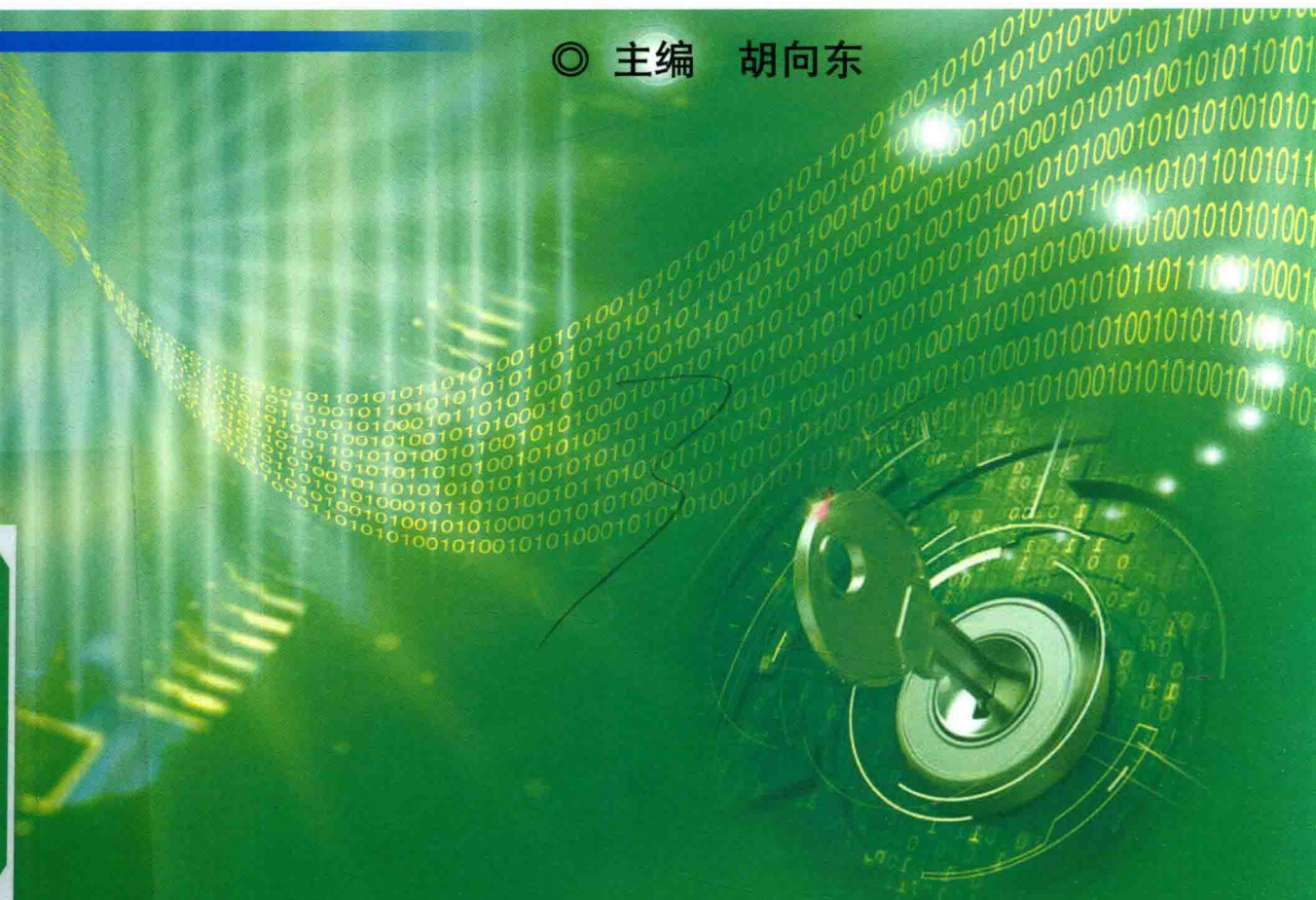
普通高等教育物联网工程专业规划教材

强化工程教育和“学思交融”学习模式特色教材

物联网安全

——理论与技术

◎ 主编　胡向东



机械工业出版社
CHINA MACHINE PRESS

普通高等教育物联网工程专业规划教材

物联网安全——理论与技术

主　编　胡向东
胡向东　胡　蓉　韩恺敏　张　峰
魏琴芳　杨　翔　王　浩　林家富　编著

机械工业出版社

本书是一本支持物联网安全翻转课堂教学和强化工程教育实践的特色教材。本书全面系统地介绍了物联网安全的基本概念、基础理论和关键技术。结构上分为物联网概述、物联网安全基础、物联网安全的密码理论、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全系统设计。为强化教学的适宜性，每一章首先给出引领学习和目标导向的导学表，包括本章的知识单元与知识点、能力点、重难点和学习要求，以及关联学习内容的问题导引；章节中有针对性地设置了若干结合当前内容的交流与微思考题目，推行“学思交融”的学习模式；章末还给出了适量的学习拓展与探究式研讨题目作为巩固深化知识之用，大部分章节提供复杂工程问题实践项目，以强化包括非技术要素在内的工程研究及创新能力训练与素质提升。

本书可作为高等院校物联网工程、信息安全、通信工程、网络工程、智能电网信息工程、计算机科学与技术等专业高年级本科生和研究生教材，也可供对物联网安全怀有兴趣者，或从事物联网安全相关领域管理、应用和设计开发的研究人员、工程技术人员参考。

图书在版编目（CIP）数据

物联网安全：理论与技术/胡向东主编．—北京：机械工业出版社，2017.3

普通高等教育物联网工程专业规划教材

ISBN 978-7-111-55679-4

Ⅰ.①物… Ⅱ.①胡… Ⅲ.①互联网络－安全技术－高等学校－教材 ②智能技术－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 302626 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：于苏华 路乙达 责任编辑：于苏华 路乙达

责任校对：樊钟英 封面设计：张 静

责任印制：李 洋

保定市中画美凯印刷有限公司印刷

2017 年 1 月第 1 版第 1 次印刷

184mm×260mm · 17 印张 · 410 千字

标准书号：ISBN 978-7-111-55679-4

定价：39.00 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

服务咨询热线：010－88379833

读者购书热线：010－88379649

网络服务

机 工 官 网：www.cmpbook.com

机 工 官 博：weibo.com/cmp1952

教育服务网：www.cmpedu.com

金 书 网：www.golden－book.com

前　言

以物联网、云计算、大数据、人工智能、虚拟现实等为代表的新一代信息技术与现代制造业、生产性服务业等的融合创新，为数字经济、智能制造、大数据驱动的经济增长提供了新动力。物联网推动经济发展方式的转变、促进经济结构的战略性调整，对经济社会走上创新驱动、内生增长、科学发展轨道的引领作用正在不断显现，具有市场前景广阔、经济技术效益好、带动性强的突出特点。随着“互联网+”等深入发展，物联网将信息技术的融合程度、覆盖领域、包容对象拓展到一个前所未有的巨大空间，以数字化、网络化、智能化的万物互联为核心的物联网应用正在快速地改变着人们的工作模式、生活习惯和思维方式，我国正在大力培育和发展物联网等战略性新兴产业，“互联网”+“双创”+“中国制造2025”将掀起新一轮科技革命和产业变革。随之而来的物联网等网络空间安全和隐私保护问题急需解决，并需要大量的专门人才为支撑；网络空间的竞争与攻防对抗，技术是保障，但归根结底是人才的竞争。相关数据显示，当前我国重要行业需要各类网络安全人才70万，预计到2020年增至约140万，而我国高等学校每年培养的信息安全类人才不足1.5万。2016年7月，中央网信办、国家发改委、教育部、科技部、工信部等多个部门联合下发《关于加强网络安全学科建设和人才培养的意见》，从国家战略层面大力推动物联网等网络安全人才的培养。

任何安全问题都有其复杂的一面，物联网安全尤其如此。且翻转课堂等教学变革、解决复杂工程问题能力训练、非技术要素培养等工程教育理念对教材内容的组织与编排等提出了新需求。本书的编著从提出到成稿历经近三年，尽管已有撰写出版国内第一本《物联网安全》专著的基础，但是仍然不敢有一丁点儿懈怠，借着对教学改革的热情，抱持以创新适应教学新需求和对读者高度负责的态度，经过长时间构思、推敲并查阅大量文献，以长期从事传感网、物联网安全相关研究成果为基础，结合物联网工程、信息安全等专业建设和课程教学需要编著了本书。

本书全面系统地介绍了物联网安全的基本概念、基础理论和关键技术。结构上分为物联网概述、物联网安全基础、物联网安全的密码理论、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全系统设计。为强化教学的适宜性，追求学习效率和效果，达成工程教育的目标，按照PBL（Problem－Based Learning）和OBE（Outcomes－Based Education）等理念的要求，每一章首先给出引领学习和目标导向的导学表，包括本章的知识单元与知识点、能力点、重难点和学习要求，以及关联学习内容的问题导引（课前）；章节中有针对性地设置了若干结合当前内容的交流与微思考题目，推行“问题牵引，学思交融，透过现象看本质”的学习模式，着力培养学生的“三思”（理性思维、批判性思维和创新性思维）能力；（课中）章末还给出了适量的学习拓展与探究式研讨题目作为巩固深化知识之用；大部分章节提供复杂工程问题实践项目以强化包括非技术要素在内的工程研究及创新能力训练与素质提升（课后）。

“以学习者为中心”“学而不思则罔，思而不学则殆”是本书写作所坚持的基本理念；良好的物联网安全教学适宜性、支持翻转课堂教学和强化工程教育是本书的主要特色；创新、亲切、善思是本书要呈现给读者的第一印象。围绕读者对象的定位、体系结构优化、内容难易度适中、主流技术覆盖到位等方面，以及导学表、问题导引、交流与微思考、学习拓展与探究式研讨以及复杂工程问题实践等项目的设置，系统优化的章节内容建构旨在支撑翻转课堂的教学模式，着眼于产出导向，始终带着问题学习与反思，并在学习过程中突出研讨交流和实践性，有助于全面理解物联网安全的基本内涵，准确把握物联网安全的发展现状和未来趋势，并激发进一步探索物联网安全的浓厚兴趣。

本书可作为高等院校物联网工程、信息安全、通信工程、网络工程、智能电网信息工程、计算机科学与技术等专业高年级本科生和研究生教材，也可供对物联网安全怀有兴趣者，或从事物联网安全相关领域管理、应用和设计开发的研究人员、工程技术人员参考。

本书由重庆邮电大学胡向东、胡蓉、韩恺敏、魏琴芳、王浩、林家富和中国移动研究院张峰、中国移动通信集团重庆有限公司杨翔等编著；秦晓鹏、牟海明、熊文韬、唐飞、刘可、李林乐、杨子明、陈国军、刘玥、白银、白浩浩等研究生参与了部分资料的整理和案例开发等工作；林金朝、刘宴兵等教授对相关课题研究、课程教学与建设等给予了关心与指导；要特别感谢参考文献中所列各位作者，包括众多未能在参考文献中一一列出资料的作者，正是因为他们在各自领域的独到见解和特别贡献为编著者提供了宝贵的资料和丰富的写作源泉，使我们能够在总结教学和科研工作成果的基础上，汲取各家之长，形成这本理论与技术兼顾、教学适宜性强、特色鲜明的物联网安全教材。本书的编著受到重庆市高等教育教学改革研究重点项目（162022）、教育部－中国移动科研基金研发项目（MCM20150202）和重庆市教委科学技术研究项目（KJ1602201）的资助。

物联网安全的内涵丰富、涉及面广、发展迅速、人才需求十分巨大而迫切，且以追求教学质量为根本目标的课程教学变革正在兴起。对本书的编著是从满足课程教学适宜性、强化工程能力训练和尝试教学改革视角在此领域的一次最新努力，其间融入了编著者“执着安全，锤炼精品，不忘初心”的情怀，以期打造一部内涵、质量、特色兼具且“接地气”的物联网安全教材，但限于自身的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教，以利修正，让更多的读者获益。联系邮箱：huxd@cqupt.edu.cn。

编著者

于重庆·南山（文峰书院）

目　录

前言

第 1 章　物联网概述 …… 1

1.1　物联网概念的提出 …… 2

1.2　物联网的基本内涵 …… 3

1.3　物联网的体系结构 …… 4

1.4　物联网的本质属性 …… 5

1.5　物联网的应用与影响 …… 6

学习拓展与探究式研讨 …… 9

第 2 章　物联网安全基础 …… 11

2.1　安全性攻击 …… 12

2.1.1　安全性攻击的主要形式 …… 12

2.1.2　安全性攻击的分类 …… 14

2.2　物联网面临的安全问题 …… 15

2.2.1　传统的网络安全威胁 …… 15

2.2.2　物联网面临的新威胁 …… 21

2.3　物联网安全概念 …… 24

2.3.1　物联网安全的基本内涵 …… 24

2.3.2　物联网安全与互联网安全、信息安全的关系 …… 25

2.3.3　物联网安全的特点 …… 25

2.4　物联网安全需求 …… 26

2.4.1　物联网感知层安全 …… 26

2.4.2　物联网网络层安全 …… 27

2.4.3　物联网应用层安全 …… 27

2.5　物联网安全体系 …… 28

2.5.1　物联网安全体系结构 …… 28

2.5.2　物联网安全技术体系 …… 29

2.6　物联网安全挑战 …… 30

2.6.1　网络资源的多态性 …… 31

2.6.2　安全威胁的多样性 …… 31

2.6.3　攻击的隐蔽性 …… 32

2.6.4　安全需求的复杂性 …… 32

2.6.5　安全支持能力的差异性 …… 32

2.6.6　安全理论与技术的滞后性 …… 32

2.6.7　安全需求与成本的矛盾性 …… 32

2.6.8　传统防火墙机制的局限性 …… 32

2.6.9　安全方案重构的困难性 …… 33

2.7　物联网安全现状与发展趋势 …… 33

2.7.1　物联网安全现状 …… 33

2.7.2　物联网安全发展趋势 …… 35

学习拓展与探究式研讨 …… 37

第 3 章　物联网安全的密码理论 …… 39

3.1　密码学基础 …… 40

3.1.1　密码学在物联网安全中的作用 …… 40

3.1.2　密码系统的组成与分类 …… 42

3.1.3　分组密码的操作模式 …… 43

3.1.4　安全模型 …… 47

3.2　对称密码体制与算法 …… 49

3.2.1　对称密码体制 …… 49

3.2.2　AES 对称密码算法 …… 51

3.2.3　SM4 对称密码算法 …… 57

3.2.4　祖冲之（ZUC）序列密码算法 …… 60

3.3　非对称密码体制与算法 …… 66

3.3.1　非对称密码体制 …… 66

3.3.2　RSA 公钥密码算法 …… 68

3.3.3　ECC 公钥密码算法 …… 70

3.3.4　SM2 公钥密码算法 …… 75

3.4　杂凑算法与消息认证 …… 76

3.4.1　杂凑函数 …… 76

3.4.2　杂凑算法 …… 78

3.4.3 消息认证 …… 84
3.5 数字签名 …… 87
3.5.1 数字签名的特殊性和要求 …… 87
3.5.2 数字签名方案 …… 89
3.5.3 数字签名标准 …… 90
3.6 密钥管理 …… 92
3.6.1 密钥管理系统 …… 92
3.6.2 Diffie – Hellman 密钥协商算法 …… 94
3.6.3 密钥的分发 …… 96
3.7 量子密码学概述 …… 97
学习拓展与探究式研讨 …… 101
复杂工程问题实践 …… 101
第4章 物联网感知层安全 …… 103
4.1 概述 …… 104
4.2 WSN 安全 …… 105
4.2.1 WSN 概述 …… 105
4.2.2 WSN 安全脆弱性 …… 105
4.2.3 WSN 安全威胁 …… 107
4.2.4 WSN 安全需求 …… 111
4.2.5 WSN 安全防御方法 …… 112
4.3 RFID 安全 …… 124
4.3.1 RFID 工作原理 …… 124
4.3.2 RFID 安全脆弱性 …… 125
4.3.3 RFID 安全威胁 …… 126
4.3.4 RFID 安全需求 …… 131
4.3.5 RFID 安全防御方法 …… 132
4.3.6 RFID 空中接口安全标准 …… 138
学习拓展与探究式研讨 …… 141
复杂工程问题实践 …… 141
第5章 物联网网络层安全 …… 143
5.1 概述 …… 144
5.1.1 网络层面临的安全形势 … 144
5.1.2 网络层安全需求 …… 145
5.1.3 网络层安全机制 …… 146
5.2 核心网安全 …… 147
5.2.1 核心网的典型安全架构 … 148
5.2.2 IPSec 安全协议与 VPN … 151
5.2.3 6LoWPAN 安全 …… 158
5.2.4 SSL/TLS …… 160
5.2.5 防火墙 …… 162
5.3 泛在接入安全 …… 165
5.3.1 远距离无线接入安全 …… 165
5.3.2 近距离无线接入安全 …… 171
5.4 异构网络安全 …… 184
5.4.1 异构网络的安全新问题 … 184
5.4.2 异构网络的安全原则 …… 184
5.4.3 异构网络的安全机制 …… 184
5.5 路由安全 …… 186
5.5.1 路由面临的安全威胁 …… 186
5.5.2 路由安全的防御对策 …… 188
5.5.3 路由安全协议 …… 188
学习拓展与探究式研讨 …… 189
复杂工程问题实践 …… 190
第6章 物联网应用层安全 …… 192
6.1 应用层面临的安全威胁 …… 193
6.2 应用层安全关键技术 …… 194
6.2.1 身份认证 …… 194
6.2.2 访问控制 …… 199
6.2.3 数据加密 …… 201
6.2.4 入侵检测 …… 202
6.3 应用层安全核心内容 …… 205
6.3.1 数据安全 …… 205
6.3.2 隐私安全 …… 208
6.3.3 定位安全 …… 212
6.3.4 云计算安全 …… 217
6.4 物联网安全管理 …… 222
6.4.1 物联网安全管理的要求 … 222
6.4.2 物联网安全管理的内容和对象 …… 222
6.4.3 物联网安全管理框架 …… 225
6.4.4 物联网安全管理体系 …… 225
学习拓展与探究式研讨 …… 227
复杂工程问题实践 …… 227
第7章 物联网安全系统设计 …… 230
7.1 物联网安全系统设计的

重要性 …… 231
7.2 物联网安全系统分析的一般方法 …… 231
7.3 物联网安全系统设计的基本要求 …… 233
7.4 物联网安全系统设计的主要流程 …… 234
7.5 物联网安全系统案例——智能家居安全 …… 239
7.5.1 智能家居网络构成 …… 239
7.5.2 智能家居安全需求 …… 240
7.5.3 智能家居安全机制 …… 241
7.5.4 智能门禁系统 …… 244
7.5.5 智能家居系统实现 …… 248
学习拓展与探究式研讨 …… 252
复杂工程问题实践 …… 252
附录 …… 254
参考文献 …… 263

第 1 章　物联网概述

知识单元与知识点	➢ 物联网概念的提出 ➢ 物联网的基本内涵 ➢ 物联网的体系结构 ➢ 物联网的本质属性 ➢ 物联网的应用与影响
能力点	✧ 基于对物联网概念及其基本内涵的理解，以及对物联网的体系结构和本质属性的认识，形成知识应用能力 ✧ 基于对物联网主要应用领域、场景和影响的了解，以及对物联网存在安全问题的初步认识，形成问题分析能力、工程研究能力，并强化环境保护意识 ✧ 基于交流与微思考，形成沟通表达能力、问题分析能力，并强化职业道德规范 ✧ 基于学习拓展与探究式研讨，形成知识应用能力、问题分析能力、终身学习能力
重难点	■ 重点：物联网概念；基于“互联网 +”的物联网含义；物联网本质属性 ■ 难点：物联网的体系结构
学习要求	✓ 熟练掌握物联网概念与物联网含义 ✓ 掌握物联网的体系结构和本质属性 ✓ 了解物联网的主要应用及影响 ✓ 初步认识物联网存在的安全问题

问题导引：

- 物联网的产生背景是什么？
- 如何从“互联网 +”角度理解物联网？
- 物联网的基本内涵是什么？
- 物联网的体系结构由哪几部分组成？各自的功能是什么？
- 如何理解物联网的本质属性？
- 物联网的典型应用有哪些？如何理解物联网的影响？

1.1 物联网概念的提出

中国政府正在大力推进“中国制造2025”、“互联网+”等强国战略，拟通过充分利用信息通信技术（Information Communications Technology，ICT）和网络空间虚拟系统即信息物理系统（Cyber-Physical System，CPS）与传统生产流程深度融合，推动建立高度灵活的个性化和数字化的产品与服务的生产模式，将信息技术及物联网（The Internet of Things，IoT）应用等推向一个前所未有的新高度，引领以“智能制造”为核心的第四次工业革命，激发大众创业与万众创新的热情，以互联网为基础的产业和服务业表现出巨大的社会需求，并正快速成长为新的经济增长点。以物联网为典型代表的“互联网+”的核心理念在于充分利用信息技术和互联网平台实现产品生产、服务提供和用户体验的信息化、智能化和便利化。

追溯物联网的发展，大致起源于1999年美国麻省理工学院自动识别中心（MIT AutoID Center）给出的“物联网”理念，即在计算机互联网基础上，利用条形码、射频识别（**Radio Frequency Identification，RFID**）、红外感应器、全球定位系统、激光扫描器等信息传感设备，通过无线数据通信等技术，构造一个覆盖世界上万事万物的网络，按约定的协议，把任何物品与互联网连接起来，进行人与人、人与物、物与物等之间的信息交换和通信，全面获取现实世界中的各种信息，以实现自动化和智能化的识别、定位、跟踪、监控和管理等功能。

2005年，在突尼斯举行的信息社会世界峰会上，国际电信联盟（ITU）发布了《ITU Internet Reports 2005：The Internet of things》，正式提出了“物联网”的概念，将应用创新作为物联网技术发展的核心，描绘的物联网时代应用场景包括：车辆上的传感器能够提醒驾驶人员道路存在的危险情况，当司机出现操作失误时汽车会自动报警；家庭中的智能传感器使电力提供商能够分析消费者的电能使用习惯，鉴定家用电器存在的问题，使消费者能够随时查阅自己的电力使用详细报告；回家前先发条短信，浴缸就能自动放好洗澡水；植物“渴了”就自动浇水；智能手环能够向朋友圈分享你每日的健身记录，保险公司还可以根据数据分析结果确定保险率；下班回家后智能机器人主动与您聊天并嘘寒问暖等等。

交流与微思考

智能手环、智能手表、Google眼镜等穿戴式智能设备正在快速兴起，它们是否属于物联网的一种应用场景？

2009年，IBM公司提出“智慧地球”的概念，在世界范围内掀起了物联网研究的热潮，物联网技术被多个国家列为重大信息发展战略，如国内的“感知中国”、日本的U-Japan计划、韩国的U-Korea计划，澳大利亚、新加坡、法国、德国等其他发达国家也加快了部署新一代智慧型网络基础设施的步伐。

物联网通过智能感知与识别、普适计算、泛在网络乃至虚拟现实（Virtual Reality，VR）等技术的融合应用，成为继计算机、互联网之后，世界信息技术的第三次革命。与物联网相关的全球信息化技术正在引发当今世界的巨大变革。

1.2 物联网的基本内涵

基于物联网的英语表述“The Internet of things”可知，物联网就是“物品级的互联网”或“有物品参与的互联网”，是“互联网+”，这里的“+”意味着传统互联网的延伸、拓展与融合，主要有三个方面的含义：

1）Internet + things，即互联网的用户端延伸到物品，最明显的变化是由人及物，强化“万物互联”，使得人与人、人与物、物与物之间的互动方式发生改变，均能基于该网络进行信息交换与通信。

2）互联网（Internet）本身拓展为互联网、电信网（特别是移动通信网）、广播电视网和传感网等不同形态网络的融合，最关键的变化是在信息传输网络基础上融合了信息感知网络。

3）互联网+各个传统行业，是互联网思维在应用实践上的拓展并推动经济形态不断演变，即利用信息通信技术及互联网平台，充分发挥互联网在社会资源配置中的优化和集成作用，将互联网的创新成果与传统行业进行深度融合，创造新的发展形态，提升全社会的创新力和生产力，形成以互联网为基础设施和实现工具的经济发展新形态。

以上是物联网基于互联网的三大革命性改变。物联网是随着当代生产力的快速发展，多学科科学技术交叉融合的推动，以及不断增长的应用需求的递进牵引的产物。多学科科学技术交叉融合表现为现代信息技术发展到一定阶段后，感知（信息获取——仪器科学与技术学科）、网络（信息传输——信息与通信工程学科）、智能信息处理（信息处理——计算机科学与技术学科）和自动化（信息应用——控制科学与工程学科）等完整信息链的各技术环节汇聚、集成，形成涌现效应，将传统的互联网改造升级成一个人与物都能够协调参与和互动的、虚实结合的智慧空间，实现虚拟空间和物理空间的融合，构建起人类社会与物质世界、自然环境之间更加紧密、便捷的逻辑联系。

物联网的目标在于将虚拟空间与现实世界完美结合，使得现实世界中的“物”可以通过虚拟空间中的“信息”进行连接和控制，实现异构网络的融合、海量终端的互联、超海量数据的增值、各行业应用的支撑等。物联网使得人和物在任何时间（Anytime）、任何地点（Anywhere），使用任何的路径或网络（Any path/Any network）、任何的服务与业务（Any service/Any business），与任何的事物（Anything/Any device）、任何人（Anyone）无缝地联系（“6A”），将聚合（Convergence）、内容（Content）、知识库（Collections）、计算（Computing）、通信（Communication）和连接（Connectivity）等元素（“6C”）集成在一起形成一个以智能化为核心的有机整体，加强人、物、环境等的互动交流，基于万物互联达成数据自由共享、价值按需分配，从而实现更便捷的信息沟通、更高的工作效率、更低的操作成本、更多的创造性劳动和更舒适的生活体验。物联网的基本内涵如图1-1所示。

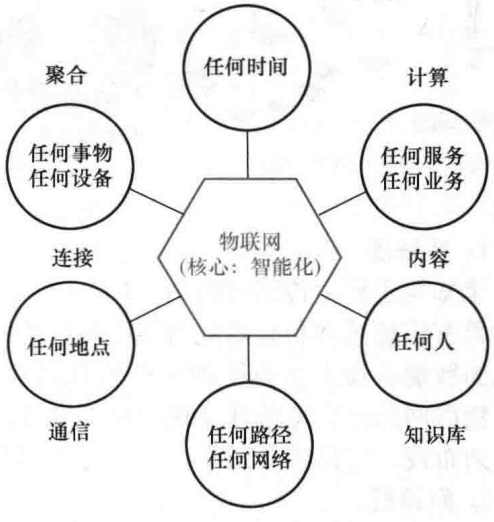


图1-1 物联网的基本内涵

交流与微思考

在传统互联网基础上，物联网依托延伸、拓展和融合实现了快速崛起，并在众多领域得到了应用推广。在物联网欣欣向荣的背后，你认为物联网的核心价值是什么？

1.3 物联网的体系结构

体系结构是一个系统或网络的一组部件及部件之间的联系。物联网的体系结构如图 1-2 所示，由感知层、网络层以及应用层组成，分别完成智能感知、接入与传输、处理与决策等功能，即基于对物理环境的智能感知，最终实现对目标对象的智能控制。

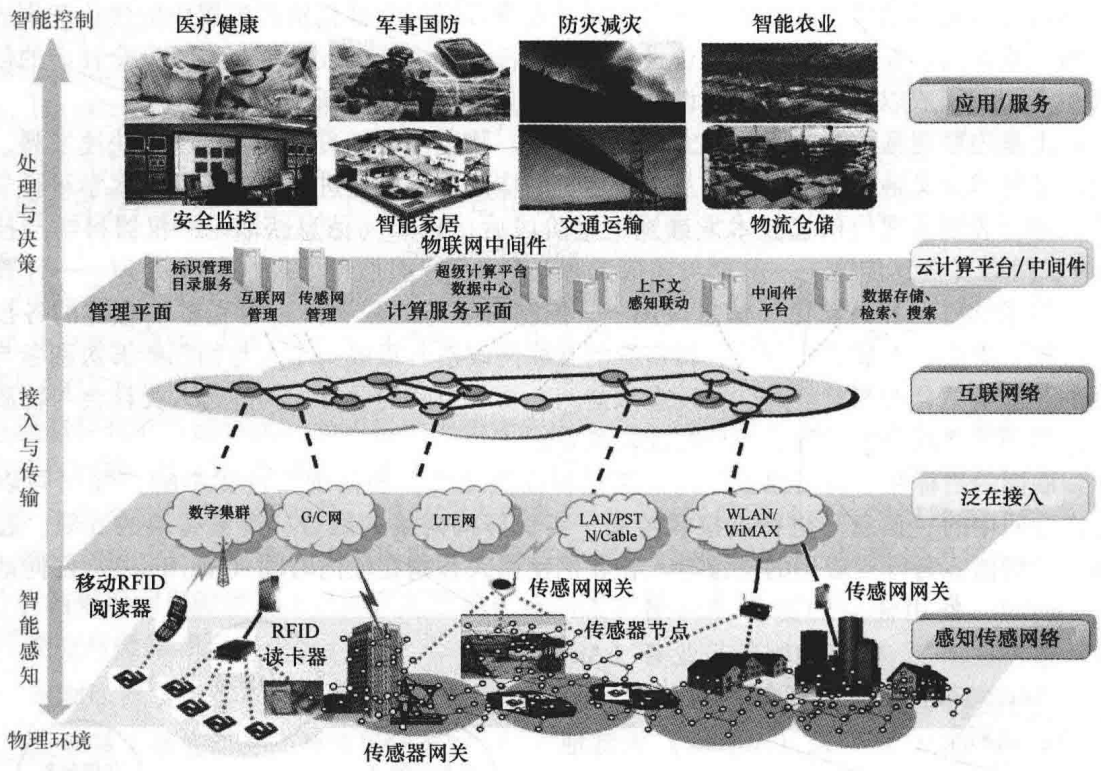


图 1-2 物联网的体系结构

1. 感知层

感知层主要由传感器网络、RFID 标签与阅读器、条形码及其阅读器、摄像头、GPS 等各种具有信息感知与采集能力的终端设备（传感器件），以及执行器（控制器件）组成（可以认为智能机器人是其中的一个特殊部件），用以完成对信息的采集、转换或执行控制操作。物联网的泛在特性就体现于感知层节点数量众多、具有广泛的覆盖能力，能够实现无所不在的布设，它是整个网络的“神经末梢”“神经元”或“信息元”。

2. 网络层

网络层包括泛在接入网和核心的骨干网。泛在接入网包括数字集群、GSM/CDMA 网、

LTE 网、LAN/PSTN/Cable 以及 WLAN/WiMAX 等，负责将感知层收集的信息汇聚起来，然后交由核心的骨干网进行传输，或者将来自骨干网的测控指令分发给感知层的测量或控制节点；骨干网以现有互联网为基础，融合电信网、广播电视网等构成，是完成物联网信息传输的主通道和核心，是物联网的“信息高速公路”。

3. 应用层

应用层主要通过对来自传输层的信息进行智能分析、处理，得出决策方案，从而实现智能控制，完成特定业务系统的应用服务。它由业务支撑平台和各种业务应用系统组成。

业务支撑平台通常以中间件的形式存在。业务支撑平台从功能上可分为管理平面和计算服务平面两部分，前者负责互联网管理、标识管理、目录管理、安全管理等，后者负责数据处理、存储、检索，以及上下文感知联动、云计算等。物联网的智能化主要体现在业务支撑平台对信息的智能处理与决策控制，即智能信息处理，为层出不穷的应用创新提供支持。

业务应用系统由物联网的实际应用领域确定，如医疗健康、军事国防、防灾减灾、智能农业、安全监控、智能家居、交通运输、物流仓储等等。

交流与微思考

物联网会给教育带来怎样的冲击和变革？物联网背景下未来的学习模式可能是什么样的？

1.4 物联网的本质属性

物联网虽起源于互联网，却超越了互联网，形成了自身特有的一些属性。物联网的本质属性可以从以下三个方面来理解：

1. 融合性

融合是物联网发展最重要的理念之一，物联网是全面的“互联网 +”，具有无穷的包容潜力，基于互联网的延伸、拓展将传统互联网、电信网、广播电视网和传感网等融合起来，将人与物更紧密地连接起来，形成一个广阔无垠的智慧空间。物联网的融合性还表现为信息感知、通信、智能信息处理和信息应用等多学科科学技术的交叉集成；通过设备融合、网络融合、平台融合、技术融合实现服务融合、业务融合和市场融合等。

2. 泛在性

物联网发展成一个覆盖世界上万事万物，以无所不在、无所不包、无所不能为基本特征的“6A”网络（Anyone、Anything、Anytime、Anywhere、Any path、Any business），基于顺畅的通信实现人与人、人与物、物与物之间按需进行信息获取、传输、处理和应用等，这就是物联网的泛在性。基于物联网的泛在特性可将其称为泛在网（Ubiquitous network）。

3. 创新性

物联网的创新性不仅表现为在传统互联网基础上实现了三大革命性改变，而且基于这三大变革为智能信息获取与处理及层出不穷的物联网应用创新提供了坚实的基石，物联网的核心理念在于智能化和创新性，从而其堪称掀起世界上第三次信息技术浪潮。

物联网是通过能够获取物体信息的传感技术来进行信息采集，通过网络进行信息传输与交换，通过信息处理系统进行信息加工及决策。物联网在整个信息获取、传输、处理与应用的过程中展现出融合性、泛在性和创新性。

为了便于与传统互联网对比，一般认为物联网有五个基本特征：一是全面感知，即利用条形码、射频识别、传感器等各种可用的感知手段，实现对物品自身或环境状态信息的全面实时采集；二是无缝互联，即通过各种信息通信技术和网络技术的融合，实现异构网络的无缝连接与互通；三是可靠传递，即通过现有的互联网、广播电视网、通信网等网络设施和通信技术，基于可信的数据传输机制或冗余的网络通信链路等实现数据的可靠传输；四是智能处理，利用云计算、模糊识别、人工智能（Artificial Intelligence，AI）、神经网络、数据挖掘等智能计算技术对海量的数据和信息进行分析和处理，以便按需、自动地获取有用信息并对其进行利用，表现出高度的智能化；五是协同互动，嵌入传感器和微处理器的物品越来越具有智能性，能够协同获取和处理感知信息，为高效管理和控制提供决策支持。正是基于对物联网特征的深入认知，业界通常将物联网分为感知层（全面感知）、网络层（无缝互联、可靠传递）和应用层（智能处理、协同互动）三个层次。

交流与微思考

如何理解物联网的本质属性与基本特征？

1.5 物联网的应用与影响

物联网以“互联网+”的拓展融合能力、智能化的内在本质和创新应用的根本追求在世界范围内掀起新的信息技术浪潮，物联网的革命性变革植根于ICT技术充分应用于各行各业、各个领域和所覆盖的物品，使得每一个信息化的物品（如智能终端，统称为信息元）成为网络信息交换的节点，实现对现有互联网组成模式、覆盖范围和应用对象的极大拓展，最终形成一个无所不在、无所不包、无所不联的泛在网络，使人们生活的环境也具备“智慧”，人与人、人与物、物与物之间可以方便地进行“对话”，建立起以信息交换为纽带、信息沟通无障碍、信息元广泛分布为特征的更加紧密的逻辑联系，实现人类社会与物理环境的高度关联与深度融合。因此，物联网在很大程度上可以看作是互联网的应用拓展，与其说物联网是网络，不如说物联网是业务和应用。

物联网的“ICT基因”、泛在属性和智能化能力使得其用途十分广泛，遍及智能交通、智慧物流、智能家居、智能电网、智能农业、城市管理、环境监测、防灾减灾、保健护理、安全保卫、工业监控、国防军事等众多民用与军事领域，如图1-3所示。物联网产业将覆盖人类生产生活的各个方面，它以信息感知获取为基础，以信息传输处理为纽带，以信息行业应用为平台，以信息增值业务为媒介，实现面向各个用户的信息服务产业链条。随着物联网的应用与发展，世界上物与物互联的业务将远远超过人与人通信的业务，在物联网普及以后，用于动物、植物、机器、物品等的传感器与电子标签及配套的接口装置的数量将大大超过手机的数量，物联网将会发展成为一个上万亿美元规模的高科技市场。

为加快转变经济发展方式、促进经济结构的战略性调整，引领经济社会走上创新驱动、内生增长、科学发展的轨道，我国正在大力培育和发展物联网等战略性新兴产业。战略性新兴产业体现了新兴科技和新兴产业的深度融合，既代表科技创新的重要方向，也代表产业发展的重要方向，具有市场前景广阔、经济技术效益好、带动性强的突出特点。作为战略性新兴产业的重要代表，在“工业化与信息化深度融合”“智慧地球”“传感中国”“中国制造2025”“互联网+”等理念的引领下，并随着技术的发展、应用需求的牵引和产业支撑能力

图 1-3　物联网的典型应用领域

的推进，物联网将前所未有地加强人与物的联系，物联网变革给人类社会带来的影响无疑将是颠覆性的，能够通过高效协作和行业细分来优化配置社会的各种资源，不浪费任何一颗螺丝、善待每一个灵魂，将整个社会带入价值创造、吸收和升华的大循环。人们能够以更加精细、动态、便捷和智能的方式管理生产、经营商品、享受生活，提高资源利用率、生产力水平、经济效益和工作效率，降低成本，改善人与人、人与物、人与自然的关系，达到人与所处环境的和谐统一。

交流与微思考

很早以前，人们就幻想着“千里眼”“顺风耳”。试设想在物联网技术背景下，如何实现“千里眼”“顺风耳”？你能从中国的北斗导航系统得到怎样的启发？

物联网作为一个新兴的融合创新技术，具有明显的多学科交叉特点，物联网中无处不在的数据收集和使用，以及自身不成熟及资源有限导致的安全脆弱性和潜在攻击手段的复杂多变，使得物联网环境下的信息安全和隐私保护面临着空前的挑战和严峻的安全形势。如智慧物流中 RFID 标签信息被非法复制，阅读器不能进行有效的认证与访问控制，或者物流数据库被非法入侵，都会导致物流管理的混乱或损失；商业建筑或居民家庭的智能家居系统中监控视频如果被非法获取，将导致用户隐私泄露或更严重的后果；智能交通中的 RFID 识别和 GPS 定位系统如果受到攻击，可能导致停车场无法实现对车辆进出的自动管理、ETC 收费系统无法实现正常扣费、对交通违章车辆无法进行有效的处罚；医疗设备在走向智能和互联的同时，却面临着计算机病毒等信息安全困扰，若无适当的对策，可能会导致病患数据失窃或设备被恶意控制，当攻击者获得设备的控制权并且伤害到患者，甚至危及其生命时，就会演变成严重的医疗安全事件。

尽管科技界、产业界、政府部门以及广大普通民众基于各自不同的背景对物联网有不同

的理解和期待，但有一点是需要共同认知的，即“没有安全就没有应用，没有应用就没有发展”；业界普遍认同：公司在研究开发物联网设备或物联网应用系统时应该采取合理的安全措施。在越来越强调生命尊严、生活质量和工作效率的今天，与人们的生产、生活息息相关的物联网的安全尤其重要！

交流与微思考

“智能设备正带着你我走近无隐私的赤裸世界”，这不是一句危言耸听的玩笑话！如今，人们正行进在物联网和大数据时代的快车道上，每天使用的电脑暗地里收集着你的IP地址和上网记录；而随着正在普及化的智能设备成为人们生活中不可或缺的一部分，相比电脑，它们以更加亲近的方式成为新的信息显示和收集单元，智能电视、智能家居、智能手机、智能手环、智能医疗、智能汽车……都在以自己独特的方式获取信息、跟踪用户、了解用户的使用习惯，最终汇聚成不同领域的大数据。

当大数据展现出诱人的商业价值时，以何种方式采集用户数据、收集到的数据被如何利用就会成为问题，如人们常常受到被精确推送的广告的骚扰，而用户往往是被动的、不情愿的，并且是难以抵抗的。

设想一下，未来当人们身边的一切都智能化之后，如果你的个人数据没有得到强而有力的保护，任凭厂商或别有用心的人收集、买卖、利用，信息之间产生交叉将会造成非常可怕的后果。也许会出现这样的场景：清晨醒来，伸了一个懒腰的你穿上“踩印问”牌智能拖鞋，它精确地收集到你每天早晨的体重变化；来到“妆得像”智能梳妆镜前，它悄然扫描你的眼底，分析你的视网膜是否有病变，并观察和记录下你身上是否佩戴了任何珠宝首饰等；接着你打开“防走光”牌智能窗帘，它监测窗外阳光的照度，还顺便探测了屋内的湿度；你拎着LVV智能手提袋出了门，它探测到你钱夹里放着哪些银行的银行卡；你富有个性地大喊一声“出发”，行进在大街上回头率极高的“忐死啦”（被人戏称为“吓死啦”）最新款智能汽车经过声纹分析确认了你的主人身份后向你敞开怀抱，一路上“无人驾驶”便将你送往著名的“乱劈柴”公司，并记录下车辆状态与运行参数。接下来，你到了办公室，发现秘书早已为您准备好的“逼急奔”电脑里正显示着“老板，‘随便花’银行卡，足不出户，一秒轻松贷”；你拿起“遂君意”牌智能水杯品了一口刚沏好的新茶，你的DNA信息就被收集和分析，是否存在缺陷的提醒及健康建议被及时地显示在杯子的LED屏上；不一会儿，电脑屏幕上弹出专为你准备的个性化广告：“女人，每天都要璀璨如明珠、靓丽如天使——用‘本女神’珠宝吧，您值得拥有！”；正当你沉浸在广告的引诱之中还未拿定主意之时，“宝宝乐”牌智能耳机中传来定向广告：“宝贝，您还在为卧室空气干燥而烦恼吗？试试‘湿在好’加湿器吧”；然后，电话铃响起：“美女，我们医院创新开展高科技减肥疗法，欢迎您来‘瘦柔精’旗舰店免费体验”；这时，你去智能厕所方便了一下，用过的“舒服+”智能马桶立即分析你的尿蛋白水平，并向你报告关于肾脏疾病和糖尿病的指标检测结果。因受到无尽骚扰而气急败坏、没有心情工作的你准备回到自己的爱车里找个清静之所，你刚打开文峰书院首席教师“秦时明月征

西还”开设的微信公众号“传感器与检测技术精品资源课程”准备充充“电”，不料，智能的“忒死啦”发声了：“主人，欢迎您回来！更换‘滑得卓’牌机油对您的爱车保养更有利，它的总店地址在找不着北路520号，一般人我不告诉他，呵呵”……被垃圾信息一整天折磨得哭笑不得的你，终于在夜深时感受到难得的惬意；正当你含情脉脉地看着自己的另一半，眼神中透露出无尽爱意，手指在衣襟前轻拂欲撩之时，你的“爱疯”手机响了：“亲，1314牌智能床头柜温馨提醒：剩余‘都累死’即将情趣不足，为了安全，欢迎您登录www. 欢乐无限 . com 继续网购相同款式超值套装”。诚如这样，你是否觉得有一双无形的眼睛始终在自己周围注视着你？你是否会怀念今天这个虽不算太智能、却倍觉美好的时代？

智能硬件的蓬勃发展与大数据的积累正在开辟一个不可逆转的智能时代，现实世界将会以前所未有的形式和人类互动。当我们置身于一个充满各种感应器（传感器）的智能世界，却同时成了一个不由自主的“透明”人，无法拥有安全的隐私和不受骚扰的信息环境。物联网尽管美好，但如果落入信息应用无序和隐私泄露的状态，没有安全的物联网是不是一场难以想象的灾难。如果你作为一名出色的物联网工程师，会向用户提供这样的物联网产品或服务吗？应有的作为是什么？

☆ 学习拓展与探究式研讨

1. 以“我身边的物联网”为题，结合自身对物联网的了解和应用体验，谈谈对物联网的具体认识。

2. 试从技术和产业角度概述世界各国的物联网发展现状。

3. 为什么物联网成为了互联网的下一个发展阶段？物联网的下一个发展阶段又会是什么？未来的物联网节点是否很大部分将由同时具备感知和执行能力的智能机器人充当？是否会融入大量的人工智能（AI）和虚拟现实（VR）技术？更进一步的物联网发展会否将人作为网络的高级节点，演化成“人”“物”高度融合统一的“天人网”或“合一网”，呈现出比“万物互联”包容性和沉浸感更强的“全互联”景象？会不会出现有情感的物联网？未来最熟知人类（包括秘密）的可能是机器，在人工智能的管控下，人类或至少其中一部分是否将听命于机器而身不由己？

4. 你认为物联网的未来发展趋势有哪些？

5. 如何理解物联网存在安全问题？为什么说“物联网的安全尤其重要”？