、控制、通信、计算机、情报、监测、侦察、目标捕获（Command，Control，Communications，Computers，Intelligence，Surveillance，Reconnaissance and Targeting，C4ISRT）系统的主要部分。对于军事 C4ISRT 系统而言，传感器网络的迅速部署、自组织和容错特性使其成为一项非常有前景的传感技术。由于传感器网络是基于密集部署一次性的、低开销传感器节点，在敌方作战中一些节点的拆除不会像传统节点的拆除那样影响一次军事行动。一些军事应用包括盟军追踪、战场监测、侦查，目标捕获，战斗损伤评估和化学、生物、放射和核（Chemical Biological Radiological and Nuclear，CBRN）检测。

2）环境应用：传感器网络的一些环保应用包括跟踪物种的移动，如栖息地监

测、监测影响农作物和牲畜的环境状况、灌溉、对于大规模土地监测的宏观调控手段、行星探测、生化检测。

3）商业应用：有很多潜在的和新兴的商业无线传感器网络和执行器网络应用，如库存管理、生产质量监测、智能办公室、病人和老年人监控、材料的疲劳监测和办公楼的环境控制。未来会有更多的无线传感器网络和执行器网络应用，如医疗植入通信服务，许多传感器和执行器被植入人体，用于持续的检测、人工免疫系统的建立和瘫痪肌肉的刺激等各种目的。

2.2.2 挑战

无线传感器网络和执行器网络在许多方面不同于传统网络系统。它们通常包括大量在空间中分布的、能源受限的、自配置和自感知的节点。此外，它们往往是自治的，并且需要高度的协作和适应，以执行需要协调的任务和网络功能。因此，除了那些传统无线自组织网络产生的问题（Akyildiz et al.，2002），它们带来了新的挑战。

2.2.2.1 拓扑改变

传感器节点可以在一些无线传感器网络和执行器网络中静态部署。但是，由于能源枯竭或销毁，设备故障是一个常见的问题。在传感器网络中也可能有高速移动的节点。此外，随着任务动态变化，传感器节点和网络经历不同的变化，它们可能是蓄意干扰的目标。因此，传感器网络拓扑可能比传统的自组织网络更易于频繁的变换。

2.2.2.2 容错

传感器网络应该能够保持它们的功能，不会因传感器节点故障而产生任何中断。协议和算法可以设计成能够表示传感器网络应用所需的容错级别。应用的需求通常互不相同。例如，一个军事传感器网络的容错需求可以被认为高于那些家庭应用的需求，因为传感器节点在军事传感器网络中有更高的故障率，在军事领域里，传感器网络故障的影响比一个家庭传感器网络故障的影响严重得多。

因为几乎所有的因素都会影响传感器网络的设计，可以看到各种传感器网络应用的需求是不同的。此外，因为有相关的严格限制，所以一般需要在这些因素之间权衡。因此，万能的通用设计对于传感器网络中的许多任务来说是不可能的。总的来说，需要不同的方案满足不同应用的需求。

2.2.2.3 可扩展性

部署在一个传感器区域的传感器节点数量在一些应用中可能达到上百万。此外，在一些应用中，节点的密度可能高达每立方米 20 个。为传感器网络开发的各种方案必须具备足够的扩展性，以应付在数量级上高于所有其他类型网络的节点密度和数量。

2.2.2.4　传感器节点硬件

一个传感器节点由四个基本组件构成：感知单元、处理单元、收发器单元和能量单元。它们也可以有与应用相关的其他组件，如一个位置查找系统、一个能量产生装置和/或一个自移动装置（Mobilizer）。感知单元通常由两个子单元组成：传感器和模-数转换器（Analog-to-Digital Converters，ADC）。由传感器基于观察到的现象或刺激产生的模拟信号被模-数转换器转换成数字信号，然后送到处理单元。一个传感器节点可能附属于不止一个传感器。例如，一个温度传感器和一个湿度传感器可能连接同一个传感器节点。处理单元管理让一个传感器节点和其他节点相互合作，以完成指定感知任务的过程，处理单元通常与一个小的存储单元相关联。收发器单元把节点连接到网络上。

一个传感器节点的最重要组件之一是能量单元。能量单元可能由一个能源提取工具如太阳电池支持。还有其他子单元，这取决于应用。大部分传感器网络路由技术和感知任务需要高度精确的位置信息。这样，对于一个传感器节点来说，有一个位置查找系统是正常的。在需要完成指定任务时，有时可能需要一个自移动装置移动传感器节点。所有这些子单元希望能适合于一个火柴盒大小的模块。在一些应用中，所需尺寸甚至小于 $1cm^3$。

2.2.2.5　生产成本

如在 2.2.2.3 节所述，一个传感器网络可能包括上百万个传感器节点。因此，为了使这种网络可行，传感器节点的成本必须低廉。

2.2.2.6　环境

传感器节点密集部署在非常接近或直接在被观察的事物里面。因此，它们通常在无人的情况下在偏远的地区工作，一般是在极度严峻的环境下。它们在海底高压下、在废墟或战场等困难环境下、在飞机发动机喷嘴或在北极地区等极端温度下、在有意干扰等极端嘈杂环境下工作。

2.2.2.7　功耗

无线传感器网络节点只能装备一个有限的能源。在一些应用情景下，能源补给可能不可行。因此，传感器节点的寿命完全取决于电池的寿命。因此，能量保存和能量管理成为另一个重点。在其他移动和自组织网络中，功耗成为设计上重点考虑的因素，但不是主要考虑的因素，只是因为能源可以被用户替换。在传感器网络中，能效（Power Efficiency）是一个重要的性能指标，直接影响到网络的寿命。

在传感器网络中的功耗可以被分为三个区域：感知、通信和数据处理。能量感知随应用种类而变化。数据通信是能源消耗的主要原因，这包括数据传输和接收。可以证明，对于低辐射功率的短距离通信，传输和接收消耗的能量几乎一样。另一个关系到数据通信的重要考虑因素是路径损耗指数 λ。由于低洼天线（Low-lying Antennae），在传感器网络中，λ 接近于 4。因此，有更多跳数的短距离路径能比更

少跳数的长距离路径有更高的能效。

在数据处理上的能源消耗比数据通信时低得多。在 Pottie 和 Kaiser（2000）文献中所描述的例子有效地解释这种不对等。假设瑞利衰落（Rayleigh Fading）和四次幂距离损失（Fourth Power Distance Loss），100m 传输 1000bit 能量消耗大约和用每瓦每秒处理 1 亿条指令的处理器执行 300 万条指令的能量消耗差不多。

2.3 Mesh 网络

在无线 Mesh 网络（WMN）中，各个节点既可以是一个路由器，也可以是一个主机。有两个基本的 Mesh 网络节点类型，称为 Mesh 路由器和 Mesh 客户端。除了这些，其他节点的类型，例如个人计算机（Personal Computer，PC）、个人数字助理（PDA）、电视（TV）或音频设备和摄像机，也能凭借 Mesh 路由器连接到无线 Mesh 网络上。一个 Mesh 路由器通常有至少两个无线电装置和各种网络接口如 IEEE 802.3、IEEE 802.11、IEEE 802.15 和 IEEE 802.16，因此它可以接入其他类型网络，如因特网、蜂窝网络、局域网、无线局域网或者其他自组织网络等。Mesh 路由器通常用其中一个无线电和 Mesh 客户端通信，用另一个无线电发送数据包给其他 Mesh 路由器。

我们可以进一步将 Mesh 路由器分为接入路由器、骨干网路由器或网关 Mesh 路由器。Mesh 客户端通过一个接入 Mesh 路由器接入到一个 Mesh 网络，一个 Mesh 骨干网通过一个网关 Mesh 路由器连接到一个外部网络（如因特网）。一个单一的 Mesh 路由器也能执行所有这些功能。例如，在图 2-5 中，接入网络中的 Mesh 路由器就是一个接入路由器、骨干网路由器和网关 Mesh 路由器。

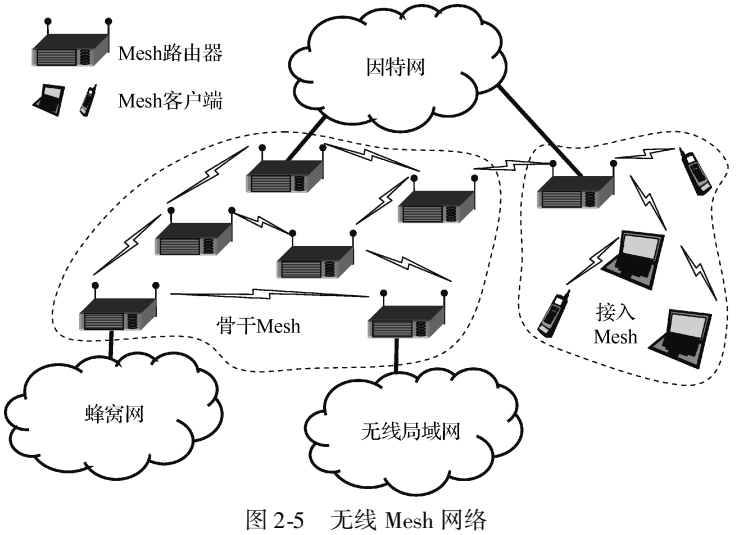


图 2-5 无线 Mesh 网络

有两种类型的 Mesh 网络：骨干 Mesh（Backbone Mesh，BM）网络和接入 Mesh（Access Mesh，AM）网络。一个骨干 Mesh 网络可以通过使用 Mesh 路由器形成，如图 2-5 所示。另外，一个接入 Mesh 网络可以通过 Mesh 路由器和 Mesh 客户端创建。此外，接入 Mesh 网络可以连接到骨干 Mesh 网络。把因特网或其他类型的陆地网络或卫星网络整合成一个无线 Mesh 网络是可行的。与传统的自组织网络、无线传感器网络和执行器网络相比，无线 Mesh 网络有以下四个特征：

1）Mesh 路由器比无线传感器网络和执行器网络、传统自组织网络中的节点更有能力，有更少的能量限制，并且能传送宽带流量。

2）尽管接入 Mesh 网络或者骨干 Mesh 网络可以在本地区域形成，骨干 Mesh 网络也可以在更广阔的区域提供连接。

3）骨干 Mesh 网络可以通过无线骨干网络把各种类型的网络（如因特网和广域网）互相整合。

4）在自组织网络、无线传感器网络和执行器网络中，把节点聚集起来并提供一个分层拓扑是可行的。在这种拓扑中，簇头用一个无线电和集群中的节点通信，用另一个无线电在簇头中提供连接。这是在 Mesh 网络中的主要设计方法，其中 Mesh 路由器至少有两个无线电，一个用于 Mesh 客户端，另一个用于和其他 Mesh 路由器组成骨干网络。

2.3.1　应用举例

几乎每个自组织网络应用情景也可以作为一个无线 Mesh 网络实现。但是，无线 Mesh 网络和其他自组织网络之间的主要区别是，基于通过自形成和自愈架构长距离传送宽带数据的能力。因此，Mesh 网络对于在城域网和广域网中的无线宽带骨干网络而言是一项杰出的技术。无线 Mesh 网络的典型特征使得如下应用成为现实（Akyildiz et al.，2005）：

1）宽带家庭网络；

2）社区和邻里网络；

3）企业网络；

4）运输系统；

5）楼宇自动化和控制网络。

2.3.2　挑战

自组织网络中的所有挑战同样适用于无线 Mesh 网络。此外，一个无线 Mesh 网络需要更多有能力的 Mesh 路由器，这些路由器能够长距离传输宽带流量。一个骨干 Mesh 网络集成了各种类型的无线和有线网络。这引入了一些新的挑战，尤其在传输层。在异质环境中，保证服务质量也是一个重要问题。最后，因为无线 Mesh

网络中的很多 Mesh 路由器是在个体监护之下的，所以无线 Mesh 网络也带来了新的可靠性和安全性挑战。

2.4 军事通信和网络

很多移动军事网络实际上是无线自组织网络。此外，大部分明显的无线传感器网络和执行器网络应用都在军事领域。因此，在本节中专门讲军事通信。但是请记住，我们的目标不是解释一个国家或组织所拥有的特定军事通信系统。相反，我们在本节中非常简洁地介绍军事通信的设计原则和挑战。

设计一个好的军事通信系统的本质是提高生存能力和快速部署能力。因为这个目标通常必须在非常苛刻和不利的环境下达到，军事通信系统是通信中最具有挑战性的应用领域之一。军事通信其他重要的特性如下（Cayirci and Ersoy，2002；Onel et al.，2004）：

1）各种移动模式：尽管一些用户以超音速移动，其他的可能是固定的。

2）广泛的终端类型：范围广泛的设备，如传感器（摄像机、雷达、热像仪等）、单声道收音机和计算机，可能是军事通信网络的终端。

3）可变的通信距离：通信距离从几米到几千千米。

4）可变的通信媒介特征：各种媒介类型（如有线、光纤、空气和海水）可能会被使用。

5）快速改变通信地点：被广泛的通信网络覆盖的区域可能需要清空，同时在一次军事行动中，同样的网络在不同的地区内几天之内能够安装好。

6）敌对和嘈杂的环境：在战场上，对方的通信设施是高优先级目标。此外，上千的炸弹爆炸、车辆和故意干扰会产生噪声。

7）突发流量：通信流量常常是与时间和空间相关的。长时间的无线电静默可能在特定的地区突然被极其密集的报告和通信需求打破，然而其他的地区保持静默。

8）各种类型的应用：军事通信网络拥有各种应用，这些应用需要满足不同的端到端服务质量需求。

9）各种安全限制：非涉密数据与绝密数据在同一个通信信道里传输。

为了满足这些需求，已经深入开展了一些研究项目，例如国防信息系统（Defense Information System，DISN），2000 年后军事通信（Post-2000 Tactical Communications，TACOMS）和全球移动通信。图 2-6 展示了来自 DISN 项目和 TACOMS 项目成果的代表当前水平的军事通信系统架构。这种架构有四个子系统：局域子系统（Local Area Subsystem，LAS）、广域子系统（Wide Area Subsystem，WAS）、移动子系统（Mobile Subsystem，MS）及系统管理和控制子系统（System Management and

Control Subsystem，SMCS）。一个安全系统也集成到架构之中。广域子系统作为一个广域骨干和其他子系统互连，一般是一个预部署的高容量网络，设计和管理得比其他子系统好。它也可能在和平时期被部署和使用。局域子系统可以被认为是一个游牧局域网，它可以接入到广域子系统或可用的商业网络。在受限区域的总部和类似组织通过局域子系统提供局域网支持。在战场上的移动用户通过移动子系统接入到军事通信系统。一个移动子系统通过接入广域子系统，可以作为一个独立的通信网络或整个军事通信系统的一部分而运转。系统管理和控制子系统是一个集成到架构之中的子系统，提供带有系统管理功能的网络管理员。

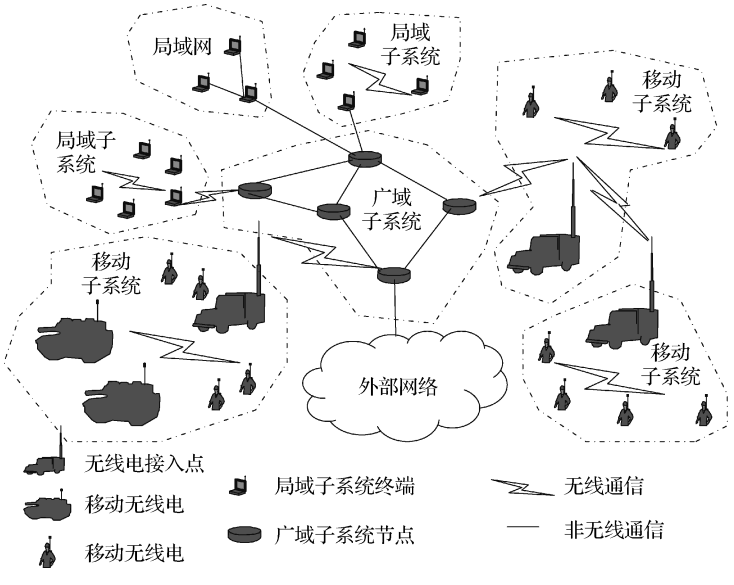


图 2-6　军事通信系统

在这些子系统中，移动子系统对于使用 WASM 技术来说是最重要的候选。移动子系统有两个重要的技术组成，即移动无线电（Mobile Radio，MR）和无线电接入点（Radio Access Point，RAP）。一个移动子系统的用户通过移动无线电接入到由军事通信系统提供的综合服务，这个移动无线电大部分时间是一个终端站（Terminal Station）。但是，在移动子系统中的移动无线电也可以中继其他流量，就像一个无线自组织网络节点。无线接入点可以在移动无线电之间、在一个广域子系统和一个移动子系统之间传输多媒体业务。在很多方面，它们执行类似 Mesh 路由器执行的功能。

移动子系统有一个快速可部署的移动基础设施，并且运用蜂窝网络和自组织技术。图 2-7 展示了军事通信系统的移动子系统架构。在这个移动子系统架构中有四层：

1）移动无线电层（Mobile Radio Tier，MRT）：移动无线电层单元是移动无线电的一个簇，它不能接入到任何无线电接入点。在各个移动无线电层单元（即一

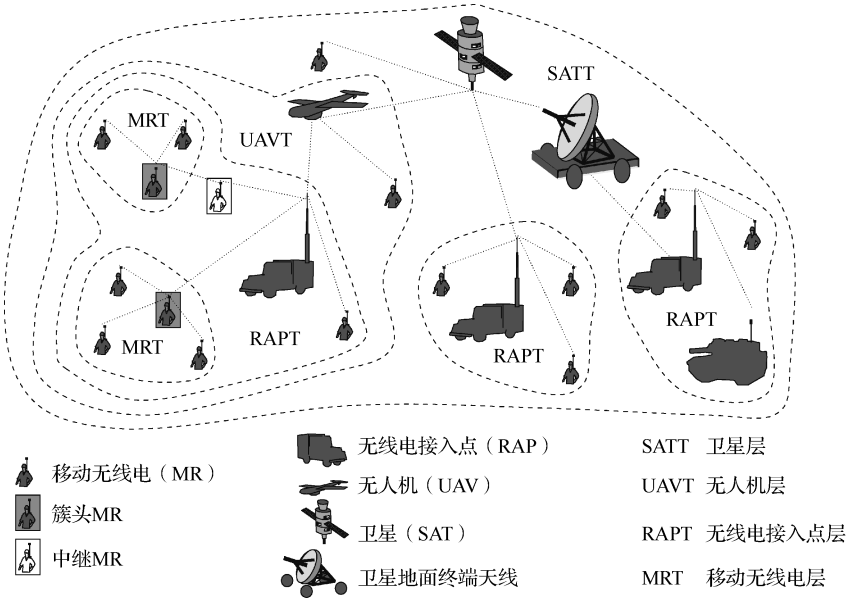


图 2-7 多层移动子系统

个移动无线电簇），其中一个移动无线电成为单元的首部（即簇）。如果有一个移动无线电可以接入到无线电接入点，且能通过移动无线电层单元首部接入，那么这个移动无线电层单元就是凭借移动无线电连接到无线接入点的，这个移动无线电在移动无线电层单元和无线电接入点之间中继信息。

2）无线电接入点层（Radio Access Point Tier，RAPT）：无线电接入点是移动子系统的移动基站。它们创造了无线电接入点层。当一些移动无线电层单元通过中继移动无线电和无线电接入点层连接时，无线电接入点层单元也可以为其他移动无线电层单元构造一个底层的簇。

3）无人机层（Unmanned Aerial Vehicle Tier，UAVT）：这是移动子系统的第一层覆盖层。无人机层单元覆盖那些没有被更低层覆盖的区域。更低层单元也可以通过无人机层接入到广域子系统中。

4）卫星层（Satellite Tier，SATT）：这是最上面的覆盖层。卫星层单元通过卫星生成，且包括许多低层单元。低层单元利用卫星接入到广域子系统中，并且和其他单元通信。

对于一个军事通信系统来说，关键系统需求包括以下几个方面：

1）多媒体通信；

2）多层网络；

3）移动网络；

4）移动和迅速可部署的基础设施；
5）可存活的基础设施；
6）可特制的（Tailorable）基础设施；
7）多功能基础设施；
8）模块化基础设施；
9）灵活的基础设施；
10）陆地和非陆地网络；
11）水平和垂直通信（Horizontal and Vertical Communications）能力；
12）高电路品质、高带宽；
13）安全的网络；
14）实时和批量联网（Batch Networking）；
15）在全天候和各种地形条件下的执行能力。

蓝队跟踪系统

蓝队跟踪系统（Blue Force Tracking，BFT）由三个主要组件组成：一个计算机、一个无线收发器（典型的是一个卫星收发器）和一个全球定位系统（Global Positioning System，GPS）接收器。这三个组件被集成，并放入一个装置中。全球定位系统定位装置，计算机在地理信息系统中显示装置和附近其他装置的位置。蓝队跟踪系统也给在计算机中的文本消息通知和信息报告提供接口。这种能力也被用来报告敌军位置和其他战场情况。

这种系统有很多用途，其中提供给各级决策者的状态感知（Situational Awareness）是最重要的。指挥官可以通过蓝队跟踪系统追寻部队的行踪。炮兵和飞机可以有更佳的盟军位置信息，且可以避免由于失误与盟军交战。智能的和更有效的后勤系统可以在蓝队跟踪系统基础上开发。我们可以希望蓝队跟踪系统节点被部署得更加广泛，部署到所有的部队、运载工具、关键设备、作战系统和军火，以跟踪它们的位置和状况。大概它们会成为一个陆地自组织网络的组合，通过能够接入卫星网络的大型网关节点相互连接起来。

几乎所有现代化部队都有将蓝队跟踪系统部署到所有部队的计划，安全是蓝队跟踪系统的最大问题。已经为自组织网络和传感器网络安全列出的每个挑战对于蓝队跟踪系统同样有效。对这样一个应用而言，几乎所有用于确保自组织网络和传感器网络安全的措施都是必需的。因此，这里强调了无线自组织网络和传感器网络安全对于蓝队跟踪系统的重要性。

2.5　影响无线自组织网络、传感器网络和 Mesh 网络设计的因素

在本章的每节中我们详细阐述相关的挑战，这些挑战实际上等同于影响 WASM

协议和算法设计的因素（见表 2-2）。在本节中，我们将更加全面地讨论这些因素。

表 2-2 影响无线自组织网络、传感器网络和 Mesh 网络设计的因素

因 素	自组织网络	Mesh 网络	传感器网络和执行器网络
无线媒介	工业、科学和医疗频段	工业、科学和医疗频段	工业、科学和医疗频段，声学的、低洼天线
网络体制	随机一对一	随机一对一，网关节点	一对多、多对一、多对多
流量	随机，多媒体	随机，多媒体	与时间和空间相关的数据
服务质量需求	带宽，延迟，抖动，可靠性	带宽，延迟，抖动，可靠性	功耗，延迟，可靠性
移动性	可移动	通常固定	通常固定，网络移动
容错性	通常没有故障关键点	故障关键点	故障关键点，高容错需求
操作环境	通常日常环境	通常日常环境	敌对和苛刻，通常无法到达
能效	不十分关键	不关键	关键
可扩展性	上百数量级	上十数量级	上千数量级
硬件限制	笔记本电脑、个人数字助理（PDA）	没有限制	微小的，低处理和存储能力
生产成本	没有硬性限制	没有硬性限制	必须有成本效益的

2.5.1 无线媒介

对于大部分自组织应用来说，无线是唯一可行的媒介，例如无线电、红外线或光。如前所述，这存在局限和挑战。为了满足自组织部署和全球运作等诸多需求，选择的传输媒介必须全球可用和免许可证。因此，无线电链路的一个选择是使用工业、科学和医疗（Industrial Scientific and Medical，ISM）频段，这在大部分国家里都可提供而无需许可证的通信。国际频率分配表（International Table of Frequency Allocations）规定了一些频段（见表 2-3），作为在工业、科学和医疗应用上可用的频段。其中的一些频段已经用在无绳电话系统和无线局域网中的通信。因此，这些频段被许多无线系统和应用的频段挤占。但是，它们还有很多优势，如在全球范围内提供免费和巨大的频谱分配。它们不是受缚于

表 2-3 工业、科学和医疗频段

6765 ~ 6795kHz
13553 ~ 13567kHz
26957 ~ 27283kHz
40.66 ~ 40.70MHz
433.05 ~ 434.79MHz
902 ~ 928MHz
2400 ~ 2500MHz
5725 ~ 5875MHz
24 ~ 24.25GHz
61 ~ 61.5GHz
122 ~ 123GHz
244 ~ 246GHz

一个特定的标准，从而在实现上更加自由。另一方面，有各种各样的规则和限制，如能量限制和来自于现有应用的有害干扰。

另一种在自组织网络节点间通信的可能模式是通过红外线。红外线通信是免许可证的，且对电子设备有很强的抗干扰能力。基于红外的收发器更便宜，更容易建立。现在很多的笔记本电脑、个人数字助理（PDA）和移动电话都提供红外数据协会（Infrared Data Association，IrDA）接口。红外线的主要缺陷是需要发送者和接收者之间的视距（Line of Sight）。这使得红外线在自组织网络传输媒介中成为一种比较勉强的选择。

一个有趣的发展是智能尘埃（Smart Dust）模式，它是利用光介质传输的自动感知、计算和通信系统。两种传输方案都为智能尘埃进行检查，其中被动传输采用一个三面直角棱镜反射器（Corner-Cube Retro-reflector，CCR）、主动通信使用激光二极管和可控镜子（Steerable Mirror）。前一种方案的模式不需要板载光源。三个镜子的配置是用来通信数字高电平或低电平。后一种方案采用板载激光二极管和主动操控激光通信系统来发送紧密校准光束给指定接收者。

自组织网络的特殊应用需求使传输介质的选择更具有挑战性。例如，海上应用也许需要利用水传输介质。海洋提供了一个非常不同的传播环境，不适于用射频通信。低于 100kHz 的声道代表目前唯一的载体选择。声信号传输速度为射频信号传输速度的 $1/10^5$，并且产生很高的传播延迟，即每 100m 延迟 67ms。极高的延迟影响了物理层、网络层和传输层协议的性能。

传感器网络和自组织网络、Mesh 网络不同的主要原因是严格的能量限制、低容量和微型传感器节点的小尺寸。在传感器网络中，能量最小化假设具有重大意义，超过衰变、散射、阴影（Shadowing）、反射、衍射、多径效应和衰落影响。总的来说，在距离 d 内传输信号需要的最小输出功率与 d^n 成比例，其中 $2 \leqslant n < 4$。指数 n 对于低洼天线和近地信道来说接近于 4，这在传感器网络通信中是有代表性的。因此，有着更多跳数和更短距离的路径比那些少跳数长距离的路径，能效更高。

因为无线媒介容易遭到窃听，使得自组织网络易受攻击。传输功率限制和较短的范围既有缺点，也有优点。低能量传输很容易受到干扰（Jamming）。另一方面，大多数系统对于干扰（Interference）更有弹性，一个节点需要足够接近才能窃听低功率传输系统。

2.5.2　网络体制

无线 Mesh 网络和传统自组织网络的一个主要区别是，无线 Mesh 网络中的流量通常是来自于与因特网相连接的网关节点，而传统自组织网络中的流量来自一对随机节点。这和无线传感器网络和执行器网络相似。在无线传感器网络和执行器网络

中流量通常来自于数据收集节点（cnode），即汇聚节点（Sink）。但是，无线传感器网络和执行器网络流量和无线 Mesh 网络不完全一样。尽管无线 Mesh 网络流量通常有点对点的属性，在传统传感器网络中流量或者是一对多或者是多对一，汇聚节点发送一个任务给传感器节点，或者传感器节点报告它们的结果给汇聚节点。在包括执行器的情况下，这种关系可以变成多对多，多个传感器节点报告它们的测量给多个执行器。同样，在军事通信中有一个等级性质，流量通常到或来自于更高的指挥梯队（Echelons）。注意并非总是如此，在无线传感器网络和执行器网络或无线 Mesh 网络应用中，源点和目的地可以都是网络中的随机节点。

在无线传感器网络和执行器网络或无线 Mesh 网络中，一个中心点（Point of Gravity）或一个关键节点的存在使得它们在敌对环境中更加脆弱。通过分析流量可能发现一个 Mesh 路由器或收集节点（cnode），并且在这些关键节点中监视或阻止所有数据流量。

在每种自组织网络中，即传统的 Mesh 网络或传感器网络中，节点间相互依靠来传送一个包。这种多跳自组织特性也带来了额外的弱点，使它们易受攻击。当一个恶意节点使其他节点相信它是一个中继节点时，它可以接收它们的包，且不转发它们。在下面的章节中，将详细讨论这些攻击和挑战。

2.5.3 流量特性

除了网络体制、自组织网络、传感器网络和 Mesh 网络也有其他与流量有关的特点。在自组织网络和 Mesh 网络中，数据生成率通常是随机的，而且取决于用户和应用的行为方式和细节。另一方面，在传感器网络和军事网络中，数据流量通常是与时间和空间相关的。传感器覆盖范围通常是重叠的，因此当一个事件发生时，它在同一个区域触发多个传感器。同样，节点通常是安静的，除非正在接触敌军，这时每个在接触区域中的节点开始报告。时间和空间的相关性表明，对于某些区域和时间段来说过度使用，对另一些区域和时间段来说未充分利用。这给通信协议和算法设计包括安全方案带来了额外的挑战。当数据流量是相关的，对付流量分析攻击变得更具有挑战性。

2.5.4 服务质量需求

对于数据流的服务质量（Quality of Service，QoS）一般由三个参数来表征：带宽、延时和可靠性。还有另一个参数，与延时中的变化有关，称为抖动（Jitter）。

首先，在传统自组织网络和 Mesh 网络中的应用特性和那些局域网或广域网中的并非完全不同。音频、视频和数据流量通过它们传输，对于这种流量的服务质量需求在无线环境中不会改变。然而，由于在无线媒介中有限的频谱、高误码率（BER）和时间上误码率的变化，加上自组织网络带来的移动性和自组织问题，保

证所需的服务质量水平更有挑战性。

在传感器网络中，由于严格的功率限制，问题更加严重。在许多传感器网络应用中，功率是首先要考虑的，当然这取决于应用。当传感器网络和执行器网络用于实时应用方面时，延时也是一个重要的限制，通常和功率限制相冲突。对于传感器网络，带宽需求可能会高些。例如，长时间声学测量需要高带宽才能无损耗送回。还有一些传感器网络应用中，延时和带宽问题是一个最重要的挑战。水下声纳网络就是这方面的一个例子。对于声纳水下介质，传播延迟很长时间（平均每 100m 为 67ms），容量十分有限（5 ~ 30kbit/s）。

2.5.5　移动性

移动性是许多自组织网络的主要特性。在许多 Mesh 网络和自组织网络应用中，节点可能随机地和独立地四处移动。这又与许多传感器网络不同，因为它们的节点通常一起移动。尽管在方向和速度上各个节点会有小的变化，因为节点移动归于共同的力量，它们趋于在网络中保持相对的位置。例如，如果没有抛锚固定，海上监视网络将随水流移动。

2.5.6　容错性

尽管自形成和自愈使得自组织网络比固定网络更具有容错性，在 Mesh 网络中的 Mesh 路由器和在传感器网络中的收集节点代表了故障的关键点。数据通过这些节点中继到外部系统，若它们不存在，网络将变得不相连。这在传感器网络中尤其重要，因为如果传感器收集的数据没有到达用户，它们不会有任何用处，而且传感器节点中的数据只能通过收集节点访问。因此，它们可能成为拒绝服务攻击的重要目标，容错性方案应该考虑到这一点。

2.5.7　操作环境

传统自组织网络和 Mesh 网络的操作环境与固定网络相比，通常不需要强加特殊的处理，除了它们可能部署在有较少基础设施的广阔的区域外。这只说明对于服务提供者来说有额外的管理问题。但是，传感器网络的设计是在恶劣和难以接近的地区无人值守运行的，这给容错方案带来了额外的挑战。此外，传感器网络可能在敌后的对抗性环境中。在这种情况下，它们易受物理攻击，且更容易篡改。

2.5.8　能效需求

传统自组织网络和 Mesh 网络没有十分严格的功率限制。但是，功耗是影响传感器网络协议设计的最重要因素之一，这也需要安全方面的特殊处理。传感器网络的安全方案必须在计算和网络需求方面都是低成本的。

2.5.9 可扩展性

在可扩展性方面，传感器网络与另外两种自组织网络又不相同。每个传感器网络方案需要高度可扩展，如2.2节中解释的那样。这也影响到了安全协议。例如，对于许多传感器网络应用来说，可扩展性需求和功率限制一起阻碍了后部署密钥分配（Post-deployment Key Distribution）方案的适用性。总的来说，在这种应用中，密钥在节点部署之前安装。

2.5.10 硬件需求和生产成本

与传感器网络相比，Mesh网络和自组织网络硬件更少受到限制，传感器网络中节点的存储和计算能力有限。因此，有着更少存储和计算需求的安全方案更适合于传感器网络和执行器网络。

2.6 复习题

2.1 如何区分自组织网络和蜂窝网络？

2.2 与光纤媒介相比，无线媒介有哪些缺点和优点？

2.3 隐藏和暴露终端的后果是什么？

2.4 什么是拓扑管理？怎样分类拓扑管理方案？

2.5 为什么TCP/IP簇中的TCP在自组织网络中表现得不如在固定网络中？在这方面比较中什么是性能的评判标准？哪些因素影响TCP的性能？

2.6 在无线传感器网络和执行器网络中，执行器对于网络体制的影响是什么？

2.7 接入和骨干Mesh网络的主要不同是什么？

2.8 在军事通信中，移动子系统和局域子系统的区别是什么？

2.9 怎样理解水平和垂直通信？

2.10 声频媒介和射频媒介的主要区别是什么？

第 3 章　无 线 媒 介

本章阐释无线通信相关的基本概念。本章提供的是与安全问题有关的介绍性材料。更多的关于物理层数据通信概念的细节，感兴趣的读者可以参考 Stallings 著作（2000）。

3.1　无线信道基础与安全

电磁信号可以是模拟的，也可以是数字的。模拟信号的强度是不同的，信号强度的变化经常是平稳持续的。另一方面，数字信号强度在某个时期是一个定值，过一段时期它会变换到另一个离散的水平（Discrete Level）。图 3-1 表示的是模拟信号和数字信号。

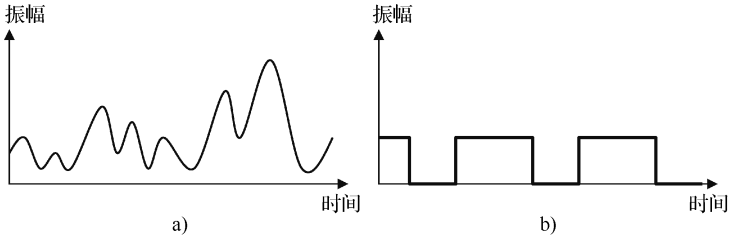


图 3-1　模拟信号和数字信号

a）模拟信号　b）数字信号

当在某个时间周期之前的信号强度和某个时期 T 的信号强度相同，并且每个 T 内都重复，这种信号叫周期（Periodic）信号。图 3-2 表示的是代表模拟周期信号的正弦波和代表数字周期信号的矩形波，这里

$$s(t) = s(t - T) \tag{3-1}$$

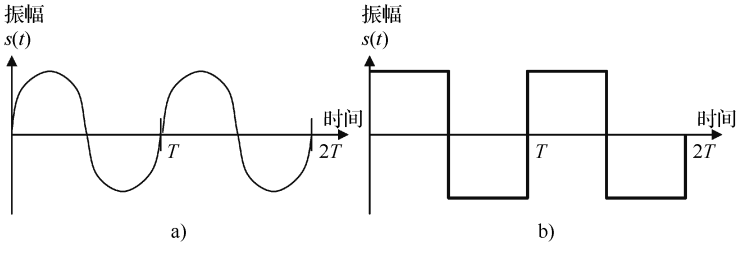


图 3-2　正弦波和矩形波

a）正弦波　b）矩形波

周期信号的频率（f）是指每秒信号重复一个完整周期的速度，即 $f=1/T$；这个速度是以赫兹为单位的（每秒的周期数）。例如，一个完整的正弦波是在每个 T 内完成 2π 循环，也就是 360°，再开始一个新的周期。如果给出一个正弦波的峰值振幅 A、频率 f 和初始相位 ϕ，则时间 t 的信号强度是

$$s(t)=A\sin(2\pi ft+\phi) \tag{3-2}$$

图 3-2a 的正弦波有一个单频率 f，式（3-2）足以能表示正弦波为时间函数。不过，一个典型的电磁信号有不止一个单频率分量，因此电磁信号强度也需要表示成频率函数。例如，图 3-3d 的信号有三个频率分量。对三个频率来说，初始相位 ϕ 是 0，表示起初正弦波的相位对所有的三个频率为 0。图 3-3a 中第一个频率 f 的

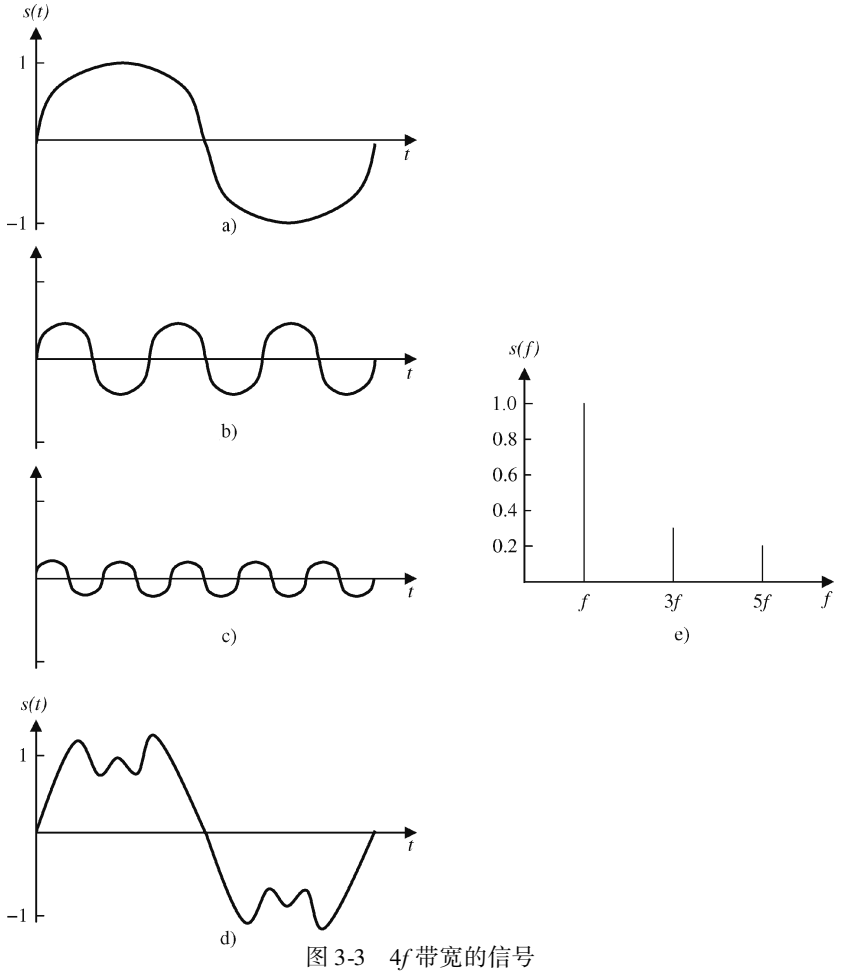


图 3-3　4f 带宽的信号

a）$\sin(2\pi ft)$　b）$\frac{1}{3}\sin(2\pi 3ft)$　c）$\frac{1}{5}\sin(2\pi 5ft)$

d）$\sin(2\pi ft)+\frac{1}{3}\sin(2\pi 3ft)+\frac{1}{5}\sin(2\pi 5ft)$　e）频率分量

峰值振幅 A 是 1。第二个频率是第一个的 3 倍，即 $3f$，峰值振幅是其 1/3，即 $A/3$。第三个频率是 $5f$，峰值振幅是 $A/5$。这个信号涵盖了 $f \sim 5f$ 之间的频率，带宽为 $4f$。例如，如果 f 是 2MHz，这个信号的带宽为 8MHz。

当把图 3-3 中频率为 f、$3f$ 和 $5f$ 的波形叠加在一起时，可以得到如图 3-3d 所示的波形。它看起来像数字矩形波。加在此信号的频率分量（Frequency Component）越多，它就越接近一个矩形波，失真也会越少。实际上，当有无数个频率分量时，它变成矩形波。换言之，矩形波有无穷个频率分量，可以把它表示成

$$s(t) = \frac{4A}{\pi} \sum_{kodd, k=1}^{\infty} \frac{1}{k} \sin(2\pi kft) \tag{3-3}$$

注意，随着每个额外频率分量的增加，它的峰值振幅会降低，比如 kf 的峰值振幅是 A/k。因此，大部分能量是在最初的一些频率分量里。另外，每一个频率分量的衰减也是不一样的。所以，一些频率分量在传输过程中是减少的，收到的信号会失真。到达接收端的频率范围定义了绝对带宽（Absolute Bandwidth）。有兴趣的读者可以在 Stallings（2000）文献中找到有关时间和频率领域概念的更多细节。

3.1.1　容量

我们可以得出结论，频率分量数越高，接收到的信号失真就越少，这使得能以高比特率发送和接收信号。有最高能量的频率分量也会对容量有影响。可以说一个零噪声信道的容量 C 是受到绝对带宽 B 限制的，可以表述如下：

$$C = 2B \tag{3-4}$$

式（3－4）给出了一个信号率，它表示在 1s 内能改变信号的次数。如果每个信号指示两个值或者更多值中的一个，可以增加容量。例如，当每个信号可能有四个不同电压值之一时，每次可以发送 2bit。在本章后面解释调制时，将讨论一个信号表示多个值的各种方法。当每个信号可以负载的值数量是 M，以比特每秒（bit/s）为单位的信道容量 C，以赫兹（Hz）为单位的绝对带宽 B，有

$$C = 2B \log_2 M \tag{3-5}$$

式（3-5）叫做奈奎斯特（Nyquist）公式，给出了可用带宽的容量上限。当信道不是零噪声时，噪声在接收信号里引入了额外失真，因此也减小了容量。香农（Shannon）用下式表述接收信号强度 S 和噪声 N 的信道容量：

$$C = B \log_2 (1 + S/N) \tag{3-6}$$

3.1.2　电磁波频谱

容量是可用带宽的函数，如图 3-4 所示电磁波频谱的一个范围。随着中间频率的增加，电势带宽（Potential Bandwidth）也会增加，这表示更高的电势容量（Potential Capacity）。

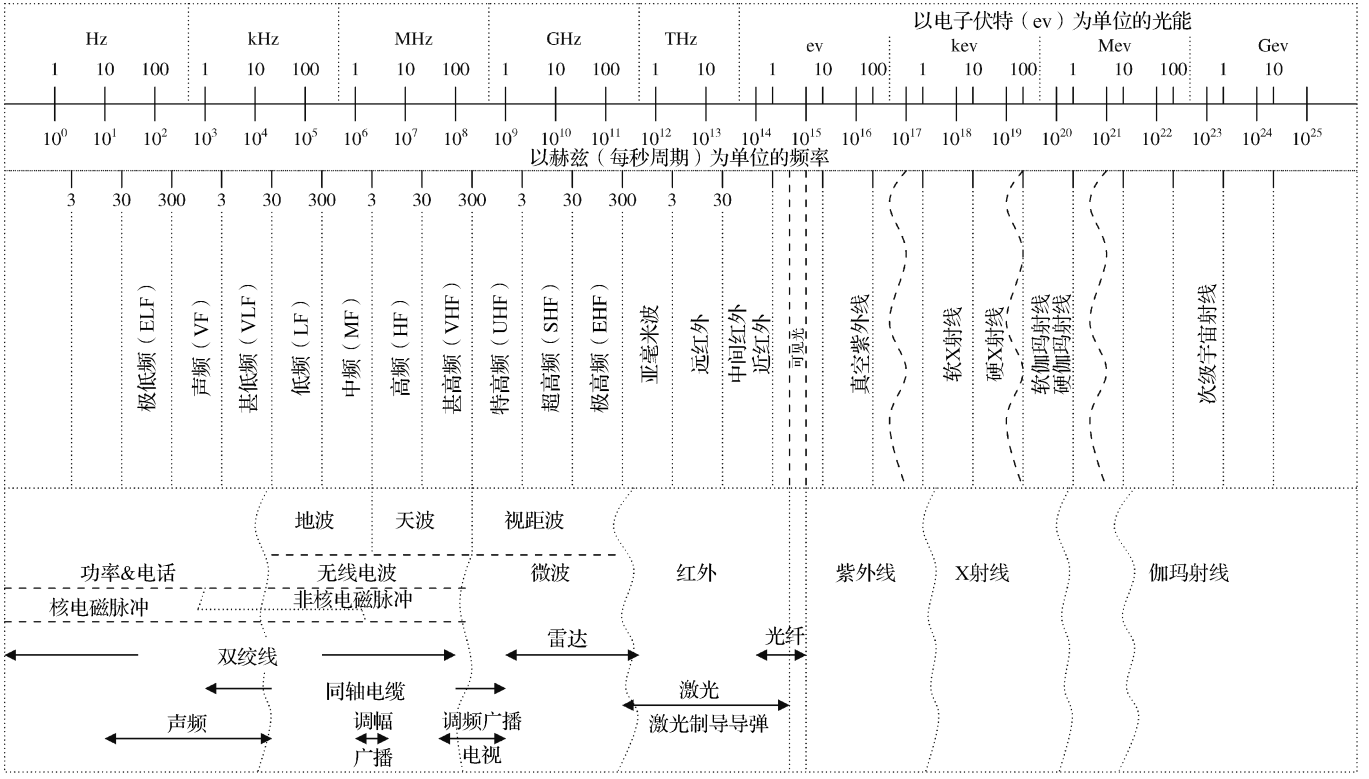

以电子伏特（ev）为单位的光能
Hz
kHz
MHz
GHz
THz
ev
kev
Mev
Gev
以赫兹（每秒周期）为单位的频率
极低频（ELF）
声频（VF）
甚低频（VLF）
低频（LF）
中频（MF）
高频（HF）
甚高频（VHF）
特高频（UHF）
超高频（SHF）
极高频（EHF）
亚毫米波
远红外
中间红外
近红外
可见光
真空紫外线
软X射线
硬X射线
软伽玛射线
硬伽玛射线
次级宇宙射线
地波
天波
视距波
功率&电话
无线电波
微波
红外
紫外线
X射线
伽玛射线
核电磁脉冲
非核电磁脉冲
雷达
光纤
双绞线
同轴电缆
激光
声频
调幅
广播
调频广播
电视
激光制导导弹

图 3-4　电磁波频谱

例如，光纤的可用频率范围是 10^{14} ~ 10^{15} Hz。该范围的电势带宽是 9×10^{14} Hz。这表示光纤有巨大的电势容量。不过，发射和中继信号的机电设备的可用性和性能是限制因素。因此，只能利用光纤的一小部分电势容量。

声频属于电磁波频谱的低端部分。初看这部分频谱可能对自组织网络不重要，可是，它提供了水下声纳网络最可行的介质。超过 50kHz 的无线电波不能提供水下通信必需的特性。介于 200Hz 和 50kHz 之间的声频带宽是水下通信最合适的频段，可是它也有一些缺点和限制。首先，当通信距离小于 1km 时，在这个范围内可用带宽提供的潜在容量局限为约 20kbit/s。此外，在水下声频信道的传播速度是 1500m/s，这为射频（Radio Frequency，RF）信号的 $1/10^5$。一个声频信号在 67ms 内可以传输 100m，这样的低速使得传输延迟成为任何协议或算法设计的一个重要问题，尤其是对声频多跳网络。声频信号的速度也是一个深度和温度的函数。海洋里有些层温度突然变化 1℃或 2℃，由于声频信号的速度是基于温度改变的，则声频信号在这些层里会被折射并丢失。

此外，水下的吸收损耗很高，这限制了 100kHz 以上的频率，声频信号会被外部自然和人造的噪声源干扰，比如风、潮汐、海洋动物和机械。

在声频之上的无线电波开始于 30kHz 附近。无线电波是全方向的（Omnidirectional），即它们可以在所有方向传播，并能穿过墙壁和门。因此，它们广泛使用在室内和室外应用中。在低频（LF）段和中频（MF）段，例如在 30kHz ~ 3MHz 之间，无线电波沿着地面传播，称之为地波（Ground Waves）（见图 3-5a）。在高频（HF）段，甚高频（VHF）段的低半部分，即在 3MHz ~ 100MHz 之间，接近地面的信号会被吸收。然而，它们也会被折射和散射回距离地球 100 ~ 500km 之间的电离层上去。因此这些无线电波可以在电离层的帮助下远距离传输，被称之为天波（Sky Waves）（见图 3-5b）。军用无线电波，称为甚高频波，是通过甚高频段的低半部分通信的。

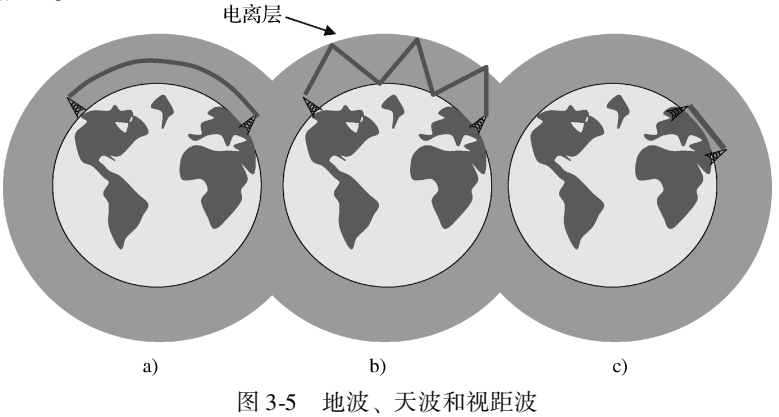


图 3-5　地波、天波和视距波

a）地波（$f < 2$MHz）　b）天波（2MHz $< f <$ 100MHz）　c）视距波（$f > 30$MHz）

在甚高频以上的频带，无线波几乎直线传播。这种情况下，优先选择定向天线，即传输一般不是全方向的。在这些频带里的信号不能像无线电波那样穿过墙壁。无线电波也会有其他损耗，这种损耗对微波的损耗影响更甚。我们在 3.1.4 节中讨论这些内容。

由于微波几乎是沿着直线传播的，地球表面的曲率就会对视距波的范围有物理限制（见图 3-6）。这个范围限制是天线高度的一个函数。如果忽略接收天线高度 h_2，微波的范围限制可以根据发射天线的高度 h_1 按下式计算出来：

$$d_1 = 3.57\sqrt{kh_1} \tag{3-7}$$

式中，$k = 4/3$。当接收天线也有一个高度时，微波传输的范围限制 r 将扩大。

$$r = 3.57(\sqrt{kh_1} + \sqrt{kh_2}) \tag{3-8}$$

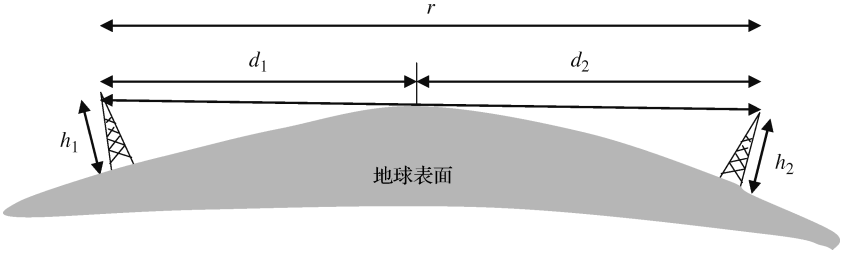


图 3-6　视距波范围限制

如我们在第 2 章中讨论那样，部分电磁波频谱用于无需许可的工业、科学和医疗（ISM）频段。WASM 应用一般使用 ISM 频段。433 ~ 464MHz、902 ~ 928MHz、2.4 ~ 2.5GHz 和 5.725 ~ 5.875GHz 间的 ISM 频段是传感器网络、Mesh 网络、无线局域网（Wireless Local Area Network，WLAN）和无线个域网（Wireless Personal Area Network，WPAN）的首选频段。注意，这些是微波的频段，它们落在特高频（UHF）和超高频（SHF）表示的低段部分。更高频率的微波经常用在卫星通信上。

3.1.3　路径损耗和衰减

电磁波的信号强度是受制于取决于距离的路径损耗（Path Loss）。因此，接收天线的信号功率 P_r 比发送天线的信号功率 P_t 要小。这个不同还与发送端和接收端天线增益、传输和接收电路损耗及其他随机因素有关，将 P_r 和 P_t 之差建模为

$$\frac{P_t}{P_r} = \left(\frac{4\pi d}{\lambda}\right)^{\gamma} = \left(\frac{4\pi f d}{c}\right)^{\gamma} \tag{3-9}$$

式中，λ 是载波波长，即光速 c（$3 \times 10^8 \mathrm{m/s}$）和频率 f 之间的比率，$\lambda = c/f$；d 是发送端和接收端之间的传输距离；γ 是路径损耗指数，在自由空间里通常为 2，在人口稠密的城市空间里，为 4。当应用专门接收技术时，路径损耗指数可降到 2 以下；在气候恶劣和人口稠密传播受阻（Densely Obstructed）的地区，该指数可上升

至 6。根据发送端和接收端信号功率级的比率，路径损耗可以用分贝表示为

$$L_{\mathrm{dB}} = 10\log\frac{P_{\mathrm{t}}}{P_{\mathrm{r}}} = \gamma 10\log\left(\frac{4\pi fd}{c}\right) \tag{3-10}$$

在自由空间里，路径损耗指数 γ 为 2，式（3-10）可进一步简化为

$$L_{\mathrm{dB}} = 20\log\left(\frac{4\pi fd}{c}\right) = 20\log(f) + 20\log(d) - 147.56\mathrm{dB} \tag{3-11}$$

如式（3-11）所示，信号强度的损耗不只与距离有关，还有与频率有关的衰减。频率越高，衰减越厉害。电磁信号更容易受到水和水蒸气吸收性损耗的影响。例如，中心频率超过 5GHz 的信号对雨、冰雹和雾的敏感程度要比中心频率大约是 1GHz 的信号高。这说明要达到同样的射程，频率高的信号要比频率低的信号需要更大的传输功率。这也说明它们会在到达预期的接收端之后，在更短距离内衰弱。

路径损耗的特点对安全方面的考虑有启示作用。频率越高，期望的通信范围之后所需控制空间也越小，因为更高频率的信号衰减得更快。这对安全是有利的。另一方面，更高的频率意味着更高的潜在带宽。因此，当一个更高频率的节点或载波受破坏时，更多的数据将会传送到敌手方。

3.1.4　其他传输衰减和干扰

除了衰减，还有其他原因降低接收端的信号质量。可以把这些障碍分成三大类：噪声、物理环境引起的失真和多普勒衰落。

3.1.4.1　噪声

噪声是由干扰信号干扰载波（Carrier）引起的。有各种形式的噪声：

1）白噪声：经常被称为热噪声，因为它是温度的函数，并且与电子的热运动有关。白噪声不能消除。此外，当我们也消除其他噪声时，根据式（3-6），载波的容量上限也不会有一个理论上的上限。热噪声与频率无关，因此被称为白噪声。对 1Hz 的带宽，热噪声是

$$N_0 = \mathrm{k}T \tag{3-12}$$

式中，N_0 表示每 1GHz 带宽的热噪声（W/Hz）；k 是玻耳兹曼常数，k = 1.3803 × 10^{-23}J/°K；T 是开尔文温度。对一个 WHz 的带宽，热噪声变为

$$N = \mathrm{k}TW \tag{3-13}$$

2）互调噪声：在不同频率 f_1 和 f_2 的信号中，可能会产生一个频率为 $f_1 + f_2$ 的信号和一个频率为 $f_1 - f_2$ 的信号，或是原频率乘积，比如频率为 nf_k 的信号。

3）串扰：当在多于两个无线传输中有重叠时间，并且它们由相同的天线接收时，它们会互相干扰。这和电话中的串话现象一样，两根电话线无意连在一起，一方可以听到另一方的通话。

4）脉冲噪声：无线信道中观测到的不规律的、出乎意料的非常短的噪声尖峰

信号。它们的形成有各种原因，尤其对数字通信有影响。

3.1.4.2 物理环境

树木、建筑等也能引起信号质量的失真，这是因为有波传播现象（见图 3-7）：

1）反射：当电磁波到达一个光滑平面时，它部分会被吸收，部分会被反射。

2）衍射：如果一个电磁波到达一个锐边时，它的方向会沿着边缘改变。

3）散射：在电磁波传播路径上的物体如柱子和树，会使得电磁波分散许多份。

这些现象也是另一重要传输障碍——多径衰落（Multipath Fading）的形成原因。除了信号源和目的端的直接信号以外，反射信号和散射信号也会到达目的端。因为这些信号比直接信号传播得更远，所以它们到达目的端时会有一个延迟，这对直接信号是一个干扰，会降低接收信号的质量。

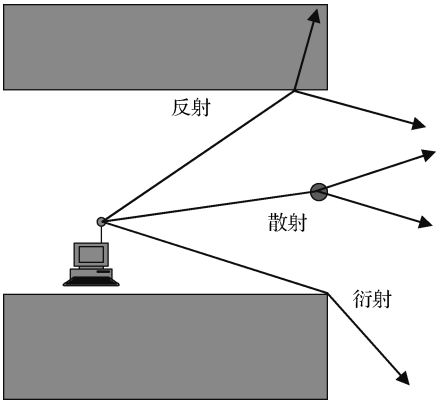


图 3-7 反射、散射和衍射

3.1.4.3 多普勒衰落

通信过程中，当信号源、目的端或链路的两端移动，它们的相对位置发生变化时，会产生多普勒衰落（Doppler Fading）。随着两端越来越接近，信号传输距离会越来越短，距离变短会使信号频率变得更高。当两端越来越远时，信号频率会降低。这会使接收端以错误的频率对信号采样。

当这些传播障碍导致目的端的信噪比（Signal-to-Noise Ratio，SNR）太低时，接收端就不能恢复信号。知名的拒绝服务攻击称为干扰或阻塞（Jamming），是由这种现象引起的。为了阻塞载波，会产生一个在那个频率有效的有意噪声，这会使在相关频率中链路的信噪比变得比所需水平低。

3.1.5 调制和解调

信号通过无线信道传输时，数字信号需要转化成波形信号。接收端再把波形信号转化为数字信号。这些过程分别称为调制（Modulation）和解调（Demodulation）。实际上，数字通信中数字信号和模拟波形信号之间的转化不局限于“数字-模拟-数字”的顺序。模拟信号可能需要转化为另一个模拟信号，以便于它在原频率以外的信道中传输。另外，为了更有效地存储和传输，模拟信号（如声音）可以数字化。因此，模拟-模拟-模拟和模拟-数字-模拟转化在无线传输中也是常见的。当然，模拟与数字的各种组合，像模拟-数字-模拟-数字-模拟，也是可能的。例如，语音首先会被数字化，调制之后接着传输。接收端首先解调输入的波形信号，然后

把恢复出的数字信号转化为原始的语音信号。

对于数字-模拟转化，正弦波的振幅、频率或相位为了表示数字信号，都可以进行调制（见图 3-8）。注意，正弦波是一个模拟周期信号。在振幅调制中，振幅的一个离散等级代表 1，另一个离散等级代表 0。相似地，一个频率可以指示 1，另一个频率可以指示 0。最后，当输入比特流的下一比特和前一比特不同时，正弦波的相位会在符号持续期（Symbol Duration）之初转变。或者离散相位比如 π，在符号持续期之初会等于 1，另一个相位比如 2π，可能等于 0。

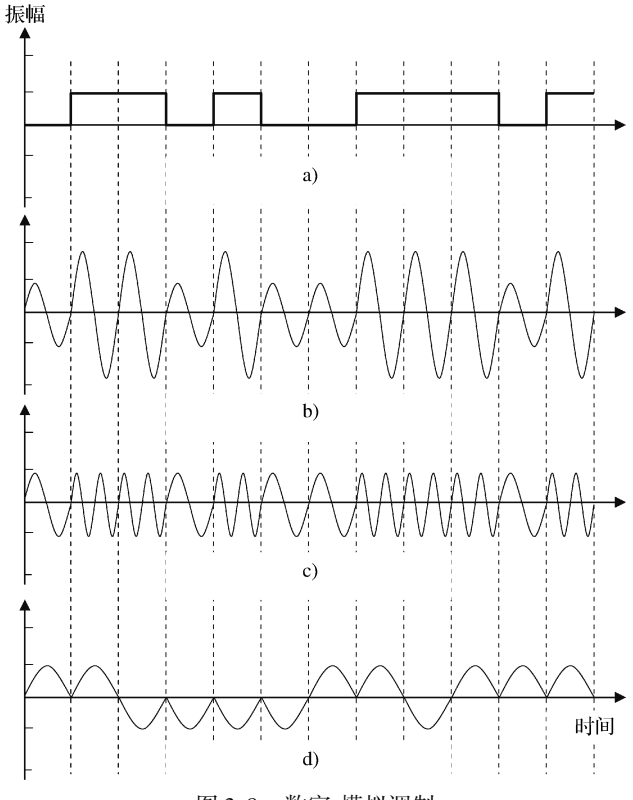


图 3-8　数字-模拟调制

a）数字信号　b）振幅调制　c）频率调制　d）相位调制

图 3-8 所示的例子表示双调制（Binary Modulation），其中波形的振幅、频率或相位通过符号持续期的两个可用的离散值之一进行调制。符号持续期是对波形一次取样的时间周期。符号持续期的倒数叫做符号率（Symbol Rate）或波特率（Baud Rate）。在双调制中，数据率或比特率，即在 1s 内传输的比特数等于波特率。

当在持续期内，选择多于两个振幅等级或相位之一时，数据率会比符号率高。例如，如果有四个振幅等级可用，则在每个符号间隔调制 2bit（见图 3-9b）。相似地，正弦波能转化为四个相位之一，2bit 可以在每个符号中再次转化。后一种技术

叫做正交相移键控（Quadrature Phase Shift Keying，QPSK）。另外，多相位和多振幅等级可以一起应用。例如，四个振幅等级和四个相位等级组成 16 个组合的正交调幅（Quadrature Amplitude Modulation，QAM-16），每个符号有 4bit 可以转化，可以达到比符号率高 4 倍的数据率。振幅等级的数量会进一步增加，直到每比特的能量变得太低，使接收端不能恢复比特为止。设计无线电的环境时，也应考虑数据率与符号率的比率。有拥塞和强干扰的对抗环境会强迫降低这个比率。

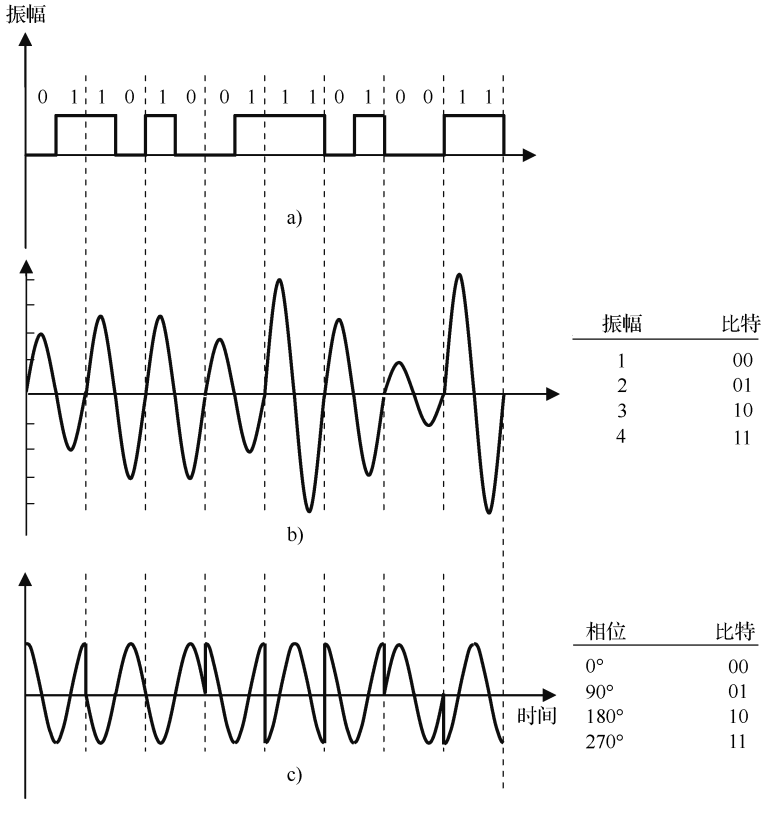


图 3-9 多级振幅和相位调制

a）数字信号 b）多级振幅调制 c）多级相位调制

振幅和频率调制也经常用在模拟-模拟调制中（见图 3-10）。在振幅调制中，波的振幅根据原始信号的频率进行调制，也可能把一个信号频率转化成更高频率或更低频率。

脉冲编码调制（Pulse Code Modulation，PCM）、差分 PCM 和增量调制是模拟-数字调制，例如数字化技术。在 PCM 中，在每个抽样间隔 S 抽取模拟信号，抽样间隔信号的振幅也会被记录下来。调制的保真度取决于抽样间隔的长度和用来表示抽样间隔信号振幅的比特数。抽样率越高，数字化失真就越低。根据抽样定理，当

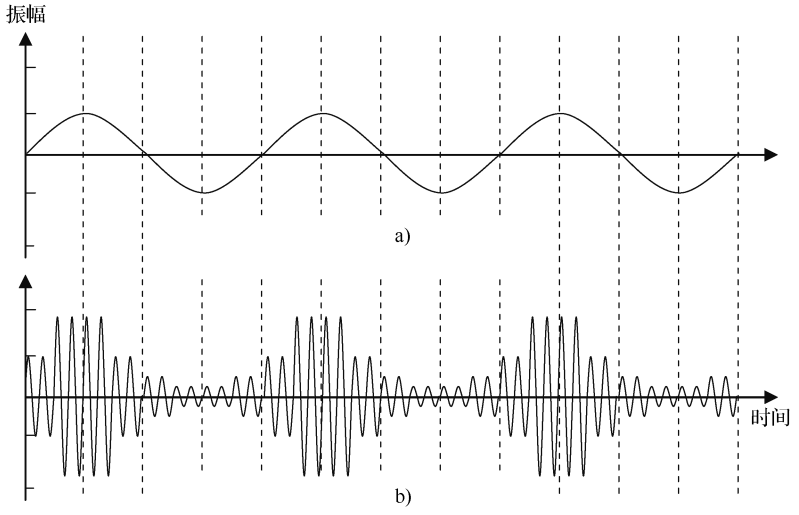


图 3-10　模拟-模拟调制技术

a）原始信号　b）振幅调制

抽样率 $1/S$ 至少是最高信号分量频率的 2 倍，即 $2f \leqslant 1/S$ 时，数字化过程的结果包括原始模拟信号的所有信息。

在差分 PCM 中，不是记录每个周期的振幅，而是用小比特数记录相比之前时间间隔振幅的变化。当只用 1bit 来表示振幅比之前抽样间隔高还是低时，这种技术称为增量调制（Delta Modulation）（见图 3-11）。由于模拟信号有时比表示它的增量调制信号变化得快，数字化的数据并不总是和原始信号一样。原始信号和数字化信号的差别称为数字化噪声（Digitization Noise）或数字化损耗（Digitization Loss）。

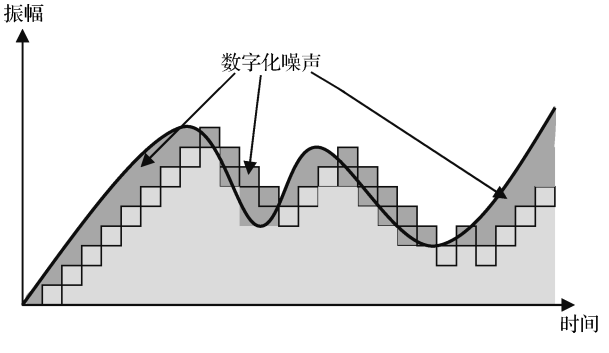


图 3-11　增量调制

3.1.6　曼彻斯特编码

当链路两端的时钟不能完美地同步时，发送端和接收端的每个抽样间隔在一长串 1 或 0 后，会变得不相同。接收端可能不能区分什么时间 1bit 开始或结束。因此，需要一个能明确确定每 1bit 开始时刻和结束时刻的方法。曼彻斯特编码提供了这种机制。

在曼彻斯特编码中，每个比特周期划分为两个相等的时间间隔，每个比特都发送 1 和 0。这是为了确保在比特周期中间，有一个从 1 到 0 或从 0 到 1 的跳变。这项技术有两个版本，称为曼彻斯特编码和差分曼彻斯特编码（见图 3-12）。在曼彻斯特编码中，先 0 后 1，发送一个 0bit；先 1 后 0，发送一个 1bit。在差分曼彻斯特编码中，当数据流的一个新比特与之前比特不一样时，在传输的数据流中也会有一个跳变。否则，在比特间隔结束时就不会有跳变发生。注意，在每个比特间隔中间，总会有一个从 1 到 0 或从 0 到 1 跳变，因此确保每个比特间隔有一个波形模式变化，这有助于两端（比如发送端和接收端）同步。然而，为此需要付出 100% 的开销，因为每比特都需要发送 1 和 0。

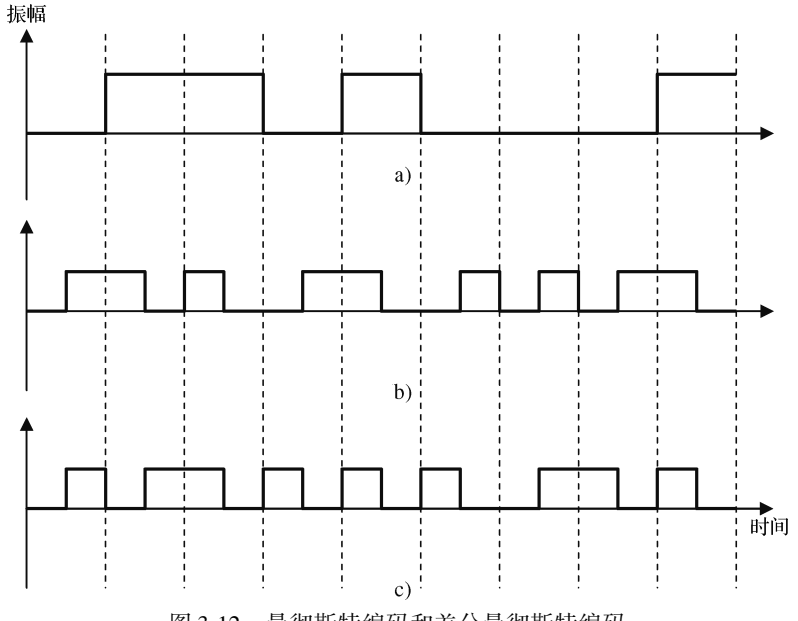


图 3-12　曼彻斯特编码和差分曼彻斯特编码

a）原始信号　b）曼彻斯特编码　c）差分曼彻斯特编码

3.1.7　复用和双工

在物理层的另一个挑战就是多个信道共享同一个链路。这可以通过复用（Multiplexing）来完成。它是把多个信道合成为一个单一链路的处理过程。在另一端，多路信号分解成多个信道，这个过程叫去复用（Demultiplexing）。注意，这和下一章要讲的多路接入是不一样的，因为多路接入是一个信道被多个终端共享。可以通过多路复用和去复用技术把给定容量分为多个信道，然后使用多路接入方案来让多个用户共享这些信道。

两个著名的多路复用技术是频分复用（Frequency Division Multiplexing，FDM）

和时分复用（Time Division Multiplexing，TDM）。在频分复用中，可用频谱分成更小份的频率，每份变成了一个频率信道。为了避免频率信道之间的干扰，它们也会用防护频带（Guard Band）隔开。在时分复用中，更大带宽的信道分成了时间段，每一段分配了一个信道。

同样的方法可以用于把容量分成两个通信节点之间的两个方向。一些频率信道分配到一个方向，而其余一些信道通过使用频分双工（Frequency Division Duplexing，FDD）被分配到了相反方向。类似地，用基于时间段的时分双工（Time Division Duplexing，TDD）也可以完成。

3.2　高级无线电技术

高级无线电技术能增加同一带宽的容量和降低相同传输范围和传输容量下的传输功率。这些技术大部分是基于更好的噪声和干扰处理技术。它们通过选择更合适的频率、规划更有效的传输调度、尽可能地限定传输在预期通信区域，减少了干扰。它们也用频分、时分和空分技术使得对噪声更有适应性。以上所有方案都对安全方面有一定的启示，也为开发更新、更有效的安全方案提供了机会。新的无线电技术也提供更灵活且可重配置的无线电，这种无线电更易受到节点篡改、病毒、蠕虫和特洛伊木马攻击的影响。

3.2.1　定向天线和智能天线

定向天线在空间上限制并指引传输朝向期望的通信区域，减少其他方向的干扰。这会使容量更高。因为它们更大、更贵，对移动性反应更灵敏，所以定向天线不适合用在移动自组织网络节点上，它们大多用在接入点、基站和主干 Mesh 路由器上。可以区分两种类型的定向天线方案，即切换波束（Switched Beam）天线和适应性（Adaptive）天线，如图 3-13 所示。

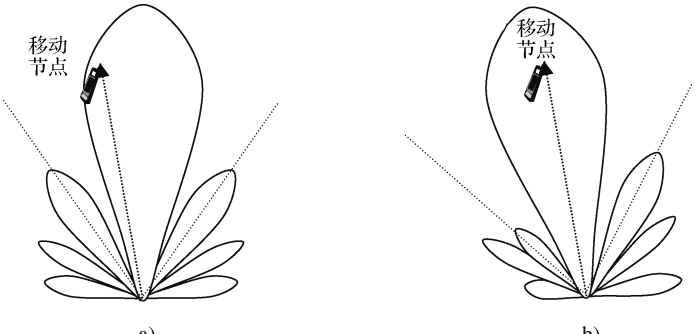


图 3-13　定向天线

a）切换波束天线　b）适应性天线

在切换波束方法中，有固定波束模式。使用为移动节点提供最强信号的模式。然而，因为波束模式是固定的，所以移动节点可能不在主波瓣的中轴线上。另一方面，在适应性天线方案中，没有固定波束模式，信号模式能动态地朝向移动节点而改变。因此，适应性天线的范围比切换波束天线的范围大，干扰抑制比后者高。当优先考虑安全时，智能天线是有优势的，因为朝向计划外方向的发射是受限的，因此在这些地区的敌手不能收到传输信号。

3.2.2 软件无线电

传统无线电对特定的频率和协议最优，并在硬件上实现。软件无线电用以下几种方式改变传统的方法：

1）尽可能靠近天线的模-数转换（Analog-to-Digital Conversion，ADC）：在传统的无线电中，接收信号首先转化成一个更低的频率，叫做中频（Intermediate Frequency，IF）。接着中频信号被过滤噪声，然后放大、解调。模-数转换完成后，输入信号的数字处理过程开始。模-数转换离天线越近，数字化处理应用得越快，这意味着更多的无线电元件能在软件上实现。实现这些本身有大量挑战。首先，需要高速的信号处理器对高频模拟信号进行精确采样。其次，这也需要线性放大器能放大宽频带信号。

2）通用硬件：为了进行数字化处理，需要通用硬件，而不是只对特定频率和协议集优化的特定硬件。这种通用硬件，一般是有成本效益的、灵活的、时间高效的，但功率不大。

3）数字化处理的软件实现：通过通用硬件，之前章节提到的无线电功能在软件上都能实现，例如，生成信号、调制、解调、曼彻斯特编码、跳频，以及其他协议如媒介访问控制、编码、加密等。因此，无线电波变得可以重配置，同一无线电波可以应用在多个协议集和频率中。不过，它们也会变得易受病毒、蠕虫、特洛伊木马攻击。

3.2.3 认知无线电

软件无线电为实现认知无线电提供了基础，认知无线电可以检测可用频谱，动态选择工作的频率和其他参数。传统的无线电通过使用固定的协议集（至少在物理层上的），在预置的频率信道上运行。认知无线电能根据参数，比如可利用性、容量、拥塞状况，选择频率信道和协议集。即使某些信道已经严重拥塞，大部分可用频率通常不使用。认知无线电会在未占用的频率上选择一个信道，而不是与已经拥塞的信道竞争。因此，它不用分配新的频谱，就可以有非常大的容量。

认知无线电也提供了一些与安全相关的因素和应用的新特性。它们能找到安全信道，避免拥塞信道。它们也可以监控使用各种通信技术的大范围的信道，侦测、

监听其中正在进行的通信。因此，认知无线电也可以用于安全攻击。

3.2.4 多无线电/多信道系统

用在无线 Mesh 网络的 Mesh 路由器经常使用多信道和多无线电。它们一般至少有一个主干信道和接入信道。此外，为了接入各种网络，它们通常支持多无线电技术，如 IEEE 802.11、蓝牙、ZigBee 技术。多无线电和多信道技术的可利用性引入了其他安全挑战，特别是在网络层和传输层。另外，在这些系统上有更多的攻击点，因此为抵御安全攻击需要更多努力。另一方面，它们对拒绝服务攻击更有弹性，因为这些系统有可替换的路由能继续转发。除了这一点，数据还能通过多信道分割（Partitioned）和传输，这让窃听变得更困难。多路由有助于研发更有效的错误检测和恢复方案，我们将在后面章节中阐释。

3.2.5 MIMO 系统

多输入多输出（Multiple Input，Multiple Output ，MIMO）是针对多天线通信系统的一个模型。MIMO 概念是基于多天线和利用多路径现象。MIMO 算法组合接收信号的直接副本和多路径副本，使用信号的多路径副本是为了装载更多信息。因此，MIMO 通过使用多路径传播而提高了无线通信系统的频谱效率。

MIMO 系统在至少两条天线上发射。在一个 MIMO 系统中，当天线数量增多时，数据吞吐量和范围会增加，误码率会降低。IEEE 802.11n 任务组将 MIMO 作为无线局域网规范基础，其至少有 100Mbit/s 的容量。IEEE 802.11n 可用于无线 Mesh 网络中。

3.3 复习题

3.1 有一个基于甚高频（VHF）的通信系统，它能提供比最大范围噪声级高 25 个数量级的信号强度。

（a）系统总的容量是多少？假设所有的 VHF 都分配在此系统上。

（b）为达到此容量，每个符号需要表示的最小值是多少？

3.2 计算五跳水下声纳网的传播延迟，每跳平均 100m。假设每跳没有处理延迟。

3.3 假设没有传输功率限制，天线高度为 30m，接收端是某人持有的手机，在最坏的情况下，运行在 1.8GHz 信道的基站的最大传播范围是多少？

3.4 一个波长为 3m 的波在 100m 的路径损耗是多少 dB？

3.5 在 900MHz 运行的一个传感器网络。一个节点有两个发送数据包给收集节点的路由。一个路由 100m 有 10 跳，另一个路由 200m 有 5 跳。由于天线处于低

洼地带，路径损耗指数是4。假设节点在处理转发数据包时，不消耗能量。哪条路由在功率上更高效？

3.6 讨论系统运行的频率是否越高越安全。

3.7 当温度是20℃时，30kHz信道的热噪声是多少？

3.8 什么是多普勒衰落？

3.9 什么是多径衰落？

3.10 解释符号率和数据率的不同。

3.11 画出以下十六进制数据流表示的QAM-16波形图：

A01E983D

3.12 比较PCM和增量调制。

3.13 写出以下数据流的曼彻斯特编码和差分曼彻斯特编码产生的比特流：

0100110001110010 11

3.14 讨论与智能天线有关的安全考虑。

3.15 讨论与软件无线电有关的安全考虑。

3.16 讨论与认知无线电有关的安全考虑。

3.17 讨论与多信道/多无线电系统有关的安全考虑。

第 4 章　媒介访问和差错控制

为了满足移动和易错无线环境中的宽带需求，需要一种有效的媒介访问控制（Medium Access Control，MAC）方案。MAC 方案对于系统的性能、系统的容量以及硬件复杂性有重要的影响。一个成功的 MAC 方案需要充分利用数据流和网络特性来满足 WASM 的强制性需求。

MAC 在开放系统互连（Open Systems Interconnection，OSI）参考模型（Tannenbaum，2003）中被认为是数据链路层（Data Link Layer，DLL）的一部分。数据链路层也包括在链路基础上的差错控制和流控制。无线网络为流控制和差错控制带来了更多挑战。虽然自组织网络的移动性和自配置需求加剧了这些挑战，以及 WASM 严格的资源和能量限制，但是特别为无线网络开发的错误控制方案也能够适用于很多 WASM 应用。

4.1　媒介访问控制

无线网络中的 MAC 方案已经得到了广泛的研究，文献中也提出了大量的 MAC 协议。本章首先通过整体的方法对 MAC 方案进行分类，然后讨论那些在无线和受限网络中普遍使用到的方案。之后阐释专门为 WASM 设计的 MAC 协议。

4.1.1　一般的 MAC 协议

MAC 协议在广义上可以分为三种类型：基于竞争的（Contention-Based）、无冲突的以及混合式方案（见表 4-1）。在基于竞争的方案中，帧的传输，例如数据链路层中要传输的一块数据，不能保证成功完成。传输可能会和其他节点传输发生冲突。基于竞争的 MAC 协议会在冲突发生时解决它。无冲突协议确保帧所传输的数据不会和其他帧传输时发生重叠，例如与另一个传输发生干扰。在无冲突技术中，在所有资源被分配到一个节点之后，它们会为节点所拥有，直到节点不再需要它们，并将它们退回。

表 4-1　一般 MAC 方案

基于竞争的	无冲突的	混合式
ALOHA：当准备好时进行传输	FDMA：分配频带	PRMA，D-TDMA：基于竞争来维持信道，当信道被使用时，通过无冲突方法使用它们

（续）

基于竞争的	无冲突的	混合式
时隙 ALOHA：在一个时隙的开始进行传输 CSMA：在传输前感应信道 CSMA/CD：当探测到冲突时停止传输并重试 CSMA/CA：通过通告隐藏终端避免冲突	TDMA：组合分配频带和时隙 FH-CDMA：频率在多个频道跳变 DS-CDMA：将数据扩展到更大的频谱	PRMA，D-TDMA：基于竞争来维持信道，当信道被使用时，通过无冲突方法使用它们

在这期间，所有的资源可能不会100%被节点利用。混合式方法使用了一个基于竞争的时段来为传输获得资源，之后跟随着一个无冲突时段可用于动态分配资源。因此，它们提供了对稀缺资源的动态分配和更好地利用。将无冲突技术划分为固定分配或者动态分配无冲突技术，同时将混合式方法看成一种动态分配无冲突技术都是可行的。

基于竞争的技术也经常被称为基于载波侦听多址访问（Carrier Sense Multiple Access，CSMA）的技术。然而，这一技术范畴的本质不是CSMA，而是另外一种叫做Aloha的协议。因此，这一类范畴的技术也被称为Aloha家族。Aloha是一个非常简单的协议，这种协议中节点会在其拥有一个帧时就进行传输。如果传输帧没有到达目的地，就会进行重传。这种操作会持续到成功传送帧完成为止。Aloha拥有很低的开销，同时在均匀分布的低流量负载中可以减少延迟。然而，当数据流量大并且突发时，Aloha中的冲突率就会变得很高。

Aloha可以通过引入时间段的方式得到加强。节点都是时间同步的，同时它们只会在某个时间段的开始时刻传输某个帧。这确保了一次传输可以在无冲突的情况下开始时，就会成功地完成。这一方法以损害邻居节点间的同步为代价而降低冲突发生率，被称为时隙Aloha（Slotted Aloha）。

CSMA是Aloha家族演化的下一个阶段产物。在CSMA中，首先要感应载波（Carrier）来确保没有正在进行中的传输，而在载波空闲时就会开始传输。虽然CSMA相比于Aloha极大地减少了冲突发生率，但是正在传输的帧和其他帧发生碰撞的可能性仍然存在，这是因为多个节点可能会在同一时刻感应载波，并错误地认为载波空闲而进行传输。另外，由于存在时延（Latency），某个节点可能在检测到载波空闲时，而另外一个节点已经开始了传输。因此，CSMA中的冲突发生概率 P_c 是一个关于共享同一信道的节点数量 n、平均时延 d 和平均帧长度 l 的函数，如式（4-1）所示。节点的数量和平均时延越高，发生冲突的概率就越大。另一方面，随着平均帧长度的增加，发生冲突的概率就会降低。

$$P_c \approx dn/l \tag{4-1}$$

CSMA 可以分为三个版本：持续 CSMA（Persistent CSMA）、非持续 CSMA（Nonpersistent CSMA）和 P 持续 CSMA（P-persistent CSMA）。这三个版本之间的差别表现在它们检测到载波忙碌时的反应上。在持续 CSMA 中，检测到载波忙碌的节点将会等待直到载波空闲，而且当载波空闲时，节点再开始传输它的帧。然而，在这种情况下，冲突发生概率可能会增加，这是因为存在其他的节点同样侦测到载波忙碌，并等待当前的传输结束。为了处理这种情况，非持续 CSMA 在检测到载波忙碌时，会等待一个随机的时间段，随后在传输之前再次感知载波。P 持续 CSMA 适用于时隙载波（Slotted Carriers）。在这一方案中，当某个节点检测到载波空闲时，它开始进行传输的概率是 p。节点将不会在概率为 $q = 1 - p$ 的情况下开始传输，即使它检测到载波此时是空闲的，同时会等待直到下一个时段，并重复相同的算法。

通过受限传输节点可以检测冲突。带碰撞检测的 CSMA（CDMA with Collision Detection，CSMA/CD）利用碰撞检测来进一步改进 CSMA 的性能。在 CSMA/CD 中，传输者一检测到冲突时就退出传输。在 MAC 层，以太网使用了 CSMA/CD 算法，这里检测到冲突的节点时，首先等待一个随机的时间，然后重复算法。如果发生了另一个冲突，节点会再一次停止传输，并再次等待一个随机时间段。然而，第二次随机时间段持续时间均值是先前的随机时间段均值的两倍。通过加倍以前的均值而增加随机时间段会一直持续，直到帧成功地进行了传输。因此，这种机制被称为指数撤回（Exponential Back-off）。它提供了一种隐式方式对数据流负载作用。

无线节点只使用一个天线，无法同时进行发送和接收。另外，隐藏终端问题阻止了无线节点对冲突的检测。而且，因为隐藏终端问题而引发的数据碰撞会引起重发（Retransmission），同时会因为暴露终端问题消耗能量而导致监听数据传输。很明显，隐藏终端问题和暴露终端问题都导致不必要的能量损耗。在带碰撞避免的（CSMA with Collision Avoidance，CSMA/CA）CSMA 中，需要传输消息的节点会给接收者发送一个小的请求发送（Request-To-Send，RTS）消息。接收者立刻以一个消除发送（Clear-To-Send，CTS）消息进行响应。在接收到 CTS 之后，发送者就会进行消息的传输。RTS 和 CTS 消息中都存在一个指示数据消息长度的字段。对于发送者或者接收者来说，隐藏的节点会接收到 RTS 或者 CTS 消息，同时在至少等于 RTS 和 CTS 信号中给出的消息长度的时间段内，避免接入媒介。因此，避免冲突是以额外的消息为代价的。4.1.2 节会更详细地介绍关于冲突避免问题。这里我们愿意强调无线网络和有线网络之间的冲突发生概率之间的不同。当无线网络中不提供冲突避免机制时，某个帧和其他帧发生碰撞的概率 P_c 和节点间的平均延迟 d、节点数量 n 以及平均帧长度 l 有关，如下式所示：

$$P_c \approx dnl \tag{4-2}$$

根据式（4-2），帧的长度越长，冲突发生概率就越高。这与式（4-1）中的关系相反。

无冲突传输可以通过为某个节点分配信道并确保其他节点无法接入这一信道来实现。为实现这一目标，可以从时间、频率、混合时间频率或者码元的角度来看待信道。因此，一个多接入信道可以通过使用频分多址（Frequency Division Multiple Access，FDMA）技术以基于频率的方式共享，可以通过使用时分多址（Time Division Multiple Access，TDMA）技术以基于时间的方式共享，或者使用码分多址（Code Division Multiple Access，CDMA）技术以基于编码的方式共享（见图 4-1）。

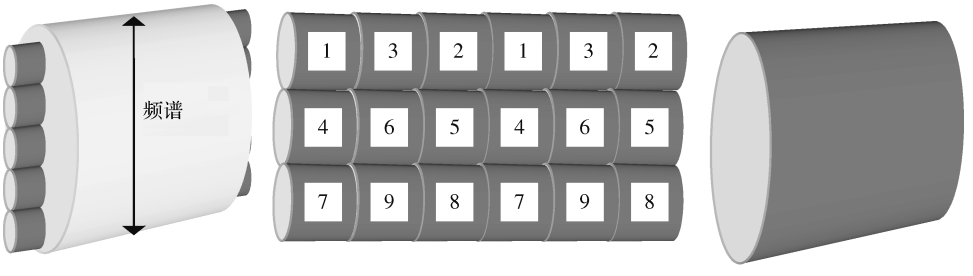


图 4-1 免冲突多路接入方案

a）FDMA b）TDMA c）CDMA

在 FDMA 中，频谱被分成了均等的频道，例如每 30kHz 为一个频道，同时频道之间存在适当的间隔。之后，每一个频道都会被分配给一个单一的节点。TDMA 使用了数字技术。在 TDMA 中，可用的频谱首先被分配比 FDMA 中的频道更宽的频道。例如，在 GSM 中，每个频道是 200kHz。这些频道进一步被分割为时间段，例如 0.5ms。在这之后，每个节点都会被分配给一个特殊的频率/时段的组合。CDMA 是一种扩频技术，这里更宽范围的频道被多个节点同时使用。

CDMA 技术有两种：跳频（Frequency Hopping，FH）以及直接序列（Direct Sequence，DS）。跳频接收端和传输端在每一次主动呼叫中被分配了 N 个频道，同时它们会通过双方都知道的跳频模式来在这 N 个频道中进行跳频。例如，一个节点可以在 100 个 10kHz 的信道中进行跳变。基本的跳频模式有两种；一种叫做快速跳变，这种模式在一次标记（Symbol）中完成两次或多次跳变；另一种叫做慢速跳变，这种模式在每跳中完成两次或者多次标记。

DS-CDMA 是一种多址接入技术，在这种技术中，多个独立用户通过调制签名波形同时接入一个信道，它被称为伪噪声（Pseudo Noise，PN）序列或者扩频码（Spreading Codes）。这一过程称为扩频（Spreading）。接收端的接收信号是这种信号的叠加。接收者通过使用和发送者相同的扩频码解调和解码接收到的信号。这一过程被称为解扩频（Dispreading）。

扩频过程如图 4-2 所示，这里数据传输率为 $1/T_d$，扩频序列传输速率为 $1/T_c$，

扩频序列传输速率被称为码元速率（Chip Rate）。由于 T_d 是 T_c 的 10 倍，例子中的码元速率是数据传输速率的 10 倍。当数据流和扩频序列相乘时，得到的信号的传输速率和扩频序列的相同。换句话说，源比特流被转换为拥有码元速率的另一比特流。因此我们将数据扩散到了一个更大的频谱。如果将得到的信号再一次和扩频序列相乘，则刚好能获得原始信号。这是最好的情况，因为没有其他传输的干扰。当存在干扰时，只要干扰不太强烈，仍然可以解扩频接收到的信号，并将其和原始数据进行关联。因此，CDMA 拥有干扰受限的软容量（Interference-limited Soft Capacity）。所有减少干扰的行为都能增加其容量。感兴趣的读者，可参阅 http://www. umtsworld. com/technology/cdmabasics. htm，以获得更详细的信息。

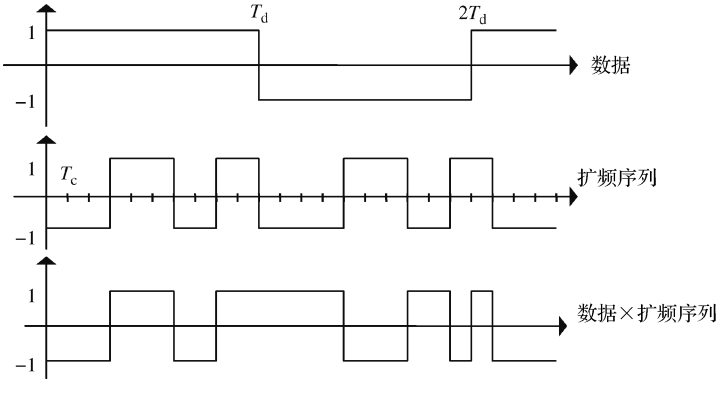


图 4-2　扩频过程

另一类无冲突 MAC 方案被称为令牌传输（Token-passing）技术。在这种技术中，一个单一（逻辑的或物理的）的令牌将在用户中间进行传递，只允许令牌的拥有者进行传输，从而确保了无干扰。令牌环和令牌总线就是这种类型的实例。由于基于令牌的 MAC 方案在当前的系统和协议栈中使用得越来越少，我们将不再对它们作详细介绍。

在混合 MAC 方案中，信道会被按需分配，因此恰巧空闲的节点将不会浪费信道资源。这些方案始于当节点宣布它的传输意图时的一个基于竞争的分配时段。在这些通知的基础上，资源被分配给节点，获得资源的节点就会在分配给它们的信道上传输信号。分组预约多址接入（Packet Reservation Multiple Access，PRMA）和动态 TDMA（D-TDMA）是基于预约的协议的例子。

4.1.2　无线自组织网络、传感器网络和 Mesh 网络 MAC 协议

WASM 应用程序引入了对 MAC 协议性能有影响的新因素。如第 2 章中所阐述的，大多数的传感器网络协议受限于严格的能量约束。水下声纳网络（Underwater Acoustic Networks）解决了过度时延（Latency）的问题。由于高延迟，它们无法支

持 RTS-CTS 信号发送。它们同时也需要在有限的带宽中提供服务。Mesh 网络需要在一个相对更宽的带宽下满足高吞吐量的需求。在这些约束中，能量效率吸引了大量的研究工作，节能的无线 MAC 协议在 20 世纪 90 年代末已经被深入地研究。

节能的无线 MAC 协议应该使四种能量浪费最小化：空闲侦听、冲突、协议开销和串音（Overhearing）。表 4-2 给出一个按年代顺序的节能 MAC 协议表。它被分为两类：基于 CSMA 的协议和基于 TDMA 的协议。本书只对这些协议中的一部分进行阐述。关于这些协议的更详细的信息请参见 Kumar 等（2006）文献。表中上半部分的协议最初是为无线网络和自组织网络设计的，而表中下半部分的协议则是专门应用于传感器网络中的。

表 4-2 WASM 应用中的 MAC 协议

<table>
<tr><td colspan="4">基于 CSMA 的协议</td><td colspan="3">基于 TDMA 的协议</td></tr>
<tr><td>ALOHA（1970）</td><td>MACA（1990）</td><td colspan="2">MACAW（1994）</td><td colspan="3">分布式 TDMA（1996）</td></tr>
<tr><td colspan="2">MACA-BI（1997）</td><td colspan="2">PICONET（1997）</td><td>蓝牙（1999）</td><td colspan="2">SMACS（2000）</td></tr>
<tr><td colspan="2">PAMAS（1998）</td><td colspan="2">IEEE 802.11（1997/1999）</td><td rowspan="2">NAMA，LAMA，
PAMA（2001）</td><td colspan="2" rowspan="2">LEACH
（2000）</td></tr>
<tr><td>RBAR（2001）</td><td>ARC（2001）</td><td colspan="2">SEEDEX（2001）</td></tr>
<tr><td>OAR（2002）</td><td>S-MAC（2002）</td><td colspan="2">LPL/Pre.
Samp.（2002）</td><td rowspan="2">ER-MAC
（2003）</td><td rowspan="2">TRAMA
（2003）</td><td rowspan="2">EMACS
（2003）</td></tr>
<tr><td>T-MAC（2003）</td><td>SIFT（2003）</td><td colspan="2">WiseMAC（2003）</td></tr>
<tr><td colspan="2">B-MAC（2004）</td><td>DMAC（2004）</td><td colspan="2">IEEE 802.15.4（2003）</td><td colspan="2">LMAC（2004）</td></tr>
<tr><td colspan="3">SEESAW（2005）</td><td colspan="2">Z-MAC（2005）</td><td>MMAC（2005）</td><td>BitMAC（2005）</td></tr>
</table>

避免碰撞多址访问（Multiple Access with Collision Avoidance，MACA）（Karn，1990）是第一个讨论了隐藏终端和暴露终端问题的方案。来自于 MACA 和 CSMA/CA 的 RTS-CTS 信号方案基于这一协议。为应对不可靠的无线信道并保证传送成功，MACA 无线（MACAW）协议通过在 RTS-CTS-DATA 帧的顶端加入第四个帧来改进 MACA 协议。当一个帧被正确接收时，将会有一个明确的应答（ACK）信息返回发送者节点。如果发送者节点没有及时接收到应答（ACK）信息，它将会重新传输数据。RTS-CTS-DATA-ACK 序列同时也是 IEEE 802.11 中 MAC 协议的基础。

注意，这里 RTS 和 CTS 帧假定比数据帧短，同时 RTS 和 CTS 信号也可能会和其他基站的 RTS 和 CTS 信号发生碰撞。然而，由于 RTS 和 CTS 信号更短，它们发生碰撞所产生的开销要远小于 DATA 帧冲突所造成的开销。当 DATA 帧比 IEEE 802.11 标准中的 dot11RTSThreshold 属性值小时，RTS-CTS 发信号方案就没有用了。

RTS-CTS-DATA-ACK 序列同时也被用于传感器 MAC（S-MAC）（Ye et al.，2004）和超时 MAC（T-MAC）（Dam 和 Langendoen，2003）。在这两种方案中，节点对一个公共时间段结构形成一致，并根据一个工作周期来周期性地交替打开和关

上它们的无线电装置。S-MAC 协议由三个主要的部分组成：周期性的侦听和休眠、避免冲突和串音、消息传递。节点会广播它们的休眠时间表。当节点们从它们的邻居节点处接收到这一时间表时，它们会调整自身的休眠时间表，使得所有节点同时进入休眠。在传输数据阶段，节点使用 RTS-CTS-DATA-ACK 发信方案交换数据。如果某个节点没有数据要发送或者接收，它就会进入休眠。周期性的监听和休眠通过避免空闲监听减少了能量消耗。

T-MAC（Dam and Langendoen，2003）在 S-MAC 基础上进行了改进，引进了一个活动/休眠工作周期，它通过一个简单的超时机制来适应网络信息流。节点使用 RTS-CTS-DATA-ACK 帧进行通信，这和 S-MAC 相似。T-MAC 协议通过传输可变长度突变和在突变之间休眠中的所有消息来避免空闲监听。在 T-MAC 中，某个节点只要是处于活动工作周期时就会进行监听和传输。活动工作周期会在一定时间内没有检测到活动事件（数据接收等）时结束。

在这些 MAC 协议中，节点在相同的传输能量等级下传输它们的帧。通过应用能量控制（Cayirci and Nar，2005；Karlidere and Cayirci，2006），节点可以根据其预定的接收者调节它的传输能量等级。然而，出于能量控制的目的，为不同的节点分配不同的传输能量等级会造成不对称链路问题，即节点 A 可以到达节点 B，但是节点 B 无法到达节点 A，这种结果会造成严重的冲突。为了解决由不对称链路现象而引起的冲突，RTS 和 CTS 在传输过程中处于最高的能量等级，而 DATA 和 ACK 在传输过程中处于使其到达目的地所需最低的能量等级，这就是 BASIC 方案中提出的思路（Jung and Vaidya，2002）。

能量控制 MAC（Power Control MAC，PCM）（Jung and Vaidya，2002）被提出用来改进 BASIC 方案。PCM 和 BASIC 方案的不同之处在于，PCM 在 DATA 帧传输过程中周期性地增加传输能量等级直到最大值。在 PCMAC 方案（Lin et al.，2003）中，RTS、CTS、DATA 和 ACK 的传输能量等级处于能够将帧传输到目的地所需的最小能量等级上，同时加入了一个独立的能量控制信道来防止帧在接收端发生冲突。

4.2　差错控制

特别在数据传输中，错误是无法容忍的。它们要被检测出来并进行纠正。处理传输错误的方法有两种：前向差错控制（Forward Error Control，FEC）和后向差错控制（Backward Error Control，BEC）。这两种方法都基于每次传输的帧中的冗余比特。在 FEC 中，冗余比特足以完成探测和修正错误。在 BEC 中，在帧中只加入相对较少的冗余比特用于检测错误。在这种方法中，接收者在检测到错误时要求发送者重发帧数据。对于使用 FEC 和 BEC 的选择问题主要是基于预期的比特错误率。

如果媒介非常容易出错，在传输的每个帧中至少会出现 1bit 的错码，那么 BEC 技术不是一个适用的技术。

4.2.1 纠错

FEC 方案的种类很多，例如卷积码和 Turbo 码。汉明码（Hamming Code）是这些方案中的一种。虽然汉明码并没有非常普遍地实现，但是其他的纠错方案都是基于汉明码所提出的基本概念。因此，我们在这一节将介绍汉明码。

汉明码中的基本概念是将数据块彼此进行区分，这样在发生传输错误时，接收到的数据块仍然可以和原始数据关联起来。可以通过在数据块中加入被称为校验位的冗余比特来实现。某个数据块和其他数据块不同的最小比特数称为汉明距离（Hamming Distance）。汉明距离指出可以被修正的错误比特位数。举例来说，如果汉明距离为 3，那么当有 1bit 数据在传输时发生变化时，接收到的数据块相比于其他可能的数据块更像原数据块，这是因为它和原数据块只有 1bit 不同，而与其他的数据块至少有 2bit 不同。因此，单一比特的错误可以被纠正过来。

假设将所有数据按照每 2bit 分成数据块。通过这 2bit 就会得到四种不同的组合。现在对每 2bit 数据块使用 3bit 的校验位来纠正传输错误。在这种情况下，可以为每 2bit 的数据建立一个代码（Codeword），这些代码彼此至少有 3bit 不同，如表 4-3 所示。当这 5bit 数据中的一位在任何符号上发生变化时，结果将会只是与源码存在 1bit 的区别，但与其他代码则至少有 2bit 的不同。举例来说，要传输 00，5bit 数据即 00000 将会被发送。如果这些比特中的一位在接收时出错，例如 00010，接收到的代码将不是表 4-3 所示的有效数据和校验位组合中的一组。然而，它与 00000 的距离只有 1，而它却与其他的有效代码间存在至少 2bit 的差异。因此，假设只存在 1bit 的错误，我们就能在移除接收数据块的冗余比特后推断出传输的数据块是 00。当接收到的数据有不止 1bit 的错码时，我们就无法将其和任何有效的代码联系起来。例如，01001 不是有效的代码，同时和 00000 及 01111 的汉明距离均为 2，这可能出现在传输其中任一代码出现 2bit 错误的情况中。因此，我们能够检测到但无法修正这一错误。在出现更多位数的错码的情况下，这一方案就无法检测到错码，甚至会将接收到的数据与错误的代码进行关联。

表 4-3 数据块和编码

原始数据块	数据和校验位
00	00000
01	10101
10	11010
11	01111

汉明码是一种遵循这一基本概念的块编码系统。在拥有 m 位校验位时，最小汉明距离为 3，同时 $2^m - 1$bit 数据块中出现单一比特错码可以被纠正。校验码的插入位置相当于 2 的幂，从最低位开始。这确保了当它们在代码中的位置表示为二进制形式，只有处于检验位相对位置的比特为 1，其余的为 0。

例如，假设使用 4 个校验位。它们被插入在传输数据块中 2^0、2^1、2^2 和 2^3 的位置。以二进制的形式它们分别表示为 0001、0010、0100 和 1000。这些比特串被称为位置串，它们的长度等于校验位的数量。包括校验位在内的数据块中的最大比特数不能超过 $2^m - 1$，因为这是 $m$bit 所能表示出的最大可能值。

在汉明码生成过程中，数据比特首先被插入不是为校验位准备的位置。之后数据块中的所有“1”比特的位置串进行异或操作。结果中的每比特是相关校验位的值。举例来说，如果结果为 1001，这表明最高和最低校验位是 1，而其他的为 0。在这之后，如果将所有“1”比特的位置串进行异或，包括校验位，除非出现传输错误，这一结果应该等于 0。若有单一比特错误，这种操作的结果给出了传输中变化的比特的位置串。

在例 4-1 中，位于位置 5、9、11 和 15 的比特位为 1。如果将这些位置串的比特进行异或，得到的结果为 8，这表明只有最高校验位为 1，其他的校验位为 0。基于此，例 4-1 中所示的数据块将会进行传输。假设在传输中第 7 位的比特出现变化。当对 7 的位置串比特应用异或操作时，结果显然等于 7，这表明第七位的比特在传输中发生了改变。

例 4-1

校验位数 m：4

最大数据块长度：$2^4 - 1 = 15$

数据块：10001010010

位数	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
位置串	1111	1110	1101	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001
数据	1	0	0	0	1	0	1		0	0	1		0		
校验位								1				0		0	0
数据块	1	0	0	0	1	0	1	1	0	0	1	0	0	0	0

1111
1011
1001
0101

1000

4.2.2　错误检测

检测错误的最简单技术是在传输的比特中加入校验位。校验位的开销很小，而

且不需要太多的计算。然而，它可能无法检测区间误差（Burst Error）。当两个或更多的比特在传输中发生改变时，它们可能会相互抵消；接收者可能无法检测到帧发生混乱的现象。因此，另一种称为循环冗余校验（Cyclic Redundancy Check，CRC）的技术经常用于错误检测。

在这种技术中，被称为生成多项式的一个字符串首先被确定下来。它被称为生成多项式，是因为 CRC 被看做一种多项式运算，其中输入和生成字符串表示成系数为 0 或 1 的多项式。一个生成多项式用来生成校验和，它附加于帧的末尾。接收者通过使用相同的生成多项式对输入进行检查，检测传输错误。选取生成多项式有两个准则：

1）它必须比帧长度短；

2）它必须以 1 开始并以 1 结束。

生成多项式也有其他期望的特性：

1）我们可以使用 $x+1$ 作为生成多项式的因子，即生成多项式的最后 2bit 为 11。

2）我们可以选择一个不能除尽 x^m+1 的生成多项式，即不是 x^m+1 的一个因子，这里的 m 表示最大帧长度。

这种算法基于除运算的一个基本性质。如果一个除运算中的余数从被除数中减去，结果对于除数来说就是可整除的。CRC 在接下来的三步算法中使用了这种性质来产生校验和。

假设存在一个 $i$bit 的帧 $F(x)$ 和一个 $k$bit 的生成多项式 $G(x)$。

1）在帧的末尾处添加 $k-1$ 个 0。得到的多项式为 $M(x)=x^{k-1}F(x)$，同时其长度为 $m=i+k-1$。

2）将 $M(x)$ 除以 $G(x)$，注意这里是一个多项式除法，例如模 2 除法，不存在加法进位和减法借位。余数为 $R(x)$。

3）使用模 2 减法将 $R(x)$ 从 $M(x)$ 中减去。结果就是要传输的帧，长度为 m 的 $T(x)$。

目的节点接收 $T(x)$ 并对它除以 $G(x)$。如果能够除尽，即没有余数产生，就表明传输没有出现错误。CRC 确保了以下几点：

1）可以检测到所有单一比特错误；

2）当 $x+1$ 是生成多项式中的一个因式时，可以检测所有颠倒奇数比特的错误；

3）当 $G(x)$ 不能整除 x^m+1 时，所有单独的 2bit 错误都会检测出来；

4）所有小于 k 的区间误差都能检测到。

总的来说，当生成多项式选择适当时，CRC 无法检测到错误的概率非常低。也有实用的硬件方案来实现算法。因此，它用于许多标准和协议栈中，例如

IEEE 802。

例 4-2

生成多项式 $G(x)$：1011，$k=4$

输入帧 $F(x)$：1110010100，$i=10$

步骤 1：附加 $k-1$ 个 0 于输入帧的尾部

输入帧 $M(x)$：1110010100000，$m=13$

步骤 2：用 $G(x)$ 除 $M(x)$

```
1110010100000
1011
0101010100000
 1011
 000110100000
    1011
    011000000
     1011
     01110000
      1011
      0101000
       1011
       000100
```

余数 $R(x)$：100

步骤 3：从 $M(x)$ 中减去 $R(x)$

传输帧 $T(x)$：1110010100100，$m=13$

$T(x)$ 可以被 $G(x)$ 整除。因此，如果没有出现传输错误，接收端的 $T(x)$ 就能够被 $G(x)$ 整除，这表示传输成功。

4.3　无线城域网

4.3.1　IEEE 802.16

用于宽带无线接入（Broadband Wireless Access，BWA）的无线城域网（Metropolitan Area Network，MAN）标准从 2001 年开始不断演进。最初工作中提出的 IEEE 802.16、IEEE 802.16a 和 IEEE 802.16c 最后合并为 IEEE 802.16—2004，同时也被

称为 IEEE 802.16d。它同时为固定宽带无线接入（BWA）系统（ANSI/IEEE，2004）定义了媒介访问控制层和物理层规范。经过修正的 IEEE 802.16e—2005 随后发布用于包含固定和移动操作（IEEE，2005b）。

标准为不同的频段定义了多个物理层规范，例如配置文件。在 10～66GHz 频带上的单载波调制被用于基站间的固定的、点到点和视距通信中。对于低于 11GHz 的频率，采用了单载波或者正交频分复用（OFDM）或者正交频分多址接入（OFDMA）的方式。基站和多个固定用户站之间的非视距通信发生在 2～11GHz 的频带上，而移动基站使用 2～6GHz 带宽的频率范围。物理层同时支持时分双工（TDD）和频分双工（FDD）操作。

和多物理层规范相对应的，标准提供了一个单一的 MAC 层。MAC 层主要支持点到多点（Point-to-MultiPoint，PMP）的架构。另外，提供了低于 11GHz 频带的可选的 Mesh 拓扑。为 PMP 拓扑结构提供的 MAC 是一个无冲突方案，其中基站为用户站分配了一个动态时间段。下行链路数据使用时分复用（TDM），而 TDMA 被用于上行链路传输。在 Mesh 模式中，所有基站和它们的单跳邻居之间都存在直接的链路连接。因此，它们被要求广播它们的时间表，通过一种三次握手机制和邻居进行协调。

4.3.2 WiMAX

全球微波接入互操作性（WiMAX）确保了某个 WiMAX 设备和其他经过 WiMAX 认证的设备的互操作。此外，它和 IEEE 802.16 以及欧洲电信标准学会（European Telecommunications Standards Institute，ETSI）的高性能无线电城域网（HiperMAN）标准一致。WiMAX 论坛（http：//www.wimaxforum.org）包括 400 多个企业成员，执行认证过程。由 WiMAX 论坛设计的一致性和互操作性测试目前在分别位于韩国、西班牙和中国的三个实验室中完成。

目前，认证过程并没有涵盖所有的频段。只有服务提供商和设备制造商需要的关键频段被进行了处理。为固定无线应用设计的产品在 3.5GHz 和 5.8GHz 频带内得到了认证。然而，2.3GHz、2.5GHz 和 3.5GHz 被用于移动应用程序。随着频谱分配的演化，WiMAX 论坛已经形成了频谱和规范数据库来在全球许可活动中向成员提供当前数据。

在宽带无线接入最后一公里技术中，作为电缆或者数字用户线路的替代，WiMAX 论坛已经证明了固定系统可以达到在半径 3～10km 范围内每个信道 40Mbit/s 的速率。另一方面，移动应用可以在 3km 内提供最大 15Mbit/s 的容量。

4.4　无线局域网

4.4.1　IEEE 802.11

用于无线局域网的物理层和媒介访问控制层规范在 IEEE 802.11 标准（ANSI/IEEE, 1999）中给出了定义。标准定义了两种模式的操作：点协调功能（Point Coordination Function, PCF）和分布式协调功能（Distributed Coordination Function, DCF）。DCF 针对自组织网络。

IEEE 802.11 标准的 DCF 主要建立在 MACA 无线（MACAW）的基础上，遵循由一个 4 帧 RTS-CTS-DATA-ACK 握手组成的带碰撞避免的载波侦听多址访问（CSMA/CA）竞争机制，来实现发送者和接收者之间的数据传输。IEEE 802.11 同时支持物理（空中接口）和虚拟载波（在 MAC 层）侦听。物理载波侦听通过来自于其他源的相对信号强度来检测活动行为。虚拟载波侦听通过为 RTS/CTS 和 DATA 帧头部的每一帧发送 MAC 协议数据单元持续时间信息来实现。持续时间字段指示完成帧传输所需花费的时间。网络分配矢量（Network Allocation Vector, NAV）将被更新为其他目的地的传输持续时间的值。使用 NAV，节点的 MAC 知道什么时间为当前传输结束。NAV 在接收到一个来自于发送者的 RTS 或者接收者的 CTS 时进行更新，因此避免了隐藏终端问题。

节点的载波侦听范围可以被分成两个区域：传输范围以及载波侦听区。节点传输范围内的传输可以被接收到，同时它们的内容可读。另一方面，载波侦听区内的节点传输没有足够的 SNR 使其内容可读，但是传输可以被侦听到。位于传输范围内的节点根据接收到的 RTS 或者 CTS 信号设置它们的 NAV，而位于载波侦听区的节点由于无法解码帧而将它们的 NAV 设置为扩展帧间空间（Extended Inter-Frame Space, EIFS）持续时间，它是一个很长时间的计数器。如果物理或虚拟载波侦听机制中的任意一个指出信道忙碌，那么就认为信道此时是忙的，同时接入将会推迟到当前传输结束之后。

IEEE 802.11 拥有很多个版本，见表 4-4。这些版本之间的主要区别在于物理层规范。在 MAC 层，它们都遵循 CSMA/CA 方案。

表 4-4　IEEE 802.11 版本

协 议 版 本	工作频率/GHz	最大数据率/Mbit/s	范围/m
802.11	2.4 ~ 2.5	2	未给出
802.11a	5.15 ~ 5.35/5.47 ~ 5.725/5.725 ~ 5.875	54	75
802.11b	2.4 ~ 2.5	11	100
802.11g	2.4 ~ 2.5	54	75
802.11n	2.4 或 5	54	125

4.4.2 Wi-Fi

无线保真（Wi-Fi）是分配给符合 IEEE 802.11 系列标准设备的一个证书标记，同时和其他的 Wi-Fi 认证设备进行互操作。拥有至少 300 个会员的 Wi-Fi 联盟（http：//www.wifialliance.com）负责开展认证过程。

Wi-Fi 提供了两种操作模式：使用一个或多个接入点（AP）的基础设施网络和没有接入点的自组织网络。基础设施网络中的数据流发生在接入点和基站之间的星形拓扑中。因此，接入点周期性地传输其服务集标识符（Service Set Identifier，SSID），基站用它确定将要连接的接入点。另一方面，点对点通信被用于自组织模式的操作中。

经 Wi-Fi 认证的设备对于 2.4GHz 或者 5GHz 的 ISM 带宽或者双频有效。它们能够根据本地规则和用户喜好来操作 14 个信道中的某个信道。Wi-Fi 物理层使用直接序列扩频（Direct-Sequence Spread Spectrum，DSSS）传输系统。数据传输率可以达到 11Mbit/s 或者 54Mbit/s，同时随着信号质量降低而衰减。基本的 MAC 功能必须符合 IEEE 802.11 标准中描述的 CSMA/CA 方案。

4.5 无线个域网

4.5.1 IEEE 802.15.1

IEEE 802.15.1 标准同时定义了无线个域网（WPAN）（IEEE，2005a）通信中的物理层和 MAC 层规范。处于 WPAN 中的设备被认为形成了一个 piconet。其中的某个设备被称为主机（Master），而其他设备被称为伺服设备（Slave）。伺服设备只允许和主机节点进行通信。在同一时刻最多只能存在 7 个活动的伺服设备，而同时 255 个未激活伺服设备可以等待被主机激活。主机节点为 piconet 提供同步时钟和跳频模式。在 2.4GHz 带宽的 79 个信道中使用了跳频扩频（Frequency Hopping Spread Spectrum，FHSS）。主机节点的地址和时钟被用来共同确定跳频模式。

只要 piconet 使用不同的信道，而且它们的主机节点不同，那么就不止一个 piconet 可以出现在同一个区域。某个设备可以通过使用时分复用（TDM）属于多个 piconet。这些 piconet 可以形成一个 scatternet。scatternet 中的路由超出了标准的范围。

标准将物理信道分为四个种类。查询扫描信道用于发现设备。已发现设备间的连接通过页面扫描信道建立。已建立连接的设备之间的通信可以在基本 piconet 信道上或者适应性 piconet 信道上进行。在数据包首部传输的接入码确定了要使用的物理信道类型。某个设备只要在某时刻只有一种信道被使用时，可以通过使用

TDM 在所有类型的信道上进行操作。

媒介接入方案是根据使用的物理信道种类来区分的。基本 piconet 信道由一些时间段组成，这些时间段都和跳频模式中的射频频率相关联。时间同步和时间段编号基于主机节点的时钟。piconet 主机节点的传输只能在偶数时隙开始同时持续五个时隙。伺服设备的传输由主机节点控制。每个来自于主机节点的数据包定义了伺服节点的响应方式。跨伺服设备间的通信在基本 piconet 信道中不会出现。适应性 piconet 信道和基本 piconet 信道拥有相同的特性，但以下两方面除外：首先，来自于伺服设备的响应使用和主机相同的频率；其次，跳频模式包含少于 79 种频率，同时将其他频率标记为未使用。查询扫描信道和页面扫描信道中的通信都基于点对点连接。设备或者发送一个（页面扫描或查询）请求或者在所有（查询或页面扫描信道）频率上随机地侦听响应。设备在两个信道中均保持被动状态直到接收到请求，同时它们使用一个比 piconet 信道更低的跳变比率。另一方面，进行响应的设备使用一个更快的比率，因此在一个短时间内覆盖所有频率。

4.5.2　蓝牙

IEEE 802.15.1 是基于蓝牙的一个标准。事实上，2002 年审核通过的 IEEE 802.15.1 的最初版本采用了蓝牙 v. 1.1 的物理层和 MAC 层协议。因此，它们在底层协议栈部分几乎是相同的。蓝牙是一个由工业界提出的旧标准（始于 1994 年），有更大范围的协议层。

在这一节中，我们不解释所有的蓝牙协议，而是定义蓝牙规范（Profiles），它们是蓝牙设备之间的标准化接口。每个蓝牙设备都必须在应用范围内和蓝牙规范相一致。因此，以下列出的蓝牙规范列表同时也是蓝牙设计所应用的领域：

1）蓝牙立体声声频传输规范（Advanced Audio Distribution Profile，A2DP）；
2）声频/视频远程控制规范（Audio/Video Remote Control Profile，AVRCP）；
3）基本图像规范（Basic Imaging Profile，BIP）；
4）基本打印规范（Basic Printing Profile，BPP）；
5）通用 ISDN 接入规范（Common ISDN Access Profile，CIP）；
6）无线电话规范（Cordless Telephony Profile，CTP）；
7）设备 ID 规范（Device ID Profile，DID）；
8）拨号网络规范（Dial-up Networking Profile，DUN）；
9）传真规范（Fax Profile，FAX）；
10）文件传输规范（File Transfer Profile，FTP）；
11）通用声频/视频分配规范（General Audio/Video Distribution Profile，GAVDP）；
12）通用访问规范（Generic Access Profile，GAP）；
13）通用对象交换规范（Generic Object Exchange Profile，GOEP）；

14）免提规范（Hands-Free Profile，HFP）；

15）硬拷贝电缆替代规范（Hard Copy Cable Replacement Profile，HCRP）；

16）蓝牙耳机规范（Headset Profile，HSP）；

17）人机界面规范（Human Interface Device Profile，HID）；

18）网内通信规范（Intercom Profile，ICP）；

19）对象交换规范（Object Push Profile，OPP）；

20）个域网规范（Personal Area Networking，PAN）；

21）电话簿访问规范（Phone Book Access Profile，PBAP）；

22）串行端口配置规范（Serial Port Profile，SPP）；

23）服务发现应用规范（Service Discovery Application Profile，SDAP）；

24）SIM 卡访问规范（SIM Access Profile，SAP，SIM）；

25）同步规范（Synchronization Profile，SYNCH）；

26）视频分享规范（Video Distribution Profile，VDP）；

27）无线应用协议承载（Wireless Application Protocol Bearer，WAPB）。

正如这一规范列表中指出的，蓝牙主要用于个人设备的相互无线连接，或者用于连接它们的外围设备。

4.5.3 IEEE 802.15.4

另外一个用于 WPAN 的标准主要针对有限电池消耗需求的设备，例如互动玩具、智能徽标（Smart Badges）、远程控制和家庭自动化。它为 10m 范围内个人操作空间的低数据率无线连接定义了物理层和 MAC 层规范（IEEE-SA Standards Board，2003）。

物理层规范取决于本地规范和用户偏好。全球 2.4GHz 频段带宽支持 16 个信道的 250kbit/s 数据率。在欧洲和北美，单个信道 20kbit/s 和 10 个信道 40kbit/s 分别定义在 868MHz 和 915MHz 频率带宽上。使用二相相移键控（Binary Phase Shift Keying，BPSK）调制的直接序列扩频（DSSS）用于 868/915MHz 物理层，而 2.4GHz 物理层使用偏移正交相移键控（Offset Quadrature Phase Shift Keying，O-QPSK）调制的 DSSS。能量探测（Energy Detection，ED）、链路质量指示（Link Quality Indication，LQI）和空闲信道评估（Clear Channel Assessment，CCA）是物理层中要执行的一些任务。

标准定义了 WPAN 中的两类设备。全功能设备（Full Function Devices，FFD）可以和其他任何设备通话，同时可以作为一个 PAN 协调器或者一个设备。另一方面，精简功能设备（Reduced Function Devices，RFD）只允许和 FFD 进行通信。如果只有少数 FFD，设备就会被组织成为星形拓扑，否则用点对点拓扑。

协调器可以传输形成 16 时隙超帧结构的信标帧。无竞争和基于竞争的接入在

超帧时段都是可能的。无竞争时段（Contention-Free Period，CFP）由 PAN 协调器贡献给低时延应用程序的保证时段（Guaranteed Time Slot，GTS）组成。剩余的时间段通过使用分时段的 CSMA-CA 机制接入。超帧的使用是可选的。因此，未分时段的 CSMA-CA 被用于无信标帧使用的网络，以及端点必须不间断或者同步地接收对方信号的点对点网络中。点对点同步不在标准范围内。

4.5.4　ZigBee

ZigBee 被 ZigBee 联盟定义为一个可靠的、有成本效益的、低功耗的、无线网络监视控制产品。ZigBee 联盟是一个致力于为 ZigBee 开发一个开放的全球性标准并为标准提供认证服务的公司的联合。ZigBee 包括用于物理层和 MAC 层的 IEEE 802.15.4。另外，ZigBee 协议簇还对网络和应用层提供支持。ZigBee 希望通过提供以下特点而发展成为全球控制/传感器网络标准：

1）低成本、低容量设备；
2）低能耗；
3）简单高效的协议族；
4）对高密度部署的可扩展性；
5）可靠的短距离数据传输；
6）适当的安全级别。

在 ZigBee 中，有两类物理设备：全功能设备（FFD）和精简功能设备（RFD）。FFD 可以和任何拓扑中的其他 ZigBee 设备进行对话，并变成一个协调器。RFD 是只能和一个 FFD 通信的简单设备。因此，它们在星形拓扑网络中只能作为伺服设备。每个 ZigBee 网络都需要至少一个 FFD。

ZigBee 的典型的数据流类型对于传感器网络来说是周期性的，对于控制网络来说是间断性的，而对于低延迟实时设备来说是重复性的。它的网络和应用层被设计用于支持这些无线传感器网络和执行器网络的数据流种类。在 ZigBee 联盟的网站上可以找到更多的细节。

4.5.5　WiMedia

WiMedia 和 IEEE 802.15.1 以及 IEEE 802.15.4 一样，是为 WPAN 设计的。然而，它在多媒体和数字图像应用中使用了特宽频带（Ultra-Wideband，UWB）技术提供更高的传输速率，与 IEEE 802.15.1 支持 3Mbit/s 相反，它更适合于视频流传输。

IEEE 802.15.3 和 IEEE 802.15.3a 是实现 WPAN 中更高速率的第一个标准化尝试。这两个尝试在 2006 年被废弃。另一方面，以前标准化方面的工作之后被一个叫做 WiMedia 联盟的组织取代（http：www.wimedia.org）。

WiMedia 是用于 WPAN 中高速低能量多媒体数据传输的 UWB 通用无线电平台。它的 MAC 层和物理层规范是通过两个基于 ISO 的规范定义的，即 ECMA-368 和 ECMA-369（ECMA，2005）。在 3.1 ~ 10.6GHz 频带内的物理层的操作使用多频带 OFDM（MB - OFDM）复用。WiMedia 支持高达 480Mbit/s 的数据传输率。另外，它可以和其他的一些无线技术共存，例如蓝牙和 Wi-Fi。

MAC 层包括了基于预订的和基于竞争的接入。由于没有协调器设备，所以所有设备为了实现协调，周期性地交换信标帧。预订和调度信息嵌入在信标帧中。信标时段（BP）由可变数量的媒介接入时段组成，它位于超帧的首部。超帧由 256 个媒介接入时隙组成。在信标时段之后，参加预订的设备在它们的时隙发送它们的帧。剩余的时隙使用优先竞争接入（Prioritized Contention Access，PCA）进行占用。

PCA 基于四种接入种类（Access Categorie，AC）。一个帧被分为背景（Background）、最佳耗费（Best Effort）、视频（Video）或者音频（Voice），分别代表由低到高的一个优先顺序。对于每个 AC，定义了不同参数集，例如，仲裁帧间空间（Arbitration Inter-Frame Space，AIFS）和竞争窗口（CW）。使用为这一种类定义的参数，定义了一个类似于 CSMA/CA 的接入过程，来获得一次传输机会（Transmission Opportunity，TXOP）。

4.6 复习题

4.1 讨论 CSMA 中时延（Latency）、节点数量和冲突发生概率之间的关系。讨论局域网中 SNR、冲突概率和诸如范围和节点数量限制等设计因素之间的关系。

4.2 非持续 CSMA 和 P 持续 CSMA 之间的区别是什么？以太网是否是一种基于持续 CSMA 的方案？

4.3 FH-CDMA 和 DS-CDMA 之间有什么区别？

4.4 S-MAC 是一种能量控制方案吗？能量控制如何影响一个自组织网络 MAC 协议的性能？自组织 MAC 协议的能量控制还有哪些其他挑战？能量控制是否对于安全考虑更加有利？为什么？

4.5 WiMedia 和 IEEE 802.11 之间有什么关系？

4.6 IEEE 802.11、IEEE 802.15.1、IEEE 802.15.3、IEEE 802.15.4 和 IEEE 802.16 之间有哪些区别？

4.7 假设下列开销和错误控制方案有关：

2% 用于错误探测

40% 用于错误修正

当方案对 500bit、1000bit 和 1500bit 帧是实用的，最大比特错误率分别是多少？假设接收者发送 100bit 的帧来要求以 BEC 进行重传。

4.8　为例 4.1 回答以下这些问题：

(a) 如果 $T(x)$ 中的最低比特位被逆转时是否能够检测到？

(b) 如果 $T(x)$ 中的最低 2bit 位被逆转时是否能够检测到？

(c) 如果 $T(x)$ 中的最低比特位和最高比特位被逆转时是否能够检测到？

(d) 如果 $T(x)$ 中的任意 4bit 位被逆转时是否能够检测到？

第 5 章　路　　由

路由协议通常是任何协议簇的核心。比如，在传输控制协议/互联网协议（Transmission Control Protocol/Internet Protocol，TCP/IP），IP 就是路由。在 TCP/IP 的其他协议中，如 ftp、SMTP、TCP、UDP、IGMP 等，或更低层如 IEEE 802.11、IEEE 802.3、IEEE 802.16 等，这些协议可能会也可能不会用在因特网的数据传输中。然而，任何在因特网中的传输都必须封装在一个 IP 包里。

虽然我们关注点是 WASM，但是在 WASM 应用中 IP 并不总是首选。由于许多 WASM 与因特网相连，IP 仍然是重要的。WASM 接入因特网的点能使一些安全攻击有机可乘。也有这样一种情况，当一个 WASM 节点正和一个因特网主机通信时，IP 包会被封装在 WASM 协议里。此外，特别是一些 Mesh 网络应用可能会直接运行 IP。因此，本章也要讨论 IP。

5.1　互联网协议和移动 IP

IP 是链路层协议，比如每一个路由器多路复用 IP 报头，根据 IP 报头的参数决定哪一个包发送给下一个路由器，并且再次把 IP 包封装进去。IP 上层的协议，比如 TCP，是端到端的协议，这意味着它们的报头只有在两个主机彼此通信时，才能被多路复用和封装。IP 从一个路由表中选择下一个路由器，这个路由表能手动更新或在某些情况下由互联网控制消息协议（Internet Control Message Protocol，ICMP）更新。这些路由表也可以由路由协议管理，比如开放最短路径优先（Open Shortest Path First，OSPF）和边界网关协议（Border Gateway Protocol，BGP）。还有一种情况是，IP 可以使用受限源路由，其中下一跳路由器已经在报头，因为源节点已经在 IP 报头可选域里写入了路由。因为源路由会避免较不安全的路由和路径，所以源路由带来额外的安全。

5.1.1　IPv4、IPv6 和 IP 安全

IP 的功能是基于 IP 报头的。图 5-1 所示的是 IPv4 报头。

在本书中，我们不会解释报头里的每一个字段。感兴趣的读者可以参考 Tannenbaum 文献（2003）获取更多细节。

报头固定部分是 20B，其他任选字段可以扩充报头。因此，它的长度是可变的，IP 报头长度（IP Header Length，IHL）字段决定了报头的长度。因为 IHL 字段

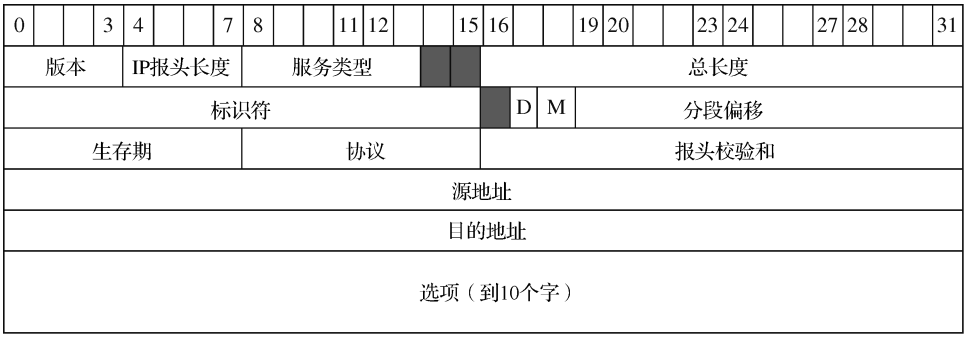


图 5-1　IPv4 报头

是 4bit，IPv4 报头总的长度最多是 15 个字，即 60B，所以这意味着任选字段最多有 40B 的空间。IPv4 起初有 5 个任选字段，其中一个是有关安全的，用来说明包的保密程度，以及源节点不希望传输包通过的路由器。虽然明确指出哪个文件是保密的，这多少有些用处，尤其在军用方面，但是这也有助于敌手识别哪个包有机密内容。结果，这个字段一般不使用，也没能证明它的有效性。

IP 安全协议（IPsec）是为了 IP 提供数据机密性、数据完整性和抗抵赖服务而开发的。这个设计是与加密算法相独立的、允许多粒度，比如保护两个路由之间所有通信或两个主机之间的一个单向 TCP 连接。它有两种工作模式：传输模式和隧道模式（见图 5-2）。

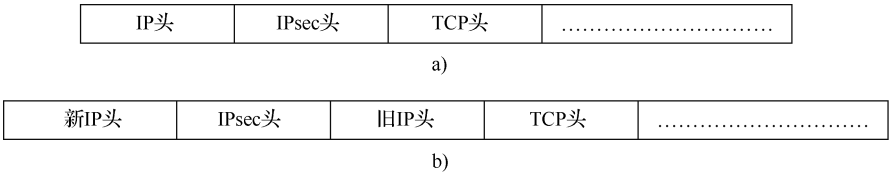


图 5-2　IPsec 协议模式

a）传输模式　b）隧道模式

为了把一个可选报头插入 IP 报头和 TCP 报头之间，传输模式使用了 IPv4 的“协议字段”。协议字段通常是指封装在 IP 包里的传输层协议。它可能是 TCP、用户数据报协议（User Datagram Protocol，UDP）或者是其他协议。当使用 IPsec 协议时，这个字段指的是 IPsec 协议的报头。

当优先使用隧道模式时，IP 包是封装在另一个应用 IPsec 协议的 IP 包里，这是为了在两个节点之间创建一个安全隧道，这两个节点不必是在一个连接终端节点的主机或路由器（见图 5-3）。像这样一个隧道也能用在聚合多个流为一个单个数据流时，这使敌手更不容易进行流量分析。

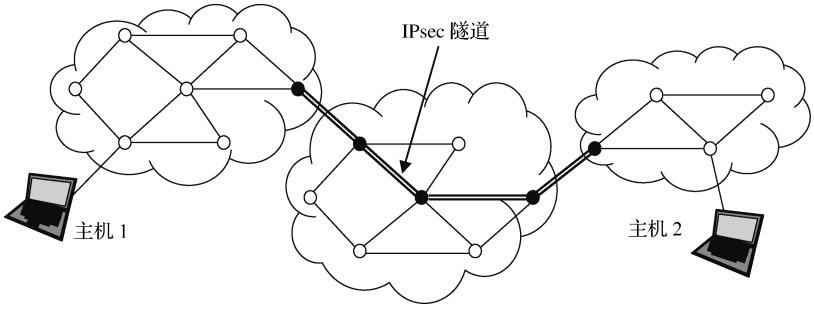


图 5-3 IPsec 协议隧道模式

IPsec 协议报头有两种形式：认证头（Authentication Header，AH）和封装安全载荷（Encapsulating Security Payload，ESP）。图 5-4 是认证头中字段的示意图。认证头的安全参数索引是安全关联（Security Association，SA）的标识符。虽然 IP 不是一个基于端到端的、面向连接的协议，但是 IPsec 协议要求创建一个安全关联，这个安全关联是对安全参数索引在一段时间内有效的基本协定。序列号（Sequence Number，SN）是每一个有相同安全参数索引的 IPsec 协议报头的唯一号码。当所有序列号都用在同一个安全参数索引时，会选择一个新安全参数索引，这意味着终止了之前的安全关联，并创建了一个新的安全关联。这两个字段是为了保护免受重放攻击。认证数据是对包和共享密钥进行哈希运算的结果，例如，一个哈希消息认证码（Hash Message Authentication Code，HMAC）。我们将在第 9 章中详细解释用于认证的哈希方案。认证数据确保 IP 包的完整性。

图 5-4 认证头

认证头用于数据完整性和抗抵赖服务，但不能用于数据机密性。封装安全载荷头支持数据机密性，除了安全参数索引和序列号字段，还有用于加密的初始矢量字段。这个初始矢量通过选择的加密算法使用。

IPsec 协议报头插入到 IP 报头和 IP 包其余部分之间，这通过 IPv4 报头的 protocol 字段来表明。IPv6 有一个字段叫 next header（下一个报头），它取代了 IPv4 中

的 protocol 字段（见图 5-5）。IPv6 包的报头是可以扩展的，next header 字段会告诉现在报头之后将是哪种类型的报头。因此，认证头（AH）和封装安全载荷（ESP）是 IPv6 的报头扩展。

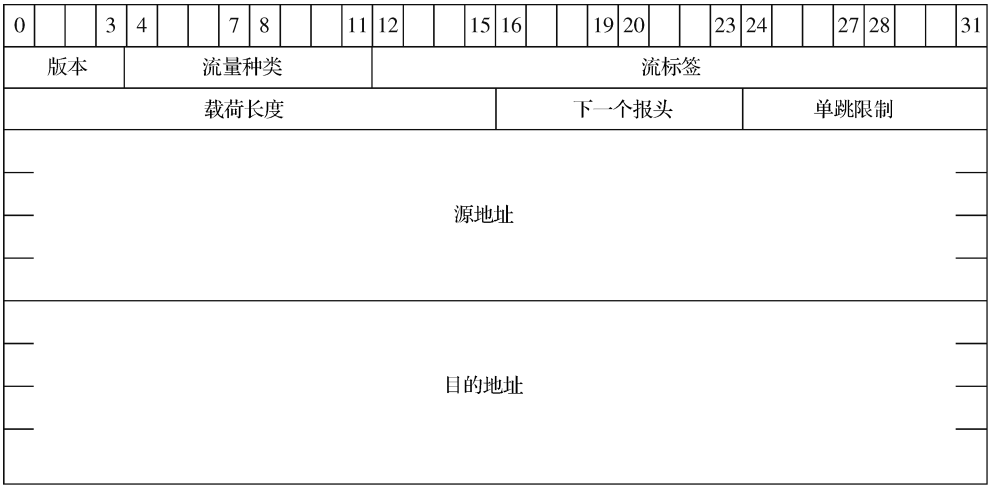


图 5-5　IPv6 报头

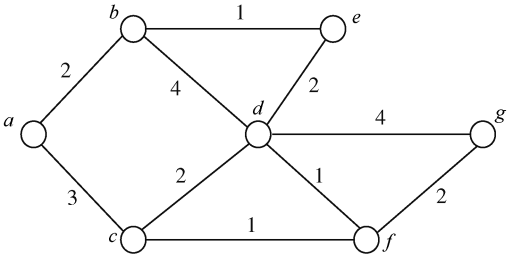
5.1.2　距离矢量和链路状态算法

IP 在链路层运行，在到目的地的路由中，把包发给下一个路由器。在路由算法维护的路由表里，查找下一个路由器。为此目的开发的早期路由算法是基于距离矢量（Distance Vector）方案的。之后的路由算法使用链路状态方法。

在距离矢量方案中，每一个路由器维护一个表，表中规定下一跳路由器和一个表明通过这个路由器路由成本的度量，通过该路由器的路由到达网内的每一个其他路由器。路由的成本可以由一个参数决定，比如跳数、拥塞概率等。路由器周期地把表发送给它们的邻居。当路由器接到来自邻居的新路由表时，它将新的表和它自己的表比较，检查是否有通过发送表的邻居的更好路由。为此，该路由器把到达邻居的成本添加到接收表里的路由成本中。如果结果比它的表的值小，路由器就把下一跳的 id 用发送此表的邻居 id 替换掉，用该特定目的端的计算结果替换掉路由成本，这样就更新了路由表。

例如，假设图 5-6a 的节点 *b* 最初有路由表（见图 5-6b），然后它收到节点 *e* 的路由表（见图 5-6c）。节点 *b* 和 *e* 间的成本是 1。根据节点 *e* 的路由表，节点 *e* 和 *d* 间的成本是 2。因此，如果节点 *b* 通过节点 *e* 发送一个到节点 *d* 的包，总的成本是 3。然而，在节点 *b* 的表中，节点 *b* 和 *d* 的成本是 4，成本更高。因此，节点 *b* 就通过节点 *e* 发送一个到节点 *d* 的包，这样也就更新了节点 *b* 的表。类似地，它也更新

与节点 f 和 g 有关的记录。



a)

目的地	下一个	成本
a	*a*	2
c	*a*	5
d	*d*	4
e	*e*	1
f	*d*	5
g	*d*	8

b)

目的地	下一个	成本
a	*b*	3
b	*b*	1
c	*d*	4
d	*d*	2
f	*d*	3
g	*d*	5

c)

目的地	下一个	成本
a	*a*	2
c	*a*	5
d	*e*	3
e	*e*	1
f	*e*	4
g	*e*	6

d)

图 5-6 距离矢量算法

a）示例网络 b）节点 *b* 的初始路由表 c）节点 *e* 的路由表 d）节点 *b* 的更新路由表

距离矢量算法引入了一个“无限计数”（Count-to-infinity）的问题，就是路由器崩溃后，有关它的更新不能有效地扩散。为了理解这个问题，跟踪这种情况的算法，其中图 5-6a 中的每一个节点都有一个完美的路由表。节点 d 崩溃时，节点 e 发现这一情况，节点 b 和 e 用以下次序交换它们的路由表：b、e、b、e 和 b。有兴趣的读者可以参考 Tannenbaum（2003）文献，了解更多“无限计数”问题。

链路状态方案不会有无限计数的问题。在该方案中，每个节点通过“ECHO”消息发现到邻居节点的延迟，并通过泛洪方式把此信息传播到网络上去。有一些与泛洪方式有关的小的挑战，比如负载邻居节点消息的循环和延迟。不过，相应地也有解决它们的办法。通过收集这些数据，每个节点对网络有一个完整的图像。然后，可以运行一种最短路径算法，决定网络中通向每一个其他路由器的最佳路由。

路由信息协议（Routing Information Protocol，RIP）是阿帕网（ARPANET）和因特网最初的路由算法，它是基于距离矢量方案的。之后的算法像开放最短路径优先（OSPF）算法和中间系统-中间系统（Intermediate System-Intermediate System，IS-IS）都是链路状态算法。

注意：各种攻击可以基于错误的更新或路由表信息设计。例如，一个恶意节点可以通过散布错误的路由表或链路数据，伪装成一个对其他路由器有吸引力的节点。这尤其对自组织网络中的路由更有威胁。我们将在以下章节和第 8 章中讨论对

路由方案的各种类型的攻击。

5.1.3　网络互连

因特网是许多自治（Autonomous）网络的网络。每个自治网络是由一些边界和网关路由器以及它们之间的链路组成的。边界路由器把自治网络连接在因特网上。虽然任何个人都不拥有因特网，它是由自治网络志愿加入产生的，但是自治网络是某些机构、组织和个人所有的，自治网络内或通过自治网的流量受到自治网拥有者控制。例如，图 5-7 所示的自治网络 B 可能会阻止要发送到自治网络 D 的包通过网络 B 运送。因此，有一些区别于自治系统的一些网络互连的考虑，这需要两类不同的网络互连协议：针对自治网络内部路由的内部网关协议（Interior Gateway Protocol，IGP）和针对自治网间路由的外部网关协议（Exterior Gateway Protocol，EGP）。

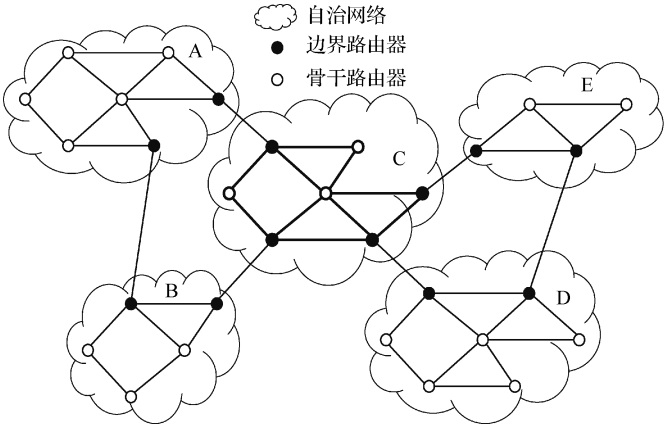


图 5-7　网际网（链接网络的网络）例子

路由信息协议（RIP）、开放最短路径优先（OSPF）算法和中间系统-中间系统（IS-IS）大体上设计得像内部网关协议。而边界网关协议（BGP）是最有名的外部网关协议。通过使用外部网关协议，以下策略将应用在路由判定上：

1）到达或来自自治网络 D 的包不能通过自治网络 B；

2）自治网络 E 不允许任何中转通信。

从安全角度出发，可以应用这些策略。因此，外部网关协议可能会在网络层提供一些安全。

5.1.4　多播、地域群播、任播和广播

最简单最常见的通信是发生在两个随机主机间，不过也有其他类型的通信模式，一个节点把一个包发送给多个节点，例如多播（Multicasting）。最普通的多播

方法是为每一个目标节点生成单独的副本，并分别发送它们。这也是成本最高的方法。虽然目的地不同，但是源节点和目标节点之间的路由可能遵循到达某个路由器的相同路径。因此，为沿着同一个路径的包发送一个单副本，比通过这些路径发送多个副本，性价比更高。尽管这是一个挑战性的问题，Obraczka（1998）文献中已有解决方案。

多播的最基本方式是在一个源节点和一个随机目标节点集之间。当目标节点代表一个区域里的所有节点，这个区域能在地理上描述时，这被称为地域群播（Geocasting）。例如，地域性多播的地址可能是下面其中的一项：

1）在层 A 或在房间 B 的节点；

2）在城市 Q 或国家 R 的节点；

3）在坐标 X 和 Y 之间区域的节点。

有时，同一个包能被发送到许多目标节点，但是如果此包只被其中一个节点收到就足够，则这被称为任播（Anycasting）。

最后，一个广播（Broadcast）包发送到网络中其他每一个节点。多播和广播引入了额外的安全弱点，因为一个多播包或一个广播包被窃听的概率比将一个包发送给单一目标节点被窃听的概率更高。

5.1.5 移动 IP

IP 不是为了移动网络设计的。它是以路由器上可用的路由信息为基础的。在 IP 里，当一个主机变换位置时，位置的改变也意味着通向它的路由也要改变，在这些改变路由上的路由器的路由表也必须更新。移动设备可以在各大洲游历。因此，一些移动性模式可能需要更新因特网的所有路由器。结果，移动性对 IP 是很耗费成本的，设计移动 IP（见图 5-8）主要是为了解决这个挑战。

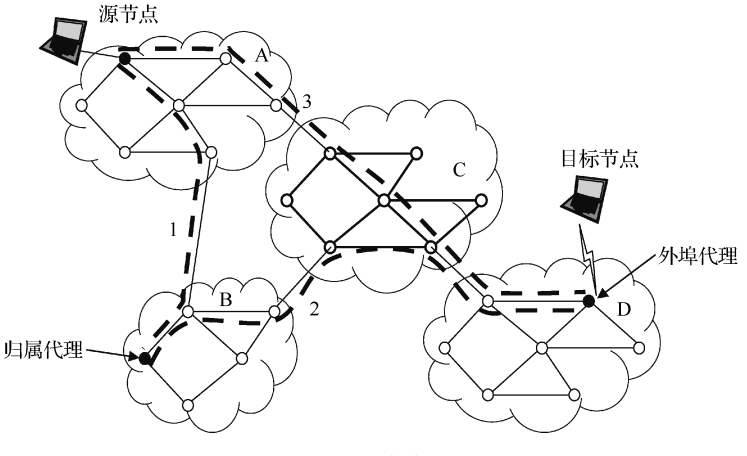


图 5-8 移动 IP

移动 IP 的两个重要成分是归属代理（Home Agents）和外埠代理（Foreign Agents）。每一个移动主机有一个归属代理和由归属代理分配的 IP 地址。除了归属代理，外埠代理分配一个临时 IP 地址来访问移动主机，这个临时 IP 地址称为转交地址（Care-of-addresses）。为此，外埠代理发布它们服务的“代理公告”。当一个移动主机漫游出本地网络时，它首先等待这些“代理公告”，当它接到一个公告时，会向外埠代理发送一个注册请求。收到该请求的外埠代理分配一个转交地址给拜访主机，并将分配的转交地址通知到拜访主机的归属代理。还有一种情况，不能收到任何“代理通告”的拜访节点将发送一个“hello”包，来寻找一个外埠代理。分配转交地址称为“绑定”，它需要定期更新。否则，“绑定”将会取消。因此，访问后没有撤销访问登记的拜访者并不无谓地阻碍一个地址。

如果一个主机把一个包发送给漫游主机，这个包传到归属代理，如图 5-8 步骤 1 所示。归属代理把这个包传给移动主机的转交地址，如步骤 2 所示。然后，两个节点的连接通过直达转交地址的路由维持。

这种方案引入了额外的安全挑战。首先，敌手可能会用假身份标识尝试接入外埠代理，这样就可以接收到发送给另一个节点的包。通过在注册访问节点之前认证该节点可以解决此问题。其次，一个恶意节点可能发送通告，让在它附近的移动主机都在此节点注册。恶意节点的另一种攻击形式是，它冒充外埠代理，但这次它把错误的绑定信息发给归属代理，让它们发送其他的包到恶意节点，例如或者发送给它自己，或者发送给其他恶意节点。无例外地，一个新能力总会带来敌手可利用的新的安全弱点。

5.2 无线自组织网络路由

移动 IP 不能满足无线自组织网络的路由要求，因为在无线自组织网络中不只是主机还有主干网都是移动的，并允许许多链路组成的有不同服务质量（QoS）的多跳无线连接。因此，需要更多的自适应网络层协议。当设计一个自组织网络路由算法时，可以采用主动（Proactive）或响应（Reactive）的方法。

主动方法，经常也被称为表驱动法（Table-Driven Approach），由像 RIP、OSPF、IS－IS 和 BGP 这样的因特网路由算法使用。在这些算法中，路由器维护一致的、最新的路由信息给网内的其他节点。当拓扑结构改变时，路由表就会被更新。以下是主动自组织路由协议的范例（Haas and Liang，1999；Royer and Toh，1999）：

1）目的序列距离矢量路由协议；

2）簇头网关交换路由；

3）无线路由。

在响应技术（也称为按需技术）中，拓扑维护即维护每个路由器上最新的拓

扑信息，不是连续的而是按需的。当一个新包需要传递，但没有一个有效路径可用于完成这个传送时，就要发现一个新路由。响应技术的范例如下：

1）泛洪（Flooding）；

2）自组织按需距离矢量路由（Ad hoc On-demand Distance Vector routing，AODV）协议；

3）动态源路由（Dynamic Source Routing，DSR）协议；

4）临时秩序路由（Temporarily Ordered Routing，TOR）协议；

5）基于关联的路由协议；

6）信号稳定性路由协议。

在主动方法中，一个路由在它被使用之前，没有必要更新许多次。另一方面，每次需要路由时发现路由的成本，可能比持续维护网络最新、一致的视图的成本要高。这取决于流量生成和拓扑改变的比率。对于当代无线自组织网络应用，优选像AODV 和 DSR 这样的响应技术。

5.2.1 泛洪和 gossiping 协议

在泛洪协议中，每一个收到包的节点通过广播重复发送，除非达到了包的最大跳数或者包的目标节点是这个节点本身。泛洪是一个响应技术，不需要为保持网络拓扑信息和实现复杂的路由发现算法而消耗计算资源。然而，它有如下一些缺点：

1）信息爆炸（Implosion）问题——这种情况是多个副本消息会发送到同一个节点。例如，如果节点 A 有 n 个邻居，这 n 个邻居节点同时也是节点 B 的邻居，则节点 B 会收到节点 A 发送的 n 份相同的包。

2）泛洪协议不考虑节点或链路上的可利用资源。例如，“资源盲点”。

泛洪的改进方法是 gossiping，节点不会给它的每一个邻居节点广播新收到的包，而是会把包发给随机选择的一个邻居节点。一旦某个邻居节点收到数据，它就会随机再选一个节点发送出去。虽然这个方法在任意节点只有一个包的副本，这样可以避免信息爆炸问题，但是传播消息给所有节点会花费很长时间。

5.2.2 自组织按需距离矢量路由（AODV）

AODV 是一种按需自组织路由方案，使距离矢量算法适合在移动主骨干网络上运行。在 AODV 中，每个节点维护一个路由表，这个路由表中一个目标节点最多只有一个条目。每个条目包含一些字段如邻居节点，中继接收的数据包到一个特定节点，也有些字段比如挑选的路由的成本。这类似距离矢量算法。AODV 和距离矢量算法的不同在于路由表的维护机制。当一个节点收到一个包时，它首先检查它的路由表，来决定能到达包内目标节点的下一跳路由器。如果有一个目标节点的条目，包将直接被发送到下一跳路由器。否则，将会通过广播一个路由请求

（RREQ）包来发现新的路由。一个路由请求包包括以下字段：源地址、请求 id、目标地址、源序列号、目标地址序列号和跳数。源地址是路由请求发起者的地址。

当节点收到一个和之前路由请求包有相同源地址和请求 id 的路由请求时，它将丢弃这个包。否则，它将检查路由表里是否有目标地址的条目。如果有，将表内的目标地址序列号与路由请求的目标地址序列号做比较。如果路由器在其路由表内有一个到目标地址的路由，并且如果它不能通过此路由到达目标地址，它将增加目标地址序列号，并发送一个路由请求。因此，目标地址序列号表明一个路由的新鲜度。如果一个路由器在其表内有一个目标地址的条目，请求的序列号比表内目标地址的序列号小，这意味着路由器知道的路径比发送请求的路由器知道的路径要新。这种情况下，接收者会发送一个路由应答（RREP）。这个路由应答将通过收到请求的路由，发回源节点。

再一次，这个路由方案引入了新的安全挑战。一个恶意节点会对所有路由请求发送路由应答消息，并让其他节点发送它们的包给恶意节点。然后汇聚接收的包，把它们发送给另外的敌手或获得对包内容的未授权访问。

5.2.3 动态源路由

自组织网络中，另一个自形成和自愈的路由协议是动态源路由协议（DSR）。DSR 协议也是基于“路由发现”和“路由维护”机制的，是响应技术，这和 AODV 是相似的。另一方面，DSR 使用源路由，而不是依赖于路由器维护的路由表。

在 DSR 协议中，当一个节点有一个包，但它并不知道通往目标节点的路由时，它将发出一个“路由请求”包。当这个包在网络中转发时，它经过的所有节点都会被记录在包的报头中。知道到达目标节点路由的节点不会继续转发包，而是把此路由追加在包内已累积的路由信息中，再向源节点返回一个“路由应答”包。之后，源节点在它的“路由缓存”中维护已发现的路由，并通过使用源路由已发现的路径，把这些包传给目标节点，即源节点会把到达目标节点要访问的每一个路由器的地址记录在包的报头上。如果通过之前发现的路由失败，发现路由失败的节点将会生成一个“路由错误”消息，并将此消息发回源节点。错误的路由将从“路由缓存”中移除，并启动通向目标节点的新路由发现程序。

DSR 也引入了与 AODV 中相似的安全挑战。另一方面，源节点控制所有路由经过的节点，这对安全有利，因为源节点可以避免不可靠节点。

5.3 无线传感器网络和执行器网络路由

传统自组织网络和无线传感器网络有很大的不同，这些在第 2 章中有详细叙述。特别地，不同于传统自组织网络，传感器网络苛刻的能量限制和可扩展性要

求，在为自组织网络设计的路由算法如 AODV 和 DSR 中难以满足。因此，人们专门为无线传感器网络和执行器网络设计了许多路由算法。

我们可以把传感器网络的路由算法分成以数据为中心的、基于聚类的或基于位置的算法。以数据为中心的算法是基于数据的特性的。像定向扩散、基于信息协商的传感器协议（Sensor Protocols for Information via Negotiation，SPIN）和能量感知多对多路由协议可以归于此类。低功耗自适应聚簇分层（Low-Energy Adaptive Clustering Hierarchy，LEACH）算法是基于聚类的传感器网络路由算法的一个例子。最小能量通信网（Minimum Energy Communication Network，MECN）和地理自适应保真路由协议（Geographic Adaptive Fidelity，GAF）是基于位置的路由算法。

5.3.1 定向扩散

在定向扩散（Directed Diffusion）（Intanagonwiwat et al.，2000）中，数据采集节点称为汇聚节点（Sink），它发送描述任务的兴趣消息给所有传感器，如图 5-9a 所示。任务描述符是通过分配描述任务的属性/值对来命名的。每个传感器节点把兴趣条目存在它的缓存里。兴趣条目包括一个时间戳字段和一些梯度字段。当兴趣消息在传感器网络中传播时，从源节点回到汇聚节点的梯度将被建立。当源节点有兴趣消息的数据时，源节点会沿着兴趣消息的梯度路径发送数据，如图 5-9b 所示。兴趣消息和数据的传播、聚合由局部决定。同样，当汇聚节点开始从源节点接收数

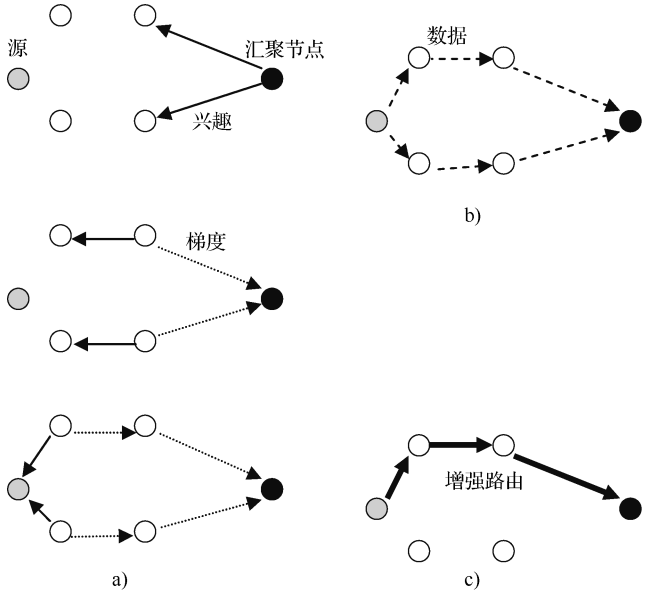


图 5-9 定向扩散

a）兴趣消息的传播 b）数据传播 c）路由增强

据时，它必须刷新兴趣消息并增强一条路径。当一条路径被汇聚节点增强时，源节点开始只沿增强路径发送数据包，而不是通过所有可用的梯度路径。注意定向扩散是以数据为中心的路由算法，其中汇聚节点广播兴趣消息。

5.3.2　基于信息协商的传感器协议（SPIN）

SPIN 是一个自适应协议族，它是基于这样的思想：只发送描述传感器的数据而不是发送整个数据会使传感器节点操作更有效，并能节约能量，除非明确请求整个数据（Heinzelman et al.，1999）。SPIN 有三种类型的消息：ADV、REQ 和 DATA。在发送 DATA 消息之前，传感器先广播包含一个 DATA 描述符（例如元数据）的 ADV 消息。如果一个邻居节点对该数据有兴趣，它将发送一个 REQ 消息来请求 DATA，然后 DATA 被发送到这个邻居传感器节点上。然后，邻居传感器节点重复这一过程，如图 5-10 所示。结果，对数据有兴趣的节点将收到一个副本。

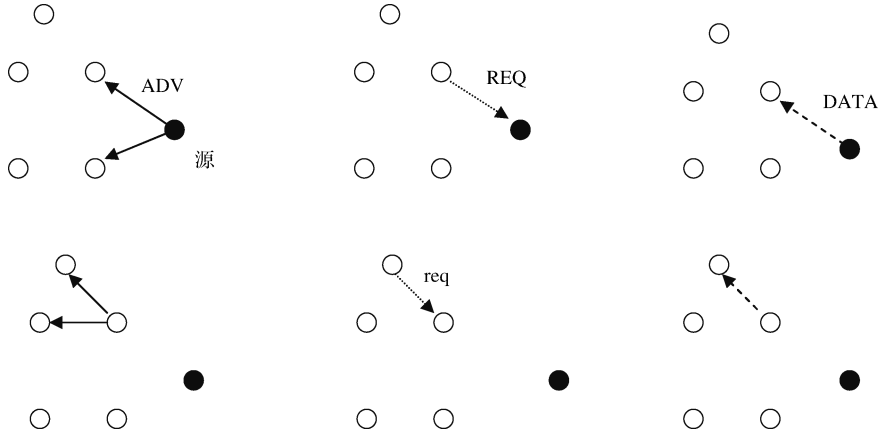


图 5-10　SPIN

5.3.3　低功耗自适应聚簇分层（LEACH）路由协议

LEACH 是一个基于聚类的路由协议，它能最小化传感器网络里的能量损耗（Heinzelman et al.，2000）。LEACH 的目的是随机选择传感器节点作为簇头，这样与基站通信时的高能量消耗就分散到了传感器网络的所有传感器节点上。执行 LEACH 分成两个阶段：建立阶段和稳定阶段。为了使负载最小化，稳定阶段持续的时间要比建立阶段持续的时间长。

在建立阶段，一个传感器节点 n 在 0 和 1 之间选择一个随机数。如果随机数比预设的门限值 t 要小，传感器节点就成为一个簇头。门限值 t 计算如下：

$$t=\begin{cases}\dfrac{P}{1-P[r\bmod 1/P]} & ,若\ n\in G\\ 0 & ,其他\end{cases} \tag{5-1}$$

式中，P 是变成簇头的期望比率；r 是当前的轮数；G 是在之前 $1/P$ 轮没有被选中作为簇头的节点集合。在一个节点自己选作簇头之后，它将通告所有的邻居节点。传感器节点收到通告后，它们根据来自簇头的通告的信号强度，决定希望归属的簇头。然后，传感器节点通知它们的簇头，它们将成为簇的成员。簇头将分配给每一个传感器节点一个时段，在这个时段内，它们可以发送数据给簇头。

在稳定阶段，传感器节点能开始感知和发送数据给簇头。簇头在把数据发送给基站之前，簇头也会聚合来自它们簇的节点的数据。在稳定阶段过一段时间后，网络再次进入建立阶段。

5.3.4 功耗感知多对多路由（PAMR）协议

PAMR（Cayirci et al.，2005）是为了传感器和执行器网络设计的，在该网络中，传感器把它们的数据直接发给感兴趣的执行器，在选择路由时，会考虑到能量和延迟。在 PAMR，执行器通过广播一个注册消息，在传感器网络中的节点注册兴趣数据。一个注册消息包括节点标识字段（node_id）、执行器标识字段（actuator_id）、等级字段（echelon）、最小可用能量字段（minPA）、全部可用能量字段（totalPA）以及任务字段。node_id 是发送节点的身份标识。当执行器广播一个注册消息时，它用自己的 id 初始化 node_id 字段，重发此消息的节点也会更新此字段。每个重发注册消息的节点用它们自己的 id 替换 node_id。echelon 表示从一个执行器到一个节点需要的最小跳数。totalPA 是把路由上每个节点的可用能量加起来得到的。minPA 是在路由上，有最少能量节点的可用能量值。转发注册消息的节点会把它的可用能量（ownPA）加到 totalPA 上。如果 ownPA 低于 minPA 值，它也会用节点自己的 ownPA 替换掉 minPA 字段。在发送注册消息之前，执行器会把 echelon 和 totalPA 初始化为 0，把 minPA 的值设为 PA 的最大可能值。

传感器节点不会重发已经接收到的所有注册消息。它们首先检查这是否是一个新路由的注册消息。满足以下标准之一的路由即为新路由：

1）在注册消息中，注册表没有执行器的任何条目；

2）注册表至少有一个执行器条目，但执行器的条目都不是来自注册消息的上行链路节点；

3）注册表有一个注册消息中执行器和上行链路节点条目。

然而，消息中至少有一项任务不是在相关注册表条目指明的。

如果这不是新路由的注册消息，它将被检查是否是一个基于 echelon、minPA 和 totalPA 字段的更好的路由。为此，将使用一个由下式表示的参数化的选择函数：

假定有一个传感器节点 s，$N=\{n_1, n_2, \ldots, n_n\}$是 s 的路由表上的上行链路节点的集合。选择函数的一般公式如下：

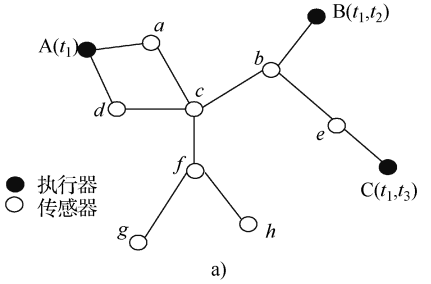
$$f_i=(w_1\times\alpha_i)+(w_2\times\beta_i)+(w_3\times\phi_i) \tag{5-2}$$

式中，w_1、w_2、w_3 是加权参数，满足 $w_1+w_2+w_3=1$，$0\leqslant w_1$、w_2、$w_3\leqslant 1$，且

$$\alpha_i=\frac{\sum_{k=1}^{n}e_k-e_i}{\sum_{k=1}^{n}e_k}\quad \beta_i=\frac{m_i}{\sum_{k=1}^{n}m_k}\quad \phi_i=\frac{t_i}{\sum_{k=1}^{n}t_k} \tag{5-3}$$

式中，e_i 是上行链路节点 i 的等级；m_i 是通过上行链路节点 i 的路由上最小可用能量值；t_i 是经过上行链路节点 i 的路由上可用的总能量值。计算完所有邻居节点的 f 值之后，有最大 f 值的节点会被选出来作为上行链路节点，把新收到的数据包发送到指定执行器上。

当一个注册消息在网络中传播时，节点要维护两个表：注册表和路由表。图 5-11 给出了注册表和路由表的例子。一个节点的注册表是执行器的列表，这些执行器已经在网络中至少注册了一个任务。路由表列出的是每个任务的最佳上行链路节点和注册表中可用的执行器对。当收到一个新的感知数据时，将为上行节点（例如下一跳）检查该表。数据包将被转发给此任务（比如传感器类型）的每一个上行节点。相同类型的感知数据将转发给多个节点。因此，在路由表中有对同一个任务的多个记录。然而，每一个单独的上行链路节点和感知任务对只有一个记录。



a)

执行器标识	上行链路标识	等级	min PA	total PA	任务(s)
A	*a*	2	5	5	t_1
A	*d*	2	4	4	t_1
B	*b*	2	7	7	t_1,t_2
C	*b*	3	3	10	t_1,t_3

b)

任务(s)	上行链路节点标识
t_1	*a*
t_1	*b*
t_2	*b*
t_3	*b*

c)

图 5-11　传感器网络和执行器网络范例

a）拓扑结构范例　b）节点 c 的注册表　c）节点 c 的路由表

5.4 复习题

5.1 假设图5-6a中的每个节点有一个完美的路由表。然后，节点 d 崩溃，节点 e 发现了这个状况。如果使用距离矢量算法，节点以 b、e、a、b、e、a 的顺序报告它们的路由表时，跟踪节点 b 和 e 的路由表会发生什么样变化？

5.2 链路状态算法和距离矢量算法有什么不同？请举出应用在因特网的链路状态算法的两个实例。

5.3 为什么我们要把因特网上的路由算法分为内部网关协议和外部网关协议？为什么我们需要外部网关协议？详细说明基于安全考虑的内部网关协议和外部网关协议。

5.4 为什么当节点是移动时，IP不能满足要求？

5.5 如果移动节点离开外部LAN，而没有在移动IP注销时，会发生什么？

5.6 移动IP带来的安全弱点是什么？如何应对这些弱点？

5.7 为什么移动IP不能满足无线自组织网络的要求？

5.8 AODV和DSR协议有什么不同？哪一个有更少的安全弱点？

5.9 当节点是移动的，比较定向扩散、LEACH和PAMR。

第 6 章　可靠性、流和拥塞控制

在 OSI 中，可靠性和流控制是数据链路层和传输层的任务。第 4 章介绍的纠错/检错方案用于保证通过数据链路层的链路传输中的可靠性。传输层提供可靠性，也提供基于端到端的流和拥塞控制。本章详细解释无线自组织网络传输层相关的挑战和解决方案。

6.1　可靠性

传输层的可靠性方案通常基于中继（Retransmission）。数据片段由源节点重发，或有时由中间节点（有以前没有发送成功的数据片段）重发。要做到这点，主要有两个挑战：

1）检测一个数据片段没有被成功发送，例如数据片段在传输中丢失或混乱；

2）初始化数据片段中继。

可由源节点或目的节点检测一次失败的传送。若接收数据的节点总是给出成功传送的应答，称为正应答（Positive Acknowledgement）。使用正应答方案时，若源节点没接收到传输片段的应答，说明数据片段没有传送成功，或者应答信息丢失。在这类方案中，源节点担负探测的责任。对应地，负应答（Negative Acknowledgement）方案中，目的节点可以报告一次失败的信息传送。

若数据片段顺序传送，每一片段赋予一个序列号，通过对最后一个片段序列号的应答，目的节点可以对包括最后收到的多个片段产生应答。因特网传输控制协议（TCP）基于多个片段的正向应答，以满足端到端可靠性。

满足端到端可靠性的 TCP 方法也可用到无线自组织网络和 Mesh 网络。然而，由于传感器网络有严格的功耗约束和大量的单跳，源节点片断应答和对每一丢失片段的重传代价太高。传感器网络的流量模式是一对多、多对一和多对多。这也有别于因特网和传统的自组织网络。另外，传感器网络的最终目标是感知利益相关事件。因为传感器节点的感知范围通常会重叠，所以相同的事件往往会被多个传感器节点报告。事件的成功通知对传感器网络很重要。数据包丢失可以容忍，除非它阻碍事件的通知。为克服这些差异，无线传感器网络需要其他端到端可靠的方案。

可靠多片段传输方案（Reliable Multisegment Transport，RMST）（Stann and Wagner，2003）为定向传播提供端到端可靠的数据包传输。RMST 是选择性负应答（Selective Negative Acknowledgement，NACK）协议，有两种模式：缓存模式（Caching

Mode）和非缓存模式（Noncaching Mode）。缓存模式中，许多节点沿着一条增强路径，例如定向传播协议用于传输数据到汇聚节点的路径，被赋给 RMST 节点。每个 RMST 节点缓存数据流片段，并为每个数据流维护看门狗定时器（Watchdog Timer）。若定时器到时而数据片段没收到，一个负应答会沿增强路径回溯方向发出。拥有路径中丢失片段的第一个 RMST 节点重传片段。汇聚节点担当最后一个 RMST 节点，在非缓存模式下变成唯一的 RMST 节点。

缓发快取（Pump Slowly，Fetch Quickly，PSFQ）方案（Wan et al.，2003）与 RMST 方案（Stann and Wagner，2003）相似。PSFQ 方案包括三个功能：消息转播（Pump 操作）、转播发起的错误纠正（Fetch 操作）和选择性状态报告（Report 操作）。PSFQ 方案中每个中间节点维护一个数据缓存。收到数据包的节点，与本地缓存对照检查包的内容，丢弃任一重复的数据包。若收到的数据包是新的，包中的 TTL 字段值递减。若递减后 TTL 字段值大于 0，而且包序列号之间没有间隔，则数据包被安排转发。数据包会在随机时间 $T_{\min}$ 到 $T_{\max}$ 之间延迟，然后转播。一旦探测到序列号有间隔，节点会转到 fetch 模式。fetch 模式下的节点请求从邻居节点重传丢失的数据包。

PSFQ 和 RMST 方案设计用于增强端到端数据包传输的可靠性。事件到汇聚节点的可靠传输（Event-to-Sink Reliable Transport，ESRT）协议（Sankarasubramaniam et al.，2003）是主要考虑无线传感器网络中端到端可靠事件传输的传输层协议。ESRT 协议中，不能确保可靠的事件传输，但通过控制传感器节点事件报告频率，增强可靠性。

在可靠事件传输方法中，事件定义为传感器节点生成的关键数据（Tezcan et al.，2004）。端到端可靠事件传输（End-to-End Reliable Event Transfer，EERET）方案设计用于传输这些关键数据包。大多数情况下，因为传感器网络中节点通常是密集分布的，不止一个传感器节点生成相同的关键数据，因而一个事件可被多个节点检测到。当至少一个报告事件的数据包被汇聚节点接收到时，事件成功传输给收集节点（cnode）。例如，图 6-1 中的节点 a、b、c 和 d 检测相同的事件。既然四个节点都能生成报告此事件的数据包，即使汇聚节点只接收到其中一个数据包，端到端的事件传输仍可以成功。

EERET 方案可分成两类：基于非应答（Non-acknowledgement based，NoACK）的方案和基于应答（Acknowledgement based，ACK）的方案。三种方法，即事件报告频率、节点密度和隐式应答可作为基于 NoACK 方案的例子。对于第二类，另外三种方案如选择性应答、强制应答和覆盖应答（Blanket Acknowledgement）可作为例子。

下面两节阐述基于 NoACK 和 ACK 的方案。基于 NoACK 的方案是不需要等待端到端应答，增强可靠性的可选方法集。相对照的，基于 ACK 的方案使用应答，

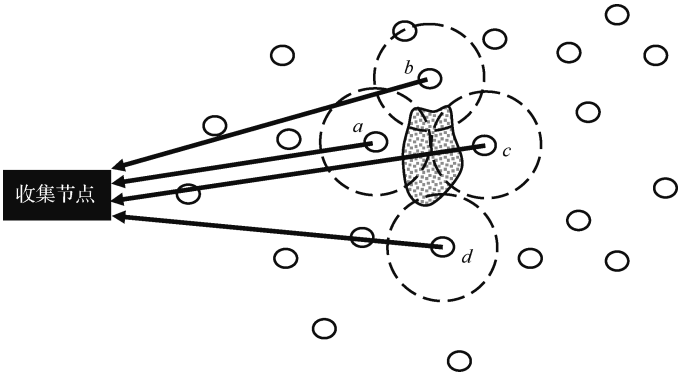


图 6-1　端到端可靠事件传输

但不是像在面向连接的端到端协议中那样使用。通过不同方式使用应答来提供可靠性。

6.1.1　基于非应答的方案

本节将考察传感器节点不等待端到端应答的各种方案。

6.1.1.1　隐式应答

隐式应答是传感器网络中可靠事件传输的一种方法，利用了无线信道的广播特征。当传感器节点发送一个数据包时，它通过梯度（Gradient）重复发送。这意味着下一个节点对数据包的成功接收。因为并不需要一个单独的应答包，所以其额外负载只是对媒介进行一定时间段的侦听。有读者会说这不是端到端的方案，而是逐跳（Hop-by-Hop）技术。这种观点是正确的。然而，这种技术增加了端到端的可靠事件传输率。

6.1.1.2　事件报告频率

这种方案在 ESRT 协议中使用（Sankarasubramaniam et al.，2003），它是基于 event-to-cnode 可靠模型的。事件传输可靠性级别由提高或降低事件报告频率控制。提高报告频率，传感器节点发送的数据包数增加。这减少了被报告事件丢失的概率。然而，这也导致额外的能量损耗。

另外需注意，报告频率可以增加到某一特定点。超过这一点，可靠性将下降。这是因为网络不能处理持续增加的数据包注入，以及由于网络拥塞导致的数据包丢失。方案的细节可参见 Sankarasubramaniam 等（2003）文献。

6.1.1.3　节点密度

在传感器网络中，通常有多个节点有重叠的感知区域。因此，多个节点有可能协作检测相同的事件。报告相同事件的节点数会对端到端事件传输可靠性产生影响。由于通过网络管理协议管理关键区域传感器节点数或参与报告事件的节点数，

端到端可靠事件传输率也可以控制。通过增加参与感知任务的节点数，达到更高的端到端可靠事件传输率。任务集概念（Cayirci et al.，2006a）可用来管理参与感知任务的节点数。

6.1.2 基于应答的方案

尽管应答机制是实现端到端可靠性的传统方式，但由于以下原因，它对许多传感器网络应用可能并不可行：

1）大多数无线传感器网络应用有严格的能量限制，因此应答数据包的负载可能并不合理；

2）因为一些数据包可能并不像其他包那样重要，为所有收到的数据包生成应答会产生不必要的代价；

3）因为许多传感器节点会汇报同一个事件，对它们产生一个单一的应答可能更有效。

在 Tezcan 等（2004）文献里介绍了更多适当的传感器网络应答方案。

6.1.2.1 选择性应答

因为无线传感器网络包含大量密集分布的传感器节点，所以对每个数据包等待应答并不合适。可替代的办法是，当传感器节点检测到关键数据时，节点可以激活应答机制。有许多方法可判断一个数据包是否携带关键数据。一种方法是使用门限值。传感器节点和汇聚节点在部署取决于应用的门限值之前达成一致。然后，传感器节点通过与协定的门限值比较，判断测量值是否是关键数据。例如，温度传感器会定期报告温度。除非报告的温度变化超过了门限值，否则可认为报告的数据是非关键数据。当观察到超过门限值的温度变化时，则认为是关键数据。其他情况，通过插入可以获得丢失的数据。

仅当关键数据被报告，传感器节点等待应答。汇聚节点对收到的每个数据包与门限值比较，并按关键和非关键数据分类。当收到关键数据包时，汇聚节点立即给传感器节点发送一个应答包。若在预定的超时期内，传感器节点没收到对包含关键数据的包的应答，则重传数据包。

6.1.2.2 强制应答

强制应答的基本思想和选择性应答几乎相同，差别在于汇聚节点不计算收到的数据包是否携带关键数据。相反，传感器节点在发送数据包之前进行这种计算，若包含临界数据，则标记数据包。汇聚节点收到标记有携带关键数据的包后，传回应答。

6.1.2.3 覆盖式应答

报告同一事件的多个传感器节点可能会由单一的应答包应答。一个单个的应答包可以向所有传感器节点广播，报告同一个事件。例如，覆盖式应答（Blanket Ac-

knowledgement）方案可用于传感器网络救灾行动应用中，传感器节点负责报告陷于瓦砾下的人员信息。当汇聚节点确认收到瓦砾下人员的存在信息时，传感器节点不必担心它们特定的报告是否被应答（Cayirci and Coplu，in press）。覆盖式应答也可以与选择性应答和强制性应答共同使用，以广播应答包。

6.2　流和拥塞控制

根据接收方能处理的速度，流控制调整源节点数据包生成的速度。若进入数据的速率高于接收方能处理的速率，接收方开始丢包。这是一种资源浪费。另一方面，尽管有数据待传送以及网络可以更高的速率传送数据，若源节点发送数据包的速率低于接收方能接收的速率，这也是一种资源浪费。流控制这两种情况都不会发生。

若来自多源的数据聚集在一个链路中，聚合通信量高于链路的容量，则发生拥塞。换言之，在一定时间周期内，当流生成速率高于网络所能传输的速率，拥塞产生。拥塞控制方案旨在预防这种情况。传输层负责处理端到端的拥塞控制和流控制相关的挑战。例如，因特网 TCP 负责拥塞控制。

为控制拥塞和流，TCP 运行一个称为 slow start（慢开始）的算法，算法基于三个参数：接收者窗口、拥塞窗口和避免拥塞的门限。接收者窗口通过接收者通知流控制，并指示接收者能接收的最大的千字节单位的容量。拥塞窗口是用来避免拥塞，且是由源节点决定的。这两个窗口的最小值是源节点某时发送，然后等待应答的最大值。

当一个 TCP 连接建立时，拥塞窗口等于一个分段，这意味着源节点发送了一个分段。分段的大小（千字节）等于连接允许的最大分段大小。如果这个分段在超时期满之前得到应答，那么拥塞窗口变成两个，且源节点发送两个分段。拥塞窗口的大小在每次传输时与上次成功传输相比翻一倍，直到达到接收者窗口大小或者门限。如果门限在接收者窗口之前达到，拥塞窗口增加的大小变成线性的，即在每次成功传输后递增一个分段。门限在开始时是 64kbit。

如果超时发生，即传输分段在期望的超时内没有得到应答，TCP 假定这是由于拥塞造成的，并且减半门限，重新开始慢开始程序，如图 6-2 的例子中所示。在这个例子中，最大分段尺寸为 1kbit。源节点在第一次传输时发送一个段。当它收到应答时，它就发送两段。这种分段数量上的指数增长一直持续，直到到达接收者窗口大小为止（我们的例子中是 56kbit）。当源节点发送 56 个分段（等于接收者窗口大小）时，由于拥塞，超时发生。源节点将当前窗口大小减半来确定新的门限，即把它设置成 28kbit，并且通过设置拥塞窗口为 1kbit 来重新开始慢开始。这次在接收者窗口大小之前达到门限值。在门限以后，拥塞窗口在每次传输成功后逐分段递增。在到达接收者窗口大小之前，当前窗口大小为 34kbit 时，另一个超时发生。

源节点将门限设置成 17kbit，然后再运行慢开始程序。

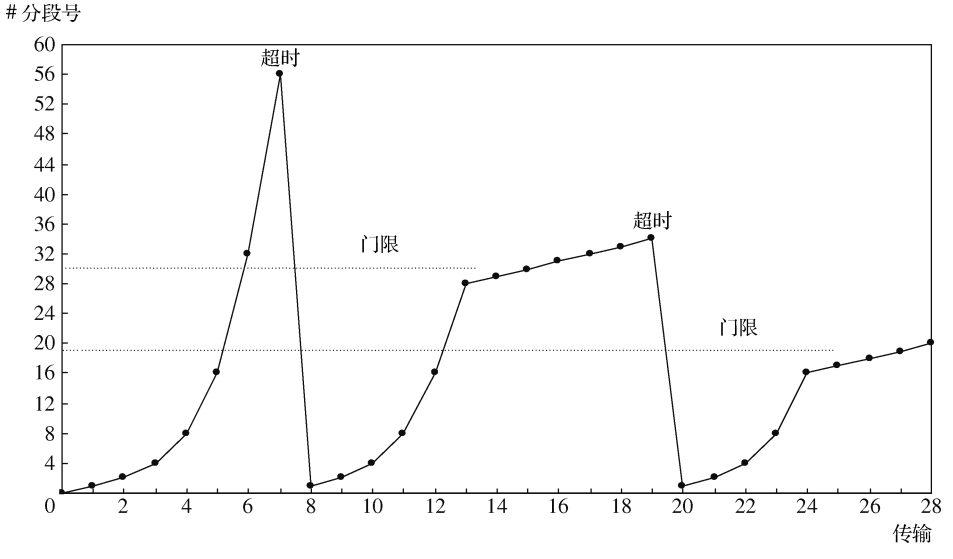


图 6-2　TCP 中的拥塞控制和流控制

TCP 拥塞和流控制机制有以下作用，使它们与无线自组织网络不相容：

1）TCP 假设通信链路是十分可靠的，因此一个分段由于拥塞丢失的概率是很高的。这种假设对于无线自组织网络是不现实的，在自组织网络中，由于节点移动和节点/连接故障，拓扑改变和分段丢失是很频繁的。

2）TCP 假设连接的平均端到端延迟是合理的，因此由于慢开始没被利用的带宽是可忽略的。这也可能与一些无线自组织网络的特性产生冲突。例如，一个在无线传感器网络的连接可能经过很多次无线跳转，使得端到端延迟对 TCP 来说太长。同样，声信号以声速传播，这可能对时延（Latency）产生影响，使 TCP 对于水下声纳自组织网络来说不切实际。

3）在慢开始时未充分利用的连接成本可能对于受限网络（Tethered Network）来说是正当的。但是，无线连接的成本比受限连接要高许多，因此它们需要被更加仔细地利用。

由于这些原因，TCP 的替代版本如 TCP-Reno、TCP-Peach 和 I-TCP 已经被开发出来，它们更适合无线网络。这些 TCP 的最新版本总体上基于以下技术：

1）负应答：在 TCP 中，接收者通过发送一个对最后接收分段的正应答来确认多个分段。没有改变这个基础方案，对一个没接收到的分段的负应答仍然可以通过多次确认丢失分段来实现。当源节点接收到对于同一个分段的多个应答，即三个应答时，这表明接收者没有接收到特定的段，然后源节点立即重新发送这个段。

2）快开始：在 TCP 连接建立之后，源节点发送一个数据段和哑分段（Dummy

Segments）来填充接收窗口。当接收者确认最后一个接收段时，源节点知道了第一轮的网络容量，并相应地调节它的速度。这急剧提高了高时延的通信连接的利用率。

3）分裂：一个连接被分裂成多段，这些段使用不同的传输层协议。例如，一个连接可能包括光纤和无线连接。当 TCP 运行在连接的光纤部分时，在无线部分可能使用另一个传输层协议。这解决了很多问题，但是需要去复用（Demultiplexing）和在一个中间节点的向上到传输层的分段封装。尽管负应答、快开始和分裂技术也许可以满足许多无线网络的需求，但它们不能完全解决无线自组织网络的一些限制，例如功耗和可扩展性。这对于无线传感器网络来说，尤其是这样，其数据生成率在时间上和空间上都是相关的，这增加了拥塞的可能性。

与拥塞控制有关的两个挑战是值得注意的，且需要对无线传感器网络进一步关注：拥塞检测和解决拥塞（Karl and Willig, 2005）。缓冲区或通道统计可用来拥塞检测。如果一个中间节点的缓冲区的占用水平超过一定程度，缓冲区充满水平就会趋于增加，这可以是拥塞的好指标。另外，连接可以在一定时期多次采样。如果链路繁忙的次数和采样总数的比值超过门限值，也可能表示拥塞。

为了解决拥塞，要么减少流量生成率，要么丢掉较不重要的包。在速率控制选项中，检测拥塞的节点可以通知之前的节点减少它们发送的包的数量。如果这导致了在之前节点的拥塞，它们也通知它们的梯度（Gradients）。这可能持续到源节点。在丢包选项中，源节点根据包的重要性给它们贴标签，且检测拥塞的节点丢掉较不重要的包直到拥塞消失。这两种技术都能激发进一步的拒绝服务攻击。例如，一个恶意节点可能发送错误的拥塞报告给它的邻居。

6.3　复习题

6.1　传统的端到端可靠性概念和可靠的端到端事件传输的主要区别是什么？

6.2　强制应答（Enforced Acknowledgement）与选择性应答相比，其优势和劣势是什么？

6.3　一个 TCP 连接通过在声纳水下自组织网络中的 10 个无线跳转建立。假设每跳平均 100m，声纳信号每秒传播 1500m，在一个连接中每秒可以发送 10kbit 的数据，源节点有 1MB 数据要发送，接收窗口的大小是 64kbit，最大的分段尺寸为 1kbit，且在每个节点路由选择的平均处理延迟为 1ms。假设以下分段没有到达目的地：67、112、137。如果没有其他通信通过它们，这个连接的平均连接利用率是多少？

6.4　缓冲区状态或连接统计对于指示拥塞是否更加可靠？讨论并且解释你的答案。

6.5　对于拥塞处理，与码率控制技术相比，包丢失策略的优势和劣势是什么？

第 7 章　其他挑战和安全因素

无线通信带来了影响各个层次网络协议和算法的更多挑战。这些额外的问题主要是由诸如移动性和扩展性等因素引起的。定位、时钟同步性、寻址、数据汇集和询问、覆盖范围、移动性和资源管理都是不受限通信（Untethered Communications）所面临的额外挑战，我们将在本章中回顾这些问题。

7.1　定位和位置

定位（Bulusu et al.，2000；Doherty et al.，2001；Savvides et al.，2001；Erdogan et al.，2003；Niculescu and Nath，2003；Patwari et al.，2003）是自组织网络特别是传感器网络中的一个关键问题，因为在很多应用程序中，传感数据如果没有和地理位置数据联系在一起将会变得几乎没有意义。此外，一些任务中也需要定位，例如节点的空间寻址以及地理位置路由。和其他很多与自组织网络相关的因素一样，应用程序所需要的定位精确度等级不尽相同。例如，在某个应用程序中，只需指出在哪个空间进行的测量就足够了。另一方面，在其他应用程序中，就可能会需要达到厘米数量级的精确度。

节点定位的第一选择就是全球定位系统（GPS）。然而，GPS 对于自组织网络来说并不总是可行的。节点可能放置在对来自卫星的信号用必需的强度也不能接收的地方。此外，在一些应用程序中，使用 GPS 组件来连接所有节点的开销将会很高。因此，间接技术非常重要，尤其是在传感器网络中（见图 7-1）。

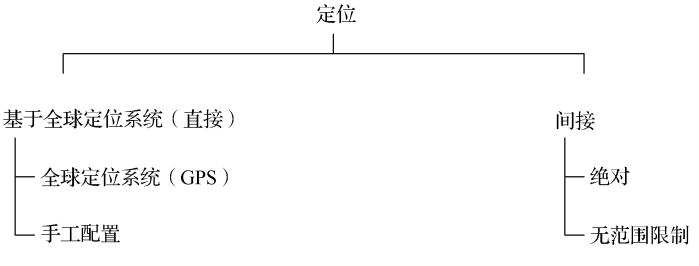


图 7-1　定位方案分类

间接技术可以是绝对的或者是无需测距的（Range-free）。绝对的技术（Absolute Technique）可以通过一个局部性或者一个全球性的参考坐标系给出节点的绝对位置。它们基本上都是基于三角测量（Triangulation）法、三边测量（Trilateration）

法或者多边测量（Multilateration）法（见图 7-2）。三角测量法是通过估计和信标节点之间的角度来实现的。当使用三角测量法时，从信标节点以估算的方向出发的直线的交点给出节点的位置，如图 7-2a 所示。三边测量法和多边测量法是基于到信标节点距离的。以相关信标节点为圆心、半径等于自身到信标节点距离的所有圆的交集就是节点的估计位置，如图 7-2b 和 7-2c 所示。

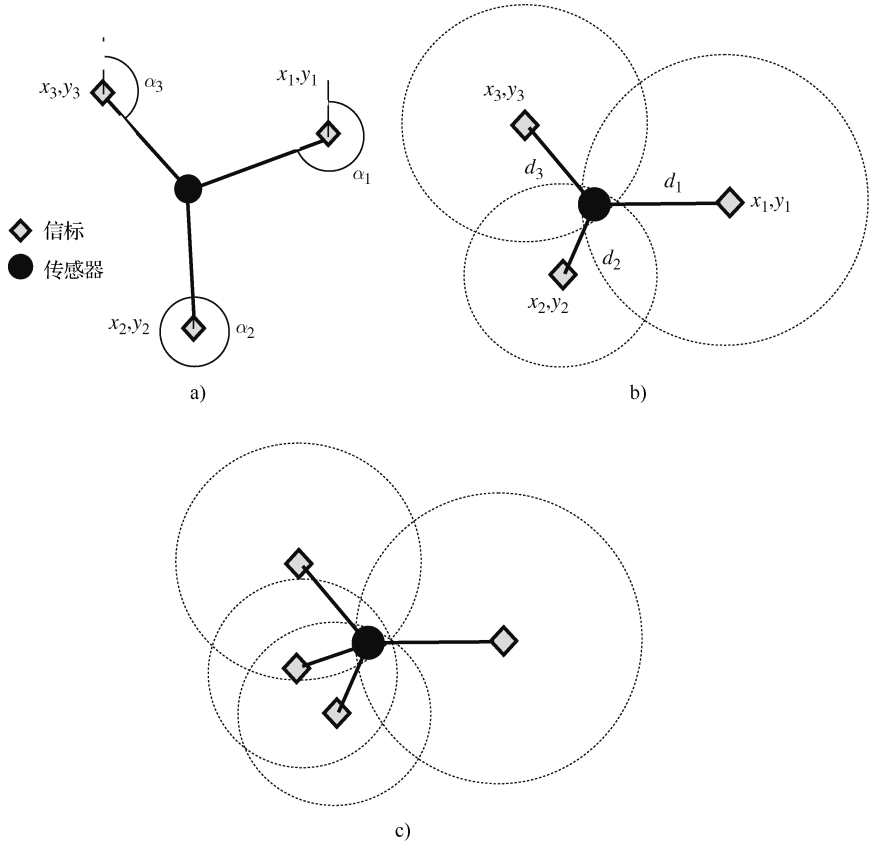


图 7-2　三角测量法、三边测量法和多边测量法

a）三角测量法　b）三边测量法　c）多边测量法

多边测量法中的基本观点是拥有至少 n 个方程来估算 n 个变量。例如，当三个信标节点的位置（x_i，y_i）和一个点到它们的距离（d_i）是已知的，那么就可以得到以下三个等式，足以找到点的坐标 x 和 y：

$$\begin{aligned}(x-x_1)^2+(y-y_1)^2&=d_1^2\\(x-x_2)^2+(y-y_2)^2&=d_2^2\\(x-x_3)^2+(y-y_3)^2&=d_3^2\end{aligned}\tag{7-1}$$

注意式（7-1）中假设信标节点的位置和节点到它们的距离确切知道。这可能不符合实际情况，因为在估计到信标节点的距离时可能会出现误差。防止这种误差的一种方法是最小均方估计（Minimum Mean Square Estimation，MMSE）法，它基于最小均方差 ε。例如，假设有 m 个信标节点，已知它们的位置（x_i，y_i），就可以估算到它们每个的距离 d_i。式（7-2）表示的最小均方差 ε 给出了估计位置（x，y）的方法。

$$\varepsilon = \frac{\sum_{i=1}^{m} \left(d_i - \sqrt{(x - x_i)^2 + (y - y_i)^2}\right)^2}{m} \tag{7-2}$$

到信标节点的距离可以通过以下技术之一估算出来：接收信号强度（Received Signal Strength，RSS）、到达时间（Time Of Arrival，TOA）或者到达时间差（Time Difference Of Arrival，TDOA）。用于估计信标节点方向的技术称为到达角度（Angle Of Arrival，AOA）。对所有这些技术既有支持也有反对。在 RSS 中，节点知道信标节点的位置以及它们传输信号的强度。之后，它将通过一个传播模型和接收到的信号强度来估算到信标节点的距离。结果可能会因为多路径影响以及其他损伤，例如阴影（Shadowing）、散射（Scattering）和非视距（Non Line-of-sight）条件，而不是非常精确的。

在 TOA 中，节点和信标节点是时钟同步的。它同时知道信标节点的位置和信号的传输时间。当节点同时知道了接收时间，那么通过信号的传播速度就可以很容易地计算出到达信标节点的距离。通过 TOA 获得的结果也会因为多路径影响和非视距条件而受到损害。另外，射频信号的传播速度对于大多数情况下仅限几米的节点距离的传感器网络来说过于快速。因此，在 TDOA 中，就用到了射频信号以及传播速度较低的超声波信号。尽管在同一时刻发射，超声波和射频信号会在不同时刻到达目的地。在知道这两种信号的传输速率差之后，通过它们到达时间的差值得到与源节点之间的距离。

AOA 技术需要使用特殊的天线配置。它也可能会因为无线媒介中的多径影响、非视距条件和其他损伤来源而不精确。

自组织网络中，进行节点定位计算的方法有三种：集中式、分布式和局部集中式（Locally Centralized）。在集中式方法中，所有节点的测量结果都会送到一个中央节点中。中央节点通过这些测量结果来确定这些节点的位置，然后发布结果信息。由于传感器节点拥有的计算能力和存储空间有限，这一方法对于一些传感器网络应用程序来说是可行的。另外，在一些应用程序中，传感器节点可能不需要定位信息，但是执行一些例如路由优化、最优传感器区域覆盖计算、空间数据聚合等任务的中央节点，可能会需要定位数据。而且，集中式方法在协作式多边测量中可能会表现得更好（下面将解释）。在分布式方式中，节点将会自己找到它们的位置。

局部集中式方法建立簇，每个簇的中央节点计算簇中所有节点的位置。

在协作式多边测量（Collaborative Multilateration）中，传感器节点在没有从足够数量的信标节点接收到信号时，会和其他的传感器节点合作进行定位。例如，从两个信标节点接收信号的两个传感器节点可以通过合作来容忍第三个信标节点没有信号，如图 7-3 所示。这里的基本想法依然是至少 n 个等式来估算 n 个变量。协作式多边测量的细节可以在 Savvides 等（2001）文献中找到。

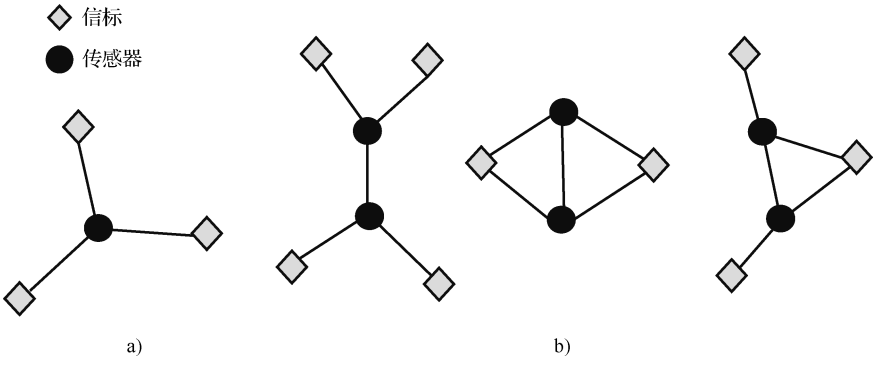


图 7-3　协作式多边测量

a）单跳多边测量　b）两跳协作式多边测量

间接技术也可以是无需测距的。两种无需测距技术的例子：sectoral sweepers（SS）（Erdogan et al. , 2003）和质心（Centroid）方案，如图 7-4 所示。虽然无需测距技术的分辨率通常不像这一节所讲到的其他技术那样高，但它们足够简单，可以在不需要节点附加任何额外硬件和软件组件的情况下实现。此外，它们的分辨率对于很多自组织网络和传感器网络应用程序来说已经足够高了。

SS 方案是基于使用定向天线的任务分发。每个任务与最小和最大的 RSS 值、唯一的任务标识相关联。当传感器节点报告一个任务时，任务标识就标志着一个特殊的区域，并通过天线的方向指出这一区域散布任务，以及为任务指定的最小和最大 RSS 值。注意这里任务区域的边界并不能很好地定义，而且并没有固定的形状，这

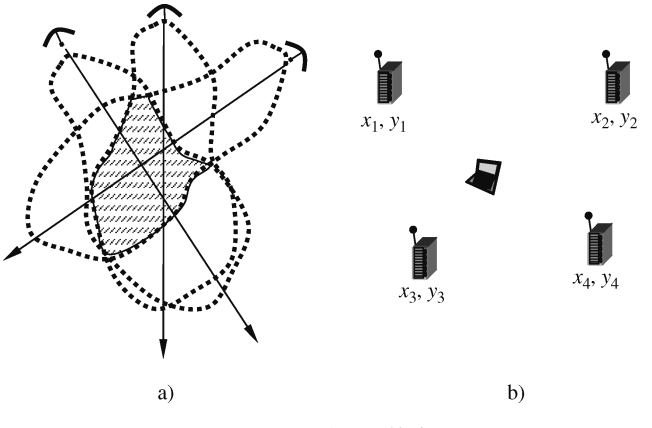


图 7-4　无需测距技术

a）sectoral sweepers　b）质心方案

是因为存在多路径及非视距的影响，如图 7-4a 所示。

为相同的任务创建重叠的任务区域可以提高 SS 方案的分辨率。当某个传感器节点发布多任务通告时，被报告的任务区域的重叠部分是节点的所在位置。重叠区域要比任务区域小。因此，可以实现更高分辨率的位置估计。

在质心技术中，节点要计算锚点（Anchor Nodes）集合的质心。在信标节点的位置已知、并且从它们那里接收到的信号强度彼此相近的情况下，式（7-3）给出信标节点质心计算公式。

$$(x,y) = \left(\frac{\sum_{i=1}^{n} x_i}{n}, \frac{\sum_{i=1}^{n} y_i}{n}\right) \tag{7-3}$$

节点定位技术同样为新攻击提供了机会。例如，一个恶意节点可能将自己伪装成一个信标节点，并散布错误的位置信息，从而妨碍节点定位。另外，还有很多其他的针对节点定位方案的安全攻击，这些攻击在第 8 章中将给出更详细的介绍。

7.2 时钟同步

时钟同步（Time Synchronization）对于自组织网络，尤其是传感器网络来说也非常重要，不只因为它是不同层协议的需要，例如媒介访问控制层（例如时间表）和网络层（例如路由和聚合）等，也因为传感数据经常需要与一个时间相关。影响大型系统中的时钟同步的因素主要有以下几点（Mills，1994，1998；Levine，1999；Elson et al.，2002）：

1）温度：一天中的天气变化可能会引起时钟的加速或者减速（每天几微秒的变化）。

2）相位噪声：硬件接口位置会发生访问波动；操作系统对于中断的响应变化、抖动延迟等。

3）频率噪声：晶体的频谱与其相邻的频带之间有很宽的边频带。

4）非对称延迟：某条路径的延迟对各个方向可能会有不同。

5）时钟干扰：硬件或者软件上的异常情况可能会引发时间上的突变。

这些因素会造成两个节点时钟的时间差异。这些在时间上的差异可以被分为以下几类（Ganeriwal et al.，2005）：

1）偏移（o）：节点的启动时间可能不同。因此，当网络在时刻 t_0 启动时，节点 A 的时钟 C_A 和节点 B 的时钟 C_B 可能会有所不同。

$$o = C_A(t_0) - C_B(t_0) \tag{7-4}$$

2）倾斜（s）：频率噪声和硬件等因素可能会使得节点的晶体工作在不同的频率。这会引起时钟倾斜，这种倾斜对传感器节点硬件来说，大概在每百万分之

±30 ~40 范围内。在两个节点出现偏移的基础上，相距越来越近或者越来越远的情况下会出现倾斜现象。单位时间 t 内与倾斜相关的变化是一个常量。

$$s = \frac{\partial C_A}{\partial t} - \frac{\partial C_B}{\partial t} \tag{7-5}$$

3）漂移（d）：温度、相位、非对称性延时和时钟干扰可能会随着时间的延长而改变两个节点间的偏移。由于这些因素是随时间变化的，所以时钟上的变化，称为漂移（Drift），它在单位时间内的值不是固定的。

$$d = \frac{\partial^2 C_A}{\partial t^2} - \frac{\partial^2 C_B}{\partial t^2} \tag{7-6}$$

自组织网络的时钟同步算法可以根据三种标准进行分类：同步过程的分发、在时钟同步中节点扮演的角色以及时钟同步的精确度，如图 7-5 所示。在集中式时钟同步中，所有节点和一个中心时间服务器相同步。网络时间协议（Network Time Protocol，NTP）（Mills，1994）属于这一类。NTP 是互联网中的最广泛采纳的协议。在 NTP 中，存在通过外部时间源进行同步的时间服务器，例如 GPS。所有网络中的其他节点和这些时间服务器保持同步。在分布式方法中，节点不和中心时间服务器保持同步，而是和它们需要保持同步的节点进行同步。参照广播同步（Reference Broadcast Synchronization，RBS）方案（Elson et al. ，2002）就是分布式方法的一个例子，在这种方案中，节点通过一个来自于中心节点的参考时间戳来和网络中其他节点保持同步。在第三种方法中，网络会进行时钟同步上的自组织。节点会在簇内进行同步，之后簇与簇之间会进行同步。

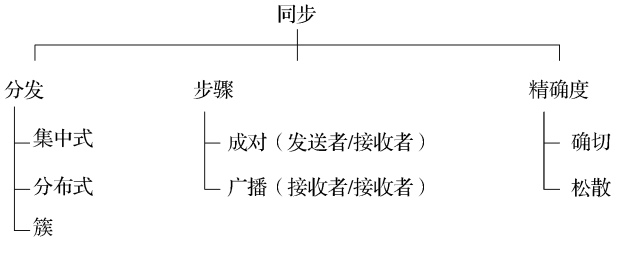


图 7-5　时钟同步方案

我们也可以根据同步步骤流以及步骤流中不同节点的任务对同步方案进行分类。从这方面可分为两类：发送者/接收者同步基本上是成对的时钟同步，而接收者/接收者同步是用于广播同步。

在发送者/接收者同步中，发送者会发送一个时间戳同步信息，同时接收者通过消息中的时间戳使自己和发送者保持同步。传感器网络时序同步协议（Timing-sync Protocol for Sensor Network，TPSN）（Ganeriwal et al. ，2003）就是一个发送者/接收者算法。

在接收者/接收者同步中，一个节点周期性地广播一个时钟同步消息，它被加入了一个时间戳。网络中的节点并不使用这一消息与发送者进行同步，但是消息中的时间戳为所有接收到这一消息的节点构成一个参考时间。之后，当某个节点需要和其他接收到相同消息的节点进行同步时，它们会交换从它们消息的时间戳中得到的偏移量。这一方案的一个好处就是节点能够知道其他节点的偏移量和漂移。RBS属于这一类。

最后，节点之间可能并不需要精确的时钟同步。有时候，所有节点都和其他节点准确同步的代价过于高昂，时钟偏移在一个规定的限度内是可以容忍的。不能保证准确的时钟同步，但时钟偏移控制在一个适当的限度内的时钟同步协议称为松散时钟同步方案（Loose Synchronization Scheme）。

7.3 寻址

无线自组织网络的独特特性和应用需求为节点寻址带来了新的挑战。对于很多自组织网络和传感器网络应用程序来说，节点的固定寻址和通用寻址（Universal Addressing）并不是一个很好的选择。因此，基于属性的命名或者节点的本地识别迄今为止被认为是为了各种目的（例如节点管理、数据查询、数据汇集或者路由）而对一个特殊节点进行寻址。我们将适用于自组织网络和传感器网络的节点寻址技术分类如下：

1）基于属性的命名和以数据为中心的路由：基于属性的命名（Intanagonwiwat et al.，2000）是最早用于无线传感器网络中节点寻址的技术之一。在这种技术中，对于某个指定的特性测量确定值的节点被称为，比如说，“测量温度超过35℃的节点”。

2）空间寻址：空间寻址在查询主要基于节点位置的入侵检测和目标追踪这类应用中非常有用。在空间数据汇集和地理路由方案中也同样需要。在这种技术中，某个区域的边界是定义好的，之后查询节点内部、外部或沿着区域边界具有一定深度的缓冲带中的节点。区域的边界可以通过一种事件边界检测算法（Ding et al.，2005）进行检测，也可以通过给定一系列地理位置指定。

3）sectoral sweepers（Erdogan et al.，2003）：空间区域也可以通过使用定向天线来具体指定，这里接收到具有一定范围接收信号强度指示的信号的传感器节点将响应一次查询。

4）为节点使用本地标识并将用户查询的目的地映射成本地标识：在这一方案中，每个节点都通过传感区域的本地标识来获得地址。到达任务数据包或者查询的目的地会通过中间节点映射到本地标识。使用者既可以通过使用基于属性的命名或空间寻址方案来指明目的地。网关节点会将这一地址映射到一个本地标识。

5）地址重用：地址重用对于媒介访问控制层来说尤其有用。只要不发生冲突，同一个地址可以分配给多个节点。在文献（Schurgers et al.，2002）中提出了一种用于地址重用的分布式协议。在这个协议中，节点首先广播一个“Hello”消息。收到这一消息的节点会回复一条宣布它们的本地地址的“Info”消息。广播“Hello”消息的节点通过使用“Info”消息中的数据，随机选择一个没有被它的邻居节点所使用的地址。如果由于隐藏节点问题而发生冲突，首先发现冲突的节点会向它们两者发送一个“Conflict”消息，它们两个节点中的一个就修改地址。

地址重用、本地标识和空间寻址技术为认证带来了新的挑战。

7.4　数据聚合和融合

在传感器网络中，数据聚合是非常重要的，其中包含两方面原因：首先，对数据进行融合并从中提取信息是必要的；其次，可以理解为减少通信开销的一种手段。因此，对于数据聚合已有很多研究，可以将其分类如下：

1）时间或空间聚合：数据可能会通过一种基于时间或者位置的方式被汇聚到一起。例如，用每个小时的温度记录或者某个传感器地区的各种区域的温度记录可以求平均值。同时基于时间和位置的汇聚的混合方法也可能会用到。

2）快照或周期性聚合：数据聚合可能会在快照中进行，例如一次性的，在收到查询之后，或者时间性的聚合数据可能会进行周期性的报告。

3）集中式或分布式汇聚：一个中央节点可以将数据收集起来然后进行汇聚，或者数据会在传感器网络中进行传送时被聚合起来。混合方法也可以行得通，这种方法中设置了簇，每个簇中的某个节点对簇中的数据进行汇聚。

4）提前或稍后的汇聚：数据可能会在最早出现的机会下聚合，或者为了不干扰邻居节点之间的协作，在经过一定跳数之前可能不允许数据聚合。

数据相关性、数据关联和融合技术用于关联来自于多个传感器节点的数据到某个事件，关联来自于传感器的数据到多个事件，并将数据融合成一个公共图像。数据聚合方案不应该阻碍这些任务的完成。

7.5　数据查询

传感器网络中的一个最有挑战性的任务就是综合用户请求的信息和由大量的传感器节点测量或感知的可用数据。由于传感器网络中存在大量的能量严格受限节点，聚集所有节点读数用于集中处理是不可行的。取而代之的，需要有效的数据查询和聚合技术。这一节，我们主要关注传感器网络中的数据查询。

传感器网络中的数据查询可以是连续的和周期性的、连续的和事件驱动或快照

型的，例如单次查询。我们也可以将传感器网络查询分为聚合式和非聚合式。查询也可以是复杂的或者简单的。最后，对复制数据的查询也可以进行。用户通过使用传感器网络的数据查询方案应该可以完成任何一种类型的数据查询。实现这一目标的一个方法就是将传感器网络理解为一个分布式数据库（见图 7-6），例如通过模数寻址的数据聚合和稀疏（DADMA）方法（Cayirci，2003）。

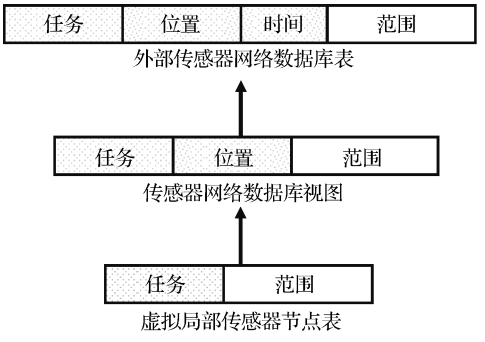


图 7-6 视为分布式数据库的传感器网络

7.5.1 数据库方法

在 DADMA 中，传感器网络被看做是一个分布式关系数据库，而这个数据库是由连接位于传感器节点中的本地表的单一视图构成的。本地表中的记录是对到达查询的度量并包含两个字段，即任务（Task）和范围（Amplitude）。由于某个节点的依附节点可能不止一个，任务字段，例如温度、湿度等，用于指示进行测量的传感器。节点的存储容量有限，所以它们并不存储每一个测量的结果。因此，任务字段是本地表中在查询请求到达时生成的关键字字段。对传感器网络的这一理解，使得对于提取传感器数据而不需要更多的存储需求，关系代数是实际可行的。

传感器网络数据库视图（Sensor Network Database View，SNDV）可以在中央节点或者外部代理服务器中临时创建。一个 SNDV 记录有三个字段：位置（Location）、任务（Task）和范围（Amplitude）。当从一个节点提取数据时，传感数据通过节点的位置被连接起来。由于多个节点可能拥有相同类型的传感器，例如，多个传感器会执行相同的传感器任务，位置和任务字段成为 SNDV 中的关键字。对于很多 WSN 应用来说，传感数据需要和位置数据相结合。例如，在进行目标追踪和入侵检测的传感器网络中，传感数据在没有和位置相关联的情况下，基本上没有任何意义。因此，节点的位置感知是很多 WSN 应用的强制性需求。如果位置数据对于应用来说不可用也不重要，节点的本地标识字段就会取代位置字段。

在一个远端代理服务器中维持数据库也是可行的，这里从查询中获得记录，例如，一个 SNDV 的记录在和一个时间（Time）标签连接之后存储。举例来说，一个后台程序（Daemon）可以在特定的时间间隔生成查询请求，并把从查询中得到的 SNDV 记录插入到它们与时间字段连接之后的数据库。注意每次查询结果产生一个新的 SNDV，这里查询结果被临时聚集起来。

在 DADMA（Cayirci，2003）中，查询是由具有以下结构的一个语句发起的。注意，这个语句中使用了标准结构化查询语言（SQL）符号，除了最后以关键字

“based on”开始的部分。

Select[task, time, location, [distinct | all], amplitude,
[[avg| min |max | count | sum] (amplitude)]]
from[any , every , aggregate m , dilute m]
where[power available [< | >] PA |
location [in| not in] $RECT$ |
t_{min} < time < t_{max} |
task = t |
amplitude [<| = = |>] a]
group by task
based on[time limit = l_t| packet limit = l_p| resolution = r | region = xy]

一个用户可以提取 SNDV 中可用的数据字段的一个子集，并通过基于任务的分组数据或者通过使用式（7-7）中给出的聚合 m 函数来聚合范围数据。其中的一些节点也可能会从一次查询中被式（7-8）中给出的稀疏 m 函数排除。

$$f(x) = x \mathrm{div} m \tag{7-7}$$

$$f(x) = (x/r) \bmod (m/r) \tag{7-8}$$

式中，x 代表和一个坐标轴相关的某个节点的网格位置；r 代表以米为单位的分辨率；m 代表稀疏或聚合因子。

当用户给出 dilute m 命令后，每个节点首先使用式（7－8）找到它在水平和垂直坐标上的位置索引，并将这些索引和查询中的“base on”字段的区域值 x 和 y 进行比较。如果它们匹配，节点将会对查询进行回复。例如，对 $m=8$ 同时 $r=2$，位于 {46，74} 位置的节点的位置索引是 {3，1}。因此，如果查询中的区域值是 {3，1}，那么这个传感器就应该作出响应。因此，只有位于每米内的 $r \times r$ 平方米内的汇聚节点才会对查询作出反应，而其他节点则保持空闲。这是一种实用的技术，特别是在节点根据均匀分布被随机部署，传感器网络用于监控诸如温度、湿度和压力等环境条件的情况下。

对于同一个例子，通过式（7-7）所得到的索引是 {5，9}。当接收到 aggregate m 命令时，由某个节点所测量的值将会和其他拥有相同索引的节点所测量得到的值进行聚合。因此，我们可以基于节点的位置，在一定的地理位置定位汇聚节点，并聚合数据。

7.5.2　任务集

提出任务集的概念是为了将传感器区域分成多个子区（subregions），并在每个子区中为每个任务集分配特定数量的节点（Cayirci et al.，2006a）。每个子区中的节点数量由于节点非均匀分布而不同。因此，在不同的子区中查询传感区域的代价就

会有差别。为了平衡这一开销，Cayirci et al. （2006a）提出了在每个象限通过特定数量的节点生成任务集（TS）的方法。通过使用任务集，用户就拥有了平衡精确性/可靠性和通信开销的主动权。任务集中的节点数量表明了通过查询任务集能够收集到的数据分辨率。任务集中存在更多的节点意味着更高的准确性和可靠性。另一方面，任务集中的节点数量的增加会消耗更多的能量。

例如，TS1 可能会被定义为每个子区中拥有最大可用能量的两个节点。相似地，TS2 可能被定义为所有不在 TS1 中的节点。在任务集建立之后，查询请求将会被送到 TS1 或者 TS2。

7.5.3 其他数据查询方案

在传感器网络主动查询转发（Active Query Forwarding in Sensor Network，ACQUIRE）方案中（Sadagopan et al.，2003），每个发送查询请求的节点都试图解析查询。如果某个节点进行了查询解析，它就不再重发查询而是将结果返回。节点会和它的 n 跳邻居合作来完成查询解析。参数 n 被称为 look-ahead 参数。如果节点在和它的 n 跳邻居节点合作后，不能够完成查询解析，它就将查询发送给另一个邻居节点。当 look-ahead 参数是 1 时，ACQUIRE 在最坏情况下进行泛洪。

大规模移动传感器网络中的移动性辅助查询解析（Mobility-Assisted Resolution of Queries，MARQ）（Helmy，2003）利用了移动汇聚节点从传感器网络中收集数据。在 MARQ 中，每个节点都有一些其他的节点作为联系人。当联系人移动时，它们会和其他节点进行交互并收集数据。节点会和它的联系人合作来解析查询。

文献（Shen et al.，2001）提出传感器查询与任务分配语言（Sensor Query and Tasking Language，SQTL）作为提供一种脚本语言的应用层协议。SQTL 支持三种事件，由关键字 receive、every 和 expire 定义。关键字 receive 定义了当节点接收到一个消息时所产生的事件；关键字 every 定义了由于定时器超时而周期性发生的事件；关键字 expire 定义了一个定时器到期时发生的事件。如果节点接收到了一个预期要发送给它的消息，并且其中含有一个脚本文件，节点就会执行这个脚本文件。

7.6 覆盖

无线自组织网络中的覆盖这一术语包含了两方面的内容：网络所覆盖的通信区域或者在传感器网络中能够被传感器监测到的区域。通过相同数量的节点来提供最大的覆盖范围是与以下因素相关的一个重要挑战（Cardei and Wu，2005）：

1）节点部署方案；

2）传感和通信范围；

3）能量效率和连通性需求；

4）算法范式，即集中式或者分布式。

覆盖范围问题可以分为以下三类（Cardei and Wu，2005）：

1）在区域覆盖（Area Coverage）中，要达到的目标是覆盖一个区域，对于感知覆盖问题，这就意味着要确保给定区域中的每个节点都能被检测到。同时，对于通信覆盖区域问题而言，这意味着区域中的任何一个节点都能够接入网络。

2）在点覆盖（Point Coverage）中，目标是确保给定的一个节点集被网络所覆盖。

3）在障碍覆盖（Barrier Coverage）中，目标是确保网络中不存在隐藏路径，例如，若没有穿过至少一个节点的覆盖区域，入侵者无法穿过网络。

解决覆盖区域问题的基本办法主要有两种。在第一种方法中，假定按照某种分布随机地部署节点，同时满足覆盖给定概率的最小节点数已经确定。在第二种方法中，假设节点可以在特定的位置进行部署，同时每个节点的位置确定使得在给定节点数目的情况下，使覆盖区域达到最大。很多种遵循这些算法的方法可以在文献（Cardei and Wu，2005；Cayirci et al.，2006b）中找到。

可以设计新的攻击用于发现未覆盖的区域，或者通过威胁传感器网络中执行覆盖区域相关算法的节点而产生入侵隧道。

7.7　移动性管理

虽然基础架构由于被设计用于提供全球性的无缝漫游而不具有移动性，但是在节点是移动的网络中需要移动性管理，这是一个有基础架构网络中非常有挑战性的问题。在自组织网络中，移动性一般限于网络内部。因此，自组织网络移动性管理所吸引的研究者比较少。在基础架构网络例如蜂窝网络中移动性管理面临两个任务：位置管理和移交管理。位置管理是为了记录用户，这样使得对他们的呼叫可以到达他们当前所在的位置。移交管理可以允许用户在一次活动连接中进行漫游。一个正在进行通信的移动节点可以离开某个接入点的覆盖区域并进入另一个接入点的覆盖区域，移交管理可以允许这一操作，并且不中止当前已经建立起的连接。由于在自组织网络中不是接入点而是路由组成多个无线跳，路由协议就会处理活动连接中的路由变化。因为节点可以在多个自组织网络中进行漫游，所以位置管理也可以成为自组织网络中的一个问题。因此，和移动 IP 中相似的位置管理技术在自组织网络中也要用到。

蜂窝网路中的位置管理包括了两方面任务：位置更新和分页（Paging）。移动终端（Mobile Terminal，MT）的位置信息通过位置更新来维护。在当前的系统中，单元（Cell）例如接入点，被聚集成位置区域（Location Area，LA）。一个位置区域可能含有一个或多个分配给它的单元。一个移动终端只要到达一个新的位置区域都将报告其位置。由于一个位置区域由多个单元所组成，移动终端的确切位置应该通

过呼叫传送而确定。这一操作通过在最后一次注册的位置区域中的单元分页完成。

当一个位置区域由一群永久性的分配给这一位置区域的单元所组成，同时对于所有的移动终端是固定的时候，位置管理方案被称为静态的。动态位置管理技术更加适合于移动终端的移动性特征。它们允许动态选择位置更新参数，以及减少由于位置管理带来的发送信号的数据流。基于时间的、基于运动的以及基于距离的位置更新技术是知名的动态方案（Cayirci and Akyildiz, 2002；2003）。在基于时间的技术中，一个移动终端在一个预先定义的时间间隔内周期性地进行位置更新。在基于运动的技术中，位置更新会在经过一定数量的单元边界后进行初始化。基于距离的位置更新会在与最近一个注册单元的距离超过预定值时执行。

在文献中，还有一些其他的动态位置更新技术。在基于方向的方案中，移动终端只在它的运动方向发生变化时报告其位置。在选择性位置更新技术中，位置更新并不是在每个位置区域中执行，一些位置区域会根据跃进概率（Transition Probabilities）和单元停留时间（Dwell Times）被跳过。基于状态的位置更新技术中，由移动终端根据其当前状态来决定是否对其位置进行更新，这是另外一种动态技术。文献（Cayirci and Akyildiz, 2002）中也提出了当前已知方法的结合策略，例如基于时间和距离的方案。

位置更新的主要目标是减少分页开销（Paging Cost），同时分页策略的性能和位置更新方案密切相关。位置更新方案必须为网络提供足够的信息，来使得分页开销在给定的延时要求下得到降低。在分页开销和分页延迟以及分页和更新开销之间存在着一个平衡问题。由于解析的位置更新信息增加，将要分页的单元的数量就会减少。相似地，分页延迟越久，被分页的单元数量就越少。

最小分页延迟（Least Paging Delay）由地毯式投票（Blanket Polling）技术保证，这里位置区域中的所有单元会在一次呼叫到达时同时被分页。这一方案的分页开销很高。选择性分页（Selective Paging）是地毯式投票方法的替代方法，它减少了分页开销，但同时提高了分页延迟。在选择性分页中，基于位置的概率对移动终端的位置进行预测，同时单元会相继被分页，并从移动终端最有可能出现的那个单元开始。已提出的还有很多其他的分页策略，例如最短距离优先以及速率分页。在速率分页中，系统会基于移动终端的平均速度以及最后一次注册时间来计算其最大移动距离，并将这一距离内的从最近一次注册单元开始的所有单元进行分页。带有延时限制作为一项 QoS 限制的分页方案也已被提出，这里位置区域被分割为簇。一个位置区域中的簇的数量保证了系统可以连续地对其进行分页而不超过给定的延时限制。

7.8 跨层设计

我们希望以介绍跨层方法的一个短的小节来结束本书的第 1 部分。在这一节

中，我们的目标仅是对它给出定义，并让读者考虑一下跨层协议的安全问题。因为它超出了本书的范围，所以我们并不会给出属于这一类的一系列协议的细节。

OSI 的分层方法是设计用来提供网络协议和方案的互操作性和可重用性。然而，它并不能总是得到最优方案。在 OSI 分层的方法中，相比于跨层设计，以成本更高的协议栈为代价，可以实现更低层细节的透明性、协议的互操作性和可重用性。

由于 WASM 引入了一些非常严格的限制，跨层协议在我们的领域中是很常见的。跨层优化允许在层与层之间进行通信，这就会带来网络性能的提高。跨层交互在恰当地使用下，可以通过层与层之间传递信息而促进自组织网络中的效率，这会有效地适应动态环境。举例来说，网络层可以和数据链路层进行交互，使得被观察到的存在更多竞争的链路在路由选择时得以避免，可以设计一个能够更好地满足 WASM 需求的适应性跨层拥塞控制方案。相似地，媒介接入调度和路由确定就可以共同优化，得到更高的效率和更好的 QoS。

跨层设计存在两种方法（Aune，2004）：进化式和革命式。进化式方法试图扩展分层结构来维持兼容性。大多数的跨层设计都是进化式。允许两个或三个层共享信息的简单解决办法可以很大地提高效率和适应性。革命式方法并不试图扩展一个已经存在的基础架构或者维持兼容性，虽然它们并不是通常的方案，但是相比于其他方法，革命式跨层设计有可能提供更高的效率和适应性，所以这种方式对于特定体系架构来说可能会非常有用。

跨层设计会带来新型安全攻击，这些我们会在下一章中进行细致描述。例如，敌手可能会通过降低特定链路的特性，利用一个路由方案适应链路特性，来促使另一个链路连接到恶意节点。另一方面，一个安全方案可以为多层优化来减少安全开销，或者处于某个特定层级的安全方案可以被设计成跨层的，这样它就可以适应来自于其他层的信息。当阅读第 8 章时，请特别记住关于跨层方法的这一简短的小节。

7.9　复习题

7.1　请列出并解释能够用于发现到达信标节点距离的技术。这些技术的缺点是什么？

7.2　某个节点接收到了来自于三个坐标分别是（100，220）、（150，180）和（60，80）的锚点（Anchor Node）的信号。注意这些坐标表示以米为单位的相对参照点的距离。

（a）使用质心（Centroid）方案估计节点的位置。

（b）假设节点也发送拥有与射频信号完美传输时钟同步的超声波信号，同时

超声波信号以声速传播而射频信号以光速传播。如果对于每个锚点来说，超声波信号和射频信号的到达时间有如下差异，节点的绝对坐标是多少？

锚点 1：67 ms

锚点 2：100 ms

锚点 3：80 ms

（c）你能否根据（b）中的值找到位置？如果你不能，原因是什么？

7.3 出现时钟倾斜（Clock Skew）的原因是什么？调查关于时钟偏移值的至少一个微处理器的技术规范。

7.4 为每个传感器节点配置一个全球唯一地址是否可行？如果不行，原因是什么？解释一下传感器节点寻址的替代方法。

7.5 什么时候使用稍后的汇聚？

7.6 数据联合（Data Association）、数据关联（Data Correlation）和数据融合（Data Fusion）之间的区别是什么？

7.7 你认为将传感器网络视为一个可查询数据库的方法是否可行？提供一种实现这一目标的技术。

7.8 区域覆盖和障碍覆盖之间的区别是什么？哪一个问题更有挑战性？为什么？

7.9 给出位置管理中的两个任务，并简要描述它们。

第二部分

无线自组织网络、传感器网络和 Mesh 网络安全

第 8 章　自组织网络、传感器网络和 Mesh 网络中的安全攻击

在本章中，我们对安全攻击和攻击者进行分类。首先，我们给出了安全攻击的分类和攻击场景的例子。不同动机的不同类型的攻击者会实施同种类型的攻击。防御机制不仅应对攻击类型，还应对各种类型攻击者反应灵敏。因此，我们也对攻击者进行归类。在本章最后解释各种攻击者的动机。

8.1　安全攻击

安全攻击分为两大类：被动攻击和主动攻击。被动攻击主要针对数据机密性，敌手并没有进行任何发射。在主动攻击中，敌手实施恶意行动，不仅破坏数据机密性，还破坏数据完整性。主动攻击也会以未经授权访问和使用资源或以干扰敌方的通信为目标。一个主动攻击者进行发射或采取行动时，会被检测到。

除了安全攻击，无意的失误（Needlessness）也是一种重要的安全威胁。由于失误，用户可能将节点暴露于诸如篡改和破坏、未经授权访问机密数据和资源等威胁之中。安全和容错方案也应该解决由于用户粗心使用或因不可预知事件而产生的安全挑战。

8.1.1　被动攻击

在研究被动攻击之前，请注意射频（RF）不是唯一的无线媒介。还有其他无线媒介，比如红外线和其他光纤通道，这些对搭线窃听有更强的适应性。这些类型的信道是定向的，它们的传输会受到空间限制。为了能实现窃听，需要定位敌手的接收方。这使得敌手更难完成任务，也更容易被检测到。

被动攻击的攻击者一般是伪装的，比如隐藏起来，通过窃听通信线路来收集数据。被动攻击分为窃听（Eavesdropping）和流量分析（Traffic Analysis）（见图 8-1）。

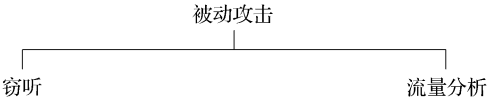


图 8-1　被动攻击

8.1.1.1　窃听

机密数据能通过搭线通信线路被窃听，无线链路更容易被窃听。因此，无线网络更容易遭受被动攻击。尤其是使用已知的标准和无线发送明文（未加密）数据

时，敌手能很容易地接收和读出数据，监听或监视影音传输。例如，如果在不安全的无线链路中采取明文传输，敌手容易窃听信用卡卡号和密码。

事实上，与其他射程更远的无线技术相比，自组织网络和传感器网络在防窃听方面更安全，这是因为信号的射程更短。敌手需要距离目标节点足够近才能窃听。如果使用无线技术的设备有足够的可控空间来防御入侵者（比如未授权的人和设备），它就能变得更加安全。然而，它们永远不会比受限通信（Tethered Communications）更安全。与目标设备足够近的内部人员能接收设备所有发出或接收的帧，把它们存储在某些媒介，并从设备中带出去。仔细检查离开的每一人或检测设备发射的电磁波能降低这种风险。尽管如此，使用无线技术时，这种风险要高得多。

另外，无线通信使在单一设备上实现不同安全级别的多网络更加困难。例如，如果在同一个设备中有机密网络和接入因特网的一个网络，无线接入机密网络是允许的，但是由于被动攻击和无意的失误，因特网和机密网络的去耦合会变得十分困难。注意，不允许不受限通信（Untethered Communications）并不能使安全风险消失，但是允许不受限通信会增加安全风险。无论是否允许无线通信，无意的失误、内部攻击者和发射安全总会是问题。

在本节，我们会把隐私从机密性中区别开。为了获取机密数据和私密信息，基于无线自组织网络和传感器网络实现的有感知环境和普适计算可能会被滥用。例如，为了观察他人的私生活，一个安全系统的摄像头会受到被动攻击。分析非机密数据也可能泄露私密信息。因此，乍看不能认定是机密的某些系统和数据，可能是私密的，应该受到保护。

隐私保护中，匿名是重要的。攻击隐私可能首先以攻击匿名化开始。敌手首先需要知道，哪个节点是以何种目的为哪个用户服务的。类似地，敌手也应该知道哪个数据包来自于哪个节点。完成这些之后，收集到的数据可能会变得更有意义。因此，匿名能增强隐私保护和机密性。

8.1.1.2　流量分析

和数据包的内容一样，流量模式对敌手来说也是很有价值的。例如，有关网络拓扑的重要信息能通过分析流量模式推导出来。在自组织网络中，尤其是在传感器网络中，更靠近基站的节点（如汇聚节点（Sink）），因为它们比远离基站的节点传递更多的数据包，所以它们会比其他节点具有更多的通信量。类似地，聚类是自组织网络里的重要工具，簇头比网内其他节点更加繁忙。要检测出基站，靠近它的节点或簇头可能对敌手很有帮助，因为针对节点的拒绝服务攻击或窃听发往节点的数据包可能会有更大的影响。通过分析流量，这种有价值的信息就能被提取出来。

流量分析也能用来发起针对匿名的攻击。检测某些数据包的源节点也可能是敌手的目标之一。这种信息有利于检测出事件位置、弱点、能力和功能或节点的拥有者。

另外，流量模式会涉及其他机密信息，如行动和意图。在军事通信中，寂静可能会暗示在准备进攻、战术转移或渗透。与之相似，流量速率的骤增可能暗示着将发起蓄意攻击或突袭。民用网络中的流量分析也能推断出类似信息。为了列出每一个终端的频繁联系方，这在情报工作中称为友谊树（Friendship Trees），敌手会实施流量分析。通过筛选网络流量，节点的联系方能被确定。分析目标节点和联系方之间的信号，会更有意义。

流量分析中会用到以下技术之一：

1）物理层的流量分析：这种攻击只有载体能觉察到，分析流量速率是为了判断在某一位置的节点。

2）MAC 层和更高层的流量分析：MAC 帧和数据包可以去复用（Demultiplexed），敌手分析帧头和包头。这样能暴露网络的路由信息、拓扑结构和友谊树。

3）事件关联的流量分析：在传感器网络或终端用户传输中探测的这些事件，可与流量相关联，能推出更多的详细信息，如路由等。

4）主动流量分析：流量分析也可以实施为主动攻击。例如，破坏一定数量的节点会刺激网络中的自组织，关于拓扑结构的有价值的数据会被收集。

8.1.2 主动攻击

在主动攻击中，敌手实际上影响着受攻击网络的运转。这种影响可能是攻击的目的会被检测到。例如，攻击的结果可能使网络服务下降或中断。有时，敌手会努力不被检测到，目的是获得系统资源的未经授权访问或威胁网络内容的机密性和/或完整性。我们把主动攻击分成四类，如图 8-2 所示。

图 8-2 主动攻击

8.1.2.1 物理攻击

敌手为了终止节点，会物理毁坏硬件。这个安全攻击也可以认为是属于容错领域，容错是指节点发生故障时，维持网络功能不中断的能力。针对硬件的物理攻击可能会变成一个严重的问题，尤其是在军事通信和传感器网络上。传感器节点会部

署在无人值守但敌手能接近的区域。因此，它们可能会被移出传感器网络区域或被破坏。当这些危险来临时，节点需要适应物理攻击。

当节点无人管理且又对敌手物理可达时，它们会受到篡改（Tampering）技术攻击。篡改技术包括微探（Microprobing）、激光切割、操控聚焦离子束、脉冲攻击（Glitch Attacks）和功耗分析（Komerling and Kuhn, 1999）。篡改节点有助于伪装和拒绝服务攻击（我们将随后解释）。因此，容错（Tamper Resilience）的问题是在许多传感器网络和军事通信应用中需要认真考虑的问题。

我们可以把篡改节点的方案分成两类：入侵篡改和非入侵篡改。入侵技术的目的是能无限制地访问一个节点。在非入侵篡改中，对节点的无限访问不是目的。相反，通过分析节点行为如能量消耗或各种输入情况下算法的执行时限，可以推导出程序的加密数据和加密方案使用的密钥。

电磁脉冲（EMP）攻击也是在列的物理安全攻击之一。电磁脉冲是具有高强度电磁能量的短时爆发，它能产生电压浪涌（Voltage Surges），这会破坏到射程内的电子设备。电磁脉冲是核爆炸的自然结果之一。现在已经有能产生电磁脉冲的便携装置。虽然电磁脉冲技术的实用化仍有未解决的问题，但是电磁脉冲是对军事领域各种电子设备的一种威胁。这可被认为是容错领域的一部分。制造对电磁脉冲更具适应能力的电子设备是可能的。因此，我们将电磁脉冲攻击列为一种安全攻击。

8.1.2.2　伪装、重放和消息篡改

一个伪装（Masquerading）节点行动仿佛是另外一个节点。伪装节点会截获并重放消息。最后，被截获的消息内容在重放之前会被修改。基于这些方法会产生各种场景和威胁。

自组织网络和传感器网络有针对伪装特殊的优势。移动自组织网络的节点可能改变它们的位置。这个位置不是给定的或是固定的，自形成和自愈的机制应该适应拓扑结构的变化。因为对路由来说，响应技术是首选，拓扑结构可能无法维持，所以检查节点的网络接入点的一致性可能是困难的。此外，如果节点已经通过另外一个网络接入点连入网络，这也许不能检查出来。传感器网络中更容易伪装，因为全球识别可能不会用在传感器网络里。相反，像以数据为中心的路由和地址重用技术可能是寻址方案。

伪装、消息重放和内容篡改可能用于攻击消息内容和网络服务的完整性。特别是传感器网络，有一些基于许多节点协作的网络功能容易受到特殊类型的安全攻击。例如，节点定位方案可能遭受以下某一安全攻击：

1）一个恶意节点伪装成信标（Beacon），并错误地传播它的地址。当节点用恶意节点发射的信标信号进行三角测量或多边测量时，这将妨碍节点定位程序。

2）信标节点可能会被篡改并引入错误位置信息，用高于或低于预期的能量发射信标信号，这样做的目的是为了损害基于接收信号强度指示器（Impair Received

Signal Strength Indicator Based Schemes）的方案，或者在使用到达时间差算法时，使射频传输和超声波信号传输略微去同步。

3）恶意节点可能会重放信标信号。

4）物理攻击可能会破坏信标节点。

5）为了阻塞直接的视距，敌手会在信标节点和网络之间设置障碍。

还有更多的攻击场景会破坏节点定位方案。除了节点定位方案，以下服务（在第7章中解释）的完整性，也容易遭受类似安全攻击：

1）网络的数据汇聚和融合会使传感器网络对重放和内容篡改攻击更敏感，因为改变聚合消息的内容会改变许多节点提供的数据。

2）时钟同步也是容易受到伪装攻击的服务。一些内部人员注入错误的时钟同步信息，可能会阻止系统完成时钟同步。时钟同步对重放攻击特别敏感。一个恶意节点会把一个时钟同步消息塞进一个网络的某一部分，在一个短暂的时延之后，它会重放这个消息。这会阻止正确的时钟同步，对依赖精确同步协议的所有服务会造成相当有害的影响。

3）当节点定位和时钟同步服务受到攻击时，数据相关性和关联技术也会被削弱。

4）通过篡改消息内容，事件和事件边界检测算法会受到阻碍。

5）类似地，通过篡改用于节点管理的报告节点状态或传输命令的消息，节点管理系统可以被牵制。

女巫攻击（Sybil Attack）是伪装攻击的改进版，恶意节点把自己伪装成多个节点。拥有多个标识对一个恶意节点是非常有利的。例如，女巫攻击可实施反数据关联和聚合技术。一个节点用多个不同标识发送多个数据能相当大地改变汇聚值。女巫攻击也能威胁到多路径路由方案、节点定位等。多种标识还有助于隐藏攻击，例如秘密攻击（Stealthy Attacks）。

注意，我们也能把针对服务完整性的攻击认为是拒绝服务（DoS）攻击，因为它们降低了某些服务的可用性。我们将在下节详细解释拒绝服务攻击。

伪装、消息重放和内容篡改能通过使其他节点发送机密数据给恶意节点或访问机密数据，来攻击机密性。它们也可以是未授权访问系统资源的技术。

在网络钓鱼（Phishing）中，敌手伪装起来欺骗一些人，让他们自愿交出机密信息。“phishing”这个词是“口令”（Password）和钓鱼（Fishing）的组合，它很恰当地定义了这种攻击。一个恶意节点会假冒授权节点向其他节点索要口令、密钥等信息。

伪装也是保持恶意节点匿名性的一种方法。恶意节点会提供一些非法或不道德的内容，也会攻击或非法登录远程系统，如政府或银行大型数据库。

8.1.2.3 拒绝服务攻击

拒绝服务攻击的主要目标是网络服务的可用性（Availability）。拒绝服务是指

任何降低网络正确或及时执行预期功能能力的任何事件。拒绝服务攻击有以下属性（Wood and Stankovic，2005）：

1）恶意性：实施拒绝服务攻击是为了阻止网络执行预期功能，这不是偶然的。否则，它就不属于安全领域，而应属于可靠性（Reliability）和容错性（Fault Tolerance）领域。

2）破坏性：它降低了网络提供的服务质量。

3）不对称性：攻击者只需付出与对网络产生的影响规模相比很少的努力。

每一个网络服务都可能会遭受拒绝服务攻击。在本节，我们将回顾对自组织网络和传感器网络重要的拒绝服务攻击场景。

1. 物理层的拒绝服务

8.1.2.1 节阐释的所有物理攻击也可被认为是拒绝服务攻击，因为它们阻止网络执行预期功能。在本节，物理层指出 OSI 层负责在无线媒介中正确表示 1 和 0，以及一种称为“拥塞”（Jamming）的物理层的拒绝服务攻击，意味着针对物理层的安全威胁。

一个恶意设备能通过以某频率发射信号，阻塞无线载体。拥塞信号促成载体的噪声，它的强度足够把信噪比降到某水平之下，使得节点利用此信道正确地接收数据。拥塞会在一个区域持续地产生，这阻碍了该区域所有节点的通信。或者，拥塞会以随机的时间间隔临时发生，这仍能很有效地阻碍通信。

2. 链路层的拒绝服务

链路层算法尤其是 MAC 算法，为 DoS 攻击提供许多可利用的机会。例如，以下的 MAC 层拒绝服务攻击会持续干扰一个信道：

1）每逢收到 RTS 信号，就要发送一个与 CTS 信号冲突的信号。因为在收到 CTS 前，节点不能开始发送数据，它们会一直发送 RTS 信号。

2）如果 MAC 算法基于休眠期和活跃期，只有在活跃期的拥塞能持续阻塞信道。

3）携有长数据传输参数的错误 RTS 或 CTS 信号会被持续发送出去，这使得做虚拟载波侦听的其他节点永远等待。

4）应答欺骗（Acknowledgement Spoofing），敌手对窃听到的发给邻居节点的包，发送错误的链路层应答信息。这也是一种有效的链路层拒绝服务攻击。

基于 MAC 层寻址方案还能设计出更复杂的拒绝服务攻击。例如，传感器网络不使用全局寻址方案，而使用以数据为中心的路由算法、基于属性的命名法和地址重用。一个恶意节点会实施 MAC 层的女巫攻击，这使本区域内的其他节点认为所有可用地址都已在使用。这会阻止节点成为网络的一部分。

3. 对路由方案的拒绝服务

自组织网络是无基础设施的，有着特殊的路由挑战，为自组织网络和传感器网

络的网络层协议带来新型拒绝服务攻击。这些攻击一般分为两类（Hu et al.，2005）：路由中断攻击（Routing Disruption Attacks）或资源消耗攻击（Resource Consumption Attacks）。路由中断攻击的目的是使路由方案功能失常，不能提供所需的网络服务。资源消耗攻击是为了消耗网络资源，比如带宽、内存、计算能力和能量。这两种都是拒绝服务攻击，它们的实例如下（Karlof and Wagner，2003）：

1）欺骗、修改或重放路由信息：为给路由方案造成破坏，节点之间交换的路由信息会被恶意节点修改。

2）您好泛洪攻击（Hello Flood Attack）（Karlof and Wagner，2003）：恶意节点会用足够大的传输能量广播路由或其他信息，以使网络中的每个节点相信它就是邻居节点。当其他节点发送给恶意节点数据包时，这些包不会被任何一个节点收到（见图 8-3）。

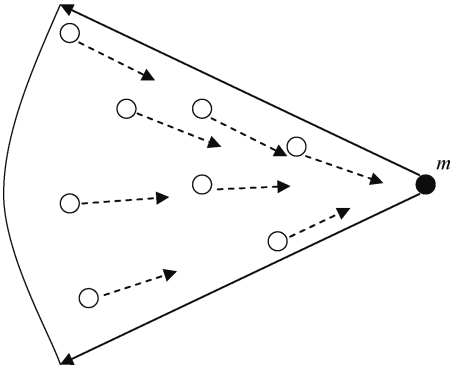


图 8-3 您好泛洪攻击

3）虫洞攻击（Wormhole Attack）：一个恶意节点能在某点窃听或接收数据包，并通过带外信道，把数据包传给网络另一部分的一个恶意节点。然后第二个节点重放数据包。这使所有“听”到第二个恶意节点传输的节点认为，发送包给第一个恶意节点的节点是它们的单跳邻居，它们是直接从邻居那里收到数据包的。例如图 8-4，节点 w_1 也会收到节点 a 发送的包，节点 w_1 是恶意节点。节点 w_1 通过一个带外信道把这些数据传给节点 w_2，这个信道对网络中除了敌手以外的所有节点来说是带外的。节点 w_2 重放数据包，节点 f 收到数据包，好像这些包是从节点 a 直接发送过来一样。沿着正常路径例如 a—b—c—d—e—f 的包，到达节点 f 晚于通过虫洞传输的包，因此沿着正常路径的包会丢弃，因为它们用了更多跳，而虫洞一般通过更快的信道建立。虫洞很难检测出来，会影响许多网络服务的性能，如时钟同步、定位和数据融合。

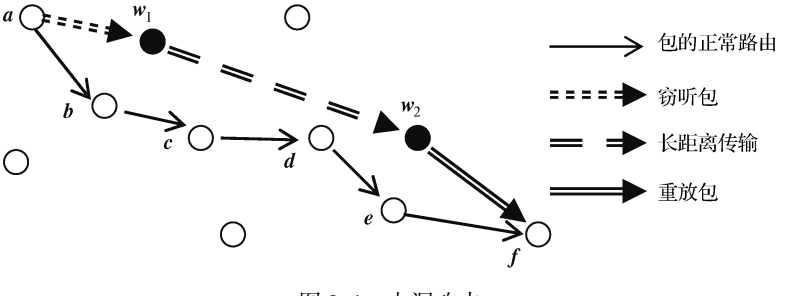


图 8-4 虫洞攻击

4）迂回攻击（Detour Attack）：攻击者可以试图使通信绕道经过一个次优路径或分割网络。有很多技术都可以用来实现绕道。例如，Hu et al.（2005）定义一个无偿迂回攻击（Gratuitous Detour Attack），路径上的节点把虚拟节点添加到路径上。于是和攻击者设法绕道通信的另一路径相比，此路径变得代价更高。

5）汇聚节点漏洞（Sink Hole）攻击：考虑到路由算法，一个恶意节点对周围节点是很有吸引力的。例如，很有吸引力的路由“广告”可以广播，所有邻居节点会相信该恶意节点是发送数据包给基站的最好的下一跳。当节点变成一个汇聚节点漏洞时，它变成了周边节点的“集线器”，开始接收发往基站的所有数据包。这为后继的攻击创造了很多机会。

6）黑洞攻击：一个恶意节点会丢弃掉它接收用来转发的所有数据包。当黑洞节点也是汇聚节点漏洞时，这种攻击特别有效。像这样的联合攻击会使黑洞周围的数据通信停止。

7）选择性转发（灰洞攻击）：当一个恶意节点丢弃掉所有的数据包时，这容易被它邻近的节点检测到。因此，恶意节点可能只会丢掉挑选的包，而转发其他数据包。

8）路由循环攻击（Routing Loop Attack）：迂回或汇聚节点漏洞类型的攻击，能用于产生路由循环攻击，消耗能量和带宽，以及中断路由。

9）女巫攻击（Sybil Attack）：一个节点呈现给网络其他节点多个身份。这会降低容错方案的效力，并对地理路由协议造成极大的威胁。除了这些服务，女巫攻击还会影响其他方案的性能，例如异常行为检测、基于投票机制的算法、数据汇集和融合，以及分布式存储。

10）急流攻击（Rushing Attack）（Hu et al. , 2005）：一个攻击者会散布路由请求，并通过网络快速回复消息。这会抑制以后任何合法的路由请求消息，例如节点丢弃消息，因为节点抑制了它们已经处理的路由请求的其他副本。

11）利用节点惩罚方案的攻击：敌手可以利用避免低性能节点的方案。例如，恶意节点会报告一个节点的错误消息，而实际上节点是运行良好的。因此，路由方案可能避免使用一个包括该节点的路径。类似地，一个链路可能会被阻塞一小段时间。但是，由于在这一小段时间内会产生关于链路的错误消息，即使它不再拥塞，路由方案可能会继续弃用这条链路。

12）耗尽网络资源的攻击：当节点无人值守，并依赖它们自带资源时，恶意行为会把那些资源耗尽。这种情况尤其会发生在传感器网络中。例如，一个恶意节点可能持续产生数据包，并发给收集数据的节点，例如基站，转发数据包的节点就会耗尽它们的能量。

4. 传输层的拒绝服务攻击

传输层协议也容易受到安全威胁。适用于该层中的攻击场景如下：

1）传输层应答欺骗（Acknowledgement Spoofing）：错误的应答消息或带有大量接收窗口的应答消息（见 6.2 节），可能使源节点产生更多超出网络承载能力的片段。这会导致网络拥塞和网络的性能降低。

2）重放应答：在有些传输层协议中，比如 TCP – Reno，对同一个片段多次应答意味着负应答（Negative Acknowledgement）。一个恶意节点会多次重放一个应答，使得源节点认为该消息没有成功地传送出去。

3）阻塞应答（Jamming Acknowledgement）：一个恶意节点会阻塞传输应答消息的片段。这会使连接终止。

4）改变序列号：在可靠多片段传输（RMST）和缓发快取（PSFQ）协议里，一个恶意节点可能改变片段的序列号，并使目的地相信一些片段已经丢失。

5）连接请求欺骗：一个恶意节点可以向一个节点发送许多连接请求，耗尽其资源，这样它就不能接收到其他节点的连接请求了。

这些列出的攻击实例并没有穷尽。基于传输层中的协议，人们还会制定出许多不同的策略。

5. 应用层的拒绝服务

敌手也可能利用应用层协议进行拒绝服务攻击。在 8.1.2.2 节提到过许多应用层协议。正如 8.1.2.2 节所提到的，像节点定位协议、时钟同步协议、数据汇集、关联和融合协议可以被欺骗或被阻碍。例如，一个假冒信标节点的恶意节点，释放错误定位信息或在传输功耗方面作弊，例如用比期望的功耗少或多的功耗传输，会妨碍节点定位方案。因为这种攻击会削弱相关网络服务，所以它们也可归为拒绝服务攻击。

8.1.2.4 行为不端

注意，有些拒绝服务攻击来自于网络内部的节点。一些节点为了获得有限资源中不正当的份额而行为不端，比如它们可能自私自利（Selfishness）。例如，通过使用 MAC 方案，一个行为不端的节点会迫使其他节点长时间地回退，释放出网络资源供自己使用。节点也会自私地拒绝重发其他节点的消息。如果每一个节点都这样，那么自私自利可能会产生和拒绝服务攻击类似的效果。

另一种行为不端是通过拒绝为接收到的服务付费，来攻击计费方案。乍一看，我们会认为自组织网络是一个免费环境，每个节点通过免许可信道与其他节点协作通信。但事实并非总是如此。Mesh 网络提供了无线多跳接入宽带服务。类似地，有多跳蜂窝网络，当节点不在基础设施覆盖的区域时，将允许蜂窝网络内的节点通过自组织多跳无线链路接入网络，如图 8-5 所示。在这两种情况下，节点接入服务供应商，应该为它们从供应商那里得到的服务付费。在文献 Salem et al.（2003）里，设计出几个针对这些网络中计费方案的攻击：

1）拒绝付费：源节点会对执行过的列入账单的通信抵赖。

2）不诚实的奖励：在多跳网络中，中间节点应该转发其他数据包。为了鼓励中间节点转发其他数据包而不是自私自利的，可以设计出一些奖励机制，比如给它们付费。这种情况下，一个行为不端的节点会试图表现得参与转发了一些数据包，尽管它并没有转发。

3）搭便车（Free Riding）：在源节点和目的节点之间路由上的中间节点，为避免缴费，可以在正进行的通信中加挂它们的数据包。例如，路由节点 *A* 会把要传给路由节点 *B* 的数据包加挂在从源节点到目的地节点的数据包上，如图 8-5 所示。

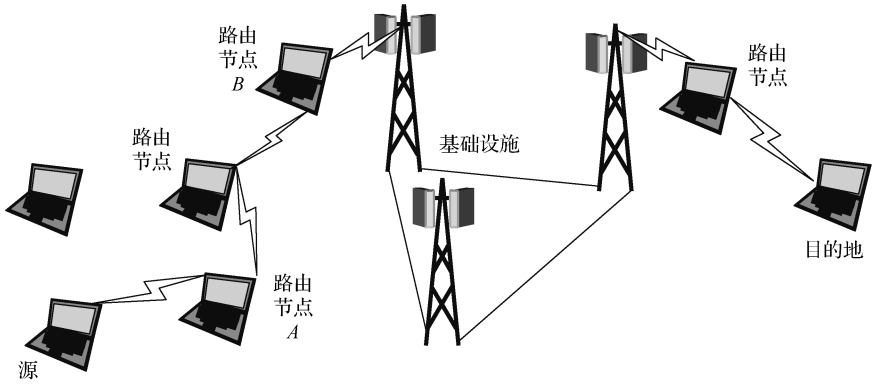


图 8-5　多跳蜂窝网络

8.2　攻击者

对攻击者也可根据很多标准分类。我们对攻击者的分类是基于图 8-6 所示的特征：发射、位置、数量、动机、合理性和移动性。首先，一个攻击者可能是主动的，也可能是被动的；这与攻击的分类是匹配的。主动攻击者实施主动攻击，被动攻击者实施被动攻击。

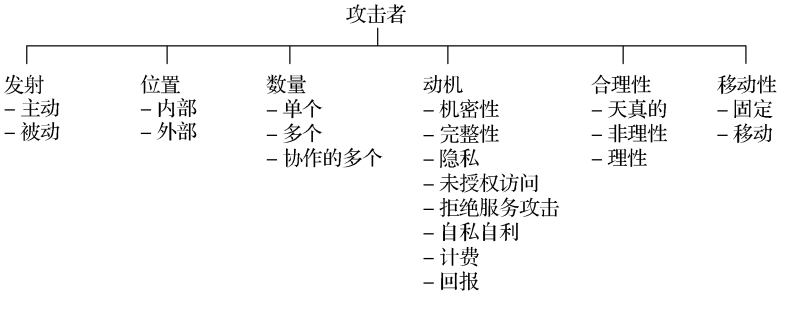


图 8-6　攻击者分类

攻击者可能是外部的，也可能是内部的。内部攻击者是一个被威胁或被收买的节点，它是被攻击网络的一部分。作为一个内部攻击者，它知道受攻击节点的所有机密信息。因此，内部攻击者会组织秘密的主动攻击。外部攻击者可能是被动的，也可能是主动的。换句话说，内部攻击者被视为网络中合法的实体，比如注册过的节点，或允许接入网络的节点。外部攻击者通常是在网络上不受欢迎的节点。

攻击者可能是单独的，也可能是不止一个。当有多个攻击者时，它们彼此合作，这种情况更难抵御。在文献 Hu et al.（2005）里，主动攻击者表示为 Active-*n*-*m*，其中 *n* 是内部攻击者节点数，*m* 是内部攻击者和外部攻击者的总数。攻击者会形成一个渐强的攻击分层结构，如下所示：

Active-0-1：攻击者只有 1 个外部节点。

Active-0-*x*：攻击者有 *x* 个外部节点。

Active-1-*x*：攻击者有 *x* 个节点，其中 1 个是内部节点。

Active-*y*-*x*：攻击者有 *x* 个节点，其中 *y* 个是内部节点。

注意：在这个组织里，所有节点代表一个单独的攻击者。因此，它们假定是合作的。

敌手会带有某种动机进行攻击，比如，破坏机密性、完整性和隐私，也可能是为了获得未授权访问的资源。攻击者也会为干扰对方运行进行攻击。自私、避免付费或不劳而获可能是另外的动机。这些已经在关于攻击那一节里解释过。

无意的失误（Needlessness）、故障节点和天真的用户也会成为网络威胁。然而，无意的失误不是那些“非理性”攻击的唯一原因，“非理性”攻击的结果可能未必抵得上攻击代价。一个攻击者实施攻击可能只是为了攻击和攻破一个安全系统，并将之视为证实他/她自身的一项挑战。理性的攻击者会为了获得一些价值大于攻击代价的东西而进行攻击。

最后，攻击者可能是固定的，也可能是移动的。检测出移动的攻击者并防御他们一般比防御一个固定的攻击者更困难。

8.3 安全目标

简而言之，安全的目标是为防御本章解释的所有威胁提供安全服务。安全服务包括以下几个方面：

1）认证：确保连接的另一端或包的发送者是其宣称的那个节点。

2）访问控制：阻止对资源的未授权访问。

3）机密性：在消息中保护整体内容或一个字段。为了防止敌手进行流量分析，也会要求机密性。

4）隐私：阻止敌手获得可能含有私密内容的信息。敌手可能会通过流量模式

分析来获得私密信息，例如频率、源节点、路由等。

5）完整性：确保数据包在传输中不被篡改。

6）授权：授权另一个节点，使其更新信息（引入授权）或接收信息（输出授权）。典型地，像认证和完整性等其他服务也会用在授权中。

7）匿名性：隐藏包或数据帧的来源。这会有助于保护数据机密性和隐私的服务。

8）不可否认性：证明数据包的来源。在认证时，源节点证明了它的身份。不可否认性可防止信号源否认其发送过数据包。

9）新鲜性：确保一个恶意节点不会再发送已捕获到的数据包。

10）可用性：主要针对拒绝服务攻击，它是维持网络功能，不会由于安全威胁而导致任何中断的能力。

11）抗攻击性：当一部分节点被攻击或被破坏时，要求能维持网络功能。

8.4　复习题

8.1　女巫攻击和伪装攻击的区别是什么？

8.2　汇聚节点漏洞（Sink Hole）攻击、虫洞攻击、您好泛洪攻击和黑洞攻击的区别是什么？

8.3　对物理主动攻击进行分类，并讨论哪一种攻击对传感器网络更具威胁。

8.4　自组织网络还是传感器网络更容易受流量分析攻击？为什么？

8.5　如果恶意节点替换了 PSFQ 片段的序列号，会发生什么？如果用同一种方法攻击 RMST，结果会改变吗？为什么？

8.6　解释 MAC 层的行为不端攻击。

8.7　SMAC 还是 CSMA/CD 更容易受到行为不端攻击？为什么？

8.8　干扰和电磁脉冲（EMP）攻击有什么区别？

8.9　哪一个具有更大的影响：攻击时钟同步还是节点定位方案？为什么？

8.10　你认为信号源与基础设施之间（从一个传感器到基站）的路由安全方案和基础设施与终端（从一个基站到传感器）的路由方案不同吗？为什么？

8.11　分别举出两个非理性攻击者和理性攻击者的例子。你认为当针对理性攻击者和非理性攻击者设计一个安全系统时，应该有不同的考虑吗？为什么？

第9章　密　码　学

基于系统中使用的密钥数量划分，密码体制一般分为两类：对称密码体制和非对称密码体制。对称密码体制中消息发送方和接收方共同拥有一个密钥，此密钥既用于加密，也用于解密。非对称密码体制中，加密和解密用不同的密钥。

根据处理输入消息的方式不同，密码体制也可分为分组密码和流密码（或序列密码）。分组密码一次处理一“块”消息，例如明文中前64个字符一起处理，然后再处理接下来的64个字符。流密码每次分别处理一个元素，如一个字符。

本章讨论密码学基础，即对称密码体制、非对称密码体制、分组密码、流密码、哈希（Hash）函数以及在认证服务中使用的哈希链和哈希树。

9.1　对称加密

对称（也称私钥/秘密/单一）密钥密码学使用发送方和接收方共享的单一密钥（见图9-1）。它是古老的技术，也是在1976年公钥密码学公开之前唯一可用的密码技术。代换（或称替代，Substitution）和置换（Transposition，Permutation）是对称加密中的两个基本要素。代换密码分成两类：单表代换（Monoalphabetic）和多表代换（Polyalphabetic）。

单表代换密码将明文字母表映射到密文字母表，明文字母表中每个字符映射到密文字母表中的唯一字符。凯撒密码是单表代换密码的一个很好的例子。凯撒密码中，明文中每一字符被字母表移动固定位置后的一个字符替代。比如，字母表向左移动4个字符得到密文字母表，明文中的“A”被“E”替换，如例9-1所示。

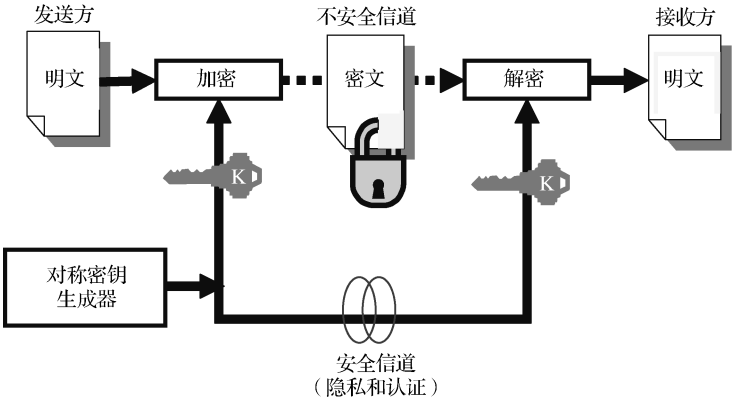


图9-1　对称密码

例 9-1

凯撒密码（左移四位）

明文字母表： ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

←——————————

循环左移 4 个字母位置

密文字母表：EFGHIJKLMNOPQRSTUVWXYZABCD

明文：HELLO WORLD

密文：LIPPS ASVPH

单表代换密码可被轻易地攻破，因而不能提供任何安全。

多表代换密码对明文中每个连续的字母，根据密钥分别使用一个单表代换密码。维吉尼亚密码（Vigenere Cipher）是多表代换密码，其中 n 个密文字母表通过对明文字母表移位建立。基于为获得密文字母表所需明文字母表的移位数，每个密文字母表用明文字母表中的一个字母表示。例如，“A”密文表对应明文字母表不移位，“B”密文表对应明文表移动 1 位。对加密而言，需要提供一个密钥。明文中第一个字母被密钥第一个字母对应的密文表中的字母替换。例如，若密钥是“SECURE”，明文第一个字母被“S”密文表中的对应字母替换，明文第二个字母被“E”密文表中的对应字母替换，如例 9-2 所示。

例 9-2

维吉尼亚密码

明文字母表： ABCDEFGHIJKLMNOPQRSTUVWXYZ

A 密文表：ABCDEFGHIJKLMNOPQRSTUVWXYZ

B 密文表：BCDEFGHIJKLMNOPQRSTUVWXYZA

C 密文表：CDEFGHIJKLMNOPQRSTUVWXYZAB

⋮

Z 密文表：ZABCDEFGHIJKLMNOPQRSTUVWXY

密钥：SECURE

明文：HELLO

密文：ZINFF

置换密码（Transposition Ciphers 或 Permutation Ciphers）通过重新排列字母顺序隐藏消息。换言之，密文保持明文所有的字母不变。例 9-3 所示的柱形置换（Columnar Transposition）是一种置换密码。

例 9-3

柱形置换密码

明文： BURN THE LETTER AFTER READING

密钥：LUCKY

密钥	L (3)	U (4)	C (1)	K (2)	Y (5)
	B	U	R	N	T
	H	E	L	E	T
	T	E	R	A	F
	T	E	R	R	E
	A	D	I	N	G

按列的方式读明文，生成密文：密钥字母给出读列的顺序。因为 C 在密钥“LUCKY”字母顺序优先级最高，所以从 C 对应的列开始读。

密文：RLRRINEARNBHTTAUEEEDTTFEG

这些基本技术的主要缺点是它们与自然语言特征（例如字频）的关联。密码需要掩盖原始明文消息的统计性质。扩散（Diffusion）和混淆（Confusion）是掩盖原始消息统计特性的两个基本手段。扩散是通过每个明文元素影响很多密文元素值，在大量的密文中消除明文的统计结构。相当于每一密文元素受很多明文元素影响。当明文中的 1bit 改变时，使得每个密文比特改变的概率是 0.5，则密码有好的扩散性质。混淆使密文的统计特性与密钥的取值之间的关系尽可能复杂化，以便阻止尝试恢复密钥的攻击。一般地，代换手段提供混淆，置换则提供扩散。

乘积密码（Product Cipher）是两个以上基本密码以最终结果或乘积的密码强度比任一密码组件更高的方式顺序执行。第二次世界大战中的转轮机曾使用过一种乘积密码，用它实现非常复杂、多变的代换密码。强度更高的密码可连续使用几个密码得到：两个代换构造一个更复杂的代换，两个置换得到一个更复杂的置换，但一个代换跟着一个置换会得到新的更强的密码。

香农（Shannon）通过两个基本要素——代换和置换引入代换-置换网络（Substitution-Permutation Networks）的思想，它们可提供消息的混淆和扩散。现代分组密码主要基于香农的可逆乘积密码的代换－置换网络概念。

对称加密的基本要素是发送者和接收者有安全信道交换秘密密钥，另外也需要一个强加密算法。即若敌手有密文、相应的明文和加密算法，它仍不能确定密钥或解密另一密文。换言之，拥有给定密文及其对应明文和加密算法的敌手不能攻破

密码。

暴力破解（Brute Force）和密码分析是破译加密算法的基本方法。暴力破解检查所有可能密钥组合，最终确定明文消息。若密钥空间非常大，这种方法会变得不实际。密码分析是一种攻击算法特征以推出特定的明文或使用过的密钥的攻击形式。若继续使用已被攻破的算法，敌手将能对所有过去和未来的（加密）消息推出明文。唯密文攻击（Cipher Text-only-attack）仅依赖对密文自身的分析、对密文应用各种统计测试。对已知明文，敌手有可能根据已知明文变换方式的知识，推出密钥。知识来自对一个或多个捕获的明文消息的分析。选择明文攻击（Chosen-plain Text-attack）中，敌手能够选择消息进行加密。因此，敌手蓄意选择精选的模式，以便发现密钥的结构。

尽管密码设计者愿意让自己的算法分析起来尽可能困难，使算法易于分析也有很多益处。即若一个算法可以进行精确的、清晰的描述，则容易分析算法的密码弱点，因而容易设计改进算法确保使其密码强度等级更高。

许多广泛使用的加密算法是对称分组乘积密码，如数据加密标准（Data Encryption Standard，DES）、三重 DES（3DES）、高级加密标准（Advanced Encryption Standard，AES）和 Rivest 密码（Rivest Cipher，RC5）。这些对称分组密码大多有类似 Feistel 密码结构，其基本密码部件顺序执行多轮，使得最终结果或乘积比任一密码部件密码强度高。Feistel 密码已证明有好的雪崩效应（Avalanche Effect），这意味着对明文或密钥一点小的改变，可导致密文产生非常大的变化。

Feistel 密码中，输入被划分成 $2n$bit 的分组（块），每一分组用密钥 K 加密，如图 9-2 所示。$2n$bit 分组中的右半部分分组，即最低 $n$bit，用函数 F 作用，并且密钥 K 作为函数的参数，然后函数 F 的结果和输入块的最高 $n$bit 进行异或运算（XOR），实现代换。接着互换输入块的最低 $n$bit 和异或运算的结果，实现置换。这是 Feistel 密码的一轮运算，同样的运算会应用 j 轮，每一轮用到上一轮的输出，如图 9-2 所示。每一轮中，新的密钥 K_i 从上一轮的密钥 K_{i-1} 衍变得到。

自从 1977 年被美国采纳为联邦信息处理标准，DES 曾是最广泛使用的加密算法。DES 几乎和图 9-2 所示的原始 Feistel 密码结构完全相同。DES 共有 16 轮处理，每一轮特定的子密钥从 56bit 长的原始密钥生成。解密密文时，应用相同的处理，只是子密钥以相反的顺序使用。DES 曾被认为是有效的加密算法，在很多应用中都有软硬件实现。然而，密钥长度是它的主要缺点。解密高手通过暴力攻击技术已攻破 DES。

3DES 对暴力攻击有更大的适应性。执行 DES 三遍，使用三个密钥（每遍执行采用不同的密钥）。用第一个密钥 K_1 加密明文，接着用第二个密钥 K_2 解密上一步的结果（即第二遍执行时，以逆序方式应用 K_2 派生的子密钥），最后用密钥 K_3 加密第二遍执行的结果。第三遍执行的结果是传给接收者的密文。解密时，应用相反的顺序。首先，密文用 K_3 解密；接着用 K_2 加密上一阶段结果；最后用 K_1 解密第二阶

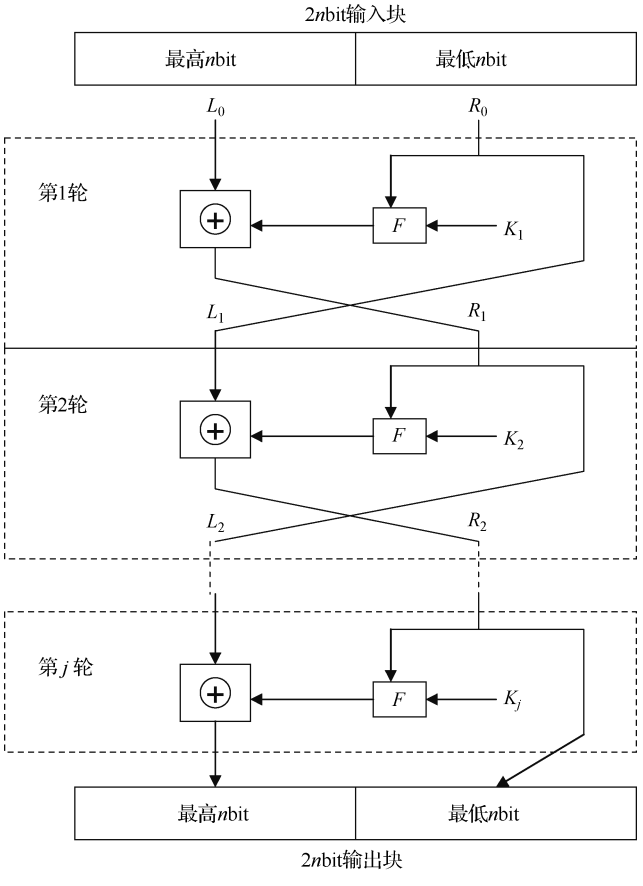


图 9-2 Feistel 密码

段执行的结果。这种方法成本低，能修补 DES 的缺点。它提供了 168bit 密钥长度，使用和 DES 一样的数据加密算法（DEA）。DEA 比其他算法经受过更多的密码攻击。因此，对 DEA 的信任级别是高的。另外，大多数广泛使用的加密硬件和软件可用于 3DES。

然而，DEA 和 3DES 也有其他弱点。首先是 64bit 的分组长度。更大的分组有益于效率和安全。其次，DEA 设计于 20 世纪 70 年代，基于当时的一般硬件，有许多算法可能更适合软件实现。因此，自从 2001 年开始，一个称为 AES 的新标准被采纳。AES 与 Feistel 密码结构有很大不同。在图 9-3 中描述了 AES 加密步骤。解密遵循相同的步骤，以逆序使用加密密钥。

对称密码学比非对称密码学实现起来更快。然而，一旦秘密密钥泄漏，通信就会受到威胁。对称密码学方法也意味着双方是对等的，因此它不能保护发送方：接收方可伪造消息并声称消息是发送方发送的。

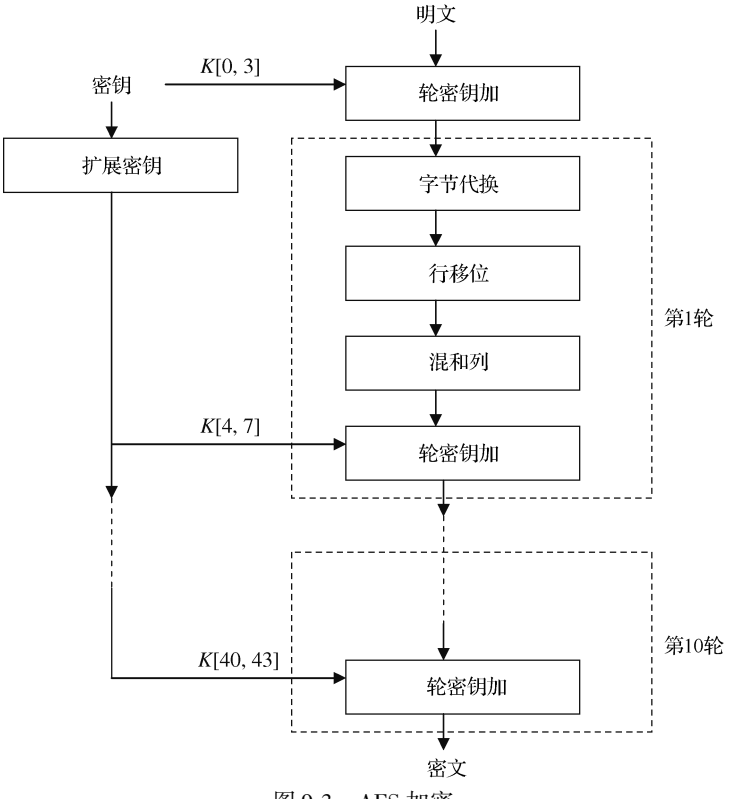


图 9-3 AES 加密

9.2 非对称加密

秘密密钥的问题是怎样通过公开网络（如因特网）实现安全交换。仅当所参与的秘密密钥仍然保密，通信才是安全的。但在公共媒介上建立安全信道传输密钥，成本高且不实用。1976 年 Diffie 和 Hellman 提出的非对称密码学（Diffie and Hellman, 1976），也称公钥密码学，为这个挑战提供了一个新思路。想法是使加密密钥和解密密钥不同，知道一个密钥并不能找到另一个密钥。下面是 Diffie 和 Hellman 给出的实现公钥密码学的必要条件：

1）一个计算容易的算法生成密钥对，即私钥 K_S 和公钥 K_P；

2）用公钥 K_P 对明文 M 加密，容易得到密文 M_C；

3）用私钥 K_S 对密文 M_C 解密，容易得到明文 M；

4）不能通过公钥 K_P 对密文 M_C 解密，得到明文 M；

5）敌手知道公钥 K_P，不能确定私钥 K_S。

有两个广泛使用的公钥密码算法：RSA 和 Diffie-Hellman 算法。例 9-4 描述了

RSA 算法（Rivest et al.，1978），RSA 是由 Ron Rivest、Adi Shamir 和 Len Adleman 提出的。

例 9-4

RSA 算法

选取公钥/私钥	例
1. 选择两个素数 p 和 q（$p \neq q$）	$p=7$，$q=13$
2. 计算 $n=pq$	$N=7\times13=91$
3. 计算 $\Omega=(p-1)(q-1)$	$\Omega=6\times12=72$
4. 选择一素数 e，$e<\Omega$	$e=5$
5. 计算 d，$de \bmod \Omega=1$	$d=29$
6. 公钥 $K_P=\{e, n\}$	$K_P=\{5, 91\}$
7. 私钥 $K_S=\{d, n\}$	$K_S=\{29, 91\}$
加密明文 M	**例**
M 必须小于 n，$M<n$	$M=2$
$M_C=M^e \bmod n$	$M_C=2^5 \bmod 91=32$
解密密文 M_C	**例**
$M=M_C^d \bmod n$	$M=32^{29} \bmod 91=2$

公钥密码学是非对称的，因为参与方不是对等的。用户的私钥保密，只有用户自己知道。用户的公钥是其他人可自由使用的。每个加密/解密过程需要至少一个公钥和一个私钥。如图 9-4 所示，公钥可用于加密信息，只有私钥拥有者可以解密。

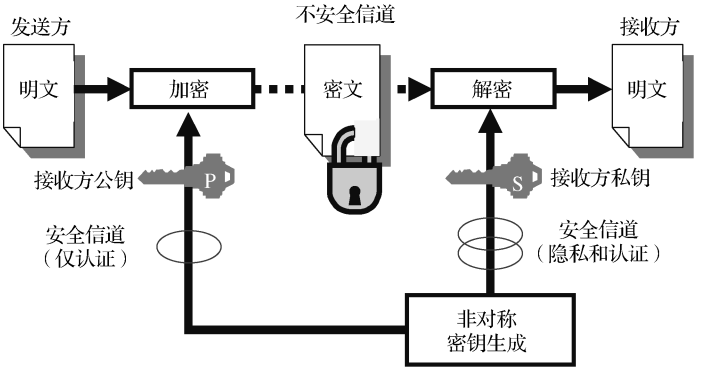


图 9-4　非对称密码

私钥可用于加密一个签名，如图9-5所示。例如，用私钥加密消息摘要，并附加在消息后作为数字签名。拥有公钥的接收方可以解密数字签名。接收者可以用相同的哈希函数生成消息摘要，并与接收到的消息摘要比较。若两者相同，可证实发送者的身份。因为只有发送者拥有私钥，才可以加密摘要，使得可以用相应的公钥解密。数字签名可用于认证（见图9-6）和非否认服务。

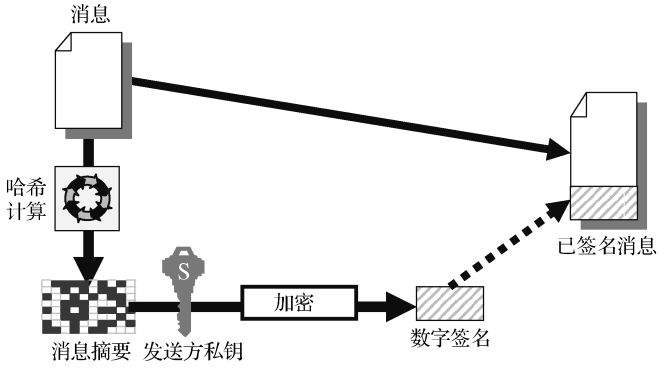


图9-5 数字签名

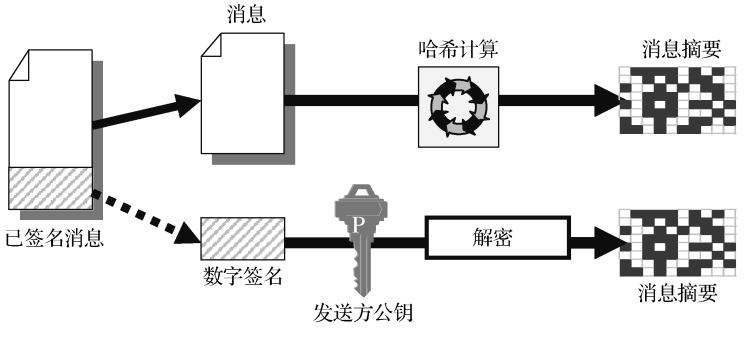


图9-6 使用数字签名的认证

认证和机密性可同时满足，如图9-7所示。当用发送者私钥对消息附加数字签名后，还可以用接收者公钥加密。因此，只有意定的接收者用私钥可以解密消息，保证了机密性；解密消息后，接收者也生成消息摘要，并与用发送者公钥解密得到的数字签名中的摘要比较。后面这一过程提供了认证和非否认。

公钥必须是真实的（可信的），尽管并不需要保密。否则，一个用户可以假冒另一个用户（例如伪装），广播一个公钥。在非对称密码学中，数字证书（或简称证书）用于提供公钥认证（见图9-8）。数字证书，包含公钥和公钥拥有者的额外信息（包括其身份标识），由认证机构（Certificate Authority，CA）创建并签发。一个实体如接收者，发送他的公钥给CA，CA返回与接收者私钥相匹配的证书。接收者通过目录（如服务器）发布证书，或把证书传给发送方。另一实体如发送方，

可用证书中的 CA 签名和 CA 公钥验证证书是 CA 创建的。发送方用证书中的公钥加密消息，接收者只有用相应的私钥才能解密。

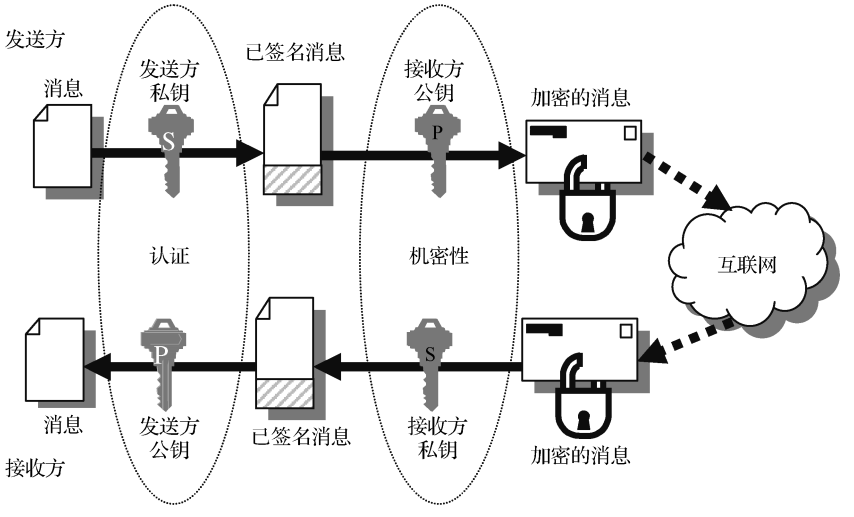


图 9-7 用公钥密码学实现认证和机密性

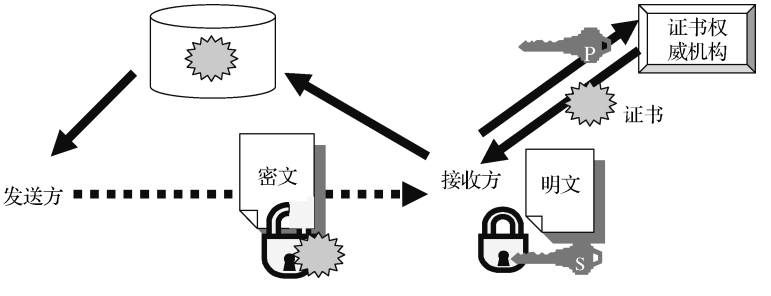


图 9-8 非对称密码学的典型应用

X. 509 是提供公钥证书认证服务的国际标准。证书存放在目录中，用户容易得到其他用户的证书。随着用户规模的增长，一个目录将不能胜任。另外，可能会有多个 CA。因此，X. 509 中，CA 按层次结构安排，同时提供了证书格式的标准。X. 509 也引入了证书撤销服务，以防证书安全受到威胁。证书撤销通过签发证书的 CA 签署的证书撤销表（Certificate Revocation List，CRL）管理。

对每个系统而言，证书管理并不是实用和负担得起的。因此，文献中提出了基于身份的加密（Identity-Based Encryption，IBE）体制[⊖]（Boneh and Franklin，2001）。

⊖ 1984 年，Shamir 首先提出基于身份密码学的概念。参见本书 10. 3. 4. 1 节“公钥方案”。——译者注

IBE 中，公钥可由任意的字符串得到，如用户 ID、角色名字、群用户名字等（见图 9-9）。私钥生成器（Private Key Generator，PKG）颁发相应的私钥。因而，IBE 消除了基于证书的公钥密码方案中必需的用大型数据库维护用户身份和相关公钥的联系，简化密钥管理、节省空间，并确保对证书库的攻击不再是威胁。这也与无证书公钥密码学（Certificateless Public Key Cryptography，CL-PKC）⊖有关。

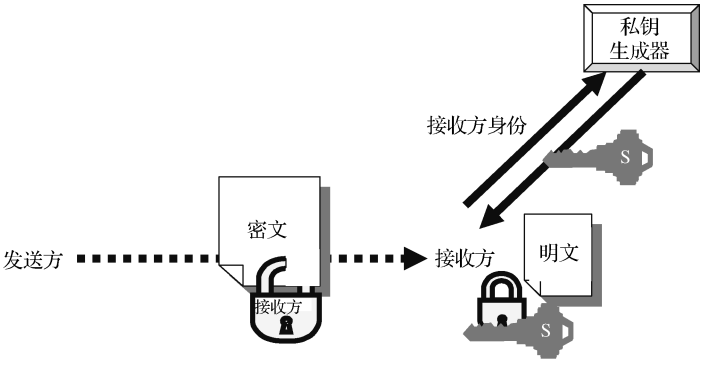


图 9-9 基于身份密码学的使用

IBE 中，公钥是任意字符串，或“身份（或称标识）”，比如姓名、角色、email 地址等。可信的私钥生成器（PKG）用主密钥从标识（IBE 公钥）中派生私钥。主密钥对于计算私钥是必需的。因此，用户间不能合谋以便获得其他用户的私钥。用户（节点）从 PKG 获得私钥。若一个节点给另一节点发送消息，它用接收者的标识加密消息。接收者用 PKG 为自己生成的私钥解密消息。这样，安全通信得以实现。基于身份的密码学（Identity-Based Cryptography，IBC）的一个主要问题是用户必须完全信任由 PKG 生成的私钥。

公钥密码学（PKC）引入了在公共信道上进行安全通信的手段。非对称加密存在的一个问题是实现速度比对称加密慢，对加密和解密，它比对称密码学需要更多的处理能力。因此，非对称密码学是对称密码学的补充而不是取代。PKC 最常见的应用是与对称加密组合使用，PKC 常用于协商一个秘密密钥，秘密密钥接着用于对称加密。

⊖ 无证书公钥密码学（CL-PKC）是介于基于证书的和基于身份的公钥密码体制之间的一种体制。CL-PKC 体系中，密钥生成中心（KGC）用自己的主密钥和用户提供的身份生成用户的部分私钥，用户选择秘密信息和得到的部分私钥结合，得到自己的私钥（用户私钥对 KGC 是保密的）。参见 S. S. Al－Riyami，K. G. Paterson. Certificateless Public Key Cryptography. Advances in Cryptography-ASIACRYPT 2003，LNCS 2894，Springer-Verlag，2003：452-473——译者注

9.3 哈希函数和消息认证码

一个密码学中的哈希函数基于运行单向压缩函数，使得从任意大小的数据块压缩到长度为 n 的固定输出。这一般通过运行许多轮运算实现，输出的长度 n 意味着哈希函数提供的安全等级。哈希函数应该容易计算，是人们共知的，并且使软/硬件实现更实际。哈希函数也应具有下列附加属性：

1）单向性：给定消息 M 的哈希值 $H=h(M)$，找到消息 M 是计算不可行的。

2）弱抗碰撞性：对任意给定的消息 M，找到 $M' \neq M$，并且 $h(M') = h(M)$，是计算不可行的。

3）强抗碰撞性：找到任意对 (M, M')，使得 $h(M') = h(M)$ 是计算不可行的。

哈希函数将输入视为 $n$bit 块的序列，每次处理一块，重复进行。例 9-5 描述了一个简单哈希函数。注意到独立于输入数据的长度，此哈希函数总是生成一个 $n$bit 的值。

例 9-5

使用逐比特异或运算的简单哈希函数

$$C_i = C_{1i} \oplus C_{2i} \oplus C_{3i} \oplus \cdots \oplus C_{mi}$$

输入流：　　111001010111000101010101100010

哈希值长度 $n=6$

块 1：1　1　1　0　0　1

块 2：0　1　0　1　1　1

块 3：0　0　0　1　0　1

块 4：0　1　0　1　0　1

块 5：1　0　0　0　1　0

值：　0　1　1　1　0　0

哈希函数可使用分组密码或模运算作为压缩函数。然而，因为密钥-子密钥处理过程使用分组密码，所以效率较低。大多数人的注意焦点是专用哈希函数如消息摘要（Message Digest，MD）系列 MD2、MD4 和 MD5，安全哈希算法（Secure Hash Algorithm，SHA）系列 SHA-0、SHA-1、SHA-256、SHA-384 和 SHA-512，RIPEMD（RACE Integrity Primitives Evaluation Message Digest）系列 RIPEMD、RIPEMD-128 和 RIPEMD-160，以及其他的如 HAVAL 和 Whirlpool。MD5 仅对数据处理一遍，生成 128bit 的摘要。已多次证实 MD5 不能满足抗碰撞性质。2006 年，公开了用简单的便携计算机，在几分钟内发现 MD5 摘要碰撞的算法（Klima，2006）。

例9-6描述的SHA-1是替代SHA-0的安全哈希算法，广泛应用在很多密码系统中。如例9-6所示，SHA-1以512bit块为单位处理数据，需要四轮运算。每轮20步，特定于某轮的一个函数如F、一个常量如K，作用于消息摘要缓冲区中的值。SHA-1产生长度为160bit的消息摘要。

例9-6

SHA-1

符号：∨ 逻辑或运算

∧ 逻辑与运算

! 逻辑反

⊕ 逻辑异或运算

← 逐比特循环左移

| 附加

输入预处理

为输入消息追加比特“1”

为输入消息填充k比特“0”，$k \geqslant 0$，最终消息长度是填充后消息的长度为512bit的某一倍数减64bit。在预处理前按比特填充消息，作为64bit big-endian整数。

初始化消息摘要缓冲区

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

以512bit块为单位处理消息，直到消息末尾。

消息摘要缓冲区赋值

A = H0

B = H1

C = H2

D = H3

E = H4

块拆成32bit的16个字，即

$w[i]$，$0 \leqslant i \leqslant 15$

扩展块成80个字，即

For i from 16 to 79

w[i] = (w[i-3] ⊕ w[i-8] ⊕ w[i-14] ⊕ w[i-16]) ← 1

第1轮

K = 0X5A827999

For i from 0 to 19

F = (B ∧ C) ∨ (! B ∧ D)　　（存在可替代的函数）

T = (a ← 5) + f + E + K + w[i]

E = D

D = C

C = B ← 30

B = A

A = T

第2轮

K = 0X6ED9EBA1

For i from 20 to 39

F = B ⊕ C ⊕ D

T = (a ← 5) + f + E + K + w[i]

E = D

D = C

C = B ← 30

B = A

A = T

第3轮

K = 0X8F1BBCDC

For i from 40 to 59

F = (B ∧ C) ∨ (B ∧ D) ∨ (C ∧ D)　　(存在可替代的函数)
T = (a←5) + f + E + K + w[i]
E = D
D = C

C = B←30

B = A
A = T

第4轮

K = 0XCA62C1D6
For i from 60 to 79

F = B ⊕ C ⊕ D

T = (a←5) + f + E + K + w[i]
E = D
D = C

C = B←30

B = A
A = T

这个块的哈希结果加到消息缓冲区

H0 = H0 + A
H1 = H1 + B
H2 = H2 + C
H3 = H3 + D
H4 = H4 + E

当所有消息处理结束，输出消息摘要（MD）

MD = H0 | H1 | H2 | H3 | H4

一个如SHA-1的哈希函数从两个固定长度的输入产生一个固定长度的输出。输

出长度一般与其中一个输入的长度相同。SHA-1 中，用于消息摘要缓冲区初始化的值的总长度是 160bit，输出也是 160bit，这与另一输入的长度（至少 512bit）无关。因此，这类哈希函数也称为压缩函数，可以将大的输入变换到短的、固定长度的输出。

哈希函数提供了数据完整性手段。对消息 M，计算哈希值 $H=h(M)$，并与消息一起发送。若接收者对接收的消息 M'，用相同的哈希函数 h 计算的哈希值 $H'=h(M')$不同于与 M 一起发送的 H，接收者必须接受 M' 是 M 的修改版。这里，H 称为消息完整性码（Message Integrity Code，MIC），应该加密传输，作为消息完整性的一种可靠度量。

另一方面，在压缩过程中使用私钥作为输入的消息认证码（Message Authentication Code，MAC）不需要加密。MAC 算法的一个例子是哈希消息认证码（HMAC）。设计 HMAC，使其能使用任何其他可用的哈希函数，如 MD5 或 SHA-1。HMAC 的设计目标如下：

1）使用任意可用的哈希函数；

2）容易替换旧的哈希函数；

3）除了使用的哈希函数的计算代价外，带来的计算代价可忽略；

4）对认证强度提供清晰的密码分析。

图 9-10 所示的 HMAC 结构，密钥首先在左端用 0 填充，变成 $b$bit 长。填充的

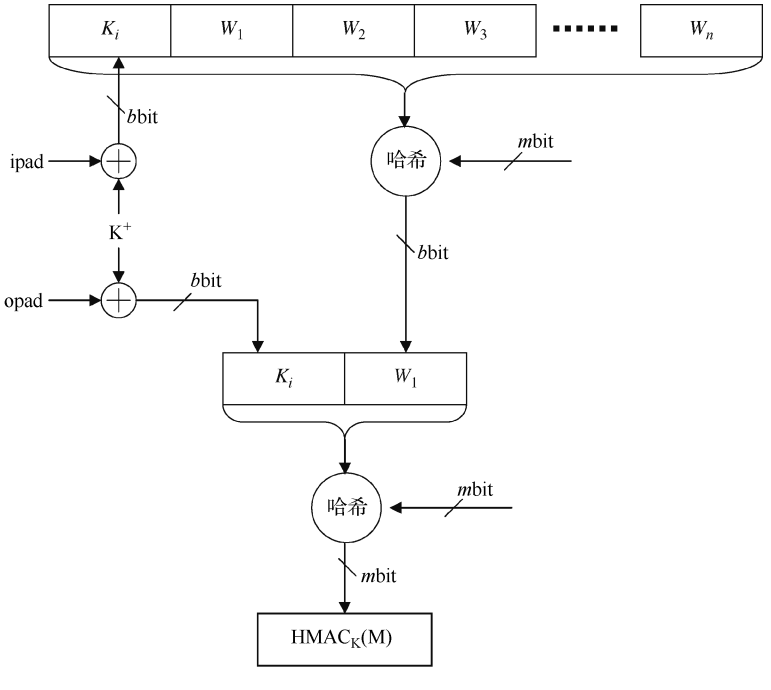


图 9-10　HMAC

密钥 K^+ 与 ipad 进行异或运算，其中 ipad 是 00110110 重复 b/8 次。运算结果填充到消息中。得到所选择哈希函数的输入。第二轮，K^+ 与另一常量 opad 进行异或运算，opad 是 01011100 重复 b/8 次。运算结果追加到第一轮的输出中。最终的比特流再应用一次哈希运算，产生 $m$bit 的消息认证码。

总之，有三种方式产生 MAC：

1）用密码学哈希函数生成 MIC，并附加在用对称加密算法加密的消息后，这提供了完整性和认证。

2）用类似 HMAC 的结构生成 MAC，并附加在传输的消息后，这也提供了完整性和认证。

3）用密码学哈希函数生成 MIC，并附加在用非对称加密算法（如数字签名）加密的消息后。除了提供完整性和认证，这种方式也保证了不可否认性。

9.4 层叠哈希

层叠哈希包括合成多个哈希函数为一个哈希函数，目的通常是提高安全性。假定哈希函数 h 和 g，一个自然的构造是 $H=(h(M)\mid g(M))$，将两个 $n$bit 的哈希函数转变成 $2n$bit 的哈希函数。然而，这种简单构造并不能提供更多的安全。层叠哈希有更多的安全方法，如哈希链和哈希树。

9.4.1 哈希链

哈希链通过对字符串 M 重复应用哈希函数 h 生成。图 9-11 给出长度为 3 的哈希链。

$$\begin{aligned} X_2 &= h(M) \\ X_1 &= h(h(M)) = h^2(M) \\ X_0 &= h(h(h(M))) = h^3(M) \end{aligned} \tag{9-1}$$

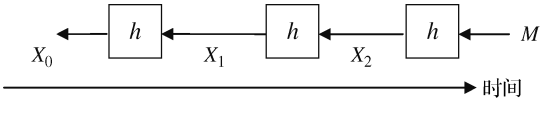


图 9-11 长度为 3 的哈希链

发送者可逆序使用这个哈希链进行认证。接收者最初存储 X_0。随后，发送者释放 X_1，接收者可通过 $h(X_1)=X_0$ 验证 X_1。类似地，通过释放哈希链中后面的哈希值，其余的信息可得到验证。这一方法在 TESLA 定时高效流容忍损耗认证（Timed Efficient Stream Loss-tolerant Authentication，TESLA）中被采用，用于广播或组播消息的认证。本章后面会详细讨论 TESLA。

9.4.2 哈希树

哈希树由 Ralph Merkle 提出，也称为 Merkle 树。哈希树是关于哈希值的树，其中叶节点是数据块（如文件中的数据块或文件集）的哈希值。树中更深的节点是它们子节点的哈希值。在图 9-12 中，H_0是对 $H_{0,0}$和 $H_{0,1}$哈希的结果：

$$H_0 = h(H_{0,0} \mid H_{0,1}) \qquad (9\text{-}2)$$

哈希树常用二叉树实现，即每一节点有两个子节点。然而，每一节点也允许有更多的子节点。通常，密码哈希函数如 SHA-1 或 Whirlpool 用于哈希运算。哈希树最顶层有一个顶哈希（Top Hash）或称根哈希（Root Hash）、主哈希（Master Hash）。

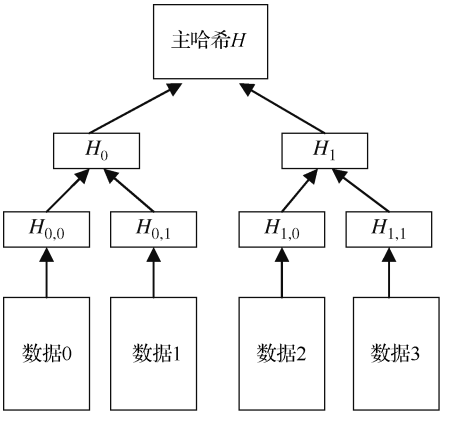


图 9-12 高度为 3 的哈希树

哈希树的一个主要应用是对 P2P 网络下载的文件进行认证。通过 P2P 网络下载前，从可信源获取文件的主哈希。接着，从任一不可信源（如 P2P 网络中的任一对等实体）可得到哈希树。用可信的主哈希验证得到的哈希树。若哈希树被破坏或是伪造的，尝试从另一信息源得到另一个哈希树，直到程序找到一个哈希树与主哈希匹配。

每次当哈希树的一个分支被下载时，即使完整的哈希树还没得到，也可立即验证每一分支的完整性。这会成为一种优势，因为分割文件成小的数据块更有效，使得若文件在传输时被破坏，只有小数据块需要重传。对于大文件的情况，其哈希树也相对较大。然而，一个小分支可以快速下载。分支的完整性可以得到验证，然后可以下载其他数据块。

9.4.3 定时高效流容忍损耗认证（TESLA）

广播认证协议使接收者能验证收到的数据包确实是由声称的发送者发送的。换言之，这种协议应该防止发送者假冒，使得任一接收者容易验证数据是合法发送者发出的。通过消息认证码对每一数据包进行简单关联，用共享的密钥计算校验和，可用于两方通信中的认证。但这并没有提供安全广播认证。这是因为广播网络中每个接收者拥有密钥，可用它伪造数据、假冒发送者。包括数字签名在内的非对称密码学，对满足广播认证的需求，提供有前景的功能。但是由于非对称密码学相关的计算负载、相对长的时间和高带宽需求，在实践中它并不是好的解决方案。

一个替代方法是仍用消息认证码和对称密码学为消息广播提供认证，但由发送者延迟泄漏密钥。在 Perrig et al.（2000a）、Perrig and Tygar（2003）文献中，定时

高效流容忍损耗认证（TESLA）属于这类方案。进一步，它被提交作为多播源认证技术的因特网工程任务组（IETF）草案（Perrig et al. , 2000b；2003）。

TESLA 方法中，发送方广播的每个消息包附带一个消息认证码，MAC 用私钥 k 生成，k 最初只有发送方知道。在一定的时间延迟 d 后，发送方会泄漏密钥 k 给接收方。接收方缓存收到的数据包，直到收到密钥才能对它进行认证。在特定时间延迟 d 后，发送方泄漏 k，接收方能够用 k 认证缓存的数据包。每个数据包附带一个单独的消息认证码而足够提供认证。这种方法需要发送方和接收方时钟同步。

TESLA 中，单向密钥链用于提供认证。单向密钥链通过对一个初始密钥重复使用相同的单向哈希函数生成。例如，在图 9-13 中，发送者随机选择 k_n，并重复应用单向哈希函数 h 生成密钥链；然后，发送者提交 k_0 给接收者。通过初始密钥 k_0，以相反的顺序泄漏值，发送者可以验证密钥链中任一元素。

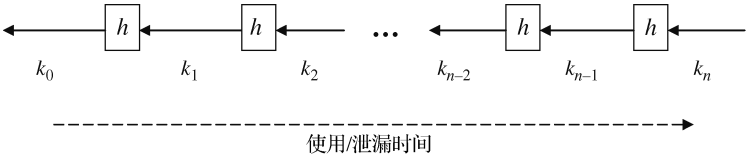


图 9-13 单向哈希密钥链的生成和使用

TESLA 包括四个阶段：发送者创建、接收者创建、消息广播、接收者消息认证。

发送者创建阶段，发送者首先划分时间为时间间隔，从单向哈希链中给每个时间间隔赋予一个密钥。通过下式计算单向密钥链：

$$K_n = F(K_{n+1}) \tag{9-3}$$

式中，F 是单向函数。单向密钥链发送到网络，按生成时的逆序方式使用。发送者定义泄漏时间间隔 d，在间隔时间 d 后，值会被发布。

接收者创建阶段，接收者与发送者保持松散的时钟同步。通过认证信道，接收者从发送方获得密钥泄漏时间表。密钥泄漏时间表包括间隔持续时间、开始时间、间隔索引、单向密钥链长度、密钥泄漏延迟 d 和发给密钥链 K_i 的密钥。

在发送者和接收者创建阶段后，发送者广播消息。其步骤如图 9-14 所示。通过密钥 K_i，利用单向函数 F'得到生成 MAC 的密钥 K'_i。发送者每次广播消息时，附加上由与消息广播的时间段对应的密钥生成的 MAC。时间延迟 d 之后，发送者广播相关的单向链值。消息应该包括以下字段：

$$P_j = \{M_j \| \mathrm{MAC}(K'_i, M_j) \| K_{i-d}\} \tag{9-4}$$

当接收者收到包时，通过比较收到包的时间和发送者泄漏密钥的时间，接收者首先检查用于计算 MAC 的密钥仍是秘密的。若 MAC 密钥仍是秘密的，接收者给包缓存。当接收者收到包的密钥时，首先验证密钥，接着用密钥验证在泄漏密钥时间

间隔中发送的缓存包。若 MAC 值正确，接收者接受包。

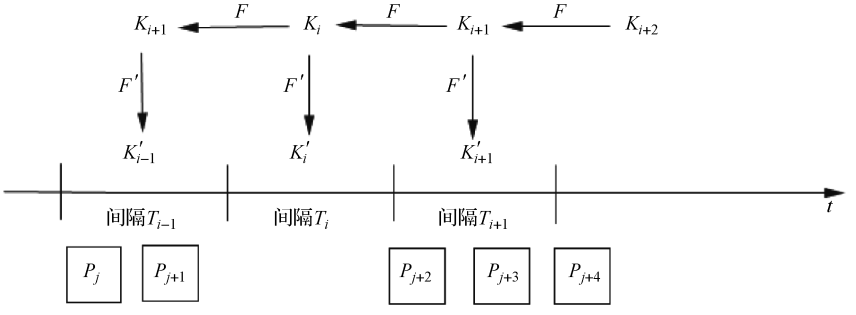


图 9-14　发送认证包

TESLA 最初为广播认证设计，需要发送者和接收者之间的松散时钟同步。因为它需要数字签名认证初始数据包、需要在内存中存储密钥链，所以应用在节点只有有限资源的传感器网络中是不实际的。第 13 章会介绍 μTESLA。

9.5　复习题

9.1　对称加密中用的基本技术是什么？

9.2　用于攻击对称加密的主要方法是什么？

9.3　对称加密的缺点是什么？

9.4　下面的密文是用凯撒密码的结果，找出对应的明文。

KNSIRJ

9.5　一个间谍使用乘积密码：加密由一个行置换密码和凯撒密码组成，密钥在住宅地址里，住宅电话是行置换密码的密钥，住宅号是凯撒密码的密钥。根据预定计划，今天的密钥与电话簿中的 John Smith 有关：

John Smith，Lagårdsveien 3，4010 Stavanger 电话：51 63 47 82

今天给间谍的消息是：

HSQQD XHDRP YFKWV HNHDL OULLQ DDWVW BDWWA RJULS

这个消息的明文是什么？

9.6　用非对称加密如何同时满足认证和机密性？

9.7　基于身份的加密体制如何工作？它的优势是什么？

9.8　用 RSA 算法，对 $p=17$、$q=11$ 生成公钥和私钥。用生成的密钥加密 52，并解密所得结果。

9.9　哈希函数所需的特性是什么？

9.10　消息认证码和数字签名的区别是什么？讨论两者彼此的优缺点。

9.11 什么是哈希链？如何使用？

9.12 什么是哈希树？如何使用？

9.13 TESLA 如何工作？它的优势是什么？

9.14 为什么 TESLA 不适于无线传感器网络？对可使 TESLA 适用于无线传感器网络的技术进行讨论。

第 10 章　挑战和方案：基本问题

无线自组织网络和无线传感器网络相关的安全挑战有很多，我们已在第 7 章中介绍过。相比于有向媒介（Guided Media），无线媒介可以公开接入、相对可靠性较低，且没有明显的物理边界。攻击者不需要打破任何物理边界来接入无线媒介，并且可以从各个地点和方向接入网络。另外，安全建立更多的复杂因素来自拓扑结构的动态变化、取决于为网络连通性的节点之间的协作、基础设施的低信任度和清晰的防卫边界的缺乏。由于自组织网络没有一个固定的基础设施和集中化的管理，用于一般受限网络（Tethered Networks）的保护机制不能够直接用于无线自组织网络和无线传感器网络。

在一个安全的无线自组织传感器网络中，节点由网络进行授权，并且只有被授权的节点才被允许访问使用网络资源。建立这样一个网络的一般步骤包括自举（Bootstrapping）、预认证、网络安全关联建立、认证、行为监控和安全关联撤销。

在这几部分中，认证是最为重要的，同时是网络安全中最基本的一项服务。其他的基本安全服务例如机密性、数据完整性和不可抵赖性取决于认证。秘密信息只有在节点进行互相验证和确认后才能进行交换。

自举（通常简称为 Booting）是网络中的节点对网络中的所有或者其他某些节点的存在情况进行认知的阶段。在自举阶段，所有想要加入网络的节点必须获取相应的识别证书（Identifying Credential），来证明它们有资格接入这个受保护的网络。识别证书的形式可以是某种节点所拥有或者节点所知道的东西。举例来说，这种证书也许是某种全球化网络的密钥或者信任节点的更新列表。在自举完成之后，网络就应该做好准备接受任何一个拥有有效证书的节点的接入。接入的节点必须向网络出示自己的证书，来证明自己有资格接入受保护的资源或者使用所提供的服务。

所有的节点都必须共享识别证书来向其他节点证明自己的身份。这种最初的证书交换叫做预认证（Pre-authentication）。一旦证书得到了验证，这些节点就一起建立了网络安全关联。而这些网络安全关联就变成了网络中进一步的授权证明。网络中的节点可以通过对称密钥、公钥对、哈希密钥链承诺或者一些上下文相关的信息安全地关联起来。安全关联会在一段经过预先商议的时间之后失效，同时也可以在过期后重新商定持续时间。节点间的通信现在就可以通过使用安全关联来进行认证。

通过使用安全关联，节点可以被认证，之后节点的行为可以被网络监控，这样就可以发现威胁节点和行为不端节点。如果网络发现某个节点已经被敌手胁迫，节

点就会通过被撤销网络关联或者拒绝其重建关联请求的方式将网络隔离。在大多数情况下，网络安全关联的建立和撤销是在网络密钥分配及交换和管理下实现的。

10.1　自组织网络自举安全

在自举阶段，网络中的节点将意识到在它们附近的节点或者整个网络中的节点的存在。无线自组织网络为这一个阶段引入了新的挑战。无线自组织网络的一个重要特征是缺少一个集中式安全基础设施。为了保护网络的安全，第一步就是要在自举阶段建立起一个节点之间的安全基础设施。可信的基础设施应该满足只有合法的节点才能加入网络的需求；新的可能加入网络的节点可以和已经存在于网络中的节点形成一个安全关联；可信基础设施可以在不知道网络拓扑结构的情况下建立起来；证书验证方案应该足够强，以抵御拒绝服务攻击，同时应该不需要非常多计算能力和存储资源。

为了建立这样一个可信基础设施，可以使用先前的相关环境（Prior Context）。如果节点在网络部署之前就已经有共享的先前相关环境，它们就可以使用这一信息进入网络。例如，若节点在相同的可信环境中发起，密钥可以进行预分配。然而，这种假设并不总是实际的。

可信第三方也可以促进这样一个基础设施的建立。可信第三方可以是认证机构（CA），也可以是某个基站或者某个指定的节点。网络中的所有节点必须认同可信第三方。另外，可信服务在网络中是集中的。因此，如果网络中存在一个类似于基站的中心稳定节点，这种节点就可以转变成一个可信第三方节点。然而，这对于大多数的自组织环境并不适用，在自组织环境下，节点是分散的，并且不存在自然形成的集中的可信候选者。

实际情况下，在无线自组织网络中，网络的拓扑结构变化非常快，因此很难形成一个可信的先前相关环境或者可信第三方。对于自组织网络来说，它可以更好地自组织一个可信基础设施，这是因为自组织网络没有特殊节点、没有基础设施、没有集中配置节点，也没有共享的先前相关环境。然而，在许多提出的协议中，经常需要带外认证通信信道。例如，在 Balfanz 等（2002）文献中，使用一种特许的旁信道进行公共信息交换，帮助节点执行用于自组织无线网络中自举安全通信的预认证协议。基于身份的安全方案是达到这一目标的另外一种手段。由用户提供的防篡改硬件令牌用于建立密钥也是一种可选方案。

10.2　传感器网络自举安全

无线传感器网络的特点如有限的电池能量和缺乏基础设施等，使得它们比传统

的自组织网络更加容易受到攻击。除了那些在传统自组织网络中介绍的自举挑战之外，以下列出的是无线传感器网络中面临的挑战（Chan et al.，2003）：

1）对节点捕获的适应性：在很多部署场景中，传感器节点都是很容易被捕获的目标。如果某个节点被捕获，对传感器节点的物理攻击有可能泄漏内存中的秘密信息。对节点捕获的适应性应该是安全系统的一个部分。此外，安全系统应该有足够的适应能力使未被捕获节点和被捕获节点之间的通信不受到威胁。

2）抵抗节点复制：通过节点捕获或者渗透，敌手就有可能获得能够复制某个合法节点的秘密信息，并进而通过对整个网络繁殖（Populating）克隆的节点直到数量上超过合法节点，从而获得整个网络的控制权。

3）撤销节点：某个行为不端的节点一旦被检测到之后，应该动态地从系统中移除。

4）可扩展性：随着网络中节点数目的增多，上面提到的安全特性可能会变弱。针对传感器网络的安全机制，应该能够容纳大量的传感器，并允许新的传感器接入网络。

5）存储和能量使用效率：安全机制应该含有少的长期和动态存储需求，低计算需求和更低的通信需求。

对于自举来说，某个传感器节点可以以最低输出功率水平（Minimum Output Power Level）开始工作，并发送一个“Hello”消息，以发现周边地区的邻居节点。之后，它可以增加输出功率水平来发现其他节点，这些节点是不在使用最小传输功率时的范围内的。这种操作可以随着逐次提高传输功率来重复进行，直到发现了特定数量的邻居节点或者是达到了最大传输功率水平。Subramanian and Katz（2000）文献中应用了另一种相似的策略，称为增量呼叫（Incremental Shouting）。在第 5 章中介绍的 LEACH（Heinzelman et al.，2000）也可以被理解为一种自举的方法，在这种方法中，节点可以声明自己是基于某一特定概率的簇头，节点将访问距离自己最近的宣布为簇头的节点。这些技术以及其他一些被提出的例如 MAC 或者路由协议可以用于发现路由节点。当它们不够安全时，就会给敌手提供引入内部攻击的机会。为了保证自举阶段的安全，密钥的分发、交换和管理起到非常重要的作用。

10.3 密钥分发、交换和管理

在一个自组织网络中，一个通信节点的可信性是至关重要的。对于安全数据交换，安全关联通常是通过设置共享证书建立起来的，例如在邻居节点之间的秘密密钥。为建立安全关联，密钥管理协议包括密钥分配协议和密钥交换协议，在自举中的作用是最重要的。在自举之后，自组织网络将进行初始化，并且可以接受任何拥有有效证书的参与者。换句话说，拥有一个有效证书成为一个新加入节点的可信赖

的证明。

从下一段开始直到 10.3 节结束为止的内容版权属于 IEEE 2006，摘引得到原作者 Hegland A M、Winjum E、Mjølsnes S F、Rong C、Kure Ø 和 Spilling P 的许可，原文参见《IEEE Communications Surveys & Tutorials》，ISSN 1553-877X，第 48 ~ 66 页，卷 8（3），第三季刊，2006。

也有其他相关的密钥管理方案综述。在 Camtepe 和 Yener（2005）文献中综述了一种无线传感器网络中的密钥分发机制。Rafaeli 和 Hutchison（2003）文献综述了对安全群组通信的密钥管理方案。关于自组织网络和无线传感器网络密钥管理协议的综述也可以在 Fokine（2002）、Djenouri 等（2005）、Law（2005）和 Merwe 等（2005）文献中找到。自组织网络密钥管理方案理想的特性有以下几点：

1）适用性（Applicability）：各种密钥管理方案专注于不同的目标。它们目标的范围可以从确立群密钥到中央管理实体的可用性。它们的适用性取决于对网络起源（规划的或真正的自组织）、网络规模、节点移动性、地理范围和人员参与所需级别等基本假设。

2）安全性：认证和入侵容忍是首要的安全考虑，确保没有未授权节点接收到随后可以用来证明自身是网络合法成员身份的密钥材料。任何人都不能为他人提供私钥或者颁发证书，除非另一方已经过了认证。入侵容忍是指系统安全不能屈从于单一的或者少数的受威胁节点。其他的重要安全问题还有信任管理和脆弱性。信任关系可能会随着网络的生命周期发生改变。系统应该能够排除受威胁节点。为了判断一个密钥管理方案的安全性，应该确认可能的漏洞。假定使用适当的密钥长度和具有足够强度的加密算法。

3）健壮性：密钥管理系统即使在出现拒绝服务攻击和不可用节点时也应该能够生存。密钥管理操作即使在出现故障节点和节点表现出拜占庭行为时也能够完成，即那些故意不遵循协议的节点。由动态群组改变引起的必需的密钥管理操作应该及时得到执行。密钥管理操作不应该要求全网范围内的严格的同步。

4）可扩展性：密钥管理操作即使在不同的节点数量和节点密度的情况下也能够及时地完成。被网络管理流量所占用的可用带宽部分应该尽可能地低。管理中的任何流量增加都会导致用于有效载荷数据的可用带宽的相应减少。因此，密钥管理协议的可扩展性极其重要。

5）简易性：关于用户友好性以及通信开销的简易性是直觉上另外应具有的，它是一个密钥管理方案成功总体上关键的因素。然而，我们认为一个安全、健壮和扩展性好的系统蕴含着简易性。在这些情况都满足的情况下，我们相信简易性是系统实现首要的和最重要的性质。

自组织网络中理想的密钥管理服务应该是简单的、在空中形成、永远不会将密钥材料泄漏或者分发给未授权的节点、保证系统安全不会屈从于少数受威胁节点，

容易允许密钥更新（Rekeying）、在节点受威胁或者密钥因为其他原因需要被取消时，能够撤销密钥，对拜占庭攻击和故障节点有鲁棒性/健壮性（Robust），具有好的可扩展性来应对预期的网络规模和节点密度，并有效管理网络分割和连接。

对路由信息签名需要一个允许一对多签名和验证的安全关联。路由消息经常进行广播，所有接收节点都应该能够检测其有效性。像邻居探测这类的消息是不会被其他节点转发的。其他的一些路由消息，例如主动（Proactive）路由协议中的拓扑信息消息以及响应（Reactive）路由协议中的路由请求和路由回复，被泛洪到整个网络中。传输节点可能不知道接收消息的节点。另外，带宽也是有限的。对每个接收者的唯一签名可扩展性差。换句话说，成对的密钥对路由信息的保护不是好的选择。

10.3.1 标准

迄今为止，已有的移动自组织网络（Mobile Ad hoc Network，MANET）因特网草案和 RFC 尚没有一个包含密钥管理。其他的标准，IEEE 802.11 无线局域网的安全修正标准 IEEE 802.11i（ANSI/IEEE，2004），假设密钥是预共享或者在固定基础设施的帮助下建立的。在真实的自组织通信情况下，预共享对称密钥是唯一的选择。IEEE 802.11i 的目的是为了保护第二层上的有效载荷（数据帧）。IEEE 组织从 2005 年已经开始研究覆盖管理帧安全的 IEEE 802.11w 标准。其他的无线通信标准包括 ZigBee（ZigBee Alliance，2004）/IEEE 802.15.4（IEEE-SA Standards Board，2003）和用于个域网的蓝牙（Bluetooth SIG，2004）规范。这些标准的前提是基于基础设施的网络，并不适用于 MANET。ZigBee 为 IEEE 802.15.4 的安全要素规定了密钥管理。ZigBee 假设初始密钥是预分配的、带外安装或者从可信中心通过空中明文接收。蓝牙中的密钥是在 PIN 码的协助下得到的。一个普通 PIN 码是希望通信的成对节点由带外输入的。

10.3.2 密钥管理方案分类

我们可以将密钥管理分为两类：分担式（Contributory），这种情况下所有的节点平等地参与密钥管理；分配式（Distributive），在这种情况下某一个簇头进行单独的密钥管理。

在分担式密钥管理方案中，每个节点都要对密钥的生成和分配做贡献。换句话说，密钥管理是基于网络中所有节点协作努力所做出的贡献。这里研究的一些分担式密钥管理方案需要依靠一个中心实体，其他的则不用。这种方法尤其适合于节点数量较少的网络，并且可以提供较强的安全性，例如密钥独立性和前向安全（Forward Secrecy）。

在分配式密钥管理方案中，每个密钥来源于一个单一节点。节点在密钥分配阶

段有可能继续合作。分配式密钥管理方案可以是集中式也可能是分布式。在后一种方式中，每个节点都生成一个密钥，并试图将它分配给其他节点。分配式密钥管理方案可能包含一个或更多可信实体，并同时包含公钥系统和对称系统。公钥方案包括传统的基于证书的和基于身份的方案。对称方案则被分为 MANET 方案或 WSN 方案。

“分担式”和“分配式”的分类很好地反映了方案中密钥的来源。密钥管理方案分类如图 10-1 所示。

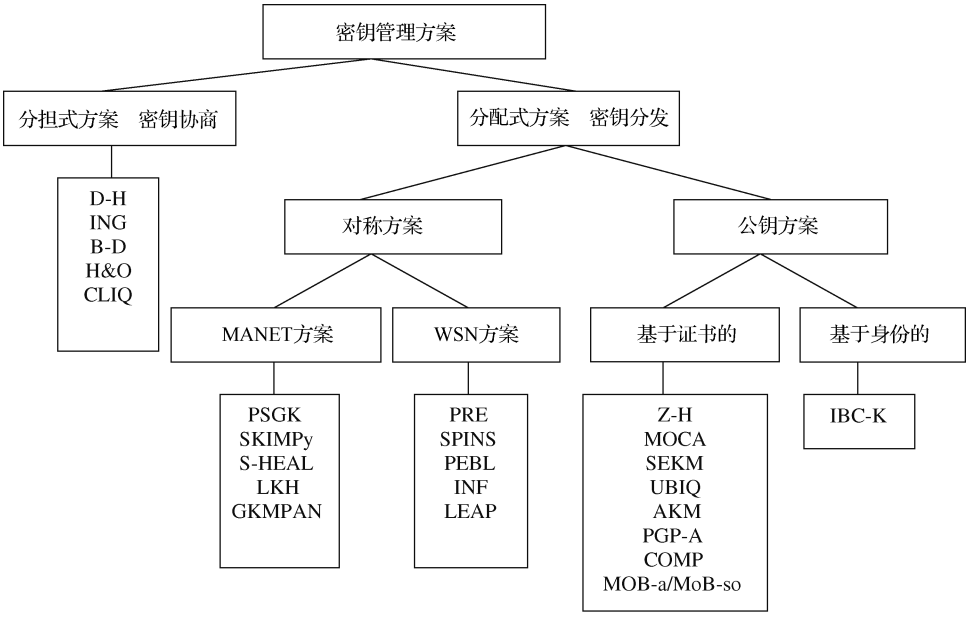


图 10-1　密钥管理方案分类

10.3.3　分担式方案

分担式方案的特点是没有负责生成和分发密码学密钥的可信第三方。取而代之，所有通信各方进行合作来建立（例如协商）一个秘密对称密钥。参与者的数量从两方（建立成对密钥）到多方（建立群密钥）不等。虽然未必是为自组织网络专门设计的，但是直观来讲，合作和自组织的分担式方法看起来符合自组织网络的本性。很大一部分的分担式方案在这部分中都进行了回顾和评价。这些方案中只有一种是为自组织网络特别设计的。

10.3.3.1　Diffie-Hellman（D－H）

D-H（Diffie and Hellman，1976）建立了一种两方之间的唯一的对称密钥。它基于离散对数（Discrete Log，DL）问题；在给出 $g^S \bmod p$ 的情况下，求 S 是困难的。

图 10-2 中给出 D-H 算法框架。双方协商使用一个大素数 p 和一个生成元 g。

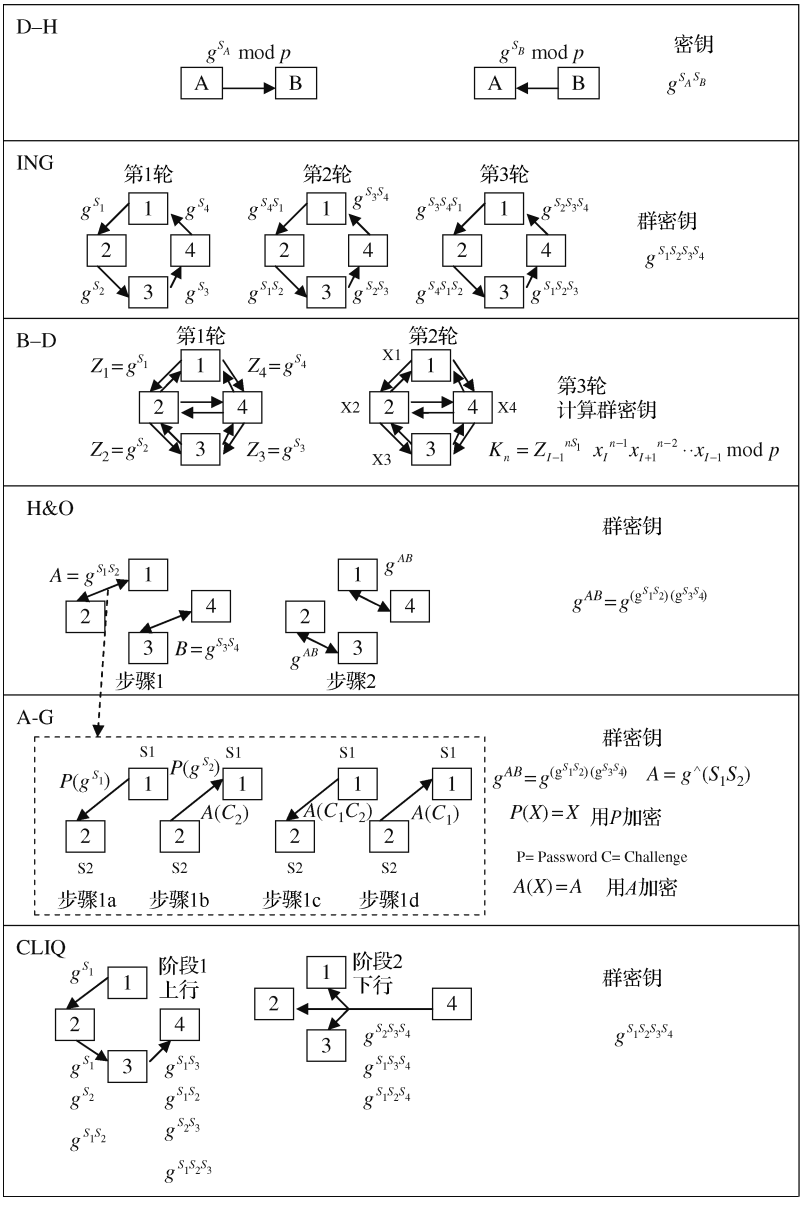


图 10-2 分担式方案概览（生成元 g 的所有指数都是模素数 p 运算）

每个参与者随机选取一个秘密 S_A 和 S_B，并传输公开值 $g^{S_A} \bmod p$ 和 $g^{S_B} \bmod p$，如图 10-2 所示。对另一方接收的数用自身的密钥做幂运算，得到一个只有两方共享的公共密钥 $g^{S_A S_B} \bmod p$。

和任何使用成对唯一密钥的方案一样，D－H 算法提供了入侵容忍（Intrusion Tolerance）能力。某个被捕获节点只威胁到了与它进行通信的对等实体共享的密钥。遇到拜占庭攻击的节点和故障节点基本上只能干扰它们和通信对等实体间的密钥建立。D-H 算法容易受到中间人攻击（Man-In-the Middle，MIM）。由节点来判断相信谁。但是由于缺少认证，Alice 就不能确定她是否真正和 Bob 进行通信而非 Charlie。

一般的 D-H 方案不适于保护自组织网络中的路由信息。它只适用于两个实体之间。使用成对密钥对路由消息的保护，要求对每个可能的接收者有不同的签名，这种方法的可扩展性很差。在 D-H 方案的基础上，大多数的分担式方案都在寻找补救 D-H 算法易受中间人攻击的缺点，以及多于两个实体的可扩展性。

10.3.3.2　Ingemarsson，Tang 和 Wong（ING）

ING（Ingemarsson et al.，1982）通过将两方参与的 D-H 方案扩展为 n 个参加者，提供了一个对称群密钥。图 10-2 给出了四个节点的原理。所有节点被排列成一个逻辑环。在经过 $n-1$ 轮之后，每个节点都可以计算秘密密钥。每一轮中包含了来自节点的一次幂运算，同时每个节点必须将自己的秘密份额传输给逻辑环中的下一节点，如图 10-2 所示。

ING 缺少认证，并且容易受到中间人攻击。它的可扩展性很差，通信复杂性和节点数目的二次方成正比。拜占庭行为或者故障节点可能会阻止成功的密钥建立。出现被捕获节点意味着群密钥受到了威胁，并有必要进行一次密钥更新。方案中并没有说明如何检测受威胁节点。节点在密钥协商阶段组成一个逻辑环的要求，使得 ING 不适用于自组织网络。用于保护路由信息的密钥的确立，意味着只能形成单跳邻居（所有在直接传输范围内的节点）之间的逻辑环。由于存在移动节点和不稳定的链路，ING 是否能够成功地完成需要探究。

10.3.3.3　Burmester 和 Desmedt（B-D）

B-D（Burnester and Desmedt，1994）算法试图建立一个群密钥。它基于离散对数问题。但是，与其他这里所介绍的分担式方案相反，它并不是基于 D－H 算法的。一个有四个节点的 B-D 算法框架如图 10-2 所示。B-D 算法通过三轮完成。每个节点选择一个秘密值 S_i，然后将它的公共值 $Z_i = g^{S_i}$，通过多播发送给组群中的其他所有节点。在第二轮中，每个节点计算并多播一个新的公共值。这个值是通过下一个节点收到的公共值除以逻辑环中前一个节点接收到的公共值，得到的结果再用自己的密钥 S_i 进行幂运算所得到的，如图 10-2 所示。在第三轮即最后一轮中，每个节点通过自己的秘密值和从前几轮中所有其他节点接收到的信息来计算会议密钥。

B-D 算法因为在三轮内就可以完成而明显要比 ING 算法更加有效。然而，每一轮中都需要进行大量幂指数运算和可靠多播。可靠多播在受限网络中很难实现，而

在自组织网络中实现更具有挑战性。群成员的变化要求重新启动密钥协商过程。在存在移动节点的自组织网络中，就可能因此而永远无法使用 B-D 算法建立一个群密钥，也不可能解决随后的群成员变化的问题。群组的变化肯定会引起延时和分裂。B-D 算法同样需要依靠一个已经在工作的路由协议或者单跳邻居，例如密钥协商方案取决于一个已经建成的路由基础设施，但是基础设施在密钥创建完成之前无法建立。B-D 算法的公共值认证（图 10-2 中未给出）可以借助于预分配公钥实现。信任是通过证书颁发者来进行管理的。这就意味着一个有规划的网络和基本密钥管理问题回归到了公钥方案上。

10.3.3.4 Hypercube 和 Octopus（H&O）

H&O（Becker andWille，1998）通过把节点整理成超立方体的方法，即一个 d 维立方体，将 ING 方案中的轮数和幂指数运算从 n 减少到了 d（$n = 2^d$）。图 10-2 举例说明了网络中拥有四个（2^2）节点的 H&O 算法。在第一步中，节点 1 和 2 执行一次 D-H 密钥协商协议。节点 3 和 4 也进行同样的操作。在第一步中建立的对称密钥是第二步中新的 D-H 密钥协商协议的秘密值：节点 1 和节点 4 执行一次 D－H 密钥协商协议，同时节点 2 和 3 也同样执行一次 D-H 密钥协商协议。H&O 算法实际上包括两个协议：Hypercube 和 Octopus。Hypercube 假设参与者的数量是 2 的幂次。Octopus 将 Hypercube 扩展为允许任意数量的节点。

H&O 算法由于缺乏认证而易受到中间人攻击。拜占庭攻击或者故障节点可能会阻止密钥协商成功进行。群成员变化需要密钥更新（Rekeying）。何时进行密钥更新将由节点来决定。和 B-D 以及 ING 一样，H&O 取决于一个底层通信系统来为所有的群成员提供一致的节点次序视图（Node-ordering View）。除了在节点动态进入和离开时保持节点次序的一致性较为困难外，它还意味着需要一个已经在工作中（不受保护的）的路由协议或者仅仅单跳邻居。后者的可扩展性非常差。总之，H&O 并不适合自组织网络的网络层安全。

10.3.3.5 口令认证密钥协议（A-G）

A-G（Asokan and Ginzboorg，2000）是唯一一种特意考虑应用于自组织网络而设计的分担式系统。A-G 算法基本上是 H&O 算法加上口令认证扩展，如图 10-2 所示。它假设所有的合法参与者会接收到一个离线口令（写在会议大厅黑板或通过另一个场所受限信道分发）。节点必须在 H&O 协议的偶对 D-H 密钥协商阶段证明自己拥有口令，如图 10-2 所示。图中给出了两个节点之间的口令认证密钥协商。口令用于加密公共值和一个挑战应答协议中的初始挑战，如图 10-2 所示。

A-G 相比于 H&O 成倍地增加了消息数量，并增加了计算复杂性。它以可扩展性为代价弥补了 H&O 对于中间人攻击的脆弱性。A-G 继承了 H&O 在已建立的通信基础设施和节点次序方案可靠性方面的不足。因此，它并不适用于移动自组织网络中的网络层安全。

10.3.3.6　CLIQUES（CLIQ）

CLIQ（Steiner et al.，1998；2000）如图 10-2 描述。它是一般 D-H 协议的扩展，用于支持动态的群组操作。CLIQ 区分初始密钥协商（Initial Key Agreement，IKA）和辅助密钥协商（Auxiliary Key Agreement，AKA）。IKA 在群组形成时发生。AKA 处理随后的所有密钥协商操作。在两种情况下，用于同步密钥协商程序的群控制器（Group Controller）是必需的。

图 10-2 中给出了四个节点的 IKA 协议。第一步（上行阶段）开始于节点 1，它将选取一个秘密指数 S_1，并将 g^{S_1} 单播给下一节点。节点 2 选取一个秘密指数 S_2，并将图中所示的值单播给节点 3。这一过程将重复一直到达最终节点——群控制器。群控制器就可以计算秘密群密钥，例如，生成元 g 进行群组中所有节点的秘密指数次幂的运算。在第 2 步中（下行阶段），群控制器将多播群组中的其他每个节点计算秘密群密钥所需的中间值，如图 10-2 所示。

AKA（图 10-2 中未给出）和 IKA 都依赖于群控制器。因此 CLIQ 的群控制器代表了单点失效（Single Point of Failure）。每次的 AKA 操作导致生成一个和所有先前的密钥相独立的新的群密钥。使用 AKA 来添加一个新的成员基本上是对有一个节点的 IKA 协议的第一阶段的扩展。群控制器的角色可以是固定的或者不定的。允许任何一个节点成为群控制器会使得系统容易受到恶意节点的攻击。CLIQ 忽略了认证。设计者们将注意力放在群变化上，而不考虑例如认证这类的安全性质，他们认为认证容易加入到方案中。CLIQ 的其他主要缺点和 B-D 一样，是取决于可靠多播和节点次序一致性视图的可用性。由于存在可变的连接性，IKA 和 AKA 是否能够成功地完成是有争论的。由于存在不稳定链路、高速移动节点和快速分割及接入，可能导致不稳定性。

10.3.3.7　其他分担式方案

已经提出大量基于已分配密钥的密钥协商方案。因此基本的密钥管理问题回归到初始密钥的分配上。还有很多方案也是不适合网络层安全的两方协议，因此留待进一步深入讨论。这样的例子包括基于传统公钥的 MQV（Certicom Corp.，2004）、基于身份的公钥方案，例如 Chen 和 Kudla（2003）和 Wang（2005）文献，还有在 Cagalj et al.（2006）中提出的基于 D-H 算法的协议。

10.3.3.8　分担式密钥管理方案总结

自组织网络中的各种类型分担式方案的主要内涵和局限性都已通过本节讨论的方案进行了说明。虽然分担式方法乍看上去也许符合自组织网络中的自组织特性，但是没有一种分担式方案是自组织网络密钥管理的好的候选方案。D-H、ING 和 H&O 因为缺乏认证，所以可以略过。它们容易受到中间人攻击。B-D 和 CLIQ 可以被排除，无论它们是否包含了认证方案，因为它们由于取决于可靠多播而存在内在的可存活问题。由于取决于节点次序和在群变化时所有节点的可用性，A-G 在可扩

展性和健壮性方面表现不佳。

10.3.4 分配式方案

分配式方案包含一个或多个可信实体，同时包括公钥系统和对称系统。真正的自组织网络需要在网络初始化阶段能够临场建立起可信实体。分配式方案分为对称密钥方案和公钥方案。

10.3.4.1 公钥方案

基于证书的公钥方案需要公钥以允许接收节点能够验证密钥材料的真实性的方式分发。有线网络的解决办法是使用公钥基础设施（Public Key Infrastructure，PKI），在这种设施中使用集中的认证机构（CA）颁发证书，用于绑定那些发送给特定用户和节点的公钥。

如果节点被怀疑落入坏人之手或者节点因为其他原因要被移除时，它的证书将被撤销。被撤销的证书将被加入到证书撤销列表（Certificate Revocation List，CRL）。认证机构的签名保证了证书和证书撤销列表的真实性。假设一个集中的可信实体不适合自组织网络，在这里不能一直保证自始至终的可用性，为自组织网络提出的密钥管理方案（包括基于证书的 PKI）提倡用各种方式分散 CA 功能。简单的认证机构复制的直观办法由于有差的入侵容忍问题而被认为不够理想。随着越来越多的节点拥有私有 CA 密钥，这使得它受到威胁的风险更高。

1. 部分分布式门限 CA 方案（Z-H）

Z-H（Zhou and Haas，1999）假设了一个 PKI 系统，并提出一个架构来为自组织网络提供可用的、入侵容忍的和健壮的 CA 功能。私有 CA 密钥是通过一个（k，n）秘密共享方案（Shamir，1979）分布在一个服务器节点集中。这个私有 CA 密钥由 n 个节点以这种方式共享，即需要至少 k 个节点合作才能恢复密钥。得到私有 CA 密钥 S 等同于给定次数为 $k-1$ 的多项式 $f(x)$ 和 k 个值 $f(1)$，$f(2)$，...，$f(k)$，求 $f(0)$。

当询问时，每个服务器通过使用它们共享在门限签名方案（Desmedt，1994）中的私钥生成证书的部分签名。另外有一个服务器扮演合成器（Combiner）的角色来收集这些部分签名，并生成一个有效的签名证书。

Z-H 建议通过更新秘密份额来对付移动敌手，例如敌手暂时威胁一个服务器而之后攻击下一个。先应式秘密共享（Proactive Secret Sharing）方案（Herzberg et al.，1995）允许份额持有者（Shareholders）通过合作周期性地更新其份额。因此敌手要想威胁到系统就必须首先威胁多于 t 个秘密份额。原始的秘密信息将不会被改变，改变的只是服务器所拥有的秘密份额。[记住同态性质：如果（s_1，s_2，...，s_n）是 S 的（k，n）分享，并且（a_1，a_2，...，a_n）是 A 的（k，n）分享，那么（s_1+a_1，s_2+a_2，...，s_n+a_n）是 $S+A$ 的一个秘密分享（Zhu et al.，2005）。] 选

择 $A=0$，得到 S 的一个新的分享。这一方案通过可验证秘密分享（Pedersen，1991）对丢失和错误的秘密份额具有健壮性：不需要泄漏份额，额外的公共信息可以证实每个份额的正确性。

虽然没有明确的陈述，但是系统依赖于一个中心可信庄家（Dealer）来引导完成密钥管理服务，决定哪一个节点将扮演服务器的角色。Z-H 假定一个基础的（不安全的）路由协议。

根据 Zhou 和 Haas（1999）所提出的方案，节点在 CA 服务不可用的情况下，不能得到其他节点的当前公钥或者和其他节点进行安全通信。然而，每个节点都应该拥有一个自身证书的备份。对于网络层安全，直接从通信对等实体（或者其他邻居节点）接收证书将会更加有效。如果需要使用证书来验证路由信息签名，有问题的节点必须是可用的；否则就不需要再去验证它的路由信息了。因此，联机 CA 接入的需求是受限的。每个节点必须联系 CA，以获得它们最初的证书（同时接收 CA 的公钥），如果节点因为某种原因丢失了私钥或者它的证书被撤销，节点同样要这样做。然而，要得到一个新的证书，节点就必须接受 CA 服务的认证——这使得节点和 CA 服务之间的某种物理接触成为必需。证书更新需要 CA 服务。像一些紧急事件和救援行动的情况下，最好确保证书在准备阶段就已经更新而不是在网络运转阶段更新。

CA 服务在证书撤销列表的撤销和发布阶段要被使用到。Z-H 算法假设不再可信的或离开网络的节点的公钥应该被废除。在一个自组织网络中要判断一个节点是否真正离开了网络是很困难的。由于暂时的失去连接而撤销节点是不明智的。更重要的是撤销属于被捕获节点的密钥。用于紧急事件和救援行动网络的这种撤销操作频率将被预期在一个很低的水平。

周期性的秘密份额更新意味着某种形式的同步。同步在自组织网络中是消耗带宽，同时也是困难的。服务器节点和证书交换之间的管理数据流同样非常消耗带宽资源，并使得 Z-H 算法的可扩展性很差。单个 CA 或者分层 CA 证实可能要比 Z-H 方法好。交叉证书在各自域内的高效发布将是一个有待进一步研究的问题。更新 CA 私钥和公钥对，并确保告知每个节点，并不是一件容易的事情。

2. MOCA

MOCA（Yi and Kravets，2002a；2002b）基本上是 Z-H 方案（Zhou and Haas，1999）的一个扩展。它主要关注节点和服务器节点之间的分布式 CA 服务和通信——即移动认证机构（MObile Certificate Authorities，MOCA）。然而由于 Z-H 没有规定如何选择 CA 服务器，MOCA 方案建议表现出最好的物理安全性和计算资源的节点应该作为移动认证机构。MOCA 方案此外还将 Z-H 的合成器函数从 CA 服务器端移到了请求端节点。这样做的好处是节点不再取决于 CA 服务器节点的可用性来合成部分证书签名，从而减少了方案的易受攻击性。

一个 MOCA 认证协议 MP，是用于提供客户端和 MOCA 之间的高效和有效通信的。根据 MP，证书请求应该基于刷新路由条目信息或短距离，单播到 β 个特定的有可能接入的 MOCA。根据（k，n）门限方案，需要 k 个 MOCA 来完成一次认证服务。为了增加接收到至少 k 个响应的概率：$\beta = k + \alpha$。当可用性丢失时，协议将变成泛洪（和 Z-H 方案中一样）。这里假设 MP 能够维护它自身的路由表，同时和一个“标准的”自组织路由协议共存。

3. 安全和高效的密钥管理（SEKM）

事实上，SEKM（Wu et al.，2005）建议 MOCA 的服务器形成一个多播群组。目的是实现秘密份额和证书的高效更新。某个节点向 CA 服务器群广播一个证书请求。第一个接收到请求的服务器生成一个部分签名，并将请求转发给另外的 $k + \alpha$ 个服务器（并非真正意义上的多播）。只需要 k 个部分签名。另外的是冗余部分，以防万一出现某些签名丢失或被破坏的情况。SEKM 没有说明一个服务器如何判断它是否是第一个接收到刷新请求并开始 $k + \alpha$ 个转发。大体上，SEKM 和 MOCA 有相同的特点。所需数量的服务器依然需要联系起来，同时部分签名将会返回。

4. 普适的安全支持（UBIQ）

UBIQ（Kong et al.，2001）是一个完全的分布式门限 CA 方案。和部分分布式 CA 方案 Z-H、MOCA 和 SEKM 相似，它依赖于一个使用私有 CA 密钥的（k，n）秘密分享的门限签名系统。和部分分布式 CA 方案不同的是，所有节点都会得到私有 CA 密钥的秘密份额。一个包含 k 个单跳邻居节点的联盟形成本地 CA 功能。它不需要任何底层的路由协议——只需要保证 k 的节点密度或者更多的单跳邻居节点。移动性可以帮助找到所需要的 CA 节点的数目。UBIQ 规定了秘密份额更新。

节点在接收到有效的证书之后，将获得整个网络的信任。任何一个拥有证书的节点都可以得到一个私有 CA 密钥的秘密份额。一个新的秘密份额是通过增加从 k 个邻居节点的联盟所接收的部分份额来计算的。最初的节点在加入网络之前，从庄家接收它们的证书。这 k 个节点经过初始化之后，庄家就会被移除。由于认证服务是通过单跳邻居节点来交付的，作者建议新节点的认证可以使用一些可靠的带外物理证明方法，例如人的感知。

将 CA 服务请求限制在单跳邻居之间可以提高带宽利用率，并且有利于提高可扩展性。一个本地联盟可以决定是否允许来自不同域的节点进入网络。这样做的一个缺点就是可能需要人为参与。另外，k 的值应该慎重选择。较小的取值会降低入侵容忍能力。较大的 k 值将需要很多邻居节点。Joshi et al.（2005）建议每个节点得到更多的秘密份额，使得使用少于 k 个邻居节点也能成功。实际上，这种方案只是在减小 k 值上做出了一点贡献。分散 CA 功能推动了私钥秘密份额的可用性。任何一个能够收集到 k 个或者更多秘密份额的节点都可以重构私有 CA 密钥。和所有依赖于可信实体的公钥方案一样，在操作阶段改变 CA 私钥和公钥对是非常困

难的。

Capkun 等（2003a）文献认为，UBIQ 可能无法抵御单个节点使用多个身份的女巫攻击（Douceur, 2002）。通过新节点的离线认证和作为可信性证明的证书服务，这几乎不是实际的威胁——至少不会发生在像紧急事件和救援行动这类情况中。安全和高效的撤销操作是一个尚未解决的挑战。

5. 自主密钥管理（AKM）

AKM（Zhu et al. , 2005）提供了一种自组织和完全分布式门限 CA 方案。当网络中存在少数节点时，这个方案与 UBIQ 相类似。每个节点都会接收私有 CA 密钥的一个秘密份额。随着节点数量的增加，引入了一个密钥份额分层的概念。新的节点之后接收私有 CA 密钥的一个秘密份额。

根 CA 私钥/公钥对是一群邻居节点通过分布式可验证秘密分享自行建立起来的（Gennaro et al. , 1999）：n 个邻居节点中的每一个选择一个秘密值 S_i，并将它的秘密份额通过一个（k，n）秘密分享方案分配给其他的邻居节点。这种方法实质是一种分担式方法。然而，派生出节点单独的私钥/公钥对并不是分担式的。AKM 也因此被归类为一种分配式方案。认证过程是在离线情况下加入的。单独秘密值的和 $S = (S_1 + S_2 + S_3 + \cdots + S_n)$ 表示私有 CA 密钥。相对应的公开 CA 密钥等于 g^S（$mod\ p$ 运算）。假设节点发布了个人的公开值 g^{S_i}，那么公钥值就可以不需要泄漏私有 CA 密钥，而是通过将个人公钥值相乘而得到 $g^S = g^{S_1} * g^{S_2} * \cdots * g^{S_n}$。其原理如图 10-3 所示。

节点 $N_1 \sim N_6$ 以及它们的秘密份额 $f(N_i)$，可以看成是一个树结构的叶子。图 10-3 中的“R”是一个虚拟节点，代表私有 CA 密钥。受威胁的概率会随着更多的节点拥有私有 CA 密钥份额而增长。因此，当秘密份额所有者的数量增长到一定的程度时，所有节点就会分裂成一些更小的局部群组，并建立一个新的局部密钥。在分裂之前，节点 $N_1 \sim N_6$ 拥有私有 CA 密钥的份额 $f(N_1) \sim f(N_6)$。假设节点 $N_1 \sim N_3$ 决定形成一个新的群组，$N_4 \sim N_6$ 形成另一个新的群组，N_1 会将它自身的份额 $f(N_1)$ 中的一个秘密份额分配给新的群组中的其他节点。其他节点对各自的秘密份额也进行类似的操作。N_1、N_2 和 N_3 的新的局部秘密值等于它们份额的总和 $S' = f(N_1) + f(N_2) + f(N_3)$，如图 10-3 中虚拟节点 G 所示。

当任何一个区域中的秘密份额拥有者的数量达到指定的级别时，区域就会进行分裂。区域也会进行合并。当节点数量少于 k 个时，节点太少以至于不能提供 CA 服务。经过区域性密钥签名的证书要比经过 CA 密钥签名的证书可信度低。一个可信度高的证书需要来自不同区域节点的部分签名。这一方案假定网络是从初始化 AKM 服务的节点演化而来的。

在 AKM 中，每个节点会维护一个证书撤销列表。AKM 没有规定撤销信息的全网络传播。一个证书会在至少 k 个邻居节点发出了针对它的指控后才被撤销。从安

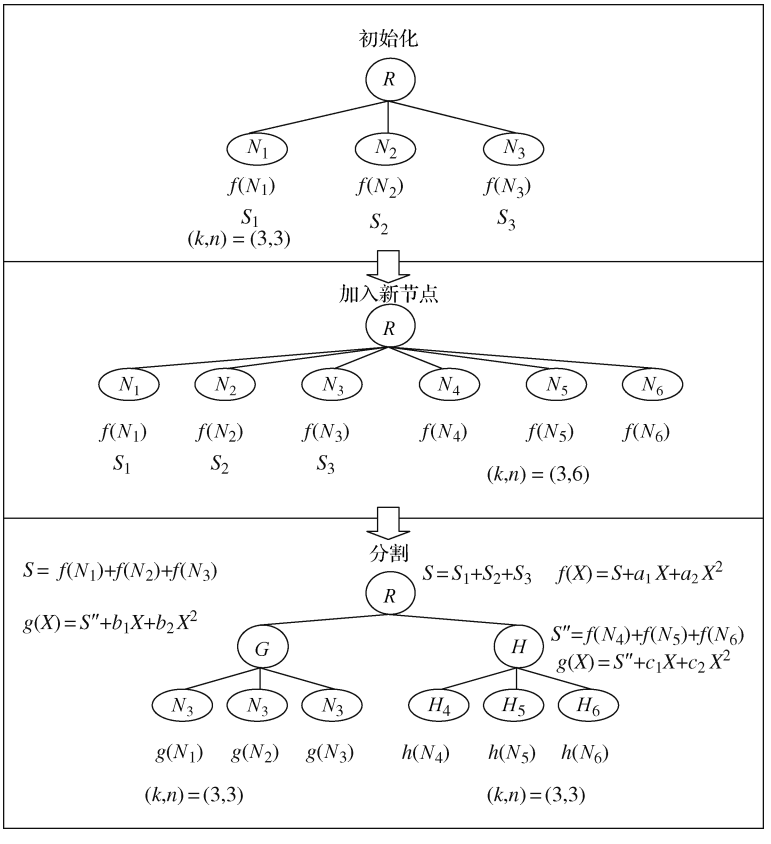


图 10-3 AKM 密钥分享原理：初始化、节点增加和区域分割（所有操作都是模素数 p 运算）

全的角度来看，私有 CA 密钥签名的证书在何种程度下才应该被只拥有私有 CA 密钥秘密份额的群组所撤销，这是有待探究的。

AKM 通过提高通信开销来提高入侵容忍。假设节点从网络的一个区域移动到另一个区域时，会和先前的区域分离，并加入新的区域。这就意味着节点必须拥有一个对密钥分层结构的视图，同时能够检测到区域边界。由于存在移动节点和不稳定链路，这种操作如何实现并不明显。这一方案要求节点在区域变化和密钥分层结构方面进行合作。拜占庭攻击或错误节点可能会造成这些操作的延迟。在一些紧急事件或者救援行动的情况下，首先需要 CA 服务发布初始证书和撤销消息，一个包含多个区域的分层 AKM 是一种对带宽的浪费。对于健壮性和可扩展性，使用单一区域较为合适。那么这种方案就等同于 UBIQ。

6. 自组织密钥管理（PGP-A）

Capkun、Buttyán 和 Hubaux（2003a）提出了一个完全的自组织密钥管理方案（PGP-A）——一种适用于自组织网络的 PGP 方案（Zimmermann，1994）。CA 的功

能被完全地散布。所有的节点都扮演同等的角色。它们生成自己的私有/公开密钥对，并向它们信任的节点发放证书。证书存储在节点中而不是进行集中地存储。PGP – A 假设信任是可以传递的，即如果 Alice 信任 Bob 而 Bob 信任 Charlie，那么 Alice 也应该信任 Charlie。节点会对它们的证书存储进行整合，并试图找出一个证书的可验证信任链。这里建议使用最大度算法建立一个高连通性的证书图，即使用户的证书存储容量很小——这样做的根据是小世界现象（假设世界上的每个人都可以通过一个很短的社会关系链建立联系）。证书的撤销是通过证书颁发者发送撤销消息或者隐式地在到期时撤销来实现的。更新操作需要和颁发者进行联系。证书也会在邻居节点之间进行周期性的交换。估算过期时间和周期性交换需要节点之间的一定程度的同步。从文献中不能明显看出这种同步性应该如何建立。

周期性的证书交换和与颁发者之间进行联系以获取证书更新，是耗费带宽和可扩展性差的。PGP-A 暗示需要一个已经正在工作的路由协议。可以通过使用旁信道进行物理接触和密钥交换来自组织地建立信任机制。然而，为了保证网络服务正常运转而进行的人为交互操作是不合适的。

拜占庭行为和错误节点都只有有限的能量来阻止其他节点进行证书交换。一个受威胁节点仅仅暴露了自身拥有的密钥。然而，受威胁节点可以被用于向其他的非法节点颁发证书，从而使这些节点获得接入网络的权利。

这里仅仅有一个可能的保证使得希望进行通信的两个实体之间建立一条信任链。另一方面，结合小世界现象的信任传递意味着每个人在不久后就会信任每一个人。这样的结果就不再具有入侵容忍。一个替代的方法是，正如文献（Yi and Kravets, 2004）中所建议的 COMP，限制最大跳数，允许节点对各种证书区分信任等级。

7. 自组织网络复合密钥管理（COMP）

COMP（Yi and Kravets, 2004）结合了 MOCA（Yi and Kravets, 2002a; 2002b）中的部分分布式门限 CA 和 PGP-A 证书链（Capkun et al. , 2003a）。它的目的是实现比 PGP-A 更高的安全性和与 MOCA 相比 CA 服务更高的可用性。已经经过 CA 验证的节点允许向其他节点颁发证书。请求证书服务的节点应该首先发送请求到 MOCA 的 CA。如果这一操作失败，它们应该搜索邻居中已经经过 CA 验证的节点。根据配置，和 CA 之间具有更长证书链的节点同样有资格向其他节点颁发证书。

COMP 中的每个证书都包含了一个信任值，反映证书颁发者对绑定节点身份和密钥的信任等级（0 = 不信任，1 = 完全信任）。信任值的增加提供了证书链中信任等级的一个度量。一般来说，习惯选择较短的证书链而不是长的证书链。信任链中的存在一个或者多个受威胁节点的可能性会随着证书链长度的增加而提高。和 PGP-A 相似，COMP 假设了信任传递性的等级。然而，对证书进行签名并验证，表明你相信一个密钥属于一个确定的身份，这并不一定意味着也信任这个身份正确地

签署其他人的证书。

信任值能够保证对信任的细粒度评估，并且节点并不需要完全信任 CA。然而，决定一个适当的信任级别是困难的。COMP 并没有说明证书颁发者应该如何做到这一点。拜占庭行为或者受威胁节点在任何情况下都可能会向不可信的节点赋予完全的信任度。然而，其入侵容忍相比于纯粹的 PGP-A 却增加了，这是由于 COMP 限定了证书链的最大长度。

离线认证通常包括人为交互，这在紧急事件和救援行动情况下是繁琐的。然而，和一个邻居节点的交互要比 UBIQ 需要包含多个邻居节点参与的要求低。同时，COMP 的可扩展性并不比 MOCA 好，这是因为节点请求 CA 服务应该首先尝试 MOCA 的 CA。另外，证书链的传输限制了可扩展性。

在 MANET 中如紧急事件和救援行动这类应用中，希望 CA 主要用于颁发和撤销证书。在救援行动中，不应该在线发生周期性的证书更新。COMP 没有提到撤销操作。发布证书的节点有权撤销它的证书是合理的。但是仅仅因为节点拥有经 CA 签名的证书，授权单一的普通节点撤销由 CA 单独颁发的证书，使得系统容易受到受威胁节点和拜占庭行为节点的攻击。允许单个节点颁发证书与分布式 CA 的目的相矛盾。

为获得初始证书搜寻经过 CA 认证的邻居节点，需要知道 CA 公钥。因此，在某时刻搜寻节点和 CA 之间必须存在一个认证信道。初始认证信道基本上是通过物理接触或者短距离的旁信道获得的。对于被要求提供 CA 服务的节点，另一个自然而然的问题是：为什么请求节点不同时通过认证信道接收其自身证书？

8. 基于移动性的密钥管理方案（MOB）

MOB（Capkun et al. , 2003b; 2006）寻求模仿人类行为：如果人们想要安全通信，他们就会互相接近对方，以交换信息。安全关联将会在接近的节点对之间建立起来。这一方案可以实现完全自组织（MOB-so）或者依赖于离线机构（MOB-a）。MOB-so 可以基于对称密钥或者公开密钥。MOB-a 本质上是基于公开密钥的。

MOB-so 和 MOB-a 之间的一个主要区别在于人为参与的级别。在 MOB-so 中，用户必须在他们建立起安全关联之前对进行通信的对等实体进行物理上的认证。这个安全证件 triplets，之后会在一个安全（短距离）旁信道中进行交换。triplets 包括用户标识符、密钥和节点地址。节点同时也会签名，并交换一条证明安全关联已经在两者间建立起来的声明。MOB-so 接受同级层的信任传递：安全关联可以在朋友（即双方彼此具有安全关联的节点）中间建立起来。MOB-a 假定进行证书预分配，并建议安全证件的交换受限于单跳邻居节点。

在 MOB-so 和 MOB-a 中，当一个节点遭到捕获时，只有特定节点所持有的密钥会受到威胁。拜占庭行为或者故障节点无法阻止其他节点交换安全证件。由 MOB-a 假定的离线权威机构意味着不存在撤销行为。作者建议受威胁节点应该撤销它们自

己的证书。然而，很难判断是否有威胁行为发生。因为怀疑而发生的撤销意味着容易受到攻击。这种情况也许是对可用性的一种威胁。此外，如果节点遭到捕获，它将不再按照协议的要求进行操作。对于 MOB-so 来说，是由用户来决定它的哪些安全关联不再有效，哪些朋友节点变成了敌对节点。

MOB 方案由于安全证件仅在单跳邻居节点之间交换，在这个意义上带宽利用是高效的。同时，它的扩展性也有限。MOB 方案需要一个很长的延时来建立所有通信实体的安全关联。这同样不适用于紧急事件和救援行动。

MOB-a 在没有证书交换限制的证书预分配方面贡献很小。根据路由协议，限制单跳邻居节点之间的证书交换可能会影响高效的网络形成。没有这种限制下的安全成就。权威机构的签名确保了证书的有效性，无论证书是从谁那里接收到的。MOB 关于任何人都不能与没有接近的实体进行安全通信的假设和 PKI 的演进产生了矛盾。

9. 基于身份的公钥（IBC-K）

Shamir 提出基于身份的密码学［Shamir（1984）］，去掉了对证书的需求。基于身份的公钥方案代表了一种新型的公钥系统。它们允许使用用户的身份例如 email 或者 IP 地址来作为公钥，这样就会使得证书变成多余。然而，还需要一个可信实体来生成和分发与各种身份对应的私钥。可信实体在撤销操作中也会用到。可信实体可以签署撤销身份的列表。与传统的公钥系统一起，已有方案提出将可信实体散布到更多的节点。

身份信息一般都很短——和拥有几千字节大小的证书相比至少是很短的。假设在路由消息中默认传输的信息可以被用作公钥，基于身份的方案可扩展性可能会比传统基于证书的方法要好。这使得基于身份的协议在带宽受限的自组织网络领域受到注意。

Shamir 构造了一个基于身份的签名方案（IBS）。要验证一个签名，只需要知道发送者的 ID 和公共系统参数。公共系统参数是由私钥生成器（PKG）在系统建立阶段定义的。公共系统参数包括 PKG 的公钥和消息空间的信息。PKG 同时也生成与用户 ID 相匹配的私有签名密钥。

图 10-4 给出了 Shamir 的 IBS 方案的草图。在创建（Set-up）阶段，PKG 选择一个秘密主密钥，并生成相对应的公共系统参数。

之后，在私钥提取（Extraction）阶段，它将颁发私钥。私钥通过 ID 和 PKG 私有主密钥唯一给定。

后来有很多 IBS 方案被提出。我们可以在 Fiat and Shamir，1987、Cha 和 Cheon，2002、Waters，2005 文献中找到一些例子。Boneh 和 Franklin（2001）文献提出了首个实用的基于身份的加密（IBE）方案。这一方案之后得到了扩展（Lynn，2002），它在没有增加任何开销的情况下提供了消息认证。密文本身被使用作为消息认证码。

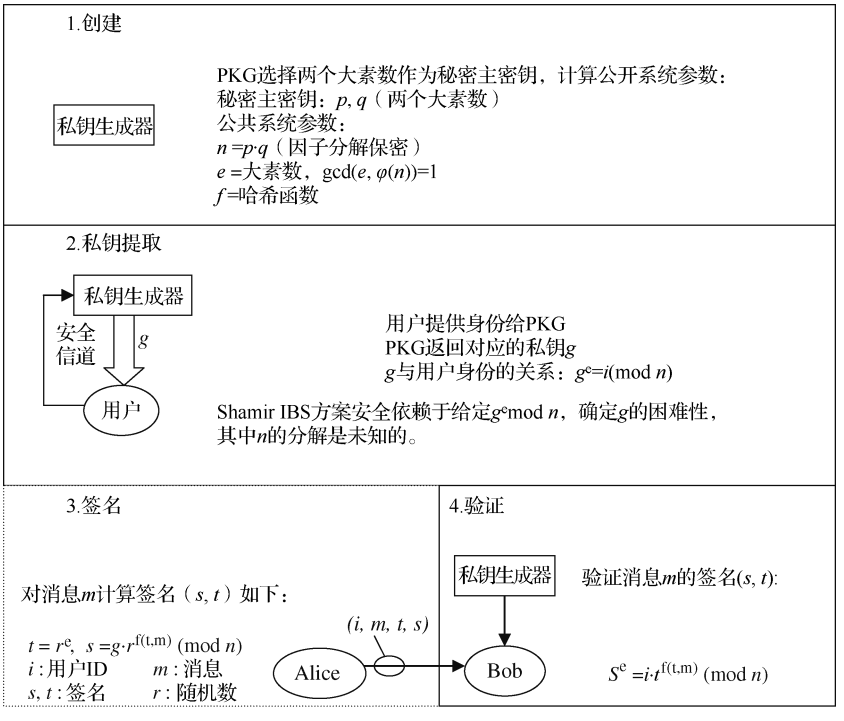


图 10-4 Shamir 提出的基于身份的签名方案（IBS）

在 Boyen（2003）文献中研究了综合基于身份的签名和加密（IBSE）方案。IBE 最新的进展包含加强的安全性。Boneh 和 Boyen（2004）提出了第一个不需要随机预言（Random Oracles）的安全模型下可证明安全的 IBE 方案。Waters（2005）则提出了一个更高效的版本。然而，IBE、IBSE 和 IBSC 方案预先假定通信是成对的。它们中没有一个可以适用于网络层一对多路由信息的签名和验证。

PKG 代表了单点失效（Single Point of Failure）。如果 PKG 的秘密主密钥受到威胁，整个系统就会受到威胁。为了防止这种情况，Boneh 和 Franklin（2001）建议使用门限密码将 PKG 主密钥分散到更多地方。

Khalili、Katz 和 Arbaugh（2003）结合基于身份的密码学和门限密码学（Desmedt，1994），提出了一种用于自组织网络的密钥管理技术（IBC-K）。初始化自组织网络的节点形成一个门限 PKG，将 PKG 秘密主密钥通过一个（k，n）门限方案扩散到最初的节点集合。这消除了 PKG 的单点失效，并增加了入侵容忍。它使得服务变得健壮，这种健壮在某种意义上是因为一个敌手为了恢复秘密主密钥，必须威胁到至少 k 个节点。同样也降低了易受攻击性，因为只要在范围内有 k 个行为正确的 PKG 节点，服务就可用。

为了接收与某些身份对应的私钥，节点必须将自己的身份发送给 n 个 PKG 节

点中的 k 个（或者更多个）。节点会接收到从它们每个节点处发来的私钥的一个份额。当拥有了 k 个正确的份额，节点就可以计算其个人私钥。

当时间不足时，许多地理位置上分布的 PKG 节点的物理交互并不是一个好的解决方案。因此，对于紧急情况和救援行动这类情形，一个单一的 PKG，例如位于现场救援管理中心，或者一个分层的 PKG（Boneh et al. , 2005），会更能满足需要。

明确的密钥撤销仍然是一个未解决的问题。这里并没有简单的方法来发布撤销列表（用于撤销 ID）和确保所有的节点都被告知。另一个可供选择的方法是改变 PKG 主密钥和系统参数。所有的私钥都源自于这些参数。实质上，PKG 密钥的更新会使得系统中的所有密钥作废。

10. 公钥方案小结

使证书交换变得多余的 IBC-K，是自组织网络的一个令人感兴趣的候选方案。然而它仍然依赖于 PKG。

10.3.4.2　对称方案

对称系统的目的在于在安全信道中分发一个或多个共享秘密。文献中的许多用于自组织网络的对称密钥管理系统有意用于无线传感器网络（WSN）。传感器节点相比于传统 MANET 节点来说只有有限的能源、内存和计算资源。对称系统也就因此成为了唯一的选择。WSN 一般包含一个基站。即 WSN 含有一定数量的基础设施，同时也因此不是真正的自组织网络。这个综述区分用于传统 MANET 和用于 WSN 的对称方案。很多 WSN 方案都被包括进来用于评估它们在传统 MANET 中的适用性。

对称密钥可以通过在线密钥分发服务器或者密钥预分配来完成。对于无线自组织网络和传感器网络，在线密钥分发服务器不能作为一个选择。

密钥预分配方案由三个阶段组成：密钥预分配、共享密钥发现和路径密钥确立。密钥服务器首先生成大量密钥形成一个密钥池，之后每个节点都会被给予由池中选择的多个不同的密钥，同时每个密钥都将被赋予一个唯一的标识符。在节点随机部署在某个区域之后，开始共享密钥发现阶段。在这一阶段，每个节点都将试图发现在它通信范围内的其他传感器，并将交换密钥标识符。如果节点发现自己和它的邻居节点共享相同的密钥，它们就可以使用这一密钥进行通信。如果节点及其邻居间没有相匹配的密钥，它将通过一个密钥路径来建立一个它们之间的秘密通信。密钥路径意味着在两个节点之间存在着一系列的节点，同时路径中每两个相邻的节点共享一个相匹配的密钥。要建立与节点 j 的一个安全路径，节点 i 需要寻找一条自身和节点 j 之间的路径，这条路径上的任意两个相邻节点拥有共同的密钥。因此，从节点 i 发出的消息就能够安全到达节点 j。

密钥预分配的方法有很多种。第一种就是主密钥预分配。在这种解决方案中，所有节点都有一个匹配的主密钥 K，同时任何一对节点可以使用这一主密钥 K，通

过一种特定算法来生成一个新的会话密钥。这一方案没有很强的弹性（Strong Resilience），这是因为如果网络中的一个节点受到了敌手的威胁，整个网络的安全性就将受到破坏。将主密钥存储于防篡改硬件能够增加密钥的安全性，但是它也会同时增加开销和能量消耗。

偶对密钥预分配（Pairwise Key Predistribution）也可以在这里使用。在这种方法中，网络中的每个节点都为网络中的其他节点携带不同的密钥，这样每对节点 N_i 和 N_j 共享一个秘密对偶密钥 K_{ij}。这对节点之后就可以使用这一共享密钥 K_{ij} 来生成用于它们之间将来通信的会话密钥。节点认证在偶对关系下也是可用的。这一方案的弹性（抗攻击性）很强，这是因为如果某个节点受到了来自敌手的威胁，其他节点的安全性将不会受到影响。这一方案的不足之处在于，如果网络中的节点数量很大，这些节点就需要很大的存储空间。另外，在网络中加入新节点将变得十分困难，这是因为已经存在的节点没有新节点的密钥。因此，这一方案的可扩展性不好。

另一种方案是随机密钥预分配。在这个方案中，每个节点在被部署在网络中之前被随机地赋予一个来自密钥池的密钥集合。每个节点就能够通过共享相同的密钥或建立路径密钥来和其他的节点进行连接。密钥发现和路径密钥建立成功概率期望为 p。一个路径密钥可能包含一跳或者多跳。这个方案具有一定的扩展性和灵活性，因为新节点容易接入网络，同时它可以在某个传感器受到威胁时提供更好的安全性。当网络中存在可供选择的安全路径时，少数受威胁节点只能造成轻微的影响。这一方案的不足之处在于，存在一定的概率使得一些节点无法找到与其他节点建立秘密连接的密钥路径。在概率为 $1-p$ 的情况下，当既没有直接共享密钥也没有发现路径密钥时，方案可能会出现连接失败。

1. 预共享群密钥（PSGK）

这是一个比较老的并且很好地被证明了的密钥管理方案，它具有一个密钥分发中心用于向群组所有成员预分配一个对称密钥。密钥分发中心也可以提供偶对唯一密钥，但是这里的焦点在于群密钥。对称群密钥可以用于对路由信息通过密码校验和——消息认证码（MAC）进行“签名”。

PSGK 缺乏入侵容忍，在某方面是因为它的安全性会被单个遭捕获的节点所危害。但如果安全策略允许，它是一个简单的解决方案。这里假定存在离线密钥分发中心和预分配密钥，方案的可扩展性好。它对于故障节点和拜占庭攻击具有免疫性。认证操作应该离线加入。由于使用单个群密钥，使得排除受威胁节点并不容易实现。

PSGK 并不是特别为自组织网络设计的。因为几种主要研究的对称方案是对这一方案的扩充，所以这部分包括 PSGK。

2. SKiMPy

SKiMPy（Puzar et al.，2005）是为 MANET 设计的。它寻求建立一个存在于整个 MANET 的对称密钥，用来保护网络层路由信息或者应用层用户数据。在 MANET 初始化时，所有节点生成一个随机的对称密钥，并将其通过单跳邻居节点使用“Hello”消息进行广播。最佳密钥，即拥有最小 ID 号码的、最新的时间戳或者其他，被选作本地群密钥。最佳密钥会通过一个在预分配证书协助下建立的安全信道传输到使用较坏密钥的节点。这个过程将会一直重复，直到所有 MANET 中的节点都共享到这个最佳密钥为止。一旦建立之后，群密钥将起到可信性证明的作用。SKiMPy 提出周期性的群密钥更新来应对密码分析。更新的密钥来源于初始群密钥。

SKiMPy 中节点在本地对最佳密钥达成一致，在这个意义上是带宽有效的。因为密钥信息只在邻居节点之间进行交换，它并不需要一个已经在运行的路由协议。SKiMPy 存在最佳密钥向所有节点传播时的延迟问题。而且，当前的本地最佳密钥可以用于安全通信，一直到接收到“最终”密钥。

拜占庭行为或者故障节点可能会干扰本地密钥协商，例如，通过宣布一个更好的密钥但并不响应。

拥有特别角色或者等级的实体可能会被授权来管理证书。然而，在线撤销操作在网络初始化之前是不可能进行的。随着网络完成初始化，对称群密钥也同时建立。一旦对称密钥已经被接收，就没有有效的方法来驱逐后来参与进网络的节点。群密钥（或者源自于群密钥的某个密钥）现在就起到可信性证明的作用。因此，SKiMPy 相比 PSGK 增加了复杂性，但并没有增加相应的安全性。

3. 自愈会话密钥分发（S-HEAL）

S-HEAL（Staddon et al.，2002）是一种带有撤销功能的对称群密钥分发方案，设计用于存在不可靠连接的网络。这一概念需要预共享秘密和一个广播当前用多项式 $h(x)$“伪装”过的群密钥值 K 的群管理者；$f(x)=h(x)+K$。独立的秘密值 $h(i)$是预分配的（i 代表节点的 ID 值）。每个成员节点之后就能够通过计算接收到的表达式（令 $x=i$），并减去秘密值，来计算出当前的密钥值：$f(i)-h(i)=K$。所有的操作都发生在一个有限域 F_q 内，这里 q 是一个比节点数目大的素数。

通过将多项式 $h(x)$替换成二元多项式 $s(x,y)$，使得撤销操作成为可能。群管理者将通过 $f(N,x)=s(N,x)+K$ 将密钥 K 进行“伪装”后，并将其进行广播。为了提取密钥，节点必须首先恢复多项式 $s(x,i)$，再计算 $s(N,i)$。之后，它就必须将得到的结果从接收到的 $s(N,x)+K$ 中减掉（令 $x=i$）；得到 $K=f(N,i)-s(N,i)$。

这一思想在于只有非撤销节点可以进行多项式 $s(x,i)$ 的恢复。给定度为 t 的多项式 s，为得到 $s(x,i)$，需要知道 $t+1$ 个值。N 值和单独的秘密值 $s(i,i)$ 是预分配的。用于计算 $s(x,i)$ 的其他 t 个值 $s(r_1,x)$，$s(r_2,x)$，…，

$s(r_t, x)$，合并进来自群管理者的密钥更新消息。如果被撤销的节点被包含在集合 $\{r_1, r_2, \cdots, r_t\}$ 中，这些节点就只能获得所需要的 $t+1$ 个值中的 t 个。因此，它们就不能提取新的群密钥。这个方案支持最大 t 个节点的撤销操作。

S-HEAL 的一个主要特点就是它的自愈特性。丢失一个或更多个密钥分配的节点依然可以泄漏丢失的密钥。每条密钥更新消息中都包含了所有先前密钥和未来可能密钥的秘密份额。在密钥分配之前和之后，节点接收到的密钥秘密份额是互补的。假设 $p(x)$ 是在密钥 K 分配之前接收到的份额，那么在密钥 K 分配之后，接收到的密钥更新消息中的份额就应该等于 $K-p(x)$。因此，丢失的密钥可以通过结合丢失更新前的份额和丢失更新后的份额衍生出来。尽管自愈这一特性对于邮件系统和相似的应用中会有很大的价值，而对于网络层路由信息只有即时的价值。因此，取回早先的密钥并没有很大价值。所以在这里略去更进一步的细节。

S－HEAL 对于为了提供初始群密钥而对可能是在多跳以外的群管理者的信赖，使得它并不适合于保护路由信息。群密钥需要用来自引导（Bootstrap）网络服务，但是 S-HEAL 需要一个已经在执行的网络服务来分发群密钥。虽然如此，S-HEAL 还是有可能用于撤销操作和密钥更新，这里可以设定一个受保护的网络服务已经被一个初始的预分配群密钥（PSGK）引导完成了。这种方式相比于单纯的 PSGK 提高了入侵容忍。Staddon 等（2002）文献指出，通过周期性的重传最新的密钥更新消息而不是等待下一个密钥更新，可以提高对于数据包损失的健壮性。

就可扩展性而言，消息的大小和密钥更新消息的数量独立于网络中的节点数。密钥更新消息的大小只和多项式的大小成比例（如果忽视了自愈情况）。

缺少来自群管理者广播的源认证是这种方案的一个缺点。一个由先前群密钥生成的消息认证码（MAC）可以很容易地添加。而且，一个拜占庭行为的节点可能潜在地传输混淆信息，声称是来自群管理者的下一个密钥，从而引发破坏。

4. 逻辑密钥分层（Logical Key Hierarchy，LKH）

群密钥可以被强制进行更新：一个密钥管理者分配新的群密钥，通过单独的密钥为每个节点进行加密。事实上，LKH 代表了改进这种暴力方法的可扩展性的一系列方案，这类方案将密钥组织成为一个逻辑分层结构，并给予节点额外密钥。

LKH 是由 Wong、Gouda 和 Lam（1998）以及 Wallner、Harder 和 Agee（1999）提出的。这一概念如图 10-5 所示。所有群成员（$N_1 \sim N_8$）都拥有群密钥 $K_{12345678}$。子群密钥 K_{1234} 由节点成员 $N_1 \sim N_4$ 共享，同时 K_{12} 由 N_1 和 N_2 共有。$K_1 \sim K_8$ 代表独立密钥。假定节点 N_8 将要被撤销，N_8 所知道的所有群和子群密钥（$K_{12345678}$、K_{5678} 和 K_{78}）都应该进行更新。节点 N_7 和 N_8 共享了所有从叶子到根的中间密钥。节点 N_7 因此必须接收通过它的独立密钥加密的更新密钥。新的群密钥和子群密钥可以通过 N_5 和 N_6 的公共密钥 K_{56} 加密后分配给它们。对于节点 $N_1 \sim N_4$，群管理者向它们发送通过 K_{1234} 加密的新的群密钥 $K_{1234567}$。因此带宽和计算开销相比于使用独立密

钥加密更新信息的方式有所节省。

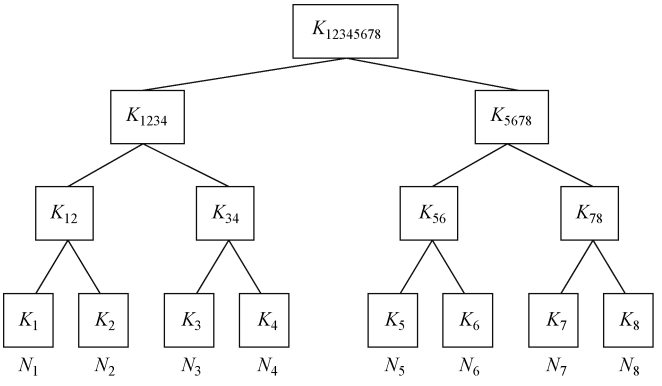


图 10-5　逻辑密钥分层

密钥树可以是二叉树或者 k 叉树，可以是平衡的或者非平衡的。

然而基本的 LKH 方案并不是为自组织网络特别设计的，Rhee、Park 和 Tsudik（2004，2005）提出了一种用于分级自组织网络的 LKH 方案。他们提出将群管理者的功能分配给多个管理者，每个控制网络中的不同单元（Cell）。这一方法是蜂窝状、基于基础设施的而非自组织网络的。节点完全依赖于单元管理者。每个单元拥有一个不同的群密钥。

节点在从一个单元向另一个单元移动时，必须联系单元管理者来接收密钥。换句话说，节点必须有能力检测到单元的边界，并在单元管理者的通信范围之内。另外，这一方案需要单元管理者在密钥从一个单元到另一单元传递时能够进行通信。这一方案的目的是为了限制密钥更新在部分网络内。这样做的代价是降低了健壮性，并提高了带宽开销。这一方案不适合于 MANET 使用。

已经提出一些其他的基于 LKH 的改进方案（Wong et al.，1998；Wallner et al.，1999），它们的焦点在于通信和计算开销。OFT（Balenson et al.，2000）、OFC（Canetti et al.，1999）、ELK（Perrig et al.，2001a）、LKH +（Balenson et al.，2000）、EBHT（Rafaeli et al.，2001）、LKH + +（Pietro et al.，2002）、Poovendran 和 Baras（1999）以及由 Selcuk、McCubbin 和 Sidhu（2000）提出的因特网草案都提出了不同的减小通信开销的方法——主要焦点在于消息大小。这些方案中，只有 LKH + +是为无线网络设计的。

ELK 通过只发送部分密钥值以及一个密钥验证值来减小密钥更新消息的大小。接收者必须通过暴力方式搜索密钥的剩余部分。验证值用来确定是否已经找到正确的密钥值。LKH + 和 EBHT 提出新的密钥可以在添加新成员时对旧的密钥应用一个单向函数。在 OFT、OFC 和 LKH + +方案中，父节点的密钥和子节点的密钥通过一个单向函数相互关联起来。在发生群变化之后，群管理者只发送足够的信息，

以确保节点能够自己计算剩余的更新密钥。Poovendran 和 Baras（1999）指出，可以通过将最有可能被撤销的节点放置于根节点附近，来减小通信开销，例如，只赋予它们一个最小数量的密钥值。类似的想法在 Selcuk 等（2000）文献中也有提及。在实际情况中，很难确定哪一个节点最有可能受到威胁。此外，在自组织网络中，消息的数量可能更具压倒性地胜过消息的大小（Winjum et al.，2005）。因此，这些提出的改进方案实际收益并不明显。需要进行一些仿真来确定哪一种方法是最好的。

LKH ++要求降低消息数量，因为一些节点可以自己计算出新的密钥。父节点的密钥和子节点的密钥通过一个单向函数相互关联起来。根据 LKH + +以及参考图 10-5，K_{12}等于 K_1的哈希值，K_{1234}代表 K_{12}的哈希值。结果，左边的子节点就能够计算它们父节点的新密钥。其他的节点从群管理者那里接收这一密钥。另外，左边的节点也需要知道必须进行密钥更新。LKH + +没有阐述这一操作如何进行。

在一个自组织网络中，每当新节点加入或者离开网络时，就进行一次密钥更新（Rekeying）是不必要和不期望的。路由信息只有实时价值。加入网络或者离开网络的节点的后向和前向安全性并不重要。然而，LKH 可能会对用于撤销目的 PSGK 的扩展有些价值。假设网络服务已经经过初始化（在预分配群密钥的协助下），LKH 可以被用于除去受威胁节点。一个足够保存所有预期成员密钥的静态树需要在这里使用，以避免添加新节点时的密钥更新。

对于自组织网络中的针对紧急事件和救援行动的撤销操作（不经常发生），健壮性要比计算和通信开销更加重要。在基本的 LKH 方案中，丢失来自群管理者更新信息的无辜节点（Innocent Nodes）将被剔除。周期性地重发最后一次更新信息能够起到帮助。在 ELK 中，群管理者发送重复的提示信息，使得丢失密钥更新信息的节点能够计算密钥。Wong 和 Lam（2000）提出密钥更新信息中的前向纠错码（Forward Error Correction Code，FEC），使得能够进行比特位错误的纠正，但无法帮助丢失整个更新信息的节点。

群管理者代表单点失效。为了可靠性和性能而对群管理者的复制（Replication）[如 Wong 等（1998）文献所提]，对于自组织网络来说，并没有很大的价值。复制需要时钟同步的服务器，同时会增加安全攻击的目标数。

仅依赖对称密钥体制方案的一般缺点是无法进行源认证。某个拜占庭行为的节点可能会假装成群管理者，并造成破坏。Wong 等（1998）提出通过数字签名进行认证。基本的密钥管理问题就回归到公钥分发的问题。

5. 概率的密钥预分配（Probabilistic Key Predistribution，PRE）

PRE（Eschenauer and Gligor，2002）假定 WSN 节点具备一个预安装的密钥环，即一个从大的密钥池中随机抽取的密钥集。当网络进行自举（Bootstrapping）时，节点将广播它们密钥环中的密钥的标识符。无线链路只有在两个节点共享一个密钥

时才建立起来。因此，对于拜占庭行为和错误节点的适应性很好。这一方案依赖一个控制节点（基站）来广播一个经过签名的将要被撤销的密钥标识符列表。

已经提出很多用于 WSN 的概率密钥预分配方案。Chan、Perrig 和 Song（2003）扩展了 Eschenauer 和 Gligor（2002）的工作，增加了对于节点捕获的适应性。这一操作需要 q 个公共密钥（$q>1$）而不是只用一个单一密钥来建立连接。Liu 和 Ning（2003a）提出通过概率预分配多项式建立 WSN 中的成对密钥。多项式秘密份额增强了对受捕获节点的适应性。一个可信实体定义一个二元多项式 $f(x, y)$，具有这一特性 $f(x, y) = f(y, x)$。秘密的多项式秘密份额 $f(i, y)$ 被预分配给每个传感器节点 i。任意两个节点 i 和 j，可以通过计算多项式值 $f(i, j)$ 和 $f(j, i)$ 来分别创建一个成对密钥。类似地，Du、Deng、Han 和 Varshney（2003）提出另外一种基于概率的预共享多项式方案来生成传感器网络中的成对密钥。Du 等（2004）提出使用部署信息来增加两个节点找到公共密钥的概率。后者可能用在传感器规划布置的 WSN 中，但在 MANET 中则行不通。

Zhu 等（2003a）提出了结合概率密钥预分配和秘密分享来在 MANET 中建立唯一的成对密钥。一个希望和另一个节点安全通信的节点需要选择一个秘密对称密钥。之后它将发送这一秘密对称密钥的份额给另一方，这一操作将使用不同的预分配密钥加密，这些份额通过不同的逻辑路径进行发送。假设使用的预分配密钥的聚合子集仅被两个有问题的节点知道，其他的节点不能从解密足够的份额来恢复秘密对称密钥。根据配置，这一方案可能会产生大量的消息。Zhu 等（2003a）声称在自组织网络中以计算代价换取通信效率是适当的。这一假设并不是普遍成立。

PRE 中使用密钥环的目的是入侵容忍，代价是可用性。对于某个节点真正和单个或者多个邻居节点共享一个密钥并能自行启动通信，只能在概率上进行保证。紧急情况和救援行动情况下，可用性是最关心的，需要一个足够大的密钥环来确保达到接近零概率失败。这样做的结果就是使得入侵容忍度降低到了和预分配群密钥（PSGK）相当的水平。这和方案的初衷相违背。网络层安全的适应性和可扩展性是有限的。各种邻居节点拥有的不同密钥意味着每个路由消息需要更多的签名。将要被泛洪的路由消息的端到端签名会被防止。

6. 传感器网络中的安全协议（SPINS）

WSN 的 SPINS 安全协议（Perrig et al. , 2002）假定在传感器节点以及基站之间预安装单独（成对）密钥。想要进行安全通信的节点向基站请求一个公共密钥。基站返回这个密钥，并用它们的单独密钥加密。这一方案需要一个已经在运行的路由协议以及基站的可靠接入。它不适用于保护传统 MANET 中的路由信息。

SPINS 也包括一个认证广播方案 μTESLA，描述了如何将其用于为传感器网络提供经认证的路由协议。μTESLA 取决于预分配承诺，即一个单向密钥链的最后一个密钥，以及延时泄漏密钥链中随后的密钥。密钥链可以通过使用一个初始随机密

钥重复进行哈希运算衍生出来。在时刻 i 使用的密钥等于时刻 $i+1$ 所使用的密钥的哈希值（或类似的单向函数）。承诺方案使得节点可以验证后来泄漏的密钥始于所声称的源。对泄漏的密钥重复进行哈希运算应该返回承诺。要发送一个认证数据包，发送者应通过一个当时是保密的密钥来计算消息认证码。接收者将信息存储起来，直到密钥之后被公布。节点必须是松散时钟同步的，并且知道密钥发布时间表。否则，敌手就可以伪造数据包，因为接收者不知道用于计算进入数据包消息认证码（MAC）的密钥是否已被公布。

SPINS 认证路由协议借助于从基站泛洪的 μTESLA 密钥发布数据包，发现从节点到基站的路由。发送者，从那里一个节点首先接收到有效的 μTESLA 数据包，将被设置为到基站的路由的父节点。预分配的承诺使得节点能够验证接收到的数据包源自基站。

这种方式可以用于从传感器节点到基站间的通信。相同的技术不能用在使用分散通信模式的传统 MANET 中。一种可能性就是给所有的节点预装载所有其他节点密钥链的承诺。这就使得所有的节点都能够认证从其他节点发送来的信息。入侵容忍会比较好，同时对拜占庭行为和故障节点的抵抗性也会很好。然而，节点必须是松散时钟同步的，并且要知道所有其他节点的密钥发布时间表。方案的灵活性很低，而且可扩展性差。另外，延时的密钥发布在移动节点和快速变化的网络拓扑情况中是有问题的。总之，SPINS 密钥管理方案和认证路由协议不适合于保护传统 MANET 中的路由信息。

7. GKMPAN

GKMPAN（Zhu et al.，2004）设计用于自组织网络中的安全多播。它以 PRE（Eschenauer and Gligor，2002）和 μTESLA（Perrig et al.，2002）为基础，基本上是 PSGK 的撤销和密钥更新方案。GKMPAN 假设一个预分配群密钥和预分配承诺。群密钥用于保护多播通信。承诺信息用于认证来自密钥服务器的撤销消息。另外，GKMPAN 假定每个节点都拥有一个预装的取自一个大密钥池的对称密钥的子集。

相比于 PRE，密钥集合中的密钥是由节点的 ID 所决定的。在撤销操作中，密钥服务器会发布一个含有要撤销节点的 ID 的撤销消息。被撤销节点密钥集中的所有密钥都应该被清除或者更新。任何节点都可以自动从 ID 区分哪个密钥被撤销。撤销消息同样会识别一个不在被撤销节点密钥集合中的密钥被用作“更新密钥”。

一个新的群密钥是通过旧的群密钥在相应的带密钥的单向函数的参与下生成的。旧的群密钥会作为数据输入，“更新密钥”会作为密钥输入。输出是新的群密钥。拥有“更新密钥”的节点可以在没有帮助的情况下计算出新的群密钥。其他的节点就会从其父节点处接收这一密钥，这一密钥会通过它们密钥集合中的一个（未被撤销的）密钥进行加密。它通过一个根节点位于密钥服务器处的多播树进行分配。撤销信息的有效性在密钥服务器稍后发布用于计算消息认证码的密钥之前无

法进行检验。

为了避免潜在的破坏行为，旧的和新的群密钥应该共存，直到所有的节点都接收到了新的群密钥。然而，要确保所有的节点都接收到了新的群密钥并不是一件容易的事情。拜占庭行为或者故障节点可能会影响有效的排除操作和密钥更新。依赖密钥服务器和时钟同步是它的另一个弱点。GKMPAN 在新的群密钥可以由节点自行计算或在本地传输方面表现尚可。另外，GKMPAN 相比于 PSGK 增加了入侵容忍，因为它使节点能够被去除。代价是可用性降低。无辜节点可能会在它们所有密钥都恰巧包含在要撤销的密钥集中时被剔除。这在紧急情况和救援行动情况下是不可接受的。

8. 安全 Pebblenets（PEBL）

Pebblenets（Basagni et al.，2001）是指大型的自组织网络，这里的节点称作 pebbles，因为它们的尺寸很小，并且数量很大，例如 WSN。PEBL 的目的是保护应用程序数据。它建立并更新一个全网络的数据流加密密钥 TEK。在网络层一个预安装的群密钥确保了一个 pebble 属于群组成员的真实性。因此 PEBL 可以被看做是 PSGK 的扩展。这里假设只有拥有群密钥的节点才能够正确地加密和解密“Hello”消息。另外，PEBL 假设 pebble 组织成为单跳邻居簇。每个簇选择一个簇头节点。所有簇头形成一个中枢，并竞争成为密钥管理者。密钥管理者可以生成数据流加密密钥 TEK，它预期被用于加密应用层数据流。TEK 从密钥管理者那里通过簇头分配给各个常规节点。它会进行周期性的更新。每次 TEK 更新之前都要进行重新聚类，并重新选择簇头。这种簇头角色的轮转是为了避免作为簇头的节点过度消耗，同时为了适应移动性。在簇形成时还是单跳邻居的节点可能已从邻居范围中移出。

不遵循协议规定的节点可能会影响簇的形成和 TEK 的更新。PEBL 没有提供对重放和入侵攻击的保护。PEBL 的安全性会因为篡改而遭受破坏。网络层的“Hello”消息和 TEK 都是由群密钥生成的密钥所保护的。任何拥有群密钥的一方都可以参与 TEK 的更新。PEBL 整体以及簇的形成和周期性的 TEK 更新，是非常消耗带宽的，需要同步性和可用性假设使得它不适合 MANET 使用。

9. 密钥影响（Key Infection，INF）

INF（Anderson et al.，2004）是为 WSN 提出的。这一方案假设静态传感器节点和大量部署。INF 在节点和它们的单跳邻居之间建立起对称密钥。这一安全性的基础令人吃惊：它基于在网络部署阶段，任何攻击者只能监听一个固定比例的通信信道的假设。在自举阶段，每个节点只生成一个对称密钥，并将其明文发送给它的邻居。在这里用到了一种叫做密钥密语（Key Whispering）的方法，即密钥最初在一个低能量级进行传输。传输能量之后会增长，直到至少一个单跳邻居节点收到了密钥，并收到回复信息。INF 是简单的、自组织的，同时对于拜占庭行为和故障节点具有健壮性。它的带宽利用率很好，同时可扩展性好。然而，它的安全性是弱的。

INF 对于密钥密语时的窃听行为的抵抗力很弱。另外，在通信双方之间没有认证。INF 的“通过惊讶的安全性”对于 MANET 来说是不可行的，其中静态节点和瞬时大量部署行不通。

10. 局部加密和认证协议（Localized Encryption and Authentication Protocol，LEAP）

LEAP（Zhu et al.，2003b）是为静态 WSN 设计的。LEAP 建议不同的密钥用于不同的目的。它需要一些预分配密钥。预分配的单独密钥（Individual Keys）用于传感器节点和基站之间的通信。采用预共享群密钥保护基站广播信息。预装的全网络的初始密钥（Initial Key）K，用来产生成对密钥（Pairwise Keys）。成对密钥用于单跳邻居间的安全通信。

紧接着部署之后邻居节点发现阶段，此时，每个节点 n 产生各自的主密钥 K_n。主密钥是节点 ID 和初始密钥的一个函数：$K_n = f_K(\mathrm{ID}_n)$。这个主密钥用于“签署”“Hello”消息。任何知道初始密钥的节点都能计算出任意其他节点 ID 的主密钥。因此，每个节点均能验证来自其邻居节点的“Hello”消息。这个节点然后会计算出与其邻居节点共享的成对密钥 v，它是主密钥和节点 ID 的一个函数：$K_{nv} = f_{Kv}(\mathrm{ID}_n)$。

在静态节点假设之下，能容忍入侵；成对密钥创建之后，网络密钥会被消除。已被消除网络密钥的节点将不再能创建成对密钥。然而，网络中仍然可以添加新节点。当新节点还没有消除群密钥时，它们可以用邻居节点建立成对密钥。当一个节点被捕获时，只有被捕获节点的密钥会受到威胁。

成对密钥用在保护普通数据安全和分配簇密钥（Cluster Keys）。使用簇密钥是为了用于安全的本地广播。任何节点仅仅产生一个簇密钥，把它用各自的成对密钥加密发送给所有邻居节点。

尽管 LEAP 可以工作在静态的传感器网络里，然而这种密钥管理方案的核心——创建成对密钥，将不能在传统的自组织网络中工作。删除初始密钥和移动节点与持续改变网络拓扑结构是不相容的。在移动自组网（MANET）评估 LEAP 的可扩展性意义不大，因为消除初始密钥后，成对密钥创建已被排除。

11. 分布式对称方案小结

我们已经对分布式对称密钥管理方案功能给出概要介绍。WSN 密钥管理方案基本上是假设节点是静态的、大量分布的、节点对基站的通信模式或者创建成对密钥。

这些方案的目标和假设使它们不适用于在拥有移动节点的传统自组织网络中保护路由信息。PSGK 或 PSGK 扩展的 S-HEAL 或用于撤销的 LKH 看起来是对称方案最有希望的替代者。

10.4 认证问题

在数据通信中，敌手很容易篡改数据，并把一些消息注入数据，这样接收者应

该确保接收到的数据来自一个合法的发送方，并且没有被篡改过。数据认证允许接收方验证数据真正是由声称的发送方发送的。这样，接收方需要确保任何决策过程用到的数据来自正确的源节点。另外，认证对网络构建的很多管理任务是必需的。数据认证在传感器网络中也是重要的。

在双方通信情况下，发送方用秘密密钥计算消息内容的校验和，产生一个消息认证码（MAC）。数据认证能被接收方验证，这个接收方拥有用于产生相同消息认证码（MAC）的共享密钥和源消息。然而在多方通信中，比如基站广播数据给一些节点时，就不能使用对称的数据认证。这种情况下，将采用非对称机制如 TESLA。在这种方法中，首先发送方用密钥产生的消息认证码（MAC）广播一个消息，这里的密钥稍后将公开。当节点收到消息时，如果它还没收到发送方透露的密钥，将首先缓存消息。当节点收到密钥以后，它将用密钥和缓存的消息产生消息认证码（MAC）来认证此消息。TESLA 的缺点是认证的初始参数应该单播给每一个接收方，这对拥有庞大数量节点的网络来说是低效的。在 Liu 和 Ning（2003b）文献中，多级密钥链用于密钥分配中，初始参数是预设的，并广播给接收方，而不是单播发送。这样做增加了拥有大量节点网络的可扩展性，同时可抵抗重放攻击和拒绝服务攻击。

10.5　完整性

数据完整性的含义是接收方收到的数据和发送方发出的数据是一样的。在 WSN 里，如果一个节点被敌手捕获，敌手可能会修改数据或把一些错误的信息注入网络里。由于节点有限的资源和节点部署在恶劣的环境中，通信数据会丢失或被损坏，或数据的完整性可能会受到破坏。为了保护数据完整性，最简单的办法是使用循环冗余校验（CRC）；另一个方法是使用基于加密的完整性方法，比如在认证时使用消息认证码 MAC，这会更加安全，但也更复杂。

机密性可以阻止信息泄漏。然而，为了扰乱通信，敌手仍然可能会篡改数据。比如，一个恶意节点可能会在一个包里添加片段或操纵包中的数据。这个新数据包会被发送给原接收方。由于恶劣的通信环境，甚至都不需要出现恶意节点，数据就会丢失或遭到破坏。因此，数据完整性要确保任何接收到的数据在传输过程中不会被修改。

10.6　复习题

10.1　与无线自组织网络和传感器网络相关联的安全挑战是什么？

10.2　创建一个安全网络的基本步骤是什么？

10.3 比较无线自组织网络和无线传感器网络自举的基本需求。

10.4 概述密钥预分配的不同方法。

10.5 使用基站作为在线密钥分发服务器的优点及缺点。

10.6 网络安全中的数据认证和数据完整性是指什么？

第 11 章　挑战和方案：保护

11.1　隐私和匿名

我们周围存在的无线自组织网络和传感器网络使隐私问题更加恶化，为了阻止未授权的观察者，我们必须解决这个问题。无处不在地部署传感器节点，这将导致收集的信息更有可能被滥用。与直接站点监测相反，敌手可以通过远程登录无线传感器网络使用信息；一个敌手也可以以一种低风险、匿名的方式，同时监控多个站点。另外，主要的挑战可能来自使用相关数据集来产生新的信息。如果方法运用得当，就可以从看起来无害的数据中衍生出敏感信息。例如，传感器中的位置信息可能会识别出用户身份，使得持续的活动跟踪切实可行。所有这些使隐私问题更恶化（Chan and Perrig，2003）。

一方面需要使用公共信息，另一方面要求保护个人隐私，这里存在着明显的冲突。例如，某些应用需要传感器检测出事件的位置，而用户的位置信息属于隐私问题。在许多情况下，完全匿名是困难的，必须有一些折中办法。

匿名技术用来防止敌手识别出发送方和接收方。为了实现匿名，数据在公布之前需要去个性化（Depersonalized）。有四种著名的匿名化方法（Priyantha et al.，2000；Smailagic et al.，2001；Gruteser et al.，2003）：

1）分散敏感数据，例如，通过生成树（Spanning Tree）分散数据，这样原始数据的完整视图需要分散节点集的合作才能得到。

2）利用安全的通信协议如 SPINS，可以阻止窃听和主动攻击。

3）为了防止流量分析，数据流可以通过简单的数据传输去模式化（De-patterning）来改变。例如，当需要时，填充一些假的但看起来为真的随机数据，能极大地改变流量模式。信息泛洪将在本章后一部分深入讨论。

4）与位置感知有关，提高传感器节点的移动性是保护隐私的有效方法。位置传感器可以放置在移动设备上，而不是在监控基础设施里。利用被动式监听器，收听和分析遍及区域内的信标信息，能确定物理地址。现在，位置信息在用户手里，用户可以选择信息应该发送至哪一方。

正如以上提到的，信息泛洪是提供匿名性、解决传感器网络隐私问题的一个有效方法。我们将在 12.1.5 节中具体讨论提供额外隐私和匿名性的基于泛洪的算法。最后，基于策略的访问控制判定和认证也能用来解决隐私问题。不同域的隐私策略

可以基于诸如身份、时间、地址等标准来说明。例如，从客户端对一个集中的位置服务器的访问控制，可以通过验证 XML 编码的应用隐私策略实现。

11.2 入侵检测

无线自组织网络有一些易受攻击的特点，例如露天传输、没有固定基础设施或集中管理的自组织。结果，自组织网络更容易受到攻击，安全挑战更加复杂。作为防御的第一道防线，像加密和认证这样的入侵防御技术，能用来抵御入侵者。然而，甚至在有线网络中，单独使用主动防御也不能有效地防止所有渗透，以使系统安全。防御系统的第二道防线需要检测出网络中正在进行的攻击。如果能检测到，则危害能减至最小。

一个入侵检测系统（Intrusion-Detection System，IDS）监控系统里的活动，并分析审计数据来判定是否存在违反安全规则的行为。如果判定出一个恶意的破坏，就会给出一个警告。IDS 也会相应地对攻击做出反应。可用的技术包括异常检测、滥用检测及基于规范的检测（Mishra et al.，2004）：

1）为了检测出异常，用户正常行为轮廓（Profiles）保存在系统里。任何偏离相应轮廓基线的系统活动，都被认定为一个可能的入侵。对于这种方法，正常行为参数的周期性更新是基本的。

2）为了检测出滥用，系统用保存在系统内的已知攻击模式与之匹配，识别出已知入侵。然而，这不能检测出新类型的攻击。

3）在基于规范的检测里，先定义一个约束条件集来描述程序或协议的正常操作。任何违反这些约束条件的行为，被认定为一种可能的入侵。

无线自组织网络中的入侵检测系统架构

无线自组织网络的特性使得它们非常容易受到攻击。首先，移动节点是独立的，它们移动不受系统控制，这样节点就可以轻易地被捕获、破坏和劫持。其次，对敌手来说，在无线网络中没有物理障碍，所以攻击可以来自任何方向，以任何节点为目标。再次，在无线自组织网络中，敌手可能会利用去中心化的管理来实施新型的破坏协作式算法的攻击。为了处理这些额外的挑战，人们设计了一些可能的 IDS 架构，包括独立 IDS、分布式与协作 IDS 和分层 IDS。

1. 独立 IDS

每一个节点有它自己的 IDS，在这种结构里，节点能独立检测攻击。节点之间没有合作，所有的判定取决于单个节点收集的信息。虽然这种架构不是很有效的，但是它也可以用在并非所有节点能够运行 IDS 的网络中。

2. 分布式与协作 IDS

由于无线自组织网络是分布式的，基于节点间的协作，入侵检测和响应系统自

然也应该是分布式和协作的。在这个架构（Zhang et al.，2003）中，每个节点有一个 IDS 代理，独立做局部检测判定。同时，所有节点参与全局检测过程。

与独立 IDS 架构类似，分布式与协作 IDS 架构比基于簇的多层结构更适合扁平网络配置。

3. 分层 IDS

在多层无线自组织网络中，节点分成簇（Clusters）。为了适应多层无线自组织网络的要求，提出了分层入侵检测系统，系统中的每个节点都有负责局部入侵检测的 IDS 代理。同时，簇头的 IDS 代理负责局部和全局入侵检测。每个簇头里的活动的全局代理确保全部的网络覆盖。然而，簇也会增加可能的受攻击点、开销以及创建和维护簇的复杂性。

在 Roman 等（2006）文献里，有一种称为“自发看门狗”（Spontaneous Watchdog）的可选择的分布式方案。它是针对平面传感器网络架构的，这种结构不用把节点分成簇，或是增加更强大的节点。有些传感器节点独立地选为自发看门狗，来监控它们邻居节点的通信。这种技术取决于传感器通信的传播特性，并且利用了部署在这一区域内传感器节点的高密度。在一个广播范围内或者在一个转发包下一跳的传感器节点集可以接收每一个循环包。因此，为了监控这些包，所有的传感器节点都有机会激活它们的全局代理。

4. IDS 的移动代理

一个基于移动代理的 IDS 可被看做分布式和协作式入侵检测技术，也可以与分层 IDS 一起使用。因为一个代理有能力穿过网络、与节点交互，并能从中收集信息，所以代理是可移动的。入侵检测的任务被分发布置到这些移动代理中。每一个移动代理被分配了一项具体任务，按照沿着移动路径收集到的信息行动。

使用移动代理有很多优点（Mishra et al.，2004）。首先，因为任务是分布式的，每个节点只有一部分任务而不是全部任务，因此降低了网络的能量消耗。其次，提高了总体系统容错性，这是因为 IDS 任务分布在网络的不同部分，当一些代理受到破坏，或部分网络分离时，其他代理仍能正常工作。再次，因为移动代理可以是一个与平台无关的，IDS 能在不同操作系统环境下运行。此外，当一个中央处理单元被分布式移动代理替换时，机器之间分担了计算负载，这样网络负载就减少了。然而，这些移动代理仍然需要在每个节点的安全模块下运行，以此来保护远程主机上它们自身的安全。

5. 传感器网络的 IDS

无线传感器网络和无线自组织网络有很多相似之处，但是它们之间也有很多不同。在无线传感器网络中，微小且简单的传感器节点受到能量供应和计算能力的约束。由于范围有限，无线传感器网络的节点密度通常高于自组织网络。在无线传感器网络中，大部分的传感器是固定的，缺乏移动性。无线传感器网络本身的这些固

有限制和传感器网络的结构，使得很难设计出一个针对无线传感器网络的 IDS。

虽然用于自组织网络的以上 IDS 方案能应用到传感器网络中（Zhang et al.，2003），但是不适于直接应用。比如，因为受到能量限制，所以每个节点都有一个充满能量的 IDS 代理可能是不可行的，或者强迫每个节点分析所有来自高密度传感器网络区域邻居节点的包也是不可能的。怎样把检测任务分配给节点是与传感器网络中 IDS 解决方案相关的最基本的问题。

无线传感器网络的 IDS 系统必须面对以下挑战（Roman et al.，2005）：

1）为了分析具体的网络协议和应对传感器网络中的具体威胁，需要一个简单而又高度专用的 IDS 架构。传感器网络的 IDS 在分析检测规则集和与节点进行通信交换信息时，传感器网络的 IDS 应该使用尽可能少的资源。例如，管理存储空间是至关重要的。IDS 的扫描结果必须消耗很少的存储空间，当存储空间满时，策略必须能持续工作。

2）一旦任何代理发现网络中可能有破坏安全的行为，它必须很快创建一个警报，并把它发送给基站。

3）IDS 系统必须是分布式的，并为了达到更好的性能互换信息；这意味着数据收集和分析将在不同位置进行。

4）IDS 应该能经受得住敌对行动。

11.3 抵御流量分析

无线传感器网络由许多小的、资源受限的传感器节点和一些基站组成。这些基站比普通的传感器节点具有更多的能量和更强的计算能力。它们在系统中起重要作用，因此也成为攻击的主要目标。

如果敌手能成功攻击一个基站，很容易使整个系统无效。因此，定位一个基站对敌手是很有帮助的。即使包是加密的，敌手也能仅通过监测流量模式和流量值来定位基站，并获得网络的重要信息。在传感器网络中，传感器节点收集的数据一般经由相对固定的路径传往基站，离基站近的节点比离基站远的节点发送更多的包。基于这些性质，敌手会分析流量模式，不用理解包内容就能获得基站的位置。这被称作“速率监测攻击”（Rate Monitoring Attack）（Deng et al.，2005）。为了蒙骗和误导敌手，传感器节点收集的包可能会被随机发送，而不是发送给父节点，使敌手不容易找到通向基站的确切路径。

另外，还有“时间关联攻击”（Time Correlation Attack）。在这种攻击中（Deng et al.，2005），敌手能通过只产生一些事件，并监测传感器节点把包发至何方，来推断基站的位置。一种防御时间关联攻击的方法是在发送之前的随机时刻，把进来的数据包缓存在节点里。另外一种方法是，以某种概率产生一个假数据包，每当节

点想要发送数据包时，把假数据包发送给另一个节点。这个假数据包利用“存活时间”（Time-To-Live，TTL）决定什么时间停止发送。

11.4　访问控制和安全人机交互

许多在安全上的失败根源在于人为错误或人员的介入。在一些情况下，如果不正确地使用或用户绕过安全系统，即使最安全的系统也可能会失败。然而，只是把用户标注为“安全链上最弱的一环”，并不能给我们更安全的系统。当设计安全系统时，仔细考虑人机交互（Human-Computer Interaction，HCI）是重要的。一个用户不友好的系统，会使用户产生与安全有关的严重错误和后果。人们可以将之前人机交互的知识和技术用于预防和解决已知问题，设计对用户更加友好的安全系统。

当考虑到与用户行为相关的部分时，使用口令的访问控制是一个好的 HCI 范例。访问控制指的是授权个人进入受限区域的行为。一个计算机系统的访问控制包括身份识别、认证和审计。身份识别和认证是服务的两个步骤，用于判定谁被允许进入系统。

身份识别是用户告诉系统他/她是谁，这是基于一个相对简单的机制如用户名或用户 id。认证是验证用户声称身份的过程。对给定的用户名，通过比较输入的口令和存储在系统内的口令，当两者匹配时，用户可以访问系统，否则用户被拒绝。如果用户不能在连续 3 ~5 次之内，给出一个正确的匹配，该用户身份可能会被停用，需联系系统管理员重置后才可能继续使用。

不过，与使用口令机制相关还有许多问题。首先，由于每一个系统有它自己的口令机制，当用户希望登录进入不同的系统时，他/她需要多次输入用户名和口令。对此，一个显然的解决方法是系统自动存储用户名和口令，这样用户就不用再输入它们。可是，这种方案的安全性并不好。其次，根据口令策略，用户选中的口令需要满足以下要求：口令必须强壮，例如，伪随机组合字母、数字和符号；对每个系统，用户应该使用不同的口令；口令应定期更换，不遵从的用户账户应该被删除或停用。这意味着需要人们更多的记忆来应对口令服务。再次，由于不同系统对用户名和口令的要求有很大不同，用户需要记忆更多。他们必须记住不同系统的口令和用户名，还有每个系统的口令约束条件。

我们的日常生活和工作场合越来越广泛地需要数字化访问。因此，需要我们每个人记忆越来越多的用户名和与之对应的口令。大部分人很难准确记住所有的口令和用户名。用户逐渐难以应对越来越多的口令。如果忘记了口令，就需要重置口令，这并不是没有成本。许多普通用户选择简单的办法：写下不同系统的用户名和相关口令，然后把它们放在一个“安全的地方”（例如桌子上）。这违反了基于知识的认证原则，即口令只能留在系统内部和用户心里。

为了系统的安全，必须研究人类记忆，研究成果需要融入到口令设计中。以下重要特性应该是普遍接受的（Sasse et al.，2001）：

1）人们不大可能100%正确地回忆起一个条目；

2）比起无提示的回忆，人们更容易记起一个熟悉的条目；

3）经常回忆的条目比很少使用的条目更容易记住，提取非常频繁回忆的条目会变成自动的；

4）人们不能“按照需要忘记”，即使不再需要的条目，一段时间以后，它们也会继续留在记忆中；

5）有意义的条目比无实际意义的条目更容易回忆起来；

6）截然不同的条目可能彼此联系在一起，用来促进记忆；相似的条目在回忆时，彼此对抗（不利于记忆）。

单点登录（Single Sign-On，SSO）是一种访问控制的方法，认证用户一次，能获得访问多个系统资源的权限。这不但可以减少用户需要记忆的口令数量，也能减少登录次数。不过，SSO要求一个同质的架构（Homogeneous Infrastructure），或至少是有一个统一的用户实体认证方案和一个集中的用户数据库。

如果单点登录不可用，另一种方法是多个系统只用一个用户名和口令。起初，这种方法看起来不是一个好选择，因为如果敌手知道这个单独的口令，则所有的系统都会受到威胁。不过，从可用性这方面来讲，这是一个好方法，因为它减少了用户的记忆量。因此，用户可以选择更强的口令，这样反过来也能使系统更加安全。

强口令的问题是它们很难被记住。一个好的解决方法是添加对用户有意义的字母、数字和符号组合来创建口令。这能使口令便于记忆，同时，也使敌手难以破解。实验表明，对普通的用户来讲，连接一些单词和符号创建口令是一个好的选择。对于经常使用的口令，许多系统管理员用一个句子创建口令。例如，“Mb-Cg40K!”可以从句子“My boat can go 40 knots.”生成。

一些使用提示回忆的认证机制被开发出来，来帮助人们更容易地记忆口令。复合的弱认证，像认知口令（Cognitive Passwords）和联合口令（Associative Passwords）都是此类口令方案（Sasse et al.，2001）。对于复合弱认证，用户可以为认证提供一些记忆条目来识别自己。认知口令是以用户容易回忆起的个人事实、兴趣和观点为基础的。当用户向系统提供一系列问题集的准确答案时，他就通过了认证过程。对于联合口令，一些有关联的单词对用来形成口令。

替代的，还有一些系统使用视觉记忆作为用户认证的一种手段。在这些系统中，人们不用回忆口令，只需回忆先前看到的图像。一般情况下，人们更容易认出某物，而不容易独立地回忆出相同的信息。基于识别的认证系统比基于记忆的认证系统可实现更好的安全。

总的来说，有几种方法可以容易实现基于口令的访问控制系统。首先，为了提

供管理用户认证的统一机制，可以使用单点登录。通过单点登录机制，用户认证和授权的一个单一操作，允许用户接入他/她能接入的所有计算机和系统。通过减少强行改变和不同系统使用相同的口令，可以降低口令膨胀。这比把口令写下来记住更安全。对于不常使用的口令，两步法可能是一个好的选择，因为它有助于回忆起一个口令。最后，当设计口令机制时，也应该考虑到用户知识和动机。一些人可能会建议基于知识的认证应该被生物统计认证取代。不过，这在一段时间内是不可能发生的，因为基于生物统计的认证并不能在所有的安全系统中运行得很好。

11.5　基于软件的防篡改技术

目前，软件破解是软件行业的一个大问题。为保护软件不被破解，人们开发了基于硬件和软件的防篡改技术。现在软件保护受到极大关注，为此，越来越多的防篡改技术被提了出来。

防篡改技术是为了检测或感知对软件任何未经授权的修改或使用。一旦检测出这样的篡改，软件的防篡改部分将采取措施使软件对敌手不可用。软件破解修改一个应用的执行代码，来触发或阻止程序执行中一个特定的关键分支。软件破解的一个普通例子就是去掉软件限时试用中的试用期限。有几种攻击被归入软件破解，包括获得未授权访问、逆向工程和破坏代码完整性。为了获得未授权访问，攻击者通过使访问控制机制失效，进入软件。如果攻击者能获得对软件的未授权访问，他/她就能获得一个非法复制或修改软件的某些功能。逆向工程能使程序的机器代码逆转为源代码，它是通过使用调试器逆转编译的程序代码，并写出实现的。其目标是研究程序如何执行某些特定操作，以去除软件的保护或在其他软件中重新利用部分代码。破坏代码完整性是指在程序内注入恶意代码。执行恶意代码使攻击者获得执行程序时的特权。

为了与软件破解做斗争，人们近来研究了大量防篡改保护机制（Atallah et al.，2004），包括水印技术、代码扰乱（Code Obfuscation）、完整性验证、包装器和一些基于硬件的保护技术。不过要记住：上述方法都不能保证免受攻击。不同保护技术联合使用，每一项技术弥补了其他技术的不足，这样才能提供更好的保护。以下将讲解基于软件的保护技术。

11.5.1　加密包装器

在加密包装器系统中，软件被加密，使用之前需解密。为了提高效率，只有程序最关键的部分才加密。在使用之前，这些关键部分软件在运行时解密。换句话说，为了得到程序的解密映像，敌手不得不运行程序。

为防止攻击者得到整个未加密软件的快照，只有系统中要执行的代码才被解

密，软件其余部分代码仍应处于加密状态。这不能确保保护，因为敌手仍能得到许多系统快照、比较它们、产生全部的未加密程序。

另外，解密密钥必须保护起来不被泄漏。敌手主要的攻击方法是运行时工具，例如调试器、内存转储，还有在虚拟机环境下运行或分析程序。为防止攻击，必须限制使用运行时工具。同时，利用各种各样的保护机制，使在虚拟机环境下更难运行和分析程序。加密包装器可以同时使用压缩和加密，来降低存储，并提高系统的安全性。

加密包装器是一个有效的保护方案。攻击者需要设计更复杂的攻击、消耗更多的时间，来分析和获得解密程序的映像。然而，加密包装器也增加了运行时解密的开销。

11.5.2 代码扰乱

在逆向工程工具的帮助下，程序能被逆向编译成源代码。代码扰乱（Code Obfuscation）是一项把原始程序转化为一些不含一致流的代码，来防止逆向工程和篡改攻击的技术。扰乱变换技术应该维持程序的功能性，对代码执行和存储利用只能有适度影响。同时，扰乱变换必须对来自自动逆向工程工具的各种攻击有很强的适应性。扰乱变换的质量会根据它们的潜力（Potency）（可以迷惑读程序的人到什么程度?）、适应性（抵御自动去扰乱攻击怎么样?）、开销（对应用增加了多少开销），被分类和评估。

人们提出了几种扰乱变换（Collberg and Thomborson，2002）：布局变换（Layout Transformation）、数据变换、控制变换以及预防性变换。布局变换通过去除代码的格式（例如嵌套的条件语句）和用随机字符串替换重要变量的名称，来修改代码的外观。一旦原始格式丢失，就很难恢复。这只在与其他变换联合使用时有效。数据变换改变了程序中用到的数据结构，包括如何改变数据在内存的存储方式、如何解析存储数据、如何把数据聚集和如何排列数据。控制变换是为了操控程序控制流，例如改变语句组织的方式、语句执行的次序以及识别程序里循环结构和块结构。

预防性变换的目的是使去扰乱器（Deobfuscators）更难得到程序代码、使自动去扰乱技术变得更难，以及利用去扰乱器的已知的弱点。

可以在源码级和汇编级实现扰乱。源码级的变换使用更广，但是如果源码级变换设计得不好，编译器里的编码优化器就不能完成扰乱，敌手就会很容易地发现在哪里进行了变换。由于能有效地隐藏二元运算，汇编级的扰乱会更有效地工作。

为了评估扰乱变换的质量，潜力和适应性（Collberg et al.，1997）是评价考虑的两个主要因素。换句话说，扰乱变换的质量由转换代码比原始代码扰乱的程度和转换代码抵御自动去扰乱攻击的程度来衡量。适应性（Resilience）的衡量标准包

括程序员创建一个去扰乱器花费的努力以及运行去扰乱器所用的时间和空间。添加到某项应用的扰乱器的安全级别取决于扰乱中变换的精巧、可用的去扰乱算法的力度，以及去扰乱器使用的资源。为了使扰乱达到最好的效果，上面提到的扰乱变换技术可以联合使用。

11.5.3　软件水印和指纹识别

软件水印技术在保护知识产权、防止盗版和非法复制数字化产品方面，有着重要的影响。它是一种嵌入在软件里的特殊数据结构，用来证明软件拥有权和著作权。指纹识别技术是水印技术的特殊类型，用来识别非法分发软件的叛逆者。

如果水印受到扭曲或破坏，嵌有水印的程序运行会受到影响。为了起到保护作用，水印应该隐藏使用，例如隐写术（Steganography）。水印应该健壮（不容易去除），换言之，一个水印能经受得起各种攻击，即使受到强烈攻击后，也能提取出来拥有权和原始出处的证据。然而，为了提供篡改证据，也需要脆弱的水印，即使很小的修改也能破坏水印。

指纹识别技术是一种水印技术，为跟踪叛逆者，软件的每一个实例中嵌入唯一的信息。换句话说，指纹识别技术是用不同的许可信息分发。其缺点（Atallah et al.，2004）是，如果敌手能获得一些目标的指纹识别副本，通过比较这些副本，敌手就能确定出指纹的位置。这样，敌手可能会绕开指纹，重建原始程序。

软件水印技术包括静态水印和动态水印技术。在静态水印中，标记直接藏在数据或代码区里，不用运行程序就能读出。在动态水印里，标记隐藏在程序的运行结构里，只有程序运行时，才能读出。为了读出标记，动态水印和静态水印都需要一个密钥。

水印也能用来跟踪软件复制，证明经授权拥有软件以及软件已被盗版的事实。但是如果敌手能得到密钥，他就能获得存在水印里的版权拥有者和许可使用软件的用户的信息。因此，需要注意：水印技术不能应对逆向工程或经授权的执行问题（Atallah et al.，2004）。

11.5.4　守卫

只使用一种简单的保护方案会增加漏洞，因为无论单一保护点多么有效，它会被定位，并处于危险境地。相反，为了提供强大的保护，多种保护技术（可能是简单的技术）应该协同使用，来抵制软件篡改、加强安全政策。这些小的安全单元称为守卫（Guards）。

一个守卫（Chang and Atallah，2001）是在程序运行时，负责执行某些安全相关操作的代码片段。守卫插入软件代码中，来保护代码的特定区域。在软件和其他对象（如硬件）的代码区能实现交叉保护（Cross-guarding）。如果受保护程序有未

授权的篡改，就会触发守卫采取措施。其他情况下，守卫必须不能妨碍程序的基本功能。

这些守卫通过程序代码校验、代码修复等，为编程提供保护。大量的守卫可以组成网络（Chang 和 Atallah，2001），通过相互保护加强各自的安全。基于软件的守卫也能和基于硬件的保护联合使用，确保受保护的软件只有在授权的环境下才能运行。

守卫能提供多层防御来化解攻击，例如它具有自愈能力、种类多样、随机执行。守卫应该对攻击具有适应能力（Resilient）。为抵御各种攻击，脚本稍作修改，会产生很不同的结构和代码流。使用高层脚本时，开发者可以选取哪一个特定守卫实例插入，或把哪一个特定序列用于变换。守卫允许开发者精确控制保护代码的放置。如果需要，守卫对攻击的反应可以灵活。也就是说，当检测到攻击时，守卫的反应取决于软件发行商的商业模式和预期敌手。

11.6 防篡改：硬件保护

传感器网络的节点易受物理攻击，因为它们以分布式方式部署在易接近的环境中。对无线传感器网络的物理攻击之一是捕获节点，也就是，敌手能通过直接的物理接入，控制某些节点。目前，随着硬件篡改技术的发展，一个受过良好训练的攻击者在很短时间内就能破坏传感器节点。一个节点受到破坏之后，节点里的秘密信息可能会泄漏，节点行为会被未授权的接入控制。这些对整个网络的安全具有很大威胁。软件和硬件保护都可用来抵御攻击。一些方法使用硬件让敌手难以得到存在传感器节点里的信息，其他方法可能同时使用硬件和软件来保护节点。由于硬件成本的快速降低，对无线传感器网络基于硬件的保护方法会变得更有效。

为了保护节点免受物理攻击，当节点检测到一个可能的攻击时，节点能选择销毁它自己所有的数据和密钥。网络可以通过杀死受破坏节点，有效避免潜在的攻击。所有节点需要做的是检测出可能的入侵。只要用一个低频传感器检测出攻击，传感器中的信息就会对攻击者不可见，或者电路被毁坏来防止攻击者获取节点中的信息。

有许多针对无线传感器网络的物理攻击，包括手工探测传感器获得信息、激光切割和能量分析。例如使用芯片测试设备，像智能卡（Komerling and Kuhn，1999）这样的防篡改设备可以进行逆向工程。借助一些特殊技术（Anderson and Kuhn，1997），像差别故障分析（Differential Fault Analysis）、芯片重写和内存剩磁（Memory Remanence），逆向工程的成本急剧下降。为保护网络的安全，人们提出了一些使这类攻击更困难的方法（Komerling and Kuhn，1999）。例如，我们可以利用随机

化的多线程在执行算法时增加更多的不确定性；在任何可观察的反应和关键操作之间插入随机时延，可以增加攻击的难度；添加额外的金属层在实际电路之上形成传感器 Mesh，并且不会携带任何关键信号，仍然是对微探针攻击者最有效的刺激之一。

我们把用这些方法的基于硬件的保护方案分成两类（Atallah et al.，2004）：使用防篡改处理器（Tamper-Resistant Processor）用于保护和使用轻量级硬件如令牌。在防篡改处理器这种方法中，系统依赖安全处理器来防止非法软件复制、未授权软件修改和未授权软件逆向工程。安全处理器结构采用一些特性创建一个安全环境，使得只有授权的和未经篡改的硬件和软件才能存在。当数据和指令进入到防篡改处理器时，通过加密和动态完整性检查保护位于硬件设备里的数据，实现安全。当执行应用程序时，该架构确保敏感数据和应用指令在任何时间都不会泄漏，始终保证软件的完整性。安全处理器架构既能用来防止可能的对受保护应用基于软件的攻击，又能阻止许多硬件攻击。

另外一种基于硬件的保护机制是用更轻量级硬件，比如硬件令牌或防篡改智能卡，来防止各种攻击。在这种保护机制中，通过硬件防复制片段嵌入一份用户许可。软件或操作系统检查是否有令牌，如果没有，就拒绝运行。检查硬件令牌的机制是基于一个密码学密钥，这个密钥从来不在防篡改令牌之外存储或使用。

基于硬件的保护既有优点也有缺点，其最重要的优点是应用程序在可信处理器上运行，这可以阻止攻击者接入内存，提供更大的保护。软件以加密的方式存储在系统中，它只在运行前在处理器内部解密，这能阻止对系统有完全控制权的任何用户检查明文指令。更重要的是，为了防止代码的逆向工程，所有在处理器和内存之间通信的数据都被加密。基于硬件的保护还有另外一个优点，只有通过加密和动态完整性检查的程序才能进入防篡改处理器中。

然而，基于硬件的保护方法也有很多缺点。与基于软件的保护相比，硬件更难修改和更新，需要花更多时间安装、整合和进行硬件测试。另一个缺点就是硬件成本高于基于软件的保护方法。另外，由于每次数据输入防篡改处理器时，都需要进行加密和动态完整性检查，基于硬件的保护在能量、时延和系统资源如内存和进程时间上是更耗成本的。

基于硬件和软件防篡改技术的底线是用来阻止对软件未授权的修改和使用，它们都有优点和缺点。基于软件技术包括水印、代码扰乱、完整性验证和包装器。软件防篡改方法的主要缺点是程序运行在一个不被信任的主机上（Atallah et al.，2004）。可是由于基于硬件防篡改技术能使用一个可信装置来保证程序安全，通过联合使用基于软件和基于硬件的防篡改技术，我们就能更好地保护节点。

11.7 可用性和合理性

可用性表示在给定时间周期内网络正常工作的持续时间占时间周期的比例。对于无线传感器网络，可用性是指能收到信息并成功发送到汇聚节点的传感器的比例。在一个安全的网络中，可用性应该很高。本书讲的所有安全技术都可以增加自组织网络和传感器网络的可用性。

在无线自组织网络和传感器网络中，汇聚节点接收和聚合数据时，需要验证数据一致性。这一需求称为数据合理性（Data Plausibility）。检查接收数据的合理性是防御受破坏节点的一种有用方法。真实性、完整性和机密性并不能保证合理性，原因是即使是合法发送方的消息也可能包括错误数据。例如，入侵者可能会通过用黑色的外衣覆盖以欺骗一个光敏感元件。基于冗余的防御机制可以设计用来抵御这种欺骗。通过与来自邻居节点消息的一致性来保证消息的合法性。因此，通过比较从所有邻居节点接收的数据和通过传感器或预定义规则获得的周围环境状态，可以检查接收数据的合理性。

11.8 复习题

11.1 描述无线传感器网络中保护隐私的方法，并给出使用每一种方法的原因。

11.2 描述用于入侵检测系统的检测技术和无线自组织网络的入侵检测系统架构。

11.3 无线传感器网络中入侵检测系统的特点是什么？

11.4 口令机制和网络安全的关系是什么？

11.5 简述与口令设计有关的用户特点。

11.6 什么是基于知识的认证系统？它是怎样工作的？

11.7 有多少基于软件的保护机制用于软件保护中？这些机制是怎样工作的？

11.8 比较基于软件和基于硬件保护机制的优点和缺点。

11.9 什么是数据的可用性和合理性？我们应如何实现？

第 12 章　安 全 路 由

第 8 章阐述了有关针对路由方案的安全威胁。本章我们将介绍对这些威胁的防范措施。首先我们总结安全路由的方法，我们主要关注虫洞攻击、女巫攻击、选择性转发和安全多播/广播。同时还阐述了改进为其他服务的安全措施性能的路由技术。所选的安全路由协议在本章的第 2 部分中给出。

12.1　抵御对自组织路由的安全攻击

由于路由是自组织网络和传感器网络中的一个重要挑战，所以吸引了很多研究者进行了广泛的研究。其中绝大多数的研究主要集中在自组织网络的服务质量保证和无线传感器网络的能效。然而，很多自组织网络和传感器网络应用被设计用于部署在敌对环境中、常遭受敌对行动。因此，安全性应该是影响路由协议设计的一个主要因素。

设计一个安全的路由协议的方法有以下三种（Parno et al.，2006）：

1）攻击预防；

2）攻击检测以及受攻击后的恢复；

3）对安全攻击的适应性。

路由协议可以设计得使敌手无法威胁节点和消息或使路由机制发生故障。这种方法对于安全方案开销以及提高抵抗安全威胁的效率是最有效的。因此，大多数技术都属于这一类方法。预防性措施被设计用于反击已知威胁，对未知的威胁可能无效。用于检测不端行为或者故障节点的检测方案可以被设计得更为通用。另一方面，它们也会比预防性措施需要更大的开销。最后，路由协议可以被设计成仍能向存在攻击的目标发送数据包。这种适应性的技术同样需要很大的开销。我们将同时给出检测和适应性技术的例子。

12.1.1　抗虫洞攻击技术

虫洞（Wormholes）很难被检测，因为敌手通过使用单跳带外信道，将数据包发送到一个距离收到该包的端点远的端点。网络无法监听这种信道。此外，数据包真正的备份到达接收重放备份端点的时间要晚于重放备份到达该点。因此，重放的备份要比真正的备份更新鲜。抵抗虫洞攻击的检测机制可以基于对数据包的时间和空间分析。在 Hu 等（2003）文献中介绍的地理和时间上的数据包绑定遵循了这种

方法。地理位置绑定（Geographical Leash）方案假设各个节点松散同步，同时是地理位置感知的（Location Aware）。源节点 S 将自身的地理位置信息 l_S 和数据包传输时间信息 t_S 作为地理信息绑定到它发送到目的节点 D 的数据包 P_S 中。

$$S \rightarrow D : l_S, t_S, P_S$$

网络中的节点时钟同步误差在 $\pm\Delta$ 范围内。两节点之间的距离上限是 d_b，同时是基于两节点的传输距离而定的。节点定位的误差上限是 δ。同样的，传输信号 v 的速率上限也是已知的。之后每个位于位置 l_i 并在 t_i 时刻接收数据包进行转发的节点 i 可以检查以下条件：

$$d_b \leqslant |l_i - l_S| + 2v(t_i - t_S + \Delta) + \delta \tag{12-1}$$

如果条件不成立，就表明由节点 i 所接收的数据包比预期的早到达，网络可能遭受了虫洞攻击。当节点之间的平均距离不够长，并且正常路径中的跳数不够高时，这种技术也许无法检测出虫洞攻击。

时间绑定（Temporal Leashes）的方式只使用数据包的发送和接收时间来检测虫洞。当节点 A 发送或转发某个数据包给节点 B 时，数据包 P_A 中也将包含传输时间 t_A。

$$A \rightarrow B : t_A, P_A$$

节点 B 将检查数据包的发送时间 t_A 和接收时间 t_B 之间的差值 d_{AB}，如果 d_{AB} 小于给定的门限值 θ，就表明遭到了虫洞攻击。时间绑定方式需要严格的时钟同步。

当定向天线在节点中可用时，它也可以被用于检测虫洞（Hu and Evans，2003），如图 12-1 所示，这里由节点 a 所传输的数据包被恶意节点 w_1 所接收，并通过虫洞传输给了另一个恶意节点 w_2，并且被节点 w_2 进行了重放。重放数据包被节点 f 接收。因此，节点 a 和 f 相信它们互为邻居节点。

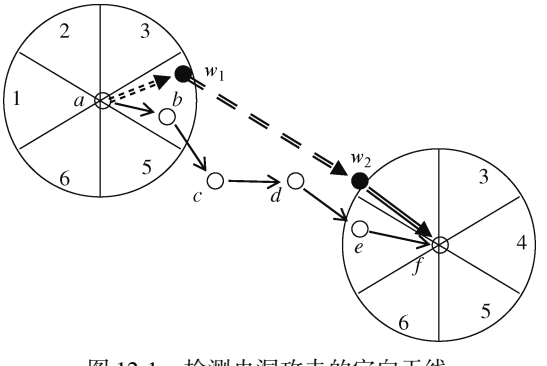


图 12-1　检测虫洞攻击的定向天线

我们假设节点 a 和 f 都装备了拥有六个扇区的定向天线，同时两个节点的扇区是对齐的，例如节点 a 的 1 号扇区和节点 f 的 1 号扇区在同一个方向上。因此，由节点 a 的 4 号扇区所发送的数据包应该在节点 f 的 1 号扇区进行接收。然而，由虫洞所重放的数据包是由节点 f 的 2 号扇区接收的。若数据包也包含传送它们的扇区的数据信息，这就表明产生了虫洞攻击，同时可以被节点 f 检测出。

攻击者可以通过在相同的接收扇区进行重放数据包来适应定向天线。然而，即使是使用这种最简单的方式，攻击者的能力也被削减了。更多的基于这一思想的更

复杂的方案在 Hu 和 Evans（2003）文献中给出了介绍。

12.1.2　抗女巫攻击技术

要防止女巫攻击（Sybil Attacks），每个节点的身份都要进行验证。这种验证可以直接进行，也可以间接进行。在直接验证中，节点直接验证邻居节点的身份是否有效。例如，某个节点可能会为它的每个邻居节点分配一个单独的信道进行通信，并要求它们在某一时段传输信息。之后，这个节点将在这段时间内随机地检查这些信道。如果某个节点正在它的分配信道中传输信息，这个节点就是一个物理节点。如果在信道中没有检测到传输行为，那么就表明分配给这一信道所对应的节点可能不是一个物理节点（Newsome et al.，2004）。

在间接验证中，另外一个可信节点将为节点提供身份验证。例如，所有的节点都和基站共享一个唯一的密钥。当两个节点之间需要建立连接时，它们使用这一密钥通过基站来验证彼此的身份（Karlof and Wagner，2003）。同时它们可以被分配一个会话密钥。每个节点也可以和有限数量的邻居节点建立连接。因此，受威胁节点只能和数量有限的经验证的邻居节点进行通信，这样也可以限制女巫攻击所造成的影响。分配给节点的随机密钥同样可以提供针对女巫攻击的保护。由于每个节点的可用密钥数量有限，节点就没有足够的密钥来生成多个身份（Newsome et al.，2004）。

12.1.3　抗选择转发技术

防御虫洞、汇聚节点漏洞（Sink Holes）和女巫攻击无法保证减缓黑洞攻击和选择性转发攻击。受威胁节点依然可以扮演一个黑洞或者丢弃所选择的数据包。有两种方法可以防止选择性转发攻击：检测进行选择转发的节点，开发更加具有适应性的路由方案，能够在存在选择性转发攻击的情况下传输数据包。

有一种基于应答的检测选择性转发节点的方法（Yu and Xiao，2006）。每个转发数据包的中间节点将需要等待来自下一跳的应答。如果下一跳的节点没有返回与发送包数相同数量的应答，节点将产生关于下一跳节点的报警信息。然而，受威胁节点同样可以为它们丢弃的数据包产生应答信息，这样就会使得这种方案失败。此外，某个恶意节点可以生成一个伪造的报警信息来组织一次拒绝服务攻击。认证方案和加密可以用于防止这类恶意行为（Yu and Xiao，2006）。数据链路层应答也可以通过端到端可靠性方案补充。

多路径路由是一种减缓选择性转发和黑洞攻击的有效手段（Karlof and Wagner，2003）。这种方法至少需要链路分离（Link-disjoint）的路径，这里的两条路径可以共用一些节点，但是没有共用链路。当然，节点分离（Node-disjoint）路径，就是两条路径中不存在相同的节点，要比链路分离路径更好，并且能够降低选择性转发

攻击带来的风险。然而，分离路径并非总是可用的，当路径不是分离的，如果进行选择性转发的节点是所有路径的共用节点，那么选择性攻击就变得和使用单一路径路由一样有效。

12.1.4 传感器网络安全路由

无线传感器网络中的数据流体制主要是广播或者多播方式。在一个典型的情况下，基站广播管理信息，并对网络提出查询，各个传感器将响应基站发出的广播询问。因此，由基站流向节点的信息流，例如下行信息流，既可以是广播的形式，也可以是一对多的形式，而由节点流向基站的信息流，例如上行信息流，是多对一的。当使用了执行器（Actuators）或者多个基站时，上行信息流就会具有多对多的性质。在这种信息流体制中的路由方案的安全问题和一对一路由中的安全问题是不同的。因此，专门为以下类别的路由选择所设计的安全方案是无线传感器网络中所需要的：

1）下行信息流的安全广播；

2）下行信息流的安全多播；

3）从多个节点路由至基站时的安全数据聚合；

4）从多个节点向多个基站或者执行器路由时的安全数据聚合和多播。

由于这些关系在传感器网络和执行器网络中很典型，所以我们在“传感器网络的安全路由”的主题下进行介绍。在传统的自组织网络中也需要安全广播和多播，在这一节中所阐述的方法也适用于自组织网络。

12.1.4.1 安全多播和广播

在安全多播和广播中，一个主要挑战是群密钥和信任管理，它们可以通过某种集中的、簇的或者分布式的方式实现。群密钥和信任管理在 10.3 节中给出了解释。在中央群密钥管理中，中央密钥管理者管理整个网络的密钥，包括进行广播或者多播的节点。逻辑密钥树（Di Pietro et al.，2003）就是中央群密钥管理方案的一个实例。在簇方式中，密钥管理职责被分给多个密钥管理者，每一个管理者负责一群节点的密钥管理。在分布式方法中，群密钥管理是由进行多播的节点实现的。TESLA 和 μTESLA 是实现这种方法的两个例子。μTESLA 在 13.1.2 节中给出了解释。

12.1.4.2 安全数据聚合

每一个传感器节点都是一个可以向基站发送消息的独立实体。因此，传感器网络中的联网体制可以理解为一种传感器节点和基站之间的一对一通信模式。然而，传感器节点和基站之间的实际关系是多对一的，这是因为传感器网络中的数据流会因为存在重叠感知区域而同时具有时间和空间相关的性质，同时，覆盖大面积区域的事件发生时会被多个传感器检测到。多个传感器可以几乎同时报告相同的事件或

者回复相同的请求。不仅如此，当网络中传输多个数据包时，将这些数据包汇集成为单一的一个数据包进行传输将更加有效。将数据包进行汇聚的节点，例如聚合器（Aggregators），可以是任何一个节点，并且可以事先选定。聚合操作生成一个反向多播树，它在基站处结束。

数据聚合将会使得传感器网络更容易受到攻击，原因如下：

1）对聚合器的危害会使得在所有节点的数据到达聚合器之前对数据进行伪造变成可能；

2）单个数据包的完整性代表了通过聚合方式形成这一数据包的多个数据包的完整性。

因此，聚合器成为虫洞攻击、沉洞攻击、黑洞、选择性转发攻击以及女巫攻击的主要目标。当这些攻击在聚合器处完成时，就会产生更大的影响。所有为了反击这些攻击所设计的技术也改进了数据聚合方案的安全性。

防止敌手对信息流进行分析的技术可以帮助隐藏聚合器。当聚合器是隐蔽的时，针对它们的攻击就无法轻易地被组织起来。另外，认证和加密方案为聚合器和聚合信息提供了额外的措施，以防止它们受到威胁。

最后，聚合器可以在将每一个数据包进行聚合之前检查它们的一致性。为此，可以进行统计学的分析。相似的方法已经被引入其他的服务安全中，例如安全事件边界检测和安全定位，这些将在后面的章节中进行介绍。

12.1.5　增强安全的路由方案

安全性不仅仅是面向路由方案的安全。路由方案有时设计成能够为保证匿名、隐私以及防止包含流量分析的攻击的安全措施做出一些贡献。例如，一个基于随机游走的路由方案可以设计用来防止流量分析。

在一个随机游走（Random Walk）策略中，节点不是总向它们的下一跳节点发送数据包。取而代之地，它们可能会偶尔将它们的数据包发送给一个随机选择的节点（Deng et al.，2004）。这样有助于缓解试图通过监控链路中数据流的比率来检测基站和聚合器的流量分析攻击。在一个可替代策略中，当节点向基站发送数据包时，它的邻居节点同时向一个随机选取的节点转发一个伪造的数据包（Deng et al.，2004）。这一伪造的数据包在经过足够的跳数后将被舍弃。这种方法可以防止敌手通过检查数据传送计时来探测基站和聚合器。

另外一种基于随机游走的技术是基于贪心算法的随机游走（Greedy Random Walk）（Xi et al.，2006），在这种方法中，基站和源节点同时开始随机游走。当这些随机游走创建的路由相交汇时，由源节点发送的数据包将按照始于基站的随机游走生成的路径进行路由。

泛洪也被认为是一种对流量分析具有很强适应性的路由技术（Walters et al.，

2006)。在 Ozturk 等 (2004) 文献中，提出了相比单一路径路由而言提供附加隐私措施的基于泛洪的技术：

1) 基线泛洪 (Baseline Flooding)：这种泛洪方案在 5.2.1 节中介绍过。所有的节点都将广播它所接收到的每个数据包，同时只执行一次这种操作来避免出现回路的情况。

2) 概率性泛洪 (Probabilistic Flooding)：所有节点的一个子集在泛洪时不会使用，同时将它们收到的数据包丢弃。这种技术不能保证对每个数据包的传送。

3) 带有伪造消息的泛洪：一些敌手依然可以在采用基线泛洪和概率性泛洪技术的情况下分析数据流和监听个别的数据包。为了减小这种风险，在这种技术中采用了随机节点产生伪造的消息，并将其和真正的数据包一起进行泛洪的办法。

4) 幻影泛洪 (Phantom Flooding)：这种技术包含两个阶段。在第一阶段中，某个数据包将根据某种随机的或直接的游走技术来确定跳数。在第二阶段中，在游走阶段结束时，数据包将被到达游走阶段末端的节点泛洪出去。

当这些技术受到其他方案的支持并用于匿名性时，例如敏感数据的去中心化、安全通信信道和使用移动节点，对于敌手来说，流量分析将会变得非常困难 (Walters et al., 2006)。用于匿名情况的技术已经在第 11 章中进行了阐述。

12.2 安全自组织路由协议

这一节将介绍表 12-1 中所列出的安全自组织网络和传感器网络的路由协议。其中的一些协议在 Fonseca 和 Festag (2006) 文献中也进行了分析。本章中所列出的协议并不是详尽的。文献中还有很多种类的路由协议。我们的目的是更好地洞察安全自组织路由协议的需求。因此，我们从大量文献所阐述的方法中选取了一些具有代表性的协议。

表 12-1 安全自组织路由协议

名 称	路由方案	安全服务
无线传感器网络中的入侵容忍路由 (INSENS)	—固定传感器网络路由方案 —多路径链路状态路由 —基站计算路由并广播	—对被破坏节点和物理攻击的弹性 —认证 —对 DOS 类泛洪攻击的弹性 —对称密码学
自组织网络认证路由 (ARAN)	—在基于泛洪的路由请求阶段设置梯度的定向传播类的路由协议 —为自组织网络设计	—证书管理 —数据完整性 —非对称密码学

（续）

名　　称	路 由 方 案	安 全 服 务
按需安全自组织路由（ARIADNE）	—动态源路由 —为自组织网络设计	—认证 —对节点受破坏的弹性 —对 active-1-x 和 active-y-x 攻击的弹性（见 8.2 节） —对称密码学
看门狗和路径评价（Watchdog Pathrater）	—动态源路由 —为自组织网络设计	—检测和恢复方案
安全自组织按需距离矢量（SAODV）	—自组织按需距离矢量路由 —为自组织网络设计	—引入授权 —源认证 —完整性 —数据认证 —非对称密码学和哈希链
安全链路状态路由协议（SLSP）	—链路状态路由 —为自组织网络设计	

12.2.1　无线传感器网络入侵容忍路由（INSENS）

INSENS（Deng et al.，2003）遵循三个设计原则。首先，只有基站可以进行广播和多播。独立的节点只能够向基站进行单播。基站将为每一个节点建立发送表。整个网络向基站发送自己的邻居信息，同时基站为节点生成发送表，并将之分配给所有节点。构建发送表使每个源的路由变为多路径路由。其次，所有的路由和控制信息都必须进行认证。最后，对称密钥被用于这种认证。这种认证包括路由发现和数据传送两阶段。路由发现阶段还可以再细分为三个步骤：路由请求、路由反馈、路由计算和传播。

12.2.1.1　路由发现阶段

每当基站需要构建发送表时，它都会广播一条路由请求消息。路由请求消息将会在网络中进行泛洪。每个接收到路由请求消息的节点，首先将其身份添加到消息中，并将消息进行转发。同时，它会将发送者的身份记录在它的邻居集合中。当某个节点接收到了相同路由请求的另一个备份时，它将只记录发送者而丢弃请求。

为了防止这一过程中的电子欺诈攻击，使用了一种类似于 TESLA 的广播认证方案。这里定义一个数的集合 $K=\{K_0,K_1,\cdots,K_n\}$，满足 $K_i=F(K_{i+1})$，这里的 F 是一个单向密码哈希函数，并且 $0\leqslant i<n$。在整个网络进行部署之初，F 和 K_0 是已知的。只有基站中有 K 的所有取值，并且基站使用 K_i 广播第 i 个路由请求。接收到第 i 个路由请求的节点将通过使用函数 F 由消息中的 K_i 生成 K_{i-1}，并将生成的 K_{i-1}和之前已知的 K_{i-1}进行比较。如果两者匹配，就表明消息是可信的。由于函数 F 是单向函数，其他的节点都无法通过 K_i 生成 K_{i-1}。因此，受威胁节点就无法通

过生成新的密钥来欺骗基站。然而，它可以重发路由请求信息，这样只能破坏从受威胁节点处的下行过程。

每个节点也同时配置了一个只与基站共享的独立密钥。节点会在将自身的身份加入路径之后，再对整个路径生成消息认证码（MAC），并在传输消息之前，将消息认证码（MAC）追加在消息中。基站之后使用这些消息认证码（MAC）来验证路径上的节点。如果某个节点是受威胁节点，那么只会有一个密钥泄漏，所以攻击者就无法威胁到整个网络或者通过威胁某一个节点而发起女巫攻击。

在某个节点传送一个进入的路由请求消息之后，将会等待一个时间间隔 t。在时间 t 内，这个节点将会接收到从它的邻居节点发送来的相同的路由请求消息，同时记录它的邻居集合中的邻居节点的身份和消息认证码（MAC）。在时间 t 结束时，它将通过接收路由请求消息的反向路径向基站发送一个路由反馈消息。路由反馈消息同时包括了邻居集合和由邻居集合通过节点的密钥生成的另一个消息认证码（MAC）。后一个消息认证码（MAC）确保了邻居集信息的完整性。

基站通过接收的路由反馈信息来构建网络的拓扑数据。由于每一个节点发送了其邻居集的信息，所以关于邻居集完整性的报告可以进行相互比较，从而检测出不一致的地方。所有的节点也基于它们的消息认证码（MAC）来验证。当网络的拓扑结构构建完成并通过验证时，基站将会为每个节点计算多路径路由和发送表。然后发送表从第一跳节点开始传播直到基站。

12.2.1.2 数据转发阶段

某个节点的转发表包含很多条目，例如一条记录对应一个路由（该节点是此路由的一部分）。每个记录由三个元素组成：

$$<\text{目的地，源节点，直接发送者}>$$

目的地是消息将被送达的节点。源节点是生成消息的节点。直接发送者是将这一消息发送给发送表的拥有者的节点。例如，如果假设多路径路由表中的某一条路径如下：

$$S \text{ 到 } D\text{：}S \rightarrow a \rightarrow b \rightarrow c \rightarrow D$$

对于这一路径来说，a 的发送表包括一个记录 $<D, S, S>$，b 的发送表包括 $<D, S, a>$，c 的发送表包括 $<D, S, b>$。当节点接收到一个数据包时，它将首先检查它的发送表。如果它发现了和包中目的地、源节点和直接发送者相匹配的元组，就说明了节点在路由路径中，并要转发数据包给下一跳。因此，它只要将数据包中的直接发送者字段替换成自身的 id 并广播消息。

12.2.2 自组织网络认证路由（ARAN）

ARAN（Sanzgiri et al.，2002）相比于无线传感器网络更多的是为自组织网络所设计的。虽然它是可扩展的，并且足以适用于很多传感器网络应用，但是它是基

于非对称加密的，因此它不能很好地适应典型传感器节点的硬件约束条件。另外一个不同于安全传感器网络路由协议的重要特点是，ARAN 需要一个可信的证书服务器来同时完成节点认证和向它们发放临时证书。可信证书服务器的公钥对于每个节点是已知的。此外，ARAN 假设存在一种当节点申请证书时对节点进行认证的机制。协议中并没有说明是何种机制。

ARAN 为认证、完整性和不可抵赖性提供了相应的机制。当节点 A 首次接入网络或者需要一个证书来进行路由发现时，它将向可信服务器 T 发出证书请求。服务器 T 首先认证节点 A，并在之后向其发送一个证书：

$$T \rightarrow A: certificate_A$$

这里，$certificate_A = \{IP_A, K_{A+}, t, e\}_{\langle K_{T-}\rangle}$。其中 IP_A 是节点 A 的 IP 地址；K_{A+} 是 A 的公钥；t 是证书的生成时间；e 是证书的过期时间；K_{T-} 是 T 的私钥。

拥有一个有效证书的节点 S 可以为另一个节点 D 通过广播路由发现数据包（RDP）来开始一次路由发现：

$$S \rightarrow \text{broadcast}: \{RDP, IP_D, certificate_S, N_S, t\}_{\langle K_{S-}\rangle}$$

这里的 N_S是一个新鲜值，它是序列号，即源节点 S 每执行一次路由发现操作时就单调增加新鲜值，这样来确保期望从目的节点 D 所回复的消息新鲜性。

当节点接收到一个 RDP 消息时，它首先对消息进行解密，然后记录发送消息的邻居节点，作为消息源节点的下一跳节点。如果这个节点接收到了关于这个 RDP 消息的回复消息，它就将回复发送给记录中的邻居节点。最终，它使用自身的私钥加密消息，添加自身的证书，并广播消息。

$$B \rightarrow \text{broadcast}: \left\{ \{RDP, IP_D, certificate_S, N_S, t\}_{\langle K_{S-}\rangle} \right\}_{\langle K_{B-}\rangle}, certificate_B$$

注意到每个中间节点都要解密接收到的消息，并且用自己的私钥再次加密，在发送之前将自身的证书加入消息中。为了解密消息，节点需要接收消息来源的邻居节点的公钥。公钥存在于添加入消息的证书中，证书由可信服务器的私钥加密。每个节点都知道可信服务器的公钥，证书由可信服务器加密后颁发，这已在前面说过。例如，如果节点 C 接收到由节点 B 发送的 RDP 消息，由节点 C 广播的消息是这样的：

$$C \rightarrow \text{broadcast}: \left\{ \{RDP, IP_D, certificate_S, N_S, t\}_{\langle K_{S-}\rangle} \right\}_{\langle K_{C-}\rangle}, certificate_C$$

每个节点都要对路由中的前一节点进行认证，因为消息在每一跳时都进行了签名。另外，RDP 消息中不含有跳数信息或者源路由记录。因此，恶意节点没有机会通过隧道或者修改路由序列号、跳数或源路由来改道传输（Redirect Traffic）。

当目的节点 D 接收到路由中最后一个节点发送来的路由发现消息时，假设它为 C，它将首先验证源的签名，之后准备一个回复消息（REP），并将其单播至 C：

$$D \rightarrow C: \{REP, IP_S, certificate_D, N_S, t\}_{\langle K_{D-} \rangle}$$

像 RDP 消息一样，REP 消息同样被加密和解密，例如被所有的中间节点签名。每个中间节点也都对添加入消息的证书进行替换。传送 REP 消息到源节点 S 和传输 RDP 消息的主要区别在于，REP 消息并非进行广播，而是通过每个中间节点单播到传输 RDP 消息时所记录的下一跳节点的。

$$C \rightarrow B: \left\{ \{REP, IP_S, certificate_D, N_S, t\}_{\langle K_{D-} \rangle} \right\}_{\langle K_{C-} \rangle}, certificate_C$$

当源节点 S 接收到 REP 消息时，它将验证目的地的签名和新鲜值，之后就完成了路由建立。每个中间节点都通过路由表维持路由机制。当在现存的路由中，没有流量发生的时间大于路由的生存周期时，这一路由在路由表中就失效了。当接收到的消息将在一个失效的路由中被发送时，节点将生成一个错误消息（ERR），并将其发送到朝源节点的反向路径的下一跳节点。错误消息也会在节点发现链路由于节点移动等原因被破坏时发送出去。每个错误消息都进行了签名，并进行单播。中间节点 C 向另一节点 B 发送错误消息的格式如下：

$$C \rightarrow B: \{ERR, IP_S, IP_D, certificate_C, N_C, t\}_{\langle K_{C-} \rangle}$$

这一消息在发送至源节点的过程中不会被修改。当它到达了源节点时，这一路由也会被源节点释放。

和路由一样，证书也可以被撤销。要撤销证书，可信证书服务器将广播一个宣布撤销证书的消息：

$$T \rightarrow \text{broadcast}: \{REVOKE, certificate_R\}_{\langle K_{T-} \rangle}$$

撤销消息将被存储，直到被撤销的证书到期。

12.2.3 按需安全自组织路由（ARIADNE）

ARIADNE 是一种安全动态源路由协议（Hu et al.，2005）。它通过利用多种方法，例如 TESLA、消息认证码（MAC）和数字签名，提供安全的路由发现和维护服务。当 ARIADNE 路由发现使用 TESLA 时，每一跳认证“路由请求”中的信息。目标缓存“路由请求”，直到中间节点释放其 TESLA 密钥之后才发回一个“路由回复”。之后，它就完成源节点和中间节点的认证，并将“路由回复”按传输“路由请求”的路径原路反向发回。

ARIADNE 假设每个通信源节点 S 和目标节点 D 共享消息认证码（MAC）密钥 K_{SD} 和 K_{DS}，并且每个节点拥有一个 TESLA 单向密钥链，所有节点都知道其他节点的密钥链中的第一个密钥。

ARIADNE 路由发现过程始于一次“路由请求”，它包括以下字段：

1）路由请求：一串表明数据包是路由请求包的码字；

2）源节点；

3）目的节点；

4）id：路由请求的标识；

5）时间间隔：对传输数据包到目的地所需时间的悲观估计；

6）哈希链：路由中所有节点生成的哈希值；

7）节点列表：路由中节点的列表；

8）MAC 列表：路由中每个节点所计算出的消息认证码（MAC）值的列表。

源节点分配源、目的地节点、id 和时间间隔，并且它们在数据包到达目的地节点 D 之前不会改变。哈希链、节点列表和消息认证码（MAC）列表在每一跳时都发生改变。源节点 S 首先按下式计算哈希链：

$$h_0 = MAC(K_{SD}, REQUEST|S|D|id|t_i) \tag{12-2}$$

在计算了 h_0 之后，源节点将初始化节点列表和消息认证码（MAC）列表为空表，并广播“路由请求”消息：

$$S \rightarrow \text{broadcast}: \{REQUEST, S, D, id, t_i, h_0, (), ()\}$$

每个接收到路由请求的节点，首先检查其缓冲区的 $<source, id>$ 字段。如果这一请求已经被接收，则丢弃新来的请求。节点也将检查时间间隔。如果间隔时间还有很长时间到来或者与之相关的密钥已经被泄漏，那么数据包将会被丢弃。否则，接收数据包的节点将修改哈希链 h_i。假设 A 为距离源节点 S 一跳距离的节点。它将这样计算 h_1：

$$h_1 = H(A, h_0) \tag{12-3}$$

它同时也会通过 TESLA 密钥链中的下一个密钥 K_{Ati} 来计算它的消息认证码（MAC）值，将其地址和消息认证码（MAC）值加入“路由请求”消息，并进行广播：

$$M_A = MAC(K_{A_{ti}}, REQUEST|S|D|id|t_i|h_1|(A)|())$$

$$A \rightarrow \text{broadcast}: \{REQUEST, S, D, id, t_i, h_1, (A), (M_A)\}$$

这一过程将被每个中间节点重复进行。例如，第三个中间节点 C 计算其哈希链和消息认证码（MAC）值，广播“路由请求”消息如下：

$$h_3 = H(C, h_2) \tag{12-4}$$

$$M_C = MAC(K_{C_{ti}}, REQUEST|S|D|id|t_i|h_3|(A,B,C)|(M_A, M_B))$$

$$C \rightarrow \text{broadcast}: \{REQUEST, S, D, id, t_i, h_3, (A,B,C), (M_A, M_B, M_C)\}$$

当目的节点接收到“路由请求”时，它将通过确定密钥在所规定的时间间隔内还没有被泄漏，来检查请求的有效性，最终的哈希链等于

$$H(a_n, H(a_{n-1}, H(\cdots, H(a_1, MAC(K_{SD}, REQUEST|S|D|id|t_i))\cdots)))$$

式中，a_n 是位于位置 n 的节点地址，同时在节点列表中存在 n 个节点。如果这些条件都成立，请求就是有效的。之后目标节点 D 计算目的地消息认证码（MAC）值 M_D，准备一个“路由回复”消息，并将其沿着通过“路由请求”消息的节点列表

中的单跳序列逆向得到的源路由返回。

$$M_D = MAC(K_{DS}, REPLY \mid D \mid S \mid t_i \mid (A,B,C) \mid (M_A, M_B, M_C))$$

$$D \rightarrow C: \{REPLY, D, S, t_i, (A,B,C), (M_A, M_B, M_C), M_D, ()\}$$

在反向路径中，每个节点都要等待直到它能够公开自己的 TESLA 密钥。之后它将自己的 TESLA 密钥添加进去，并按反向路径发送到下一跳。

$$A \rightarrow S: \{REPLY, D, S, t_i, (A,B,C), (M_A, M_B, M_C), M_D, (K_{C_{ti}}, K_{B_{ti}}, K_{A_{ti}})\}$$

当源接收到“路由回复”消息时，它将验证每个密钥和消息认证码（MAC）值的有效性。如果它们有效，它将接受“路由回复”消息。否则消息将被丢弃。在这之后，路由被维护在“路由缓存”中直到接收到“路由错误”消息。当某个中间节点 B 试图向路由中下一跳节点 C 发送消息失败时，就会生成如下的“路由错误”消息，它将沿着反向路径被送回源节点 S：

$$B \rightarrow A: \{ERROR, B, C, t_i, M_B, K_{B_{ti-1}}\}$$

M_B通过使用在时间 t_i后被公开的下一个 TESLA 密钥 $K_{B_{ti}}$，设为错误消息中先前字段的 MAC 值。反向路径中的每个节点都要等待，直到检测到错误的节点在时间 t_i之后公开其下一个 TESLA 密钥。如果公开的密钥验证通过 MAC 值，路由就从“路由缓存”中被移除。

12.2.4 看门狗路径评价方案

看门狗路径评价（Watchdog Pathrater）方案（Marti et al.，2000）是另外一种安全路由方案，它被设计作为 DSR 的一种扩展。它不是一种预防性技术，而是基于检测和恢复的方法。在这种方案中，每个节点在后台运行两个附加进程，称为看门狗 pathrater。看门狗维护一个传输数据包的缓冲区。它同时监听下一跳节点，观察它们是否将接收到的消息进行了转发，例如被动应答。当下一跳节点转发数据包时，看门狗将其从缓冲区中删除。如果某个数据包在缓冲区中的停留时间长于规定的时间间隔，看门狗将给负责传输数据包的节点的故障计数器加一。如果节点的计数器高于门限值，节点将被标记为行为不端（Misbehaving）。

pathrater 可以基于链路的可靠性和对行为不端节点的认知对链路进行分级。每个节点对网络上的其他节点进行分级。当链路被成功使用时，它的等级将被提高。当链路发生断路时，链路的等级就会降低。大负数值被赋给怀疑存在行为不端的节点。

路径的分级是通过计算路径中各链路的平均等级实现的。当源节点到目的地节点有多条可选路径时，它将选择路径等级最高的路径。含有行为不端节点的路径将被避开。当到目的地之间没有免行为不端链路（Misbehaving-link-free）的路径时，源节点将启动“路由请求”进程。

12.2.5　安全自组织按需距离矢量（SAODV）算法

安全自组织按需距离矢量（Secure Ad hoc On-demand Distance Vector，SAODV）算法为自组织按需距离矢量（Ad hoc On-demand Distance Vector，AODV）算法提供了接入授权、源认证、完整性和数据认证服务。SAODV 假设存在一个密钥管理系统将公钥分配给节点，并验证节点身份和公钥之间的关系（Zapata and Asokan，2002）。这一安全服务中使用了两种机制：保证跳数计数安全的哈希链和认证消息中字段的数字签名。

为了保证跳数计数的完整性，哈希链是对随机选择的种子值 s 应用单向哈希函数 H 生成的。在传输某个路由请求（RREQ）或路由回复（RREP）消息之前，源将给种子 s 赋予哈希值 h。最大跳数被赋予生存时间值 ttl，哈希值 T 的最终值通过对种子值 s 应用 ttl 次哈希函数计算得到。

$$h = s \tag{12-5}$$

$$T = H^{ttl}(s) \tag{12-6}$$

当节点 i 接收到来自源节点的经过 i 跳的消息时，它将首先检查以下条件是否满足：

$$T = H^{ttl-i}(h) \tag{12-7}$$

由于每个中间节点在转发数据之前都将对消息中的哈希值 h 进行一次哈希运算 H，所以当 H 对当前 h 值使用了 $ttl - i$ 次时，它将给出哈希值的最终值 T。否则就表明哈希值 h 或跳数 i 中至少有一个是错误的。在检查之后，节点 i 对 h 进行哈希运算 H，并将其发送出去。

$$h = H(h) \tag{12-8}$$

为了保护消息中其他字段的完整性，源节点会对消息中除被每个中间节点修改的跳数和哈希值 h 字段以外的所有部分进行签名。只要目的地节点允许传回对某个路由请求的路由回复消息时，这样做就足够了。然而，如果某个中间节点存在一条到达目的地节点的新路由，它同样也可以发回一个路由回复消息，而不再继续发送路由请求消息。要做到这一点，中间节点必须能够代替目的地节点对路由回复消息进行签名。

第一种解决办法是不允许中间节点生成路由请求消息，这种方式并不是最理想的，但是很安全。第二种解决办法中，生成路由请求消息的节点包括可以被中间节点使用的数字签名，以及 RREP 标志和前缀大小。当某个中间节点生成一个路由回复消息时，路由有效期相比于中间节点以前接收的最初取值会发生变化。中间节点将同时包含从目标节点获得的旧的有效期值和从路由回复消息中的新的有效期值。旧的有效期值用于验证目的地节点的数字签名。新的有效期值由中间节点进行签名。

12.2.6 安全链路状态路由协议（SLSP）

安全链路状态路由协议（Secure Link State routing Protocol，SLSP）（Papadimitratos and Haas，2003）保证链路状态路由协议中链路状态发现的安全，例如邻居发现和链路状态分布如链路状态更新（LSU）。它不能试图使网络安全免受稍后阶段的攻击，例如传送数据的完整性。

在 SLSP 中，每个节点配有一个公钥 E_v 和一个私钥 D_v，以及一个单向哈希函数 H。节点通过 IP 地址标识身份，同时散播它们的链路状态更新（LSU）数据包，并维持 R 跳内的节点子集的拓扑信息，它被称为一个区域（Zone）。节点周期性地在其区域中广播它们经过验证的密钥，这样接收消息的节点就可以验证它们的链路状态更新数据包。要做到这样，节点要么使用为此目的而特别设计的公钥分发数据包，要么将它们的密钥附加到路由状态更新数据包中。密钥广播根据网络状况和设备特点进行定时。例如，某个节点检测到区域中拓扑发生大量变化时，就会重播其密钥。节点只有在第一次收到始发者的公钥时，才对公钥分发数据包进行验证。经过验证，公钥 E_v 和相应的 IP 地址将被本地进行存储。

每个节点通过广播经签名的“Hello”消息，将自己的媒介访问控制（MAC）地址和 IP 地址（MAC_v，IP_v）向它的邻居节点承诺。接收节点对签名进行验证，并通过保留媒介访问控制（MAC）地址和 IP 地址来更新邻居表。这两个地址记录的映射关系将保存在表中，直到从其他相应节点的传输被窃听。一个丢失邻居节点的超时时间和每个表条目相关联。当在超时时间内没有听到节点的消息时，就从表中删除相应的条目。节点 V 通过链路状态更新（LSU）数据包广播它的链路状态数据：$V \rightarrow \text{broadcast}: \{TYPE, R, Zone\_R, LSU\_Seq, LSU\_signature, Hops\_Traversed, LS\_Data\}$ 这里，$TYPE$ 是数据包类型；R 是节点到区域边界所经过的跳数，且 $Zone\_R = H^R(X)$；$Hops\_Traversed = H(X)$；X 是一个随机值；H 是每个节点已知的哈希函数；LSU_Seq 是 LSU 数据包的序列号；$LSU\_signature = \{TYPE, R, Zone\_Radius, LSU\_Sequence\}_{\langle D_V \rangle}$。

接收节点首先验证签名。如果 LSU 数据包是有效的，它们就可以获得数据包中的链路状态信息。然后，它们会对 LSU 数据包中的 $Hops\_Traversed$ 值进行哈希运算。

$$Hops\_Traversed = H(Hops\_Traversed) \tag{12-9}$$

如果进行哈希运算后的新的 $Hops\_Traversed$ 等于 $Zone\_R$ 的值，就表明数据包已经到达了区域边界，不需再继续转发了。

12.3 进一步阅读

另外还有许多关于自组织网络和传感器网络的安全路由协议。安全辅助定位自

组织路由（Secure Position-Aided Ad hoc Routing，SPAAR）就是其中之一。SPAAR 用于保护高风险环境中的位置信息。在 SPAAR 中，节点通过位置信息的帮助，在包括它们的单跳邻居进入路由之前，验证它们。SIGF（Wood et al.，2006）是另一种依靠节点位置感知的安全传感器网络路由协议。

在 Parno 等（2006）文献中介绍了一种以安全和效率作为主要设计参数的传感器网络路由方案。这种协议包含了所有的三个安全方法：预防、检测/恢复和对攻击的适应性。另一方面，检测和纠正恶意数据（DCMD）方案（Golle et al.，2004）专注于对攻击的检测和受到攻击后的恢复。

在 Buchegger 和 Le Boudec（2002）、Capkun 和 Hubaux（2003）、Pan 等（2007）文献中，介绍了其他的安全自组织网络协议。Fonseca 和 Festag（2006）文献提供了多种安全自组织路由协议之间的分析和比较。

12.4　复习题

12.1　在安全自组织路由协议的设计中，为什么预防性方法要比适应性方法更加有效？

12.2　时间绑定（Temporal Leashes）和地理位置绑定（Geographical Leashes）有什么区别？哪一个更有效？

12.3　设计一个基于定向天线的协议使它可以检测到与接收数据的扇区反向相对的、重放数据包的虫洞攻击。讨论你的设计的实用性和有效性。

12.4　一个节点如何确保它的所有邻居都是物理上相互独立的节点？

12.5　基于正或负应答的方案是否能更好地检测到恶意节点选择性转发？为什么？

12.6　传感器网络中的数据汇聚和多路径路由之间怎样产生联系？

12.7　基于随机游走的方案如何改进安全性？它有哪些缺点？

12.8　幻影泛洪可以在基线泛洪和概率性泛洪技术所提供的保护之外提供什么？

12.9　在 INSENS 的路由发现阶段如何防止电子欺诈攻击？

12.10　active-1-1 或者 active-0-10 攻击更难处理吗？为什么？

12.11　位置信息如何改进自组织路由的安全性？它是否还引入了额外挑战？如果是，是否还值得这样做？

12.12　TESLA 是怎样用于安全路由协议的？为什么？

12.13　你认为 ARIADNE 或者 ARAN 也可以用于传感器网络中吗？为什么？

12.14　在 SLSP 中如何检测一个通过广播公钥分发数据包将自己引入区域的恶意节点？

第 13 章　特定挑战和方案

本章主要讨论针对自组织网络和传感器网络的其他安全挑战。本章并没有对一个特定挑战综述所有解决方案，而是针对每个挑战详细叙述一个或两个著名的方案。我们的目标是介绍特定的挑战和它们的技术问题。

13.1　传感器网络安全协议（SPINS）

第一个挑战是严格的资源限制，特别是在无线传感器网络中。第 2 章讨论了传感器网络的硬件限制。一个典型的传感器节点的可用内存是千字节数量级。另外，一个传感器节点有有限的计算能量，它的寿命取决于自身携带的电池寿命，因此，能量消耗总是一个重要的考虑因素。最后，传感器节点通常发射短数据包，比如 30B。这说明即使一个非常低消耗的安全机制，也可能会引起高开销，例如，3B 就占 30B 包的 10%。

所有这些因素都要求有一种消耗很低的安全方案。例如，需要长签名和高开销的非对称加密方案，每个包有 50 ~ 1000B，这对传感器网络是不实际的。类似地，像 AES 和 DES 这样的分组密码，需要大量计算编码或大的查找表，这对传感器网络可能也是不实际的。SPINS（Perrig et al.，2001b）可能是试图解决这些挑战的最早的安全协议。SPINS 有两个构建模块，即传感器网络加密协议（Sensor Network Encryption Protocol，SNEP）和 μTESLA。它们提供以下安全服务：

1. SNEP

1）数据机密性；

2）认证；

3）数据完整性；

4）新鲜性。

2. μTESLA

认证广播。

13.1.1　传感器网络加密协议（SNEP）

为了加密消息和产生消息认证码（MAC），SNEP 采用了轻量级版本的 RC5。使用了分离的密钥，加密用 K_{encr}；产生消息认证码（MAC）的是 K_{mac}；产生随机数的是 K_{rand}。所有的密钥都是由初始的主密钥自举的（Bootstrapped），这个主密钥是

由基站和节点共享的。一个伪随机函数 F 用来派生出密钥。由于 $F_K(X)=MAC(K,X)$ 是引导密钥的函数，并且消息认证码（MAC）有很强的单向性，所以密钥是计算上独立产生的。这意味着如果有一个密钥被损坏，双方不用传送任何机密信息，就能派生出一个新的密钥。

SNEP 另外一个重要特点是，它是由发送方 A 和接收方 B 共同维护的计数器（Counter）。每一次成功的传输之后，A 和 B 双方将计数器累加，这将确保新鲜性和语义安全。对加密来说，计数器的值是一个输入。因此，即使相同的明文传输了两次，每次传输中的密文也是不同的。这为数据机密性提供了语义安全。

在 SNEP 里，A 方为了发送数据片段 D，发送以下消息给 B 方：

$$A\rightarrow B:\in,M$$

其中，$\in$ 是加密数据片段，例如 $\in=\{D\}_{<K_{\text{encr},c}>}$；$M$ 是消息认证码（MAC），例如 $M=MAC(K_{\text{mac}},c|\in)$；$c$ 是计数器的值。

注意：计数器的值 c 和加密消息 $\in$ 首先连接到一起，即 $c|\in$，并被传给消息认证码（MAC）生成函数。得到的消息认证码（MAC）和加密消息 $\in$ 一起传输。这提供了数据机密性和认证。因为加密和生成消息认证码（MAC）时，均用到计数器的值 c，这也提供了语义安全。计数器还确保了新鲜性。然而，应用在普通 SNEP 里的计数器只能保证弱新鲜性，例如，它能确保相同的消息不被多个节点重放。而强新鲜性，通过发送一个新鲜数（Nonce）η，即一个不可预测的随机数，挑战发送方。为做到这一点，需要做到：

1）节点 A 随机产生一个新鲜数 η_A，把它和请求消息 ρ_A 一起发送。

$$A\rightarrow B:\eta_A,\rho_A$$

2）节点 B 返回应答消息 ρ_B 和经消息认证码（MAC）计算后的 ρ_B 和新鲜值 η_A。

$$B\rightarrow A:\{\rho_B\}_{\langle K_{\text{encr},c}\rangle},\text{MAC}(K_{\text{mac}},\eta_A|c|\{\rho_B\}_{\langle K_{\text{encr},c}\rangle})$$

如果消息认证码（MAC）验证是正确的，节点 A 知道当它发出请求时，节点 B 生成响应。如果需要数据机密和认证，第一个消息也能用普通 SNEP。

13.1.2　μTESLA

μTESLA 用来认证广播消息。它基于消息认证码（MAC），每个消息认证码（MAC）密钥是密钥链里的密钥，这个密钥链是由一个单向函数 F 产生的，即 $K_i=F(K_{i+1})$。这意味着如果你知道以前的密钥，你可以认证下一个密钥，但不能从先前的密钥产生下一个密钥。这是 μTESLA 核心思想之一。

另外一个重要思想是把时间分成密钥公开的时隙 t_i，使所有节点松散地时间同步（见图 13-1）。在每一个时隙中，一个密钥用来产生广播包的消息认证码（MAC），这个密钥在同一时隙的最后将被公开。由于接收方知道之前的密钥，它

们能首先认证那个时隙的密钥；如果此密钥是可信的，则接收同一时隙里所有包。

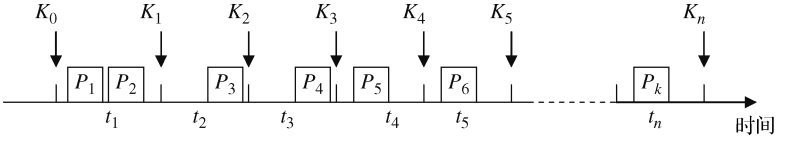


图 13-1 μTESLA 中的密钥公开时隙

一个广播阶段是以发送方建立会话开始的，发送方产生一个从 K_n 开始的密钥集合 $K=\{K_0,K_1,K_2,\cdots,K_n\}$。然后，松散的时钟同步应该完成，所有的接收者需要用 K_0 自举。为完成这些，发送方 S 比如广播节点，通过发送一个新鲜值 η 受到挑战。这个方案工作过程如下：

1）接收方节点 R 随机产生一个新鲜值 η_A，把它发给发送方 S。

$$R\rightarrow S:\eta_A,\rho_A$$

2）发送方 S 回复消息，这个消息包含现在时间 T_s、在之前密钥泄漏时间间隔用到的密钥 K_i、之前时间间隔 T_i 的开始时间、密钥泄漏时间间隔 T_{int} 的长度及泄漏延迟 δ，例如，在泄漏时间间隔 δ 为泄漏密钥的最大延迟。

$$S\rightarrow R:T_s\,|\,K_i\,|\,T_i\,|\,T_{\text{int}}\,|\,\delta,MAC(K_{SR},\eta_A\,|\,T_s\,|\,K_i\,|\,T_i\,|\,T_{\text{int}}\,|\,\delta)$$

回复里的消息认证码（MAC）用到了发送方和接收方共享的密钥。由于 μTESLA 不是针对机密性，而是为了认证广播节点，发送方不需要加密回复的内容。

13.2 垃圾邮件攻击的隔离区方案

隔离区方案（Quarantine Region Scheme，QRS）是由 Coskun 等（2006）提出的，它是另一种降低数据安全方案成本的方法。在 SPINS 里，已经设计了低成本的认证和加密机制。类似地，隔离区方案使用了一种低成本的认证机制。另外，它试图定位被称为“反节点”（Antinodes）的恶意节点以及在反节点范围内的节点。覆盖所有反节点及在反节点范围内的节点的区域称为隔离区（Quarantine Region）。只有在隔离区内的节点需要认证。这相当大地降低了认证的成本，同时阻止恶意节点运行耗尽网络资源的有效攻击（参看 8.1.2.3 节“拒绝服务攻击”）。

在 QRS 里，隔离的节点集合和隔离区用分布式方法动态确定。通过间接检查在传输范围内的认证失败，每个传感器节点自己决定它是否应该隔离。认证检查的持续时间是被定义为一个系统参数的随机变量，将在这一小节的剩余部分描述。

未隔离节点在两个交替的周期里有两种不同的工作模式：① 在检查状态的周期里，节点核查垃圾邮件活动；② 在保持状态周期，节点不执行任何垃圾邮件检查。

在一个检查状态周期 t_c 里，一个传感器节点不会转发没有认证的消息。如果它在 t_c 内，收到一个没有认证的消息，它会首先要求来自消息上一跳节点的认证；若上一跳节点认证失败，这说明上一跳节点可能是反节点；因此节点将状态转变为隔离。隔离区的概念如图 13-2 中举例所示。隔离区基本上是一个抽象区域，反节点的传输可能被接收到。由于不可预测的传播环境，此区域没有固定的形状。隔离区的节点是在 t_c 里捕获反节点垃圾信息的节点。

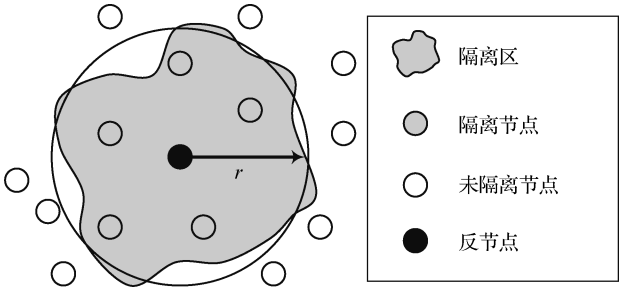


图 13-2　隔离区边界

图 13-3 所示的是一个传感器领域的例子。隔离区标识为灰色区域。节点 3、4、7、8 和一个反节点在隔离区里，因此它们必须发送和转发已认证的消息。即使是来自隔离区的最初已认证的消息，隔离区外的节点发送消息时，无需认证，除非消息要通过隔离区。例如，由于节点 11 不在隔离区，如果它收到来自节点 7 或 8 已认证的消息，节点 11 无需认证，直接将信息发送给汇聚节点（Sink）。另一方面，如果一个在隔离区的节点（例如节点 3）收到来自隔离区外的节点（例如节点 1 或节点 2）传来的未经认证的消息，它首先请求来自相应节点的认证，只有经过成功的认证之后，再转发数据包。

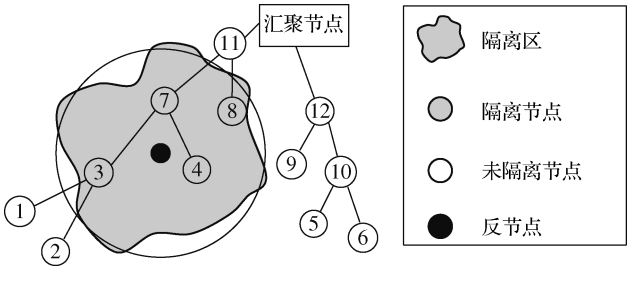


图 13-3　一个样本传感器网络和隔离区

QRS 是一个动态的机制，传感器节点可以周期性地检查节点状态的有效性。如果一个节点在检查状态周期 t_c 内，没有检测出认证失败，节点状态就变为未隔离。节点保持一段保持状态周期 t_k，经过时间 t_k 后，节点开始新一轮的检查状态周期。如果节点在检查状态周期检测到认证失败，它就会把状态变为“已隔离”。这

就是图 13-4 中 a 点描述的情况：节点在 a 点检测到认证失败，则启动一个隔离期。节点处在保持状态周期时检测到另一个认证失败，它立即就会启动新一轮的保持状态周期。只有在持续的保持状态周期里，节点没有检测到任何认证失败，它才会退出隔离模式，启动一个检查状态周期。

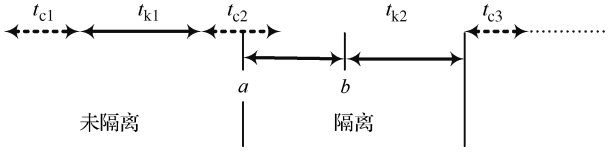
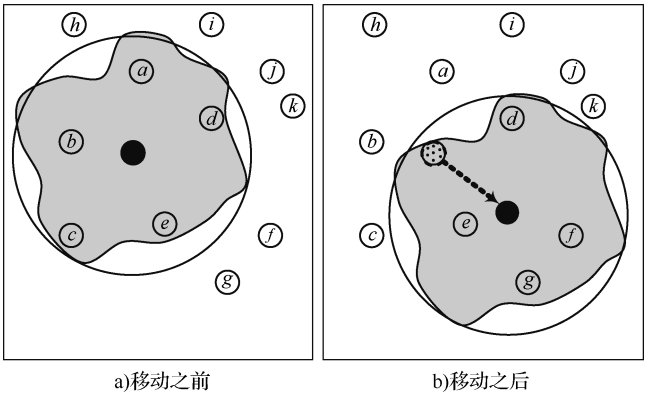


图 13-4　隔离周期计时

t_c 和 t_k（例如，$t_c \geqslant t_{cmin}$，$t_k \geqslant t_{kmin}$，$t_c \in R^+$，$t_k \in R^+$）都是为各个周期选择的随机变量，即 t_c 和 t_k 在每个检查状态周期和保持状态周期可能是不同的。传感器节点根据系统定义的平均值、分布函数以及 t_{cmin}、t_{kmin} 确定 t_c 和 t_k 的值。由于反节点可能是移动的或者传播环境会暂时改变，所以需要这种动态的方法。

图 13-5 用一个例子解释了这个过程以及它怎样动态地改变隔离区的位置。在这个例子中，节点 a、b、c、d 和 e 独立地、异步地找出它们传输范围内的一个节点，这个节点在时间 t_c 结束时，不能成功地认证，如图 13-5a 所示。因此它们变成隔离的（Quarantined）。节点 f 和 g 不在反节点的传输范围内，因此它们不能在时间 t_c 内检测到任何认证失败，它们变成未隔离的（Not Quarantined）。如图 13-5b 所示，反节点移动到一个新的位置，传输覆盖范围也发生了变化：节点 f 和 g 被纳入了新的范围。由于节点 f 和 g 在每个保持状态周期 t_k 后，会启动检查状态周期，它们会在第一个检查状态周期发现它们已处在反节点的范围内，则变成隔离的。另一方面，当节点 a、b 和 c 在整个保持状态周期 t_k 没有检测到任何认证失败时，它们就把状态更改为未隔离的。



a)移动之前　　b)移动之后

图 13-5　隔离区边界变化

当某个节点是未隔离的，在其处于保持状态周期时，垃圾邮件信息可能会通过该节点。本地告警（Local Alarms）是用来使在此刻通过网络的垃圾邮件信息影响减至最小。一个检测到认证失败的节点向它的 d 跳（d-hop）邻居散播一个本地告警。这个本地告警是通过调用本地告警广播（broadcast_local_alarm）功能完成的，d 称为本地告警深度。节点一收到本地告警，它就开始了检查状态周期。通过使用本地告警机制，节点变得更警觉，未请求消息从一个节点通过的周期变得有限了。

一旦节点发出一个本地告警，它不应该在周期 kt_k 内再发送另一个本地告警，即使该节点又收到了其他垃圾邮件信息，其中 k 是本地告警因子，$k \in \mathrm{R}^+$。这么做是为了使网络不被本地告警淹没。图 13-6 所示的例子，展示了受到攻击的节点发出本地告警时。节点在 a 点第一次侦测到了未经请求的消息，于是它发出一个本地告警。在等待至少时间 kt_k 之后，该节点发出另一个本地告警。在这段时间内，节点既不对检测到的垃圾邮件信息发送本地告警，也不转发其他节点的本地告警消息。例如，在 b、c 和 d 点，节点侦测到了其他的非请求消息，但它没有发出本地告警。过了时间 kt_k 后，在 e 点检测到非请求消息之后，节点发出另一个本地告警。

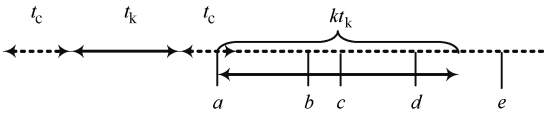


图 13-6　本地告警计时

通过使用本地告警，隔离区周围的缓冲带也随之被创建，如图 13-7 所示。在缓冲带内的节点仍然是未隔离的，但却比未隔离的节点更灵敏。缓冲带的节点和未隔离的节点运行的是同一个算法。它通过乘以一个保持状态因子 s，$0 < s < 1$，缩短保持状态周期。节点一收到本地告警就启动检查状态周期，这表明该节点在隔离区的缓冲带里。如果在时间 kt_k 里，它没有收到另一个本地告警，则节点可以假设它不在缓冲带里。

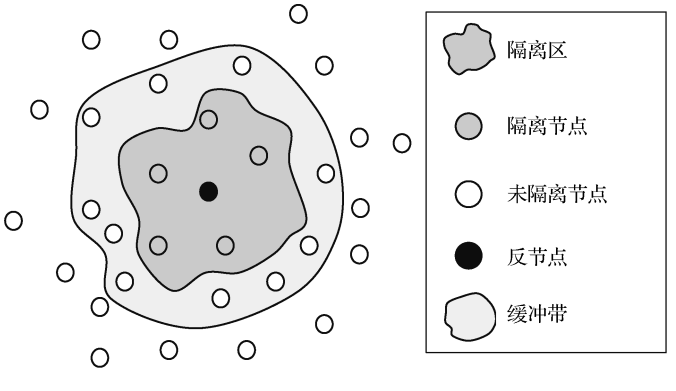


图 13-7　缓冲带（Buffer Zones）

QRS 机制还可以处理具有长传输距离的反节点。这种反节点能从一段距离之

外试图攻击整个传感器网络。QRS 独立于反节点的位置和传输范围。由于反节点不能被认证，无论它在哪里广播垃圾邮件信息，传感器节点都不会转发这种消息。在 QRS 里，只有能接收到反节点传输的节点需要认证，其他节点则不需要认证。

13.3 安全计费和奖励机制

计费和奖励机制是面向那些接收来自多跳蜂窝网络的服务却拒绝付费的节点的。这被称为关于计费机制的行为不端，在 8.1.2.4 节中已详细地讨论过。

图 13-8 描述了一个范例场景。节点 A 发起了与节点 B 的通信。节点 A 经过多跳后从基站 BS_A 接入基础设施，从 A 到基站 BS_A 的路由称为上行路由（Upstream Route）。节点 B 经过多跳后从基站 BS_B 接入基础设施，从 BS_B 到 B 的路由称为下行路由（Downstream Route）。转发从 A 到基站 BS_A 数据包的节点是上行转发节点；BS_B 和 B 之间的节点称为下行转发节点。在我们的范例中，有一个上行转发节点如 u 和一个下行转发节点如 f。

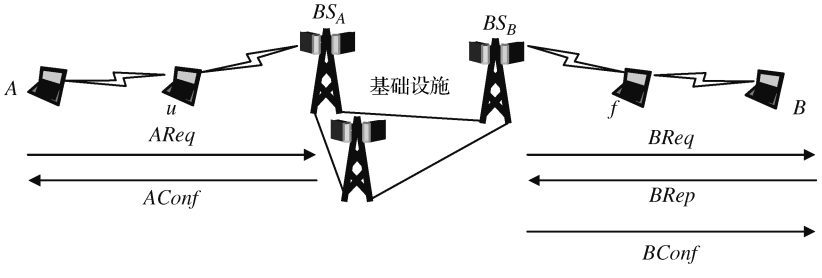


图 13-8 多跳蜂窝网络中的计费和奖励会话创建

计费和奖励方案（Charging and Rewarding Scheme，CRS）是由 Salem 等在 2003 年提出的，它基于以下方法：

1）认证初始节点 A，并在数据包实际传输之前，使其为通信付费。这样可以防止拒付费攻击。

2）识别转发节点，并认证它们。这样可以确保只有被选中的节点才能转发；没有转发的节点不能宣称它们已经转发了。

3）当数据包由 A 到达 BS_A 时，奖励上行节点。

4）当 B 确认来自 A 的数据包已传到 B 时，奖励下行节点。

5）当来自 A 的数据包通过 BS_B 转发到 B 时，对 B 收费；当 B 确认数据包传输时，补偿 B 的这一计费，这是对能够奖励下行转发节点所需的。

13.3.1 建立会话

A 通过发送一个建立请求 *AReq*，启动会话创建程序，格式如下：

$$A \rightarrow BS_A : AReq_0$$

$$AReq_0 = AReqID \mid oldASID \mid ARoute \mid TrafficInfo,$$

$$MAC(K_A, AReqID \mid oldASID \mid ARoute \mid TrafficInfo)$$

AReqID 是顺序产生的请求标识。如果请求重建一个之前失效的会话，则这个失效会话的标识 *oldASID* 也会出现在请求里。如果没有重建，*oldASID* 为 0。CRS 假设有一个支持该机制的安全源路由协议。*A* 从安全的源路由协议中得到 *A* 和 BS_A之间的路由例如 *ARoute*，将它包含在 *AReq* 里。最后，将要发送的关于流量的信息即 *TrafficInfo*，也和消息连接在一起。*A* 也会通过使用密钥 K_A，对总的消息生成消息认证码（MAC）。

每个上行转发节点 *i* 都会检查 *TrafficInfo*。如果节点 *i* 决定要在这个连接中发送未来的数据包，通过使用它自己的密钥，它将对收到的前一个上行转发节点的请求计算出消息认证码（MAC），即 $AReq_{i-1}$，替换请求里的消息认证码（MAC），然后把 $AReq_i$ 发送给下一个上行转发节点。

$$AReq_i = AReqID \mid oldASID \mid ARoute \mid TrafficInfo, MAC(K_i, AReq_{i-1})$$

因此，传送到 BS_A的请求包括由 *A* 和所有上行转发节点计算出来的一个消息认证码（MAC）。BS_A重复所有消息认证码（MAC）计算，来与收到请求里的消息认证码（MAC）核对结果。这也能证实 *AReqID* 是新的。这个过程认证上行路由的所有节点，也认证 *A*。最后，如果 *oldASID* 值不为 0，BS_A也会检查它是否有效。如果有任一验证不成功，则 BS_A会丢掉请求。否则，它会通过主干将请求发送给 BS_B。

当 BS_B收到请求时，它将请求转发给将发到 B 的第一个下行转发节点：

$$BS_B \rightarrow B : BRq_0$$

$$BReq_0 = BReqID \mid oldBSID \mid BRoute \mid TrafficInfo$$

注意，*BReqID* 是由 BS_B产生的新的标识。像上行节点一样，每个下行节点 *j* 也会检查 *TrafficInfo* 来决定是否参加会话，在转发之前，生成新消息认证码（MAC）并替换 $BReq_{j-1}$里的 MAC：

$$BReq_j = BReqID \mid oldBSID \mid BRoute \mid TrafficInfo, MAC(K_i, BReq_{j-1})$$

当 *B* 收到请求时，如果它接受这个连接，则 *B* 会准备回应并发回。回应只包括 *BReqID* 和消息认证码（MAC）。它们是由上一个下行转发节点发送给 *B* 的总消息产生的：

$$BReq_j = BReqID, MAC(K_B, BReq_{B-1})$$

BReq 经过同样的下行路由，不做修改地传回 BS_B。BS_B产生该路由的消息认证码（MAC），并与返回的消息认证码（MAC）核对。如果通过验证，它会通知 BS_A。然后 BS_A和 BS_B分别产生确认消息 *AConf* 和 *BConf*，将它们发给 *A* 和 *B*：

$$AConf = AReqID \mid ASID \mid AMAC_A \mid AMAC_1 \mid \cdots \mid AMAC_a$$

$$AMAC_i = MAC(K_i, AReqID \mid ASID \mid oldASID \mid ARoute \mid TrafficInfo)$$

$$BConf = BReqID \mid BSID \mid BMAC_A \mid BMAC_1 \mid \cdots \mid BMAC_a$$

$$BMAC_j = MAC(K_j, BReqID \mid BSID \mid oldBSID \mid BRoute \mid TrafficInfo)$$

每个初始路由的节点 i 和对应路由的节点 j 验证各自的 $AMAC_i$ 和 $BMAC_j$，然后分别存储会话标识 *ASID* 或 *BSID*。当收到确认消息时，会话建立。

13.3.2 包传递

在包传递中，源 S 可能是初始节点 A 或是对应节点 B，目的地 D 也可能是 A 或 B（可交替）。在任一情况下，A 为通信付费。当 B 把一个包发给 A 时，只要 A 一确认，就要暂时计费并补偿。这是为了防止 B 的不端行为和欺骗 A。

由 S 发出的第 η 个包 $SPkt_{0,\eta}$ 包括会话标识 *SSID*（如果 S 是 A，则是 *ASID*；如果 S 是 B，则是 *BSID*）、序列号 η 和负载 $payload_\eta$。另外，消息体包括用密钥 K_S 对包计算的消息认证码（MAC）：

$$SPkt_{0,\eta} = SSID \mid Body_{0,\eta}$$

$$Body_{0,\eta} = \eta \mid Payload_\eta \mid MAC(K_S, SSID \mid \eta \mid Payload_\eta)$$

$SPkt_{0,\eta}$ 里的消息认证码（MAC）只能被 BS_S 验证，因此所有的上行节点忽略它。相反，每个上行节点 i 加密包体，包括消息认证码（MAC）与 $PAD_{i,\eta}$ 进行异或：

$$SPkt_{i,\eta} = SSID \mid Body_{i,\eta}$$

$$Body_{i,\eta} = PAD_{i,\eta} \oplus Body_{i-1,\eta}$$

PAD 是由流密码产生的。会话标识 *SSID* 和密钥 K_i 是初始化流密码的种子。$PAD_{i,\eta}$ 被选作长度为 *MaxLength* 的第 η 个分组，这是以字节为单位允许的最大包长度。如果包实际长度小于 *MaxLength*，丢弃不必要的字节。

当收到包时，源节点的基站 BS_S 验证包的完整性和 *SSID*。如果验证失败，则丢包。否则，它将包发送给目标节点的基站 BS_D，这时 *SSID* 更换为 *DSID*，计算出新的消息认证码（MAC），为每个下行节点 j 计算 $PAD_{j,\eta}$，用每个 $PAD_{j,\eta}$ 和包做异或运算。每个下行节点 j 一收到包，首先用它的 $PAD_{j,\eta}$ 将包解密，然后发送给下一个下行节点。因此，当包被传至 D 时，所有的加密 *PAD* 被解开。

13.3.3 应答传递

目标 D 必须确认收到包。但是，并不是对每一个包确认。当 D 认为会话将结束时，发送一个如下格式的批确认：

$$DAck = DSID \mid Batch \mid LastPkt \mid LostPkts,$$

$$MAC(K_D, DSID \mid Batch \mid LastPkt \mid LostPkts)$$

为了计算 *Batch*（批确认），每一个包的 $MAC(K_D, SSID \mid \eta \mid Payload_\eta)$ 需要确认，例如，除了丢失的包以外，所有的包都要异或计算。注意，*LostPkt* 是上个接收包的

序列号；*LostPkts* 是没有成功传递包的序列号列表。

13.3.4　终止会话

当会话发起时，参与会话的每个节点启动一个定时器。会话中一个包被转发，这个定时器就设置一次。当定时器终止时，节点就会关闭会话，这意味着节点从内存中删除相关的状态信息。关闭会话还有一个原因是检测出了以下某个错误：

1）包不能转发到下一跳；

2）源节点 S 收到了带有未知会话标识的包；

3）节点不再想参加转发包。

13.4　安全节点定位

节点定位在许多自组织网络应用中具有关键作用，特别是在无线传感器网络中。对节点定位方案的攻击能阻止自组织网络完成预期功能。正如在第 8 章中讨论的那样，有很多特别以定位方案为攻击对象的安全攻击。有一些方法可以抵御这些攻击：

1）防止伪装、重放、篡改节点的技术也会对安全定位机制有益。

2）安全的路由技术可以抵御用于阻碍节点定位的虫洞攻击。

3）多模定位（Multimodal Localization）机制能用于估计到信标的距离，这种节点定位是基于同时使用接收信号强度指示器（Received Signal Strength Indicator）和到达时间差（Time Difference Of Arrival）等多种方案。如有不一致，这表示可能是一个恶意节点。

4）可以进一步发展评估信标可靠性的特殊技术；这些技术会被挑战，产生的数据一致性会被检查，每个信标节点会被分配一个表示可靠性等级的值。

5）可以用统计方法检查来自信标节点数据的一致性，不一致的数据会被丢弃。

6）一个节点定位机制会被设计得足够健壮，来容忍少数输入错误。在这一节里，我们将详细阐述遵循这些方法的几个方案。

13.4.1　检测恶意信标节点和重放信标信号

产生错误定位信息的节点能被已知它们位置的节点检测到，典型的是被其他信标节点检测到。为做到这一点，从另一信标节点 n_a 收到信标信号的信标节点 n，能根据收到的信标信号估计出它的位置（x'，y'），然后比较实际的位置（x，y）和估计的位置。如果这两个位置的差高于特定门限值 τ，这可能表示产生信标信号的节点 n_a 是恶意的。在 Liu 等（2005a）文献中，这一方法用于这种情况，即位置估计基于接收信号强度指示器（Received Signal Strength Indicator，RSSI），并且当非

信标节点发出请求时，信标信号单播给非信标节点。该方案由下列步骤组成：

1）一个信标节点 n，例如检测信标，请求一个来自另外信标节点的信标信号 B_{req}。这个检测信标执行功能时，就好像它不是信标节点。

$$n \rightarrow n_{\text{a}} : B_{\text{req}}$$

2）目标信标发送一个信标信号 B_{beacon}。信标信号通常也包括目标信标 n_{a} 的位置（x_{a}，y_{a}）。

$$n_{\text{a}} \rightarrow n : B_{\text{beacon}}$$

3）检测信标根据 RSSI 计算，估计到目标信标位置（x_{a}，y_{a}）的距离 d_{a}。

4）因为检测节点已经知道它的位置，就能计算出它到 B_{beacon} 发出的目标节点位置的距离 d。如果估算距离 d_{a} 和计算出的距离 d 的差高于门限值 τ，这表示这个目标节点是恶意的，即

$$\text{如果} \left| \sqrt{(x - x_{\text{a}})^2 + (y - y_{\text{a}})^2} - d_{\text{a}} \right| > \tau, \text{则目标节点是恶意的}$$

虽然这项技术能检测出信标信号的异常，但是因为信标信号可能会被其他节点重放，所以它们不能总是指出信标是恶意的。当受到虫洞攻击时，这种情况尤为突出。为了处理这个问题，被重放的信标信号应该被过滤掉。在之前章节中讲过的阻止虫洞攻击的技术，能消除经由虫洞发送的信标信号。然而，它们不能检测出局部重放的信标信号，例如与一个信标为邻的恶意节点阻塞了它的信号，重放信标信号，就好像恶意节点是信标节点一样。

在 Liu 等（2005a）文献中介绍了基于往返时间（Round Trip Time，RTT）的方案。在这个方案中，在部署之前，两个节点之间的最大 RTT 期望值被测试并已知。节点对一个信标信号挑战信标，用式（13-1）计算出信标信号的 RTT。如果计算出的 RTT 高于 RTT 期望值，这说明它是被重放的信标信号，因此丢弃。

$$\text{RTT} = (t_4 - t_1) - (t_3 - t_2) \tag{13-1}$$

式中，t_1 是发送方发送完第一个比特的时刻；t_4 是它接收完回复中的第一个字节的时刻。基本上，$(t_4 - t_1)$ 是发送方发送请求和收到回复的时间差。t_4 和 t_1 在发送方都是可用的。然而 $(t_4 - t_1)$ 也包括了回复方处理的时间和由于消息认证码（MAC）的延迟。因此，这个值会基于许多参数不同而不同。为了从 RTT 中消除这些不可预测的因素，从中减去 $(t_3 - t_2)$。$(t_3 - t_2)$ 是接收方收到请求的第一个字节时刻 t_2 和发送完回复的第一个字节时刻 t_3 的时间差。

检测到恶意信标不足以阻止它们的攻击。一个恶意节点会声称信标是敌手。因此，一个机制需要确保检测信标是友好的，它们的报告是正确的。为达到这一目的，Liu 等（2005a）文献中依靠信标节点和基站之间的认证机制。信标向基站报告它们的发现。基站为每一个信标维护一个报告和警报计数器。信标不允许以超过规定的速率报告。为此，使用了报告计数器。每个警报计数器是信标的可靠性值。每当收到一个信标的负面报告时，它的警报计数器值增加。当警报计数器值超过门

限值时，信标被撤销。

13.4.2　抗位置估计攻击

位置数据的不一致性能通过检查均方差估计值（MMSE）检测到，如下式给出：

$$\varepsilon = \frac{\sum_{i=1}^{m} \left(d_i - \sqrt{(x - x_i)^2 + (y - y_i)^2}\right)^2}{m} \tag{13-2}$$

式中，ε 是均方差；(x_i, y_i) 是信标节点 i 的位置；(x, y) 是估算位置；d_i 是到信标节点 i 的距离；m 是用于估算位置使用的信标节点数。

当对于至少三个信标节点 n_i，三元组 (x_i, y_i, d_i) 是已知的，即三边测量（trilateration）法，我们通过最小化 ε 推导出 (x, y)。由于估算 d_i 时总会有误差，ε 在实际中永远不为 0，但是，如果所有节点都是良性的，它应该降至可以接受的水平。基于这种观察，Liu 等（2005b）文献提出了一个把错误数据从位置估算中过滤掉的方案。这个均方差 ε 称为不一致指示器（Inconsistency Indicator）。当不一致指示器 ε 超过门限值 τ 时，说明存在引入错误数据的恶意节点。方案的目标是找到用于估算位置的信标节点最大集，使得不一致指示器 ε 低于门限值 τ。为此，提出了一个贪心算法。该算法以从 n 个信标节点收到的所有信标信号开始。如果不一致指示器 ε 在门限值 τ 之上，则 $n-1$ 个信标节点就尝试联合在一起。第一个返回低于门限值 τ 的不一致指示器 ε 的联合，被选择作为一个解答。如果 $n-1$ 个信标节点没能解决问题，这可能说明有不止一个恶意节点，然后检查 $n-2$ 个信标联合。这个过程一直持续下去，直到找到不一致指示器 ε 低于门限值 τ 的一个解答，或者对三个或更多节点联合，仍然没有解答。后一种情况说明使用可用的信标信号不能估算出位置。

确定门限值 τ 大小是该算法的一个重要问题。如果门限值过高，恶意信标信号可能检测不到。另一方面，当它太低时，一些良性的信标信号可能被判为错误的，并被过滤掉。在 Liu 等（2005b）文献中，不一致指示器的分布是由仿真和分析研究得出的，这用来确定门限值。进行现场实验也能得到门限值的分布。

Li 等（2005）文献还介绍了一种类似的健壮的统计方法。把它留给读者作为进一步的阅读练习。

所有这些统计方法都假设低于某个门限值的误差是可以接受的，这个误差取决于信标节点的数量和信标节点与其他节点的平均距离。另一个基于同样假设的抵御攻击的定位技术称为基于投票的位置估算法（Voting-Based Location Estimation）（Liu et al.，2005b），其中场被分成更小的正方形单元格，每个单元格基于信标信号被赋予一个值，如图 13-9 所示。在基于投票的方案中，单元格的值是从信标节

点 i（到其他节点）的范围 $d_i - e$ 到 $d_i + e$的距离，它是递增的。d_i是从信标节点 i 的估算距离，e 是可接受的误差。距离 d_i是由节点 i 的信标信号产生的。

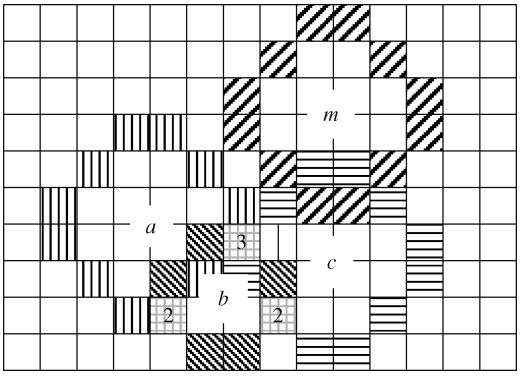


图 13-9　节点定位的投票方案

对每一个收到的信标信号做完这些之后，有最大值的单元格中心就是节点的位置。例如，在图 13-9 中，有来自节点 a、b、c 和 m 的四个信标信号。节点 a、b 和 c 是良性的。当应用基于信标信号的投票方案时，它们中的一个单元格有三张选票，两个单元格有两张选票，其他所有单元格有一张或没有选票。对恶意节点 m 应用信标信号不改变这个结果，有三张选票的单元格的中心就是节点位置。

13.5　安全时钟同步

时钟同步的安全威胁和抵御威胁的防卫机制与节点定位里的威胁和对策是类似的。在本节中，我们介绍一些检测针对同步方案的重放攻击的技术。一个恶意节点可以阻塞同步消息，稍后再重发该消息。这叫做重放攻击，可能会对时钟同步有不利影响。本节提到的技术在 Ganeriwal 等（2005）文献中有介绍，该技术是基于 RTT 观测的，就像节点定位中抵抗重放攻击的技术（Liu et al.，2005a）。注意这种技术不能保证重放攻击下的时钟同步，但是能检测出重放攻击。它包括三个步骤（Ganeriwal et al.，2005）：

1）步骤 1：$A(t_1) \rightarrow (t_2)B: A, B, N_A, synch$。

节点 A 在 t_1时刻发送给节点 B 一个同步消息，节点 B 在 t_2时刻收到消息。该消息包括节点 A 和 B 的标识、一个新鲜值 N_A（即节点 A 产生的随机数）、时间戳 $synch$。如在之前章节所介绍，新鲜值用来保证包的长期新鲜性。这防止恶意节点使用从同步消息窃听的消息认证码（MAC）。

2）步骤 2：$B(t_3) \rightarrow (t_4)A: B, A, N_A, t_2, t_3, ack, MAC(K_{AB}, B \mid A \mid N_A \mid t_2 \mid t_3 \mid ack)$。

节点 B 在 t_3时刻回复节点 A，节点 A 在 t_4时刻收到回复信息。时刻 t_1和 t_4对节点 A 是已知的。因此，节点 B 告知节点 A 时刻 t_2和 t_3。N_A 也在回复消息里，它也用于识别被回复的消息。用回复消息和节点 A 和 B 之间的密钥 K_{AB}产生的消息认证码（MAC）也附加在消息中。

3）步骤 3：如果$(t_4 - t_1) - (t_3 - t_1) < \theta$，继续运行。否则，中止。

节点 A 计算 RTT。如果 RTT 小于最大 RTT 门限值，同步完成。否则，同步失败。

Ganeriwal 等（2005）文献里还介绍了为多跳和群发送者/接收者同步设计的类似安全方案。

13.6　安全事件和事件边界检测

对很多应用而言，传感器网络的最终目的是检测出预定义事件或目标集合，并把它们分类。传感器网络技术能部署很多传感器节点，使得多个节点能检测出相同的事件。因此，它们依靠许多节点的协作努力来侦测出一个事件。

实际上一个事件很少发生在一个单独的点上，但是会影响到整个空间。例如，一次化学攻击能污染一大片区域。这种区域的边界称为事件边界（Event Boundary），检测边界也是传感器网络的一项重要任务。这项任务在恶意节点或错误节点出现时，会更具挑战性。敌手可能会尝试注入错误数据来阻止传感器网络正确地检测出事件或事件边界。像认证和加密的传统技术能用来防御此类攻击。一项可替代或互补的技术是基于这样的事实：每个节点周围有其他的节点能检测出同一事件；传感器网络中的节点能通过协作来过滤错误的事件数据。

在 Ding 等（2005）文献中提出的事件边界检测机制，能在多至 20% 的节点错误时，正确地检测出事件边界。这些错误节点包括恶意节点或有故障的节点等。他们假设在二维欧几里得平面 R^2 里，N 个节点均匀部署。由 E 表示的事件是 R^2 的子集，以致在 E 内节点的读数和在 E 外节点的读数有很大不同。当任意以 x 为中心的盘面包含了 E 内和 E 外的点时，点 $x \in \mathrm{R}^2$ 称为在 E 的边界里。这个方案有三个阶段，其概要如下所述。

13.6.1　阶段 1：错误节点检测

Ding 等（2005）文献中的基本思想是传感器的测量应该与其附近的事件相关，这些事件也能被事件边界里的其他节点检测出来。因此，他们比较了传感器 S_i 和在集合 $N(S_i)$ 中的传感器的读数。$N(S_i)$ 表示传感器 S_i 的附近的邻居。令 x_i 表示传感器 S_i 的读数，x_{i1}，x_{i2}，…，x_{ik}表示 $N(S_i)$ 内其他节点的读数。d_i是 x_i和 $\{x_{i1}, x_{i2}, \cdots, x_{ik}\}$ 中心的差值：

$$d_i = x_i - med_i \tag{13-3}$$

式中，med_i 是 $\{x_{i1}, x_{i2}, \cdots, x_{ik}\}$ 的中值，但不是平均值，例如不是 $(x_{i1} + x_{i2} + \cdots + x_{ik})/k$。中值是首选的，因为它是样本中心的鲁棒估计值，并能过滤出极值。

下一步是检查传感器 S_i的差值是否正常或与 S_i附近其他 $n-1$ 个传感器的差值 d 相比是否过大。为此，另一个在传感器 S_i周围的传感器有界闭集 $N^*(S_i) \subset \mathrm{R}^2$ 被

选中。典型的 $N^*(S_i)$ 比 $N(S_i)$ 要大，但也可以等于 $N(S_i)$。$N(S_i)$ 是为了计算差值 d_i 的，而 $N^*(S_i)$ 是为了计算传感器 S_i 附近集合 $D=\{d_1,\cdots,d_i,\cdots,d_n\}$ 的均值 μ 和标准方差 σ 的。然后，对 $N^*(S_i)$ 里的每个传感器计算 d 值。例如图 13-10 中，$N(S_1)$、$N(S_i)$ 和 $N(S_n)$ 分别用来计算 $N^*(S_i)$ 里的传感器 S_1、S_i 和 S_n 的差值 d_1、d_i 和 d_n。注意：

$$N(S_i)\subset N^*(S_i)$$

$$N^*(S_i)\subset(N(S_1)\cup N(S_i)\cup N(S_n))$$

$$N^*(S_i)=\{S_1,\cdots,S_i,\cdots,S_n\}$$

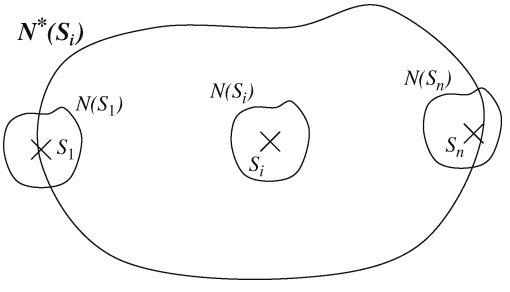


图 13-10 计算差值的邻居集

集合 $D=\{d_1,\cdots,d_i,\cdots,d_n\}$ 的均值 μ 和标准方差 σ 如下：

$$\mu=\frac{1}{n}\sum_{i=1}^{n}d_i \tag{13-4}$$

$$\sigma=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d_i-\mu)^2} \tag{13-5}$$

现在，根据传感器附近其他节点的差值，可以将它们的差值通过下式标准化：

$$y_i=\frac{d_i-\mu}{\sigma} \tag{13-6}$$

标准化差值 y_i 能很好地指示出传感器 S_i 是否产生了错误的读数。如果 $|y_i|\geqslant\theta$，$\theta>1$ 是预定义的门限值，则我们能得出结论，S_i 是错误的。需再次说明，门限值 θ 是一个重要的值。如果它太低，正确的读数会被当成错误的接受。另一方面，如果它太高，错误消息可能不会被检测出来。

13.6.2 阶段 2：事件边界节点检测

令 Ω_1 表示在第一阶段发现的错误节点的集合。在第二阶段，事件边界节点从不在 Ω_1 的节点中挑出，即 $S-\Omega_1$。为此，节点 S_i 的差值 d_i 在把 $N(S_i)$ 分解成更小的邻域 $NN(S_i)$ 之后，要重新计算。对一个事件边界节点，大部分在事件区域 E 外的子域的差值要高于在事件区域 E 内的子域差值。这一观察被用于定位边界上

的节点。

例如，在图 13-11 中，代表 $N(S_i)$ 的盘面被分成了三个 120°的扇区。假设 S_i 是在事件边界上的节点，这意味着 S_i 检测事件，例如它在事件区域 E 里，但是许多在 $N(S_i)$ 内的节点不能检测事件，因为它们不在 E 里。因此，扇区 A 和 B 的差值 d_{iA} 和 d_{iB} 会比扇区 C 的差值 d_{iC} 高，因为扇区 C 内所有的节点像 S_i 一样检测事件，而扇区 A 和 B 的许多节点不是这样。

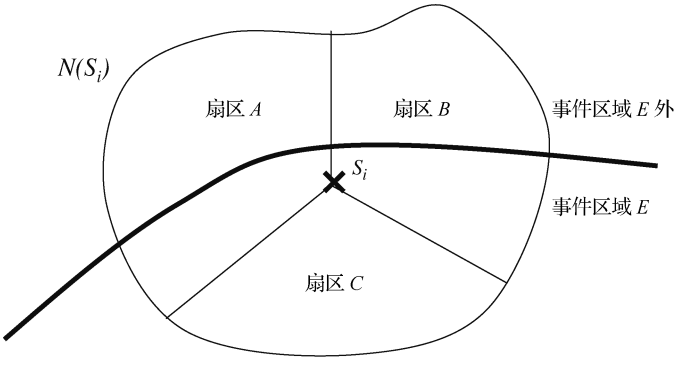


图 13-11　邻居盘面的分割

Ding 等（2005）文献中对检测边界节点的算法概括如下：

1）通过运行阶段 1 的算法，构造错误节点集合 Ω_1。

2）对不在 Ω_1 里的每一个传感器 S_i，即 $S_i \in S-\Omega_1$，执行以下步骤：

① 把 $N(S_i)$ 分割成扇区。

② 计算每个扇区 j 的差值 d_{ij}。

③ 分配最大的 d_{ij} 作为新的 d_i 给 S_i。

④ 不用改变其他节点的差值，为 $N^*(S_i)-\Omega_1$ 和新 d_i 重新计算均值 μ、标准方差 σ 和 y_i。

⑤ 如果重新计算后 $|y_i| \geqslant \theta_2$，S_i 进入由 Ω_2 表示的边界节点集合。

13.6.3　阶段 3：改进事件边界节点检测

在事件边界上节点 S_i 的标准化差值 y_i，正常情况下比在事件边界内或外的节点差值高。因此，在 Ω_1 的一些节点，例如阶段 1 结束时发现的错误节点，可能在事件边界上。类似地，在 Ω_2 的一些节点，例如在阶段 2 结束时发现的边界节点，可能并不真在事件边界。阶段 3 减少了这类错误推导。这个算法是基于假设：节点均匀分布，在边界节点一定距离 c 内，应该至少有一个其他的边界节点。算法概括如下：

1）对每个在 $\Omega_1 \cup \Omega_2$ 的节点 S_i；

2）如果至少有一个其他节点 S_j（即非 S_i）在 $\Omega_1 \cup \Omega_2$ 里，且比 c 到 S_i 要近，则 S_i 在 Ω_3 里。

这里，Ω_3 是事件边界节点的集合。注意在这个算法中，与 θ 和 θ_2 类似，c 是一个重要的参数，应该非常仔细地选择。

13.7 复习题

13.1 SNEP 提供哪一种安全服务？SNEP 与提供相同安全服务的传统方案有什么区别？

13.2 TESLA 和 μTESLA 有什么区别？

13.3 假设节点 A、B 和 C 在隔离区；节点 D、E 和 F 不在隔离区。下列哪种传输是需要认证的？

（a）$B \rightarrow A$

（b）$D \rightarrow B$

（c）$D \rightarrow A$，然后 $A \rightarrow E$

（d）$C \rightarrow F$

（e）$E \rightarrow F$

13.4 什么时候可以对一个混合蜂窝网络和自组织网络中的数据包源的节点收费？为什么？

13.5 怎样防止自组织节点通过声称它们代表其他节点发送数据包来欺骗系统，尽管它们并没有这么做。

13.6 列举出两种检测恶意信标节点的方法。

13.7 在节点定位和时钟同步中，怎样使用往返时间来检测重放攻击？

13.8 节点 S_i 的差值 d_i 分别为 {5，7，9，2，3，6，4，11，5，6}，如果门限值是 1.5，则有哪些节点是错误的？

第 14 章　信息战和电子战

我们希望用一个免责声明开始本章内容，“本章表达的定义、见解和观点不一定反映任何国家或国际组织的官方观点。”我们从开放的、不涉密的因特网材料，编辑非常简短的章节内容。目标是对相关术语给出简要的概览。我们并不试图提供解释所有挑战和解决方案的详尽的综述。

自组织网络和传感器网络应用已经部署到许多军事系统中，如盟军追踪、无人值守传感器网络（Unattended Sensor Networks）、局部地区通信、海上和陆地侦查。军事通信也是一种自组织网络应用。网络中心战等概念使得自组织组网能力对军事领域越来越重要。因此，一个趋势是增加这些技术在防御系统中的使用，这些系统往往是信息战的攻击目标。此外，由于基于效果（影响）的军事行动方法和其他最新概念，连接国家基础设施重要节点和用于关键基础设施中的民用系统，是战争中敌方的首要目标。另外，由于非对称战争和低强度冲突，在危机时期与和平时期，对信息系统的威胁都存在（Hammes，2007）。因此，民用系统也易遭受威胁，并且这种威胁是持续的。

当今时代，因特网和其他网络互连手段将重要的国家资产以及全球资源连接起来。公众可以 24h 访问资料丰富的和/或欺骗性的消息渠道。所有这些增加了全球和国家的脆弱性。当前，通过使用信息战，国家权力的经济和外交支撑比因特网时代之前更容易被拖入混乱的、不确定的疲软状态。泛在计算、有感知的和普适计算及其广泛使用，进一步加大了这种风险。银行系统、股票交易系统、智能办公室和家庭、病人和老年人照顾系统、监视系统、居住地监控系统、自动化应急基础设施、自动化交通网络和基础设施以及许多其他使用这些技术的系统，当它们没有被保护时，会成为非对称威胁（例如恐怖行动）的目标，这不仅导致财产损失，还会带来人员伤亡。通过使用自动化系统、有感知的和泛在计算工具，可能会给人群设置圈套、引起火车或飞机相撞、着火或使房间充满化学物。因此，作者相信，如果没有采取慎重的、协调和集成的手段并演练，甚至不使用常规破坏性手段，信息战也可以是致命的、破坏性的。注意到这一关于致命性（毁灭性）的观点，不同于当前一般的关于信息战和电子战的理解。所有这些也会对公众士气产生影响，这反过来也会削弱军事力量和信息战、电子战的有效使用。

底线是即使在和平时代，信息战是持续的，需要引起民众和军方的注意。信息战可以实施为进攻性的或防御性的，目标是：

1）有效阻止敌方使用他们的信息系统、指挥和控制（C2）基础设施；

2）获取情报；

3）使用敌方拥有的信息和自动化系统，组织非致命的或破坏性攻击；

4）保护己方利益、信息和信息系统、基于信息的行动、C2 基础设施，抵御敌方的进攻性信息战。

在军事术语中，这需要使用下列能力：

1）电子战（Electronic Warfare，EW）：对电磁频谱友好使用的控制和保护，并拒绝敌方使用。

2）军事行动安全（Operational Security）：确保盟军行动安全，使敌人不能获悉盟军能力或未来计划。

3）心理战（Psychological Operations）：一些规划和引导的活动，以影响盟军、中立方或敌方受众的态度和行为，使其支持盟军行动。

4）军事迷惑（Military Deception）：用于误导敌方采取有利于盟军利益的一系列行动，可通过操纵、歪曲和/或伪造证据和情报来实施。

5）物理毁灭（Physical Destruction）：通过海陆空军事行动，毁灭敌方的情报和 C2 系统。

6）特别行动（Special Operations）：在信息战中，由特别行动单位规划和指导的行动，目的是破坏或瓦解敌方的情报和 C2 系统，以及进入敌方的信息系统。特别情报行动可能需要通过特别行动单位远距离渗入敌方领域，以实施电子战、军事行动安全、心理战、军事迷惑和物理毁灭任务。

这些能力应该以良好的协调、集成的方式进行规划和应用，以及需要所有指挥、控制、通信、计算机、情报、监测和侦察（C4ISR）系统手段的相互支持。所有这些能力都属于信息战的范畴。但本章仅讨论电子战，因为这一内容与无线自组织网络、传感器网络和 Mesh 网络中的安全更相关。再次提醒我们的意图不是对这一话题进行广泛、详尽的讨论。我们仅给出电子战相关的定义。对这一领域感兴趣的读者可以参考 Joint Chiefs of Staff（2007）文献。

电子战是一种非致命但是很重要的能力，它可能会影响各种冲突中行动的结果。全部电磁频谱属于电子战的范围，包括下列主要三类活动：

1）电子支持（Electronic Support，ES）：电子支持手段（Electronic Support Measure，ESM）主要由搜索、截获、识别和定位电磁发射源的被动技术组成，一般提供时间敏感（时效性强）的情报。

2）电子攻击（Electronic Attack，EA）：电子攻击包括预防敌方有效使用电磁频谱和 C2 系统的电子对策（Electronic Counter Measure，ECM）。

3）电子保护（Electronic Protection，EP）：电子保护包括抵御电子支持手段和电子对策手段。

14.1　电子支持

电子支持包括信号情报（Signal Intelligence，SIGINT）活动，可分成两类：电信侦查（Communications Intelligence，COMINT）和电子情报（Electronic Intelligence，ELINT）。电信侦查是检测和截获敌方的通信，可以是监控通信节点的流量分析的形式，或者是用以捕获报文内容的窃听的形式。实施电子情报，用于检测和定位非通信用途的电磁放射源，例如雷达发射（Radar Emission）。

电信侦查一般通过两阶段实施。第一阶段是信号采集，而第二阶段（流量选择）是记录通信。当需要对采集的海量信号进行处理时，选择一个有情报价值的数据包或通话录音可能是非常困难的任务。信号采集通过窃听实现，可认为比流量选择要容易。因此，标记包含机密情报的数据包可能不是一个好主意。记得么？IPv4 可选安全头信息用于标记包含机密数据的数据包，这可能是有益的，但对敌手更有益！

RF 指纹识别（RF Fingerprinting）是一种重要的电子支持技术。从两个基站发出的信号，用相同带宽和协议簇以相同的中心频率通信，因为无意的调频、谐波等原因，通常有一些差别。这些差别可通过仔细的信号分析检测到，无线电通信可与其他通信区别开。这使得更难达到匿名性。当共同使用节点定位方案和 RF 指纹识别时，节点运动可以被监控，这可能会泄漏重要的军事情报。

我们在第 7 章中从节点拥有者的角度研究节点定位。然而，用于定位一方自己节点的三角测量或多边测量（Triangulation or Multilateration）技术，也有助于敌手定位这些节点。因此，为军事系统开发的节点定位方案，也应认为是敌方的信号情报（SIGINT）活动。

最后，预警（Threat Warning）也是一种重要的电子支持手段。电磁发射可以指示和定位敌方攻击目标、情报、追踪和指挥系统。检测这种威胁，并随后向盟军和集结编队发出警报，有助于及时部署电子对抗手段。例如，可以给飞行员发出关于一个导弹正在追踪他/她的飞行器的警报。

14.2　电子攻击

电子攻击包括进攻性和防御性电子对策（ECM）。如下所列的进攻性电子对策，通过打击敌人对电磁波频谱的有效使用，支持作战行动：

1）拥塞（Jamming）：拥塞和其他拒绝服务攻击已在第 8 章中论述。在电子战术语中，它们也称为软杀伤技术（Soft Kill Techniques）。拥塞可用于攻击目的，例如干扰敌方通信，以便支持盟军攻击。

2）物理毁灭（Physical Destruction）：拥塞技术暂时中断敌方在一定带宽的传输或发射。另一方面，链路或节点可以被物理毁坏，这称为硬杀伤（Hard Kill）。

3）反辐射导弹（Anti-radiation Missiles）：可使用制导系统引导军事武器朝向（光、热等）发射源。它们一般用于压制敌方雷达制导武器系统，如高射炮。

4）电子迷惑（Electronic Deception）：迷惑与伪装、重放和欺骗攻击同义。制造假的辐射为敌方传达误导信息。用于欺骗和迷惑敌人的有意的假的信息传输称为电磁干扰（Electro Magnetic Intrusion）。电子迷惑的另一种方法是电子探测（Electronic Probing），即信号发送给敌方设备，用以探知其功能或能力。

5）定向能量（Directed Energy，DE），高能量 RF（High Energy RF，HERF）：这些是通过发射强大电流破坏未保护的电子线路的系统。电磁脉冲设备通过使用电磁辐射构成有意破坏。

防御性电子对策用于保护盟军，包括：

1）干扰（Jamming）：干扰也可用于防御目的。例如，敌方雷达可以被干扰，保护盟军免受雷达制导导弹的攻击。

2）消耗品（金属碎箔、照明弹和诱饵）：军事消耗品也是防御性干扰技术。金属碎箔（Chaff）用于干扰雷达信号，由许多细小的传导金属薄片组成，大小是目标信号波长的一半。它们被散布在雷达和目标之间，导致错误的雷达信号反馈。类似地，诱饵（Decoy）被放在雷达和目标之间，形成防护罩。照明弹（Flare）可以干扰追踪热源的指挥系统。

3）反无线电操控的简易爆炸设备（Radio-Controlled Improvised Explosive Devices，RCIED）：简易爆炸设备常被远程控制。干扰这些远程控制并且避免意外触发它们，是一种重要的电子防范措施。

14.3 电子保护

电子保护包含所有抵御敌方电子支持手段的措施，例如小心使用电磁频谱、认证和密码学，以及所有抵御敌方电子对策的电子对抗措施，如硬化设备以抵抗定向和高能量攻击及敌方干扰器的破坏。本书讨论的所有流量分析、匿名性和认证技术都是抵抗敌方电子支持手段的保护措施。电子攻击包括：

1）发射控制（Emission Control，EMCON）：电磁频谱的控制使用。发射被敌方传感器检测到的概率通过发射控制达到最小化。发射也应遵守迷惑计划。

2）频谱管理（Spectrum Management）：对电磁频谱的有效利用也是重要的。再次注意频谱是一种宝贵的资源，盟军的电磁发射也会给自己的电子设备带来干扰。另外在战场上，频谱也易遭受敌方的电子对抗措施的破坏。因此，其使用需要仔细地规划和管理。对敌方电子对抗措施，频谱管理步骤也应是可感知的和自适应的。

3）电子伪装（Electronic Masking）：通过干扰敌方电子支持手段，隐蔽盟军的电磁发射。盟军频率的受控辐射可以从敌方电子支持手段（并不干扰敌方）中，掩盖己方发射。例如，有向天线可用于这种用途。

4）电子安全（Electronics Security）：包括否认电子情报的技术。

5）电磁硬化（Electromagnetic Hardening）：抵抗电子对策的防范措施。通过过滤、接地、焊接和屏蔽，个人和设备可以在敌方电子攻击中受到保护。本书第 8 章可看做关于电子攻击的章节，随后各章是关于电子保护的。当然，本书范围比电子战更宽泛，也包括信息战。

14.4　复习题

14.1 将下列概念与本章讨论的对应电子战术语建立联系：

（a）容错（Tamper Resilience）

（b）女巫攻击（Sybil Attack）

（c）完整性、机密性和隐私保护

（d）伪装、欺骗、网络钓鱼（Phishing）

（e）TESLA

（f）安全节点定位和时钟同步

（g）安全事件边界检测

第 15 章　标　　准

15.1　X.800 和 RFC 2828

ITU-T 建议规范 X.800（OSI 安全架构）和 IETF RFC 2828（因特网安全术语表）可作为系统地评估和定义安全需求的参考资料。虽然来自于不同的标准化组织，但是这两种标准具有很多相同点。X.800 用于定义保护开放系统间通信时所需的一般的安全架构基础。为了改进现存的规范和/或在 OSI 框架下提出新的规范，X.800 规范设立了指导方针和约束条件。类似地，RFC 2828 规范为信息系统安全术语规定了简称、解释以及规范。

X.800 以及 RFC 2828 都是被设计用来帮助安全管理者定义安全需求，以及满足这些安全需求的可行方法。它们也帮助软硬件生产厂商开发遵循相应标准的产品和服务的安全特性。X.800 和 RF 2828 都提到了安全系统的多个方面，即安全威胁和安全攻击、安全服务、安全机制和安全管理。这一节给出这些标准的简介。我们强烈建议读者阅读原始的标准文件来获得更多的信息。

15.1.1　安全威胁和攻击

根据 X.800 规范，“对于系统安全的威胁包括以下这些：破坏信息和/或其他资源；腐化（Corruption）或者篡改信息；盗窃、转移或者丢失信息和/或其他资源；泄漏信息和中断服务”。另一种来自 RFC 2828 的定义，更明确地将安全威胁定义为“当有某种可能破坏安全并造成危害的特定情境、能力、行为或者事件时，存在的一种潜在的安全危害”。换句话说，安全威胁是一种利用脆弱性造成的可能发生的危险。

安全威胁既可以是意外发生的，也可以是蓄意策划的，既可以是主动的，也可以是被动的：

1）意外威胁和蓄意威胁：正如它们各自名字的含义，意外威胁不存在预谋，例如系统故障或者软件漏洞。另一方面，蓄意威胁是有特殊目的的事先已经计划好的行为。

2）被动威胁和主动威胁：被动攻击不会修改受害系统中的信息或操作；例如，搭线窃听。另一方面，主动威胁将会修改受害系统中的信息或操作；例如，改变系统的防火墙规则，使得允许非授权访问。

当威胁是一种可能引起安全破坏的潜在安全问题时，它还不是一种产生效果的行动。另一方面，攻击是一种利用安全破坏的行为。攻击同样也可以分为内部攻击或外部攻击，主动攻击或被动攻击：

1）内部攻击和外部攻击：内部攻击发生在系统的合法用户以非预期的方式表现。外部攻击由处于安全边界以外的非法系统用户发起。

2）主动攻击和被动攻击：主动攻击试图改变系统资源或者影响系统的操作。主动攻击的例子有伪装、重放、消息篡改和拒绝服务。被动攻击试图在不改变系统资源的前提下利用系统的信息。被动攻击的例子有消息内容泄漏和流量分析。

15.1.2　安全服务

根据 RFC 2828 标准，安全服务是由一个保护系统资源的系统提供的处理或者通信服务。安全机制实现安全服务，安全服务实现安全策略。安全服务可以划分为五类：

1）认证服务：这类安全服务用于验证实体所声称的身份或者为实体验证身份（参考 RFC 2828 第 16 页）。认证服务可以分为两类：数据起源认证和对等实体认证。

① 数据起源认证：这类安全服务用于验证声称是接收到数据的来源的系统实体的身份（参考 RFC 2828 第 53 页）。尽管有时认为这种认证可以使接收者验证数据在传输过程中有没有被篡改，但是这种认证服务不能防止数据单元被复制或者修改。

② 对等实体认证：这种服务提供对等实体之间在建立连接或者在两者之间传递信息时的确证。这种服务可以保证在没有权威机构的情况下，实体没有进行伪装或者重放先前的连接（参考 X. 800 规范第 8 页）。

2）访问控制：这种服务提供防止对资源的未授权使用，例如计算资源、存储资源、通信链路等资源。为了使用某种资源，用户必须首先进行认证，之后他们才能被授予使用特殊系统资源的权利。

3）数据机密性：这种服务可以防止数据从源向目标传输时遭到未经授权的泄漏。加密和解密经常被用于提供数据的机密性。数据机密性可以分为以下四类：

① 连接机密性：这种服务可以保证用户数据在连接时的保密性。

② 非连接保密性：这种服务可以保证无连接服务下的用户数据保密性，例如，它可以保护个人数据块。

③ 选择字段机密性：这种服务可以保证在连接中或者个人数据块中的用户数据的选择字段的保密性。

④ 数据流机密性：这种服务防止通过监控数据流而得到信息。它用来防止流量分析。

4）数据完整性：这种服务用于确保数据在发送之后被准确地接收，同时保证数据没有被篡改或重放。数据完整性可以分为五类（参考 X. 800 规范第 9 和 10 页）：

① 可恢复的连接完整性：这种服务为所有处于连接中的用户数据提供完整性保护，它可以检测出整个数据序列中对于数据的任何篡改、插入、删除和重放操作，并且在探查到攻击时试图恢复数据。

② 不可恢复的连接完整性：这种服务为所有处于连接中的用户数据提供完整性保护，它可以检测出整个数据序列中对于数据的任何篡改、插入、删除和重放操作，但是在检测到攻击时，不对数据进行恢复。

③ 选择字段连接完整性：这种服务用于提供在连接中传输用户数据的选择字段完整性保护，以确定选择字段的数据是否已经被篡改、插入、删除或者重放。

④ 无连接完整性：这种服务用于个人数据块的完整性保护，确定接收到的数据块是否已经被篡改。另外，提供有限形式的重放检测。

⑤ 选择字段无连接完整性：这种服务用于个人数据块中的选择字段的完整性保护，确定选择字段是否已经被篡改。

5）不可否认性：这种服务可以保证一个实体一旦参加过某一次通信，则之后不能否认自己的参与。这种服务可以通过以下的某一种或者同时使用两种方式实现：

① 带源证明的不可否认性：数据接收者会得到数据来源证明。这样可以防止发送者否认他们发送数据或者内容的企图。数字签名就是一个带源证明提供不可否认性的例子（参考 X. 800 规范第 10 页）。

② 带发送证明的不可否认性：提供给数据的发送者数据传送的证明。这样可以防止数据接收者收到数据后否认已经接收数据或其内容的企图（参考 X. 800 规范第 10 页）。

15. 1. 3 安全机制

安全机制是一个用于某系统来实现由系统提供或参与的安全服务的方法（或者是一种结合这类方法的设计）。安全机制的例子有认证交换、校验和、数字签名、加密和流量填充（参考 RFC 2828 第 153 页）。安全机制被划分为两类：特殊的安全机制，可以结合特殊协议层使用；普适的安全机制，不针对于任何特殊的协议层。以下的概念取自 X. 800 规范。

1. 特殊的安全机制

1）加密：加密可以通过将原有信息转换成为一种无法理解的形式来保证数据或者信息流的机密性。加密算法可以是可逆的，也可以是不可逆的。一般的可逆加密算法有两种，分别是对称加密（即秘密密钥）和非对称加密（即公共密钥）。

2）数字签名：这种机制是在传送的数据中附加一些特殊信息，使得数据接收者可以验证数据来源和数据完整性。数字签名和公钥密码学关系密切。

3）访问控制：这种机制通过使用认证的实体身份、实体信息或者实体能力来授予实体访问权。

4）数据完整性：数据完整性的两方面是：① 单个数据单元或字段的完整性；② 一连串数据单元或字段的完整性。一般来说，使用不同的机制来提供这两种完整性服务，尽管在没有第一种情况下提供第二种服务是不实际的。

5）认证交换：对等实体之间的认证是依靠信息交换来完成的。

6）流量填充机制：流量填充机制可以提供各种级别的防护来抵抗流量分析。流量填充通过向数据流的间隙中插入比特来实现。

7）路由控制：这种机制允许路由在传送信息时进行适当的选择。终端系统为了更安全的通信，可能会希望使网络服务提供者通过不同的路由来建立一个连接。

8）公证机制：这种机制需要第三方的参与来确保两个实体间数据交换时的某些性质。

2. 普遍的安全机制

1）可信的功能：能够被用于增加其他安全机制的作用范围或者建立效果。任何向安全机制提供接入的功能都应该是可信的。

2）安全标签：含有数据项的资源都应该有与之相关的安全标签，例如指出数据的敏感级别。通常需要在数据传输中加入适当的安全标签。

3）事件检测：安全相关事件检测包括对明显破坏安全事件的检测，也包括对“常规”事件的检测。

4）安全审计跟踪：提供了一种有价值的安全机制，因为通过允许随后的安全审计而潜在的允许对安全破坏行为进行检测和调查。安全审计是为了检测系统控制是否适当，为了确保遵循既定的策略和操作步骤，为了辅助进行危害评估，为了指出任何在控制、策略和操作中的明显改变，而对系统记录和活动进行的独立的审查和检测。

5）安全恢复：安全恢复处理来自安全机制的请求，例如事件处理和管理功能，由于应用一套规则而进行恢复操作。这些恢复操作分为三种：即时的、临时的和长期的。

15.1.4　安全服务和安全机制的关系

表 15-1 说明了安全服务和安全机制之间的关系。认证服务需要使用数字签名机制，用于帮助认证数据发送者（双向认证）。这里也要用到加密机制。另外，对等实体认证同样需要认证交换来认证连接时的双方实体。

表 15-1 安全服务和安全机制之间的关系（参考 X. 800 规范 第 15 页）

服务项目	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由选择	公证机制
数据来源认证	Y	Y	—	—	—	—	—	—
对等实体认证	Y	Y	—	—	Y	—	—	—
访问控制	—	—	Y	—	—	—	—	—
连接保密性	Y	—	—	—	—	—	Y	—
非连接保密性	Y	—	—	—	—	—	Y	—
选择字段保密性	Y	—	—	—	—	—	—	—
数据流保密性	Y	—	—	—	—	Y	Y	—
可恢复的连接完整性	Y	—	—	Y	—	—	—	—
不可恢复的连接完整性	Y	—	—	Y	—	—	—	—
选择字段连接完整性	Y	—	—	Y	—	—	—	—
无连接完整性	Y	Y	—	Y	—	—	—	—
选择字段无连接完整性	Y	Y	—	Y	—	—	—	—
来源证明的不可否认性	—	Y	—	Y	—	—	—	Y
发送证明的不可否认性	—	Y	—	Y	—	—	—	Y

注：Y 表示是适合于这种机制的，无论是对于其本身还是和其他机制相结合；—表示是不适合于这种机制的。

不可否认性服务需要进行数字签名用于证明参与者的身份。然而，这种服务不需要加密，因为交换的数据没有保密性要求（例如：常规邮件）。取而代之的，这种服务需要数据完整性机制来确保接收到的信息没有被改动过，也需要公证机制使另一端确信本端的真实性，解决任何可能发生的争端。对其他安全服务和机制的组合可以有类似的说明。

15.1.5 安全服务和安全机制的布置

表 15-2 和表 15-3 概括了安全服务和安全机制在 OSI 协议层的部署方式。

表 15-2 OSI 协议层中安全服务的位置（参考 X. 800 规范 第 27 页）

服务项目	所在层						
	1	2	3	4	5	6	7*
数据起源认证	—	—	Y	Y	—	—	Y
对等实体认证	—	—	Y	Y	—	—	Y
访问控制	—	—	Y	Y	—	—	Y
连接保密性	Y	Y	Y	Y	—	Y	Y
非连接保密性	—	Y	Y	Y	—	Y	Y

（续）

服务项目	所在层						
	1	2	3	4	5	6	7*
选择字段保密性	—	—	—	—	—	Y	Y
数据流保密性	Y	—	Y	—	—	—	Y
可恢复的连接完整性	—	—	—	Y	—	—	Y
不可恢复的连接完整性	—	—	Y	Y	—	—	Y
选择字段连接完整性	—	—	—	—	—	—	Y
无连接完整性	—	—	Y	Y	—	—	Y
选择字段无连接完整性	—	—	—	—	—	—	Y
来源证明的不可否认性	—	—	—	—	—	—	Y
发送证明的不可否认性	—	—	—	—	—	—	Y

注：Y 表示本层支持这项服务；—表示本层不支持这项服务；*应当指出，对于第七层，应用进程自身有可能提供安全服务。

表 15-3　OSI 协议层中安全机制的位置

机制项目	所在层						
	1	2	3	4	5	6	7
加密	Y	Y	Y	Y	—	Y	—
数字签名	—	—	Y	Y	—	Y	Y
访问控制	—	—	Y	Y	—	—	Y
数据完整性	—	—	Y	Y	—	Y	—
认证交换	—	—	Y	Y	—	—	Y
流量填充机制	—	—	Y	—	—	—	Y
路由选择控制	—	—	Y	—	—	—	—
公正机制	—	—	—	—	—	Y	Y

注：Y 表示这种机制在所示的层中支持；—表示这种机制在所示的层中不支持。

15.2　有线对等保密（WEP）

作为 IEEE 802.11 无线网络标准的一部分，有线对等保密（Wired Equivalent Privacy，WEP）协议用于保护 IEEE 802.11 无线网络（Wi-Fi）。由于 Wi-Fi 技术使用无线电通信，而这种方式容易被窃听，所以使用某种机制来确保 Wi-Fi 网络的私密性是必要的。设计之初，WEP 期望能提供与传统的有线网络同等的安全。它的主要目的是防止 Wi-Fi 通信被窃听。另外，WEP 用于防止未经授权的 Wi-Fi 网络接入。

15.2.1 WEP 工作机制

WEP 通过使用共享密钥加密来进行移动客户端和无线接入点之间的安全通信。为了接入 Wi-Fi 网络，移动客户端需要一个与在适当的接入点所配置的密钥相匹配的 WEP 密钥。在检查了这一 WEP 密钥的有效性之后，接入点授权移动客户端接入网络。图 15-1 举例说明了一个简单的基于 WEP 的无线局域网配置。

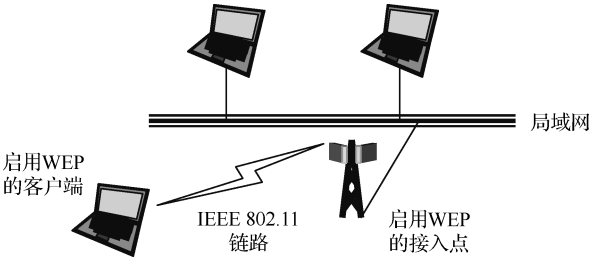


图 15-1 基于 WEP 的简单 WLAN 配置

由于 WEP 对于一个接入点的所有客户端使用相同的 WEP 密钥，WEP 的唯一目的就是防止外部攻击者进行信息窃听。它不能防止接入网络中所有其他客户端的攻击。出于保密的目的，WEP 加密解密使用 RC4 流密码。为了形成一个 64bit 的 RC4 密钥，WEP 使用一个 24bit 的初始矢量（IV）和一个 40bit 的密钥。这两部分连接起来形成一个 64bit 的 WEP 密钥。在扩展配置的 128bit WEP 密钥中，密钥长度为 104bit 加上 24bit 初始矢量。

图 15-2 描述了 WEP 的加密，其工作流程如下：在发送端，发送者使用初始矢量和 40bit WEP 密钥形成密钥流。密钥流与明文进行异或运算生成密文。由明文生成的循环冗余校验 CRC-32 用于接收端的消息完整性校验。

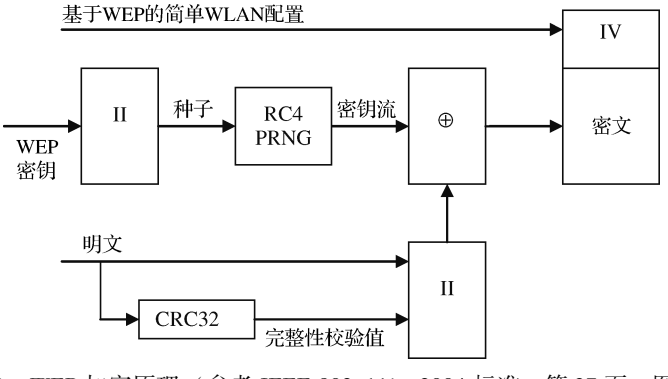


图 15-2 WEP 加密原理（参考 IEEE 802.11i—2004 标准，第 37 页，图 43a）

要解密密文流，接收者可以使用异或操作的基本原理，即：

密文 = 密钥流⊕明文

密钥流⊕密文 = 密钥流⊕（密钥流⊕明文）

= （密钥流⊕密钥流）⊕明文

= 明文

因此，在接收端，拥有相同 WEP 密钥的接收者可以使用接收消息中的初始矢量，恢复与发送端相同的密钥流。接收者就可以按照上述的规则，将接收到的密文和密钥流进行异或运算来恢复出明文。WEP 解密的原理如图 15-3 所示。

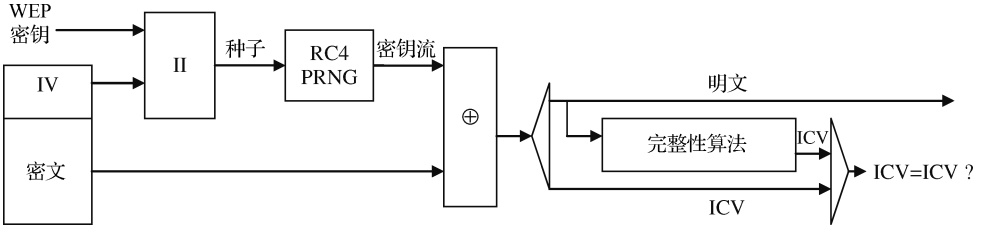


图 15-3　WEP 解密原理（参考 IEEE 802.11i—2004 标准，第 38 页，图 43b）

在发送端生成的 CRC-32 是用于进行完整性检查的值（Integrity Check Value，ICV），它用来检查接收到的信息是否在传送中被修改过。只有这个值和由完整性算法生成的值相匹配时，消息才能被认为是有效的。

15.2.2　WEP 缺陷

一些研究人员所做的工作和报告表明，WEP 存在安全缺陷。根据加州大学伯克利分校 ISAAC 组织（http：//www.isaac.cs.berkeley.edu/）发表的研究结果，WEP 使用流密码的操作容易受到很多种类型的攻击。

如果密文在发送到接收端的过程中受到攻击，并造成了一些比特位的改变，解密后的明文中相应的比特位也将会发生改变。同样，如果攻击者捕获了两条使用相同密钥流进行加密的密文，并将这两个密文进行异或运算，结果将会变为两个相应明文的异或结果。在获取并收集了这一信息后，攻击者就可以使用统计学的攻击来恢复出明文。加密时某一密码流使用得越频繁并被攻击者截获，攻击者就越容易通过统计学的方法进行攻击获取明文。当攻击者恢复出其中的一个明文时，也可以恢复出其他的明文。

WEP 的设计者已经认识到了这些缺陷，并且制定了相应对策来提高 WEP 的安全性。为了解决传输中数据包的完整性问题，他们在数据包的包头中加入了完整性检查字段。为了避免使用相同的密钥流进行加密，他们使用初始矢量部分来生成不同的加密密钥（见图 15-4）。然而，这些方法无法完全解决 WEP 的安全问题。

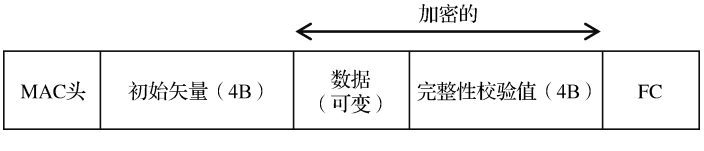


图 15-4　WEP 包格式

以上所提到的完整性校验字段是 32bit CRC 码的校验和，同时此字段也被加密。然而研究表明，由于 CRC-32 是线性的，有可能根据获取的消息之间的比特差分来计算两个 CRC 码之间的比特差分。这就意味着，如果攻击者改变了原始消息中的某一比特，他们也可以通过某种方式计算出 CRC 码中相应被改变的比特位，使得校验和的结果依然正确。通过使用这种技术，使得 WEP 创建者们保证消息完整性的努力变成了徒劳。

另一个提高 WEP 安全性的努力是使用 24bit 的初始矢量来生成不同的密钥流。然而，研究结果表明，只使用 24bit 来区分密钥流是不够的，因为这种方式只能生成大约 1600 万个密钥。在负载较重的网络中，传输 1600 万个数据包只需要很短的时间。这就意味着，用不了很长时间，网络中就会出现使用相同密钥流加密的两个数据包。这同样会导致前面提到过的统计学攻击。

以下列出的是由加州大学伯克利分校 ISAAC 组织报告指出的几种攻击（http：//www. isaac. cs. berkeley. edu/）。

15.2.2.1 被动攻击解密信息流

在这种攻击中，被动窃听者可以截获所有无线信息流，直到发生初始矢量冲突。通过将使用相同初始矢量的两个数据包进行异或运算，攻击者可以获得两个明文进行异或运算后的结果。异或运算的结果可以用来推测两条消息中的数据内容。

由于 IP 数据流通常是可预测的，同时包含很多冗余信息，攻击者可以消除消息内容中的很多可能性。对于其中一个或者两个数据包内容的进一步有根据的猜测，可以用于统计学的方法来缩小可能的消息空间。在某些情况下，就有可能得到准确的消息内容。

当仅基于两个消息的上述统计学分析不确定时，攻击者可以寻找更多使用相同初始矢量而产生的冲突。仅仅是所需时间的一小部分，就有可能恢复出一部分使用相同密钥流加密的消息，而统计分析的成功率会快速增长。一旦可能恢复出其中的一条消息的整个明文，其他所有使用相同初始矢量加密的消息明文就都能直接得到，这是因为所有成对的异或值已知。

这种攻击的一种扩展形式是利用因特网上的处于无线网络之外的某一主机，向无线网络内的某一主机发送数据流。这些数据流的内容对于攻击者来说是已知的，产生已知明文。当攻击者截取了他通过 IEEE 802. 11 发送的加密消息之后，他就可以对所有使用相同初始矢量的数据包进行解密。

15.2.2.2 主动攻击注入数据流

假设攻击者知道某个已经加密消息的确切明文。基于 RC4（x）$\oplus x \oplus y$ = RC4（y）这样一个性质，这里 x 和 y 是两个相互独立的比特流，攻击者可能使用这一知识加密其他数据包。这一过程包括构造一个新的消息，计算 CRC-32 码以及为了将明文转换为新消息而进行的对原始加密消息的逐比特转换。这个数据包就可

以被发送到接入点或者移动基站，并且将作为合法数据包而被接受。

对这种攻击的一个小小的改动将使得这种攻击更加危险。即使没有获得对数据包的完整知识，有可能对消息中所选择的比特进行翻转并且成功地调整加密的 CRC 码，得到对被修改过的数据包依然正确的加密形式。如果攻击者拥有数据包内容的部分信息，他就可以截取数据包，并对其进行选择性地修改。例如，有可能修改发送到远程登录会话或者与文件服务器交互的 shell 指令。

15.2.2.3　来自通信两端的主动攻击

前面提到的攻击可以进一步扩展用于破解任意的信息流。在这种情况下，攻击者对数据包头进行猜测，而不猜测数据包的内容。这一信息通常很容易获取或者猜测；特别地，所有必须猜测的对象是目的 IP 地址。知道了这一知识，攻击者可以适当地转换某几位比特值来改变目的 IP 地址，使数据包被送到攻击者所控制的机器，并通过流氓移动基站传送这个数据包。大多数的无线装置具有因特网连通性，数据包将会被接入点成功解密，并在非加密的状态下通过适当的网关和路由器转发到攻击者的机器中，攻击者将直接得到明文。如果可以猜测 TCP 数据包的包头内容，攻击者甚至可以将 TCP 数据包的目的端口改为 80 端口，这将使得数据包可以直接通过大多数防火墙。

15.2.2.4　基于表的攻击

初始矢量空间允许攻击者建立一个译码表。一旦攻击者得到了某些数据包的明文，他就可以计算通过初始矢量生成的 RC4 密钥流。这一密钥流就可以用于解密其他所有使用相同初始矢量的数据包。久而久之，也许通过使用以上的技术，攻击者就可以构造出一张初始矢量表以及与其相对应的密钥流表。这张表所需要的存储空间不大（15 GB）；一旦表建成，攻击者就可以解密所有经由无线链路传输的数据包。

15.2.2.5　监控

不管解码一个 2.4GHz 数字信号的难度，攻击者可以很轻易地从消费者支持 IEEE 802.11 的硬件产品中监听 IEEE 802.11 协议的传输。这些产品可以实现所有的必要监控功能，而给攻击者留下的问题是确信这些产品为他们工作。虽然支持 IEEE 802.11 标准的设备在设计时忽略了不知道密钥的加密内容，但是攻击者却能够通过改变硬件驱动的配置，成功地截获加密的 WEP 传输信息。他们就可以成功地迷惑计算机固件（Firmware），这样带有无法识别数据包的密文将被送回给他们进行进一步的检查和分析。

主动攻击（需要传输信息而不只是监控）看似更难实现，但是并非不可能实现。很多支持 IEEE 802.11 协议的产品使用可编程的固件，这些固件可以被逆向工程或修改来用于为攻击者提供注入信息流的能力。的确，这类逆向工程是值得花时间进行的工作，但是，需要强调的是，这种行为是一种一次性投入。一群有能力的

人可以投入努力，然后在秘密的圈子里分发这种流氓固件，或者将它卖给感兴趣的企业间谍。后者是一项高利润的买卖，因此时间上的投入很容易得到回报。

15.3 Wi-Fi 保护接入（WPA）

在等待 IEEE 802.11i 标准进展和批准之际，Wi-Fi 联盟提出 Wi-Fi 保护接入（Wi-Fi Protected Access，WPA）用于代替 WEP 增强 Wi-Fi 网络安全性。WPA 现在已经是 IEEE 802.11i 标准的一部分。WPA 可以在两种模式下工作：使用 IEEE 802.1X 进行认证的 WPA 企业模式，以及使用预共享密钥进行认证的 WPA 个人模式。WPA 使用一种叫做临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）算法来进行加密，同时使用另外一种叫做 Michael 算法来保证消息完整性。

类似于 WEP，WPA 中的数据加密使用 RC4 流密码，使用 128bit 的密钥和 48bit 的初始矢量。然而，WPA 使用 TKIP 对密钥进行动态改变。改变密钥的能力以及初始矢量更大的空间，使得在 WPA 中进行密钥恢复攻击在理论上是不可能的。对于消息完整性，WPA 使用可以防止重放攻击的消息完整性码（MIC）代替 WEP 使用的 CRC 码。

通过增加加密密钥规模和初始矢量空间，WPA 减少了使用相关密钥发送的数据包的数量。另外，通过建立一个更好的消息完整性检查机制，WPA 使得攻破 Wi-Fi 网络更加困难。

15.3.1 WPA 工作机制

WPA 可以在两种模式下工作：WPA 企业模式和 WPA 个人模式。在 WPA 企业模式中，存在多个移动客户端、一个接入点和一个认证服务器（RADIUS 或者 LDAP）。在这一模式下，当某个移动客户端希望接入网络时，他会联络相应的接入点进行认证。客户端将认证信息发送至接入点。这一信息随后被转发给认证服务器进行验证。在检查有效的证件后，认证服务器将指示接入点允许客户端接入网络。服务器同时会向接入点和客户端发送一个加密密钥。客户端可以使用这一密钥对其和接入点所交换的信息进行加密。图 15-5 给出了 WPA 企业模式的配置。WPA 企业模式一般使用于拥有大量客户

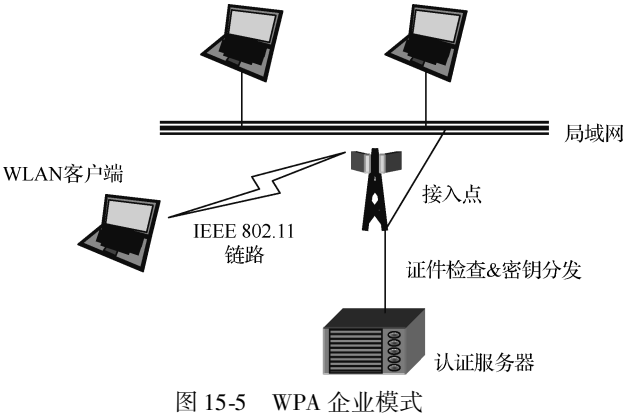


图 15-5 WPA 企业模式

端和可用信息技术基础设施的公司和组织。

与此同时，WPA 个人模式用于家庭用户或者小型办公环境，在这些地方部署认证服务器是不可行的。因此，WPA 个人模式有时被称为 WPA 小型办公/家庭办公（Small Office，Home Office，SOHO）。它也被称为预共享密钥（Preshared Key，PSK）模式。在这种预共享密钥模式下，通行口令在接入点手动输入，同时口令被发放给移动客户端。当客户端希望接入网络时，接入点首先检查用户的口令和自身的口令是否匹配。如果匹配，则接入点将允许客户端接入网络。之后接入点将加密密钥发送给移动客户端并开始信息交换。WPA 个人模式如图 15-6 所示。

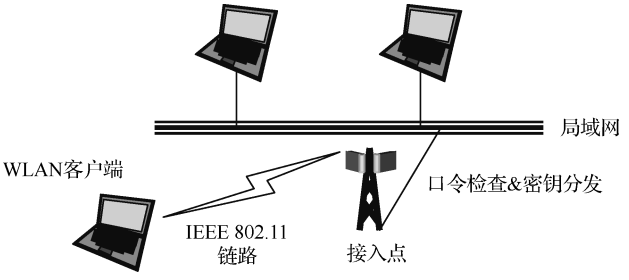


图 15-6　WPA 个人模式

WPA 可以概括为：WPA = IEEE 802.1x + EAP + TKIP + MIC（对于 WPA 个人模式，EAP 被 PSK 所代替）。WPA 数据包中的各字段如图 15-7 所示。WPA 的安全性基于安全认证、强加密和数据完整性。在接下来的章节中我们将依次介绍它们。

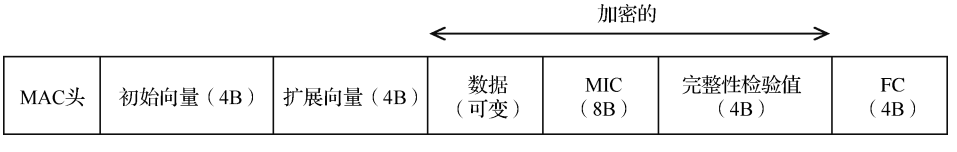


图 15-7　WPA 包格式

15.3.1.1　认证

WPA 认证与 IEEE 802.1x 规范相一致，它为集中型用户和/或无线网络认证提供了可扩展的认证协议（Extensible Authentication Protocol，EAP），同时也提供了加密密钥管理和分发功能。WPA 支持两种基于不同目的的认证模式，见表 15-4。

表 15-4　WPA 认证支持

认证模式	协　　议	是否需要认证服务器
WPA 企业模式	IEEE 802.1x + EAP	是
WPA SOHO	IEEE 802.1x PSK	否

在企业模式下，WPA 使用 IEEE 802.1x 和 EAP，同时需要使用认证服务器。WPA 使用 EAP 为移动客户端和无线网络传输认证信息。EAP 是一种可扩展的认证协议，同时支持不同的认证方式，例如通行口令、数字证书和智能卡。移动客户端

可以使用任何一种在认证服务器中所安装的并被支持的认证方法。如果所有的认证方法失败，接入点就会拒绝移动客户端的证件。

使用 WPA 的接入点支持广播信标消息。当一个移动终端接近这类接入点时，它将自身的子系统标识符 SSID 和接入点关联。如果关联成功，移动终端开始认证过程。

在认证之后，两组密钥即对偶密钥（Pairwise Keys）和群密钥（Groupwise Keys），被传送到移动客户端。这些密钥用于在无线传输之前对 IEEE 802.11 数据包进行加密。群密钥用于使所有的移动客户端和同一个接入点建立连接。对偶密钥是某个移动客户端和接入点之间唯一的密钥。这种 IEEE 802.1x 密钥分发机制解决了认证和数据加密中所有移动客户端共享相同的 WEP 密钥的 WEP 认证问题。

在个人模式中，由于不存在认证服务器，所以使用了一种简单的通行口令匹配方案。这种认证方式被称为预共享密钥模式（WPA-PSK）。在这种模式中，一个简单的预共享密钥（或者通行口令）是在每个移动客户端和接入点处手工输入的。移动客户端可以在它的通行口令和接入点中所持有的口令相匹配的情况下被允许接入网络。

不考虑所使用的 WPA 认证方法，在认证成功之后，使用 TKIP 加密传输的消息。这种加密方法使得 WPA-PSK 不同于 WEP。这也是 WPA 个人模式比 WEP 更安全的原因。

15.3.1.2 加密

WEP 加密的问题主要是源于无线传输的初始矢量未经加密。在一个重负载 Wi-Fi 网络中，初始矢量每几个小时就会重新出现一次。通过捕获具有相同初始矢量值的数据包，攻击者就可以通过重复地对密文进行异或运算来找出 WEP 密钥，然后就可以非法接入网络。

使用了 TKIP 的 WPA，通过以下手段解决了 WEP 中的这一问题：

1）使用了更长位数的初始矢量（48bit）；

2）将密钥的长度从 40bit 增加至 128bit；

3）每 10000 个数据包就重新生成一个加密密钥；

4）使用每个数据包的密钥和初始矢量进行混合。

加密密钥是通过添加一个 48bit 的初始矢量、一个 104bit 的 RC4 密钥以及客户端的物理地址生成的，之后将结果输入一个混合函数来生成一个 128bit 的 RC4 加密密钥值。

15.3.1.3 消息完整性

WPA 中的消息完整性检测（MIC），正如它的名字，提供了保证完整性的功能。正如前面提到过的，WEP 的 CRC-32 码不能保证消息的完整性，所以 MIC 单

向哈希函数被用于替代 WEP 中的 CRC-32 校验和。在 MIC 方案中，接收者和传输者分别计算并比较 MIC 值。如果它们不匹配，就会认为数据在传输过程中已经被改变，数据包被丢弃。

MIC 使用了一种叫做 Michael 的算法，它通过源和目的地消息认证码（MAC）地址和数据域来计算得到一个 64bit 的值。通过源和目的地计算得到 MIC 值，数据包就将发送者及接收者联系起来，这样就可以阻止基于伪造数据包的攻击。

15.3.2　WEP 和 WPA 比较

表 15-5 给出了 WEP 和 WPA 之间的简单比较。

表 15-5　WEP 和 WPA 的比较（经 Wi-Fi 联盟批准的翻印，2003）

	WEP	WPA
加密	有缺陷，曾经被科学家和黑客攻破 40bit 密钥 静态密钥：所有网络上的用户使用同一密钥 密钥的手工分配：为每个设备手动输入	弥补了 WEP 的所有缺陷 128bit 密钥 动态会话密钥：每个用户每次会话每个数据包一个密钥，自动分配密钥
认证	有缺陷，使用 WEP 密钥自身用于认证	强用户认证，利用了 IEEE 802.1x 和 EAP

总之，如果某个组织需要一个更加安全的无线网络，我们强烈建议使用 WPA 来替代 WEP。

15.3.3　WPA2

在 2004 年，IEEE 批准了完整的 IEEE 802.11i 规范，紧接着 Wi-Fi 联盟推出一个称为 WPA2 的新的互操作测试认证。WPA2 基于鲁棒安全网络（Robust Security Network，RSN）机制，同时支持 WPA 中可用的所有机制。

实际上，WPA 和 WPA2 之间有许多共同点。它们都使用 EAP 和 IEEE 802.1x 机制用于认证。它们都可以工作于企业和个人模式。它们之间唯一的不同点是加密机制。WPA 使用基于 RC4 流密码的 TKIP 方式；WPA2 则使用计数器模式密码块链消息认证码协议（CCMP）加密机制的高级加密标准（AES）。AES 比 RC4 的安全强度高，它可能被一些团体用户或者政府机构所采用。

在 2006 年 3 月，对于所有经 Wi-Fi 联盟认证的设备，WPA2 认证变成了强制性的，这样以确保所有当前的硬件同时支持 WPA 和 WPA2。

参 考 文 献

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) 'Wireless Sensor Networks**:** A Survey', *Computer Networks*, **38**, 393–422.

[2] Akyildiz, I. F., Wang, X. and Wang, W. (2005) 'Wireless mesh networks: a survey,' *Computer Networks*, **47**, 445–487.

[3] Anderson, R. and Kuhn, M. (1997) 'Low Cost Attacks on Tamper Resistant Devices', proceedings of the 1997 Security Protocols Workshop, Paris, Springer *LNCS*, **1361**, 125–136.

[4] Anderson, R., Chan, H. and Perrig, A. (2004) 'Key infection: Smart trust for smart dust,' Proceedings of the 12th IEEE International Conference on Network Protocols, ICNP'04, pp. 206–215.

[5] ANSI/IEEE (1999) Standard 802.11/ Standard 802.11a/ Standard 802.11b/ Standard 802.11i.

[6] Arisha, K., Youssef, M. and Younis, M. (2002) 'Energy-Aware TDMA-Based MAC for Sensor Networks,' in *Proceedings of the IEEE Workshop on Integrated Management of Power Aware Communications, Computing and Networking (IMPACCT 2002)*, New York City, New York, May 2002.

[7] Asokan, N. and Ginzboorg, P. (2000) 'Key agreement in ad-hoc networks,' *Computer Communications*, **23** (17), 1627–1637.

[8] Atallah, M., Bryant, E. and Stytz, M. (2004) 'A Survey of Anti-Tamper Technologies', *CrossTalk: The Journal of Defense Software Engineering*, November.

[9] Aune, F. (2004) 'Cross Layer Design Tutorial', Norwegian University of Science and Technology, Trondheim, November.

[10] Balenson, D., McGrew, D. and Sherman, A. (2000) 'Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization,' IETF Internet-Draft, August 25 2000, draft-irtf-smug-groupkeymgmt-oft-00.txt.

[11] Balfanz, D., Smetters, D., Stewart, P. and Wong, H. (2002) 'Talking to strangers: Authentication in ad hoc wireless networks,' in Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, USA.

[12] Barakat, C., Altman, E. and Dabbous, W. (2000) 'On TCP performance in a heterogeneous network: a survey,' *IEEE Communications Magazine*, **38**(1), 40–46.

[13] Basagni, S., Herrin, K., Bruschi, D. and Rosti, E. (2001) 'Secure pebblenets,' MobiHoc 2001, pp. 156–163.

[14] Becker, K. and Wille, U. (1998) 'Communication complexity of group key distribution,' *proceedings of the 5th ACM conference on Computer and Communication Security*, pp. 1–6.

[15] Bluetooth SIG (2004) 'Bluetooth Core Specification Version 2.0 + Enhanced Data Rate,' Bluetooth SIG.

[16] Boneh, D. and Boyen, X. (2004) 'Secure Identity Based Encryption Without Random Oracles,' proceedings of Crypto 2004, *LNCS*.

[17] Boneh, D. and Franklin, M. (2001) 'Identity-based encryption from the weil pairing,' *proceedings of Crypto 2001*, pp. 213–229.

[18] Boneh, D., Boyen, X. and Goh, E. J. (2005) 'Hierarchical Identity Based Encryption with Constant Size Ciphertext,' proceedings of EUROCRYPT'05, *LNCS*, **3494**, 440–456.

[19] Boyen, X. (2003) 'Multipurpose Identity-Based Signcryption – A Swiss Army Knife for Identity-Based Cryptography,' proceedings of Crypto 2003, *LNCS*, **2729**, 383–399.

[20] Buchegger, S. and Le Boudec, J. (2002) 'Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad Hoc Networks,' MobiHoc 2002.

[21] Bulusu, N., Heideman, J. and Estrin, D. (2000) 'GPS-less low cost outdoor localization for very small devices,' *IEEE Personal Communication*, **7**, 28–34.

[22] Burmester, M. and Desmedt, Y. (1994) 'A secure and efficient conference key distribution system,' *proceedings of EUROCRYPT' 94*, pp. 275–286.

[23] Cagalj, M., Capkun, S. and Hubaux, J. P. (2006) 'Key Agreement in Peer-to-Peer Wireless Networks,' *Proceedings of the IEEE*, **94**(.2), 467–478.

[24] Camtepe, S. A. and Yener, B. (2005) '*Key Distribution Mechanisms for Wireless Sensor Networks: a Survey*,' Technical report TR-05-07, Rensselaer Polytechnic Institute, NY, USA.

[25] Canetti, R., Garay, J., Itkis, G., Micciancio, D. and Naor, M. (1999) 'Multicast Security: A Taxonomy and Efficient Constructions,' *proceedings of INFOCOMM'99*.

[26] Capkun, S., Buttyán, L. and Hubaux, J. P. (2003a) 'Self-Organized Public-Key Management for Mobile Ad Hoc Networks,' *IEEE Transactions on Mobile Computing*, **2**(1), 1–13.

[27] Capkun, S. and Hubaux, J. (2003) 'BISS: Building secure routing out of an incomplete set of security associations,'

WiSE.
[28] Capkun, S., Hubaux, J. P. and Buttyán, L. (2003b) 'Mobility Helps Security in Ad Hoc Networks,' *proceedings of MobiHoc'03*.
[29] Capkun, S., Hubaux, J. P. and Buttyán, L. (2006) 'Mobility Helps Peer-to-Peer Security,' *IEEE Transactions on Mobile Computing*, **5**(1), 43–51.
[30] Cardei, M. and Wu, J. (2005) 'Coverage in Wireless Sensor Networks,'in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press.
[31] Carter, S. and Yasinsac, A. (2002) 'Secure position aided ad hoc routing protocol,' IASTED International Conference on Communications and Computer Networks (CCN02).
[32] Cayirci, E. (2003) 'Data Aggregation and Dilution by Using Modulus Addressing in Wireless Sensor Networks', *IEEE Communications Letters*, August.
[33] Cayirci, E. and Akyildiz, I.F. (2002) 'User Mobility Pattern Scheme for Location Update and Paging in Wireless Systems', *IEEE Transactions on Mobile Computing*, **1**, 236–247.
[34] Cayirci, E. and Akyildiz, I.F. (2003) 'Optimal Location Area Design to Minimize Registration Signaling Traffic in Wireless Systems', *IEEE Transactions on Mobile Computing*, **2**, 76–85.
[35] Cayirci, E. and Coplu, T. (in press) 'SENDROM: Sensor Networks for Disaster Relief Operations Management,' *ACM/Kluwer Wireless Networks*.
[36] Cayirci, E. and Ersoy, C. (2002) 'Application of 3G PCS Technologies to the Rapidly Deployable Networks', *IEEE Network Magazine*, September/October, pp. 20–27.
[37] Cayirci, E. and Nar, P. (2005) 'Power Controlled Sensor MAC Protocol,' EWSN'2005.
[38] Cayirci, E., Coplu, T. and Emiroglu, O. (2005) 'Power Aware Many To Many Data Centric Routing In Wireless Sensor and Actuator Networks,' EWSN'2005.
[39] Cayirci, E., Cimen, C. and Coskun, V. (2006a) 'Querying Sensor Networks by Using Dynamic Task Sets,' *Computer Networks*, **50**(7), 938–952.
[40] Cayirci, E., Tezcan, H. and Coskun, V. (2006b) 'Wireless Sensor Networks for Underwater Surveillance Systems,' *AdHoc and Sensor Networks*, **4**(4), 431–446.
[41] Certicom Corp. (2004) 'MQV: Efficient and Authenticated Key Agreement,' *Code & Cipher*, Certicom's bulletin of security and cryptography, Crypto Column, **1**(2).
[42] Cha, J. C. and Cheon, J. H. (2002) 'An Identity-Based Signature from Gap Diffie–Hellman Groups,' *Cryptology* eprint Archive, Report 2002/18.
[43] Chan, H. and Perrig, A. (2003) 'Security and Privacy in Sensor Networks' in *IEEE Computer Magazine*, October.
[44] Chan, H., Perrig, A. and Song, D. (2003) 'Random key predistribution schemes for sensor networks,' proceedings of the IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 197–213.
[45] Chang, H. and Atallah, M. (2001) 'Protecting Software Code By Guards,' proceedings of ACM Workshop on Security and Privacy in Digital Rights Management, Philadelphia, PA, pp.160–175.
[46] Chen, L. and Kudla, C. (2003) '*Identity Based Authenticated Key Agreement Protocols from Pairings*,' HP Technical Report HPL-2003-25.
[47] Collberg, C. and Thomborson, C. (2002) 'Watermarking, Tamper-Proofing, and Obfuscation Tools for Software Protection,' *IEEE Transactions on Software Engineering,* **28**(8), 735–746.
[48] Collberg, C., Thomborson, C. and Low, D. (1997) '*A Taxonomy of Obfuscating Transformations*,' Department of Computer Science, University of Auckland, New Zealand.
[49] Coskun, V., Cayirci, E., Levi, A. and Sancak, S. (2006) 'Quarantine Region Scheme to Prevent Spam Attacks in Wireless Sensor Networks,' *IEEE Transactions on Mobile Computing*, **5**(8), 1074–1086.
[50] Dam, T. and Langendoen, K. (2003) 'An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks,' ACM SenSys, November.
[51] Deng, J., Han, R. and Mishra, S. (2003) 'INSENS: intrusion tolerant routing in wireless sensor networks,' 23rd IEEE International Conference on Distributed Computing Systems (ICDCS).
[52] Deng, J., Han, R. and Mishra, S. (2004) '*Countermeasures against traffic analysis in wireless sensor networks*,' Technical Report CU-CS-987-04, University of Colorado at Boulder.
[53] Deng, J., Han, R. and Mishra, S. (2005) 'Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks', in first IEEE/CerateNet Conference on Security and Privacy in Communication Networks (SecureComm 2005), Athens, Greece, September 2005, pp. 113–124.
[54] Desmedt, Y. G. (1994) 'Threshold Cryptography,' *European Transactions on Telecommunications*, **5**(4), 449–457.
[55] Diffie, W. and Hellman, M. E. (1976) 'New Directions in Cryptography,' *IEEE Transactions on Information Theory*, **IT-22**(6), 644–654.
[56] Ding, M., Chen, D., Xing, K. and Cheng, X. (2005) 'Localized Fault Tolerant Event Boundary Detection in Sensor

Networks', INFOCOM 2005.
[57] Di Pietro, R., Mancini, L. V., Law, Y. W., Etalle, S. and Havinga, P. (2003) 'LKHW: A directed diffusion based secure multicasting scheme for wireless sensor networks,' First International Workshop on Wireless Security and Privacy (WiSPr'03).
[58] Djenouri, D., Khelladi, L. and Badache, N. (2005) 'A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks,' *IEEE Communications Surveys & Tutorials*, **7**(4), fourth quarter 2005.
[59] Doherty, L., Pister, K. S. J. and Ghaoui, L. E. (2001) 'Convex position estimation in wireless sensor networks,' Infocom'01, Anchorage.
[60] Douceur, J. R. (2002) 'The Sybil Attack,' 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), pp. 251–260.
[61] Du, W., Deng, J., Han, Y. S. and Varshney, P. (2003) 'A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks,' proceedings of CCS'03.
[62] Du, W., Deng, J., Han, Y. S., Chen, S. and Varshney, P. K. (2004) 'A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,' proceedings of INFOCOM '04.
[63] ECMA (2005) International Standards 368 and 369, High Rate Ultra Wideband PHY and MAC Standards.
[64] Elson, J., Girod, L. and Estrin, D. (2002) *Fine grained network time synchronization using reference broadcasts*, OSDI, Boston.
[65] Erdogan, A., Cayirci, E. and Coskun, V. (2003) 'Sectoral Sweepers for Task Dissemination and Location Estimation in Ad Hoc Sensor Networks', MilCom'2003, Boston.
[66] Eschenauer, L. and Gligor, V. D. (2002) 'A key-management scheme for distributed sensor networks,' proceedings of the 9th Conference on Computer Communication Security (CCS2002), pp. 41–47.
[67] Fiat, A. and Shamir, A. (1987) 'How to Prove Yourself: Practical Solutions to Identification and Signature Problems,' proceedings of Crypto '86, pp.186–194.
[68] Fokine, K. (2002) '*Key Management in Ad Hoc Networks*,' Masters thesis, LiTH-ISY-EX-3322-2002, Lindköpings tekniska högskola.
[69] Fonseca, E. and Festag, A. (2006) '*A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS*,' NEC Technical Report NLE-PR-2006-19.
[70] Ganeriwal, S., Kumar, R. and Srivastava, M. D. (2003) 'Timing Synch Protocol for Sensor Networks,' first ACM Conference on Embedded Networked Sensor Systems (SenSys), November 2003, pp 139–149.
[71] Ganeriwal, S., Capcun, S., Han, C. and Srivastava, M. B. (2005) 'Secure Time Synchronization Service for Sensor Networks,' WiSE.
[72] Gennaro, R., Jarecki, S., Krawczyk, H. and Rabin, T. (1999) 'Secure Distributed Key Generation for Discrete-Log Based Cryptosystems,' proceedings of EUROCRYPT'99.
[73] Golle, P., Greene, D. and Staddon, J. (2004) 'Detecting and correcting malicious data in VANETs,' first ACM Workshop on Vehicular Ad Hoc Networks (VANET).
[74] Gruteser, M., Schelle, G., Jain, A., Han, R. and Grunwald, D. (2003) "Privacy-aware location sensor networks', in 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX).
[75] Haas, Z. J. and Liang, B. (1999) 'Ad Hoc Mobility Management with Uniform Quorum Systems,' *IEEE/ACM Transactions on Networking*, **7**(2), 228–240.
[76] Hammes, T. X. (2007) 'Fourth Generation Warfare Evolves, Fifth Emerges,' *Military Review*, May–June, pp. 14–23.
[77] Havinga, P. and Smit, G. (2000) 'Energy-efficient TDMA medium access control protocol scheduling,' *proceedings of the Asian International Mobile Computing Conference (AMOC 2000)*, November 2000.
[78] Hegland, A. M., Winjum, E., Mjølsnes, S. F., Rong, C., Kure, Ø. and Spilling, P. (2006) 'A Survey of Key Management in ad hoc Networks,' *IEEE Communications Surveys & Tutorials*, **8**(3), 48–66.
[79] Heinzelman, W. R., Kulik, J. and Balakrishan, H. (1999) 'Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,' MobiCom'99, pp. 174–185.
[80] Heinzelman, W. R., Chandrakasan, A. and Balakrishnan, H. (2000) 'Energy-Efficient Communication Protocol for Wireless Microsensor Networks,' IEEE Hawaii International Conference on System Sciences, pp. 1–10.
[81] Helmy, A. (2003) 'Mobility-Assisted Resolution of Queries in Large-Scale Mobile Sensor Networks,' *Computer Networks* special issue on Wireless Sensor Networks.
[82] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M., (1995) 'Proactive secret sharing or: How to cope with perpetual leakage,' proceedings of Crypto'95, pp. 339–352.
[83] Hu, L. and Evans, D. (2003) 'Using Directional Antennae to Prevent Wormhole attacks,' 11th Network and Distributed System Security Symposium, 2003.
[84] Hu, L., Perrig, A. and Johnson, D. B. (2003) 'Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks,' INFOCOM 2003.
[85] Hu, Y., Perrig, A. and Johnson, D. B. (2005) 'Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,'

Wireless Networks, **11**, 21–38.

[86] IEEE (2005a) Standard for Local and Metropolitan Area Networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).

[87] IEEE (2005b) Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

[88] IEEE-SA Standards Board (2003) 'IEEE Std. 802.15.4,' IEEE.

[89] Ingemarsson, I., Tang, D. and Wong, C. (1982) 'A conference key distribution system,' *IEEE Transactions on Information Theory*, **28**(5), 714–720.

[90] Intanagonwiwat, C., Govindan, R. and Estrin, D. (2000) 'Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,' ACM MobiCom '2000.

[91] ITU-T (1991) Recommendation X.800, 'Security Architecture for Open System Interconnection for CCITT Applications'.

[92] Joint Chiefs of Staff (2007) '*Electronic Warfare*,' Joint Publication 3-13.1, 'http:// www.fas.org/irp/doddir/dod/jp3-13-1.pdf,' January.

[93] Joshi, D., Namuduri, K. and Pendse, R. (2005) 'Secure, Redundant, and Fully Distributed Key Management Scheme for Mobile Ad Hoc Networks: An Analysis,' *EURASIP Journal on Wireless Communication and Networking*, **5**(4), 579–589.

[94] Jung, E. S. and Vaidya, N. H. (2002) 'A Power Control MAC Protocol for Ad Hoc Networks,' ACM MobiCom, September 2002.

[95] Karl, H. and Willig, A. (2005) *Protocols and Architectures for Wireless Sensor Networks*, John Wiley & Sons, Ltd,.

[96] Karlidere, T. and Cayirci, E. (2006) 'A MAC Protocol for Tactical Underwater Surveillance Networks,' MILCOM'06, Washington.

[97] Karlof, C. and Wagner, D. (2003) 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,' *Ad Hoc and Sensor Networks*, **1**, 293–315.

[98] Karn, P. (1990) 'MACA – a new channel access method for packet radio,' ninth ARRL Computing Networking Conference, September 1990, pp. 134–140.

[99] Khalili, A., Katz, J. and Arbaugh, W. A. (2003) 'Towards secure key distribution in truly ad-hoc networks,' proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks.

[100] Klima, V. (2006) 'Tunnels in Hash Functions: MD5 Collisions Within a Minute,' *Cryptology* ePrint Archive, Report 2006/105.

[101] Komerling, O. and Kuhn, M. G. (1999) 'Design principles for tamper resistant smartcard processors,' USENIX Workshop on Smartcard Technology, May.

[102] Kong, J., Zerfos, P., Luo, H., Lu, S. and Zhang, L. (2001) 'Providing robust and ubiquitous security support for mobile ad-hoc networks,' proceedings of the ninth International Conference on Network Protocols (ICNP'01), pp. 251–260.

[103] Kumar, S. Raghavan, V. S. and Deng, J. (2006) 'Medium access control protocols for ad hoc wireless networks: a survey,' *Ad Hoc and Sensor Networks*, **4**, 326–358.

[104] Law, Y. W. (2005) 'Key Management and Link-Layer Security of Wireless Sensor Networks, Energy-efficient Attack and Defence,' PhD Thesis, CTIT PhD-thesis Series, Series number: 1381–3617, CTIT Number: 05-75.

[105] Levine, J. (1999) 'Time synchronization over the Internet using an adaptive frequency locked loop,' *IEEE Transactions on Ultrasonics, Ferroelectronics, and Frequency Control*, **46**(4), 888–896.

[106] Li, Z., Trappe, W., Zhang, Y. and Nath, B. (2005) 'Robust Statistical Methods for Securing Wireless Localization in Sensor Networks,' International Conference on Information Processing in Sensor Networks (IPSN'05).

[107] Lin, X., Kwok, Y. and Lau, V.K.N. (2003) 'Power Control for IEEE 802.11 Ad Hoc Networks: Issues and a New Algorithm', International Conference on Parallel Processing (ICPP).

[108] Liu, D. and Ning, P. (2003a) 'Establishing Pairwise Keys in Distributed Sensor Networks,' proceedings of CCS'03.

[109] Liu, D. and Ning, P. (2003b) 'Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks,' proceedings of the 10th Annual Network and Distributed System Security Symposium, February 2003, pp. 263–276.

[110] Liu, D., Ning, P. and Du, W. (2005a) 'Detecting Malicious Beacon Nodes for Securing Location Discovery in Wireless Sensor Networks,' 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp 609–619.

[111] Liu, D., Ning, P. and Du, W. (2005b) 'Attack Resistant Location Estimation in Sensor Networks,' 4th International Conference on Information Processing in Sensor Networks (IPSN'05), pp 99–106.

[112] Lynn, B. (2002) 'Authenticated identity-based encryption,' *Cryptology* ePrint Archive, iacr (International Association for Cryptological Research).

[113] Marti, S., Giuli, T. J., Lai, K. and Baker, M. (2000) 'Mitigating routing misbehavior in mobile ad hoc networks,' MobiCom 2000.
[114] McGrew, D. A. and Sherman, A. T. (2003) 'Key Establishment in Large Dynamic Groups Using One-Way Function Trees,' *IEEE Transactions on Software Engineering*, **29**(5), 444–458.
[115] Meguerdichian, S. *et al.* (2001) 'Localized Algorithms in Wireless Ad hoc Networks: Location Discovery and Sensor Exposure,' *Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC2001)*.
[116] Merwe, J. V. D., Dawoud, D. and McDonald, S. (2005) 'A Survey on Peer-to-Peer Key Management for Military Type Mobile Ad Hoc Networks,' Military Information and Communications Symposium of South Africa – MICSSA.
[117] Mills, D. L. (1994) 'Internet time synchronization: the network time protocol,' in *Global States and Time in Distributed Systems*, IEEE Computer Society Press.
[118] Mills, D. L. (1998) 'Adaptive hybrid clock discipline algorithm for the network time protocol,' *IEEE Transactions on Networking*, **6**(5), 505–514.
[119] Mishra, A., Nadkarni, K. and Patcha, A. (2004) 'Intrusion Detection in Wireless Ad Hoc Networks', *IEEE Wireless Communications*, **11**(1), 48–60.
[120] Newsome, J., Shi, E., Song, D. and Perrig, A. (2004) 'The sybil attack in sensor networks: analysis & defenses,' third International Symposium on Information Processing in Sensor Networks.
[121] Niculescu, D. and Nath, B. (2003) 'Localized Positioning in Ad Hoc Networks,' IEEE SNPA 2003, pp. 42–50.
[122] NIST SP-800-97 – Guide to 802.11i – Establishing Robust Security Networks.
[123] Obraczka, K. (1998) 'Multicast transport protocols: a survey and taxonomy,' *IEEE Communications Magazine*, January, pp 94–102.
[124] Onel, T., Ersoy, C. and Cayirci, E. (2004) 'Handoff Techniques for the VCL Based Mobile Subsystem of the Next Generation Tactical Communication Systems', *Computer Networks*, **46**(5), 695–708.
[125] Ozturk, C., Zhang, Y. and Trappe, W. (2004) 'Source location privacy in energy constraint sensor network routing,' second ACM Workshop on Security of Ad Hoc and Sensor Networks.
[126] Pan, J., Cai, L., Shen, X. and Mark, J. W. (2007) 'Identity based secure collaboration in wireless ad hoc networks,' *Computer Networks*, **51**, 853–865.
[127] Papadimitratos, P. and Haas, Z. J. (2003) 'Secure link state routing for mobile ad hoc networks,' International Symposium on Applications and the Internet.
[128] Parno, B., Gaustad, E., Luk, M. and Perrig, A. (2006) 'Secure Sensor Network Routing: A Clean State Approach,' CoNEXT 2006.
[129] Patwari, N., Hero, A. O., Perkins, M., Correal, N. S. and O'Dea, R. J. (2003) 'Relative location estimation in wireless sensor networks,' *IEEE Transactions on Signal Processing*.
[130] Pedersen, T. (1991) 'Non-interactive and information-theoretic secure verifiable secret sharing,' proceedings of CRYPTO'91, pp. 129–140.
[131] Perrig, A., Canetti, R., Tygar, J. D. and Song, D. (2000a) 'Efficient Authentication and Signaling of Multicast Streams over Lossy Channels,' proceedings of IEEE Symposium on Research in Security and Privacy, pp. 56–73.
[132] Perrig, A., Canetti, R. and Whillock, B. (2000b) 'TESLA: Multicast Source Authentication Transform Specification,' in draft-ietf-msec-tesla-spec-00.
[133] Perrig, A., Canetti, R., Song, D., Tygar, J.D. and Briscoe, B. (2003) 'TESLA: Multicast Source Authentication Transform Introduction,' in draft-ietf-msec-tesla-intro-03.
[134] Perrig, A., Song, D. and Tygar, J. D. (2001a) 'ELK, a new Protocol for Efficient Large-Group Key Distribution,' proceedings of IEEE Symposium on Security and Privacy.
[135] Perrig, A., Szewczyk, R., Wen, V., Culler, D. and Tygar, J. D. (2001b) 'SPINS: Security Protocols for Sensor Networks,' MobiCom 2001.
[136] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V. and Culler, D. (2002) 'SPINS: Security Protocols for Sensor Networks,' *Wireless Networks*, **8**(5), 521–534.
[137] Perrig, A. and Tygar, J. D. (2003) *Secure Broadcast Communication in Wired and Wireless Networks*, Kluwer Academic Publishers.
[138] Pietro, R. D., Mancini, L. V. and Jajodia, S. (2002) 'Efficient and Secure Key Management for Wireless Mobile Communications,' proceedings of POMC'02.
[139] Poovendran, R. and Baras, J. S. (1999) 'An Information Theoretic Analysis of Root-Tree Based Secure Multicast Key Distribution Schemes,' *LNCS*, **1666**, 624–638.
[140] Pottie, G. J. and Kaiser, W. J. (2000) 'Wireless Integrated Network Sensors,' *Communications of the ACM*, **43**(5), 551–558.
[141] Priyantha, N.B., Chakraborty, A. and Balakrishnan, H. (2000) The cricket location support system, proceedings of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MobiCom), August 2000.
[142] Puzar, M., Andersson, J., Plagemann, T. and Roudier, Y. (2005) 'SKiMPy: A Simple Key Management Protocol for

MANETs in Emergency and Rescue Operations,' proceedings of ESAS'05.
[143] Rafaeli, S. and Hutchison, D. (2003) 'A Survey of Key Management for Secure Group Communication,' *ACM Computing Surveys*, **35**(3), 309–329.
[144] Rafaeli, S., Mathy, L. and Hutchison, D. (2001) 'EHBT: An efficient protocol for group key management,' *LNCS*, **2233**,159–171.
[145] RFC 2828 Internet Security Glossary May 2000.
[146] Rhee, K. H., Park, Y. H. and Tsudik, G. (2004) 'An Architecture for Key Management in Hierarchical Mobile Ad-hoc Networks,' *Journal of Communications and Networks*, **6**(2), 156–162.
[147] Rhee, K. H., Park, Y. H. and Tsudik, G. (2005) 'A Group Key Management Architecture for Mobile Ad-hoc Wireless Networks,' *Journal of Information Science and Engineering*, **21**(2), 415–428.
[148] Rivest, R., Shamir, A. and Adleman, L. (1978) 'A Method for Obtaining Digital Signatures and Public Key Cryptosystems,' *Communications of the ACM*, February 1978.
[149] Roman, R., Zhou, J. and Lopez, J. (2005) 'On the Security of Wireless Sensor Networks', proceedings of the 2005 ICCSA Workshop on Internet Communications Security, Singapore, *LNCS*, **3482**, 681–690.
[150] Roman, R., Zhou, J. and Lopez, J. (2006) 'Applying Intrusion Detection Systems to Wireless Sensor Networks', IEEE Consumer Communications & Networking Conference (CCNC 2006), Las Vegas (EEUU), January 2006.
[151] Royer, E. M. and Toh, C. (1999) 'A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,' *IEEE Personal Communications Magazine*, **6**(2), pp. 46–55.
[152] Sadagopan, N., Krishnamachari, B. and Helmy, A. (2003) 'The Acquire Mechanism for Efficient Querying in Sensor Networks,' *Ad Hoc Networks*.
[153] Salem, N. B., Buttyan, N., Hubaux, J. and Jakobsson, M. (2003) 'A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks,' MobiHoc 2003.
[154] Sankarasubramaniam, Y., Akan, O. B. and Akyildiz, I. F. (2003) 'ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks,' ACM Mobihoc'03.
[155] Sanzgiri, K., Levine, B. N., Shields, C., Dahill, B. and Belding-Royer, E. M. (2002) 'A Secure Routing Protocol for Ad Hoc Networks,' International Conference on Network Protocols (ICNP).
[156] Sasse, A., Brostoff, S. and Weirich, D. (2001) 'Transforming the "weakest link" – a human / computer interaction approach to usable and effective security', *BT Technology Journal*, **19**(3), 122–131.
[157] Savvides, A., Han, C. and Srivastava, M. (2001) 'Dynamic fine grained localization in ad-hoc networks of sensors,' proceedings of MobiCom'01.
[158] Schurgers, C., Kulkarni, G. and Srivastava, M. B. (2002) 'Distributed On-Demand Address Assignment in Wireless Sensor Networks,' *IEEE Transactions on Parallel and Distributed Systems*, **13**(10).
[159] Selcuk, A., McCubbin, C. and Sidhu, D. (2000) 'Probabilistic Optimization of LKH-based Multicast Key Distribution Schemes,' IETF Internet-Draft, January, 2000, draft-selcuk-probabilistic-lkh-00.txt.
[160] Shamir, A. (1979) 'How to share a secret,' *Communications of the ACM*, **22**, 612–613.
[161] Shamir, A. (1984) 'Identity-based cryptosystems and signature schemes,' proceedings of CRYPTO '84, pp. 47–53.
[162] Shen, C., Srisathapornphat, C. and Jaikaeo, C. (2001) 'Sensor Information Networking Architecture and Applications,' *IEEE Personal Communications*, **8**(4), 52–59.
[163] Singh, S. and Raghavendra, C. S. (1998) 'PAMAS: Power Aware Multi-Access protocol with Signaling for Ad Hoc Networks,' *ACM Computer Communications Review*, July.
[164] Smailagic, A., Siewiorek, D.P., Anhalt, J., Kogan, D. and Wang, Y. (2001) 'Location sensing and privacy in a context aware computing environment', proceedings of the International Conference on Pervasive Computing, pp. 15–23.
[165] Sohrabi, K., Gao, J., Ailawadhi, V. and Pottie, G. (1999) 'A self-organizing sensor network,' proceedings of the 37th Allerton Conference on Communication, Control, and Computing, Monticello, Illinois, September.
[166] Staddon, J., Miner, S., Franklin, M., Balfanz, D., Malkin, M. and Deam, D. (2002) 'Self-Healing Key Distribution with Revocation,' proceedings of the IEEE Symposium on Security and Privacy.
[167] Stallings, W. (2000) *Data and Computer Communications*, sixth edition, Prentice Hall, Englewood Cliffs, New Jersey, USA.
[168] Stallings, W. (2003) *Network Security Essentials*, Prentice Hall, Englewood Cliffs, New Jersey.
[169] Stann, F. and Wagner, J. (2003) 'RMST: Reliable Data Transport in Sensor Networks,' IEEE SNPA 2003, pp. 102–112.
[170] Steiner, M., Tsudik, G. and Waidner, M. (1998) 'CLIQUES: A new approach to Group Key Agreement,' proceedings of ICDCS'98.
[171] Steiner, M., Tsudik, G. and Waidner, M. (2000) 'Key agreement in dynamic peer groups,' *IEEE Transactions on Parallel and Distributed Systems*, **11**(8), 769–780.
[172] Subramanian, L. and Katz, R. (2000) 'An Architecture for Building Self-Configurable Systems,' *proceedings of theIEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000)*, Boston, August 2000.

[173] Tannenbaum, A. S. (2003) *Computer Networks*, Prentice Hall, Englewood Cliffs, New Jersey.
[174] Tezcan, N., Cayirci, E. and Caglayan, U. (2004) 'End-to-end Reliable Event Transfer in Wireless Sensor Networks', PIMRC'2004.
[175] Wallner, D., Harder, E. and Agee, R. (1999) 'Key Management for Multicast: Issues and Architectures,' IETF RFC 2627.
[176] Walters, J. P., Liang, Z., Shi, W. and Chaudhary, V. (2006) 'Wireless sensor network security: a survey,' in *Security in Distributed, Grid and Pervasive Computing*, Y. Xiao (Ed.), Auerbach Publications/CRC Press..
[177] Wan, C.-Y., Campbell, A. T. and Krishnamurty, L. (2003) 'PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks,' ACM WSNA'02, Atlanta.
[178] Wang, Y. (2005) 'Efficient Identity-Based and Authenticated Key Agreement Protocol,' *Cryptology* eprint Archive, Report 2005/108.
[179] Waters, B. (2005) 'Efficient Identity-Based Encryption Without Random Oracles,' proceedings of Eurocrypt 2005.
[180] Wi-Fi Alliance (2003) '*Wi-Fi Protected Access: Strong, standard-based interoperability security for today's Wi-Fi networks*'.
[181] Winjum, E., Hegland, A. M., Spilling, P. and Kure, O. (2005) 'A Performance Evaluation of Security Schemes proposed for the OLSR Protocol,' proceedings of MILCOM'05.
[182] Wong, C. K., Gouda, M. and Lam, S. S. (1998) 'Secure Group Communications Using Key Graphs,' proceedings of the SIGCOMM '98.
[183] Wong, C. K. and Lam, S. S. (2000) 'Keystone: A Group Key Management Service,' proceedings of ICT 2000.
[184] Wood, A. and Stankovic, J.A. (2005) 'A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks', in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, pp. 32:1–20.
[185] Wood, A. D., Fang, L., Stankovic, J. A. and He, T. (2006) 'SIGF: A family of configurable, secure routing protocols for wireless sensor networks,' ACM SASN.
[186] Wu, B., Wu, J., Fernandez, E. B. and Magliveras, S. (2005) 'Secure and Efficient Key Management in Mobile Ad Hoc Networks,' proceedings of IPDPS'05.
[187] Xi, Y., Schwiebert, L. and Shi, W. (2006) 'Preserving privacy in monitoring based wireless sensor networks,' second International Workshop on Security in Systems and Networks (SSN'06).
[188] Ye, W., Heidemann, J. and Estrin, D. (2004) 'Medium Access Control with Coordinated, Adaptive Sleeping for Wireless Sensor Networks,' *IEEE/ACM Transactions on Networking*, **12**(3), 493–506.
[189] Yi, S. and Kravets, R. (2002a) '*Key Management for Heterogeneous Ad Hoc Wireless Networks*,' University of Illinois at Urbana-Champaign.
[190] Yi, S. and Kravets, R. (2002b) '*MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks*,' Report No. UIUCDCS-R-2004-2502,UILU-ENG-2004-1805, University of Illinois at Urbana-Champaign.
[191] Yi, S. and Kravets, R. (2004) 'Composite Key Management for Ad Hoc Networks,' proceedings of Mobiquitous'04.
[192] Yu, B. and Xiao, B. (2006) '*Detecting selective forwarding attacks in wireless sensor networks*,' IEEE.
[193] Zapata, M. G. and Asokan, N. (2002) 'Securing Ad Hoc Routing Protocols,' WiSe.
[194] Zhang, Y., Lee, W. and Huang, Y. (2003) 'Intrusion Detection Techniques for Mobile Wireless Networks', *Wireless Networks Journal* (ACM WINET), **9**(5), September.
[195] Zhou, L. and Haas, Z. J. (1999) 'Securing ad hoc networks,' *IEEE Network Magazine*, **13**(6), 24–30.
[196] Zhu, S., Xu, S., Setia, S. and Jajodia, S. (2003a) 'Establishing pair-wise keys for secure communication in ad hoc networks: A probabilistic approach,' proceedings of the 11th IEEE International Conference on Network Protocols (ICNP'03), pp. 326–335.
[197] Zhu, S., Setia, S. and Jajodia, S. (2003b) 'LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,' proceedings of CSS'03.
[198] Zhu, S., Setia, S., Xu, S. and Jajodia, S. (2004) 'GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks,' proceedings of Mobiquitous'04.
[199] Zhu, B., Bao, F., Deng, R. H., Kankanhalli, M. S. and Wang, G. (2005) 'Efficient and robust key management for large mobile ad hoc networks,' *Computer Networks*, **48**(4), 657–682.
[200] ZigBee Alliance (2004) 'ZigBee Standard, version 1.'
[201] Zimmermann, P. (1994) *PGP User's Guide*, MIT Press.

本书特色

- 介绍了新技术基础和关键问题，详细阐述了安全攻击和对策
- 覆盖拒绝服务攻击（DoS）、硬件角度的无线自组织网络和传感器网络安全、安全路由
- 包括密码学基础、电子战相关信息
- 每章最后有复习题，促进学习

国际视野　科技前沿

国际信息工程先进技术译丛

《无线自组织网络和传感器网络安全》
《纳米CMOS电路和物理设计》
《现代通信原理》（原书第2版）
《认知无线电网络》
《高速数字系统的信号完整性和辐射发射》
《UMTS中的LTE：基于OFDMA和SC-FDMA的无线接入》
《生物医学工程学概论》（原书第2版）
《全面的功能验证：完整的工业流程》
《无线Mesh网络架构与协议》
《UMTS蜂窝系统的QoS与QoE管理》
《半导体制造与过程控制基础》
《WCDWA原理与开发设计》
《下一代移动系统：3G/B3G》
《IMS:IP多媒体概念和服务》（原书第2版）
《下一代无线系统与网络》
《深入浅出UMTS无线网络建模、规划与自动优化：理论与实践》
《HSDPA/HSUPA技术与系统设计——第三代移动通信系统宽带无线接入》
《无线传感器及元器件：网络、设计与应用》
《印制电路板——设计、制造、装配与测试》
《IPTV与网络视频：拓展广播电视的应用范围》
《多电压CMOS电路设计》
《微电子技术原理、设计与应用》
《蜂窝网络高级规划与优化2G/2.5G/3G/…向4G的演进》
《基于蜂窝系统的IMS——融合电信领域的VoIP演进》
《无线网络中的合作原理与应用》
《电生理学方法与仪器入门》
《移动电视：DVB-H、DMB、3G系统和富媒体应用》
《环境网络：支持下一代无线业务的多域协同网络》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3G CDMA网络》
《UMTS-HSDPA系统的TCP性能》
《宽带无线通信中的空时编码》
《数字图像处理》（原书第4版）
《基于4G系统的移动服务技术》
《吉规模集成电路互连工艺及设计》
《高性能微处理器电路设计》

上架指导：工业技术/通信技术

WILEY
www.wiley.com

ISBN 978-7-111-34574-9

封面设计：马精明

定价：68.00元

地址：北京市百万庄大街22号　邮政编码：100037
电话服务　网络服务
社服务中心：(010)88361066　门户网：http://www.cmpbook.com
销售一部：(010)68326294　教材网：http://www.cmpedu.com
销售二部：(010)88379649　封面无防伪标均为盗版
读者购书热线：(010)88379203