普通高等教育
物联网工程类规划教材

INTERNET OF THINGS, IOT

物联网安全技术

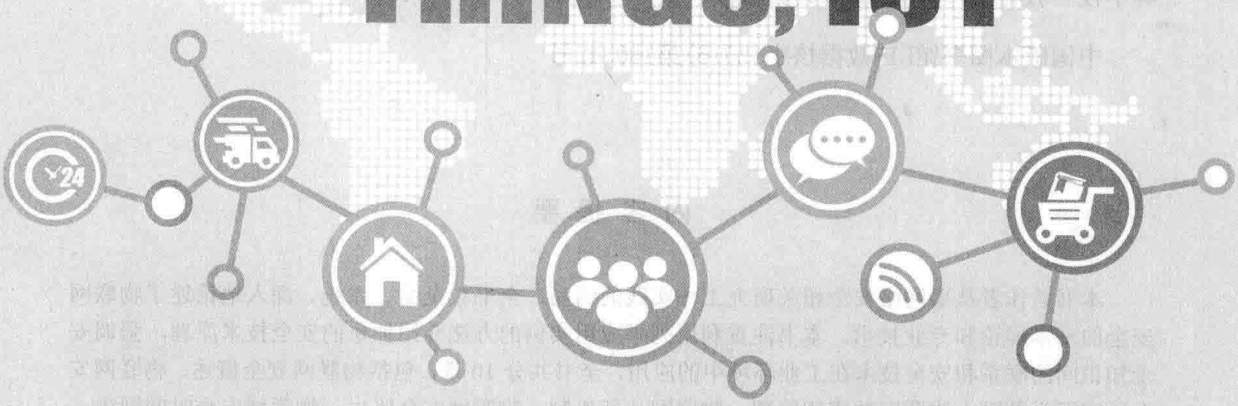
IoT Security Technology

王浩 郑武 谢昊飞 王平◎编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

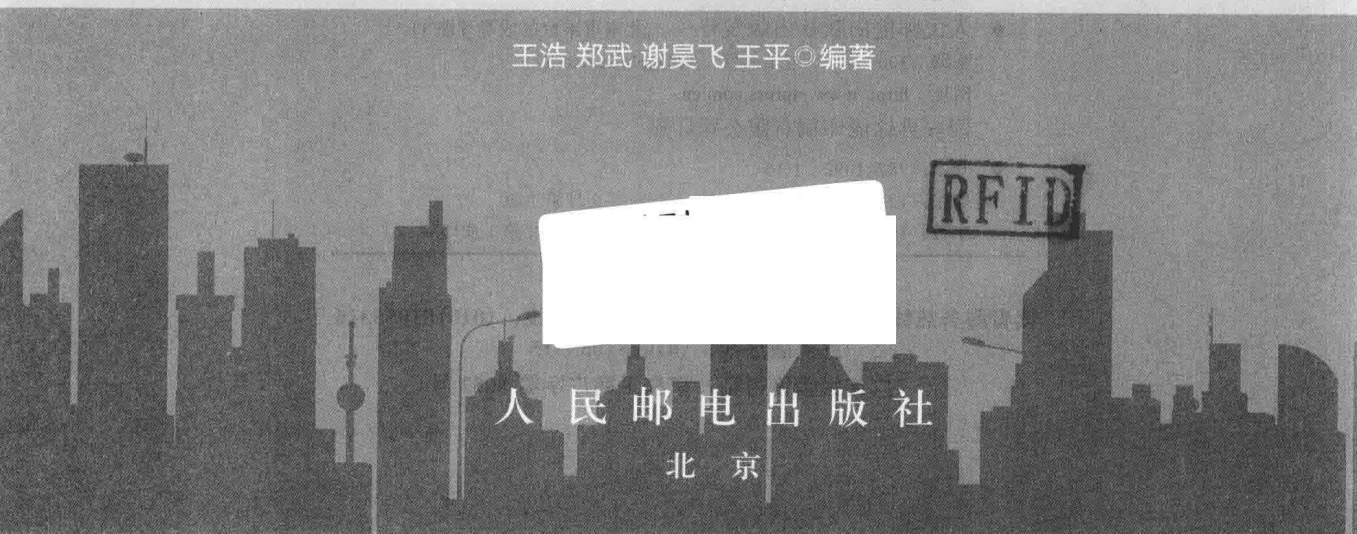
普通高等教育
物联网工程类规划教材

INTERN
THINGS, IOT



物联网
安全技术

王浩 郑武 谢昊飞 王平◎编著



人民邮电出版社
北京

图书在版编目（CIP）数据

物联网安全技术 / 王浩等编著. -- 北京 : 人民邮电出版社, 2016.9
普通高等教育物联网工程类规划教材
ISBN 978-7-115-43293-3

Ⅰ. ①物… Ⅱ. ①王… Ⅲ. ①互联网络－应用－安全技术－高等学校－教材②智能技术－应用－安全技术－高等学校－教材 Ⅳ. ①TP393.4②TP18

中国版本图书馆CIP数据核字(2016)第180342号

内 容 提 要

本书是作者从事网络安全相关研究工作实践的结晶，全书较全面、系统、深入地论述了物联网安全的基本理论和专业技术。本书注重利用列举应用实例的方法介绍抽象的安全技术原理，强调安全知识间的联系和安全技术在工业环境中的应用，全书共分 10 章，包括物联网安全概述、物联网安全的密码学基础、物联网的密钥管理、物联网认证机制、物联网安全路由、物联网安全时间同步、物联网访问控制、物联网安全数据融合、物联网的入侵检测、物联网安全系统实现。

本书可作为高等院校物联网工程、信息安全、测控技术与仪器、自动化、通信工程、计算机应用等专业的教材，也可供相关技术人员参考。

◆ 编　著　王　浩　郑　武　谢昊飞　王　平
责任编辑　税梦玲
责任印制　沈　蓉　彭志环
◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：12.5　2016 年 9 月第 1 版
字数：309 千字　2016 年 9 月河北第 1 次印刷

定价：36.00 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

前言

信息技术的高速发展与广泛应用，引发了一场全球性的产业革命，推动着各国经济的发展与人类社会的进步。信息化是当今世界经济和社会发展的大趋势，信息化水平已成为衡量一个国家综合国力与现代化水平的重要标志。随着“工业化与信息化融合”“智慧地球”“传感器中国”等理念的提出，物联网作为战略性新兴信息产业的重要领域，掀起了第三次信息技术浪潮。

物联网是一个多学科交叉的综合应用领域，物体通过 RFID、传感器等信息感知设备与网络连接起来，进行信息交换和通信，实现智能化识别、定位、跟踪、监控和管理。尽管不同的人们基于各自不同的背景对物联网有不同的理解和体会，但是有一点是共同期待和坚持的，即“有了安全才有应用，有了应用才能够发展”。在不断发展的物联网技术快速地改变人类生活、生产方式的同时，越来越多的物联网安全问题暴露出来，解决物联网的安全问题势在必行。

编写本书的主要目的是为了满足当前高等院校的物联网相关专业的教学要求，本书在内容上详细阐述了物联网中的各项安全机制，通过合理的案例材料和表现形式，一方面为教师教学提供丰富的教学材料；另一方面也为学生提供直观的、易理解的教材内容。

由于物联网安全本身涉及的内容极其广泛，本书精心挑选了其中的关键问题、特色问题、重点问题进行讨论，给出相关的安全技术、方法和应用实例，并介绍了基于多种安全技术开发的物联网安全平台。

作者在写作的过程中特别遵循了以下新的思路。

（1）内容编排先总体再局部、兼顾广度和深度。首先给出物联网的体系结构和安全框架，物联网安全问题的共性和一般的解决思路；然后根据物联网中的关键安全技术，分章节依次探讨特定的安全机制；最后介绍物联网安全开发平台的实现方法，使读者充分地将安全理论和实际应用相结合，完成物联网安全技术的学习。

（2）选材新颖、理论联系实际。选材尽量突出基本的研究问题以及新的进展，理论的论述突出共性和一般原理（如密钥管理、认证机制、安全路由机制、安全时间同步、安全访问控制机制、安全数据融合和入侵检测机制），实践部分强调工程性。

（3）注重创新能力的培养，包括对一般原理的总结和归纳、协议设计方法的比较和分析，注重对问题本质的提炼。

（4）注重对国内自主知识产权和自主创新的介绍，包括传感器网络安全体系架构（参

考国家标准《传感器网络 信息安全 通用技术规范》)、安全访问控制机制(部分安全访问控制机制参考国家标准《传感器网络 信息安全 通用技术规范》)、安全数据融合机制等。由于信息安全的行业特殊性和我国综合国力的提升,介绍这部分相关成果有利于激发读者和相关技术人员对我国自主创新成果的关注,提升我国自主知识产权成果的影响,促进我国自主知识产权成果的推广和应用。

(5)注重对实践能力的培养和对行业动态的关注。书中给出了多个密码算法(例如AES、RSA),以及多个基于密码算法的安全机制(基于ECC公钥算法的强用户认证协议、基于Hash算法的双向认证协议等),读者可深入学习后用于实践。

各章主要内容介绍如下。

章 序	章 名	主 要 内 容
1	物联网安全概述	详细介绍物联网的发展过程,以及物联网面临的安全问题
2	物联网安全的密码学基础	通过介绍相关密钥学知识,为后期学习安全技术方案奠定理论基础
3	物联网的密钥管理	密钥管理作为网络安全的重中之重,重点分析几种典型的密钥管理方案,并给出方案的优缺点,使读者深刻理解方案可行性
4	物联网认证机制	认证是物联网安全技术的第一道防线,也是物联网安全最为重要、最为基本的关键安全技术
5	物联网安全路由	通过分析物联网路由协议,指出其面临的安全威胁,介绍几种典型的安全路由协议,帮助读者深刻理解安全路由协议的基本过程
6	物联网安全时间同步	时间同步是节点与节点之间通信的关键技术,保证时间同步的安全是保障物联网设备正常通信的基础
7	物联网访问控制	目前安全访问控制技术在物联网中没有得到应有的重视,本章重点介绍国家标准《传感器网络 信息安全 通用技术规范》中提出的访问控制技术,以及通过介绍物联网访问控制方案设计例子,使读者能够充分了解安全访问控制技术的研究现状
8	物联网安全数据融合	重点分析物联网数据融合的安全问题,并针对这些问题介绍几种安全数据融合方案
9	物联网的入侵检测	重点介绍典型的入侵检测模型和算法
10	物联网安全系统实现	通过介绍电力传感器网络安全试验平台设计流程,以及该平台中所用的各种安全机制,使读者能够将理论与实践相结合,全方面地学习物联网安全技术

本书由重庆邮电大学王浩教授组织编写,第1、3、4、9、10章由王浩和陈伟编写,第2、5章由郑武和陈豪编写,第6、7、8章由谢昊飞和李勇编写,王平教授负责本书的审阅。特别感谢网络化控制重点实验室安全项目组的研究生张晓、方闻娟、王朝美等同学,以及参考文献中所列各位作者,他们在各自领域的独到见解和特别的贡献为作者提供了宝贵的参考资料,使作者得以汲取各家之长,形成本书。

作者

2016年5月

目 录

第 1 章 物联网安全概述

随着物联网概念的提出，各国政府、企业和科研机构纷纷加入物联网的研究和建设工作。物联网是新一代信息技术的高度集成和综合运用，其建设与发展必然受到物联网安全和隐私问题的制约。本章节主要讲述当前物联网的起源、安全模型，以及面临的安全威胁和攻击等。

1.1 物联网概述

1.1.1 物联网的起源与定义

1999 年美国麻省理工学院自动识别中心（Auto-ID），提出“万物皆可通过网络互联”，阐明了物联网（Internet of Things，IoT）的基本含义。同年，在美国召开的移动计算机和网络国际会议提出：“传感网是下一个世纪人类面临的又一个发展机遇”。2005 年 11 月 17 日，在突尼斯举行的信息社会世界峰会（World Summit on the Information Society，WSIS）上，国际电信联盟（International Telecommunication Union，ITU）发布《ITU 互联网报告 2005：物联网》，引用了“物联网”的概念。如今，物联网的定义和范围已经发生了变化，覆盖范围有了较大的拓展，不仅是指基于 RFID 技术的物联网，还包括应用二维码、传感器等技术的物联网。

目前，对于物联网的定义争议很大，还没有一个被各界广泛接受的定义，各个国家和地区对于物联网都有自己的定义。以下是一些国家或者地区的定义。

（1）美国的定义：通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器、气体感应器等信息设备，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。

（2）欧盟的定义：将现有互联的计算机网络扩展到互联的物品网络。

（3）国际电信联盟的定义：任何时间（anytime）、任何地点（anywhere），我们都能与任何东西（anything）相连。

（4）2010 年温家宝总理在十一届全国人民代表大会第三次会议上对物联网的定义：物联网是指通过信息传感设备，按照约定的协议，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、跟踪、定位、监控和管理。它是在互联网的基础上延伸和扩展的网络。

结合各国家和各地区对物联网的定义，现对物联网概念做出如下总结。

物联网就是“物品的互联网”，它以“智能化”为核心，让没有生命、为人服务的物品能够“开口说话”，通过网络实现互联互通，允许人和物在任何时间（anytime）、任何地点（anywhere），使用任何网络（any network）、任何服务（any service）与任何的事物（anything）、任何人（anyone）无缝地联系（见图 1.1），从而加强人与物、物与物等信息交流，实现更高的工作效率，节省操作成本，体现“服务的智能化”和“科技惠及民生”的本质[1]。

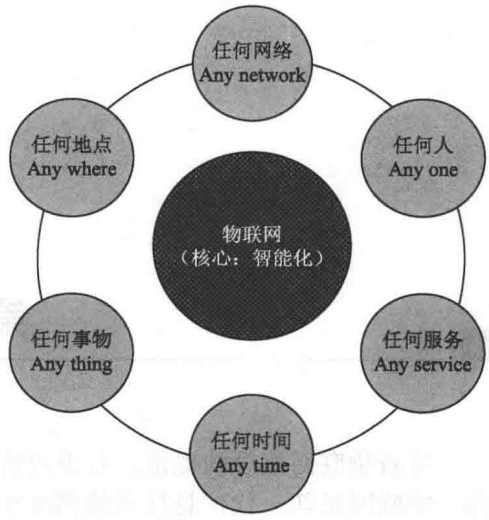


图 1.1 物联网的基本内涵

物联网的定义可以从技术和应用两个角度进行理解。

（1）技术角度：物联网是把物体的信息利用感应装置，经过传输网络，传送到指定的信息处理中心，最终实现物与物、人与物之间的自动化信息交互、处理的智能网络。

（2）应用角度：物联网是把世界上所有的物体都连接到一个网络中，形成“物联网”，然后又与现有的互联网结合，实现人类社会与物体系统的整合，从而以更加精细和动态的方式去管理生产和生活。

1.1.2 物联网的体系架构

物联网的价值在于让物体也拥有了“智慧”，从而实现人与物、物与物之间的沟通。物联网的特征在于感知、互联和智能的叠加。因此，物联网可由 3 个部分组成：感知层，即以二维码、RFID、传感器为主，实现对“物”的识别；网络层，即通过现有的互联网、广电网络、通信网络等实现数据的传输；应用层，即利用云计算、数据挖掘、中间件等技术实现对物品的自动控制与智能管理等。图 1.2 所示为物联网体系架构图。

在物联网体系架构中，三层的关系可以这样理解：感知层相当于人体的皮肤和五官；网络层相当于人体的神经中枢和大脑；应用层相当于人的社会分工。其具体描述如下。

（1）感知层

感知层是物联网的皮肤和五官，包括二维码标签、识读器、RFID 标签、读写器、摄像头和 GPS 等，其主要作用是识别物体，采集信息，与人体结构中皮肤和五官的作用相似。

（2）网络层

网络层是物联网的神经中枢和大脑，主要作用是信息的传递和处理，包括通信与互联网的融合网络、网络管理中心和信息处理中心等。

（3）应用层

应用层是物联网与行业专业技术的深度融合，与行业需求相结合，实现行业智能化，这类似于人的社会分工。

在各层之间，信息不是单向传递的，也有交互、控制等，所传递的信息多种多样，物品的信息是其中的关键，包括在特定应用系统范围内能唯一标识物品的识别码和物品的静态与动态信息。

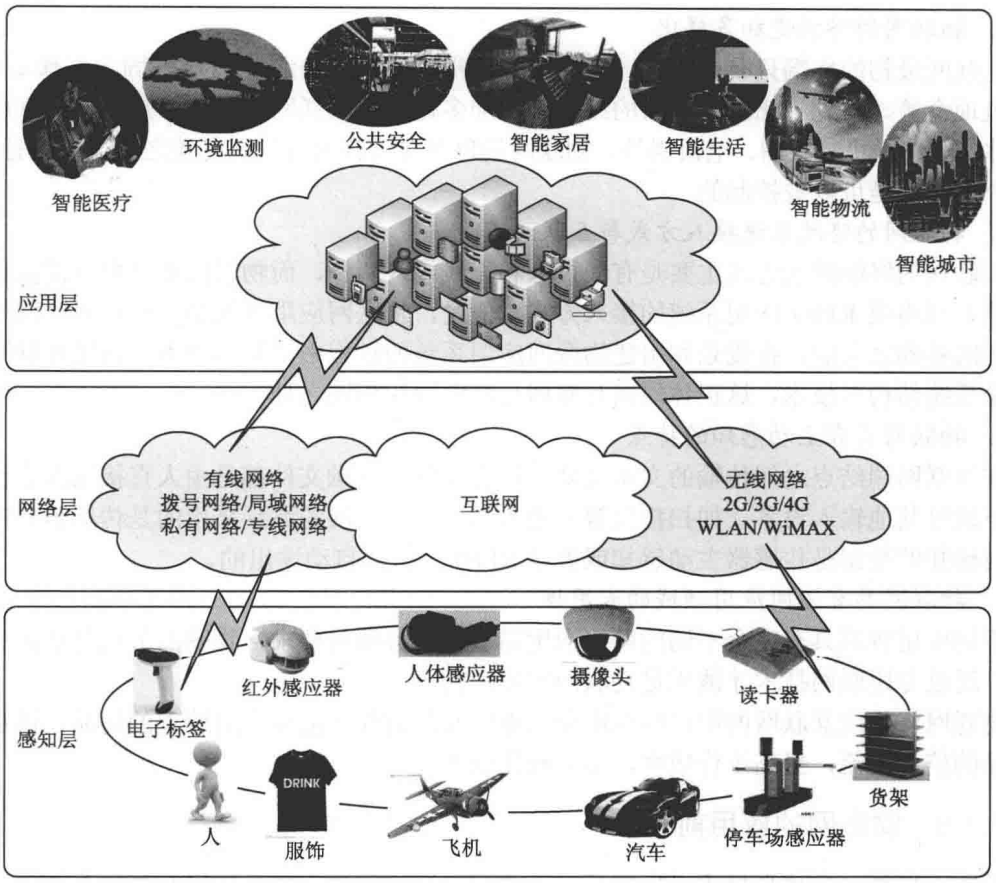


图 1.2 物联网体系架构图

1.1.3 物联网的主要特点

从物联网产生的背景及物联网的定义中，可以大致总结出物联网的 3 个特征。

（1）全面感知：利用 RFID、二维码、传感器等感知、捕获、测量技术随时随地对物体进行信息采集和获取。

（2）可靠传输：通过将物体接入信息网络，依托各种信息网络，随时随地进行可靠的信息交互和共享。

（3）智能处理：利用云计算、数据挖掘、人工智能及模糊识别等技术，对海量的数据和信息进行分析和处理，对物体实施智能化监测和控制。

1.1.4 物联网与互联网的关系

物联网和互联网的共同点是：技术基础是相同的，即它们都是建立在分组数据技术的基础之上的，它们都采用数据分组网作为它们的承载网；承载网和业务网是相分离的，业务网可以独立于承载网进行设计和独立发展，互联网是如此，物联网同样。

物联网与互联网的区别：可以从终端、接入方式、数据采集与传输、应用领域 4 方面将互联网与物联网进行比较。

1. 物联网的终端更加多样化

互联网最初的终端只有计算机，现在除计算机外还有手持终端 PDA、固定与移动电话、电视机顶盒等。与此相比，物联网的终端则更加多样化，物联网终端可以是我们的家用电器如电冰箱、洗衣机、空调、电饭锅等，物联网的每个终端都可寻址，终端之间可以进行通信，且每个终端都是可以被控制的。

2. 物联网的终端系统接入方式与互联网不同

互联网的终端接入方式主要是有线接入和无线接入两种，而物联网则是根据需要选择无线传感器网络或 RFID 应用系统的接入方式。但是，物联网应用系统是运行在互联网核心交换结构的基础之上的，在规划和组建物联网应用系统的过程中，基本上不会改变互联网的网络传输系统结构与技术，这正体现出互联网与物联网的相同之处。

3. 物联网具有主动感知的特点

在互联网端结点之间传输的文本文件、语音文件、视频文件都是由人直接输入或在人的控制下通过其他输入设备（如扫描仪等）输入的。而物联网的终端采用的是传感器、RFID，物联网感知的数据是传感器主动感知或者是 RFID 读写器自动读出的。

4. 物联网具有不同应用领域的专用性

不同应用领域具有完全不同的网络应用需求和服务质量要求，物联网节点是资源受限的节点，通过专用联网技术才能满足物联网的应用需求。

物联网将传统互联网的用户终端由个人电脑延伸到任何需要实时管理的物品，以加强人与物品的信息交流，提高工作效率，节省操作成本。

1.1.5 物联网的应用前景

物联网把新一代信息技术（Information Technology，IT）充分运用在各行各业之中，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，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理。其用途广泛，遍及智能交通、智能物流、智能电网、智能环境监测与保护、公共安全、智能家居、智能消防、工业监测、智能护理与保健等多个领域。

1. 物联网对经济的影响

物联网技术与社会连接在一起的结构将产生一种新的技术经济结构，对社会、经济活动产业产生巨大的影响。因此、将形成新的经济形态，表现出巨大的市场前景。

物联网是生产社会化、智能发展的必然产物，是现代信息网络技术与传统商品市场有机结合的一种创造。这种创造不仅可以极大地促进社会生产力发展，而且能够改变社会生活方式。我们可以充分利用物联网这一手段进行产业创新和提高商品竞争力，大大提高效率。同时，可以远程控制商品，随时随地查看和控制商品，可使得物流变得简单无比，等等。简而言之，未来的经济会因为物联网的出现而大大改变。

2. 物联网对信息产业发展的影响

如果把计算机的出现使信息处理获得了质的飞跃，视作信息技术第一次产业化浪潮；把互联网和移动网的发展使信息传输获得了巨大提升，视作第二次产业化浪潮。那么，以物联网为代表的信息获取技术的突破，将掀起第三次产业化浪潮。

物联网实现了由人操控的物与物的联系，相当于把现实世界和虚拟世界用信息联系了起来。这种新的概念的提出，必定会让人有新的想法和新的对事物的看法，这也会促使信息产

业的创新，加快社会信息化的进程。

3. 物联网对安防的影响

北京奥运会期间，物联网在视频联网监控、智能交通指挥、食品安全追溯、环境动态监测等方面获得了非常大的用武之地。上海世博会期间，约34万人在世博园就餐，保证食品安全成为了首要目标。利用物联网，在现场就可快速追溯食品和原料的来源，确保供应渠道的安全可靠。世博会的火警警报装置也利用了物联网，消除了世博会期间的火险。汶川地震事件信息通过传感网被传递到后方的决策部门，有效规避了人员实地观测可能遭遇的伤亡风险。这一切都说明了物联网的有效应用可以保证人的安全，使危险在未发生的时候就被消除。

4. 物联网对军事的影响

实际上，任何新的技术，都会优先应用于军事领域，物联网技术也不例外。美国陆军已经开始建设“战场环境侦察与监视系统”，通过“数字化路标”作为传输工具，为各作战平台与单位提供“各取所需”的情报服务，使情报侦察与获取能力产生质的飞跃。

未来的信息化战争要求整个作战系统“看得明、反应快、打得准”。毫无疑问，谁能在信息的获取、传输、处理上占据优势，谁就能掌握战争的主动权。物联网技术的发展为实现智能化、网络化的未来信息化战争提供了技术支撑。

可以设想，从卫星、导弹、飞机、舰船、坦克、火炮等单个装备到海、陆、空各个战场空间；从单个士兵到大规模作战集团，通过物联网可以把各个作战要素和作战单元甚至整个国家军事力量都铰链起来，实现战场感知精确化、武器装备智能化、后勤保障灵敏化，这必将会引发一场划时代的军事技术革命和作战方式的变革。

5. 物联网对个人生活的影响

物联网对个人生活的影响现阶段主要体现在智能卡和手机的扩充功能上。智能卡的功能又主要表现在电子交付和身份识别两个方面。商场超市购物、医院看病、乘坐各种交通工具、旅馆住宿、饭店吃饭、各种费用缴纳等消费行为都能通过刷卡解决。此外，门禁卡、图书借阅卡等还具有身份识别的功能。手机不仅是通信工具，而且正在发展成为人们不能离开的工作、学习、娱乐、通信的信息中心。人们的一切工作、学习、娱乐等将有可能全部在手机上完成。如果需要大屏幕显示，办公室、家里及公共场合都有无线键盘和显示器、打印机等外部设备；如果去野外，有无线可折叠键盘、显示器等便携式外部设备，手机的定位技术将随时随地传递手机持有者的精确位置。除此，家中的冰箱不再只是保存食物，还可以是个好“管家”，食物不足了，它会提醒；食物过期了，它会提醒；甚至它还可以在网上帮主人收集菜谱。像这样的智能冰箱、智能洗衣机、智能电视机都将是物联网生活的一部分。

1.2 物联网安全模型与安全特性

1.2.1 物联网安全模型

物联网相比于传统网络，其感知节点大多部署在无人监控的环境，具有能力脆弱、资源受限等特点，并且由于物联网是在现有传输网络基础上扩展了感知网络和智能处理平台，传统网络安全措施不足以提供可靠的安全保障，从而使得物联网的安全问题具有特殊性。图1.3所示为物联网安全模型。

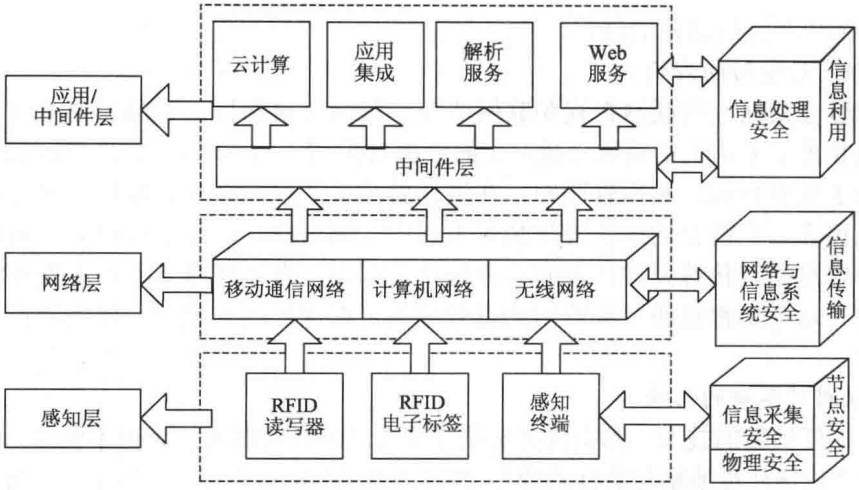


图 1.3 物联网安全模型

物联网主要由传感器、传输系统（泛在网），以及处理系统 3 个要素构成。因此，物联网的安全形态也体现在这 3 个要素上。

（1）物理安全：即传感器的安全（包括对传感器的干扰、屏蔽、信号截获等），是物联网安全特殊性的体现。

（2）运行安全：存在于各个要素中，涉及到传感器、传输系统及处理系统的正常运行，与传统信息系统安全基本相同。

（3）数据安全：存在于各个要素中，要求在传感器、传输系统、处理系统中的信息不会被窃取、被篡改、被伪造、被抵赖等。

传感器与传感网所面临的安全问题比传统的信息安全更为复杂，因为传感器与传感网可能会因为能量受限的问题而不能运行过于复杂的安全保护体系。因此，物联网除面临一般信息网络所具有的安全问题外，还面临物联网特有的威胁和攻击。

1.2.2 物联网安全特性

物联网安全特性包括物联网安全问题和物联网安全需求两个方面。从物联网的信息处理过程来看，感知信息经过采集、汇聚、融合、传输、决策与控制等过程，整个信息处理的过程体现了物联网安全的特征与要求，也揭示了所面临的安全问题。

1. 感知网络的信息采集、传输与信息安全问题

感知节点呈现多源异构性，感知节点通常情况下功能简单（如自动温度计）、携带能量少（使用电池），使得它们无法拥有复杂的安全保护能力，而感知网络多种多样，从温度测量到水文监控，从道路导航到自动控制，它们的数据传输和消息也没有特定的标准，所以无法提供统一的安全保护体系。

2. 核心网络的传输与信息安全问题

核心网络具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。此外，现有通信网络的安全架构都是从与人通信的角度设计的，对以物为主体的物联网，要建立适合于感知信息传输与应用的安全架构。

3. 物联网业务的安全问题

支撑物联网业务的平台有着不同的安全策略，如云计算、分布式系统、海量信息处理等，这些支撑平台要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统，而大规模、多平台、多业务类型使物联网业务层次的安全面临新的挑战，是针对不同的行业应用建立相应的安全策略，还是建立一个相对独立的安全架构。

另外可以从信息的机密性、完整性和可用性来分析物联网的安全需求。

1. 机密性

信息隐私是物联网信息机密性的直接体现，如感知终端的位置信息是物联网的重要信息资源之一，也是需要保护的敏感信息。另外在数据处理过程中同样存在隐私保护问题，如基于数据挖掘的行为分析等等，要建立访问控制机制，控制物联网中信息采集、传递和查询等操作，不会由于个人隐私或机构秘密的泄露而造成对个人或机构的伤害。信息的加密是实现机密性的重要手段，由于物联网的多源异构性，使密钥管理显得更为困难，特别是对感知网络的密钥管理是制约物联网信息机密性的瓶颈。

2. 完整性和可用性

物联网的信息完整性和可用性贯穿物联网数据流的全过程，网络入侵、拒绝攻击服务、Sybil 攻击、路由攻击等都使信息的完整性和可用性受到破坏。同时物联网的感知互动过程也要求网络具有高度的稳定性和可靠性，物联网与许多应用领域的物理设备相关联，要保证网络的稳定可靠，如在仓储物流应用领域，物联网必须是稳定的，要保证网络的连通性，不能出现互联网中数据包时常丢失等问题，不然无法准确检测进库和出库的物品。

因此，物联网的安全特征体现了感知信息的多样性、网络环境的多样性和应用需求的多样性。同时网络的规模和数据的处理量大，决策控制复杂，给安全研究提出了新的挑战。

1.3 物联网面临的典型威胁和攻击

1.3.1 物联网面临的威胁

物联网除了面对传统网络安全问题之外，还存在着大量自身特殊的安全问题，而这些问题大多来自感知层。具体来说，物联网感知层面临的主要威胁有以下 5 个方面。

（1）物理俘获：由于物联网应用可以取代人来完成一些复杂、危险和机械的工作，物联网感知节点或设备多数部署在无人监控的场景中，并且有可能是动态的。这种情况下攻击者就可以轻易地接触到这些设备，使用一些外部手段非法俘获感知点，从而对他们造成破坏，甚至可以通过本地操作更换机器的软件和硬件。

（2）传输威胁：首先物联网感知节点和设备大量部署在开放环境中，其节点和设备能量、处理能力和通信范围有限，无法进行高强度的加密运算，导致缺乏复杂的安全保护能力；其次物联网感知网络多种多样，如温度测量、水文监控、道路导航、自动控制等，它们的数据传输和消息没有特定的标准，因此无法提供统一的安全保护体系，严重影响了感知信息的采集、传输和信息安全，这些会导致物联网面临中断、窃听、拦截、篡改、伪造等威胁，例如可以通过感知节点窃听和流量分析获取感知节点上的信息。

（3）自私性威胁：物联网感知节点表现出自私行为，为节省自身能量拒绝提供转发数据包的服务，造成网络性能大幅下降。

（4）拒绝服务威胁：由于硬件失败、软件瑕疵、资源耗尽、环境条件恶劣等原因造成网络的可用性被破坏，网络或系统执行某一期望功能的能力被降低。

（5）感知数据威胁：由于物联网感知网络与感知节点的复杂性和多样性，感知数据具有海量、复杂的特点，因而感知数据存在实时性、可用性和可控性的威胁。

1.3.2 物联网面临的攻击

结合物联网感知节点的部署特点，感知节点可能面临以下攻击。

（1）阻塞干扰：攻击者在获取目标网络通信频率的中心频率后，通过在这个频点附近发射无线电波进行干扰，使得攻击节点通信半径内的所有物联网感知节点不能正常工作，甚至使网络瘫痪，是一种典型的 DoS 攻击方法。

（2）碰撞攻击：攻击者连续发送数据包，在传输过程中和正常的物联网感知节点发送的数据包发生冲突，导致正常节点发送的整个数据包因为校验和不匹配被丢弃，是一种有效的 DoS 攻击方法。

（3）耗尽攻击：利用协议漏洞，通过持续通信的方式使节点能量耗尽，如利用链路层的错包重传机制使物联网感知节点不断重复发送上一包数据，最终耗尽节点资源。

（4）非公平攻击：攻击者不断地发送高优先级的数据包从而占据信道，导致其他感知节点在通信过程中处于劣势。

（5）选择转发攻击：物联网是多跳传输，每一个感知节点既是终节点又是路由中继点。这要求感知节点在收到报文时要无条件转发（该节点为报文的目的地时除外）。攻击者利用这一特点拒绝转发特定的消息并将其丢弃，使这些数据包无法传播，采用这种攻击方式，只丢弃一部分应转发的报文，从而迷惑邻居感知节点，达到攻击目的。

（6）陷洞攻击：攻击者通过一个危害点吸引某一特定区域的通信流量，形成以危害节点为中心的“陷洞”，处于陷洞附近的攻击者就能相对容易地对数据进行篡改。

（7）女巫攻击：物联网中每一个传感器都应有唯一的一个标识与其他传感器进行区分，由于系统的开放性，攻击者可以扮演或替代合法的感知节点，伪装成具有多个身份标识的节点，干扰分布式文件系统、路由算法、数据获取、无线资源公平性使用、节点选举流程等，从而达到攻击网络目的。

（8）洪泛攻击：攻击者通过发送大量攻击报文，导致整个网络性能下降，影响正常通信。

（9）信息篡改：攻击者将窃听到的信息进行修改（如删除、替代全部或部分信息）之后再将信息传送给原本的接收者，以达到攻击目的。

1.3.3 物联网的安全策略

传统的网络中，网络层的安全和业务层的安全是相互独立的，而物联网的安全问题很大一部分是由于物联网是在现有网络基础上集成了感知网络和智能处理平台带来的，传统网络中的大部分机制仍然适用于物联网并能够提供一定的安全性，如认证机制、加密机制等[2]。其中网络层和物理层可以借鉴的抗攻击手段相对多一些，但因物联网技术与应用特点使其对实时性等安全特性要求比较高，传统安全技术和机制还不足以使物联网的安全需求得到满足。

对物联网的网络安全防护可以采用多种传统的安全措施，如防火墙技术、病毒防治技术等，同时针对物联网的特殊安全需求，目前可以采取以下6种安全机制来保障物联网的安全。

（1）加密机制和密钥管理：是安全的基础，是实现感知信息隐私保护的手段之一，可以满足物联网对保密性的安全需求，但由于传感器节点能量、计算能力、存储空间的限制，要尽量采用轻量级的加密算法。

（2）感知层鉴别机制：用于证实交换过程的合法性、有效性和交换信息的真实性。主要包括网络内部节点之间的鉴别、感知层节点对用户的鉴别和感知层消息的鉴别。

（3）安全路由机制：保证网络在受到威胁和攻击时，仍能进行正确的路由发现、构建和维护，解决网络融合中的抗攻击问题，主要包括数据保密和鉴别机制、数据完整性和新鲜性校验机制、设备和身份鉴别机制以及路由消息广播鉴别机制等。

（4）访问控制机制：确定合法用户对物联网系统资源所享有的权限，以防止非法用户的入侵和合法用户使用非权限内资源，是维护系统安全运行、保护系统信息的重要技术手段，包括自主访问机制和强制访问机制。

（5）安全数据融合机制：保障信息保密性、信息传输安全和信息聚合的准确性，通过加密、安全路由、融合算法的设计、节点间的交互证明、节点采集信息的抽样、采集信息的签名等机制实现。

（6）容侵容错机制：容侵就是指在网络中存在恶意入侵的情况下，网络仍然能够正常地运行，容错是指在故障存在的情况下系统不会失效、仍然能够正常工作。容侵容错机制主要是解决行为异常节点、外部入侵节点带来的安全问题。

物联网作为正在兴起的、支撑性的多学科交叉前沿信息领域，还处于起步阶段，大多数领域的核心技术正在不断发展中，物联网所面临的安全挑战比想象的更加严峻，物联网安全尚在探索阶段，而网络安全机制还需要在实践中进一步创新、完善和发展，关于物联网的安全研究仍然任重而道远。我们既要迎接挑战，更要抓住这个机遇，充分利用现有的网络安全机制，并在原有安全机制基础上通过技术研发和自主创新进行调整和补充，以满足物联网的特殊安全需求，同时还要通过技术、标准、法律、政策、管理等多种手段来构建和完善物联网安全体系。

1.4 物联网感知层——传感器网络

1.4.1 传感器网络概述

微电子、计算机和无线通信等技术的进步，推动了低功耗多功能传感器的快速发展，使其在微小体积内能够集成信息采集、数据处理和无线通信等多种功能。无线传感器网络（Wireless Sensor Networks，WSNs）是由部署在监测区域内大量的廉价微型传感器节点组成，通过无线通信方式形成的一个多跳的自组织的网络系统，其目的是协作地感知、采集和处理网络覆盖区域中感知对象的信息，并发送给观察者。传感器、感知对象和观察者构成了WSNs的3个要素[3]。图1.4所示为无线传感器网络的体系结构。