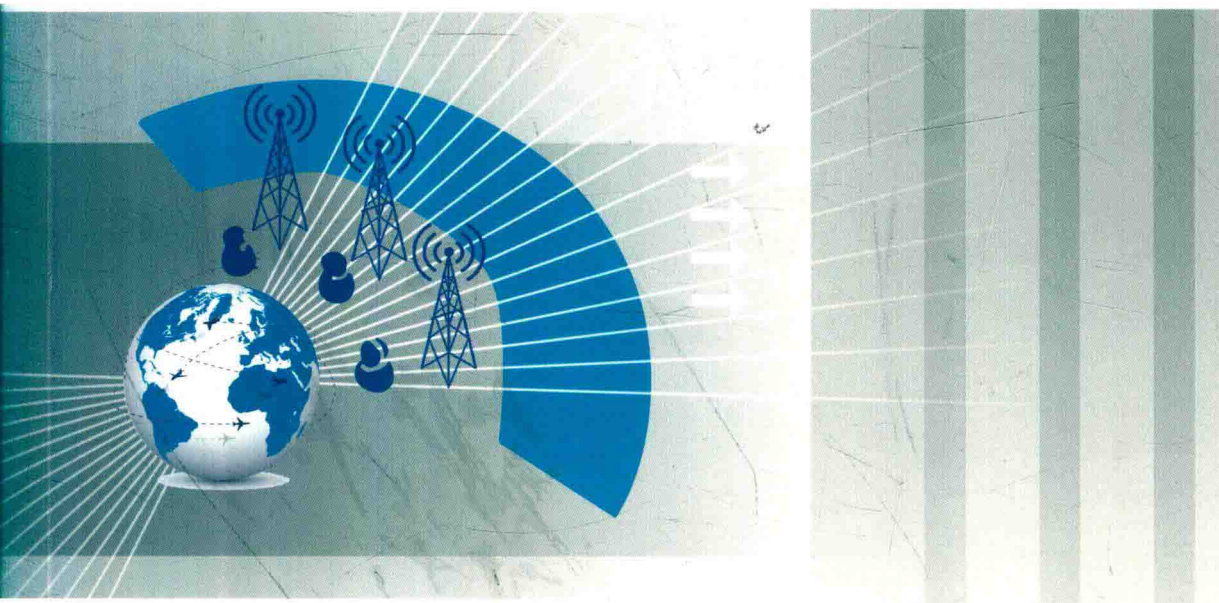
信息化网络平台研究丛书

异构无线网络的安全研究

苗许娜◎著



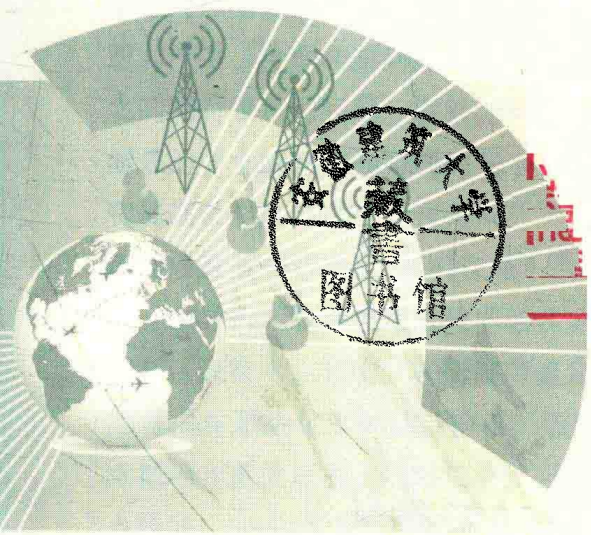
STUDY ON SECURITY OF HETEROGENEOUS WIRELESS NETWORK

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

信息化网络平台研究丛书

异构无线网络的安全研究

苗许娜◎著



STUDY ON SECURITY OF HETEROGENEOUS WIRELESS NETWORK

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目（CIP）数据

异构无线网络的安全研究 / 苗许娜著. —北京：经济管理出版社，2018.6
ISBN 978-7-5096-5839-0

Ⅰ.①异… Ⅱ.①苗… Ⅲ.①异构网络—无线网—网络安全—研究 Ⅳ.①TP393.02
中国版本图书馆 CIP 数据核字（2018）第 131448 号

组稿编辑：杨 雪
责任编辑：杨 雪 王 硕
责任印制：黄章平
责任校对：陈 颖

出版发行：经济管理出版社
（北京市海淀区北蜂窝 8 号中雅大厦 A 座 11 层 100038）
网 址：www.E-mp.com.cn
电 话：（010）51915602
印 刷：北京玺诚印务有限公司
经 销：新华书店
开 本：720mm×1000mm/16
印 张：18.75
字 数：288 千字
版 次：2018 年 9 月第 1 版 2018 年 9 月第 1 次印刷
书 号：ISBN 978-7-5096-5839-0
定 价：59.00 元

前言 Preface

在基于异构无线网络路由技术的密钥管理研究方面，本书提出了一个基于离散对数问题的两层分散式组播密钥管理方案。该方案包括密钥销毁、产生、分配和更新方案，解决了密钥计算、数据安全传输和能量节省之间同时兼顾的问题。能够为异构无线网络路由安全系统提供高适用和高能效的安全机制和可实现的安全服务，并且达到了异构无线网络节省能量和提高安全性等优点。在完成项目任务的同时，我们又在异构无线网络密钥管理算法和移动 IP 密钥管理方案等方面做了扩展性的研究。

在异构无线网络路由技术的认证机制方面，本书主要研究了身份认证和源认证技术。其中，在研究节点定位和识别的过程中，提出了基于分簇的 Merkle 散列树实体认证协议。该协议可以抵御节点被捕获攻击，防止节点抵赖和重放攻击，同时该协议可以保护数据的完整性；为了防止恶意节点伪造、Sybil 攻击和重放攻击，本书分别提出了基于秘密共享的异构无线网络实体认证方案和基于声誉和信任组的异构无线网络实体认证协议。我们的工作不仅完成了项目的研究任务，同时在研究过程中，也对异构无线网络认证的其他技术，比如防止拒绝服务攻击和恶意节点位置跟踪等方面做了一些扩展性的研究。

在基于异构无线网络路由技术的安全防御机制研究方面，本书研究了各种路由攻击行为的分析和分类，提出了一种分布协同式的入侵检测安全防御策略，采用多个代理模块分别实现数据收集、分析检测、入侵响应和

代理管理的任务。并且基于静态和动态数据库的建立，首次将灰理论应用于异构无线网络的攻击检测建模上，实现了入侵检测和响应的协同，构建了防御机制和响应机制。同时，本书为了解决异构无线网络引入入侵检测机制产生的能耗问题，提出了一种专门针对异构无线网络的轻量级本地入侵检测系统（单机 IDS）的设计方案，该系统具有较高的检测准确率和较小的能量消耗。这些工作较好地完成了项目的研究任务。

在异构无线网络安全路由协议研究方面，本书分别在平面路由和分层路由两个方面提出了基于多目标优化的安全路由协议和基于分簇的异构无线网络安全路由协议。这两个路由协议都考虑到密钥管理、认证机制和入侵检测的有机结合，将路由协议和安全机制同时进行，把能量优化、路由安全性和传输时延同时作为路由算法设计目标，这样可以增强网络的强壮性和安全性。另外本书在完成任务的同时，在异构无线网络的信息传输方式和应用环境方面做了一些扩展性研究。

目录 Contents

1 引 言

1.1 国内外研究现状

异构无线网络是由一组计算、存储和能量有限的传感器节点通过无线介质自组织构成的无线网络，节点间通过多跳转发机制进行数据通信，具有安全机制的路由技术是其关键技术。它能够在人们无法接近的恶劣或特殊环境中工作，如地震与气候监控、外层空间以及战场环境监控和信息采集系统建设等，是信息感知和采集的一场革命，在很多场合逐渐受到越来越多的重视，目前已经成为信息技术领域的研究热点。本项目主要介绍异构无线网络的历史发展、特点和应用、主要研究热点，以及论文的目的、意义、主要创新和组织结构。

1.1.1 项目的研究背景

人类生存的空间是有限的，而生存的过程是无限的。如何合理开发与利用有限空间中的有限资源来满足人类社会在无限时间中的可持续发展需求，减少资源获取的损失，保障安全健康的生活环境，通过人、物、人与物、信息四个因素的互动和协调，以达到相对安全或向绝对安全逼近，已成为人类社会的共同主题。在知识经济的信息社会中，信息不仅作为一种重要的经济资源，而且作为一种物质形式与自然资源相结合，成为人类生

存与发展的基础。因此，信息的安全获取和传输直接影响着经济建设与发展。

随着微机电系统 MEMS（Micro-Electro-Mechanical Systems）技术、无线通信和数字电子技术的进步和日益成熟，具有感知能力、计算能力和通信能力的微型传感器已经出现。1988 年，Mark Weiser 提出了 Ubiquitous Computing（缩写为 Ubicomp 或 UC）思想，即书后参考文献［2］和文献［3］中常出现的“普适计算”（Pervasive Computing），促使计算、通信和传感器三项技术相结合，产生了异构无线网络（Wireless Sensor Networks，WSN）。这种异构无线网络综合了传感器技术、嵌入式计算技术、分布式信息处理技术和通信技术，能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息，并对这些信息进行处理，获得详尽而准确的信息，传送到需要这些信息的用户。在一定程度上，异构无线网络提供用户智能终端和对环境更好的理解，作为一个新的研究领域，立即引起了人们的极大关注。

异构无线网络是一种特殊的 Ad Hoc 网络，它不需要固定网络支持，具有快速展开、抗毁性强等优势，同时还具有自组织、多跳、动态拓扑和能量资源受限等特点，可应用于环境和水文监测、安全生产监控、灾情预警、战场信息数据采集传输和损失评估、灾难拯救等。因此，异构无线网络的特性使它在军事、商业、民用和医疗等领域有广阔的应用，逐渐成为无线通信网络中的一个研究热点。

异构无线网络是一个无线移动的复杂通信网络系统，它的应用要求工作区域的节点数目多，数据传输不限于单跳，而需建立多跳的网络环境；另外，各个节点还需兼备路由器的功能和面临着比传统网络更大的安全威胁等特殊性，使其存在许多需要深入研究的问题，如体系结构、路由算法、服务质量、通信协议和安全保障等。本书对异构无线网络的安全路由技术进行了深入研究，在路由协议的密钥管理、认证机制、攻击检测等方面建立有效的安全保障，同时与路由技术相结合提出较为适用的理论和路由算法。

1.1.2 异构无线网络的概念及特点

异构无线网络是由一组传感器以自组织方式构成的无线网络，其目的

是协作地感知、采集和处理网络覆盖的地理区域中感知对象的信息，并发布给观察者。

传感器、感知对象和观察者是异构无线网络的三个基本要素，无线网络是传感器之间、传感器与观察者之间的通信方式，用于在传感器与观察者之间建立通信路径；协作地感知、采集、处理、发布感知信息是异构无线网络的基本功能。它将逻辑上的信息世界与客观上的物理世界融合在一起，改变了人类与自然界的交互方式。

一组功能有限的传感器协作地完成较大的感知任务是异构无线网络的重要特点。传感器主要由感知部件、嵌入式处理器、存储部件、通信部件、软件和电源组成，完成对感知对象的信息采集、存储和简单的计算后，传输给观察者以提供环境的决策依据。其结构如图 1-1 所示。

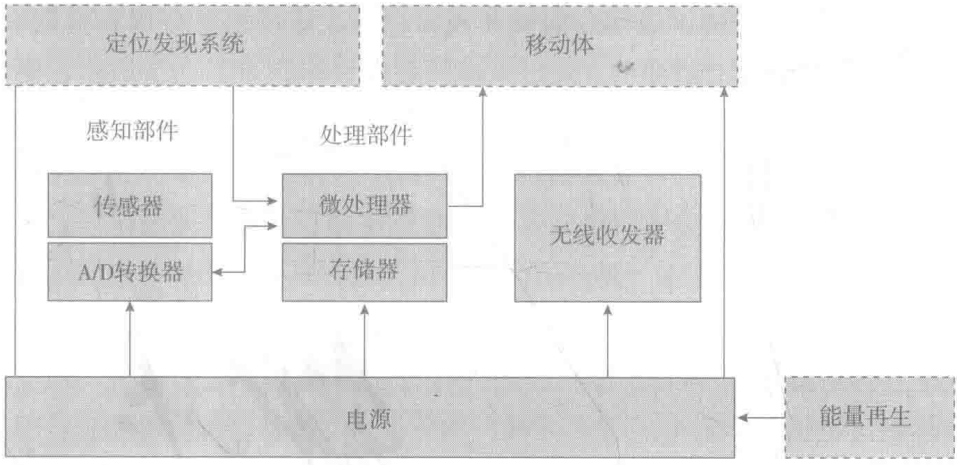


图 1-1 异构无线网络传感器节点构成示意图

异构无线网络中的部分或全部节点可以移动，相应的拓扑结构也会随着节点的移动而不断地动态变化。节点间以 Ad Hoc 方式进行通信，每个节点都可以充当路由器的角色，并且都具备动态搜索、定位和恢复连接的能力。传感器节点通过人工、机械、飞行器空投等方法进行随机播撒，然后传感器节点进入自检和启动唤醒状态，采用相关的组网算法，从而按预设方式或规律结合形成网络，根据有效的路由算法选择合适的路径进行数据通信。其一般网络拓扑结构如图 1-2 所示。

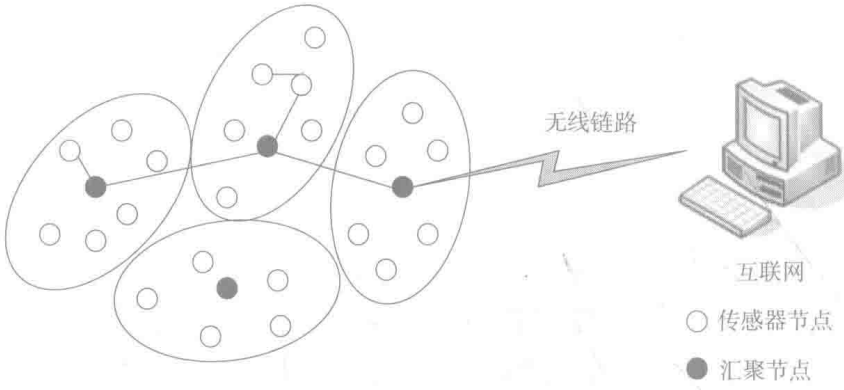


图 1-2　异构无线网络的网络拓扑结构

异构无线网络节点资源受限和动态拓扑结构决定了网络构建的复杂性。异构无线网络协议栈结合能量和路由寻找，运用网络协议整合数据，通过无线方式进行有效通信，促进节点间有效合作。如图 1-3 所示，协议栈由应用层、传输层、网络层、数据链路层和物理层，以及能量管理平台、移动管理平台和任务管理平台组成。

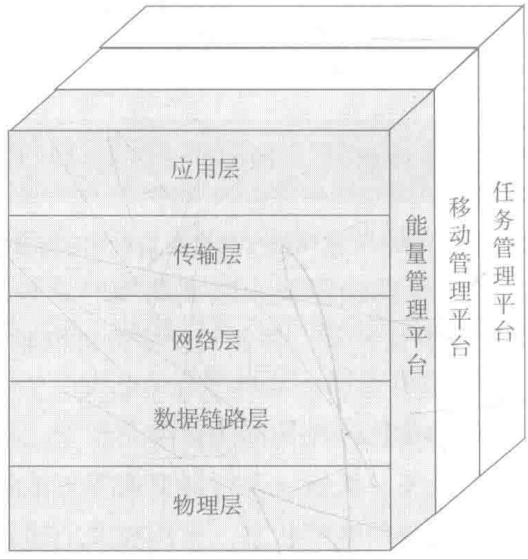


图 1-3　异构无线网络协议栈结构

协议栈的各层分工协作，功能不同。应用层由各种应用软件系统构成，为用户开发各种传感器网络应用软件提供有效的软件开发环境和软件工具。传输层按照传感器网络的需求产生数据流，并负责数据流的传输控制，它是保证通信服务的重要部分。网络层维护传输层提供的数据流，主要涉及路由技术，负责路由生成和路由选择。数据链路层考虑到网络环境存在噪声和传感器节点的移动，主要负责数据流的多路技术、数据帧探测、介质访问和差错控制，减少邻居节点广播的冲突，保证可靠的点到点和点到多点通信。物理层的关键技术是调制、发送和接收技术。

另外，能量管理、移动管理和任务管理平台分别监视传感器节点中的每个节点的能量、移动和任务，这些管理平台有助于传感器节点调整感知任务和降低总体能量消耗。

虽然无线通信网络能快速、灵活、方便地支持用户的移动性，使目前几乎所有的通信系统都与无线通信方式有关，如蜂窝系统、无绳系统、卫星通信系统、无线局域网与无线广域网（WLAN/WAN）、移动 IP、无线 ATM、分组无线网（PRNET）和移动 Ad Hoc 网络等。但异构无线网络特殊的节点组成和拓扑结构使其具有以下特性：

（1）自组织性。网络的布设和展开无须依赖于任何预设的网络设施，节点通过分层协议和分布式算法协调各自的行为，部分节点开机后就可以快速、自动地组成一个独立的网络。

（2）多跳性。网络中节点通信距离有限，一般在几十米范围内，节点只能与它的邻居直接通信。如果希望与其射频覆盖范围之外的节点进行通信，则需要通过中间节点进行路由。固定网络的多跳路由使用网关和路由器来实现，而异构无线网络中的多跳路由是由网络节点完成的，没有专门的路由设备。这样每个节点既可以是信息的发起者，也是信息的接收者和转发者。

（3）动态拓扑性。异构无线网络是一个动态的网络，节点可以随处移动；一个节点可能会因为电池能量耗尽或其他故障，退出网络运行；一个节点也可能由于工作的需要而被添加到网络中。这些都会使网络的拓扑结构随时发生变化，因此网络具有动态拓扑组织功能。

（4）资源受限性。异构无线网络中节点一般放入无人涉及的区域环

境，节点的能量和资源都是固定的初始值；同时传感器节点由于受价格、体积和功耗的限制，其计算能力、程序空间和内存空间比普通的计算机功能要弱很多，这一点决定了在节点操作系统设计中，协议层次不能太复杂。因此，考虑到它的能量资源、计算能力、通信带宽、存储容量都非常有限，要求在通信协议及算法的设计过程中，应尽可能降低能量消耗，提高能量使用的效率，避免过度使用低能量节点，从而延长网络生命周期。同时协议或算法不能占用大量存储空间，也应当尽可能减少计算量。

（5）无中心。异构无线网络中没有严格的控制中心，所有节点地位平等，是一个对等式网络。节点可以随时加入或离开网络，个别节点的故障不会影响整个网络的运行，具有很强的抗毁性。

（6）节点数量众多，分布密集。为了对一个区域执行监测任务，往往有成千上万传感器节点空投到该区域。传感器节点分布非常密集，利用节点之间相对连接性来保证系统的容错性和抗毁性。

（7）有限的无线通信带宽。异构无线网络没有固定基础设施的支持，节点间的通信均通过无线传输来完成。由于无线信道本身的物理特性，它提供的网络带宽相对有线信道要低得多。此外，考虑到竞争，共享无线信道产生的碰撞、信号衰减、噪声干扰等多种因素，移动终端可得到的实际带宽远远小于理论中的最大带宽值。

（8）安全性差。异构无线网络采用无线信道、有限电源、分布式控制等技术和方式进行通信，所以更加容易受到被动窃听、主动入侵、拒绝服务、路由环欺骗、路由重定向等各种网络攻击。因此，信道加密、抗干扰、用户认证、加密和攻击检测等其他安全措施都需要特别考虑。

1.1.3 异构无线网络的发展

异构无线网络被认为是21世纪最重要的技术之一，它将会对人类未来的生活方式产生深远影响。2003年2月美国《技术评论》杂志（Technology Review）评出对人类未来生活产生深远影响的十大新兴技术，异构无线网络被列为第一。它的研究起步于20世纪90年代末期，从2000年起，国际上开始出现有关异构无线网络相关技术的研究报道。国内研究起步稍晚些，但也取得不少成果。