物联网安全理论与技术

Internet of Things Security Theory and Technology

◎ 杨奎武　郑康锋　张冬梅　郭渊博　编著

中国工信出版集团

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

物联网安全理论与技术

杨奎武　郑康锋　张冬梅　郭渊博　编著

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

内 容 简 介

本书以无线传感器网络和 RFID 系统为典型代表，从物联网感知层、网络层、应用层安全三方面对物联网面临的安全问题及最新的物联网安全理论和技术进行了深入介绍。尤其是在感知层安全方面，本书更是从物理安全、认证机制、密钥管理、传输安全、协议安全、入侵检测、系统安全七个方面，以攻防相结合、理论与实践相结合的方法重点阐述了物联网面临的安全问题及解决方案。同时，本书还给出了诸如 PUF 技术、物理层秘钥生成、移动目标防御等近年最新的学术研究成果。

本书内容丰富、涵盖面广、系统性强，非常适合作为物联网、通信、信息安全等相关专业的高年级本科生、研究生的教材及参考书，也非常适合作为物联网及信息安全领域教师和工程技术人员的参考用书。

图书在版编目（CIP）数据

物联网安全理论与技术/杨奎武等编著. —北京：电子工业出版社，2017.1
ISBN 978-7-121-30407-1

Ⅰ. ① 物… Ⅱ. ① 杨… Ⅲ. ① 互联网络 - 应用 - 安全技术 ② 智能技术 - 应用 - 安全技术
Ⅳ. ① TP393.4 ② TP18

中国版本图书馆 CIP 数据核字（2016）第 279661 号

策划编辑：曲 昕
责任编辑：谭丽莎
印 刷：北京中新伟业印刷有限公司
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787 × 1 092 1/16 印张：17 字数：435.2 千字
版 次：2017 年 1 月第 1 版
印 次：2017 年 1 月第 1 次印刷
定 价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

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

本书咨询联系方式：quxin@ phei. com. cn。

前　言

物联网的概念从提出到现在已经有近20年了，虽然刚刚提出来的时候很多人都觉得物联网很遥远，但是随着近年来科学技术的快速发展，我们现在已经能够切身体会到物联网的无处不在了。在物联网进一步普适化、泛在化的道路上，恐怕目前技术领域的唯一绊脚石就是安全问题了，这也自然成为物联网领域研究的热点。

为适应物联网安全工作的发展需要，满足广大物联网技术领域学生、教师及工程技术人员的学习工作需求，我们结合多年课题研究的成果编写了本书，目的就是为广大读者提供参考，进一步推动物联网的广泛应用。

本书从物联网安全基础、物联网感知安全、物联网网络安全、物联网应用安全四个层面对物联网安全问题及典型的物联网安全技术进行了总结和分析。全书共12章，第1、2章主要介绍了物联网的基本概念、结构，物联网安全面临的挑战及安全框架，以及物联网安全技术的密码学基础知识。第3～9章分别从物理安全、认证机制、密钥管理、数据传输安全、MAC层协议安全、感知层入侵检测和嵌入式系统安全7个方面介绍了物联网感知层安全的关键技术，这部分内容也是本书的主体和重点，其中包含了很多作者最新的研究成果。第10章介绍物联网接入网络安全技术，主要包括无线局域网、WiMAX和移动通信接入网络的安全问题。第11章主要从被动防御和主动防御两个方面介绍了物联网核心网络的典型安全技术。第12章重点从物联网云安全的角度给出了物联网应用相关安全技术介绍。

本书由杨奎武主笔并统稿，由杨奎武、郑康锋、张冬梅和郭渊博共同编撰完成，编写过程中得到了信息工程大学和北京邮电大学的大力支持，陈越教授、贾洪勇讲师、武斌讲师等很多教师都对本书提出了宝贵的意见和建议；傅蓉蓉、肖倩、张紫楠、隋雷、姜文博、郑巧琼、肖欢、张之则等研究生协助完成了部分文档的整理工作；电子工业出版社的曲昕编辑为本书的出版付出了辛勤的劳动，在此向大家表示由衷的感谢。另外，本书很多内容参考了互联网上的资源及其他相关著作，在此对资源的分享者和其他著作作者一并表示感谢。

由于物联网安全技术发展迅速，新技术和新标准不断涌现，加之作者水平有限，编写时间仓促，本书难免存在错误和不足之处，敬请各位专家和读者批评指正。

编著者

2017年1月

目　录

第1章 绪 论

随着物联网技术研究和应用的不断发展，物联网安全面临的问题越来越突出，成为制约网络发展的重要瓶颈，这也使得物联网安全及隐私保护技术日益成为国内外学者研究的焦点。相对于传统的计算机网络安全技术，物联网安全及隐私保护技术研究涉及的内容更加广泛，也更具复杂性。本章在对物联网的基本概念、体系结构及关键技术等内容介绍的基础上，从总体上讲述了物联网面临的安全及挑战，给出了物联网的安全目标及当前物联网安全技术研究的热点。

1.1 概述

1.1.1 物联网的定义

物联网（Internet of Things，IoT）这一概念，是由麻省理工学院自动识别实验室于1999年在研究RFID时提及并引起关注的，并于2005年11月国际电信联盟（ITU）发布的《ITU互联网报告2005：物联网》中正式提出并进行扩展。针对物联网的定义，目前国际上并没有一致认同的准确和权威的定义，并且随着技术的进步，物联网的定义及其所涉及的内涵和外延也都在不断发生变化。

目前在国内被最普遍引用的物联网定义是：通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。它是在互联网基础上延伸和扩展的网络。

而“全球RFID运作及标准化协调支持行动（CASAGRAS）”项目给出的物联网的定义如下：IoT is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object - identification, sensor and connection capability as the basis for the development of independent federated services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

虽然国际上对物联网的定义并没有统一认识，但通俗地讲，物联网就是一个通过信息技术将各种物体连接成网络，使物体变得更加智能化，从而实现人与物、物与物之间的通信的网络。物联网对其所连接的物体主要有三点要求：一是物联网中每一个物体都可寻址；二是每一个物体均可以通信；三是每一个物体均可控制。

1.1.2 物联网体系结构

物联网的体系结构目前较为公认的是三层体系结构，即物联网从下到上分为三个层次，依次是：感知层、网络层（包括接入网络）和应用层（包括信息处理、云计算等平台），如

图 1-1 所示。

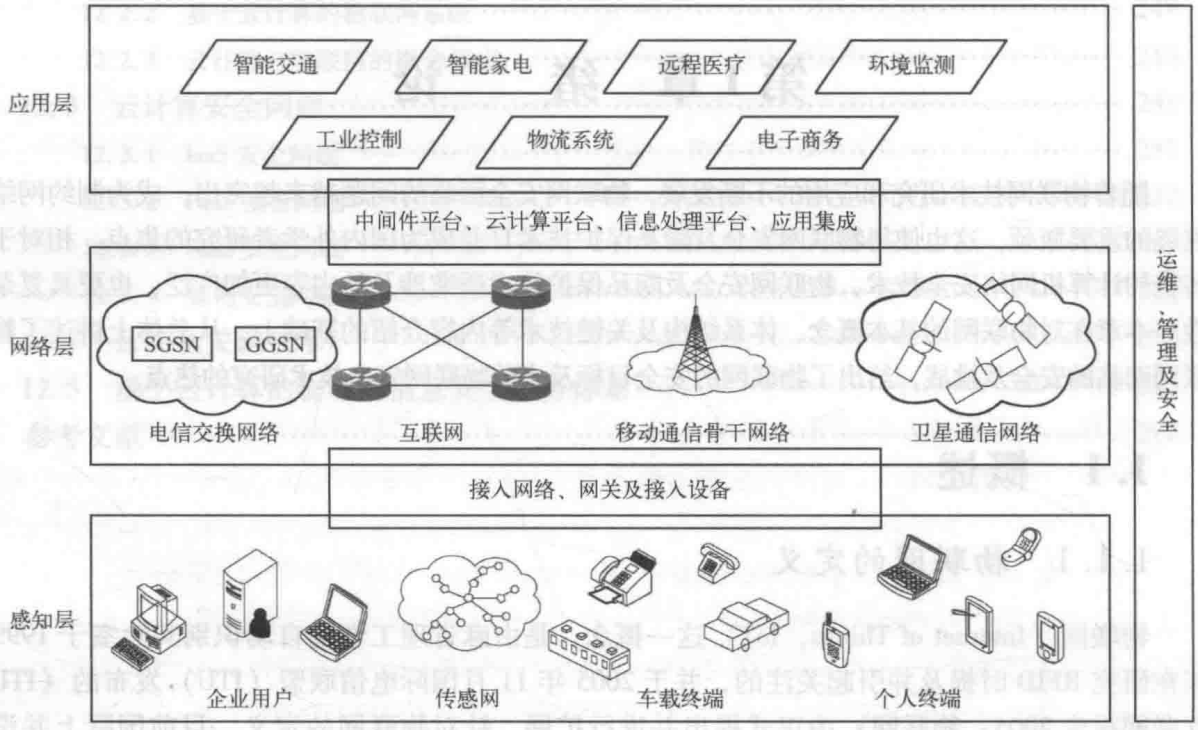

图 1-1　物联网体系结构

1. 感知层

物联网的感知层处于网络的边沿，分布最为广泛，如果将物联网比作人，则感知层就相当于人体的感知器官，主要用来完成信息的感知和采集。感知层设备多种多样，种类非常丰富，常见的有 RFID、传感器节点、红外感知设备、摄像头、智能手机、各种传感器设备，以及由这些设备组成的同构或异构的网络。根据网络应用的不同，采用的感知设备可能不同。例如智能农业系统，感知层设备主要由采集土壤温度、湿度、光照的传感器设备组成；而在物流系统中，感知层设备主要由 RFID 标签、阅读器组成；在智能交通系统中，感知层设备主要由测速仪器、GPS 定位终端、超声雷达等组成。感知层是物联网信息的来源和起点，直接与被监控的“物”相连。物联网就是通过各类传感器、RFID 及其他感知设备使得物体能够智能地表达自己，从而实现物与物之间的智能通信的。

2. 网络层

网络层是物联网的核心部分，属于网络的中枢神经系统，负责信息的传输和交互。物联网的网络层主要以互联网、移动通信网络、电信交换网络、卫星通信网络为主要组成部分，用于实现网络中各类终端设备的广泛互连，实现感知层数据的高效、可靠、安全传输，同时为各类感知层异构网络提供接入接口，实现网络层与感知层的紧密融合。电信网络、互联网技术成熟度较高，是物联网的网络层的骨干，也是物联网各类业务的主要支撑环境，但针对未来新型的物联网业务，如 RFID 标签位置查询等，现有的骨干网络结构仍需须进一步调整、优化。

感知层与网络层之间的互连互通主要通过接入网络来实现。接入网络主要有 WLAN、WiMAX、MESH 等多种网络形式，能够支持多种通信标准。感知层设备可以直接与接入网络相连，也可以通过网关与接入网络相连，接入网络再通过专用设备与骨干网络相通。

3. 应用层

物联网的应用层主要实现各类的应用服务，如智能交通、环境监测、物流管理、智能楼宇、电子支付等，不同的应用服务可能对应于网络层及感知层的不同功能。例如在智能交通应用中，用户可以通过移动通信网络或 WiMAX 网络等实时获取当前路况信息，共享娱乐资讯，利用短距离通信手段实现车与车之间的对话，同时还可以通过车内设置的各类传感器节点时刻获取车内发动机、油路、空调等系统的运行情况，并自动将车内异常情况远程上传到车辆服务中心获取技术支持。相对于互联网而言，物联网的应用类型和服务更为多样和丰富。因此物联网不仅仅是通信技术的革新，更是人类生活方式的变革。

近年来，为了进一步支撑物联网应用服务的发展，很多大公司还在网络层与应用层之间构建了专门的数据或信息处理平台，如云存储平台、云计算平台、数据分析平台等，这些平台的建立，有效降低了应用服务的成本，为应用服务的多样化提供了基础。

物联网体系结构除了以上三个层次外，还涉及一些公共技术，这些公共技术与三个层次都有关系，提供网络的管理、维护，数据的查询、挖掘，行为的分析、决策，安全的防护、检测等。

1.1.3 物联网的主要特点及应用领域

1. 物联网的主要特点

中国移动前董事长王建宙表示，物联网有三大特征：一是全面感知，即利用 RFID、传感器、二维码、GPS 等设备或标签随时随地获取物体的信息；二是可靠传递，通过电信网络、互联网的融合，将信息实时、准确地传输到目的地；三是智能处理，利用云计算、智能识别、人工智能等各种技术，对海量信息和数据进行分析、处理，实现对物体的智能化控制。

互联网是人与人之间的网络，而物联网是物与物、物与人之间的网络，因此除了全面感知、可靠传递和智能处理这三个重要特征外，相对互联网而言，物联网还有以下特点。

1）对象更广

除了人以外，相对互联网而言，物联网所涉及的对象更多，生产、生活中的物品，如服装、手表、汽车、车床、仪表等物品都可以接入网络，实现智能化通信。

2）范围更大

物联网包含互联网、移动通信网、卫星通信网等多种网络，其覆盖范围更加广泛，接入手段更加多样，终端可以静止也可以移动，终端设备可以在任何地点，通过多种接入方式实现网络的接入。

3）智能更高

通过使用大数据分析、云计算等基础平台，物联网用户可以随时随地分享平台成果，获

得强大的平台支撑，从而更为智能地处理复杂的事件。

4）能力更强

随着技术的发展，尤其是处理器技术的不断进步，物联网终端的成本不断降低、性能不断提升，能够完成的功能也日益多样。

2. 物联网的典型应用

物联网的应用前景非常广阔，遍及智能交通、路桥管理、灾害防治、卫生保健、儿童护理、环境监管、平安家居、敌情侦察、情报获取、工业控制等多个领域。物联网的出现使物品和服务都发生了质的变化，改变了人们的生活方式，为使用者提供了更高的效率。物联网最终将发展成为面向服务的网络，根据用户的需求来提供智能化的便捷服务。这一技术将会发展成为一个有着上万亿规模的高科技市场。目前典型的物联网应用如下。

1）智能环保

随着经济的发展，人们对生活质量和环境的要求越来越高。为了提高环境监测和管理水平，环保部门可以建设基于物联网的智能环保通信系统。通过建设形成一个覆盖全区的环境自动监测信息采集网络，实现对重点排污单位污染防治设施运行状态、主要污染物排放检测数据的自动传输和预警，实现重点流域水环境质量、重点城市环境空气质量自动监测数据实时传输。通过建设一个环境分析系统和一个交互式的环境监测、环境保护的动态信息发布平台向政府、公众发布环境信息，实现集环境监测的智能感知、智能处理和综合管理于一体，推进污染减排和环境保护，实现环境与人、经济乃至整个社会的协调发展，促进环境改善。

2）智能物流

RFID 技术是物联网的重要技术基础，是实现智能物流的重要手段。利用 RFID 技术，将物流中的物品贴上电子标签，利用标签阅读器便可以在物品运转的各个环境实现对物品的清点、查询和统计，节省了人力资源。同时利用电子标签，可以随时跟踪物品所处的位置、流通环节、出厂时间，也可以方便消费者对用户进行信息检索，获取商品的来源、生产日期、主要成分及其他相关信息。物联网技术能够大大增强物流中运输、保管、装卸、包装、流通加工等物流环境的功能，使物流与商流、资金流、信息流融为一体，提升生产、流通和消费的综合效益，促进物流成本的不断下降。如今，打开手机应用我们就可以知道购买的商品所处的物理阶段，随着技术的进一步发展，我们还有可能随时定位商品的位置。

3）智能交通

以往的城市交通管理基本上都是自发进行的，驾驶者根据自己的判断选择行车路线，交通提示牌、指示灯的作用非常有限。随着 GPS、RFID 等物联网技术的发展，互联网公司能够随时获得城市车辆的位置、速度等信息，从而智能地对交通情况进行分析并给出出行参考，未来这些信息与交通管理和调度机制进一步融合，就能够充分发挥道路基础设施的效能，最大化交通网络流量，并提高交通安全性，提升人们的出行体验，甚至可以降低污染排放，提升路途乐趣。

4）军事应用

美国著名军事预测学家詹姆斯·亚当斯在其所著的《下一场世界战争》中曾预言：“在

未来的战争中，计算机本身就是武器，前线无处不在。夺取作战空间控制权的不是子弹，而是计算机网络里流动的比特和字节。”物联网可以有效应用于战场情报获取、军事物资管理等领域。通过飞机抛洒传感器节点，可以实现无人区或敌占区目标信息的采集，可以感知目标区域人员、车辆的运动趋势，甚至判断出具体目标类型，为军事决策提供准确的情报来源。物联网可以应用于战争准备、战斗实施的每一个环境，能够在多种场合满足军事信息获取的实时性、准确性、全面性的需求。

1.1.4 物联网发展现状

1. 国外物联网发展现状

虽然很多资料都认为物联网的概念是1999年麻省理工RFID实验室Kevin Ashton教授提出的，但其实在此之前的1995年，微软创始人比尔·盖茨就已经在其《The Road Ahead》一书中提到物联网的概念，只不过受限于当时的技术条件并未引起大家的重视。随着技术的进步，2005年11月国际电信联盟在突尼斯举行的信息社会世界峰会上发布了《ITU互联网报告2005：物联网》，引用了“物联网”的概念，并对其进行了扩展，提出任何时刻、任何地点的任何物体之间都可以进行互连，无处不在的“物联网”通信时代即将来临，世界上的所有物体都可以通过互联网实现信息交换。传感器网络、射频识别、嵌入式、纳米技术将得到更加广泛的应用。

IBM公司2008年提出了“智慧地球”的概念，其本质是以一种更智慧的方法，利用新一代的信息通信技术来改变政府、公司和人们相互交换的方式，以提高交换的明确性、灵活性和效率。“智慧地球”在技术层面上是物联网与互联网的融合，从而使人类能够以更加精细和动态的方式管理生产和生活，形成“物联网+互联网=智慧的地球”。“智慧地球”体现了智能城市、智能家居、智能货运、智能交通、智能医疗等多个方面。这一概念得到奥巴马政府的积极响应，物联网已经上升到美国国家发展战略层面，并引起全世界的广泛关注。

2009年2月，奥巴马签署生效的《2009年美国恢复和再投资法案》（即美国的经济刺激计划）提出要在智能电网领域应用物联网，例如得克萨斯州的电网公司建立了智能的数字电网。

2009年7月，日本IT战略本部颁布了日本新一代的信息化战略——i-Japan，让数字技术融入社会的每一个角落；并且提出到2015年使行政流程简单化、效率化、标准化、透明化，并推动远程医疗和远程教育的发展。

2009年9月，欧盟第7框架下的RFID和物联网研究项目组发布了《物联网战略研究路线图》研究报告，认为物联网是未来Internet的一个组成部分，是一种动态的全球网络基础架构，它基于标准的、可互操作的通信协议，具有自我配置能力。物联网中的“物”都具有标识，拥有物理属性，使用智能接口，能够实现与信息网络的无缝结合。

2009年10月，韩国通过了物联网基础设施构建规划，将物联网市场确定为新的经济增长动力。

2013年4月的汉诺威工业博览会上，德国政府提出“工业4.0”战略，其目的是为了提高德国工业的竞争力，在新一轮工业革命中占领先机。该战略已经得到德国科研机构和产业

界的广泛认同，西门子公司已经开始将这一概念引入其工业软件开发和生产控制系统。

2. 国内物联网发展现状

我国对“物联网”的发展给予了高度重视。目前，我国对物联网的研发聚焦在传感网。《国家中长期科学与技术发展规划（2006—2020年）》和“新一代宽带移动无线通信网”重大专项中均将“传感网”列入重点研究领域。经过长期艰苦努力，我国相关机构和企业攻克了大量关键技术，取得了国际标准制定的重要话语权，具备了一定的发展传感网的产业基础，在电力、交通、安防等相关领域的应用也初见成效。

目前我国传感网标准体系已形成初步框架，向国际标准化组织提交的多项标准提案被采纳，传感网标准化工作已经取得积极进展。总的来说，我国在物联网研发上的主要动向如下。

- 江苏省政府与中国移动共同推进TD和传感网基地建设。
- 2009年9月，中国传感网标准工作组成立。
- 2009年9月，举办“感知中国”高峰论坛，探讨如何打造中国传感网产业。
- 2009年9月，无锡市与北京邮电大学就传感网技术签署合作协议，合作建设传感网技术研究院。
- 2009年11月，国家批准无锡建立“国家传感网创新示范区”，使无锡成为中国物联网研究中心。同年，中关村物联网产业联盟成立，成员包括中国移动、清华同方股份有限公司、北京邮电大学、中科院软件所、北京交通委信息中心等十二家单位，囊括了政府、院校和企业。
- 2015年5月，经李克强总理签批，国务院印发了《中国制造2025》，部署全面推进实施制造强国战略，目标是实现长期制约制造业发展的关键共性技术突破，提升我国制造业的整体竞争力。这是我国实施制造强国战略第一个十年的行动纲领。

物联网的市场前景广阔，效益巨大，据预测，到2020年，物物互联业务将达到人人通信业务的30倍，物联网已成为当前各国科技和产业竞争的焦点。

1.1.5　物联网关键技术

1. 感知层关键技术

物联网对事物的感知是以各种信息采集技术为基础的，这些技术主要有RFID、无线传感器网络、二维码、ZigBee、蓝牙、GPS定位等。其中感知层最具代表性的就是RFID和无线传感器网络技术。

1）RFID技术

RFID是英文Radio Frequency Identification的缩写，即射频识别，也称电子标签。它通过无线射频识别不同的目标，利用无线传输技术来存储和检索数据。RFID是一种非接触式的自动识别技术，不需要识别系统与目标有物理、机械或光学的接触，识别工作也无须人为干预，可以工作在较为恶劣的环境中。目前，RFID已经广泛应用于工业自动化、办公自动化、物流、交通管理等多个领域。

RFID的主要核心部件是阅读器和电子标签。RFID技术通过相距几厘米到几米甚至几十米距离的阅读器发射的无线电波来读取电子标签内部存储的信息，识别标签所代表的物品信息、状态信息等。一个典型的射频识别系统一般由电子标签、阅读器和计算机系统三部分组成，如图1-2所示。

图1-2 RFID系统组成

① 电子标签：由耦合元件及芯片组成，每个标签具有唯一的电子编码，附着在需要标识的物体上以识别目标对象，主要由具有模拟、数字记忆功能的芯片，以及依不同频率、应用环境而设计的天线所组成。标签分为无源标签（被动标签）和有源标签（主动标签）两种，无源标签由阅读器的电磁波提供能量，而有源标签自身有电池供电。

② 阅读器：RFID阅读器通过天线与电子标签进行无线通信，它主要由射频收发单元、模/数转换模块、中央处理单元及天线组成。天线在标签和阅读器间收发信号，中央处理单元用于完成信息的转换和处理。阅读器主要实现标签信息的读取和写入功能。

③ 计算机系统：计算机系统用作后台控制系统，通过有线或无线的通信方式与阅读器相连接，利用阅读器获取标签内部的信息，对读取的数据进行筛选、处理和后台控制，同时也可以根据阅读器的需要查询自身存储的信息，完成标签的认证、信息写入功能。

2）无线传感器网络技术

无线传感器网络（Wireless Sensor Networks，WSNs）是随着微电子机械系统（Micro-Electro-Mechanism System，MEMS）、计算机、通信、自动控制和人工智能等学科的飞速发展而产生的一种新型的测控网络。它是由部署在目标监测区域内大量的价格低廉的微型传感器节点组成，利用无线通信方式形成的一个多跳的自组织的网络系统，其主要目的是感知、采集和处理网络覆盖区域中被感知目标的信息，并发送给观察者或用户。感知目标、传感器节点和观察者是无线传感器网络的三要素。无线传感器网络以一种“无处不在”的计算理念，成为连接物理世界、信息世界和人类社会的桥梁，被广泛应用于环境监控、工业控制、智能家居、国防和公共安全等多个领域。

无线传感器网络通常包括传感器节点（Sensor Node）和汇聚节点（Sink Node，也称基站）。节点可以通过人工布置、飞机抛撒或弹射等方式大量地部署在监测区域内，通过自组织的方式构成无线通信网络，彼此相互协作，感知、采集被监测目标的信息，并通过多跳转发的方法将感知信息经由汇聚节点或基站发送给用户或远程管理中心。同时，用户或远程管理中心也可以对网络内部的节点进行监测和控制。图1-3给出了一个典型的无线传感器网络体系结构，其中包括分布式的传感器节点、汇聚节点和管理中心。其中传感器节点在网络中主要负责信息的采集、转发；汇聚节点收集传感器节点采集的信息，并将信息进行协议转换后通过卫星、互联网等其他通信系统发送给管理中心；用户通过管理中心获取所需要的信