



“十二五”江苏省高等学校重点教材

应用型本科 物联网专业“十二五”规划教材

物联网信息安全

李永忠 编著
张明 张绛丽 景国良 参编

- 内容新颖：新知识、新技术、新工艺
- 特色鲜明：突出“应用、实践、创新”
- 定位准确：面向工程技术型人才培养
- 质量上乘：应用型本科专家全力打造



西安电子科技大学出版社
<http://www.xduph.com>



“十二五”江苏省高等学校重点教材(编号: 2015-2-025)

应用型本科 物联网专业 “十二五” 规划教材

物联网信息安全

李永忠 编著

张 明 张绛丽 景国良 参编

西安电子科技大学出版社

内 容 简 介

本书在介绍信息安全技术和网络安全技术的基础上,按照物联网的层次体系组织教材内容,重点讲述物联网安全技术,全面而系统地阐述物联网安全中的关键技术及其典型解决方案。

本书可作为应用型本科、独立学院以及高职高专院校的物联网工程、信息安全、计算机科学与技术、通信工程、网络工程等相关专业的教材,也可作为物联网工程、信息安全等相关专业研究生和物联网领域工程技术人员的参考书。

图书在版编目(CIP)数据

物联网信息安全/李永忠编著. —西安:西安电子科技大学出版社,2016.5

应用型本科 物联网专业“十二五”规划教材

ISBN 978-7-5606-4078-5

I. ① 物… II. ① 李… III. ① 互联网络—信息安全—高等学校—教材 IV. ① TP393.4

中国版本图书馆 CIP 数据核字(2016)第 080837 号

策 划 高 樱

责任编辑 许青青 武翠琴

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com

经 销 新华书店

印刷单位 陕西华沐印刷科技有限责任公司

版 次 2016 年 5 月第 1 版 2016 年 5 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印 张 24.5

字 数 581 千字

印 数 1~3000 册

定 价 45.00 元

ISBN 978-7-5606-4078-5/TP

XDUP 4370001-1

如有印装问题可调换

应用型本科 物联网专业系列教材

编审专家委员名单

主 任：沈卫康（南京工程学院 通信工程学院 院长/教授）

副主任：张士兵（南通大学 电子信息学院 副院长/教授）

陈 岚（上海应用技术学院 电气与电子工程学院 副院长/教授）

宋依青（常州工学院 计算机科学与工程学院 副院长/教授）

张明新（常熟理工学院 计算机科学与工程学院 副院长/教授）

成 员：（按姓氏拼音排列）

鲍 蓉（徐州工程学院 信电工程学院 副院长/教授）

陈美君（金陵科技学院 网络与通信工程学院 副院长/副教授）

高 尚（江苏科技大学 计算机科学与工程学院 副院长/教授）

李文举（上海应用技术学院 计算机科学学院 副院长/教授）

梁 军（三江学院 电子信息工程学院 副院长/副教授）

潘启勇（常熟理工学院 物理与电子工程学院 副院长/副教授）

任建平（苏州科技学院 电子与信息工程学院 副院长/教授）

孙霓刚（常州大学 信息科学与工程学院 副院长/副教授）

谭 敏（合肥学院 电子信息与电气工程系 系主任/教授）

王杰华（南通大学 计算机科学与技术学院 副院长/副教授）

王章权（浙江树人大学 信息科技学院 副院长/副教授）

温宏愿（南京理工大学泰州科技学院 电子电气工程学院 副院长）

严云洋（淮阴工学院 计算机工程学院 院长/教授）

郁汉琪（南京工程学院 创新学院 院长/教授）

杨会成（安徽工程大学 电气工程学院 副院长/教授）

杨俊杰（上海电力学院 电子与信息工程学院 副院长/教授）

于继明（金陵科技学院 智能科学与控制工程学院 副院长/副教授）

前 言

物联网作为国家的战略新兴产业，正在得到大力发展，在国家科技创新、可持续发展和产业升级中具有重要的地位。在工业和信息化部发布的《物联网“十二五”发展规划》中，“加强信息安全保障”已成为主要任务之一。物联网工程是一个新的本科专业，国内已有许多大学开办物联网工程专业，“物联网安全”是物联网工程专业本科生的一门专业课。目前物联网安全的教材很少，教材内容没有形成体系，教学与教材建设差距很大。市场上已有的“物联网安全”教材内容处于两极分化的状态：一类主要讲述物联网的内容，加一两章信息安全的内容就是物联网安全；另一类主要讲述信息安全或网络安全的内容，加一两章物联网的内容就是物联网安全。针对物联网“卓越工程师”培养方案，选择一本合适的“物联网安全”课程教材比较难。本书是根据“卓越工程师计划”（软件外包应用型教材编写计划）、结合教学过程中积累的经验编写而成的，对物联网安全相关内容进行了梳理，按照物联网的层次体系组织教材内容，重点讲述物联网安全技术。

本书全面而系统地阐述物联网安全中的关键技术及其典型解决方案。全书按照物联网的层次体系分为三大部分：物联网感知层安全、物联网网络层安全和物联网应用层安全。本书共分8章：物联网安全概述、网络信息安全技术基础、物联网安全体系结构及物理安全、物联网感知层安全、物联网网络层安全、物联网应用层安全、物联网安全技术应用和典型物联网安全实例。在第2、4、5、7章的后面配有物联网安全技术应用实训内容；在第5章介绍了3G、4G移动通信系统安全机制的分析和应用；在第6章介绍了云计算安全的内容以及物联网信息安全标准；在第7章重点讲述了物联网安全技术的设计，介绍了EPCglobal网络安全技术的应用；第8章主要介绍典型物联网应用中的安全案例，重点讲述了物联网和云计算在智慧医院中的应用，例如WLAN在医院病床查询中的应用，WBAN在远程医疗中的应用及其安全技术，无线体域网远程医疗系统的安全实例，此外，还简单介绍了M2M安全实例以及车联网的安全分析。本书的参考教学时间为48~64学时，也可根据不同的教学要求灵活讲授。

本书内容编排符合认识规律，逻辑性强，概念准确，内容新颖，自成体系，便于教学和自学，可作为物联网工程、通信工程、网络工程、计算机科学与技术等专业的相关教材，也可作为相关领域工程技术人员的参考书。

全书由李永忠统筹主编，张明完成了第3、4章部分内容的编写，张绛丽完成了第5、6章部分内容的编写，景国良完成了第7、8章的编写，最后由李永

忠对全书做了修改和定稿。研究生陈兴亮、包冲、冒海波参与了本书的编辑和实验资料准备。另外，对参与本书的编写提出宝贵意见的老师和同学们，作者在此一并表示诚挚的感谢。

由于编者水平和学识有限，加之时间仓促，书中不妥之处在所难免，殷切地希望广大读者及同行专家批评指正。

作 者

2016年2月

于江苏科技大学

目 录

第 1 章 物联网安全概述	1	2.4 网络层安全协议 IPSec	56
1.1 物联网安全概述	1	2.4.1 网络安全协议综述	56
1.1.1 物联网简介	1	2.4.2 IPSec 协议	57
1.1.2 物联网的体系结构	7	2.4.3 IPSec 安全体系结构	57
1.2 物联网安全问题分析	11	2.4.4 利用 IPSec 实现 VPN	61
1.2.1 物联网安全与相关学科的关联	11	2.4.5 IPSec 存在的问题	65
1.2.2 物联网安全威胁	14	2.5 防火墙技术	66
1.2.3 物联网安全需求分析	17	2.5.1 防火墙基础知识	66
1.3 物联网的安全架构	18	2.5.2 防火墙的实现方法	68
1.3.1 物联网的安全层次模型及体 系结构概述	18	2.5.3 防火墙的分类	72
1.3.2 物联网安全的总体概貌与 整体安全架构	21	2.5.4 防火墙的发展与新技术	73
1.4 物联网安全的技术分析	25	2.5.5 黑客攻击技术	74
思考与练习一	31	2.6 入侵检测技术	77
第 2 章 网络信息安全技术基础	34	2.6.1 入侵检测的概念	77
2.1 网络安全基本概念	34	2.6.2 入侵检测方法	79
2.1.1 网络安全简介	34	2.6.3 入侵检测的步骤	82
2.1.2 网络安全面临的威胁	36	2.6.4 入侵检测系统的结构	83
2.1.3 网络安全策略与防护体系	37	2.6.5 几种常见的入侵检测系统	85
2.1.4 网络安全的发展趋势	38	2.6.6 入侵检测技术发展趋势	88
2.2 数据加密技术	39	2.7 入侵防御技术	89
2.2.1 加密基本概念	39	2.7.1 入侵防御系统 IPS	89
2.2.2 古典加密方法	40	2.7.2 入侵防御系统的设计思想以及其 应该具备的特征	91
2.2.3 对称加密方法	41	2.7.3 入侵防御系统的设计	91
2.2.4 非对称密码算法	48	2.7.4 入侵防御系统的应用部署	93
2.3 数字签名	51	2.8 统一威胁管理 UTM	94
2.3.1 数字签名的概念	51	2.8.1 UTM 提出的背景	94
2.3.2 常用的数字签名体制介绍	53	2.8.2 UTM 的定义	94
2.3.3 认证技术	55	2.8.3 UTM 的功能	95
		2.8.4 UTM 的特征	95
		2.8.5 UTM 的典型技术	96

2.8.6 UTM 的优势 97

2.8.7 UTM 目前存在的问题 98

2.8.8 UTM 的适用场合及产品 98

2.8.9 UTM 的一个典型应用解决方案 99

2.8.10 UTM 的发展趋势 101

思考与练习二 101

实训一 网络扫描与嗅探工具使用 104

第 3 章 物联网安全体系结构及物理安全 110

3.1 物联网安全体系结构 110

3.1.1 物联网安全整体结构 110

3.1.2 感知层安全体系结构 111

3.1.3 传输层安全体系结构 112

3.1.4 应用层安全体系结构 114

3.2 物联网安全技术措施 115

3.2.1 物联网安全技术 115

3.2.2 物联网安全管理 117

3.3 物理安全威胁与防范 119

3.3.1 物理安全概述 119

3.3.2 环境安全威胁与防范 119

3.3.3 设备安全问题与策略 120

3.3.4 RFID 系统及物理层安全 120

3.3.5 数据存储介质的安全 123

3.4 无线局域网 WLAN 物理层安全 124

3.4.1 IEEE 802.11 标准中的物理层特点 ... 124

3.4.2 IEEE 802.11 标准中的 MAC 层 125

3.4.3 CSMA/CA 协议 126

3.4.4 对信道进行预约的 RTS/CTS 协议 ... 127

3.4.5 WAPI 协议 128

思考与练习三 130

第 4 章 物联网感知层安全 132

4.1 感知层安全概述 132

4.1.1 感知层的安全地位 133

4.1.2 感知层的安全威胁 133

4.2 RFID 安全 134

4.2.1 RFID 安全威胁 134

4.2.2 RFID 安全技术 134

4.2.3 RFID 安全密码协议 136

4.2.4 轻量级密码算法 143

4.3 传感器网络安全 151

4.3.1 无线传感器网络简介 152

4.3.2 传感器网络安全威胁分析 155

4.3.3 无线传感器网络的安全需求分析 156

4.3.4 无线传感器网络的安全攻击与防御 157

4.3.5 传感器网络安全防护主要手段 160

4.3.6 传感器网络典型安全技术 161

4.3.7 无线传感器网络的密钥管理 164

4.3.8 无线传感器网络安全协议 SPINS 169

4.3.9 轻量级公钥密码算法 NTRU 171

4.4 物联网终端系统安全 173

4.4.1 嵌入式系统安全 173

4.4.2 智能手机系统安全 178

思考与练习四 184

实训二 RFID 安全技术应用 186

实验一 LF 低频 RFID 实验 186

实验二 HF 高频 RFID 通信协议 192

第 5 章 物联网网络层安全 197

5.1 网络层安全需求 197

5.1.1 网络层安全威胁 198

5.1.2 网络层安全技术和方法 199

5.2 近距离无线接入安全——WLAN 安全 202

5.2.1 无线局域网 WLAN 的安全威胁 202

5.2.2 无线局域网的安全机制 208

5.3 远距离无线接入安全——移动通信网安全 224

5.3.1 无线移动通信安全简介 224

5.3.2 2G(GSM)安全机制 227

5.3.3 3G 安全机制 229

5.3.4 4G 安全机制简介 234

5.4 扩展接入网的安全 237

5.4.1 近距离无线低速接入网安全 238

5.4.2 有线网络接入安全 243

5.4.3 卫星通信接入安全 248

5.5 物联网核心网安全——6LoWPAN 和 RPL 的安全性	253	7.1.1 物联网面向主题的安全模型及应用	309
5.5.1 核心 IP 骨干网的安全	253	7.1.2 物联网公共安全云计算平台系统	313
5.5.2 6LoWPAN 适配层的安全	258	7.2 物联网安全技术应用	318
思考与练习五	264	7.2.1 物联网机房远程监控预警系统	318
实训三 WLAN 安全技术应用——WiFi 模块的使用	267	7.2.2 物联网门禁系统	319
第 6 章 物联网应用层安全	274	7.3 EPCglobal 网络安全技术应用	323
6.1 物联网应用层安全需求	274	7.3.1 EPCglobal 物联网的网络架构	324
6.1.1 应用层面临的安全问题	274	7.3.2 EPCglobal 网络安全	325
6.1.2 应用层安全技术需求	274	思考与练习七	327
6.2 Web 安全	275	实训四 物联网门禁系统应用——2.4G 人员定位实验	331
6.2.1 Web 结构原理	275	第 8 章 典型物联网安全实例	335
6.2.2 Web 安全威胁	276	8.1 智慧医院——物联网在医疗系统中的应用	335
6.2.3 Web 安全防护	277	8.1.1 智慧医院概述	335
6.3 中间件安全	278	8.1.2 智慧医院建设云计算数据中心需求分析	336
6.3.1 中间件	279	8.1.3 智慧医院的云计算平台设计	338
6.3.2 物联网中间件	280	8.1.4 云平台网络安全设计	342
6.3.3 RFID 中间件安全	280	8.1.5 物联网和云计算在医疗领域的应用	344
6.4 数据安全	282	8.2 智慧医院的 WLAN 无线查房系统与安全	347
6.4.1 数据安全概述	282	8.2.1 无线查房系统介绍	347
6.4.2 数据安全保护	283	8.2.2 无线查房系统的无线网络结构设计	349
6.4.3 数据库安全	284	8.2.3 无线查房系统的 WLAN 安全设计	349
6.4.4 虚拟化数据安全	285	8.3 基于无线体域网 WBAN 的远程医疗安全	353
6.4.5 数据容灾	286	8.3.1 无线体域网 WBAN	354
6.5 云计算安全	288	8.3.2 无线体域网 WBAN 的特征	356
6.5.1 云计算概述	289	8.3.3 WBAN 安全分析	358
6.5.2 云计算安全问题	291	8.4 M2M 安全	360
6.5.3 云计算安全需求	293	8.4.1 M2M 概述	360
6.5.4 云计算的存储安全	296	8.4.2 M2M 安全	364
6.5.5 计算虚拟化安全	298		
6.5.6 云计算安全标准	300		
6.6 物联网信息安全标准	302		
思考与练习六	306		
第 7 章 物联网安全技术应用	309		
7.1 物联网系统安全设计	309		

8.5 车联网及其安全简介..... 367

8.5.1 车联网的概念及其发展..... 367

8.5.2 车联网系统存在的问题及其关键技术..... 369

8.5.3 车联网的体系结构与应用..... 371

8.5.4 车联网的信息安全问题与安全威胁..... 373

8.5.5 车联网的安全架构设计..... 374

思考与练习八..... 377

参考文献..... 379

第1章 物联网安全概述

物联网是继微型计算机技术、互联网技术之后现代信息技术的第三次技术革命，是对现代信息技术的各种新技术、新理念的高度融合，打通了电子技术、自动化技术、通信技术、生物技术、机械技术、材料技术等以往关联不大的技术之间的通道，使得这些技术真正融合为一个整体，从而实现了通信从人与人向人与物、物与物的拓展。物联网行业应用需求广泛，潜在市场规模巨大。代表下一代信息技术发展方向的物联网，将会像互联网一样成为全球经济发展的又一个驱动力。

1.1 物联网安全概述

1.1.1 物联网简介

1. 物联网的概念

物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是“Internet of Things(IoT)”。顾名思义，物联网就是物物相连的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上延伸和扩展的网络；其二，物联网的用户端延伸和扩展到了任何物品与物品之间，它们彼此之间进行信息交换和通信，也就是物物相连。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，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。因此，应用创新是物联网发展的核心，以用户体验为核心的创新是物联网发展的灵魂。

物联网的广义定义：指的是利用局部网络或互联网等通信技术把传感器、控制器、机器、人员和物等通过新的方式连在一起，形成人与物、物与物相连，实现信息化、远程管理控制 and 智能化的网络。物联网是互联网的延伸，它包括互联网及互联网上所有的资源，兼容互联网所有的应用，但物联网中所有的元素(设备、资源及通信等)都是个性化和私有化的。

物联网的狭义定义：指的是将各种信息传感设备，如射频识别(RFID)装置、红外感应器、全球定位系统、激光扫描器等装置与互联网结合起来而形成的一个巨大网络。其目的是让所有的物品都与网络连接在一起，方便识别和管理。物联网是利用无所不在的网络技术建立起来的，其中非常重要的技术是 RFID 电子标签技术。

物联网的特点是以简单 RFID 系统为基础,结合已有的网络技术、数据库技术、中间件技术等,构筑一个由大量联网的 RFID 阅读器和无数移动标签组成的,比 Internet 更为庞大的网络,在这个网络中,系统可以自动地、实时地对物体进行识别、定位、追踪、监控并触发相应事件。

由上述定义我们可以发现,物联网具有以下三个方面的重要特征:

(1) 互联网特征。物联网是解决物与物、人与物之间通信的网络形态,它是在互联网基础之上延伸和扩展的一种网络,尽管终端多样化,但其基础和核心仍然是互联网。

(2) 识别与通信特征。纳入物联网的“物”一定要具备自动识别与物物通信(M2M)的功能,通过在各种物体上植入微型感应芯片,使任何物品都可以变得“有感受、有知觉”。物联网的这一神奇功能是互联网所不具备的,它主要依靠一种名为“射频识别”的技术来实现。

(3) 智能化特征。网络系统应具有自动化、自我反馈与智能控制的特点。

另外,物联网可用的基础网络有很多,根据其应用需要可以用公网也可以用专网,通常互联网被认为是最适合作为物联网的基础网络。

目前较为成熟的分布式网络集成框架是 EPCglobal 提出的 EPC 网络。EPC 网络主要针对物流领域,其目的是增加供应链的可视性(Visibility)和可控性(Control),使整个物流领域能够借助 RFID 技术获得更大的经济效益。

物联网在国际上又称为传感网。南京邮电大学杨震教授说:“世界上的万事万物,小到手表、钥匙,大到汽车、楼房,只要嵌入一个微型感应芯片,把它变得智能化,这个物体就可以‘自动开口说话’。再借助无线网络技术,人们就可以和物体‘对话’,物体和物体之间也能‘交流’,这就是物联网。如果物联网再搭上互联网这个桥梁,在世界任何一个地方我们都可以即时获取万事万物的信息。可以这么说,物联网加上互联网等于智慧地球。”

2. 物联网的发展

物联网的实践最早可以追溯到 1990 年施乐公司的网络可乐贩售机——Networked Coke Machine。

1991 年美国麻省理工学院(MIT)的 Kevin Ashton 教授首次提出物联网的概念。

1995 年比尔·盖茨在《未来之路》一书中也曾提及物联网,但未引起广泛重视。

1998 年,美国麻省理工学院提出了当时被称为 EPC(Electronic Product Code)系统的物联网构想。

1999 年美国麻省理工学院建立了“自动识别中心(Auto-ID)”,提出“万物皆可通过网络互联”,阐明了物联网的基本含义。早期的物联网是依托射频识别(RFID)技术的物流网络,随着技术和应用的发展,物联网的内涵已经发生了较大变化。

2003 年美国《技术评论》提出传感网络技术将是未来改变人们生活的十大技术之首。2003 年 10 月,非盈利性组织 EPCglobal 成立,形成了基于 Internet 的 RFID 系统。

2004 年, IETF 成立了基于低功耗无线个域网(LoWPAN)的 IPv6 工作组 6LoWPAN,致力于研究由 IEEE 802.15.4 链路构成的低功耗无线个域网中如何优化运行 IPv6 协议。这为通过 Internet 直接寻址访问无线传感器网络节点(无需通过网关)提供了可能,使得无线传感器网络走向开放并可能成为一种 Web 服务。2004 年日本总务省(MIC)提出 u-Japan 计划,

该战略计划力求实现人与人、物与物、人与物之间的连接, 希望将日本建设成一个随时、随地、任何物体、任何人均可连接的泛在网络社会。

2005年11月17日, 在突尼斯举行的信息社会世界峰会(W SIS)上, 国际电信联盟(ITU)发布《ITU 互联网报告 2005: 物联网》, 引用了“物联网”的概念。其中, 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, 不再只是指基于RFID技术的物联网。报告指出, 世界上所有的物体都可以通过互联网主动进行信息交换, RFID、传感器技术、纳米技术、智能嵌入技术将得到更加广泛的应用, 强调M2M(Machine-to-Machine)通信。2008年, 欧洲智能系统集成技术平台(EPoSS)在《物联网 2020》报告中分析预测了未来物联网的发展阶段。可见, 欧洲的物联网是从电信部门开始主导的, 因为M2M具有巨大的市场潜力。

2009年, 欧盟执委会发表题为《Internet of Things: an Action Plan for Europe》的物联网行动方案, 描绘了物联网技术应用的前景。提出欧盟政府要加强对物联网的管理, 促进物联网的发展。物联网上升为整个欧盟的战略行为。

2009年2月24日, 在2009 IBM论坛上, IBM大中华区首席执行官钱大群公布了名为“智慧地球”的最新策略。此概念一经提出, 即得到美国各界的高度关注, 甚至有分析认为IBM公司的这一构想极有可能上升至美国的国家战略, 并在世界范围内引起轰动。今天, “智慧地球”战略被美国人认为与当年的“信息高速公路”有许多相似之处, 同样被认为是振兴经济、确立竞争优势的关键战略。该战略能否掀起如当年互联网革命一样的科技和经济浪潮, 不仅为美国所关注, 更为世界所关注。

2009年8月, 温家宝总理在无锡视察时发表重要讲话, 提出“感知中国”的战略构想。温家宝“感知中国”的讲话把我国物联网领域的研究和应用开发推向了高潮, 后来的《让科技引领中国可持续发展》的讲话中将物联网列入战略新兴产业之一, 标志着物联网产业发展已经提升到我国的国家战略。我国开始大规模介入物联网, 无锡市率先建立了“感知中国”研究中心, 中国科学院、各大电信运营商、多所大学在无锡建立了物联网研究院, 无锡市江南大学还建立了全国首家实体物联网工厂学院。物联网在中国受到了全社会极大的关注, 其受关注程度是在美国、欧盟各国以及其他国家不可比拟的。与此同时, 韩国通信委员会和日本政府IT战略本部分别提出了物联网相关战略。

物联网获得学术界与工业界的青睐是因为物联网技术给人们提供了一种前所未有的信息收集手段, 通过物联网技术, 人们可以轻松地获得自然界的各类信息。从信息的角度来讲, 整个地球就变成了物联网的信息工厂。过去一直将物理基础设施和IT基础设施分开: 一方面是机场、公路和建筑物, 另一方面是数据中心、传感器和RFID。在物联网时代, 各类建筑将与芯片、互联网有效地整合。

3. 物联网的关键技术

物联网涉及的新技术很多, 其中的关键技术主要有射频识别技术、传感器技术、网络通信技术和云计算(数据存储与计算)等。

1) 射频识别技术

射频识别技术, 俗称“电子标签”, 是物联网中非常重要的技术, 是实现物联网的基础与核心。射频技术是一项利用射频信号通过空间耦合(交变磁场或电磁场)实现无接触信息

传递并通过所传递的信息达到识别目的的技术。这一技术由三个部分构成：① 标签(Tag)，附着在物体上以标识目标对象；② 阅读器(Reader)，用来读取(有时还可以写入)标签信息，既可以是固定的，也可以是移动的；③ 天线(Antenna)，其作用是在标签和阅读器之间传递射频信号。当然，在实际应用中还需要其他硬件和软件的支持。

该项技术的基本思想是：通过先进的技术手段，实现人们对各类物体或设备(人员、物品)在不同状态(移动、静止或恶劣环境)下的自动识别和管理。由于射频识别无须人工干预，可使用于各种恶劣环境，可用来追踪和管理几乎所有物理对象，所以零售商和制造商非常关心和支持这项技术的发展和應用。比如，沃尔玛公司就成功地将射频技术应用于供应链管理中，高速公路的自动收费系统更是这项技术最成功的应用之一。

射频技术发展面临的主要问题和难点是：① 射频识别的碰撞防冲突问题；② 射频天线研究；③ 工作频率的选择；④ 安全与隐私问题。

2) 传感器技术

要产生真正有价值的信息，仅有射频识别技术是不够的，还需要传感器技术。由于物联网通常处于自然环境中，传感器要长期经受恶劣环境的考验，因此，物联网对传感器技术提出了更高的要求。

作为获取信息的关键器件，传感器是现代信息系统和各种装备不可缺少的信息采集手段。如果把计算机看做处理和识别信息的“大脑”，把通信系统看做传递信息的“神经系统”的话，则传感器就是“感觉器官”。所谓传感器，是指那些对被测对象的某一确定的信息具有感受(或响应)与检出功能，并使之按照一定规律转换成与之对应的可输出信号的元器件或装置。离开了传感器对被测的原始信息进行准确可靠的捕获和转换，一切准确的测试与控制都将无法实现。传感器技术的发展与突破主要体现在两个方面：一是感知信息方面；二是传感器自身的智能化和网络化。未来传感器技术的发展趋势大致分为如下几个方面：向检测范围挑战；集成化、多功能化；向未开发的领域——生物传感器挑战；传感技术、智者为尊——智能传感器(Smart Sensor)；发现和利用新材料。

传感器技术是一门集光、机、电、生物信息于一身的综合技术，传感器技术的水平从一个侧面反映了微电子技术、MEMS、纳米技术、光电子技术、生物技术等高新技术的水平。

3) 网络通信技术

无论物联网的概念如何扩展和延伸，其最基础的物物之间的感知和通信是不可替代的关键技术。网络通信技术包括各种有线和无线传输技术、交换技术、组网技术、网关技术等。其中 M2M 技术则是物联网实现的关键。M2M 技术是机器对机器(Machine to Machine)通信的简称，指所有实现人、机器、系统之间建立通信连接的技术和手段，同时也可代表人对机器(Man to Machine)、机器对人(Machine to Man)、移动网络对机器(Mobile to Machine)之间的连接与通信。M2M 技术适用范围广泛，可以结合 GSM/GPRS/UMTS 等远距离连接技术，也可以结合 WiFi、Bluetooth、ZigBee、RFID 和 UWB 等近距离无线连接技术，此外还可以结合 XML 和 CORBA 以及基于 GPS、无线终端和网络的位置服务技术等，用于安全监测、自动售货机、货物跟踪等领域。目前，M2M 技术的重点在于机器对机器的无线通信，而将来的应用则将遍及军事、金融、交通、气象、电力、水利、石油、煤矿、工控、

零售、医疗、公共事业管理等各个行业。短距离无线通信技术的发展和完善,使得物联网前端的信息通信有了技术上的可靠保证。

通信网络技术为物联网数据提供传送通道,如何在现有网络上进行增强,适应物联网业务的需求(低数据率、低移动性等),是该技术研究的重点。物联网的发展离不开通信网络,更宽、更快、更优的下一代宽带网络将为物联网发展提供更有力的支撑,也将为物联网应用带来更多的可能。

4) 云计算技术

云计算(Cloud Computing)是网格计算、分布式计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物。云计算的基本原理是:通过虚拟化技术将计算任务分布在大量的分布式计算机虚拟化资源池上,而非本地计算机或远程服务器,企业数据中心的运行将更与互联网相似。这使得企业能够将资源切换到需要的应用上,根据需求访问计算机和存储系统。它旨在通过网络把多个成本相对较低的计算实体整合成一个具有强大计算能力的完美系统,并借助 SaaS、PaaS、IaaS、MSP 等先进的商业模式把这强大的计算能力分布到终端用户手中。

云计算的一个核心理念就是通过不断提高“云”的处理能力,减少用户终端的处理负担,最终使用户终端简化成一个单纯的输入输出设备,并能按需享受“云”的强大计算处理能力。Google 搜索引擎是云计算的成功应用之一。

5) EPC 物联网的关键技术

目前较为成熟的物流领域的物联网 EPC 是由 EPCglobal 提出的,EPC 物联网的关键技术包括:

(1) EPC 编码:长度为 64 位、96 位和 256 位的 ID 编码,出于成本的考虑,现在主要采用 64 位和 96 位两种编码。EPC 编码分为四个字段,分别为:① 头部,标识编码的版本号,这样就可使电子产品编码采用不同的长度和类型;② 产品管理者,如产品的生产商;③ 产品所属的商品类别;④ 产品的唯一编号。

(2) Savant:介于阅读器与企业应用之间的中间件,为企业应用提供一系列计算功能。它的首要任务是减少从阅读器传往企业应用的数据量,对阅读器读取的标签数据进行过滤、汇集、计算等操作,同时 Savant 还提供与 ONS、PML 服务器、其他 Savant 的互操作功能。

(3) 对象名字服务(ONS):类似于域名服务器 DNS,ONS 提供将 EPC 编码解析为一个或一组 URL 的服务,通过 URL 可获得与 EPC 相关产品的进一步信息。

(4) 信息服务:以 PML 格式存储产品相关信息,可供其他的应用进行检索,并以 PML 的格式返回。存储的信息可分为两大类:一类是与时间相关的历史事件记录,如原始的 RFID 阅读事件(记录标签在什么时间被哪个阅读器阅读),高层次的活动记录如交易事件(记录交易涉及的标签等);另一类是产品固有属性信息,如产品生产时间、过期时间、体积、颜色等。

(5) 物理标示语言(PML):PML 在 XML 的基础上扩展而来,被视为描述所有自然物体、过程和环境的统一标准。在 EPC 网络中,所有有关商品的信息都以物理标示语言 PML 来描述,PML 是 EPC 网络信息存储和交换的标准格式。

4. 物联网的应用

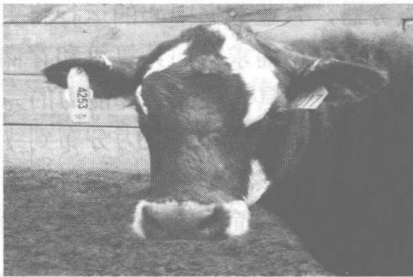
物联网用途广泛,遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能

消防、工业监测、老人护理、个人健康等多个领域。电视、洗衣机、空调甚至自行车、门锁和血压计上都能使用。专家预测 10 年内，物联网就可能大规模普及，一个上万亿元规模的高科技市场将就此诞生。

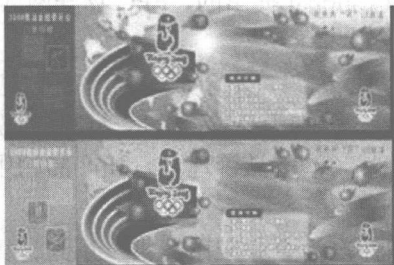
举几个例子来说明物联网的应用，购买深圳到樟木头的火车票，若使用 RFID 标签，上车不用排队检票，RFID 阅读器会自动检票；扫描牛奶包装盒的二维码可以跟踪牛奶的产地和奶牛编号；使用 RFID 标签的奥运会门票，奥运会检票就不用排长队入馆了；第二代身份证有芯片防伪功能，使用非接触式 IC 卡芯片作为“机读”存储器，芯片和电路线圈在证卡内封装，能够保证证件在各种环境下正常使用，具有读写速度快、使用方便、易于保管的特征；在物流供应和管理系统中使用 RFID 标签可以使得物流供应链的 SCM 和货物定位快捷方便。图 1-1 所示是物联网的几个典型应用。



(a) 火车票检票



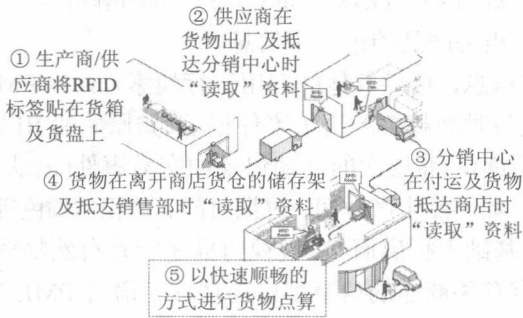
(b) 牧场奶牛信息管理



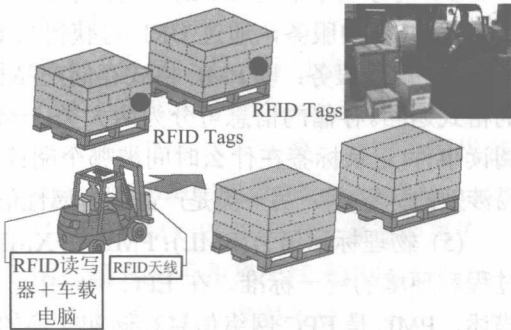
(c) 奥运会门票检票



(d) 第二代身份证



(e) 供应链管理 SCM



(f) 货物定位跟踪管理

图 1-1 物联网的典型应用

时至今日,物联网已不只是一个学术概念,而是有着非常广泛的市场需求。实际上,物联网已经在很多领域有应用案例,这些商业案例的成功是物联网获得大发展的先决条件。目前,国内外物联网具有应用优势的领域主要包括如下方面:

(1) 智能电网。智能电网,就是利用传感器、嵌入式处理器、数字化通信和 IT 技术,构建具备智能判断与自适应调节能力的,多种能源统一入网和分布式管理的智能化电力网络系统,可对电网与客户用电信息进行实时监控和采集,且采用最经济与最安全的输配电方式将电能输送给终端用户,实现对电能的最优配置与利用,提高电网运行的可靠性和能源利用效率。

智能电网是物联网第一重要的应用,很多电力企业开展的“无线抄表”应用,其实也是物联网应用的一种。对于物联网产业甚至整个信息通信产业的发展而言,电网智能化将产生强大的驱动力,并将深刻影响和有力推动其他行业的物联网应用。

(2) 智能交通。所谓智能交通,就是利用先进的通讯、计算机、自动控制、传感器技术,实现对交通的实时控制与指挥管理。交通智能化是解决交通拥堵、提高行车安全、提高运行效率的重要途径。目前,全国已经有 20 多个省区市实现了公路联网监控、交通事故检测、路况气象等应用,路网检测信息采集设备的设置密度在逐步加大,有些高速公路实现了全程监控,并可以对长途客运、危险货物运输等车辆进行动态监管。

21 世纪将是公路交通智能化的时代,人们将要采用的智能交通系统是一种先进的一体化交通综合管理系统。在该系统中,车辆靠自己的智能在道路上自由行驶,公路靠自身的智能将交通流量调整至最佳状态,借助于这个系统,管理人员对道路、车辆的行踪将掌握得一清二楚。

(3) 物流管理。物流领域是物联网相关技术最有现实意义的应用领域之一。通过在物流商品中引入传感节点,可以从采购、生产制造、包装、运输、销售到服务的供应链上的每一个环节都做到精确地了解和掌握,对物流全程传递和服务实现信息化的管理,最终减少货物装卸、仓储等物流成本,提高物流效率和效益。物联网与现代物流有着天然紧密的联系,其关键技术诸如物体标识及标识追踪、无线定位等新型信息技术的应用,能够有效实现物流的智能调度管理,整合物流核心业务流程,加强物流管理的合理化,降低物流消耗,从而降低物流成本,减少流通费用,增加利润。物联网将加快现代物流的发展,增强供应链的可视性和可控性。

(4) 医疗管理。在医疗领域,物联网在条码化病人身份管理、移动医嘱、诊疗体征录入、药物管理、检验标本管理、病案管理数据保存及调用、婴儿防盗、护理流程、临床路径等管理中,均能发挥重要作用。例如,通过物联网技术,可以将药品名称、品种、产地、批次及生产、加工、运输、存储、销售等环节的信息,都存于电子标签中,当出现问题时,可以追溯全过程。同时还可以把信息传送到公共数据库中,患者或医院可以将标签的内容和数据库中的记录进行对比,从而有效地识别假冒药品。在公共卫生方面,通过射频识别技术建立医疗卫生的监督和追溯体系,可以实现检疫检验过程中病源追踪的功能,并能对病菌携带者进行管理,为患者提供更加安全的医疗卫生服务。

1.1.2 物联网的体系结构

物联网融合了无线网络和有线网络,扩大了接入 Internet 网络的设备规模,使得网络连