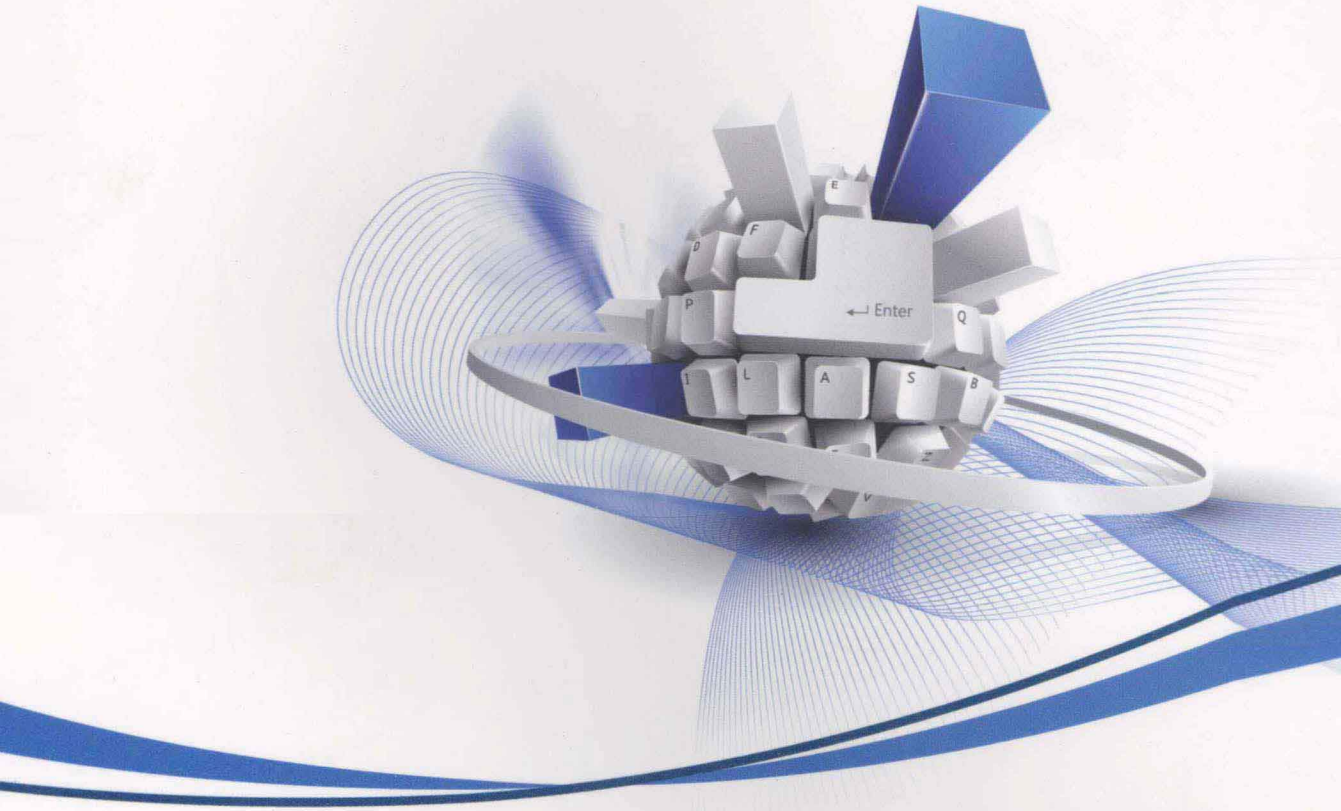
国家级特色专业（物联网工程）规划教材



物联网安全技术

施荣华　杨政宇　编著

◎ 内容全面，系统地介绍物联网面对的安全问题及其解决方案
◎ 思路新颖，从物联网的不同层次结构来讲述物联网安全技术
◎ 配有教学课件，方便教学使用

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

国家级特色专业（物联网工程）规划教材

物联网安全技术

施荣华　杨政宇　编著

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

内 容 简 介

本书是依托中南大学国家级特色专业（物联网工程）的建设，结合国内物联网工程专业的教学情况编写的。本书系统、全面地介绍了物联网安全的相关技术，首先介绍了物联网安全技术的基础知识，包含物联网面临的挑战、物联网安全的基础，以及物联网安全技术的密码理论；然后详细地介绍了物联网中三个层次面临的安全问题及其解决方案，包括物联网感知层安全、信息传输安全、以及应用层安全；最后就物联网安全技术的发展趋势进行了讨论。

本书可作为普通高等学校物联网工程及其相关专业的教材，也可供从事物联网及其相关专业的人士阅读。

本书配有教学用的 PPT 课件，读者可登录华信教育资源网（www.hxedu.com.cn）免费注册后下载。

图书在版编目（CIP）数据

物联网安全技术/施荣华，杨政宇编著. —北京：电子工业出版社，2013.7
国家级特色专业（物联网工程）规划教材
ISBN 978-7-121-20894-2

Ⅰ. ①物… Ⅱ. ①施… ②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.①TP393.4②TP18

中国版本图书馆 CIP 数据核字（2013）第 145995 号

责任编辑：田宏峰　　特约编辑：牛雪峰
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
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：787×980　1/16　印张：13.75　字数：352 千字
印　　次：2013 年 7 月第 1 次印刷
印　　数：3 000 册　　定价：39.00 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。

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。

服务热线：（010）88258888。

出版说明

物联网是通过射频识别（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相连接，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概念。物联网是继计算机、互联网和移动通信之后的又一次信息产业的革命性发展。物联网产业具有产业链长、涉及多个产业群的特点，其应用范围几乎覆盖了各行各业。

2009 年 8 月，物联网被正式列为国家五大新兴战略性产业之一，写入“政府工作报告”，物联网在中国受到了全社会极大的关注。

2010 年年初，教育部下发了高校设置物联网专业申报通知，截至目前，我国已经有 100 多所高校开设了物联网工程专业，其中有包括中南大学在内的 9 所高校的物联网工程专业于 2011 年被批准为国家级特色专业建设点。

从 2010 年起，部分学校的物联网工程专业已经开始招生，目前已经进入专业课程的学习阶段，因此物联网工程专业的专业课教材建设迫在眉睫。

由于物联网所涉及的领域非常广泛，很多专业课涉及其他专业，但是原有的专业课的教材无法满足物联网工程专业的教学需求，又由于不同院校的物联网专业的特色有较大的差异，因此很有必要出版一套适用于不同院校的物联网专业的教材。

为此，电子工业出版社依托国内高校物联网工程专业的建设情况，策划出版了“国家级特色专业（物联网工程）规划教材”，以满足国内高校物联网工程的专业课教学的需求。

本套教材紧密结合物联网专业的教学大纲，以满足教学需求为目的，以充分体现物联网工程的专业特点为原则来进行编写。今后，我们将继续和国内高校物联网专业的一线教师合作，以完善我国物联网工程专业的专业课程教材的建设。

电子工业出版社

教材编委会

前　言

PREFACE

编写背景

物联网（the Internet of Things，IOT）是通过射频识别（RFID）装置、红外感应器、全球定位系统、激光扫描器、传感器节点等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理等功能的一种网络。物联网的概念有两层含义：第一，它是互联网、移动通信网和传感网等网络的融合，是在互联网基础之上的延伸和扩展的一种网络；第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信。因此，物联网的核心是完成物体信息的可感、可知、可传和可控。

从信息与网络安全的角度来看，物联网作为一个多网的异构融合网络，不仅存在与传感器网络、移动通信网络和互联网同样的安全问题，同时还有其特殊性，如隐私保护问题、异构网络的认证与访问控制问题、信息的存储与管理等。数据与隐私保护是物联网应用过程中的挑战之一。在物联网中，RFID 系统和传感器实现末端信息的感知，构成物联网的感知层，其安全问题主要为信息保护，针对不同的系统有各自不同的安全解决方案。同时通过承载网络包括互联网、移动网、WLAN 网络和一些专业网（如数字音/视频广播网、公共服务专用网）等，以及各种网络接入设备，能够把感知到的信息快速、可靠、安全地进行传输，构成物联网网络层，其安全问题也同样承接相应的网络安全自身已有的问题和网络融合后的信息安全问题。物联网的应用层主要面向物联网系统的具体业务，其安全问题直接面向物联网用户群体，与物联网的其他层次有着明显的区别，其信息安全还涉及知识产权保护、计算机取证、计算机数据销毁等安全需求和相关的信息安全技术。

本书是“国家级特色专业（物联网工程）规划教材”之一。目前，市面上的物联网教材多是“物联网导论”、“物联网基础”之类的书籍，侧重介绍物联网的基本安全概念、基本安全技术原理以及相关应用安全等综述性知识，而介绍物联网的分层安全技术的专门教材比较少。自物联网的概念在国内被重点提出后，网络融合的相关研究与应用已经取得丰硕的成果，但是作为制约其发展的安全性问题大多还在研究中，因此编写一本较全面地概括物联网信息安全技术的相关教材，有助于引导读者开始关注其基础安全技术的研究，也是作者编写本书的初衷。

内容安排

本书系统全面地介绍了物联网的安全相关技术——感知层安全技术、网络传输层安全技术、应用层安全技术等，内容包括 RFID 系统安全技术、传感器网络安全技术、蓝牙、ZigBee、无线局域网（WLAN）、RFID 安全中间件、网络防火墙、数据安全、云计算安全技术等。全书共 7 章，各章内容安排如下：

第 1 章绪论。首先概要介绍物联网的概念与发展，并简单描述物联网的体系结构；然后介绍信息安全技术，以及物联网信息安全面临的挑战；最后分析了从互联网信息安全到物联网信息安全的转变。

第 2 章介绍物联网安全基础。首先综合描述了物联网安全技术所采用的基本密码学常识；然后对模运算、群论、有限域理论及欧几里得算法及其扩展做简要的介绍；接着对经典对称密码算法——AES 加密算法进行介绍，讲述了其加密原理与解密过程；最后对非对称加密算法——椭圆曲线加密法进行概述，并描述其加密体制的实现过程。

第 3 章介绍物联网安全的密码基础。首先对物联网安全需求进行分析，介绍物联网中感知节点的安全威胁、通信网络的安全问题及应用层安全问题；接着介绍物联网安全的特征和几项关键技术；最后给出物联网安全技术的应用模型。

第 4 章介绍物联网感知层安全。首先是感知层安全概述，介绍物联网信息感知的安全特征和面临的攻击；然后介绍 RFID 系统的安全相关技术包括访问控制和密码学相关技术方案；最后介绍传感器网络安全知识，从传感器网络的基本结构出发，介绍其安全防护主要手段、经典安全技术及安全协议等知识。

第 5 章介绍信息传输安全。首先简要介绍信息传输的安全需求；然后详细描述物联网核心网安全问题——下一代网络（NGN）安全技术和网络虚拟化安全技术；接着介绍两种短距离信息传输技术的安全问题——基于蓝牙的物联网信息传输安全和基于 ZigBee 的物联网信息传输安全；最后介绍两种长距离信息传输技术的安全问题——基于 UWB 的物联网信息传输安全和基于 WMN 的物联网信息传输安全。

第 6 章介绍应用层安全。首先从应用层安全需求讲起，依次描述其面临的安全问题；然后通过中间件安全技术和服务安全技术两方面介绍处理方法；接着介绍数据安全相关技术，包括数据安全特征与策略；然后讲述物联网中的关键技术云安全技术，从云安全概述开始介绍，再分析云应用安全与云计算总的访问控制与安全认证问题；最后介绍云计算技术的研究现状。

第 7 章介绍了物联网安全技术的发展趋势。介绍了物联网安全技术未来的发展主要在跨学科与智能化方面，物联网与传统网络的融合趋势明显，并展望了其安全技术标准的制定问题；最后介绍了物联网安全新观念，从复杂庞大的系统角度来看待其转变安全的应对方式。

本书汇聚了物联网安全技术领域各方面最新的知识结构，不仅介绍各项技术的基本原

理、安全技术特点及其在物联网中的安全解决方案等，而且对该领域的最新前沿课题给予关注，为读者进一步的深入研究奠定基础。

本书配有教学课件，读者可登录华信教育资源网（www.hxedu.com.cn）免费注册后下载。

致谢

本书由施荣华、杨政宇编著，在编写过程中，作者参阅了国内外有关各种物联网安全技术的研究成果，具体内容已列在本书末尾的参考文献中。在此对所参阅文献和论文的作者表示衷心的感谢！

感谢中南大学信息科学与工程学院各位领导和老师对本书撰写的大力支持！王国才副教授为本书的内容组织及审阅付出了大量的心血，博士研究生樊翔宇，硕士研究生陈雷、雷田子、黄玲等人为本书的资料收集、录入、排版校对、绘图等做了大量的工作，在此一并表示感谢。

本书得以顺利出版，还要感谢电子工业出版社和本书责任编辑田宏峰先生的大力支持与辛勤工作。田宏峰编辑的热情高效、细致负责的工作方式给作者留下了深刻的印象。

由于作者水平有限，本书错误和疏漏之处在所难免，恳请读者提出宝贵意见和建议，以便再版时改进。联系邮箱：shirh@csu.edu.cn。

施荣华

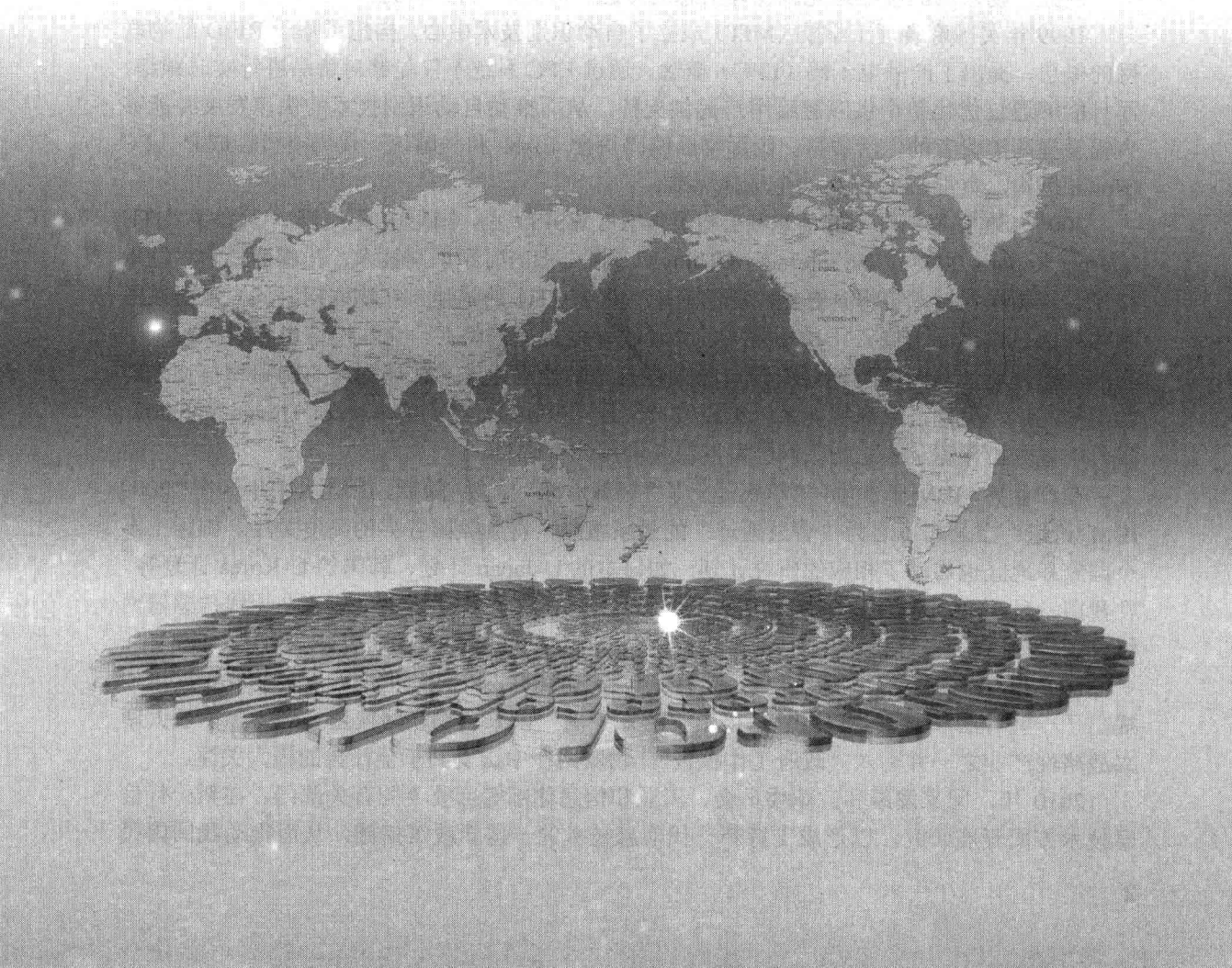
2013 年 6 月于长沙

目　录

CONTENTS

第1章

绪　论



1.1 物联网的概念

1.1.1 物联网的由来

物联网（Internet of Things，IoT）是通过射频识别（RFID）装置、红外感应器、全球定位系统、激光扫描器、传感器节点等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理等功能的一种网络。物联网的概念有两层含义：

（1）它是互联网、移动通信网和传感网等网络的融合，是在互联网基础之上的延伸和扩展的一种网络；

（2）其用户端延伸和扩展到了任何物品与物品之间，可进行信息交换和通信。

因此，物联网的核心是完成物体信息的可感、可知、可传和可控。

1999 年美国麻省理工学院（MIT）成立了自动识别技术中心，构想了基于 RFID 的物联网的概念，提出了产品电子码（EPC）概念。通过 EPC 系统不仅能够对货品进行实时跟踪，而且能够通过优化整个供应链给用户提供支持，从而推动自动识别技术的快速发展并能够大幅度提高消费者的生活质量。国际物品编码协会 EAN 和美国统一代码委员会成立 EPC Global 机构，负责 EPC 网络的全球化标准。

2005 年在突尼斯举行的信息社会世界峰会（WSIS）上，国际电联（ITU）发布了“ITU Internet Reports 2005：The Internet of Things”。报告指出射频识别技术、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。根据 ITU 的描述，在物联网时代，通过在各种各样的日常用品上嵌入一种短距离的移动收发器，人们将在信息与通信世界里获得一个新的沟通维度，从任何时间任何地点的人与人之间的沟通连接扩展到人与物和物与物之间的沟通连接。另外，欧洲智能系统集成技术平台（EPoSS）在“Internet of Things in 2020”报告中也分析预测了未来物联网的发展将要经历四个阶段。

在产业界，IBM 于 2008 年年底提出了“智慧地球”概念，随后，IBM 大中华区在“2009 IBM 论坛”上公布了名为“智慧地球”的最新策略，得到美国各界的高度关注。国际上多个国家和地区也启动了相应的研究计划，如日本的 U-Japan 计划、韩国的 U-Korea 计划等。在我国，早在 20 世纪 90 年末就开始了传感网的研究，特别是近十多年来在无线传感器网络方面，国内的高等院校、科研机构和相关企业都进行了较深入的研究，取得了一些成果。

2009 年 8 月温家宝总理在视察中国科学院无锡物联网产业研究所时，对物联网应用也提出了一些看法和要求。自温总理提出“感知中国”以来，物联网被正式列为国家五大新兴战略性产业之一并写入“政府工作报告”，物联网在中国受到了全社会的极大关注。

2010 年，国家发展和改革委员会、工业和信息化部等部委会同有关部门，在新一代信息技术方面开展研究，以形成支持新一代信息技术的一些新政策措施，从而推动我国国民

经济的发展。

时至今日，物联网概念的范畴与时俱进，已经超越了1999年MIT和2005年ITU报告所给出的范围，物联网的应用也拓展到智能家居、现代物流、军事应用、数字城市、公共安全、智能交通、智能农业等更多的领域。

1.1.2 物联网的定义

顾名思义，物联网就是“物物相连的网络”。物联网的最终目标是要将自然空间中的所有物体通过网络连接起来。物联网的核心和基础是网络，是在现有各种网络基础上延伸和扩展的网络，同时，在现实生活中的所有物体在物联网上都有对应的实体。可以说，最终的物联网就是虚拟的、数字化的现实物理空间（可参考电影《黑客帝国》想象）。国际电信联盟（International Telecommunication Union，ITU）在2005年的一份报告中曾描绘了“物联网”时代的场景：当司机出现操作失误时汽车会自动报警；公文包会提醒主人忘了带什么东西；衣服会“告诉”洗衣机对颜色和水温的要求等。

物联网本身是一个容易理解的概念，但由于其涉及现实世界的方方面面，尤其是温家宝总理发表了“感知中国”的讲话之后，各行各业都不约而同地发表了自己对物联网的理解。由于出发点和视角的差异，这些理解难免不一致，目前物联网的定义还没有完全统一，其普遍采用的定义是：利用二维码、无线射频识别（Radio Frequency Identification Devices，RFID）、红外感应器、全球定位系统（Global Position System，GPS）、激光扫描器等各种感知技术和设备，使任何物体与网络相连，全面获取现实世界中的各种信息，完成物与物、人与物的信息交互，以实现对物体的智能化识别、定位、跟踪、管理和控制。

从物联网本质来看，物联网是现代信息技术发展到一定阶段后出现的一种聚合性应用与技术提升，将各种感知技术、现代网络技术、人工智能和自动化技术聚合与集成应用，使人与物能智慧对话，创造一个智慧的世界。

物联网被称为继计算机和互联网之后，世界信息产业的第三次革命性创新。物联网一方面可以提高经济效益，大大降幅成本；另一方面可以为经济的发展提供技术推动力。物联网将把新一代信息技术充分运用到各行各业中，具体地说，就是要给现实世界的各种物体，包括建筑、家居、公路、铁路、桥梁、隧道、水利、农业、油气管道、供水及各种生产设备等装上传感器，并且将这些传感器通过有线/无线通信手段与核心网络连接起来，实现人类社会与物理世界的融合。同时网络上还将连接各种执行器，也就是说物联网不仅能感知世界，同时也能够控制世界。物联网的基础是实现网络融合，现有的互联网、电信网（包括移动通信系统）、广播电视网络首先要形成一个统一的“大网络”，即目前如火如荼的三网融合。物联网在融合大网络的基础上，能够对网络上的人员、机器设备和基础设施进行实时的管理和控制。在物联网时代，人类的日常生活将发生翻天覆地的变化。

物联网具备三个特点：一是全面感知，即利用RFID、传感器、二维码等随时随地获取物体的信息；二是可靠传输，通过各种电信网络与互联网的融合，将物体的信息实时准确

地传输出去；三是智能应用，利用云计算、模糊识别等各种智能计算技术，对天量（互联网中，人们常说海量数据，物联网的信息量比互联网大得多，因而本书将其称为天量数据）数据和信息进行分析和处理，对物体实施智能化的控制。

首先，它是各种感知技术的广泛应用。物联网上安置了海量的、多种类型的传感器，每个传感器都是一个信息源，不同类型的传感器所捕获的信息内容和信息格式不同。传感器获得的数据具有实时性，可按一定的频率周期性地采集环境信息，不断更新数据。

其次，它是一种建立在融合网络之上的泛在网络。物联网技术的重要基础和核心仍然是网络，即融合了互联网、电信网、广播电视网的新型网络，通过各种有线和无线接入手段与网络融合，将物体的信息实时、准确地传输出去。物联网上的传感器定时采集的信息需要通过网络传输，由于其数量极其庞大，形成了天量信息，在传输的过程中，为了保障数据的正确性和传输的及时性，必须适应各种异构网络和协议。

最后，物联网不仅仅提供了传感器的连接，其本身也具有智能处理和执行能力的器件，能够对物体实施智能控制。物联网将传感器和智能处理相结合，利用云计算、模式识别等各种智能技术，扩充其应用领域。从传感器获得的天量信息中分析、加工和处理出有意义的数据，以适应不同用户的不同需求，发现新的应用领域和应用模式。

物联网并不是凭空提出的概念，物联网本身是互联网的延伸和发展。目前，互联网已发展到空前高度，人们通过互联网了解世界十分便利。但随着认识的提高，人们对生活品质的要求越来越高，人们不再满足现有互联网这种人与人交互的模式，追求能够通过网络实现人与物的交互，甚至物与物的自动交互，不再需要人的参与。基于这些背景，以及技术的发展，物联网概念的提出水到渠成。物联网是在现有互联网的基础上，利用各种传感技术，构建一个覆盖世界上所有人与物的网络信息系统。人与人之间的信息交互和共享是互联网最基本的功能，而在物联网中，更强调的是人与物、物与物之间信息的自动交互和共享。

1.1.3 和物联网相近的概念

1. 无线传感器网络

无线传感器网络（Wireless Sensor Networks，WSN）是指“随机分布的集成有传感器、数据处理单元和通信单元的微小节点，通过自组织方式构成的无线网络”。无线传感器网络由大量无线传感器节点组成，每个节点由数据采集模块、数据处理模块、通信模块和能量模块构成，其中数据采集模块主要是各种传感器和相应的 A/D 转换器，数据处理模块包括微处理器和存储器，通信模块主要是无线收发器，无线传感器网络节点一般采用电池供电。无线网络传感器网络技术是物联网最重要的技术之一，也是物联网与现有互联网区别所在的主要因素之一，可广泛应用于军事、国家安全、环境科学、交通管理、灾害预测、医疗卫生、制造业、城市信息化建设等多个领域。

2. 泛在网

泛在网（Ubiquitous Network）又被称为无所不在的网络。泛在网概念的提出比物联网要早一些，国际上对其的研究已有相当长的时间，也得到了美、欧在内的世界各个国家和地区的广泛关注。泛在网将 4A 作为其主要特征，即在任何时间（Anytime）、任何地点（Anywhere）、任何人（Anyone）、任何物（Anything）都能方便地进行通信。泛在网内涵更多以人为核心，关注可以随时随地获取各种信息，几乎包含了目前所有网络概念和研究范畴。

3. M2M

M2M 即 Machine to Machine，指机器到机器的通信，也包括人对机器和机器对人的通信。M2M 是从通信对象的角度出发表述的一种信息交流方式，它通过综合运用自动控制、信息通信、智能处理等技术，实现设备的自动化数据采集、数据传输、数据处理和设备自动控制，是不同类型通信技术的综合运用，能让机器、设备、应用处理过程与后台信息系统共享信息，并与操作者共享信息。M2M 是物联网的雏形，是现代物联网应用的主要表现。

4. 信息物理系统

信息物理系统（Cyber Physical Systems，CPS）是美国自然基金会于 2005 年提出的研究计划。CPS 是“人、机、物”深度融合的系统，它在物与物互连的基础上，强调对物实时、动态的信息控制盒信息服务。CPS 试图克服已有传感网各个系统自成一体、计算设备单一、缺乏开发性等缺点，更注重多个系统间的互连互通，并采用标准的互连互通的协议和解决方案，同时强调充分运用互联网，真正实现开发的、动态的、可控的、闭环的计算和服务支持。CPS 概念和物联网的概念类似，只是目前的物联网更侧重于感知世界。

物联网与传感网、M2M、泛在网、互联网、移动网的相互关系如图 1-1 所示。

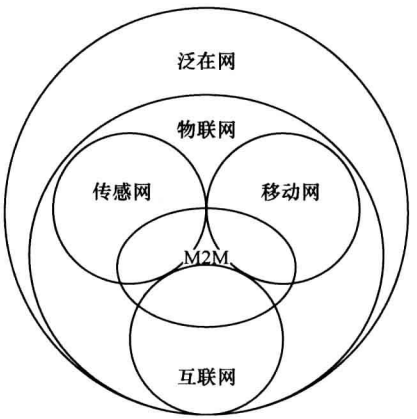


图 1-1 物联网与泛在网、M2M、传感网、互联网、移动网的相互关系