物联网关键技术及系统应用

第2版

张鸿涛　徐连明　刘臻　等编著

机械工业出版社
CHINA MACHINE PRESS

物联网关键技术及系统应用

第 2 版

张鸿涛　徐连明　刘　臻　等编著

机 械 工 业 出 版 社

本书系统地介绍了物联网的概念、3 层架构、实现技术及典型应用，首先讨论了物联网的背景、特点、架构、标准及产业链等；其次介绍了感知层技术，包括 EPC 技术、RFID 技术、传感器技术、短距离无线通信技术等；然后按照汇聚网→接入网→承载网路线展开阐述了物联网传输层技术；接着论述了物联网应用层技术，包括中间件技术、智能技术、大数据、数据挖掘、云计算、联网安全架构及策略等；最后介绍了物联网的典型行业应用。

本书是一部紧跟物联网技术前沿研究的专业性著作，主要适合物联网领域的研究人员和工程技术人员阅读，也可以作为通信工程及相关专业的高年级本科生、研究生和教师的专业性新技术参考书。

图书在版编目（CIP）数据

物联网关键技术及系统应用/张鸿涛等编著. —2 版. —北京：机械工业出版社，2016. 12

ISBN 978-7-111-55124-9

Ⅰ. ①物… Ⅱ. ①张… Ⅲ. ①互联网络 - 应用②智能技术 - 应用 Ⅳ. ①TP393. 4②TP18

中国版本图书馆 CIP 数据核字（2016）第 246421 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：朱 林 责任编辑：朱 林

封面设计：路恩中 责任校对：杜雨霏

责任印制：李 飞

北京玥实印刷有限公司印刷

2017 年 1 月第 2 版第 1 次印刷

184mm × 260mm · 16. 25 印张 · 390 千字

0001— 3000册

标准书号：ISBN 978-7-111-55124-9

定价： 49.00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 网络服务

服务咨询热线：010-88361066 机 工 官 网：www. cmpbook. com

读者购书热线：010-68326294 机 工 官 博：weibo. com/cmp1952

010-88379203 金 书 网：www. golden-book. com

封面无防伪标均为盗版 教育服务网：www. cmpedu. com

第 2 版前言

随着经济与科学技术的高速发展，物联网技术对于提高生产发展和生活质量起到了越来越重要的促进作用。物联网的推广将会成为推进经济发展的驱动器，为产业开拓潜在的发展机会。2010 年，国家发展和改革委员会及工业和信息化部出台了支持物联网产业化发展的一系列政策，2016 年李克强总理在政府工作报告中提出，在“十三五”期间要促进大数据、云计算、物联网广泛应用。数据显示，2015 年我国物联网整体市场规模高达 7500 亿元。新兴的物联网产业正在逐渐占据我国各地区战略性发展的关键领域。

由于科技发展的日新月异，物联网在短短几年内也具有长足的发展，物联网的应用已经体现在生活和生产的方方面面，这些应用和技术较之几年前已经发生了巨大的变化，本书根据物联网近来的热点和发展趋势，对第 1 版中的一些章节内容进行了增删和修改，旨在跟上时代的脚步，为后续更多研究者提供参考，并希望能对其有所启发和帮助。

本书介绍的物联网基本结构没有发生变化，主要分为 3 层：感知层、传输层和应用层。感知层处于 3 层架构的最底层，是物联网的实现基础。感知层实现对物体的感知，感知层在物联网中，如同人的感觉器官对人体系统的作用，用来感知外界环境的温度、湿度、压强、光照、气压、受力情况等信息，通过采集这些信息来识别物体。传输层所要完成的功能是将感知层搜集感知的数据信息传输给应用层，使得应用层可以方便地对信息进行分析管理，从而控制整个系统。目前，物联网传输层都是基于现有的通信网和互联网建立的，主要实现感知层数据和控制信息的双向传递、路由和控制。物联网应用层主要将物联网技术与行业专业系统相结合，感知数据处理封装，以服务的方式提供给用户，实现广泛的物物互联的应用解决方案。

本书分为 5 部分：第一部分（第 1 章）是物联网背景知识介绍，包括物联网的背景、特点、架构、标准及产业链等。第二部分（第 2 章）对物联网的感知层技术进行了介绍，包括资源寻址、EPC 技术、RFID、传感器技术、无线传感器网络技术等。第三部分（第 3 ~ 5 章）按照汇聚网→接入网→承载网路线展开阐述了物联网传输层技术。其中第 3 章论述了汇聚网，即主要采用短距离通信技术（如 ZigBee、蓝牙和 UWB 等技术），实现小范围感知数据的汇聚，其中第 2 版中增加了对低功耗蓝牙及 Bluetooth 4.0 协议的介绍。第 4 章论述了接入网，主要采用 6LoWPAN、M2M 及全 IP 融合架构等实现感知数据从汇聚网到承载网的接入。第 5 章论述了承载网的发展阶段及各阶段的承载方式。第四部分（第 6 ~ 8 章）论述了物联网应用层技术。其中第 6 章论述了应用层支撑技术，包括中间件技术、对象名称解析服务、实体标记语言、智能技术和云计算等技术，第 2 版中加入了物联网中的大数据和数据挖掘技术的应用。第 7 章论述了物联网业务系统及电信运营商的发展策略。第 8 章论述了物联网安全架构及策略，新增了物联网 3 层中关键技术的具体安全策略的实现。第五部分（第 9 章）内容全部进行了更新，介

绍了近年来物联网行业中新兴的热门应用，是对前几章物联网技术的实现，可以帮助读者更好地理解物联网的内涵。

本书作者长期从事移动通信网络和物联网研究工作，具有丰富的理论基础和实践经验。本书主要由北京邮电大学张鸿涛（国家自然科学基金61302090项目负责人）、徐连明和中国信息通信研究院刘臻编著，牛沐楚、杨梓华、孟娜等参与了部分编写工作。全书由张鸿涛、徐连明统编定稿。最后，还要感谢机械工业出版社的大力支持和高效工作，使本书能尽早与读者见面。

由于物联网技术的日新月异，在编写过程中尽管我们力求精益求精，及时吸纳最新的物联网研究成果和技术，但由于作者理论水平和时间所限，疏漏错误之处在所难免，敬请读者原谅和指正。

作　者

于北京邮电大学

2016年8月

第 1 版前言

物联网为我们展示了生活中任何物品都可以变得“有感觉、有思想”的智能图景，是世界下一次信息技术浪潮和新经济引擎。在我国，物联网已经成为国家发展战略，并且初步明确了未来发展方向和重点领域。相关部门正在着手制定相关财政、金融政策和法规以确保物联网发展体制的有效性。我国企业正在随着国家的快速发展，持续提升竞争力和国际影响力，对物联网的需求逐步呈现。企业对信息化方面的认知提高，经济支付能力也将增强。

物联网的发展离不开相关技术的发展，技术的发展是物联网发展的重要基础和保障。物联网的整体架构分为 3 层：感知层、传输层和应用层。感知层处于 3 层架构的最底层，是物联网的实现基础。感知层实现对物体的感知，在物联网中，如同人的感觉器官对人体系统的作用，用来感知外界环境的温度、湿度、压强、光照、气压、受力情况等信息，通过采集这些信息来识别物体。传输层所要完成的功能是将感知层收集感知的数据信息传输给应用层，使得应用层可以方便地对信息进行分析管理，从而控制整个系统。目前，物联网传输层都是基于现有的通信网和互联网建立的，主要实现感知层数据和控制信息的双向传递、路由和控制。物联网应用层主要将物联网技术与行业专业系统相结合，感知数据处理封装，以服务的方式提供给用户，实现广泛的物物互联的应用解决方案。

本书分为 5 部分：第一部分（第 1 章）是物联网背景知识介绍，包括物联网背景、特点、架构、标准及产业链等。第二部分（第 2 章）对物联网的感知层技术进行介绍，包括资源寻址、EPC 技术、RFID、传感器技术、无线传感器网络技术等。第三部分（第 3 ~ 5 章）按照汇聚网→接入网→承载网路线展开阐述物联网传输层技术，其中第 3 章论述了汇聚网，即主要采用短距离通信技术如 ZigBee、蓝牙和 UWB 等技术，实现小范围感知数据的汇聚，第 4 章论述接入网，主要采用 6LoWPAN、M2M 及全 IP 融合架构等实现感知数据从汇聚网到承载网的接入，第 5 章论述承载网的发展阶段及各阶段的承载方式。第四部分（第 6 ~ 8 章）论述物联网应用层技术。其中第 6 章论述应用层支撑技术包括中间件技术、对象名称解析服务、实体标记语言、智能技术和云计算等技术，第 7 章论述物联网业务系统及电信运营商的发展策略；第 8 章论述物联网安全架构及策略。第五部分（第 9 章）介绍了物联网的典型行业应用。

本书作者长期从事移动通信网络和物联网研究工作，具有丰富的理论基础和实践经验。本书由北京邮电大学张鸿涛、徐连明、张一文和宋振峰编著。全书由张鸿涛、徐连明统编定稿。最后，还要感谢机械工业出版社的大力支持和高效工作，使本书能尽早与

读者见面。

由于物联网技术的日新月异，在编撰过程中尽管我们力求精益求精，及时吸纳最新的物联网研究成果和技术，但由于作者理论水平和时间所限，疏漏错误之处在所难免，敬请读者原谅和指正。

作　者
于北京邮电大学
2011年6月

目　录

第1章 绪 论

太阳渐渐升起来了，温度也开始升高了，房屋里的光传感器和温度传感器感受到世界微妙的变化；7点钟你房间的窗帘自动拉开，天花板上显示着今天的天气情况和衣着建议。床头的电子提示器告诉你昨晚的睡眠质量和目前各项身体指标并将这些身体信息发送给你的私人医生。

衣柜前的显示屏已经根据今天的天气情况给出了3套服装搭配方案，你选择自己最喜欢的一种。在你穿衣服的时候，洗漱室的水已经调整到你设定的温度，你出门锻炼时，选择了离开模式，家门自动运行到“主人离家状态”。带有智能传感器的手表一路跟踪显示你运动消耗的热量、跑步速度、呼吸频率、脉搏等信息。30min之后，自动提示你运动任务已完成。你回到家中依靠指纹识别系统开门，灯光自动打开。

打开冰箱，按照智能冰箱提供的健康绿色的食谱做好早饭。吃完早饭，开车去公司上班。走到车库门口，车库自动感应到主人，库门、车门也自动开启，在确认了你的目的地之后，汽车提供了一套参考行车路线，行车过程中不断与道路对话，感知拥堵并不断更换最佳行车路线；汽车同时通过与其他车进行对话，感知车距以避免事故。你在车内听着当日新闻，并且通过手机查看了办公室的状态，发送了自己将要到达的信息。

当你到达公司大厅的时候，今天的工作日程早已发送到了你的手机中，你走进办公室，秘书送来了温度适宜的咖啡。美好的一天就这样拉开了序幕……

这一切看似像科幻小说中才有的场景，在物联网（Internet of Things）时代都将变成现实。

今天，物联网已经成为一个社会各界关注研究的热点问题。随着互联网的普及，借助网络，人与人之间已经能够完成跨越空间的交流互通，物联网所要做的是将我们身边的每一件物体也连入网中，实现物与物之间的交互。“物联网”是继计算机、互联网与移动通信网之后的第三次信息浪潮，通信网之后的世界信息产业的又一次创举。世界各国都非常重视物联网技术。

物联网顾名思义，就是“物物相连的网络”。实现物物相连的核心和基础仍然是目前存在的各种各样的网络，包括互联网、通信网等，物联网是在现有各种网络基础上进行延伸和扩展形成的功能更加强大的网络；网络功能延伸和完善后使得用户端扩展到了物体上，让任何物体都能够进行信息交换和通信。

物联网是一个未来网络的部分，它可以被定义为一个动态的全球网络架构，具有依据标准和互操作通信协议的自配置功能，定义了物理和虚拟的“物体”。在物联网中，物理实体、虚拟个体、智能交互界面被无缝接入到信息网络之中。

在物联网中，“物体”可以灵活地参与商业、信息和社会财产活动，它们可以互相通信，也可以通过互相交换环境感应的数据和信息与周围环境进行互动，并对环境的改变自动做出相应的反应。

如今，全世界科技的快速发展使得物联网能有更进一步的发展，通过嵌入小范围的移动

传输设备，让指定范围中的物体连接到网络中，实现人与物、物与物之间的通信。一个新的维数已经建立，如图 1-1 所示，在任何时间、任何地点、任何人都可以与任何物体建立连接。

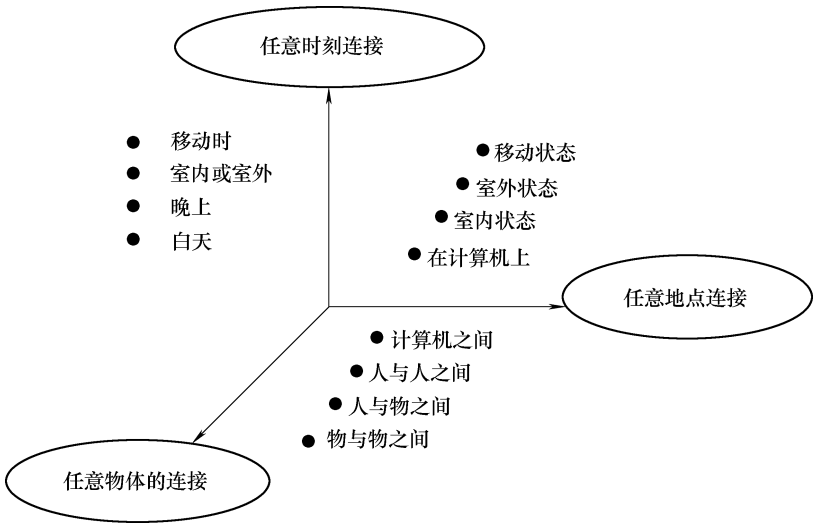


图 1-1　物联网的新维度

与其说物联网是网络，不如说物联网是业务和应用，物联网也被视为互联网的应用拓展。

1.1　物联网的定义

物联网（Internet of Things）这个词，国内外普遍公认的是 MIT Auto-ID（美国麻省理工学院自动识别中心）Ashton 教授 1999 年在研究 RFID 时最早提出来的。在 2005 年国际电信联盟（ITU）发布的同名报告中，物联网的定义和范围已经发生了变化，覆盖范围也有了较大的拓展，不再只是指基于 RFID 技术的物联网。

物联网是指通过传感器、射频识别技术、全球定位系统等技术，实时采集任何需要监控、连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各种可能的网络接入，实现物与物、物与人的泛在链接，实现对物品和过程的智能化感知、识别和管理。

物联网中的“物”能够被纳入“物联网”的范围是因为它们具有接收信息的接收器；具有数据传输通路；有的物体需要有一定的存储功能或者相应的操作系统；部分专用物联网中的物体有专门的应用程序；可以发送接收数据；传输数据时遵循物联网的通信协议；物体接入网络中需要具有世界网络中可被识别的唯一编号。

物联网通俗地讲是指将无处不在的末端设备和设施，如贴上 RFID 的各种资产、携带无线终端的个人与车辆等“智能化物件或动物”或“智能尘埃”，通过各种无线和/或有线的长距离和/或短距离通信网络实现互连互通（M2M）、应用大集成以及基于云计算的 SaaS 营运等模式，在内网（Intranet）、专网（Extranet）和/或互联网（Internet）环境下，采用适当的信息安

全保障机制实现对“万物”的“高效、节能、安全、环保”的“管、控、营”一体化。

2009 年 9 月，在北京举办的物联网与企业环境中欧研讨会上，欧盟委员会信息和社会媒体司 RFID 部门负责人 Lorent Ferderix 博士给出了欧盟对物联网的定义：物联网是一个动态的全球网络基础设施，它具有基于标准和互操作通信协议的自组织能力，其中物理的和虚拟的“物”具有身份标识、物理属性、虚拟的特性和智能的接口，并与信息网络无缝整合。物联网将与媒体互联网、服务互联网和企业互联网共同构成未来互联网。

1.2 物联网的特点

物联网具有全面感知、可靠传输、智能处理三大特点，如图 1-2 所示。

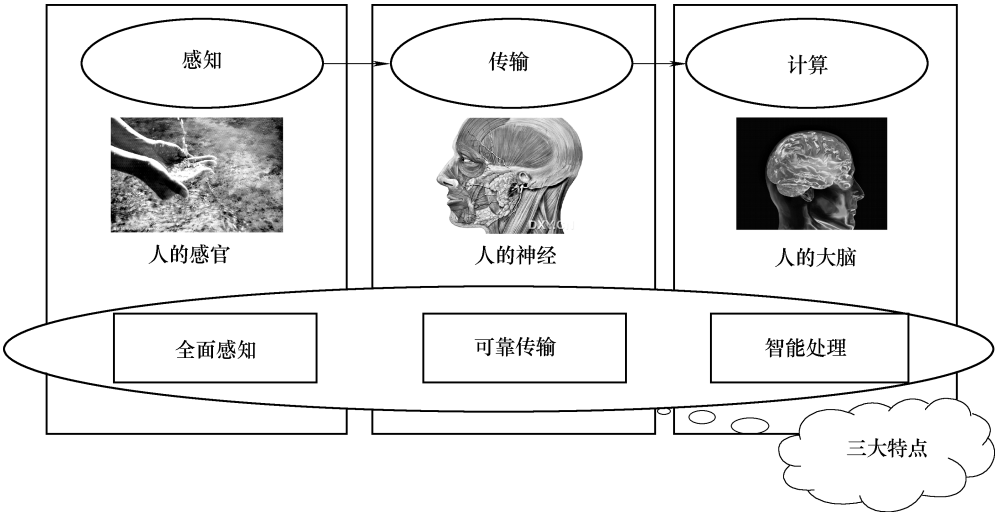


图 1-2 物联网的三大特点

物联网要将大量物体接入网络并进行通信活动，对各物体的全面感知是十分重要的。全面感知是指物联网随时随地获取物体的信息。要获取物体所处环境的温度、湿度、位置、运动速度等信息，就需要物联网能够全面感知物体的各种需要考虑的状态。全面感知就像人身体系统中的感觉器官，眼睛收集各种图像信息，耳朵收集各种音频信息，皮肤感觉外界温度等。所有器官共同工作，才能够对人所处的环境条件进行准确的感知。物联网中各种不同的传感器如同人体的各种器官，对外界环境进行感知。物联网通过 RFID、传感器、二维码等感知设备对物体各种信息进行感知获取。

可靠传输对整个网络的高效正确运行起到了很重要的作用，是物联网的一项重要特征。可靠传输是指物联网通过对无线网络与互联网的融合，将物体的信息实时准确地传递给用户。获取信息是为了对信息进行分析处理从而进行相应的操作控制，将获取的信息可靠地传输给信息处理方。可靠传输在人体系统中相当于神经系统，把各器官收集到的各种不同信息进行传输，传输到大脑中方便人脑做出正确的指示。同样也将大脑做出的指示传递给各个部位进行相应的改变和动作。

在物联网系统中，智能处理部分将收集来的数据进行处理运算，然后做出相应的决策，

来指导系统进行相应的改变，它是物联网应用实施的核心。智能处理指利用各种人工智能、云计算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与控制。智能处理相当于人的大脑，根据神经系统传递来的各种信号做出决策，指导相应器官进行活动。

1.3　物联网的背景

1999 年美国麻省理工学院（MIT）成立的自动识别技术中心，提出了基于 RFID 的物联网的概念。

2005 年 11 月 17 日，在突尼斯举行的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布《ITU 互联网报告 2005：物联网》。报告指出，无所不在的“物联网”通信时代即将来临，世界上所有的物体从轮胎到牙刷、从房屋到纸巾都可以通过互联网主动进行信息交换。射频识别技术（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。

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，人类在信息与通信世界里将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、物与物之间的沟通连接。物联网概念的兴起，很大程度上得益于国际电信联盟 2005 年以物联网为标题的年度互联网报告。

随着物联网的提出，世界各国均提出了自己的发展策略。2004 年日本提出u-Japan 构想，并且表示希望建设成一个“Anytime，Anywhere，Anything，Anyone”都可以上网的环境。同年，韩国政府制定了 u-Korea 战略，为呼应 u-Korea 这一战略，韩国信通部发布《数字时代的人本主义：IT839 战略》。

2009 年 1 月，IBM 首席执行官彭明盛提出“智慧地球”构想，其中物联网为“智慧地球”不可或缺的一部分，而美国总统奥巴马在就职演讲后已对“智慧地球”构想提出积极回应，并提升到国家级发展战略。

2009 年 11 月，欧盟提出《欧盟物联网行动计划》，制定了一系列物联网管理规则，建立了有效的分布式管理架构，涉及药品、能源、物流、制造、零售等行业。

在我国，2009 年 8 月，温家宝总理访问中科院无锡高新微纳传感网工程技术研发中心时，提出“要在激烈的国际竞争中，迅速建立中国的传感信息中心，或者叫‘感知中国中心’”。同年 11 月 3 日，在《让科技引领中国可持续发展》的讲话中，温家宝总理再次提出：要着力突破传感网、物联网关键技术，及早部署后 IP 时代相关技术研发，使信息网络产业成为推动产业升级、迈向信息社会的“发动机”。在 2011 政府工作报告中，温家宝总理再次提出，要加快构建现代产业体系，推动产业转型升级，要加快培育发展战略性新兴产业。积极发展新一代信息技术产业，促进物联网示范应用。

“感知中国”是中国发展物联网的一种形象称呼，就是中国的物联网。通过在物体上植入各种微型感应芯片使其智能化，然后借助无线网络，实现人和物体之间“对话”，物体和物体之间的“交流”。全国各地在最近几年纷纷开展关于物联网的一系列建设。

2009 年 11 月 1 日，北京 40 余家物联网产业相关企业和大学、科研院所等发起成立中关村物联网产业联盟，半年时间内就在应用示范、产业研究、产业促进等方面取得了显著效果。继中关村物联网产业联盟“呱呱坠地”之后，北京物联网产业界在加速跑中又有新突

破：2010 年 7 月 9 日，北京物联网关键应用技术工程研究中心揭牌成立，中心旨在通过“强强联合”，力求形成“产、学、研、用”一体的产业链合作创新机制，在物联网的关键应用领域实现技术创新突破。这标志着中关村物联网产业联盟成员间的合作进入新的阶段，同时也为政府加快推动物联网产业发展提供了着力点。北京是物联网高端研发和应用的聚集区，近年来在北京奥运会、国庆 60 周年等多层面、多领域积极探索利用物联网技术，实现多项成功示范应用。

2010 年 5 月，江苏省公布了《江苏省物联网产业发展规划纲要（2009—2012 年）》，提出发展物联网产业要“举全省之力”。以举省发展一大产业，使得物联网产业地位迅速提高，超越了经济发展方式转变中的其他五大战略性新兴产业。江苏力争用 3 ~ 6 年左右的时间，建设成为物联网领域技术、产业、应用的先导省。江苏省把传感网列为全省重点培育和发展的六大新兴产业之一，并提出“要努力突破核心技术，加快建立产业基地”。江苏发展物联网按照“一个产业核心区、两个产业支撑区、全省应用示范先行区”的发展思路进行。其中，以无锡为产业核心区，苏州、南京为产业支撑区，构筑物联网产业基地，并面向全省建设应用示范先行区。

2010 年 11 月 8 日，上海物联网产业联盟正式宣布成立。该联盟整合与协调物联网产业，提升联盟内感知、传输、网络、集成、应用等企业的研究开发和生产制造，促进物联网产业快速健康发展，在上海市场以及将来在全国市场的推广；发布《上海市促进电子商务发展规定》，依托信息技术，加快实现制造业与物流业的对接联动；以“物联网”建设为重点，推进 RFID、GPS、GIS、无线测控、数字集群、传感网络等技术在“物联网”中的应用。

2011 年 4 月 21 日，重庆市 28 家物联网相关企业、单位和大专院校组建成立重庆物联网产业发展联盟，为重庆物联网发展“铺路架桥”，以便在 2015 年实现产出 1500 亿元的目标。近年来，重庆围绕物联网产业的发展做了大量工作，并已取得了初步成效，比如中国移动物联网基地、中国物联网基地已相继落户重庆，重庆市政府出台了《重庆市人民政府关于加快推进物联网发展的意见》。

广东省积极参与物联网国家标准的制定，推进 RFID 技术应用和产业发展，加强粤港 RFID 应用合作，促进粤港澳物流业务融合和通关便利化，同时计划 5 年构建物联网数字家园。2011 年 4 月广东省物联网应用产业基地盛大启动，这将加快射频识别、传感器、云计算等物联网关键技术的研究和引进。随之推动智慧家具商贸、家电全生命周期管理平台、大宗物流配送等重点工程建设，最终推进物联网发展。

物联网为我们展示了生活中任何物品都可以变得“有感觉、有思想”的智能图景，是世界下一次信息技术浪潮和新经济引擎。在我国，物联网已经成为国家发展战略，并且初步明确了未来的发展方向和重点领域。相关部门正在着手制定相关财政、金融政策和法规以确保物联网发展体制的有效性。我国企业正在随着国家的快速发展，持续提升竞争力和国际影响力，对物联网的需求逐步呈现。企业对信息化方面的认知提高，经济支付能力也将增强。

1.4 物联网的现状

随着传感器技术的不断发展，传感器的种类越来越多，传感器现在正向着智能化、微型

化、多功能化发展。微型传感器可以用来测量各种物理量、化学量和生物量，如位移、速度/加速度、压力、应力、应变、声、光、电、磁、热、pH 值、离子浓度及生物分子浓度等，已经对大量不同应用领域，如航空、远距离探测、医疗及工业自动化等领域的信号探测系统产生了深远影响。智能化传感器技术也处于蓬勃发展时期，智能变送器和二维加速度传感器以及另外一些含有微处理器（MCU）的单片集成压力传感器、具有多维检测能力的智能传感器和固体图像传感器（SSIS）等相继面世。与此同时，基于模糊理论的新型智能传感器和神经网络技术在智能化传感器系统的研究和发展中的重要作用也日益受到了相关研究人员的重视。现在感知层技术已经能满足大部分应用，目前的应用是短距离为主，基本实现了嵌入式，但是目前感知层技术大部分功耗比较大，有待改进。

作为物联网发展的排头兵，RFID 技术成为了市场最为关注的技术。经过几年的发展，RFID 技术的发展也是相当迅速的。在很多关键技术点上，RFID 已日趋成熟，尤其表现在阅读器识读距离的提高、标签和识读器之间数据交互稳定性的提高，以及与无线通信技术结合等多个方面。目前 RFID 的工作频率已经从低频（30～300kHz）和高频（3～30MHz）发展到超高频、2.4GHz 微波频率。超高频的读写设备分为手持式和固定式两种，手持式识读距离在 4m 左右，而固定式识读距离则可达 15m 左右；2.4GHz 微波的距离则可达到 70～80m，甚至是 3km。

目前，物联网传输都是基于现有的通信网和互联网建立的，包括无线传输和有线传输。主要实现感知层数据和控制信息的双向传递、路由和控制。现在随着通信网和互联网的高速发展，各种传输技术层出不穷。相继出现了 6LoWPAN、ZigBee、Bluetooth、UWB 等技术。有了众多新技术的支持，针对不同系统的要求找到合适的传输方式不再是难题。

物联网采用中间件、智能技术、云计算等支撑技术来处理信息和辅助决策。

目前存在的中间件有很多种类，如通用中间件、嵌入式中间件、数字电视中间件、RFID 中间件和 M2M 物联网中间件等，中间件无处不在。IBM、Oracle、微软等公司都是引领潮流的中间件生产商。SAP 等大型（ERP）应用软件厂商的产品也是基于中间件架构的。国内的用友、金蝶等软件厂商也都有中间件部门或分公司。物联网产业的发展为物联网中间件的发展提供了新的机遇。欧盟 Hydra 物联网中间件 OSGi Alliance 是一个由 Sun Microsystems、IBM、爱立信等于 1999 年成立的开放软件标准化组织，最初名为 Connected Alliance。OSGi 中间件技术架构基于 Java，OSGi 的应用包括服务网关、汽车、移动电话、工业自动化、建筑物自动化、PDA 等许多物联网相关领域。

物联网智能是利用人工智能技术服务于物联网络的技术，是将人工智能的理论方法和技术通过具有智能处理功能的软件部署在网络服务器中去，服务于接入物联网的物品设备和人。物联网智能化也要研究解决 3 个层次的问题：网络思维，具体讲是网络思维、网络学习、网络诊断等；网络感知，让网络像人一样能感觉到气味、颜色、触觉；网络行为，研究网络模拟、延伸和扩展人的智能行为（例如智能监测、智能控制等行为）。

云计算是物联网平台的关键技术，它是由分布式计算、并行处理、网格计算发展来的，是一种新兴的计算模型。目前，对于云计算的认识在不断发展变化。云计算的“云”就是存在于互联网上的服务器集群上的资源，它包括硬件资源（如服务器、存储器、CPU 等）和软件资源（如应用软件、集成开发环境等），本地计算机只需要通过互联网发送一个需求信息，远端就会有成千上万的计算机为你提供需要的资源并将结果返回到本地，所有的处理

都由云计算提供商所提供的计算机群来完成。云计算将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。这使得应用提供者无需为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

1.5 物联网的基本架构

目前公认的物联网架构分为3层：感知层、传输层和应用层，如图1-3所示。

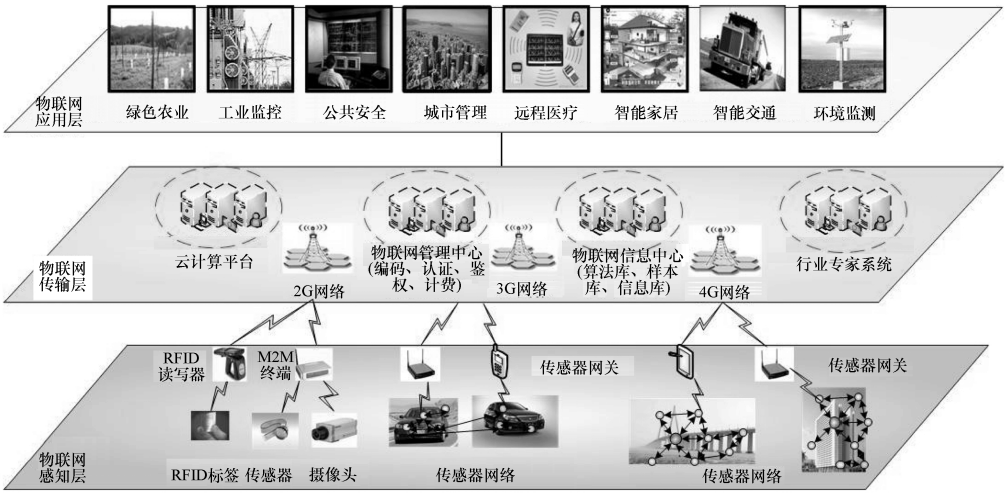


图1-3 物联网基本架构

1.5.1 感知层

感知层在物联网中，如同人的感觉器官对人体系统的作用，用来感知外界环境的温度、湿度、压强、光照、气压、受力情况等信息，通过采集这些信息来识别物体。感知层包括传感器、RFID、EPC等数据采集设备，也包括在数据传送到接入网关之前的小型数据处理设备和传感器网络。感知层主要实现物理世界信息的采集、自动识别和智能控制。感知层是物联网发展的关键环节和基础部分。作为物联网应用和发展的基础，感知层涉及的主要技术包括RFID技术、传感和控制技术、短距离无线通信技术以及对应的RFID天线阅读器研究、传感器材料技术、短距离无线通信协议、芯片开发和智能传感器节点等。

作为一种比较廉价实用的技术，一维条码和二维条码在今后一段时间还会在各个行业中得到一定应用。然而，条形码表示的信息是有限的，而且在使用过程中需要用扫描器以一定的方向近距离地进行扫描，这对于未来物联网中动态、快读、大数据量以及有一定距离要求的数据采集、自动身份识别等有很大的限制，因此基于无线技术的射频标签发挥了越来越重要的作用。

传感器作为一种有效的数据采集设备，在物联网感知层中扮演了重要角色。现在传感器的种类不断增多，出现了智能化传感器、小型化传感器、多功能传感器等新技术传感器。基于传感器而建的传感器网络也是目前物联网发展的一个大方向。

1.5.2 传输层

传输层相当于人的神经系统。神经系统将感觉器官获得的信息传递到大脑进行处理，传输层将感知层获取的各种不同信息传递到处理中心进行处理，使得物联网能从容应对各种复杂的环境条件，这就是各种不同的应用。目前物联网传输层都是基于现有的通信网和互联网建立的，包括各种无线、有线网关、接入网和核心网，主要实现感知层数据和控制信息的双向传递、路由和控制。通过对有线传输系统和无线传输系统的综合使用，结合6LoWPAN、ZigBee、Bluetooth、UWB等技术实现以数据为中心的数据管理和处理，也就是实现对数据的存储、查询、挖掘、分析以及针对不同应用的数据决策和分析。

物联网传输层技术主要是基于通信网和互联网的传输技术，传输方式分有线传输和无线传输。这两种通信方式对物联网产业来说处于同等重要、互相补充的作用。

有线通信技术可分为中、长距离的广域网络（包括PSTN、ADSL和HFC数字电视Cable等），短距离的现场总线（Field Bus，也包括电力线载波等技术）。

无线通信也可分为长距离的无线广域网（WWAN），中、短距离的无线局域网（WLAN），超短距离的WPAN（Wireless Personal Area Network，无线个域网）。

传感网主要由WLAN或WPAN技术作为支撑，同时结合了传感器技术。“传感器”和“传感网”二合一的RFID的传输部分也是属于WPAN或WLAN。

移动通信经历了1G、2G、3G时代，各自的代表性技术为GSM、CDMA2000、WCDMA、TD-SCDMA等，这些技术在物联网中被广泛应用。

1.5.3 应用层

物联网把周围世界中的人和物都联系在网络中，应用涉及广泛，应用包括家居、医疗、城市、环保、交通、农业、物流等方面。交通方面涉及面向公共交通工具、基于个人标识自动缴费的移动购票系统，环境监测系统以及电子导航地图；医疗方面涉及医疗对象的跟踪、身份标识和验证、身体症状感知以及数据采集系统；工控与智能楼宇方面涉及舒适的家庭/办公环境的智能控制、工厂的智能控制、博物馆和体育馆的智能控制应用；基于位置的服务方面涉及人与人之间实时交互网络、物品轨迹或人的行踪的历史查询、遗失物品查找以及防盗等应用。

物联网应用涉及行业众多，涵盖面宽泛，总体可分为身份相关应用、信息汇聚型应用、协同感知类应用和泛在服务应用。物联网通过人工智能、中间件、云计算等技术，为不同行业提供应用方案。

1.6 物联网技术

物联网的发展离不开相关技术的发展，技术的发展是物联网发展的重要基础和保障。

感知层是物联网发展的关键环节和基础部分。感知层涉及的主要技术包括资源寻址与EPC技术、RFID技术、传感技术、无线传感网技术等。EPC技术解决物品的编码标准问题，使得所有物联网中的物体都有统一的ID。RFID技术解决物品标识问题，可以快速识别物体，并获取其属性信息。传感器完成的任务是感知信息的采集。无线传感器网络完成了信息

的获取和上传，实现无线短距离通信。通过这些技术，实现物体的标识与感知，为物联网的应用和发展提供基础。

物联网传输层可分为汇聚网、接入网和承载网3部分。汇聚网关键技术主要是短距离通信技术，如ZigBee、蓝牙和UWB等技术。接入网主要采用6LoWPAN、M2M及全IP融合架构实现感知数据从汇聚网到承载网的接入。承载网主要是指各种核心承载网络，如GSM、GPRS、WiMax，3G/4G、WLAN、三网融合等。

物联网应用层关键技术包括中间件技术、对象名称解析服务、嵌入式智能、云计算、物联网业务平台及安全等技术。物联网中间件处于物联网的集成服务器端和感知层、传输层的嵌入式设备中，对感知数据进行校对、过滤、汇集，有效地减少发送到应用程序的数据的冗余度，在物联网中起着很重要的作用。对象名称解析服务是联系前台中间件软件和后台服务器的网络枢纽，将EPC关联到这些物品相关的物联网资源。云计算技术是构建物联网运营平台的关键技术，云计算是基于网络将计算任务分布在大量计算机构成的资源池上，使用户能够借助网络按需获取计算力、存储空间和信息服务。物联网业务平台主要针对物联网不同业务，研究其系统模型、体系架构等关键技术。随着物联网发展进入物物互联阶段，由于其设备数量庞大、复杂多元、缺少有效监控、节点资源有限、结构动态离散，安全问题日渐突出，除面对互联网和移动通信网络的传统网络安全挑战之外，还存在着一些特殊安全挑战。

1.7 物联网标准

由于物联网整体架构涉及的层面较多，因此涉及的技术也较多，比如包括传感技术、嵌入式智能技术、纳米技术、识别技术、发现技术、计算技术、网络通信技术、软件技术等。相关的技术组织和标准也非常繁杂。但总体来看，主要的物联网标准组织可以分为以下几类：

（1）总体框架类

如ITU-T SG 13以及ETSI M2M TC，主要对需求、架构、安全、编号等进行总体规范。

（2）感知延伸类

如IEEE 802.15、IETF 6LoWPAN ROLL、EPCGlobal GS1等，主要是对部分低传输速率近距离无线通信及RFID等进行寻址、标准化工作。

（3）网络通信类

如ITU-T、3GPP、GSMA、OMA等，主要是对智能SIM卡、M2M无线网络等进行优化和适配标准工作。

（4）相关应用类

如ITU-T、IEEE/FCC、CEN/ETSI等，主要是对智能交通、智能家居、智能电网、健康医疗等具体应用进行相关的标准化工作。

国内的标准组织主要以CCSA/CESI为主在进行标准化工作（CESI侧重传感器通信技术标准化、CCSA侧重M2M通信网络标准化），但从这几年的标准进展来看，国际上各标准组织之间对物联网的研究缺乏统一的协调和协作，如RFID国际上有30多个组织，一共制定了250多个标准。ZigBee联盟目前有超过225个会员，分为Promoter（促进者）、Participant（参与者）和Adopter（应用者）三级，Promoter级有16家，包括TI、ST、飞思卡尔、摩托

罗拉、飞利浦和华为等，但 ZigBee 标准仍然不够完善。每个国际标准组织的研究都是针对物联网的某一方面或某一传统的擅长内容在研究；包括国内对物联网的研究也都是根据不同的需求而进行零散的研究，没有整体系统端到端的研究。

就通信行业角度而言，物联网相关的标准组织主要聚焦在 3GPP 和 EISI 这两大标准组织上。

1）3GPP 侧重 M2M 无线网络的优化方面，重点是通过 3 个 Release 完成标准化工作，R11 对应 M2M 有一定数量，网络需要一定升级以适应 M2M 应用，R12 及以后则对应 M2M 数量激增，网络主要围绕 M2M 特点进行设计，考虑新的物理层设计。

2）ETSI TC 旨在填补当前 M2M 标准空白加速市场的快速发展，协调现有的 M2M 技术提供端到端解决方案，其优势是成员中 59% 的公司来自于设备制造商，26% 的公司为运营商，集中了主要的电信领域大公司，定位为全球范围内的协调组织。如果 M2M 成立类似于 3GPP 的 Partnership Project，极有可能是从 ETSI M2M TC 中衍生出来，应当说国内外的物联网相关标准发展还不成熟，无法匹配市场环境的发展，许多运营商、厂商均开发出自己的企业标准。

1.8　物联网产业链

我国的物联网产业链主要以集成商为主角，运营商在其中只是管道，集成商又分布在各个行业、地域中，如图 1-4 所示。同样的模式在不同的地域、行业被不同的集成商控制。

图 1-4　物联网产业链现状图

将整体产业链按价值分类，硬件厂商的价值较小，传感器/芯片厂商加上通信模块提供商约占整体产业价值的 15%，电信运营商提供的管道约占整体产业价值的 15%，剩下 70% 的市场价值均由系统集成商/服务提供商/中间件及应用商分享，而这类占产业价值大头的公司通常都集多种角色为一体，以系统集成商的角色出现。

从目前的表现来看，运营商竭力在向两端延伸价值，但产业链的演变不是以运营商的意志为转移的，运营商可以在其中努力扩大产业链的自身价值，通过构建 M2M 平台和模块/终端标准化来逐步实现，但在实际的商业模式中，要让广大的集成商使用运营商标准的模块和平台，必须价值让利，通过模块的补贴、定制、采集逐步让集成商接纳运营商的标准，进而将行业应用数据流逐步迁移到运营商的平台上。

运营商在产业链中的商机主要有以下几个方面：

首先，在网络侧，分析 M2M 对网络的影响和适配，将 M2M 通信的行业特性提炼出来，如 QoS 和安全等特性打包再卖给行业应用商/行业集成商，使得网络的通达、质量可以定制化，但该类商机会有一个很长的孵化过程，通俗地讲，等到现有公网在实现 M2M 通信时需要依赖运营商控制的时候才有大量的商机涌现（M2M 行业应用对网络的依赖性变得更强）。

其次，运营商的商机在于通过平台的数据流上，因为数据流通过运营商的平台，运营商

可以根据企业应用的具体场景和模式逐步地把现有的通信增值应用进行叠加，如彩信、短信通知、呼叫中心的外包等，再进一步对部分信息做二次提炼和处理，生产其他有价值的信息再转售，但这类商机也需要时间和努力。以上两类商机均需要运营商以平台和标准得到规模应用为前提。运营商其他的商机主要是基于管道的数据包套餐等，基于流量付费，属于纯管道费用，目前运营商主要依靠这类来实现收入，并且在较长的一段时期内仍然会是 M2M 的主要收入来源。

产业链上的其他环节商机则相对简单，随着物联网、M2M 产业规模的扩大，提供传感器/M2M 模块/M2M 网关/智能行业终端等生产厂家将获益，但目前规模化在全球均是难题。

系统集成商在未来将会有部分利益被运营商分享，但仍然是行业应用的主要力量之一。作为最终用户的政府、企业、个人而言，通过物联网基本并不能带来收入上的增加，更多的是通过信息远程控制达到提升生产效率、降低生产成本、实现节能减排等目的。

从物联网市场来看，全球物联网仍然属于新兴市场，2009 年 M2M 模块的全球发货量据统计只有 4000 万片，其中我国 400 万～500 万片，约占全球 10%，国际上欧、美、日、韩等物联网的发展时间都比我国长，但从目前的规模来看，虽然整体物联网市场增长较快，但总体规模并不大，日本 M2M 模块的存量市场约 500 万片，欧洲和美国的发展也不尽如人意。M2M 模块厂商也未创造出巨大的销售量，而欧美的运营商更多仍然依靠无线蜂窝网作为管道在保持 M2M 的收入，整体物联网产业仍然属于新兴市场，需要逐步的培育，如图 1-5 所示。

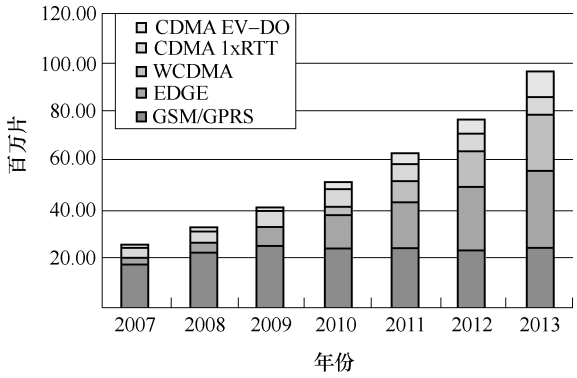


图 1-5 全球 M2M 模块发展（截至 2013 年）

尽管短期来看，物联网市场仍然需要时间来培育，但众多的参与者均看好物联网未来的潜力。就数量而言，全球可用于联网的机器和传感器数量远远大于人口数量，且随着全球经济和信息科技的快速发展，生产资料及机器的远程控制越来越重要，众多的参与者都希望通过前期的涉足逐步扩大影响力，在产业链中站稳脚跟，以便在未来的物联网“大蛋糕”中拥有一席之地。

物联网被大多数人寄予厚望，认为是继互联网后又一波信息浪潮，并且市场规模要远远大于互联网，但互联网面对的是大众市场，而物联网真正面对的主要是行业/企业市场，行业市场的标准化和壁垒性注定了物联网市场需要经过一个艰难而漫长的发展过程，任何企业在其中要想做到规模可复制均要花费大量的人力、物力及耐心，但面对这样一个及其有诱惑力的未来前景巨大的市场，是值得去长期跟踪、研究和尝试的。

物联网发展以来，业内人士几乎都认定，物联网产业链将会依次登场，这些潜在的发展空间，将改变世界，我们将生活在一个真正意义上的物联网地球村。

美国咨询机构 forrester 预测，到 2020 年，世界上物物互联的业务，跟人与人通信的业务相比，将达到 30∶1。

届时，物联网的产业链几乎可以包容现在信息技术和信息产业相关的各个领域。现阶段涉及传感器件、无线通信、信息安全和基于海量数据的分析优化，而在未来，当主动感知、数据处理后回馈控制等应用大规模兴起后，智能终端将更为广泛，进一步结合嵌入式系统和云计算技术。这无疑将成为半导体设计、制造行业和 IT 信息服务行业的巨大福音。

1.9　展望

物联网以其“无所不在”的构想在全球悄然掀起了一股前所未有的热潮，甚至有人将物联网视为比互联网大 30 倍的产业，是下一个万亿级的信息技术产业。

根据现在的趋势，我们不难预测在今后的若干年内物联网将会广泛应用于我们生活的方方面面，并将会在我们生活中发挥着重要作用。目前其开发的物联网应用产品，涵盖了物联网的主要应用领域，分别包括智能家居、智能医疗、智能城市、智能环保、智能交通、智能司法、智能农业、智能物流、智能校园、智能文博、M2M 平台等。物联网的终极应用是把身边的一切物体接入网络，为人类提供智能化的服务，构建智能化的城市。

物联网不是科技狂想，而是又一场科技革命。

在不久的将来，汽车将及时警告驾驶员车的某一个部位或任何零件发生了故障；当你出门远行时，行李箱会提醒你忘带了某些东西；当你洗衣服时，衣服会“告诉”洗衣机需要多少度的水温来洗；当你过马路时，红绿灯会根据行人状况，在时间上实现动态调控。

在智能家居中，你回家之前可以实时了解家中各个角落的状态，可以提前开始煮饭，提前打开空调，提前打开热水器等。在上班的时候，你可以通过物联网知道家里的状态：水管有没有关，电灯又没有关，窗帘有没有拉等，然后可以根据需要对其进行相应控制。

物联网使物品和服务功能都发生了质的飞跃，这些新的功能将给使用者带来进一步的效率、便利和安全，由此形成基于这些功能的新兴产业。

物联网需要信息高速公路的建立，移动互联网的高速发展以及固话宽带的普及是物联网海量信息传输交互的基础。依靠网络技术，物联网将生产要素和供应链进行深度重组，成为信息化带动工业化的现实载体。

有业内专家认为，物联网一方面可以提高经济效益，大大节约成本；另一方面可以为全球的经济复苏提供技术动力。同时，有专家认为，物联网架构建立需要明确产业链的利益关系，建立新的商业模式。

物联网的发展，带动的不仅仅是技术进步，而是通过应用创新进一步带动经济社会形态、创新形态的变革，塑造了知识社会的流体特性，推动面向知识社会的下一代创新（创新 2.0）形态的形成。移动及无线技术、物联网的发展，使得创新更加关注用户体验，用户体验成为下一代创新的核心。开放创新、共同创新、大众创新、用户创新成为知识社会环境下的创新新特征，技术更加展现其以人为本的一面，以人为本的创新随着物联网技术的发展成为现实。

参考文献

[1] Internet of Things Strategic Research Roadmap 2009.

[2] Internet of Things in 2020 A Roadmap for the Future. 2008.

[3] ITU Internet Reports 2005: The Internet of Things. 2005, 11.

[4] Luigi Atzori a, Antonio Iera b, Giacomo Morabito The Internet of Things: A survey University of Catania, Italy 2010.

[5] Andreas Heil1, Mirko Knoll2 and Torben Weis The Internet of Things-Context-based Device Federations University Stuttgart, Germany 2007.

[6] Appendix F: The Internet of Things (Background). Global Trends 2025. SRI Consulting Business Intelligence.

[7] 周洪波. 物联网：技术、应用、标准和商业模式 [M]. 北京：电子工业出版社, 2010.

[8] 肖剑, 胡忠华, 林云, 等. 物联网产业链及市场分析 [J]. 电信网技术, 2010 (10)：40-43.

第 2 章　感知层技术

感知层处于 3 层架构的最底层，是物联网的实现基础。感知层实现对物体的感知，感知层在物联网中，如同人的感觉器官对人体系统的作用，用来感知外界环境的温度、湿度、压强、光照、气压、受力情况等信息，通过采集这些信息来识别物体。感知层包括各种传感器、RFID 等数据采集设备，也包括在数据传送到接入网关之前的小型数据处理设备和传感器网络，主要实现物理世界信息的采集、自动识别和智能控制。感知层是物联网发展的关键环节和基础部分。感知层涉及的主要技术包括 EPC（Electronic Product Code）技术、RFID 技术、传感技术、短距离无线通信技术等。

本章从资源寻址与 EPC 技术、RFID 技术、传感器技术及无线传感器网络技术 4 个方面去论述感知层技术。EPC 技术解决物品的编码标准问题，使得所有物联网中的物体都有统一的 ID。RFID 技术解决物品标识问题，可以快速识别物体，并获取其属性信息。传感器完成的任务是感知信息的采集。无线传感器网络完成了信息的获取和上传，实现无线短距离通信。通过这些技术，实现物体的标识与感知，为物联网的应用和发展提供基础。

2.1　资源寻址与 EPC 技术

资源编码与寻址标准是物联网进行信息交互和共享的前提和基础，只有资源编码与寻址标准统一，才能确保联网物品的相关信息能够被高效、准确和安全地寻址、定位以及查询。从这一方面来看，物联网具有与互联网类似的资源寻址需求。

同时物联网存在多种物品编码标准共存而引起的资源寻址冲突等特有的资源寻址问题，这使得物联网资源寻址具有与互联网资源寻址的相异性。因此，物联网对互联网现有资源寻址技术提出新的挑战。

一般而言，资源地址是指访问资源的入口地址。而从资源寻址技术研究的角度来讲，资源地址是指对应于资源名称的一次资源寻址操作结束后得到的结果。与互联网资源地址相同，物联网资源地址也包含直接资源地址和间接资源地址这两种类型，其中直接资源地址同样是物理地址即物联网资源的 MAC 地址，而间接资源地址也是物联网资源名称的相对地址，可以直接作为其他物联网资源寻址系统的资源名称，用以进一步获取资源的相关地址。

但物联网资源寻址的输出不能统称为物联网资源地址。由于物联网资源名称存在不同于互联网资源名称的特殊性，如果其要参与资源寻址操作，首先需要对其存在的特性进行适当的转换，用以去除物联网资源名称分级结构可能存在的未知性和分散性。

完成转换所用到的信息需要通过物联网资源寻址操作来获取。该转换信息与相应的物联网资源名称转换而生成的物联网资源名称可以作为物联网资源寻址系统的输入，可以将经过转换信息转换生成的物联网资源名称看作是一种间接资源地址，而转换信息相应地可以看做是生成这种间接资源地址所需的信息。因此，物联网资源寻址的输出不能再仅仅局限于地址

本身，而应该扩展为生成物联网资源地址所需的信息，该信息可以本身就是物联网资源地址，也可以是将其他物联网资源名称转换为间接资源地址所需的地址生成信息。

目前，物联网资源寻址的研究仍处于起步阶段，基本上直接沿用互联网现有的资源寻址技术，而未对物联网特有的资源寻址问题提出有效的解决方案。

物品编码是物联网中特有的资源名称，而物联网资源寻址的核心工作正是完成由物品编码到与其相关资源地址的寻址，因此物品编码是物联网中最具代表性的资源名称。

最初的物品编码标准体系由成立于 1977 年的 GS1 前身 EAN 与 UCC 建立，目前全世界已有 100 多个国家和地区的超过 100 万家企业使用该标准体系对物品进行标识和供应链管理，极大地促进了全球物流及供应链管理的标准化、信息化发展。中国物品编码中心于 1991 年代表我国正式加入 GS1，全面管理和推广应用其条码技术。截止到 2004 年 12 月，我国商品条码系统成员已达 12 万家，上百万种产品包装上使用了商品条码标识，使用条码技术进行自动零售结算的超市已超万家，极大地推动了我国的物流信息化及对外贸易的发展。然而物品编码同互联网中的 MCA 地址、IP 地址以及域名等资源名称一样属于有偿资源，因此条码的使用者需要向 GS1 支付一定的费用。不难看出，随着物品制造商的增多，各国支付在物品编码上的费用总额将是相当可观的。

伴随着物联网概念的出现，该物品编码标准体系受到极大的冲击。基于 RFID 技术制造的电子标签与传统条码标签的最大区别在于物品编码容量的大大增加，如前所述，未来全球每一粒大米都可以分配到一个物品编码。由于现有的物品编码体系无法满足对物品单体进行识别的需求，并且物联网将使得物品编码成为更为重要的战略资源，因此各相关标准组织都在制定并推广新的物品编码标准，意欲打破现有的物品编码体系，从而成为新的全球物品编码标准体系管理者，或者成为某一地域或行业物品编码体系的管理者。目前针对全球领域的物品编码标准体系有 EPC Global 提出的 EPC 编码，uID Center 提出的 uCode 编码，针对国家领域的物品编码标准体系有 NIDA（National Internet Development Agency of Korea，韩国互联网发展处）提出 mRFID Cod（eMobile RFID Code，可移动的 RFID 编码），针对行业领域的物品编码标准体系有我国商务部提出的 CPC（Commerce Product Code，商务产品编码）。下面以 EPC 编码技术为例，介绍物品编码技术。

2.1.1　EPC 技术发展背景

EPC 技术首次提出是在 1999 年，被美国麻省理工学院 Auto-ID 中心提出来的。EPC 是指人们按照一定格式，把物品进行编码，这个编码号唯一。物联网中，由于要将大量的物体接入网络，EPC 技术对物联网而言非常重要，它可以将物体进行全球唯一的编号，便于接入网络。

2.1.1.1　国际发展情况

EPC 网络研究总部设在麻省理工学院，世界 5 所顶尖大学：英国剑桥大学、澳大利亚阿德莱德大学、日本庆应大学、中国复旦大学和瑞士圣加仑大学相继加入其中开始参与 EPC 的研究工作。

国际物品编码协会（EAN/UCC）在 2003 年 11 月成立了 EPC Global 小组，该小组正式接管 EPC 在全球的推广应用工作。与此同时，Auto. ID Center 更名为 Auto. ID Lab，为 EPC Global 指定了一系列标准，并提供技术支持。指定的标准包括 EPC 编码方案、通信协议、

数据接口等。

2004年6月EPC Global完成了第一个产品电子代码技术的全球标准。这宣告了第一代标签标准的完成。但是不可否认目前世界各国的EPC的规范尚存在许多差异。欧美采用UHF频段，如902MHz和928MHz，EPC位数为96位。日本采用的EPC频段2.5GHz和13.65MHz，EPC位数为128位。

2.1.1.2 国内发展情况

随着物联网在我国成为关注的热点，EPC得到了科技部、标准委等政府部门的高度重视。各相关行业、科研机构、应用企业纷纷开始研究EPC技术。

2003年2月，由国家标准化管理委员会、中国物品编码中心牵头，全国物流信息管理标准化技术委员会承办了第一届中国EPC联席会，统一了EPC和物联网的概念，协调各方关系，将EPC技术纳入标准化、规范化的管理。

2004年4月22日，我国成立了EPC Global China，并成功举行“首届中国国际EPC与物联网高层论坛”，不但从组织机构上保障了我国EPC事业整体的有效推进，同时标志着我国在及时跟踪国际EPC与物联网技术的发展动态、研究开发EPC技术的相关产品、推进EPC技术的标准化、推广EPC技术的应用等方面的工作的全面启动。

2.1.2 EPC

EPC的核心是编码，通过射频识别系统的读写器可以实现对EPC标签信息的读取。读写器获取EPC标签信息，并把标签信息送入互联网EPC体系中实体标记语言（Physical Mark-up Language，PML）服务器，服务器根据标签信息完成对物品信息的采集和追踪。然后利用EPC体系中的网络中间件等，可实现对所采集的EPC标签信息的利用。

当EPC标签贴在物品上或内嵌在物品中的时候，该物品与EPC标签中的唯一编号就建立了一对一的对应关系。

EPC的最大特点是可以实现单品识别，编码空间更大。通常条码系统只能表示某物品的产品类别和生产厂商信息，而EPC系统还可以表示物品的生产时间、生产地点以及产品编号等详细的信息。

EPC编码体系是新一代的与条形码兼容的编码标准，它是全球统一标识系统的延伸和拓展，是全球统一标识系统的重要组成部分，是EPC系统的核心。

在物联网中EPC与现行条形码相结合，因而EPC并不是取代现行的条码标准，而是由现行的条码标准逐渐过渡到EPC标准或者是在未来的供应链中EPC和EAN～CC系统共存。

2.1.2.1 EPC规则

与当前广泛使用的EAN/UCC代码不同的是，EPC提供对物理对象的唯一标识，就是一个EPC分配给一个且仅一个物品使用。

EPC标签编码的通用结构是一个比特串（如一个二进制表示），由EPC标头、EPC管理者、对象分类、序列号4个字段组成。目前，EPC编码有64位、96位和256位3种类型，见表2-1。

表 2-1　EPC 编码结构中各字段的长度　（单位：位）

编码类型		EPC 标头	EPC 管理者	对象分类	序列号
64 位	类型 A	2	21	17	24
	类型 B	2	15	13	34
	类型 C	2	26	13	23
96 位	类型 A	8	28	24	36
256 位	类型 A	8	32	56	160
	类型 B	8	64	56	128
	类型 C	8	128	56	64

（1）EPC 标头

标头标识 EPC 编码长度、识别类型和 EPC 结构，包括它的滤值（如果有的话）。当前，标头有 2 位和 8 位。2 位有 3 个可能值，8 位有 63 个可能值。标签长度可以通过检查标头最左边的头字段进行识别。标头编码见表 2-2。

表 2-2　EPC 中标头编码方案

标头值	标签长度	编码方案
01	64	64. 位保留方案
10	64	SGITN-64
11	64	64. 位保留方案
0000 0001	NA	一个保留方案
0000 001X	NA	二个保留方案
0000 01XX	NA	四个保留方案
0000 1000	64	SSCC-64
0000 1001	64	GLN-64
0000 1010	64	GRAI-64
0000 1011	64	GIAI-64
0000 1100 ~ 0000 1111	64	4 个 64. 位保留方案
0001 0000 ~ 0010 1111	NA	—
0011 0000	96	SGTIn-64
0011 0001	96	SSCC-64
0011 0010	96	GLN-64
0011 0011	96	GRAI-64
0011 0100	96	GIAI-96
0011 0101	96	GDI-96
0011 0110 ~ 0011 1111	96	10 个 64 位保留方案
0000 0000. . .		保留

（2）EPC 管理者

EPC 管理者是描述与此 EPC 相关的生产厂商的信息。EPC 管理者负责在自己的范围内

维护对象分类代码和序列号。EPC 管理者必须保证对 ONS 可靠的操作，并负责维护和公布相关的产品信息。不同版本的 EPC 管理者编码因为长度的可变性，使得更短的 EPC 管理者编号变得更为宝贵。EPC-64 TypeB 型有最短的 EPC 管理者部分，它只有 15 位。因此，只有 EPC 管理者编号小于 $2^{15}=32768$ 的才可以由该 EPC 版本表示。

（3）对象分类号

对象分类号记录产品精确类型信息和标识厂家产品种类。

（4）序列号

序列号唯一标识货物，它可以精确指出某一件产品。

对于每一个标签长度尽可能有较少的引导头，理想为 1 位，最好不要超过 2 位或者 3 位，如果可能，允许使用非常少的标头值引导头。这个引导头是为了 RFID 读写器可以很容易确定标签长度。

某些引导头目前不与特定的标签长度绑定在一起，这样为规范之外的其他标签的长度选择留下余地，尤其是对那些能够包含更长的编码方案的较长的标签，比如唯一 ID（Ubiquitous ID，UID），它被美国国防部的供应商所追捧。

为了保证所有物品都有唯一 EPC，并使标签成本尽可能降低，建议采用 96 位（8 位标头，28 位 EPC 管理者字段，24 位对象分类字段，36 位序列号字段），这样它可以为 2.68 亿个公司提供唯一的标识（远远超出 EAN-13 容纳的 100 万个制造商），每个生产商可以有 1600 万个对象分类且每个对象分类可有 680 亿个序列号，这对于未来世界所有产品已经完全够用了。

2.1.2.2　EPC 应用举例

本节通过分析物联网中的信息流通情况，具体考察 EPC 信息是如何在物联网中进行流动及物品的相关信息的获取，从而进一步了解物联网具体的工作机理。

如图 2-1 所示，EPC 系统借助于网络把分布在全球每个角落的含有标签的自然物体

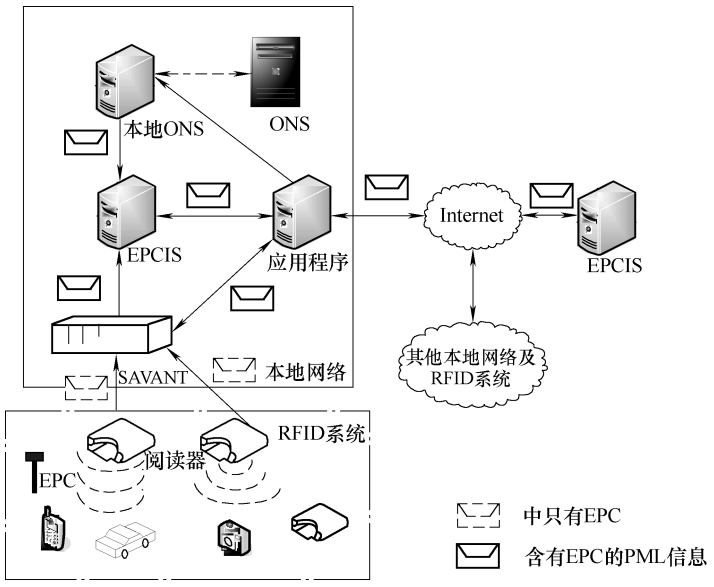


图 2-1　EPC 系统中的 EPC 信息流通图

（汽车、手机、相机等）自动无缝地连接起来。EPC 信息在 EPC 系统中流通分为三大部分，先是 RFID 系统传送 EPC，然后本地网络处理 EPC，最后是 Internet 返回物品的 PML 信息。下面来简要介绍 EPC 信息具体的流通情况。

1）当贴有 EPC 电子标签的物品进入到阅读器的阅读范围时，阅读器立即以电磁波的形式发出指令，“告知” EPC 电子标签，请将 EPC 发送给阅读器。EPC 电子标签在得到命令后，将存储器中的 EPC 代码通过内部电路调制然后借助其天线也以电磁波的方式“答复”阅读器。阅读器对 EPC 电子标签发送的电磁波进行解调后便获得了 EPC。

在实际应用中，往往是多个移动电子标签同时与阅读器进行应答的。例如某人在超市中购买了许多的商品，当他走至超市出口处时，这些商品的 EPC 电子标签同时受到了阅读器发来的指令，所有的标签同时进行“答复”时便产生了“碰撞”，此时阅读器启用防碰撞程序，先通知其中的某些“符合”条件的标签应答，然后依次的进行应答。

另外，物品上可能不仅贴有 EPC 电子标签，还可能贴有传感器。

2）在阅读器获得标签的 EPC（或传感信息）后，将其传递给本地网络层中的中间件（SAVANT）。经 SAVANT 信息过滤后，提交至企业应用程序来处理。企业应用程序根据实际情况，将 SAVANT 的信息给本地对象名称解析服务（Object Name Service，ONS）系统，由它来负责查询此 EPC 代码对应的此物品存放在互联网上的其余相关信息的通用资源标志符（Uniform Resource Identifier，URI）。

3）应用软件在得到 URI 地址后，自动连接至互联网上相应的 EPC Global 网络服务（EPC Information Services，EPCIS）服务器，此时，人们便可以查询到与物品相关的一切信息了。

在由 EPC 标签、阅读器、SAVANT、ONS 服务器、Internet、EPCIS 以及众多数据库组成的物联网中，阅读器读出的 EPC 代码没有任何实际意义，它只是一个信息参考（指针），由这个信息参考需要从 Internet 找到 IP 地址并获取该地址中存放的相关的物品信息，并采用分布式的 EPC 中间件处理由阅读器读取的一连串 EPC 信息。由于在标签上只有一个 EPC 代码，计算机需要知道与该 EPC 匹配的其他信息，因此需要 ONS 系统来提供一种自动化的网络数据库服务，计算机需要知道与该 EPC 匹配的其他信息，这就需要 ONS 来提供一种自动化的网络数据库服务，SAVANT 将 EPC 传给 ONS，ONS 指示 SAVANT 到一个保存着产品文件的 PML 服务器查找，该文件可由 SAVANT 复制，因而文件中的产品信息就能传到供应链上。

另外，物联网上所有信息（如产品的基本特征、所属类等相关数据）皆以物理标记语言（PML）文件格式来传送，其中 PML 文件也可能还包括了一些实时的时间信息、传感器信息等。PML 基于流行的可扩展标记语言（XML），因此便可以执行一些常用的企业任务。

EPC 系统非常典型的应用领域就是物流供应链领域，比如货品跟踪、采购管理、库存管理、订单控制等各个方面。其中比较成功的例子有：美国 Jacksonvihe 机场采用了电子标签技术后，识别准确率在 99% 以上，远远高于传统的条码技术；零售业巨头沃尔玛公司也从 2005 年起，全面使用 EPC 标签，极大地提高了服务效率和质量；在日本，EPC 系统国家发展战略已经制定，并在战略中强调要进行 EPC 系统研究，建立标准体系，推广 EPC 普及。丰田汽车、东京电力、日本运通等公司都开始应用 EPC 技术，无论是供应商、零售商、还是系统集成商或者硬件制造商都积极地参与到 EPC 的研究之中。

2.2　RFID

射频识别（Ratio Frequency Identification，RFID）技术是一种非接触式的自动识别技术，它利用射频信号，实现对目标对象的自动识别并获取相关数据。

RFID是物联网感知层的关键技术之一。物联网感知层需要感知各种物体，如何快速辨识物体是一个非常重要的问题，RFID这种非接触式自动识别技术的出现很好地解决了这一问题，成为物品识别最有效的方式。

RFID的基本技术原理起源于第二次世界大战时期，最初盟军利用无线电数据技术来识别敌我双方的飞机和军舰。战后，由于较高的成本，该技术一直主要应用于军事领域，并未很快在民用领域得到推广应用。直到20世纪80、90年代，随着芯片和电子技术的提高和普及，欧洲开始率先将RFID技术应用到公路收费等民用领域。

21世纪初，RFID迎来了一个崭新的发展时期，其在民用领域的价值开始得到世界各国的广泛关注，特别是在西方发达国家，RFID技术大量应用于生产自动化、门禁、公路收费、停车场管理、身份识别、货物跟踪等民用领域中，其新的应用范围还在不断扩展，层出不穷。RFID在沃尔玛超市的成功应用成为一个典型案例，据Sanford C. Bernstein公司的零售业分析师估计，通过采用RFID，沃尔玛每年可以节省83.5亿美元，其中大部分是因为不需要人工查看进货的条码而节省的劳动力成本。尽管另外一些分析师认为80亿美元这个数字过于乐观，但毫无疑问，RFID有助于解决零售业两个最大的难题：商品断货和损耗（因盗窃和供应链被搅乱而损失的产品），而现在单是盗窃一项，沃尔玛一年的损失就差不多有20亿美元，如果一家合法企业的营业额能达到这个数字，就可以在美国1000家最大企业的排行榜中名列第694位。研究机构估计，这种RFID技术能够帮助把失窃和存货水平降低25%。

目前从国内发展情况来看，RFID在很多领域都得到实际应用，包括物流、烟草、医药、身份证、门票、宠物管理等。RFID的实施成本，也随着RFID应用的推广和市场的扩大而逐步降低，RFID的应用将会从目前的托盘或整箱的货物跟踪逐步扩展到单品货物跟踪的水平。最后，从产业供应链角度看，国家目前提倡的产业升级，就是要使我国企业多生产高技术、高附加值、高利润产品，而这些领域，正是RFID用武之地。产业升级将带动我国企业提升市场竞争能力，逐步由单体企业竞争上升为产业供应链的竞争。

2.2.1　RFID简介

2.2.1.1　RFID系统分类

RFID系统按照不同的分类标准有多种分类方法：

1）根据系统工作频率不同，可将RFID系统分为低频系统、中频系统和高频系统三大类；

2）根据RFID标签内是否需要电池供电，又可将其分为有源系统和无源系统两大类；

3）根据系统保存的信息写入的方式不同，可分为集成电路固化式、现场有线改写式和现场无线改写式三大类；

4）根据读取电子标签数据的技术实现手段，可将其分为广播发射式、倍频式和反射调

制式三大类。

另外还可依据标签的材质、系统工作距离和阅读器的工作状态等方面对 RFID 系统进行分类。下面主要根据系统工作频率分类进行简介：对一个 RFID 系统来说，它的频段概念是指读写器通过天线发送、接收并识读的标签信号频率范围。从应用概念来说，射频标签的工作频率也就是射频识别系统的工作频率，直接决定系统应用的各方面特性。在 RFID 系统中，系统工作就像我们平时收听调频广播一样，射频标签和读写器也要调制到相同的频率才能工作。

射频标签的工作频率不仅决定着射频识别系统工作原理（电感耦合还是电磁耦合）、识别距离，还决定着射频标签及读写器实现的难易程度和设备成本。RFID 应用占据的频段或频点在国际上有公认的划分，即位于 ISM 波段（见表 2-3）。

表 2-3　射频标签的工作频率

分　类	典型工作频率	优　点	缺　点	主要应用
低频系统	125kHz、134.2kHz 和 225kHz	标签的成本较低、耗电量低，标签外形多样	标签内保存的数据量较少、阅读距离较短且速度较慢、阅读天线方向性不强	门禁系统、家畜识别和资产管理等
高频系统	13.56MHz	标签内保存的数据量较大、阅读距离较远且具有中等阅读速度	标签及阅读器成本较高、阅读天线方向性不强	门禁系统和智能卡
超高频系统	915MHz、2.45GHz 和 5.08GHz	标签内数据量大、阅读距离远且具有高速阅读速度、适应物体高速运性能好	标签及阅读器成本较高且阅读器与标签工作时多为视距（line of sight）读取问题	火车车皮监视和零售系统

按照工作频率的不同，RFID 标签可以分为低频（LF）、高频（HF）、超高频（UHF）和微波等不同种类。不同频段的 RFID 工作原理不同，LF 和 HF 频段 RFID 电子标签一般采用电磁耦合原理，而 UHF 及微波频段的 RFID 一般采用电磁发射原理。目前国际上广泛采用的频率分布于 4 种波段，低频（125kHz）、高频（13.56MHz）、超高频（850～910MHz）和微波（2.45GHz）。每一种频率都有它的特点，被用在不同的领域，因此要正确使用就要先选择合适的频率。

低频段射频标签，简称为低频标签，其工作频率范围为 30～300kHz。典型工作频率有 125kHz 和 133kHz。低频标签一般为无源标签，其工作能量通过电感耦合方式从阅读器耦合线圈的辐射近场中获得。低频标签与阅读器之间传送数据时，低频标签需位于阅读器天线辐射的近场区内。低频标签的阅读距离一般情况下小于 1m。低频标签的典型应用有：动物识别、容器识别、工具识别、电子闭锁防盗（带有内置应答器的汽车钥匙）等。

中高频段射频标签的工作频率一般为 3～30MHz，典型工作频率为 13.56MHz。该频段的射频标签，因其工作原理与低频标签完全相同，即采用电感耦合方式工作，所以宜将其归为低频标签类中。另一方面，根据无线电频率的一般划分，其工作频段又称为高频，所以也

常将其称为高频标签。鉴于该频段的射频标签可能是实际应用中最大量的一种射频标签，因而我们只要将高、低理解成为一个相对的概念，即不会造成理解上的混乱。为了便于叙述，我们将其称为中频射频标签。中频标签一般也采用无源设备其工作能量同低频标签一样，也是通过电感（磁）耦合方式从阅读器耦合线圈的辐射近场中获得。标签与阅读器进行数据交换时，标签必须位于阅读器天线辐射的近场区内。中频标签的阅读距离一般情况下也小于1m。中频标签由于可方便地做成卡状，广泛应用于电子车票、电子身份证、电子闭锁防盗(电子遥控门锁控制器)、小区物业管理、大厦门禁系统等。

超高频与微波频段的射频标签简称为微波射频标签，其典型工作频率有433.92MHz、862（902）~928MHz、2.45GHz、5.8GHz。微波射频标签可分为有源标签与无源标签两类。工作时，射频标签位于阅读器天线辐射场的远区场内，标签与阅读器之间的耦合方式为电磁耦合方式。阅读器天线辐射场为无源标签提供射频能量，将有源标签唤醒。相应的射频识别系统阅读距离一般大于1m，典型情况为4~6m，最大可达10m以上。阅读器天线一般均为定向天线，只有在阅读器天线定向波束范围内的射频标签可被读/写。随着阅读距离的增加，应用中有可能在阅读区域中同时出现多个射频标签的情况，从而提出了多标签同时读取的需求。目前，先进的射频识别系统均将多标签识读问题作为系统的一个重要特征。超高频标签主要用于铁路车辆自动识别、集装箱识别，还可用于公路车辆识别与自动收费系统中。

以目前技术水平来说，无源微波射频标签比较成功的产品相对集中在902~928MHz频段上。2.45GHz和5.8GHz射频识别系统多以半无源微波射频标签产品面世。半无源标签一般采用纽扣电池供电，具有较远的阅读距离。微波射频标签的典型特点主要集中在是否无源、无线读写距离、是否支持多标签读写、是否适合高速识别应用、读写器的发射功率容限、射频标签及读写器的价格等方面。对于可无线写的射频标签而言，通常情况下写入距离要小于识读距离，其原因在于写入要求更大的能量。微波射频标签的数据存储容量一般限定在2kbit以内，再大的存储容量似乎没有太大的意义，从技术及应用的角度来说，微波射频标签并不适合作为大量数据的载体，其主要功能在于标识物品并完成无接触的识别过程。典型的数据容量指标有：1kbit、128bit、64bit等。由Auto-ID Center制定的产品电子代码EPC的容量为90bit。微波射频标签的典型应用包括移动车辆识别、电子闭锁防盗（电子遥控门锁控制器)、医疗科研等行业。

不同频率的标签有不同的特点，例如，低频标签比超高频标签便宜，节省能量，穿透废金属物体力强，工作频率不受无线电频率管制约束，最适合用于含水成分较高的物体，比如水果等；超高频作用范围广，传送数据速度快，但是比较耗能，穿透力较弱，作业区域不能有太多干扰，适用于监测港口、仓储等物流领域的物品；而高频标签属中短距识别，读写速度也居中，产品价格也相对便宜，比如应用在电子票证一卡通上。

目前，不同的国家对于相同波段，使用的频率也不尽相同。欧洲使用的超高频是868MHz，美国则是915MHz。日本目前不允许将超高频用到射频技术中。

目前在实际应用中，比较常用的是13.56MHz、860~960MHz、2.45GHz等频段。近距离RFID系统主要使用125kHz、13.56MHz等LF和HF频段，技术最为成熟；远距离RFID系统主要使用433MHz、860~960MHz等UHF频段，以及2.45GHz、5.8GHz等微波频段，目前还多在测试当中，没有大规模应用。

我国在LF和HF频段RFID标签芯片设计方面的技术比较成熟，HF频段方面的设计技

术接近国际先进水平，已经自主开发出符合 ISO14443 Type A、Type B 和 ISO15693 标准的 RFID 芯片，并成功地应用于交通一卡通和第二代身份证等项目中。

此外，有源 RFID 和无源 RFID 是人们经常采用的分类方法：标签内装有电池的 RFID 系统被称为有源系统。有源系统一般具有较远的阅读距离，但是对有源系统而言，电池的寿命有限，一般是 3 ~ 10 年；标签内没有电池的 RFID 系统为无源系统。无源系统工作时，阅读器发射的电磁波转化为能量供应系统正常读取信息。由于阅读器电磁波转化的能量限制，无源系统的阅读距离有限，并且不适于在高速运动的情况下读取标签。

2.2.1.2　RFID 发展状况

1. RFID 国际状况

RFID 技术在国外的发展时间较长，尤其美国、日本、英国、德国、瑞典、瑞士及南非等国家已经得到了很大发展。在世界各国，RFID 技术已被广泛应用于众多领域：高速公路自动收费系统、智能交通监控、物品管理、工业生产自动化、安全出入检查、动物管理和车辆防盗等。

针对 RFID 技术，技术大国纷纷成立了专门的研究组织机构，专门致力于 RFID 技术基础信息网络的研究。例如：美国成立的 EPC Global 和日本成立的 UID 中心，这两个组织针对基础网络建设中存在的各种关键性问题均提出了相应的技术标准规范。

Microsoft 公司投入巨资组建了 RFID 实验室（微软 RFID 创新实验室），主要研究物联网中间件和 RFID 平台的开发。并以微软 SQL 数据库和 Windows 操作系统为依托，向大中型企业提供物联网中间件企业解决方案。2007 年微软 RFID 创新实验室推出了其产品 BizTalk RFID。

2. RFID 国内状况

我国在 RFID 方面的研究主要是跟踪发达国家的步伐。中国自动识别技术协会已经组织成立了射频工作组，跟踪国际 RFID 技术的发展及标准化进程，并且完成了 ISO/IEC. 18000 国际标准的跟踪、同步翻译及国家标准草案的起草工作。1992 年我国原经济部技术处开始推动高频 RFID 的研发计划，研发内容包括 IC 芯片、天线、读取器等重要技术。

2006 年 6 月，科技部同 16 部委联合发布了《中国射频识别技术政策白皮书》，这一我国射频识别技术与产业未来几年发展的系统性指导文件，为我国 RFID 技术的发展指明了方向。同年 9 月，国家 863 计划发布了十一五“射频识别（RFID）技术与应用项目指南”，从 RFID 技术研究、产业应用、标准制定等多方面给予了资金引导与扶持。

2006 年，中科院自动化研究所的课题“物流应用用的 RFID 技术分析测试研究”通过验收，课题组建立了面向物流应用的 RFID 技术分析和模拟测试实验平台，在此基础上对电子标签、读写器、天线、中间件均进行了详细的分析和评测。

2007 年 7 月，原信息产业部正式发布《800/900MHz 频段射频识别技术应用规定（试行）》的通知，规划了 800/900MHz 频段射频识别技术的具体使用频率，这个频段与 EPC 的频段比较吻合，极有可能成为我国物联网中使用的主要 RFID 频段。

总之，我国 RFID 技术发展是有步骤分阶段地进行：

第一阶段培育期（2006 年和 2008 年）：跟踪国际最新共性技术的研发，结合重点行业的应用，研发具有自主知识产权的 RFID 技术，制定相应的技术标准和应用标准。

第二阶段成长期（2007 年和 2012 年）：突破应用与产业化关键技术，加快相关技术标

准以及应用标准制定，基本形成中国的 RFID 标准体系，拓展应用领域。

第三阶段成熟期：形成国际同期先进水平的技术体系，实现 RFID 技术的广泛应用。

2.2.2　RFID 技术标准

2.2.2.1　RFID 标准概述

RFID 标准可以分为以下 4 类：

1）技术标准，主要定义了不同频段的空中接口以及相关参数，包括基本术语、物理参数、通信协议和相关设备。例如 RFID 中间件是 RFID 标签和应用程序之间的中介，从应用程序端使用中间件所提供的一组应用接口，既能连接到 RFID 读写器，读取 RFID 标签的数据。

2）数据内容与编码标准，主要涉及数据协议，数据编码规则以及语法，包括编码格式、语法标准、数据符号、数据对象、数据结构和数据安全等。

3）性能与一致性标准，主要涉及设备性能以及一致性测试方法，尤其是数据结构和数据内容（即数据编码格式以及内存分配），主要包括印制质量、设计工艺、测试规范和试验流程等。

4）应用标准，主要涉及特定应用领域或环境中的 RFID 构建规则，包括 RFID 在物流配送、仓储管理、交通运输、信息管理、动物识别、工业制造和体育休闲等领域的应用标准规范。

目前 RFID 存在很多标准，标准不统一是影响 RFID 发展的严重问题，因为每个 RFID 标签中都有一个唯一的标识码（ID），如果它的数据格式有很多种类且互不兼容，那么使用不同标准的 RFID 产品就不能通用，所以如何统一标准，是当前急需解决的问题。基本上编码标准和通信协议是不同标准体系争夺最激烈的部分。

2.2.2.2　主要技术标准体系

目前 RFID 存在 3 个主要的技术标准体系：欧美的 EPC Global 标准体系、日本的 Ubiquitous ID 标准系统和国际标准的 ISO/IEC 体系。

（1）EPC Global 标准

EPC Global 是由美国统一代码协会（UCC）和国际物品编码协会（EAN）于 2003 年 9 月共同成立的非营利性组织，其前身是 1999 年 10 月 1 日在美国麻省理工学院成立的非营利性组织 Auto-ID 中心。

Auto-ID 中心以创建“物联网（Internet of Things）”为使命，与众多成员企业共同制定一个统一的开放技术标准。目前 EPC Global 已在加拿大、日本、中国等国建立了分支机构，专门负责 EPC 码段在这些国家的分配与管理、EPC 相关技术标准的制定、EPC 相关技术在本国的宣传普及以及推广应用等工作。

EPC Global“物联网”体系架构由 EPC 编码、EPC 标签及读写器、EPC 中间件、ONS 服务器和 EPCIS 服务器等部分构成。EPC 赋予物品唯一的电子编码，其位长通常为 64 位或 96 位，也可扩展为 256 位。对不同的应用规定有不同的编码格式，主要存放企业代码、商品代码和序列号等。最新的 Gen2 标准的 EPC 编码可兼容多种编码。

（2）Ubiquitous ID（UID）标准

UID 中心于 2003 年 3 月成立，并得到日本政府经产省和总务省以及大企业的支持，包括

微软、索尼、三菱、日立、日电、东芝、富士通等重量级企业。

UID 中心的识别技术体系架构由泛在识别码（uCode）、信息系统服务器、泛在通信器和 uCode 解析服务器 4 部分构成。uCode 采用 128 位记录信息，提供了 340 × 1036 编码空间，并可以以 128 位为单元进一步扩展至 256、384 或 512 位。uCode 能包容现有编码体系的元编码设计，可以兼容多种编码，包括 JAN、UPC、ISBN、IPv6 地址，甚至电话号码。uCode 标签具有多种形式，包括条码、射频标签、智能卡、有源芯片等。泛在中心把标签进行分类，设立了 9 个级别的不同认证标准。

信息系统服务器存储并提供与 uCode 相关的各种信息。

uCode 解析服务器确定与 uCode 相关的信息存放在哪个信息系统服务器上。uCode 解析服务器的通信协议为 uCodeRP 和 eTP，其中 eTP 是基于 eTron（PKI）的密码认证通信协议。

泛在通信器主要由 IC 标签、标签读写器和无线广域通信设备等部分构成，用来把读到的 uCode 送至 uCode 解析服务器，并从信息系统服务器获得有关信息。

（3）ISO/IEC 技术标准研究

ISO/IEC 是国际标准化组织和国际电工委员会共同制定的一个国际标准，与 EPC Global 只专注于 860 ~ 960MHz 频段不同，ISO/IEC 对各个频段都颁布了标准，表 2-4 详细列出了 ISO/IEC 制定的一系列标准 121-221。

RFID 频率由 ISO 18000 RFID 空中接口标准系列统一管理。2004 年 9 月 ISO 出台了一套完整的相关标准。其中，ISO 18000 系列包括了有源和无源的 RFID 技术标准，主要是基于物品管理的 RFID 空中接口参数。

目前我国常用的 RFID 标准主要是用于非接触智能卡的两个 ISO 标准：ISO 14443 和 ISO 15693。

表 2-4　ISO/IEC 制定的 RFID 标准

分　类	标 准 号	内　容
技术标准	ISO/IEC 10536	密耦合非接触式 IC 卡
	ISO/IEC 14443	近耦合非接触式 IC 卡
	ISO/IEC 15693	疏耦合非接触式 IC 卡
	ISO/IEC 1 8000-1	空中接口一般参数
	ISO/IEC 1 8000-2	低于 135kHz 频率的空中接口参数
	ISO/IEC 1 8000-3	13. 56MHz 频率下的空中接口参数
	ISO/IEC 1 8000-4	2. 45GHz 频率下的空中接口参数
	ISO/IEC 1 8000-6	860 ~ 960MHz 空中接口参数
	ISO/IEC 1 8000-7	433MHz 频率下的空中接口参数
数据内容标准	ISO/IEC 15424	数据载体/特征标识符
	ISO/IEC 15418	EAN、UCC 应用标识符及 ASC MH10 数据标识符
	ISO/IEC 15434	大容量 ADC 媒体用的传送语法
	ISO/IEC 15459	物品管理的唯一识别号（UID）
接口标准	ISO/IEC 15961	数据协议：应用接口
	ISO/IEC 15962	数据编码规则和逻辑存储功能协议
	ISO/IEC 15963	射频标签（应答器）的唯一标识

（续）

分　类	标　准　号	内　容
性能标准	ISO/IEC 18046	RFD 设备性能测试方法有无源
	ISO/IEC 18047	RFID 设备一致性测试方法
	ISO/IEC 10373-6	按 ISO/IEC 14443 对非接触式 IC 卡进行测试的方法
应用标准	ISO/IEC 10374	货运集装箱识别标准
	ISO/IEC 18185	货运集装箱密封标准
	ISO/IEC 11784	动物 RFID 的代码结构
	ISO/IEC 11785	动物 RFID 的技术准则
	ISO/IEC 14223	动物追逐的直接识别数据获取标准
	ISO/IEC 17363	一系列物流容器识别的规范

2.2.3　RFID 工作原理及特性

2.2.3.1　RFID 系统工作原理

RFID 应用系统的基本工作原理（见图 2-2）：RFID 卡进入读写器的射频场后，由其天线获得的感应电流经升压电路作为芯片的电源，同时将带信息的感应电流通过射频前端电路检得数字信号送入逻辑控制电路进行信息处理；所需回复的信息则从存储器中获取经由逻辑控制电路送回射频前端电路，最后通过天线发回给读写器。可见，RFID 卡与读写器实现数据通信过程中起关键的作用是天线。一方面，无源的 RFID 卡芯片要启动电路工作需要通过天线在读写器天线产生的电磁场中获得足够的能量；另一方面，天线决定了 RFID 卡与读写器之间的通信信道和通信方式。

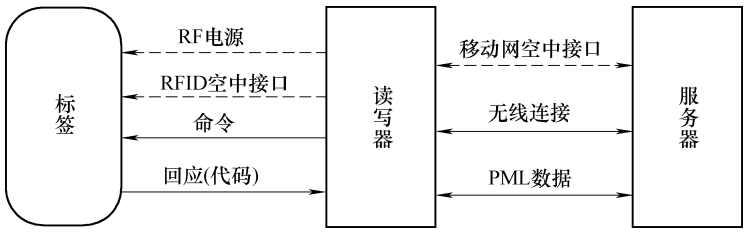


图 2-2　RFID 原理图

RFID 标签俗称电子标签，也称应答器（tag，transponder，responder），根据工作方式可分为主动式（有源）和被动式（无源）两大类，表 2-5 列出了主动式/被动式 RFID 技术比较。被动式 RFID 标签由标签芯片和标签天线或线圈组成，利用电感耦合或电磁反向散射耦合原理实现与读写器之间的通信。RFID 标签中存储一个唯一编码，通常为 64bit、96bit 甚至更高，其地址空间大大高于条码所能提供的空间，因此可以实现单品级的物品编码。当 RFID 标签进入读写器的作用区域，就可以根据电感耦合原理（近场作用范围内）或电磁反向散射耦合原理（远场作用范围内）在标签天线两端产生感应电势差，并在标签芯片通路中形成微弱电流，如果这个电流强度超过一个阈值，就将激活 RFID 标签芯片电路工作，从而对标签芯片中的存储器进行读/写操作，微控制器还可以进一步加入诸如密码或防碰撞算

法等复杂功能。有源 RFID 的电子标签自身具备电池，可提供全部器件工作的电源，因而相应阅读器的发射功率要求不高，而且有效阅读距离也较前者有所增加。

表 2-5　主动式/被动式 RFID 技术比较

	主动式远距离 RFID（有源卡）	被动式远距离 RFID（无源卡）
采用技术	射频技术	射频技术
频率/Hz	2.45G 为主	915M 为主
技术成熟度	成熟	成熟
读卡距离/m	读写卡 1～100	读卡 1～8，写卡 1～3
工作方式	主动发射	被动发射
防冲突能力	高，同时读取 255 张标签	低，20 张/3s
存储区大小/B	512K 以上	128
耗材成本/元	高：单张成本 40～100	低：单张成本 10～30
耗材通用性	差：特制	高：采用标准格式
系统价格/元	低，读卡头 3000～10000	高，读卡头 1 万～2 万
功耗	低，功耗在 0.1mW，可以达到欧洲\北美等地区安全要求	高，为了达到 10m 的距离通常需要超过安全规范
兼容性	可以兼容额 EM\M1\TI\ISO\EPC 等多种规格卡	兼容性差
使用环境要求	低：能适应大部分环境	高：粉尘、含金属玻璃无法穿透
安装便利性	方便，安装位置没有特别要求	不方便：需要安装在前挡风玻璃或者车牌，不可以安装在金属表面
使用情况	公路收费、高档写字楼、社区使用	公路收费、高档写字楼、社区使用
防伪性	高，不可复制	高，不可复制

读写器也称阅读器、询问器（reader，interrogator），是对 RFID 标签进行读/写操作的设备，主要包括射频模块和数字信号处理单元两部分。读写器是 RFID 系统中最重要的基础设施，一方面，RFID 标签返回的微弱电磁信号通过天线进入读写器的射频模块中转换为数字信号，再经过读写器的数字信号处理单元对其进行必要的加工整形，最后从中解调出返回的信息，完成对 RFID 标签的识别或读/写操作；另一方面，上层中间件及应用软件与读写器进行交互，实现操作指令的执行和数据汇总上传。在上传数据时，读写器会对 RFID 标签原子事件进行去重过滤或简单的条件过滤，将其加工为读写器事件后再上传，以减少与中间件及应用软件之间数据交换的流量，因此在很多读写器中还集成了微处理器和嵌入式系统，实现一部分中间件的功能，如信号状态控制、奇偶位错误校验与修正等。未来的读写器呈现出智能化、小型化和集成化趋势，还将具备更加强大的前端控制功能，例如直接与工业现场的其他设备进行交互甚至是作为控制器进行在线调度。在物联网中，读写器将成为同时具有通信、控制和计算功能的 C3（Communication，Control，Computing）核心设备。

天线是 RFID 标签和读写器之间实现射频信号空间传播和建立无线通信连接的设备。RFID 系统中包括两类天线，一类是 RFID 标签上的天线，另一类是读写器天线，既可以内置于读写器中，也可以通过同轴电缆与读写器的射频输出端口相连。目前的天线产品多采用

收发分离技术来实现发射和接收功能的集成。在实际应用中，天线设计参数是影响 RFID 系统识别范围的主要因素，高性能的天线不仅要求具有良好的阻抗匹配特性，还需要根据应用环境的特点对方向特性、极化特性和频率特性等进行专门设计。

对于无源系统，阅读器通过耦合元件发送出一定频率的射频信号，当标签进入该区域时通过耦合元件从中获得能量以驱动后级芯片与阅读器进行通信。阅读器读取标签的自身编码等信息并解码后送至数据交换、管理系统处理。对于有源系统，标签进入阅读器工作区域后，由自身内嵌的电池为后级芯片供电以完成与阅读器间的相应通信过程。

此外，还有服务器（后台管理系统）。后台管理系统是在阅读器与企业应用之间的中间件，RFID 系统的重要组成部分。该中间件为企业应用提供一系列计算功能，在电子产品编码（EPC）规范中被称为 SAVANT。其主要任务是对读写器读取的标签数据进行过滤、汇集和计算，减少从阅读器传往企业应用的数据量。同时 SAVANT 还提供与其他 RFID 支撑系统进行互操作的功能。

2.2.3.2　RFID 工作特性

RFID 在本质上是物品识别的手段，它被认为将最终取代如今应用非常广泛的传统条码识别，成为物品识别最有效的方式，它具有一些非常明显的优点：

1）读取方便快捷。数据的读取无需光源，甚至可以透过外包装来进行。有效识别距离更大，采用自带电池的主动标签时，有效识别距离可达 30m 以上。

2）识别速度快。标签一进入磁场，读写器就可以即时读取其中的信息，而且能够同时处理多个标签。

3）数据容量大。数据容量最大的二维条形码，最多也只能存储2725 个数字；若包含字母，存储量则会更少；RFID 标签则可以根据用户的需要扩充到数 KB 甚至更大。

4）使用寿命长，应用范围广。其无线电通信方式，使其可以应用于粉尘、油污等高污染环境和放射性环境，而且其封闭式包装使得其寿命大大超过印刷的条形码。

5）标签数据可动态更改。利用编程器可以向写入数据，从而赋予 RFID 标签交互式便携数据文件的功能。

6）更好的安全性。不仅可以嵌入或附着在不同形状、类型的产品上，而且可以为标签数据的读写设置密码保护，从而具有更高的安全性。

7）动态实时通信。标签以与每秒 50 ~ 100 次的频率与读写器进行通信，所以只要 RFID 标签所附着的物体出现在读写器的有效识别范围内，就可以对其位置进行动态的追踪和监控。

2.2.4　RFID 中的关键技术

2.2.4.1　RFID 中的天线技术

天线是一种以电磁波形式把无线电收发机的射频信号功率接收或辐射出去的装置。受到应用场合的限制，RFID 标签通常需要贴在不同类型、不同形状的物体表面，甚至需要嵌入到物体内部。RFID 标签在要求低成本的同时，还要求有高的可靠性。此外，标签天线和读写器天线还分别承担接收能量和发射能量的作用，这些因素对天线的设计提出了严格要求。当前对 RFID 天线的研究主要集中在研究天线结构和环境因素对天线性能的影响上。

对于 UHF 以上频段的 RFID 系统而言，阅读器和标签工作时就相当于一组无线电发射机

和接收机。无线电发射机输出的射频信号功率，通过馈线输送到天线，由天线以电磁波的形式辐射出去。电磁波到达接收点后，由无线电接收机的接收天线接收下来（仅是发射功率中很小的一部分），并通过馈线送到接收机。可见，天线是需要发射和接收电磁波的无线电设备中不可缺少的重要组成部分。

从功能上来说，天线是一种将线路上流过的高频电流高效率地转换成电磁波辐射到空中去的装置，或者是将空中的电磁波高效率转换成高频电流的装置。

天线有很多种类。按方向性分有：全向天线、定向天线等；而按外形，天线又可分为线状天线、面状天线和板状天线等。

标签天线主要分为三大类：线圈型、偶极子、缝隙（包括微带贴片）型。

线圈型天线是将金属线盘绕成平面或将金属线缠绕在磁心上；偶极子天线由两段同样粗细和等长的直导线排成一条直线构成，信号从中间的两个端点馈入，天线的长度决定频率范围；缝隙型天线是由金属表面切出的凹槽构成，其中微带贴片天线由一块末端带有长方形的电路板构成，长方形的长宽决定频率范围。

识别距离小于 1m 的中低频近距离应用系统的 RFID 天线一般采用工艺简单、成本低的线圈型天线。识别距离大于 1m 的高频或微波频段的远距离应用系统需要采用偶极子和缝隙型天线。

2.2.4.2　RFID 中的防冲突技术和算法设计

作为一种无线通信，RFID 系统工作时，尤其是高频远距离的 RFID 系统，不能排除一个以上的标签同时进入阅读器的工作范围。作为 RFID 的发展方向，EPC 网络中此问题更加突出。在这样的系统中存在着几种通信形式：

从阅读器到标签的数据传输为一种通信形式，阅读器发送的数据同时被所有的标签接收。

第二种通信方式为在阅读器的作用范围内，多个标签的数据同时传输给阅读器，即多址通信。由于 RFID 系统的特殊性，其多址通信问题无法直接使用经典的空分多址（SDMA）法、频分多址（FDMA）法、码分多址（CDMA）法和时分多址（TDMA）法 4 种防冲突方法。其中，前 3 种方法实施复杂，在 RFID 系统一般不予采用。从而，TDMA 就成为了 RFID 系统中的主要防冲突方法。根据信道访问的控制，TDMA 又可以分为标签控制（标签驱动）和阅读器控制（询问控制）两种方法。

标签控制法，其工作是非同步的，因为该方法对阅读器的数据传输没有控制。按照标签成功完成数据传输后是否通过阅读器的信号而判断是否断开，又分为“开关断开法”和“非开关”法（见图 2-3）。

阅读器控制法，是采取阅读器作为主控制器的方法。该方法可以同步进行观察，因为这里所有的标签同时由阅读器进行控制和检查。因为阅读器控制法可以快速地按时间顺序操作标签，所以也称作定时双工传输法。

与标签控制法和阅读器控制法相对应的，RFID 系统主要使用的防冲突算法有：ALOHA 算法系列和二进制搜索算法类。

2.2.5　RFID 的应用标签

客户可根据需要选择或定制相应的电子标签，这些标签满足国际 ISO15693、ISO18000-

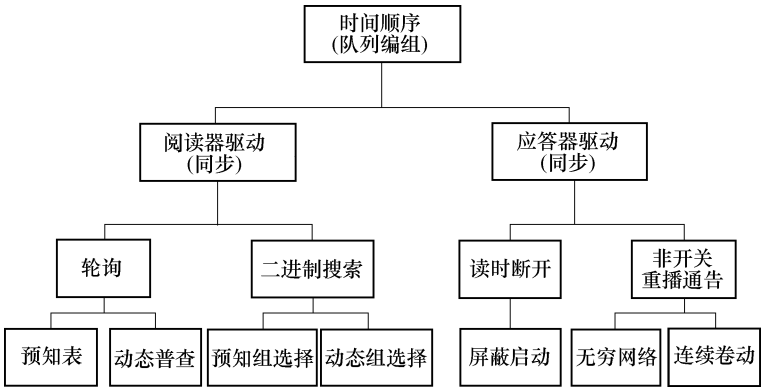


图 2-3　时分防冲突算法划分图

6B、EPC G2 等多种标准，并可采用不同的天线设计和封装材料可制成多种形式，如车辆标签、货盘标签、物流标签、金属标签、图书标签、液体标签、人员门禁标签、门票标签、行李标签等。

标签：剥离底纸直接粘贴于纸质包装箱上，带金属外壳的设备上，实现“即贴出货”的过程。适用于物流、供应链管理等。

标准卡：PVC 层压的标准卡，持在手中或挂于胸前。主要应用于人员管理、图书管理和车辆管理等。

动物标签：使用专用动物耳标签，将标签装与牲畜的耳朵上。主要用于种畜繁育、疫情防治、肉类检疫。

门票：持在手中或挂于胸前。适用于会议出入证明及门票管理等领域。

图书管理：直接粘贴于书内。主要应用于图书馆、书店等场所。

除此之外，RFID 技术也广泛用于食品管理、医疗行业、危险品管理、煤矿管理和军事领域。

2.3　传感器技术

传感器是各种信息处理系统获取信息的一个重要途径。在物联网中传感器的作用尤为突出，是物联网中获得信息的主要设备。

作为物联网中的信息感知与采集设备，传感器利用各种机制把被观测量转换为一定形式的电信号，然后由相应的信号处理装置来处理，并产生响应的动作。

人们为了从外界获取信息，必须借助于感觉器官。而单靠人们自身的感觉器官，在研究自然现象和规律以及生产活动中它们的功能就远远不够了。为适应这种情况，就需要传感器。利用传感器捕获信息是获取自然和生产领域中信息的主要途径与手段。

在现代工业生产尤其是自动化生产过程中，要用各种传感器来监视和控制生产过程中的各个参数，使设备工作在正常状态或最佳状态，并使产品达到最好的质量。

在基础学科研究中，传感器更具有突出的地位。现代科学技术的发展，进入了许多新领域：例如在宏观上要观察上千光年的茫茫宇宙，微观上要观察小到纳米的粒子世界，纵向上

要观察长达数十万年的天体演化和短到微妙的瞬间反应。此外，还出现了对深化物质认识、开拓新能源、新材料等具有重要作用的各种极端技术研究，如超高温、超低温、超高压、超高真空、超强磁场、超弱磁场等。显然，要获取大量人类感官无法直接获取的信息，没有相适应的传感器是不可能的。许多基础科学研究的障碍，首先就在于对象信息的获取存在困难，而一些新机理和高灵敏度的检测传感器的出现，往往会推动该领域内的突破。一些传感器的发展，往往是一些边缘学科开发的先驱。

传感器早已渗透到诸如工业生产、宇宙开发、海洋探测、环境保护、资源调查、医学诊断、生物工程、甚至文物保护等极其之泛的领域。可以毫不夸张地说，从茫茫的太空，到浩瀚的海洋，以至各种复杂的工程系统，几乎每一个现代化项目，都离不开各种各样的传感器。

由此可见，传感器技术是物联网感知层最核心的技术之一，并且其在发展经济、推动社会进步方面的重要作用，是十分明显的。

2.3.1　传感器工作原理及分类

根据传感器工作原理的不同，可分为物理传感器和化学传感器。物理传感器应用的是物理效应，诸如压电效应、磁致伸缩现象、离化、极化、热电、光电、磁电等效应。被测信号量的微小变化都将转换成电信号。化学传感器包括那些以化学吸附、电化学反应等现象为因果关系的传感器，被测信号量的微小变化也将转换成电信号。

有些传感器既不能划分到物理类，也不能划分为化学类。大多数传感器是以物理原理为基础运作的。化学传感器技术问题较多，例如可靠性问题、规模生产的可能性、价格问题等，解决了这类难题，化学传感器的应用将会有巨大增长。

微电子技术、通信技术以及无线通信等技术的发展，使得传感器的体积越来越小，并在微小体积的芯片内集成了信息采集、数据处理以及无线通信等许多功能。

常见的传感器包括温度、压力、湿度、光、霍尔磁性传感器等。

（1）温度传感器

常见的温度传感器包括热敏电阻、半导体温度传感器以及温差电偶（见图 2-4）。

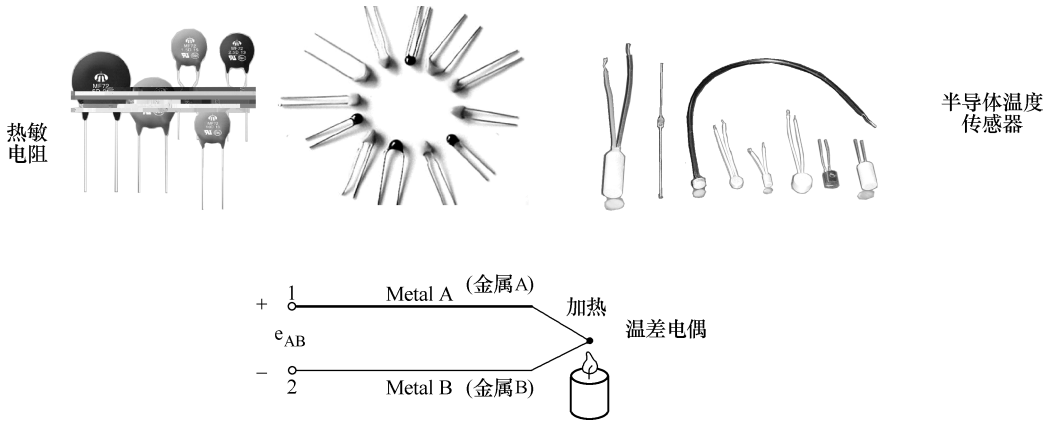


图 2-4　温度传感器

热敏电阻主要是利用各种材料电阻率的温度敏感性，根据材料的不同，热敏电阻可以用于设备的过热保护以及温控报警等。

半导体温度传感器利用半导体器件的温度敏感性来测量温度，具有成本低廉、线性度好等优点。

温差电偶则是利用温差电现象，把被测端的温度转化为电压和电流的变化；由不同金属材料构成的温差电偶，能够在比较大的范围内测量温度，例如 –200 ~ 2000℃。

（2）压力传感器

常见的压力传感器在受到外部压力时会产生一定的内部结构的变形或位移，进而转化为电特性的改变，产生相应的电信号（见图 2-5）。

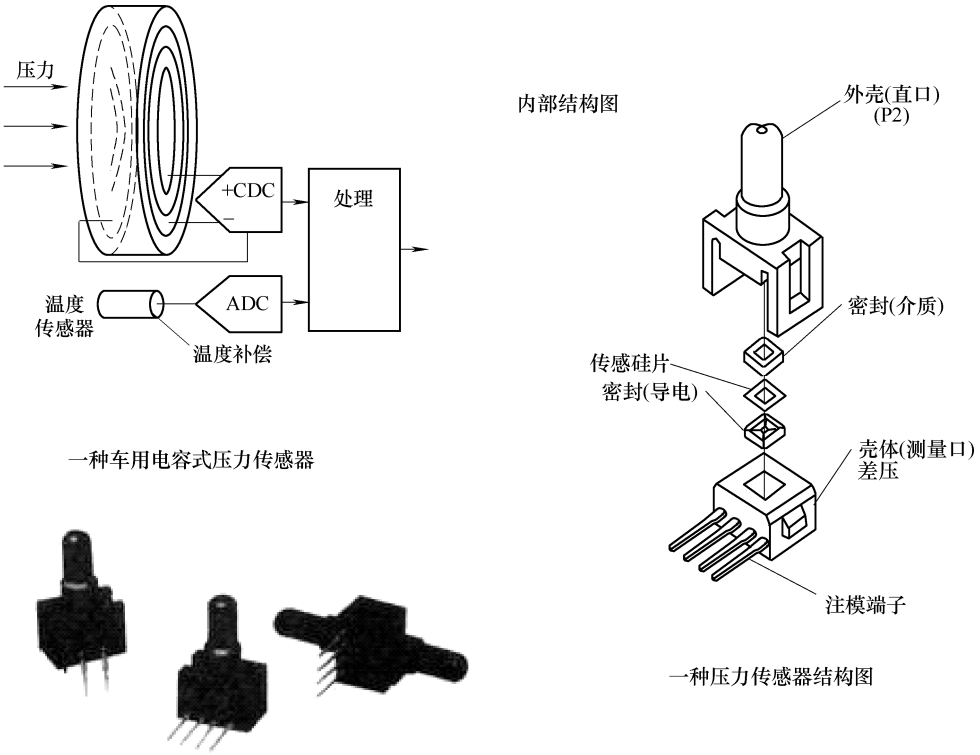


图 2-5　压力传感器

（3）湿度传感器

主要包括电阻式和电容式两个类别（见图 2-6）。

电阻式湿度传感器也成为湿敏电阻，利用氯化锂、碳、陶瓷等材料的电阻率的湿度敏感性来探测湿度。

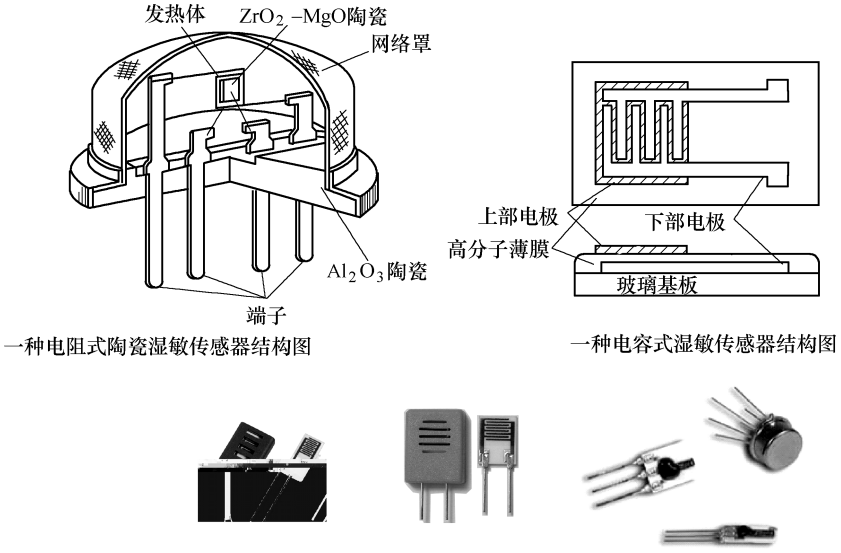
电容式湿度传感器也称为湿敏电容，利用材料的介电系数的湿度敏感性来探测湿度。

（4）光传感器

光传感器可以分为光敏电阻以及光电传感器两个大类（见图 2-7）。

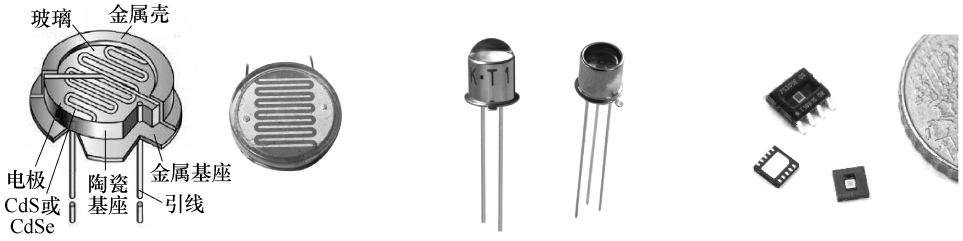
光敏电阻主要利用各种材料的电阻率的光敏感性来进行光探测。

光电传感器主要包括光敏二极管和光敏晶体管，这两种器件都是利用半导体器件对



一种电阻式陶瓷湿敏传感器结构图　　一种电容式湿敏传感器结构图

图 2-6　湿度传感器



光敏电阻结构图与实物　　光敏晶体管　　集成光传感器

图 2-7　光传感器

光照的敏感性。光敏二极管的反向饱和电流在光照的作用下会显著变大，而光敏晶体管在光照时其集电极、发射极导通，类似于受光照控制的开关。此外，为方便使用，市场上出现了把光敏二极管和光敏晶体管与后续信号处理电路制作成一个芯片的集成光传感器。

光传感器的不同种类可以覆盖可见光、红外线（热辐射）以及紫外线等波长范围的传感应用。

（5）霍尔（磁性）传感器

霍尔传感器是利用霍尔效应制成的一种磁性传感器（见图 2-8）。霍尔效应是指：把一个金属或者半导体材料薄片置于磁场中，当有电流流过时，由于形成电流的电子在磁场中运动而受到磁场的作用力，会使得材料中产生与电流方向垂直的电压差。可以通过测量霍尔传感器所产生的电压的大小来计算磁场的强度（见图 2-9）。

霍尔传感器结合不同的结构，能够间接测量电流、振动、位移、速度、加速度、转速等，具有广泛的应用价值。

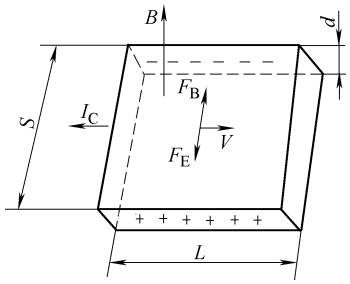


图 2-8　霍尔效应

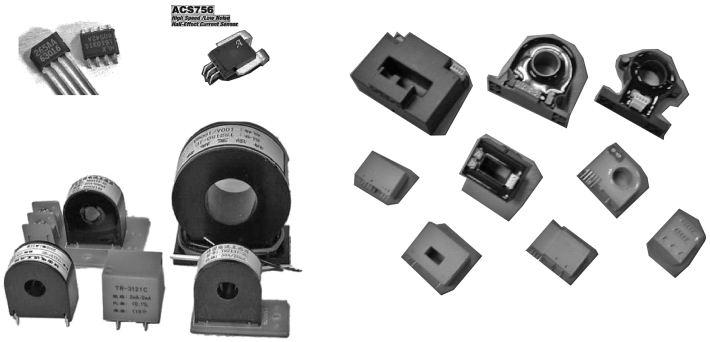


图 2-9　霍尔传感器

2.3.2　传感器技术发展趋势

传感器的发展正朝着小型化和智能化方向发展，其中最具代表性的是微机电系统（Micro-Electro-Mechanical System，MEMS）传感器和智能传感器。

MEMS 传感器由于体积小、功耗低，便于集成，在物联网时代应用非常广泛。它是一种由微电子、微机械部件构成的微型器件，多采用半导体工艺加工。目前已经出现的 MEMS 传感器包括压力传感器、加速度计、微陀螺仪、墨水喷嘴和硬盘驱动头等。MEMS 传感器的出现体现了当前的传感器小型化发展趋势。

智能传感器是一种具有一定信息处理能力的传感器，目前多采用把传统的传感器与微处理器结合的方式来制造。如图 2-10 所示，在传统的传感器构成的应用系统中，传感器所采集的信号通常要传输到系统中的主机中进行分析处理；而由智能传感器构成的应用系统中，其包含的微处理器能够对采集的信号进行分析处理，然后把处理结果发送给系统中的主机。智能传感器能够显著减小传感器与主机之间的通信量，并简化了主机软件的复杂程度，使得包含多种不同类别的传感器应用系统，易于实现；此外，智能传感器常常还能进行自检、诊断和校正。

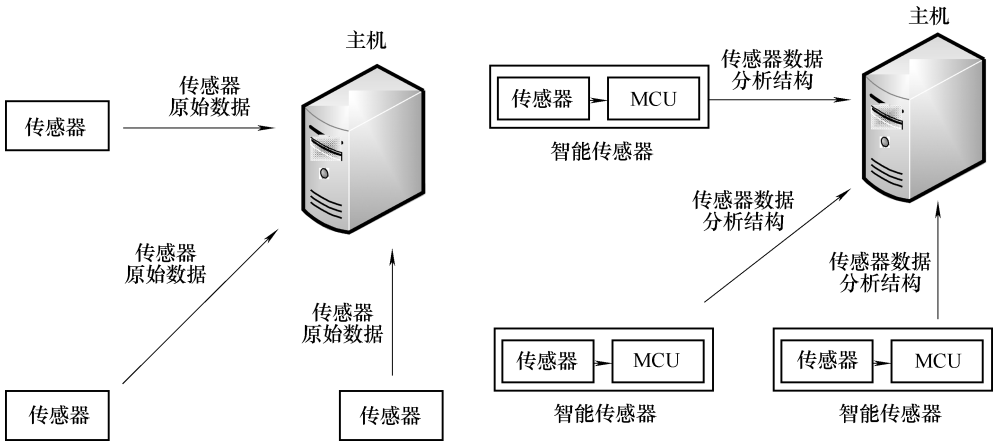


图 2-10　智能传感器

2.3.3　传感器的特性

（1）传感器静态特性

传感器的静态特性是指对静态的输入信号，传感器的输出量与输入量之间所具有相互关系。因为这时输入量和输出量都和时间无关，所以它们之间的关系，即传感器的静态特性可用一个不含时间变量的代数方程，或以输入量作横坐标，把与其对应的输出量作纵坐标而画出的特性曲线来描述。表征传感器静态特性的主要参数有：线性度、灵敏度、迟滞、重复性、漂移等。

1）线性度：指传感器输出量与输入量之间的实际关系曲线偏离拟合直线的程度。定义为在全量程范围内实际特性曲线与拟合直线之间的最大偏差值与满量程输出值之比。

2）灵敏度：灵敏度是传感器静态特性的一个重要指标。其定义为输出量的增量与引起该增量的相应输入量增量之比。用 S 表示灵敏度。

3）迟滞：传感器在输入量由小到大（正行程）及输入量由大到小（反行程）变化期间其输入输出特性曲线不重合的现象称为迟滞。对于同一大小的输入信号，传感器的正反行程输出信号大小不相等，这个差值称为迟滞差值。

4）重复性：重复性是指传感器在输入量按同一方向做全量程连续多次变化时，所得特性曲线不一致的程度。

5）漂移：传感器的漂移是指在输入量不变的情况下，传感器输出量随着时间变化，此现象称为漂移。产生漂移的原因有两个方面：一是传感器自身结构参数；二是周围环境（如温度、湿度等）。

（2）传感器动态特性

所谓动态特性，是指传感器在输入变化时，它的输出的特性。在实际工作中，传感器的动态特性常用它对某些标准输入信号的响应来表示。这是因为传感器对标准输入信号的响应容易用实验方法求得，并且它对标准输入信号的响应与它对任意输入信号的响应之间存在一定的关系，往往知道了前者就能推定后者。最常用的标准输入信号有阶跃信号和正弦信号两种，所以传感器的动态特性也常用阶跃响应和频率响应来表示。

（3）传感器的线性度

通常情况下，传感器的实际静态特性输出是条曲线而非直线。在实际工作中，为使仪表具有均匀刻度的读数，常用一条拟合直线近似地代表实际的特性曲线，线性度（非线性误差）就是这个近似程度的一个性能指标。

（4）传感器的灵敏度

灵敏度是指传感器在稳态工作情况下输出量变化 $\triangle y$ 对输入量变化 $\triangle x$ 的比值。它是输出—输入特性曲线的斜率。如果传感器的输出和输入之间为线性关系，则灵敏度 S 是一个常数。否则，它将随输入量的变化而变化。灵敏度的量纲是输出、输入量的量纲之比。例如，某位移传感器，在位移变化 1mm 时，输出电压变化为 200mV，则其灵敏度应表示为 200mV/mm。当传感器的输出、输入量的量纲相同时，灵敏度可理解为放大倍数。提高灵敏度，可得到较高的测量准确度。但灵敏度越高，测量范围越窄，稳定性也往往越差。

（5）传感器的分辨率

分辨率是指传感器可感受到的被测量的最小变化的能力。也就是说，如果输入量从某一

非零值缓慢地变化。当输入变化值未超过某一数值时，传感器的输出不会发生变化，即传感器对此输入量的变化是分辨不出来的。只有当输入量的变化超过分辨率时，其输出才会发生变化。通常传感器在满量程范围内各点的分辨率并不相同，因此常用满量程中能使输出量产生阶跃变化的输入量中的最大变化值作为衡量分辨率的指标。上述指标若用满量程的百分比表示，则称为分辨率。分辨率与传感器的稳定性有负相关性。

2.4　无线传感器网络技术

物联网在感知领域的另外一个术语就是传感网，它将各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息，通过嵌入式系统对信息进行处理，并通过自组织无线网络通信，实现对物理世界的动态协同感知。可以看出，传感网是以感知为目的的物物互联网络。无线传感器网络技术是传感网中最核心的技术之一。

自人类踏入信息时代，自然界的信息通过传感器源源而来。而随着技术的发展，人们已不满足于原有单一的、独立的传感器系统。很多时候，我们需要将来自不同区域的信息联合汇总，从而实现对现场状况的综合判断。无线传感器网络是在信息采集方面非常高效的网络。

无线传感器网络是一种由独立分布的节点以及网关构成的传感器网络，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告知对象的信息，并发送给观察者。安放在不同地点的传感器节点不断采集外界的物理信息，相互独立的节点之间通过无线网络进行通信。无线传感器网络的每个节点都能够实现采集和数据的简单处理，还能接收来自其他节点的数据，并最终将数据发送到网关。工程师可以从网关获取数据，查看历史数据记录或进行分析。

传感器网络中，除了少数节点需要移动以外，大部分节点都是静止的，它们可以运行在人无法接近的恶劣甚至危险的远程环境中，因此在物联网中有很广泛的应用前景。

无线传感器网络是一个涉及多学科高度交叉、知识高度集成的前沿热点研究领域。传感器技术、微机电系统、现代网络和无线通信等技术的进步，推动了现代无线传感器网络的产生和发展。无线传感器网络扩展了人们信息获取能力，将客观世界的物理信息同传输网络连接在一起，在下一代网络中将为人们提供最直接、最有效、最真实的信息。无线传感器网络能够获取客观物理信息，具有十分广阔的应用前景，能应用于军事国防、工农业控制、城市管理、生物医疗、环境检测、抢险救灾、危险区域远程控制等领域，已经引起了许多国家学术界和工业界的高度重视，被认为是对 21 世纪产生巨大影响力的技术之一。

物联网中，有大量数据需要采集，如何有效地采集这些数据是物联网中一个比较重要的问题。各种传感器可以有效地解决这个问题。传感器可以很灵活的配置，在恶劣的环境下也能够正常工作。能够满足各种环境中的数据采集工作。具有 RFID、条形码、电子标签等技术无法比拟的优势。但是无线传感器网络和物联网是两个不同的概念，不能混淆。

WSN 与物联网的关系，如果把物联网比作人体，则 RFID 可以视为“眼睛”，WSN 可以视为“皮肤”。RFID 解决“WHO”，利用应答器，实现的是对物品的标志与识别；而 WSN 解决“HOW”，利用传感器，实现对物体状态的把握；眼睛可以识别，皮肤可以感觉，眼睛

的功能不在于感觉温度的变化，而皮肤的功能也不是用来辨别哪个人或哪件东西。WSN 利用无线技术可以自成体系地单独使用，也可以作为物联网的“神经末梢”。

虽然无线传感器网络和物联网不是一个概念，但是无线传感器网络作为一种物理信号检测传输的高效手段，与物联网中的感知层有着十分密切的关系。物联网感知层获取物体信息的方法除了 RFID 的电子标签，更要依靠使用灵活方便的传感器。在物联网这一产业中，结合无线传感器网络中的传感器获取信息的方法和技术也是物联网发展的一个必然结果。

2.4.1　无线传感器网络的组成

无线传感器网络结构如图 2-11 所示，该体系包括传感器节点（Sensor Node）、汇聚节点（Sink Node）和任务管理单元。大量的传感器节点被随机分布在所需要监测的区域内，通过自组织的方式形成网络。传感器节点所监测到的数据通过附近的传感器节点依照一定的数据融合协议逐条地传送到汇聚节点，然后通过互联网等手段将数据传输到任务管理单元，用户可以通过任务管理单元对传感器节点进行配置管理，发布所需要监测的数据类型等任务并收集处理监测到的数据。

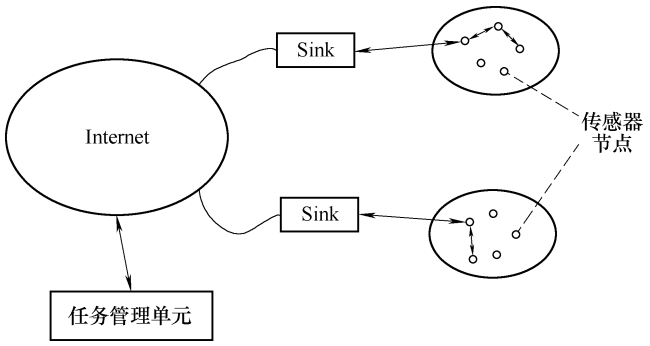


图 2-11　无线传感器网络结构

传感器节点的组成一般都由传感器模块（由传感器和模-数转换器组成）、处理模块（由嵌入式系统构成，包括 CPU、存储器、嵌入式操作系统等）、无线收发模块（由无线通信器件组成）和能量供应模块这 4 部分组成（见图 2-12）。

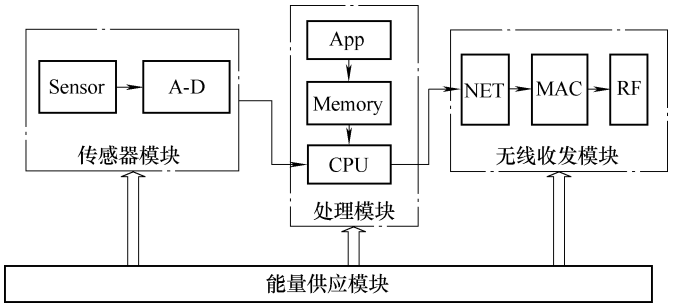


图 2-12　传感器网络节点的组成

传感器模块负责监测区域内信息的采集和数据转换；处理模块负责控制整个传感器节点的操作、存储和处理本身采集的数据以及其他节点发来的数据；无线收发模块负责与其他传感器节点进行无线通信，交换控制消息和收发采集数据；能量供应模块为传感器节点提供运行所需的能量，通常采用微型电池。

在无线传感器网络中，节点任意散落在被监测区域内，这一过程是通过飞行器撒播、人工埋置和火箭弹射等方式完成的，节点以自组织形式构成网络，通过多跳中继方式将监测数据传到汇聚节点，最终借助长距离或临时建立的 Sink 链路将整个区域内的数据传送到远程中心进行集中处理。卫星链路可用作 Sink 链路，借助游弋在监测区上空的无人飞机收集汇聚节点上的数据也是一种方式，UC Berkeley 在进行 UAV（Unmanned Aerial Vehicle）项目的外场测试时便采用了这种方式。如果网络规模太大，可以采用聚类分层的管理模式，图2-13给出了无线传感器网络体系结构一般形式的描述。

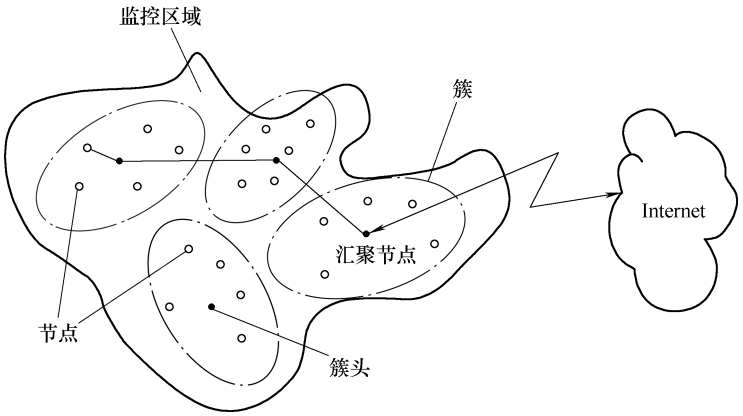


图 2-13　无线传感器网络的体系结构

2.4.2　无线传感器网络的通信协议

如图 2-14 所示是无线传感器网络汇聚节点和传感器节点的协议栈，与互联网协议栈的五层协议相对应。协议栈还包括能量管理、移动管理和任务管理。这些管理平台使得传感器节点能够以高效的方式协同工作，在节点移动的无线传感器网络中转发数据，并支持多任务和资源共享。物理层负责提供简单但健壮的调制和无线收发技术，接收和发送数据；数据链

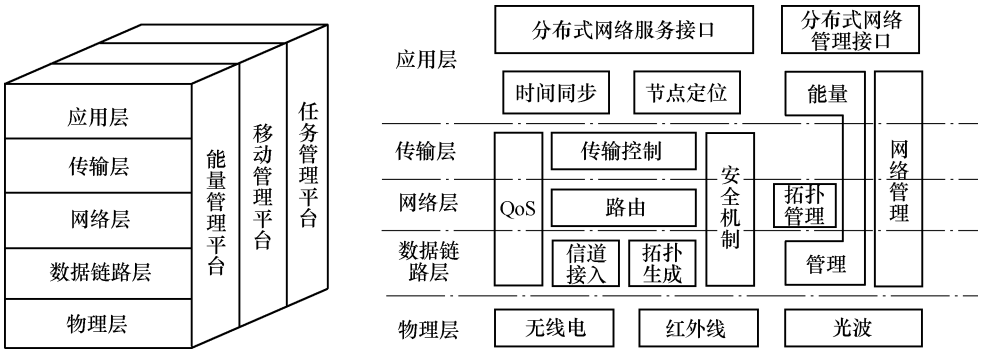


图 2-14　无线传感器网络协议栈

路层负责无线信道的使用控制，减少邻居节点广播引起的冲突；网络层实现数据的融合、负责路由生成与路由选择；传输层负责数据流的传输控制，是保证通信服务质量的重要部分；应用层包括一系列基于监测任务的应用层软件。

能量管理负责控制节点对能量的使用，为延长网络存活时间有效地利用能源；拓扑管理负责保持网络的连通和数据有效传输；网络管理负责网络维护、诊断，并向用户提供网络管理服务接口，通常包括数据收集、数据处理、数据分析和故障处理等功能；QoS 是为应用程序提供足够的资源使它们以用户可以接受的性能指标指示工作；时间同步为传感器节点提供全局同步的时钟支持；节点定位确定每个传感器节点的相对位置或绝对的地理坐标。

2.4.3　无线传感器网络的特点

（1）大规模网络

为了获取精确信息，在监测区域通常部署大量传感器节点，传感器节点数量可能达到成千上万，甚至更多。无线传感器网络的大规模性有两种情况：第一是很大的地理区域，如在原始大森林采用无线传感器网络进行森林防火和环境监测，需要部署大量的传感器节点；第二是节点密集地部署在一个面积不是很大的空间内。

无线传感器网络的大规模性具有如下优势：通过不同空间视角获得的信息具有更大的信噪比；通过分布式处理大量的采集信息能够提高监测的准确度，降低对单个节点传感器的准确度要求；大量冗余节点的存在，使得系统具有很强的容错性能；大量节点能够增大覆盖的监测区域，减少盲区。

（2）自组织网络

在无线传感器网络应用中，传感器节点的位置不能预先精确设定，节点之间的相互邻居关系预先也不知道，如通过飞机播撒大量传感器节点到面积广阔的原始森林中，或随意放置到人类不可到达或危险的区域。这样就要求传感器节点具有自组织的能力，能够自动进行配置和管理，通过拓扑控制机制和网络协议自动形成转发监测数据的多跳无线网络系统。

在无线传感器网络使用过程中，部分传感器节点由于能量耗尽或环境因素造成失效，也有一些节点为了弥补失效节点、增加监测准确度而补充到网络中，这样在无线传感器网络中的节点个数就会动态地增加或减少，从而使网络的拓扑结构随之变化。无线传感器网络的自组织性要能够适应这种动态的网络拓扑结构。

（3）动态性网络

无线传感器网络的拓扑结构可能因为下列因素而改变：环境因素或电能耗尽造成的传感器节点出现故障或失效；环境条件变化可能造成无线通信链路带宽变化，甚至时断时通；无线传感器网络的传感器、感知对象和观察者这三要素都可能具有移动性；新节点的加入。这就要求无线传感器网络系统要能够适应这种变化，具有动态的系统可重构性。

（4）应用相关的网络

无线传感器网络用来感知客观物理世界，获取物理世界的信息量。客观世界的物理量多种多样，不可穷尽，不同的无线传感器网络应用关心不同的物理量，因此对传感器的应用系统也有多种多样的要求。

不同的应用背景对无线传感器网络的要求不同，其硬件平台、软件系统和网络协议必然会有很大差别。所以无线传感器网络不能像互联网一样，有统一的通信协议平台。

只有让系统更贴近应用，才能做出最高效的目标系统。针对每一个具体应用来研究无线传感器网络技术，这是无线传感器网络设计不同于传统无线网络的显著特征。

（5）以数据为中心的网络

在互联网中，网络设备用网络中唯一的IP地址标识，资源定位和信息传输取决于终端、路由器、服务器等网络设备的IP地址。如果想访问互联网中的资源，首先要知道存放资源的服务器IP地址。可以说目前的互联网是一个以地址为中心的网络。

无线传感器网络是任务型的网络，是以数据为中心的。脱离无线传感器网络谈论传感器节点没有任何意义。无线传感器网络中的节点采用节点编号标识，节点编号是否需要全网仅取决于网络通信协议的设计。由于传感器节点随机部署，构成的无线传感器网络与节点编号之间的关系是完全动态的，表现为节点编号与节点位置没有必然联系。

2.4.4　无线传感器网络面临的挑战

（1）电源能量有限

传感器节点体积微小，通常携带能量十分有限的电池。由于传感器节点个数多、成本要求低廉、分布区域广，而且部署区域环境复杂，有些区域甚至人员不能到达，所以传感器节点通过更换电池的方式来补充能源是不现实的。如何高效使用能量来最大化网络生命周期是无线传感器网络面临的首要挑战。

（2）通信能力有限

随着节点之间通信距离的增加，通信消耗的能量也将急剧增加。因此，在满足通信连通度的前提下应尽量缩短单跳通信距离。由于传感器节点的能量限制和网络覆盖区域大，无线传感器网络采用多跳路由的传输机制。传感器节点的无线通信带宽有限，通常仅有几百kbit/s的速率。在这样的通信环境和节点有限通信能力的情况下，就需要考虑特定的网络通信机制来满足无线传感器网络的通信需求。

（3）安全性的问题

无线信道、有限的能量、分布式控制都使得无线传感器网络更容易受到攻击。被动窃听、主动入侵、拒绝服务则是这些攻击的常见方式。此外，还包括数据包的完整性鉴定、新鲜性确认等问题。因此，安全性在网络的设计中至关重要。

2.4.5　无线传感器网络的关键技术

（1）网络拓扑控制

无线传感器网络拓扑控制目前主要的研究问题是在满足网络覆盖度和连通度的前提下，通过功率控制和骨干网节点选择，剔除节点之间不必要的无线通信链路，生成一个高效的数据转发的网络拓扑结构。

通过拓扑控制自动生成的良好拓扑结构能够提高路由协议和MAC协议的效率，为数据融合、时钟同步和目标定位等很多方面奠定基础。

目前的无线传感器网络拓扑控制机制包括有传统的功率控制和层次型拓扑控制以及启发式的唤醒/休眠机制。

（2）时钟同步技术

时钟同步是网络协同工作、系统协同休眠、节省能耗以及目标定位技术的基础。目前已有多种针对无线传感器网络的时钟同步算法，主要集中在两个方面：第一，因为 WSN 中时钟同步的重要性，所以研究安全的时钟同步算法就显得尤为重要；第二，从能耗的角度，研究节能、高效的时钟同步算法。因此如何获得安全高效的时钟同步算法，是目前研究的一个热点。

（3）定位技术

地理位置信息是传感器节点采集数据中不可缺少的信息。确定事件发生的位置或采集数据的节点位置是无线传感器网络最基本的功能之一。由于传感器节点存在资源有限、随机部署、通信易受环境干扰甚至节点失效等特点，定位机制必须满足自组织性、健壮性、能量高效、分布式计算等要求。

在无线传感器网络定位过程中，通常会使用三边测量法、三角测量法或极大似然估计法确定节点位置。根据定位过程中是否实际测量节点间的距离或角度，把无线传感器网络中的定位分类为基于距离的定位和距离无关的定位。

（4）网络安全

无线传感器网络作为任务型的网络，不仅要进行数据的传输，而且要进行数据采集和融合、任务的协同控制等。如何保证任务执行的机密性、数据产生的可靠性、数据融合的高效性以及数据传输的安全性，就成为无线传感器网络安全问题需要全面考虑的内容。无线传感器网络需要实现一些最基本的安全机制：机密性、点到点的消息认证、完整性鉴别、新鲜性、认证广播和安全管理。

（5）其他关键技术

MAC 协议、路由协议、数据融合、数据管理、无线通信技术、嵌入式系统以及应用层技术等都是目前无线传感器网络领域中的研究热点问题。

2.4.6　无线传感器网络的应用

（1）军事应用

军事应用是无线传感器网络技术的主要应用领域，由于其特有的无需架设网络设施、可快速展开、抗毁性强等特点，是数字战场无线数据通信的首选技术，是军队在敌对区域中获取情报的重要技术手段。

无线传感器网络是由密集型、低成本、随机分布的节点组成的，自组织性和容错能力使其不会因为某些节点在恶意攻击中的损坏而导致整个系统的崩溃，这一点是传统的传感器技术所无法比拟的，这就使传感器网络非常适合应用于恶劣的战场环境中，包括监控我军兵力、装备和物资，监视冲突区，侦察敌方地形和布防，定位攻击目标，评估损失，侦察和探测核、生物和化学攻击。美国 DARPA（Defense Advanced Research Projects Agency）的 SensIT（Sensor Information Technology）计划就是无线传感器网络应用于军事的典型案例。

（2）商业应用

自组织、微型化和对外部世界的感知能力是无线传感器网络的三大特点，这些特点决定了无线传感器网络在社会商业领域占有一席之地。智能化电器设计就是无线传感器网络的典

型商业应用。很多智能家电带有嵌入式处理器，与执行机构组成的无线网络与互联网连接在一起，利用远程监控系统，可完成对家电的远程遥控，例如可以在回家之前半小时打开空调，这样回家的时候就可以直接享受适合的室温，也可以遥控电饭锅、微波炉、电冰箱、电话机、电视机、录像机、计算机等家电，按照自己的意愿完成相应的各种工作，也可以通过图像传感设备随时监控家庭安全情况。

（3）环境观测

环境检测中对无线传感器网络的应用主要有两个部分：

一是利用无线传感器网络的节点分布的广泛性，可以大范围地采集数据，例如：通过布置传感器节点，可以跟踪候鸟昆虫的迁移，研究它们的生活习性。另外可以通过播撒微型传感器于海洋，监测海洋状况。无线传感器网络还可以监测土壤状态，利用多种传感器来监测降雨量、河水水位和土壤水分，并依此预测爆发山洪的可能性。类似地，无线传感器网络在森林火灾准确预报、及时地预报，天气预报，精细农业，农作物中的害虫监测，土壤的酸碱度和施肥状况，农田管理等都有很大的应用前景。

另一方面，利用无线传感器网络的自组织的特点，可以借助于航天器布撒的传感器节点实现对星球表面长时间监测。除了空间工作站，目前空间探索特殊的环境需要极高的自动化。因此，无线传感器网络技术在空间探索方面有着巨大的应用。NASA 的 JPL（Jet Propulsion Laboratory）研制的 Sensor Web 就是为将来的火星探测进行技术准备的，已在佛罗里达宇航中心周围的环境监测项目中进行测试和完善。

（4）医疗护理

传感器节点小的特点使其在医学上有特殊的用途。如果在住院病人身上安装特殊用途的传感器节点，如心率和血压监测设备，医生利用无线传感器网络就可以随时了解被监护病人的病情，及时有效抢救。将传感器节点按药品种类分别放置，计算机系统即可帮助辨认所开的药品，从而减少病人用错药的可能性。还可以利用无线传感器网络长时间地收集人体的生理数据，这些数据对了解人体活动机理和研制新药品都是非常有用的。

（5）其他方面的应用

除上述作用之外，无线传感器网络还应用于生活的各个方面，例如对建筑物状态监控是利用无线传感器网络来监控建筑物的安全状态，采用无线传感网络对复杂机械进行维护能够降低人工开销。尤其是目前数据处理硬件技术的飞速发展和无线收发硬件的发展，新的技术已经成熟，可以使用无线技术避免昂贵的线缆连接，采用专家系统自动实现数据的采集和分析。

参 考 文 献

[1] 孔宁. 物联网资源寻址关键技术研究 [D]. 北京：中国科学院研究生院（计算机网络信息中心），2008.

[2] 焦宗东. EPC 物联网中流通信息的研究 [D]. 合肥：合肥工业大学，2008.

[3] 潘科. RFID 编码解析网络监控系统的研究与实现 [D]. 武汉：华中科技大学，2008.

[4] 黄小虎. 基于 RFID 技术的 EPC 网络系统研究 [D]. 广州：广东工业大学，2009.

[5] 王玉明. 移动 RFID 网络移动性研究 [D]. 南京：南京邮电大学，2008.

[6] 徐军委. 下一代互联网中无线传感器网络协议理论与技术的研究 [D]. 合肥：中国科学技术大学，2007.

[7] 肖炯强. RFID 编码解析系统的性能改进与测试 [D]. 武汉：华中科技大学，2008.
[8] 周祥. RFID 技术在物联网中应用的关键技术探讨 [D]. 南京：江苏大学，2005.
[9] 孙敏. 移动 RFID 网络与 EPC 网络互通技术的研究 [D]. 南京：南京邮电大学，2008.
[10] 余松森. 物联网 RFID 反碰撞问题研究 [D]. 广州：广东工业大学，2006.
[11] Lu Yan，Yan Zhang，Laurence T. Yang，etc. The Internet of Things：From RFID to the Net-Generation Pervasive Networked Systems [M]. 1st ed. New York：Auerbach Publications，2008.

第 3 章　传输层——汇聚网技术

物联网传输层位于感知层和应用层之间，传输层所要完成的功能是将感知层收集感知的数据信息传输给应用层，使得应用层可以方便地对信息进行分析管理，从而控制整个系统。目前，物联网传输层都是基于现有的通信网和互联网建立的，主要实现感知层数据和控制信息的双向传递、路由和控制。

物联网传输层可分为：汇聚网、接入网和承载网 3 部分（见图 3-1）。

汇聚网主要采用短距离通信技术如 ZigBee、蓝牙和 UWB 等技术，实现小范围感知数据的汇聚。

接入网主要采用 6LoWPAN、M2M 及全 IP 融合架构实现感知数据从汇聚网到承载网的接入。

承载网主要是指各种核心承载网络，如 GSM、GPRS、WiMax、3G/4G、WLAN 等。

本书按照主汇聚网→接入网→承载网路线展开阐述物联网传输层技术，本章介绍汇聚网中典型短距离通信技术：ZigBee、蓝牙和 UWB。

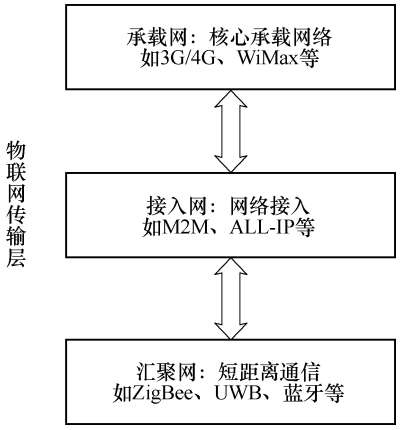


图 3-1　物联网传输层结构

3.1　ZigBee

物联网中，布置了大量的节点，这些节点不仅数目众多而且分布广泛，有很多处于室外的采集节点无法连接到电网，所以在进行无线传输的时候，要考虑到带宽、传输距离以及功耗等因素。

在物联网技术出现之初，已有的无线协议很难满足低功耗、低花费、高容错性的要求。此时 ZigBee 技术的产生带来了福音。

ZigBee 无线技术是一种全球领先的低成本、低速率、小范围无线网络标准。ZigBee 联盟是一个基于全球开放标准的研究可靠、高效、无线网络管理和控制产品的联合组织。ZigBee 联盟和 IEEE 802.15.4 WPAN 工作组是 ZigBee 和基于 IEEE 802.15.4 的无线网络应用标准的官方来源。

ZigBee 拥有 250kbit/s 的带宽，传输距离可达 1km 以上。并且功耗更小，采用普通 AA 电池就能够支持设备在高达数年的时间内连续工作。它近 10 年来，应用于无线传感器网络中，非常好地完成了传输任务，同样也可以应用在物联网的无线传输中。

3.1.1　ZigBee 技术简介

3.1.1.1　什么是 ZigBee

ZigBee 是规定了一系列短距离无线网络的数据传输速率通信协议的标准，主要用于近距

离无线连接。基于这一标准的设备工作在868MHz、915MHz、2.4GHz频带上。最大数据传输率为250kbit/s。ZigBee具有低功耗、低速率、低时延等特性。在很多ZigBee应用中，无线设备的活动时间有限，大多数时间均工作在省电模式（睡眠模式）下。因此，ZigBee设备可以在不更换电池的情况下连续工作几年。

3.1.1.2　ZigBee的产生背景

2000年12月，IEEE成立IEEE 802.15.4工作组，致力于开发一种可应用在固定、便携或移动设备上的，低成本、低功耗和低速率的无线连接技术。

2001年8月，美国HONEYWELL等公司发起成立了ZigBee联盟，他们提出的ZigBee规范被确认为IEEE 802.15.4标准。

2002年，ZigBee联盟成立。2003年，该标准通过。2004年，ZigBee V1.0诞生，它是ZigBee的第一个规范，2006年，推出ZigBee 2006，完善了2004年版本。2007年底，ZigBee PRO推出。

ZigBee的底层技术基于IEEE 802.15.4物理层和MAC层直接引用了IEEE 802.15.4。

3.1.1.3　ZigBee联盟

ZigBee联盟是一个高速成长的非盈利业界组织，成员包括国际著名半导体生产商、技术提供者、技术集成商以及最终使用者。联盟制定了基于IEEE 802.15.4，具有高可靠、高性价比、低功耗的网络应用规格。ZigBee标准由ZigBee联盟制定。ZigBee联盟有几百个成员公司。

ZigBee联盟的主要目标是以通过加入无线网络功能，为消费者提供更富有弹性、更容易使用的电子产品。ZigBee技术能融入各类电子产品，应用范围横跨全球的民用、商用、公共事业以及工业等市场。使得联盟会员可以利用ZigBee这个标准化无线网络平台，设计出简单、可靠、便宜又节省电力的各种产品来。

ZigBee联盟关注的焦点为制定网络、安全和应用软件层；提供不同产品的协调性及互通性测试规格；在世界各地推广ZigBee品牌并争取市场的关注；管理技术的发展。

ZigBee联盟对ZigBee标准的制定：IEEE 802.15.4的物理层、MAC层及数据链路层，标准已在2003年5月发布。ZigBee网络层、加密层及应用描述层的制定也取得了较大的进展。V1.0版本已经发布。其他应用领域及其相关的设备描述也会陆续发布。由于ZigBee不仅只是IEEE 802.15.4的代名词，而且IEEE仅处理低级MAC层和物理层协议，因此ZigBee联盟对其网络层协议和API进行了标准化。完全协议用于一次可直接连接到一个设备的基本节点的4KB或者作为Hub或路由器的协调器的32KB。每个协调器可连接多达255个节点，而几个协调器则可形成一个网络，对路由传输的数目则没有限制。ZigBee联盟还开发了安全层，以保证这种便携设备不会意外泄露其标识，而且这种利用网络的远距离传输不会被其他节点获得。

3.1.1.4　ZigBee性能分析

1）低功耗：由于ZigBee传输速率低，通信距离近，发射功率仅为1mW；而且在不工作的时候，启用休眠模式，此时能耗可能只有正常工作状态下的千分之一，显然ZigBee设备非常省电。

2）低成本：因为ZigBee协议简单，所以对控制要求不高。

3）低速率：ZigBee以20～250kbit/s的较低速率工作，在2.4GHz，915MHz，868MHz

的工作频率下，分别提供250kbit/s、40kbit/s和20kbit/s的原始数据吞吐率。

4）近距离：传输范围一般介于10～100m，在增加RF发射功率后，也可增加到1～3km。这指的是相邻节点间的距离。如果通过路由和节点间通信的接力，传输距离将可以更远。

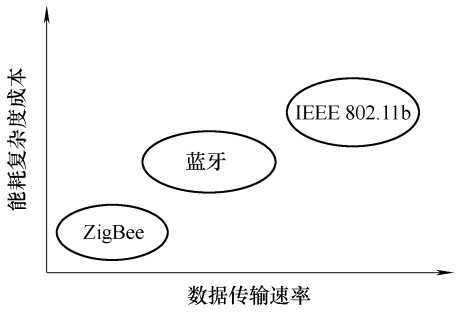
5）短时延：ZigBee的响应速度较快，一般从睡眠转入工作状态只需15ms，节点连接进入网络只需30ms，进一步节省了电能。相比较，蓝牙需要3～10s，Wi-Fi需要3s。

6）大规模的组网能力：ZigBee可采用星形、树状和网状网络结构，由一个主节点管理若干子节点，最多一个主节点可管理254个子节点；同时主节点还可由上一层网络节点管理，最多可组成65000个节点的大网。

7）高可靠性：ZigBee具有很高的可靠性，包括MAC应用层（APS部分）的应答重传功能、MAC层的CSMA机制使节点发送前先监听信道，可以起到避开干扰的作用、当ZigBee网络受到外界干扰，无法正常工作时，整个网络可以动态地切换到另一个工作信道上。

3.1.1.5　ZigBee与蓝牙、IEEE 802.11b的区别

图3-2展示了ZigBee、蓝牙和IEEE 802.11b 3种标准的不同。



	数据传输速率	典型范围/m	应用举例
ZigBee	20～250 kbit/s	10～100	无线传感器网络
蓝牙	1～3 Mbit/s	2～10	无线耳机，无线鼠标
IEEE 802.11b	1～11 Mbit/s	30～100	无线网络连接

图3-2　ZigBee、蓝牙和IEEE 802.11b比较

IEEE 802.11b是一种家庭标准，把IEEE 802.11b拿来进行比较是因为它的工作频率是2.4GHz，和蓝牙、ZigBee相同。IEEE 802.11b数据传输速率很高（最高为11Mbit/s）并且给一种无线网络连接提供了一种典型应用。典型的IEEE 802.11b的室内范围是30～100m。蓝牙是一种较低数据传输速率（低于3Mbit/s）的标准，室内范围是2～10m，蓝牙的一种广泛应用是无线蓝牙耳机。ZigBee有最低的数据率并且拥有最高的电池寿命。

ZigBee技术的低传输速率特性意味着它不适合无线网络连接或者需要CD音质保证的场合。然而，如果网络中仅需要进行一些简单命令或者其他信息的收发工作，比如无线传感器传输温度、湿度等信息时，ZigBee具有蓝牙和IEEE 802.11b无法相比的优势：成本低、功耗低，并且易于传输。

3.1.2　ZigBee网络拓扑结构

ZigBee无线数据传输网络设备按照其功能的不同可以分为两类：全功能设备（Full-Function Device，FFD）和精简功能设备（Reduced-Function Device，RFD）。FFD可以实现全部IEEE 802.15.4协议功能，一般在网络结构中拥有网络控制和管理的功能。RFD仅能实现部分IEEE 802.15.4协议功能，可以用于实现简单的控制功能，传输的数据量较少，对传

输资源和通信资源占用不多，在网络结构中一般作为通信终端。

IEEE 802.15.4 协议中规定的 PAN 协调器、协调器、一般设备在 ZigBee 网络中被称为 ZigBee 协调器、路由器和终端设备。ZigBee 网络协调者主要功能有建立网络，并对网络进行相关配置；路由器的主要功能是寻找、建立和修复网络报文的路由信息，并转发网络报文；网络终端的功能相对简单，它可以加入、退出网络，可以发送、接收网络报文。终端设备不能转发报文。

ZigBee 网络有 3 种不同的拓扑结构，分别为星形网、树状网和网状网。

3.1.2.1　星形网络

星形拓扑结构中，ZigBee 网络协调器作为中心节点，终端设备和路由器都可以直接与协调器相连，协调器属于全功能设备，如图 3-3 所示。

星形拓扑结构的网络是一种发散式网络，这种网络属于集中控制型网络，整个网络由中心节点执行集中式通行控制管理，终端设备之间要进行通信都要先将数据发送到网络协调器，再由网络协调器将数据送到目地节点。这种结构中，路由器不具有路由功能。星形网络适合小范围的室内应用：比如家庭自动化、个人计算机外设以及个人健康护理等。

星形结构的网络优点：

1）构造简单。

2）易于管理。

3）网络成本低。

星形结构的网络缺点：

1）中心节点负担过重。

2）节点之间灵活性差。

3）网络过于简单，覆盖范围有限，只能适用于小型网络。

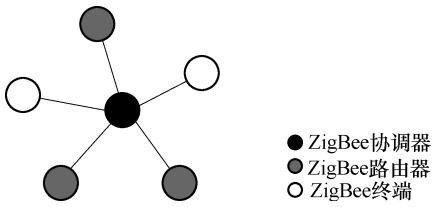


图 3-3　星形结构

3.1.2.2　树状网络

树状网络拓扑是由 ZigBee 协调器、若干个路由器及终端设备组成的，如图 3-4 所示。整个网络是以 ZigBee 协调器为根组成一个树状网络，树状网络中的协调器的功能不再是转发数据，而是进行网络的控制和管理功能，还可以完成节点注册。网络末端的“叶”节点为终端设备。一般而言，协调器是 FFD，终端设备是 RFD。

树状网络的组网过程：

同星形网络一样，创建网络也需要ZigBee协调器完成。

如果网络中不存在其他协调器：

1）FFD 作为 ZigBee 协调器选择网络标识符。

2）ZigBee 协调器向邻近的设备发送信标，接受其他设备的连接，形成树的第一级，此时 ZigBee 协调器与这些设备之间形成父子关系。

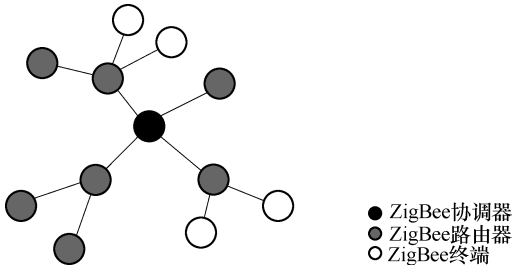


图 3-4　树状网络

3）被协调器连接的路由器所连接的目的协调器为它分配一个地址块，路由器根据接收到的协调器信标的信息，配置自己的信标并发送到网络中，允许其他设备与自己建立连接，成为其子设备。

如果网络中存在其他协调器，ZigBee FFD 以路由器的身份与网络连接，进行上述 3）步骤的过程。终端设备与网络连接时，则 ZigBee 协调器分配给它一个唯一的 16 位网络地址；路由器在转发消息时需要计算与目标设备的关系，并根据此来决定向自己的父节点转发还是子节点转发。

树状拓扑支持“多跳”信息服务网络，可以实现网络范围扩展。树状拓扑利用路由器对星形网络进行了扩充，保持了星形拓扑的简单性。然而，树状结构路径往往不是最优，不能很好地适应外部的动态环境。由于信息源与目的之间只有一条通信链路，任何一个节点发生故障或者中断时，将使部分节点脱离网络。一般来说 ZigBee 是一种高可靠的无线数据传输网络，类似于 CDMA 和 GSM 网络。ZigBee 数据传输模块类似于移动网络基站。通信距离从标准的 75m 到几百米、几千米，并且支持扩展。

树状网络的优点：

1）由于树状网络是对星形网络的扩充，所以其成本也较低，所需资源较少。

2）网络结构简单。

3）网络覆盖范围较大。

树状网络的缺点是网络稳定性较差，如果其中某节点断开，会导致与其相关联的节点脱离网络，所以这种结构的网络不适合动态变化的环境。

3.1.2.3　网状网络

网状网络是 ZigBee 网络中最复杂的结构，如图 3-5 所示。在网状网络中，只要两个 FFD 设备位于彼此的无线通信范围内，它们都可以直接进行通信。也就是说，网络中的路由器可以和通信范围里的所有节点进行通信。在这种特殊的网络结构中，可以进行路由的自动建立和维护。每个 FFD 都可以完成对网络报文的路由和转发。

网状网络采用多跳式路由通信。网络中各节点的地位是平等的，没有父子节点之分。对于没有直接相连的节点可以通过多跳转发的方式进行通信，适合距离较远比较分散的结构。

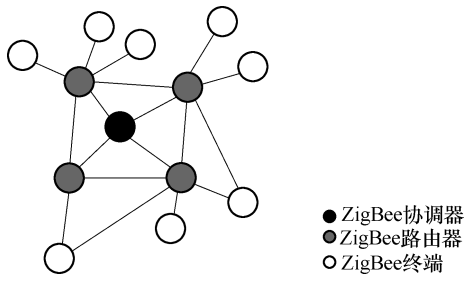


图 3-5　网状网络

网状网络的优点：

1）网络灵活性很强。节点可以通过多条路径传输数据。网络还具备自组织、自愈功能。

2）网络的可靠性高。如果网络中出现节点失效，与其相关联的节点可以通过寻找其他路径与目的节点进行通信，不会影响到网络的正常运行。

3）覆盖面积大。

网状网络的缺点：

1）网络结构复杂。

2）对节点存储能力和数据处理能力要求较高；由于网络需要进行灵活的路由选择，节点的处理数据能力和存储能力显然要求比前两种网络要更高。

一般来讲，由于和星形网络、树状网络相比，网状网络更加复杂，所以在组建网络拓扑

结构时，常常采用星形网络和树状网络。

3.1.3　ZigBee 的协议栈

ZigBee 协议栈架构是建立在 IEEE 802.15.4 标准基础上的。由于 ZigBee 技术是 ZigBee 联盟在 IEEE 802.15.4 定义的物理（PHY）层和媒体访问控制（MAC）层基础之上制定的一种低速无线个域网（LR-WPAN）技术规范，所以 ZigBee 的协议栈的物理（PHY）层和媒体访问控制（MAC）层是按照 IEEE 802.15.4 标准规定来工作的。ZigBee 联盟在其基础上定义了 ZigBee 协议的网络（NWK）层、应用层（APL）和安全服务规范，如图 3-6 所示。

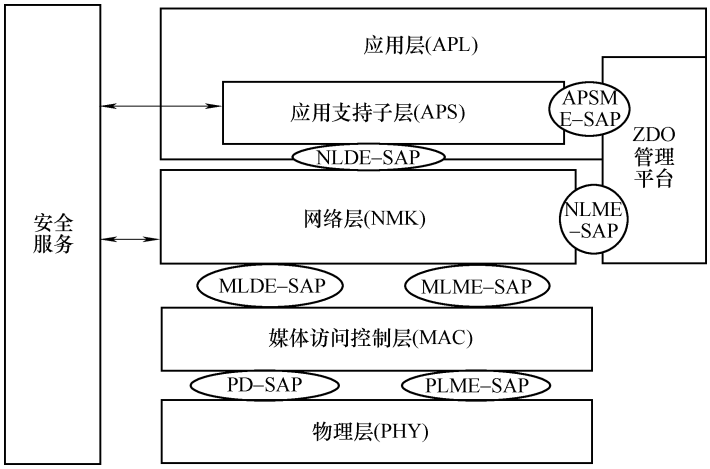


图 3-6　ZigBee 协议栈结构

其中物理层主要完成无线收发器的启动和关闭，检测信道能量和数据传输链路质量，选择信道，空闲信道评估（CCA），以及发送和接收数据包等；媒体访问控制层的功能包括信标管理、信道接入、时隙管理、发送与接收帧结构数据、提供合适的安全机制等；网络安全层主要用于 ZigBee 网络的组网连接、数据管理和网络安全等；应用层主要为 ZigBee 技术的实际应用提供一些应用框架模型。

ZigBee 协议栈中，每层都为其上一层提供两种服务：数据传输服务和其他服务。其中数据传输服务由数据实体提供，其他服务由管理实体提供。

图中 SAP 是指“服务访问点”，是每个服务实体和上层的接口。下层为上层提供某种服务功能要通过 SAP 交换一组服务原语来完成。

服务原语交换原理：

服务原语是一个抽象的概念，要实现特定服务需要由它来指定需要传递的信息。服务原语与具体的服务实现无关。

服务原语有请求、指示、响应、证实 4 种：

1）请求（request）原语。请求原语由网络服务请求方用户发送到它的服务提供层，请求启动一项服务。

2）指示（indication）原语。指示原语由网络用户的服务提供层发送到对应服务响应方用户的相应层，用于同远端服务请求逻辑相关。

3）响应（response）原语。响应原语由服务响应方用户发送到它的服务提供层，完成此前提示原语启动的过程。

4）证实（confirm）原语。证实原语由服务提供层发送到服务请求方用户，传递此前服务请求原语的结果。

在多用户存在的网络中，服务原语交换过程如图 3-7 所示。L_1-User、L_2-User 是两个对等的用户，P-Layer 是服务提供层，它们通过原语的传递，建立相关的服务。

服务是指 P-Layer 向 L_1-User 或 L_2-User 提供的功能，然而服务用户的功能是建立在其下一层提供的服务基础上的。层间信息流是一系列离散的事件，任何事件都是通过 SAP 发送服务原语来实现的。

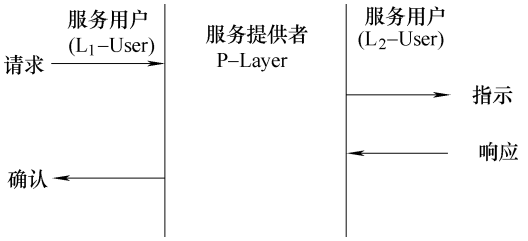


图 3-7　原语交换过程示意图

3.1.3.1　物理层

位于 ZigBee 协议栈结构最底层的是 IEEE 802.15.4 物理层，定义了物理无线信道和 MAC 层之间的接口。物理层包括物理层数据服务实体（Physical Layer Data Entity，PLDE）和物理层管理实体（Physical Layer Management Entity，PLME），分别提供物理层数据服务和管理服务。前者是指从无线物理信道上收发数据，后者是指维护一个由物理层相关数据组成的数据库。

1. *物理层参考模型*

物理层参考模型如图 3-8 所示。

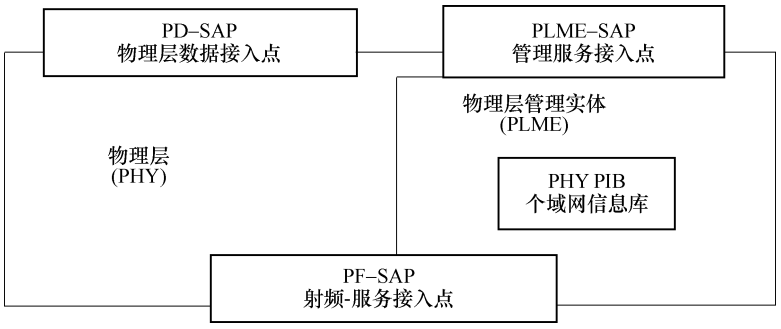


图 3-8　物理层参考模型

管理实体提供的管理服务有：信道能量检测（ED）、链路质量指示（LQI）、空闲信道评估（CCA）等。

信道能量检测主要测量目标信道中接收信号的功率强度，为上层提供信道选择的依据。信道能量检测不进行解码操作，检测结果为有效信号功率和噪声信号功率之和。

链路质量指示对检测信号进行解码，生成一个信噪比指标，为上层提供接收的无线信号的强度和质量信息。

空闲信道评估主要评估信道是否空闲。IEEE 802.15.4 中有 3 种空闲信道评估模式：

1）通过信道的信号能量来判断信道是否空闲：为要检测的信道设定一个门限值，当信

号能量低于该门限值时就认为信道空闲。

2）通过信道中传输的无线信号的特征来判断信道是否空闲，考察的信号特征包含扩频信号特征和载波频率。

3）第三种判断方法是前两种方法的综合，即同时检测信号强度和信号特征，进行判断。

2. 物理层无线信道的分配

根据 IEEE 802.15.4 标准的规定，物理层有 3 个载波频段：868 ~ 868.6MHz、902 ~ 928MHz 和 2400 ~ 2483.5MHz。3 个频段上数据传输速率分别为 20kbit/s、40kbit/s 和 250kbit/s。各个频段的信号调制方式和信号处理过程都有一定的差异。

根据 IEEE 802.15.4 标准，物理层 3 个载波频率段共有 27 个物理信道，编号从 0 ~ 26。不同的频段所对应的宽度不同，标准规定 868 ~ 868.6MHz 频段有 1 个信道（0 号信道）；902 ~ 928MHz 频段包含 10 个信道（1 ~ 10 号信道）；2400 ~ 2483.5MHz 频段包含 16 个信道（11 ~ 26 号信道）。每个具体的信道对应着一个中心频率，这些中心频率定义如下：

$$k = 0 \text{ 时，} F = 868.3\text{MHz}$$

$$k = 1, 2, \cdots, 10 \text{ 时，} F = 906 + 2(k - 1)\ \text{MHz}$$

$$k = 11, 12, \cdots, 26 \text{ 时，} F = 2405 + 5(k - 11)\ \text{MHz}$$

式中，k 为信道编号；F 为信道对应的中心频率。

不同地区的 ZigBee 工作频率不同。根据无线电管理委员会的规定各地标准见表 3-1。

表 3-1　不同地区的 ZigBee 标准

工作频率范围/MHz	国家和地区	调 制 方 式	传输速率/（kbit/s）
868 ~ 868.6	欧洲	BPSK	20
902 ~ 928	北美	BPSK	40
2400 ~ 2483.5	全球	O-QPSK	250

3. 物理层帧结构

不同设备间的数据和命令以包的形式互相传输。包的普通结构如图 3-9 所示。

图 3-9　ZigBee 的包结构

物理层包由以下三部分组成：

同步头（SHR）、物理层帧头（PHR）和物理层有效载荷，见表 3-2。

表 3-2　物理层协议数据单元

字节数：4	1	1		可 变 长 度
引导序列	帧起始分隔符	帧长（7 位）	预留（1 位）	物理层数据包
同步头		物理层帧头（PHR）		有效载荷

同步头使接收机能够同步并锁定数据流，物理层帧头（PHR）包含帧长信息，物理层载荷是由上层提供给接收者的数据或者命令信息。

引导序列：收发信机通过引导序列来获得码片和符号同步，由 32 位全 0 组成。

帧起始分隔符（Start Frame Delimiter，SFD）：表示引导序列的结束和数据帧的开始，是一个 8 位的二进制序列，格式为 11100101。

帧长：指定了物理层数据包中所包含的字节数，它的取值范围从 0 ~ 127。

物理层数据包：可变长度的字段，由网络高层提供。表示物理层所要传输的数据。

4. *物理层主要功能*

1）完成无线发射机的激活和开启。

2）对当前信道进行能量检测。

3）接收分组的链路质量指示。

4）基于 CSMA-CA 的空闲信道评估。

5）选择信道频率。

6）传输和接收数据。

5. *2.4GHz 频段的物理层技术*

由于我国应用的是 2.4GHz 频段，这里我们简要介绍 2.4GHz 频段的物理层技术。2.4GHz 频段主要采用了十六进制准正交调制技术（O-QPSK 调制）。调制原理如图 3-10 所示。PPDU 发送的信息进行二进制转换，再把二进制数据进行比特-符号映射，每字节按低 4 位和高 4 位分别映射成一个符号数据，先映射低 4 位，再映射高 4 位。再将输出符号进行符号-序列映射，即将每个符号被映射成一个 32 位伪随机码片序列（共有 16 个不同的 32 位码片伪随机序列）。在每个符号周期内，4 个信号位映射为一个 32 位的传输的准正交伪随机码片序列，所有符号的伪随机序列级联后得到的码片再用 O-QPSK 调制到载波上。

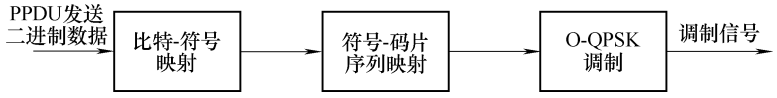


图 3-10　2.4GHz 物理层调制方案

2.4GHz 频段调制方式采用的是半正弦脉冲波形的 O-QPSK 调制，将奇位数的码片调制到正交载波 Q 上，偶位数的码片调制到同相载波 I 上，这样，奇位数和偶位数的码片在时间上错开了一个码片周期 T，如图 3-11 所示。

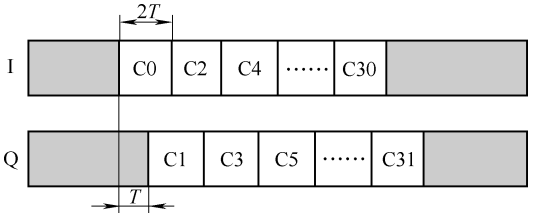


图 3-11　O-QPSK 偏移关系

3.1.3.2　媒体访问控制层

在 ZigBee 协议栈体系结构中，媒体访问控制（MAC）层位于物理层和网络层之间，也

是按照 IEEE 802.15.4 规范的定义设计的。包括 MAC 层管理实体（MLME）和 MAC 层公共部分子层（MCPS），它们向网络层提供相应服务。

1. MAC 层参考模型

MAC 层参考模型如图 3-12 所示，包括 MAC 层公共部分子层（MCPS）和 MAC 层管理实体（MLME）。

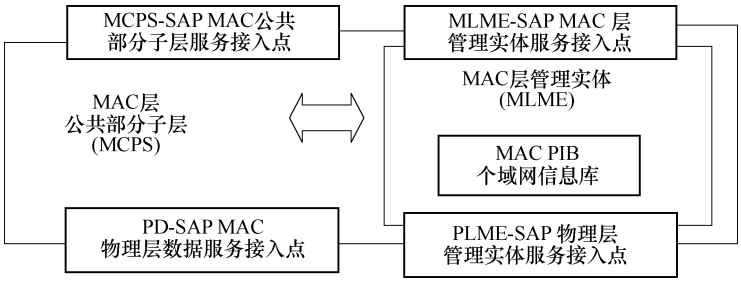


图 3-12　MAC 层参考模型

MAC 层公共部分子层服务访问点（MCPS-SAP）的主要功能是接收网络层传输来的数据，并在对等实体之间进行数据传输。MAC 层管理实体（MAC Layer Management Entity，MLME）主要负责 MAC 层的管理工作，并且维护该层管理对象数据库（PAN Information Base，PIB）。物理层管理实体服务接入点（PLME-SAP）主要负责接收来自物理层的管理信息，物理层数据服务接入点（PD-SAP）负责接收来自物理层的数据信息。

2. MAC 帧类型

IEEE 802.15.4 网络共定义了 4 种 MAC 帧结构：

1）信标帧（Beacon Frame）；

2）数据帧（Data Frame）；

3）确认帧（Acknowledge Frame）；

4）MAC 命令帧（MAC Command Frame）。

其中，信标帧用于协调者发送信标，信标是网内设备用来始终同步的信息；数据帧用于传输数据；确认帧用于确定接收者是否成功接收到数据；命令帧用来传输命令信息。

3. MAC 层帧结构

MAC 层帧，作为 PHY 载荷传输给其他设备，由 3 个部分组成：MAC 帧头（MHR）、MAC 载荷（MSDU）和 MAC 帧尾（MFR）。MHR 包括地址和安全信息。MAC 载荷长度可变，长度可以为 0，包含来自网络层的数据和命令信息。MAC 帧尾包括一个 16bit 的帧校验序列（FCS），见表 3-3。

表 3-3　MAC 帧的格式

字节数：2	1	0/2	0/2/8	0/2	0/2/8	可变长度	2
帧控制	帧序号	目的 PAN 标识码	目的地址	源 PAN 标识码	源地址	帧有效载荷	FCS
MHR						MSDU	MFR

（1）帧控制

由2字节（16位），共分9个子域。帧控制域各字段的具体含义见表3-4。

表3-4　帧控制

位：0～2	3	4	5	6	7～9	10～11	12～13	14～15
帧类型	安全使能	数据待传	确认请求	网内/网标	预留	目的地址模式	预留	源地址模式

1）帧类型：3bit。

帧类型编码	含　义
000	信标帧
001	数据帧
010	确认帧
011	MAC命令帧
其他	预留

2）安全使能：1bit。

安全使能位数据	含　义
0	MAC层没有对该帧加密处理
1	使用了MAC PIB中的密钥加密

3）数据待传：1bit。

数据待传位数据	含　义
0	发送数据帧的设备没有更多的数据要传送给接收设备
1	发送数据帧的设备还有后续数据发送给接收设备，接收设备需要再次发送数据请求命令来获得后续的数据

4）确认请求：指示帧的接收设备是否需要发出确认，1bit。

确认请求位数据	含　义
0	接收设备不需要反馈确认帧
1	接收设备在接收到数据帧或命令帧后，通过了CRC后，立即反馈一个确认帧

5）网内/网标：1bit。

网内/网标位数据	含　义
0	MAC帧中需要包含源PAN标识码和目的PAN标识码
1	目标地址与源地址在同一网络中，则MAC帧不含源PAN标识符

6）目的地址模式：2bit。

目的地址模式位数据	含　义
00	没有目的 PAN 标识码和目的地址
01	预留
10	目的地址是 16 位短地址
11	目的地址是 64 位扩展地址

7）源地址模式：2bit。

源地址模式位数据	含　义
00	没有源 PAN 标识码和源地址
01	预留
10	源地址是 16 位短地址
11	源地址是 64 位扩展地址

（2）帧序号

MAC 层为帧指定的唯一序列标识码，仅当确认帧的序列号与上一次数据传输帧的序列号一致时，才能判断数据业务成功。

（3）目的/源 PAN 标识码

占 16 位，分别指定了帧接收设备和帧发送设备的唯一的 PAN 标识符，如果目的 PAN 标识符域的值为 0xFFFF，则代表广播 PAN 标识符，是所有当前侦听信道的设备的有效标识符。

（4）目的/源地址

占 16 位或者 64 位，具体值由帧控制域中的目的/源地址模式子域值所决定。目的地址和源地址分别指定了帧接收设备和发送设备的地址，如果目的地址的值为 0xFFFF，表示广播短地址，它是所有当前侦听信道的设备的有效短地址。

（5）帧有效载荷

长度可变，它根据帧类型的不同而不同。

（6）FCS 字段

对 MAC 帧头和有效载荷计算得到的 16 位的 ITU-T CRC。

4. MAC 层主要功能

根据 IEEE 802.15.4 标准的规定，MAC 层主要功能有：

1）协调器可以产生网络信标。

2）与网络信标保持同步。

3）完成个域网的关联和解关联。

4）保证网络中设备的安全性。

5）对信道接入采用 CSMA-CA。

6）处理和维护保证时隙（GTS）机制。

7）能够在两个对等的 MAC 实体之间提供一个可靠通信链路。

3.1.3.3　网络层

在ZigBee协议架构中，网络层（NWK层）位于MAC层和应用层之间，提供两种服务：数据服务和管理服务，如图3-13所示。网络层数据实体（NLDE）负责数据传输，NLDE通过网络层数据服务实体服务接入点（NLDE-SAP）为应用层提供数据服务数据。管理实体（NLME）负责网络管理，通过网络层管理实体服务接入点（NLME-SAP）为应用层提供管理服务并维护网络层信息库（NIB）。

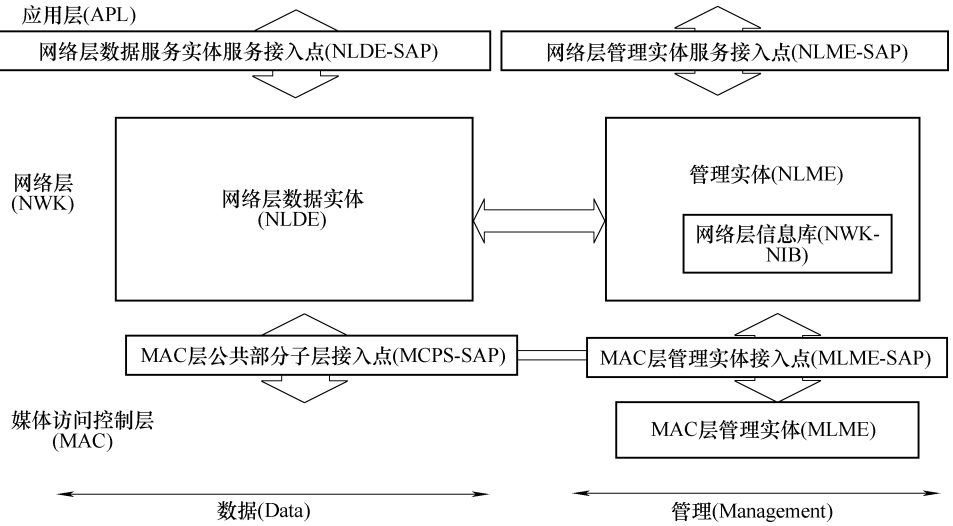


图3-13　ZigBee网络层与MAC层和应用层之间的接口

1. 网络层参考模型

网络层参考模型如图3-14所示，包括网络层数据实体和网络层管理实体。

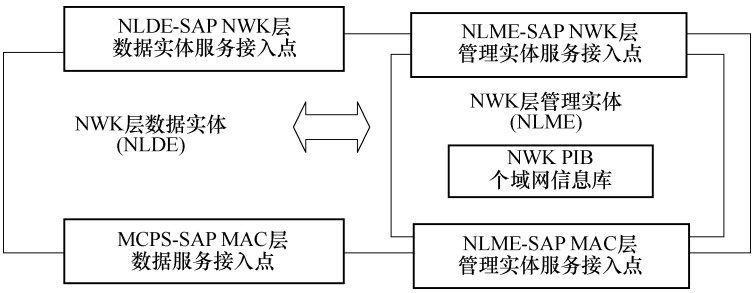


图3-14　网络层参考模型

在同一网络中的两个或多个设备之间，通过网络层数据实体提供的数据服务传输应用协议的数据单元（APDU），NLDE可以提供以下两种服务：

1）给应用支持子层PDU添加适当的协议头，形成网络协议数据单元（NPDU）。

2）根据拓扑路由，把网络协议数据单元发送到目的地址设备或通信链路的下一跳。

2. 网络层帧结构

普通网络帧结构如图3-15所示，网络层的帧结构也分为两部分：帧头和负载。帧头是

表征网络层特性的部分，负载是来自应用层的数据单元，所包含的信息因帧类型不同而不同，长度可变。

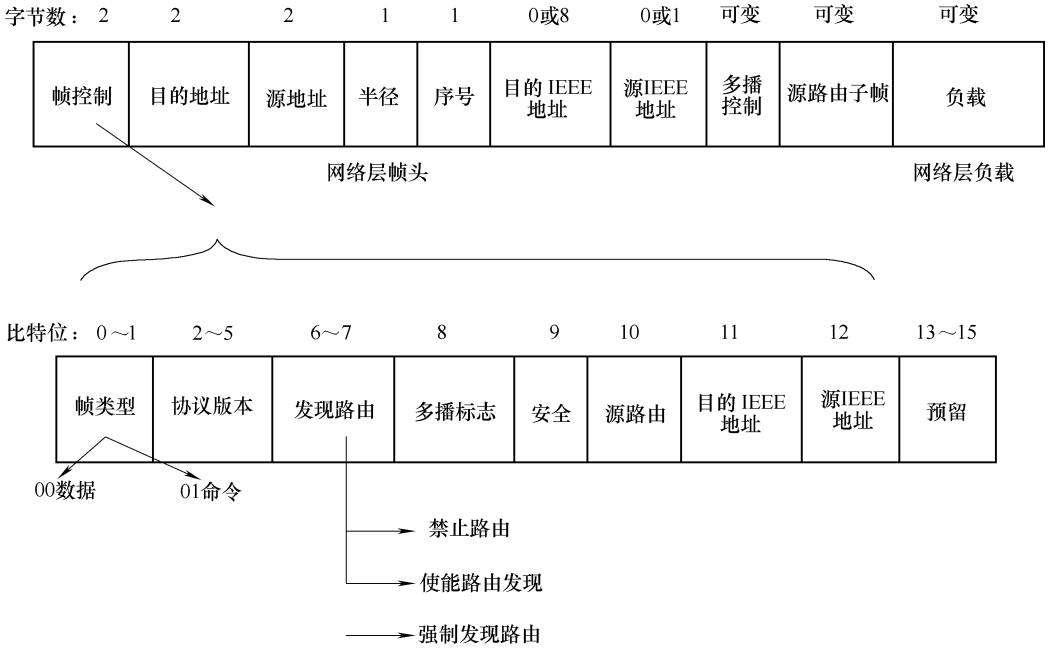


图 3-15　普通网络帧结构

（1）帧控制

帧头的第一部分是帧控制，帧控制决定了该帧是数据帧还是命令帧。帧控制共有 2B，16bit，分为帧类型、协议版本、发现路由、多播标志、安全、源路由、目的 IEEE 地址、源 IEEE 地址子项目。各子域的划分如图 3-15 所示。

1）帧类型：2bit。00 表示数据帧，01 表示命令帧，其他取值预留。

2）协议版本：4bit。表示当前设备使用的 ZigBee 网络层协议版本号。

3）发现路由：2bit。用来控制路发送帧时的路由发现操作。

发现路由编码	含　义
00	禁止路由
01	使能发现路由
10	强制发现路由
11	预留

4）安全：1bit。当值为 1，该帧执行网络层安全操作；如果值为 0，该帧在其他层执行安全操作或完全不使用安全操作。

（2）目的地址

占 2B，内容为目的设备的 16 位网络地址或者广播地址（0xffff）。

（3）源地址

占2B，内容为源设备的16位网络地址。

（4）半径

占1B，指定该帧的传输范围。如果是接收数据，接收设备应该把该字段的值减1。

（5）序号

占1B。如果设备是传输设备，每传输一个新的帧，该帧就把序号的值加1，源地址字段和序列号字段的一对值可以唯一确定一帧数据。

帧头中的字段按固定的顺序排列，但不是每一个网络层的帧都包含完整的地址和序号信息字段。

3. 网络层主要功能

1）对新设备进行配置。例如，一个新设备可以配制成ZigBee网络协调者，也可以被配制成一个终端加入一个已经存在的网络。

2）开发一个新网络。

3）加入或者退出网络。

4）网络层安全。

5）帧到目的地的路由选择（只有ZigBee协调者和路由器具有这项功能）。

6）发现和保持设备间的路由信息。

7）发现下一跳邻居节点，不用中继，设备可以直接到达的节点。

8）存储相关下一跳邻居节点信息。

9）为入网的设备分配地址（只有ZigBee协调器和路由器具有这项功能）。

3.1.3.4 应用层

应用层位于ZigBee协议栈最顶层，包括ZigBee设备对象（ZigBee Device Object，ZDO），应用支持子层和制造商定义的应用对象。ZDO负责设定设备在网络中是网络协调器还是终端设备、发现新接入网络的设备并决定设备所能提供的应用服务、初始化并响应绑定请求和在网络设备之间建立安全关系。APS维护绑定表并在绑定设备之间传递信息。

1. 应用层参考模型

应用层参考模型如图3-16所示，APS提供网络层和应用层之间的接口，同其他层相似，APS提供两种类型的服务：数据服务和管理服务。APS数据服务由APS数据实体提供，通过APSDE服务接入点接入网络。管理能力由APS管理实体提供，并通过APSME-SAP接入网络。

在ZigBee的应用层中，应用设备中的各种应用对象控制和管理协议层。一个设备中最多可以有240个应用对象。应用对象用APSDE-SAP来发送和接收数据。每一个应用对象都有一个唯一的终端地址（终端1～终端240）。终端地址0用于ZDO。为了广播一个消息给全部应用对象，终端地址设到255。终端地址允许多设备共用相同的无线资源。

ZigBee设备对象（ZDO）给APS和应用架构提供接口。ZDO包含ZigBee协议栈中所有应用操作的功能。例如，ZDO负责设定设备在ZigBee网络中是网络协调器还是路由器，或者终端设备。

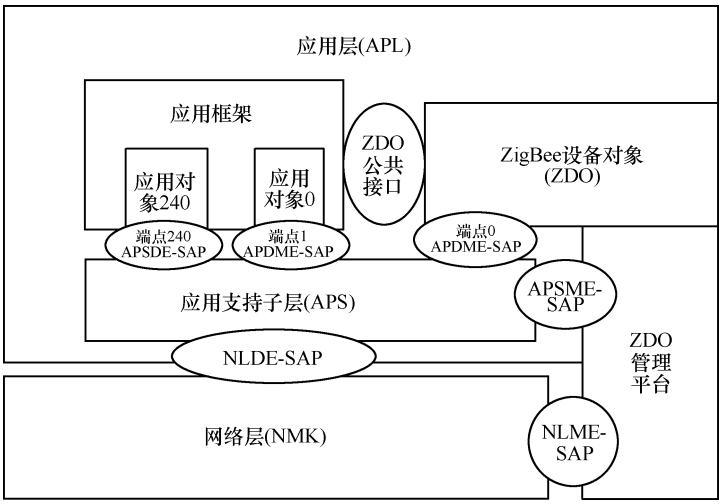


图 3-16　应用层参考模型

2. *应用层主要功能*

APS 提供网络层和应用层之间的接口。具有以下功能：

1）维护绑定表。

2）设备间转发消息。

3）管理小组地址。

4）把 64bit IEEE 地址映射为 16bit 网络地址。

5）支持可靠数据传输。

ZDO 的功能：

1）定义设备角色。

2）发现网络中设备及其应用，初始化或响应绑定请求。

3）完成安全相关任务。

3.1.4　ZigBee 在物联网中的应用前景

ZigBee 由于其低功耗的特性，有着广阔的应用前景，主要应用在数据传输速率不高的短距离设备之间，非常适合物联网中的传感器网络设备之间的信息传输，利用传感器和 ZigBee 网络，更方便收集数据，分析和处理也变得更简单。其应用领域主要包括：

1）家庭和楼宇网络：空调系统的温度控制、照明的自动控制、窗帘的自动控制、煤气计量控制、家用电器的远程控制等。

2）工业控制：各种监控器、传感器的自动化控制，例如在矿井生产中，安装具有ZigBee功能的传感器节点可以告诉控制中心矿工的准确位置。

3）商业：智慧型标签等。

4）环境控制：烟雾探测器等。

5）精细农业：与传统农业相比，采用传感器和 ZigBee 网络以后，传感器收集包括土壤的温度、湿度、酸碱度等信息。这些信息经由 ZigBee 网络传输到中央控制设备，通过对信息的分析从而有助于指导农业种植。

6）医疗卫生：借助于医学传感器和 ZigBee 网络，能够准确、实时地监测每个病人的血氧、血压、体温及心率等信息，从而减轻医生查房的工作负担。例如老人与行动不便者的紧急呼叫器和医疗传感器等。

ZigBee 技术在其他领域也有着广阔的应用前景。在运动休闲领域、酒店服务行业、食品零售业中都有 ZigBee 技术的应用。在不久的将来，会有越来越多的具有 ZigBee 功能的设备进入人们的视野，这将极大地改善人民的生活。

3.2 蓝牙

2009 年 12 月蓝牙技术联盟（Special Interest Group，SIG）正是推出了采用低耗能版本蓝牙核心规格 4.0 版的升级版蓝牙低耗能无线技术，将蓝牙技术应用延伸至医疗、保健、运动、健身、家庭娱乐等全新市场。4.0 版蓝牙拥有着低耗能、更大的传输范围、支持拓扑结构等特性，这与 ZigBee Alliance 制定的 ZigBee 标准十分类似。SIG 并没有将蓝牙技术仅局限在民用的消费级应用上，随着物联网发展的加速，蓝牙技术的未来仍将是工业化应用。

蓝牙 4.0 版本凭借其低功耗特性让业界很多人看到了新的市场机会。无线产业分析公司 WTRS 在 2010 年 7 月初发布的一份报告中称，蓝牙 4.0 版本的最显著特点在于蓝牙低功耗技术拥有巨大的市场潜力。市场调研机构 Gartner 资深无线技术分析师 Nick Jones 也表示，蓝牙 4.0 版本近日被 Gartner 评为“2010～2011 年十大移动技术”之一。随着移动互联网时代的到来，手机将成为最重要的移动互联网设备。目前超过 90% 的手机都具备了蓝牙功能，因此采用蓝牙技术作为物品接入互联网的方式具有广泛基础。在长时间通信中，低功耗特性非常关键，这是具有低功耗特性的蓝牙技术被广泛应用于物联网的内在动因之一。

3.2.1 蓝牙概念

3.2.1.1 蓝牙技术背景介绍

蓝牙，是一种支持设备短距离通信（一般 10m 内）的无线电技术，能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用蓝牙技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与互联网之间的通信，从而使数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段。其数据传输速率为 1Mbit/s。采用时分双工传输方案实现全双工传输。它的一般连接范围是 10m，通过扩展可以达到 100m；不限制在直线的范围内，甚至设备不在同一间房内也能互相连接。蓝牙设备有两种组网方式：微微网（Piconet）和散射网（Scatternet）。在 Piconet 中，多个蓝牙共享一条信道，其中一个为主单元，最多支持 7 个从单元。具有重叠覆盖区域的多个 Piconnet 构成 Scatternet，从单元时分复用的方式参加不同的 Picon，一个 Piconnet 中的主单元可以作为另一个 Piconet 的从单元。

蓝牙使用 FHSS（Frequency Hopping Spread Spectrum，跳频扩频）技术，理论跳频速率 1600 跳/s。跳频技术是把频带分成若干个跳频信道，在一次连接中，无线收发器按一

定的码序列（伪随机码）不断地从一个信道跳到另一个信道，只有收发双方是按照这个规律进行通信的，而其他的干扰不可能按照同样的规律进行干扰。跳频的瞬时带宽是很窄的，但扩展频谱技术使这个窄频带成百地扩展成宽频带，使干扰可能产生的影响变得很小。以2.45GHz为中心频率，最多可以得到79个1MHz带宽的信道。在日本、西班牙和法国，频段的带宽很小，只能容纳23个跳频点，其带宽仍为1MHz间隔。蓝牙的信道以时间长度625μs划分时隙，时隙依据微微网主要单元蓝牙时钟来编号。蓝牙系统中主、从单元的分组传输采用时分双工（Time Division Duplexing，TDD）交替传输方式，主要单元采用偶数编号的时隙开始信息传输，而从单元则采用奇数编号时隙开始信息传输，分组起始位置与时隙的起始点相吻合，由主或从单元传输的分组可以扩展到5个时隙。蓝牙采用的调制方式为GFSK，使用3种功率：0dBm（1mW）、4dBm（2.5mW）、20dBm（100mW）。

在主单元和从单元之间，可以建立不同类型的链路，如同步面向连接的链路（Synchronous Connection Oriented，SCO）、异步无连接链路（Asynchronous Connectionless Link，ACL）。SCO链路是在主单元和指定的从单元之间实现对称的、点对点连接，SCO连接方式采用预留时隙，因此该方式可看作是在主单元和从单元之间实现的电路交换链路，它主要用于支持类似于像话音这类的时限信息。ACL连接定向发送数据包，它既支持对称连接又支持不对称连接。在非SCO连接的保留时隙里，主单元可以以时隙为单位与任何从单元的分组交换连接。蓝牙支持一条异步数据通信信道、三条同步语音信道或一条同时支持异步数据和同步语音的信道。语音信道速率为64kbit/s，语音编码采用对数PCM或连续可变斜率增量（Continuous Variable Slope Delta，CVSD）调制。异步数据通信信道速率：不对称时，一个方向最大723.2kbit/s，反向时57.6kbit/s；对称时为433.9kbit/s。

3.2.1.2　蓝牙技术的应用前景

数据通信原本是计算机与通信相结合的产物。近年来移动通信迅速发展，便携式计算机如膝上型电脑、笔记本电脑、手持式电脑以及个人数字助理（PDA）等迅速普及，还有因特网的快速增长，使人们对电话通信以外的各种数据信息传递的需求日益增长。近来广泛使用的全球通（GSM）数字移动电话已经增加了数据通信的需求，不仅能够区分话音呼叫和数据呼叫，还能区分不同种类的数据呼叫。第三代移动通信更是把数据通信作为重要业务来考虑。无线数据通信是未来通信的主要方式。

蓝牙技术把各种便携式与蜂窝移动电话用无线电链路连接起来，使计算机与通信密切结合，使人们能够随时随地进行数据信息交换与传输。蓝牙不仅可以应用于家庭网络，小范围办公，而且对个人数据通信也是非常重要的。

因此计算机行业、移动通信行业都对蓝牙技术很重视，认为对未来的无线移动数据业务有巨大的促进作用，预计在最近几年内无线数据通信业务将迅速增长，蓝牙技术被认为是无线数据通信最为重大的进展之一。

蓝牙创始的5家公司中，包含了两家著名的移动通信制造公司、两家著名的便携式计算机制造公司和一家在芯片技术和数字信号处理技术（DSP）上领先的公司。他们这项计划公布后，迅速得到包括摩托罗拉、朗讯、康柏、西门子、高通、3Com、TDK等大公司在内的许多厂商的支持和采纳。自从1998年5月成立以来，共计超过1300家企业加入Bluetooth SIG。每位联盟成员都会获得一项来自其他成员的免费专利授权，以便在其产品中使用蓝牙

技术。联盟成员可取得蓝牙技术规格并参与研讨，有利于各厂商的产品开发以及相互之间更好地兼容。

蓝牙技术的应用范围很广。爱立信推出的蓝牙耳机，是人们看到的第一个蓝牙产品。支持手机、笔记本电脑只是蓝牙应用的第一个阶段。可以预见，在未来几年，手机生产商将陆续推出带蓝牙功能的移动电话。而后蓝牙的应用将由手持终端扩展到如汽车、航空、消费类电子、信息家电等领域。

目前，一些厂商已经开发了数款面向企业和普通消费者的蓝牙技术产品，其中有一款叫作 NetDrive 的便携式硬盘，它利用蓝牙技术无线接收数据并加以存储（总容量可以达到200MB）。计算机用户可以在主机与硬盘间进行无线操作，当他离开时，可将硬盘带走，防止他人非法操作，回来后只需重新装上硬盘便可继续工作。

支持蓝牙技术的车载电话也已经开发出来。汽车制造商积极响应蓝牙技术，计划在车上安装车载免提电话系统，与蓝牙相匹配的移动电话一同工作。蓝牙可保持移动电话和个人计算机的无绳连接。即使用户的个人计算机放在手提箱里，用户也可以通过电话接收电子邮件，通过移动电话屏幕阅读邮件标题。构造家庭网络是蓝牙技术最重要的应用之一。家庭内部所有信息设备之间连成网络，构成家庭网络是未来信息社会发展的必然趋势。到 2004 年，因特网有 10 亿网民，全球有 10 亿移动电话用户，因此通过蓝牙技术使得手机上网的人数将非常多，移动手机终端的市场将非常广阔。

3.2.2　架构及研究现状

蓝牙技术的协议结构如图 3-17 所示。整个协议体系结构分为底层硬件模块、中间协议层和高层应用框架三大部分。

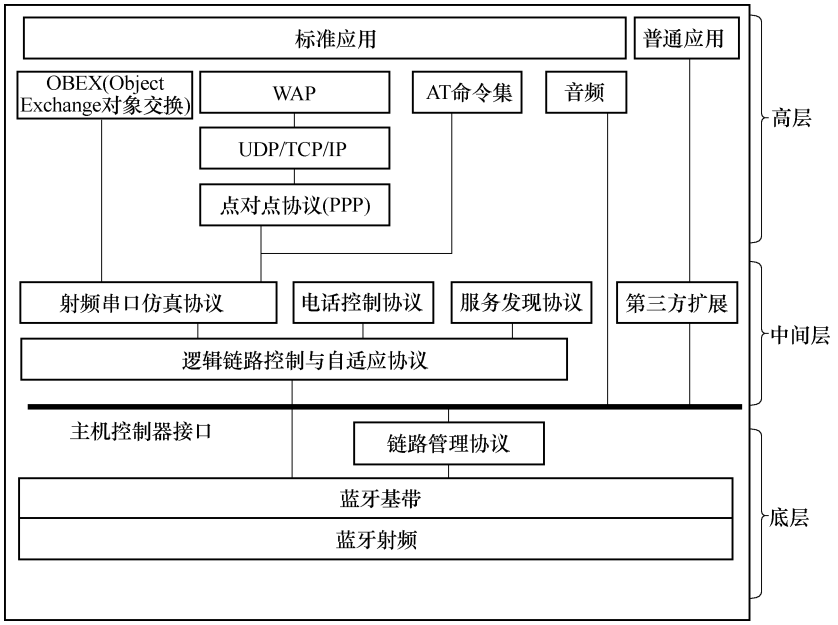


图 3-17　蓝牙技术协议结构

3.2.2.1　底层硬件模块

底层硬件模块包括无线射频（RF）、基带（Baseband，BB）和链路管理（Link Manager，LM）3层。RF层通过2.4GHz无需授权的ISM频段的微波，实现数据位流的过滤和传输，本层协议主要定义了蓝牙收发器在此频段正常工作所需满足的条件。BB层负责完成跳频和蓝牙数据及信息帧的传输。LM层负责建立和拆除链路连接，同时保证链路的安全。

3.2.2.2　中间协议层

中间协议层包括逻辑链路控制与自适应协议（L2CAP）、服务发现协议（SDP）、射频串口仿真协议（Radio Frequency Communication，RFCOMM）和电话控制协议（TCS）4项。L2CAP主要完成数据拆装、协议复用等功能，是其他上层协议实现的基础。SDP为上层应用程序提供了一种机制来发现网络中可用的服务及其特性。RF-COMM基于ETSI标准TS07.10，在L2CAP上仿真9针RS232串口的功能。TCS提供蓝牙设备间语音和数据呼叫控制信令。

在BB和LM上与L2CAP之间还有一个主机控制接口层（Host Controller Interface，HCI）。HCI是蓝牙协议中软硬件之间的接口，它提供了一个调用下层BB、LM、状态和控制寄存器等硬件的统一命令接口。

3.2.2.3　高层应用框架

高层应用框架位于蓝牙协议栈的最上部。其中较典型的应用模式有拨号网络（dialup networking）、耳机（headset）、局域网访问（LAN access）、文件传输（file transfer）等。各种应用程序可以通过各自对应的框架实现无线通信。拨号网络应用模式可以通过RFCOMM仿真的串口访问微微网。通过蓝牙技术连接在一起的所有设备被认为是一个微微网。一个微微网可以只是2台相连的设备，比如1台便携式计算机和1部移动电话，也可以是8台连在一起的设备。在一个微微网中，所有设备都是级别相同的单元，具有相同的权限。在微微网网络初建时，其中一个单元被定义为主单元，其时钟和跳频顺序被用来同步其他单元的设备，其他单元被定义为从单元，数据设备也可由此接入传统的局域网。用户通过协议栈中的音频层在手机和耳塞中实现音频流的无线传输。多台PC或笔记本电脑之间不用任何连线，即可快速灵活地传输文件和共享信息，多台设备也可由此实现操作的同步。随着手机功能的不断增强，手机无线遥控也将成为蓝牙技术的主要应用方向之一。

3.2.3　蓝牙功能模块

Bluetooth功能一般是通过模块来实现，但实现的方式不同。有些设备把Bluetooth模块内嵌到设备平台中，有些则是采用外加式。蓝牙系统由无线单元、链路控制单元、链路管理和软件功能单元组成。

3.2.3.1　无线单元

蓝牙空中接口是建立在天线电平为0dBm基础上的。空中接口按FCC有关电平为0dBm的ISM频段的标准。如果全球电平达到100mW，可以使用扩展频谱功能来增加一些补充业务。频谱扩展功能是通过起始频率为2.402GHz、终止频率为2.480GHz、间隔为1MHz的79个跳频频点来实现的。出于某些本地规定的考虑，日本、法国和西班牙都缩减了带宽。蓝牙最大的跳频速率为1660跳/s。理想的连接范围为10cm～10m，但是通过增大发送功率可以将距离延长至100m。

3.2.3.2　链路控制单元

链路控制单元由基带部分来实现，它描述了基带链路控制器的数字信号处理规范。基带链路控制器负责处理基带协议和其他一些低层常规协议。蓝牙基带协议是电路交换与分组交换的结合。在被保留的时隙中可以传输同步数据包，每个数据包以不同的频率发送。一个数据包名义上占用一个时隙，但实际上可以被扩展到占用5个时隙。蓝牙可以进行异步数据通信，还可以支持3个同步语音信道同时进行工作，还可用一个信道同时传送异步数据和同步语音。每个语音信道支持64kbit/s同步语音链路。异步信道可以支持一端最大速率为721kbit/s，而另一端速率为57.6kbit/s的不对称连接，也可以支持43.2kbit/s的对称连接。蓝牙基带部分在物理层为用户提供保护和信息保密机制。鉴权基于“请求—响应”运算法则。鉴权是蓝牙系统中的关键部分，它允许用户为个人的蓝牙设备建立一个信任域，比如只允许主人自己的笔记本电脑通过主人自己的移动电话进行通信。连接中的个人信息由加密来保护，密钥由程序的高层来管理。网络传送协议和应用程序可以为用户提供一个较强的安全机制。

3.2.3.3　链路管理和软件功能单元

链路管理（LM）和软件功能单元包括链路的数据设置、鉴权、链路硬件配置和其他一些协议。LM能够发现其他远端LM并通过LMP（链路管理协议）与之通信。蓝牙设备支持一些基本互操作的要求。对某些设备，这种要求涉及无线模块、空中协议以及应用层协议和对象交换格式。但对另外一些设备，比如耳机，这种要求就简单得多。蓝牙设备必须能彼此识别并装载与之相应的软件以支持设备更高层次的性能。蓝牙对不同级别的设备（如PC、手持机、移动电话、耳机等）有不同的要求，例如：蓝牙耳机不能提供地址簿；但配备蓝牙装置的移动电话、手持机、笔记本电脑则具有故障诊断、与外设通信、商用卡交易等功能。

3.2.4　关键技术点

包括无线通信与网络技术、软件工程、软件可靠性理论、协议的正确性验证技术、软硬件接口技术（如RS232，USB等）以及高集成、低功耗芯片技术。

1）跳频技术。跳频是蓝牙使用的关键技术之一，数据包短，抗信号衰减能力强，并具有足够强的抗干扰能力。

2）射频技术。蓝牙的载频选用全球通用免费的2.4GHz ISM（Industrial Scientific medicine）频段，无须申请许可证。

3）基带协议。当两个蓝牙设备成功建立链路后，Piconet便形成了，两者之间的通信通过无线电波在79个信道中随机跳转而完成。蓝牙给每个Piconet提供特定的跳转模式，因此它允许大量的Piconet同时存在。

4）网络特性。蓝牙支持点对点和点对多点的连接，可采用无线方式将若干蓝牙设备连成一个Piconet，多个Piconet又可互联成特殊分散网，形成灵活的多重Piconet的拓扑结构，从而实现各类设备之间的快速通信。蓝牙可以即连即用，组网灵活，具有很强的移植性，并且适用于多种场合。蓝牙的优势在于它的对等连接能力以及多重设定能力。

5）协议分层。蓝牙的通信协议也采用分层结构。层次结构使其设备具有最大可能的通用性和灵活性。

6）安全性。采用快速跳频和前向纠错方案以保证链路稳定，减少同频干扰和远距离传

输时的随机噪声影响。蓝牙系统的移动性和开放性使得安全问题极其重要，蓝牙系统所采用的跳频技术已经提供了一定的安全保障，并且在链路层中，蓝牙系统提供了认证、加密和密钥管理等功能，每个用户都有一个个人标识码（Personal Identification Number，PIN），它会被译成128bit的链路密钥（Link Key）来进行双向认证。

7）可同时支持数据、音频、视频信号传输。

8）全球性地址。任一蓝牙设备，都可根据IEEE802标准得到唯一48bit的BD—ADDR。它是一个公开的地址码，可以通过人工或自动进行查询。

9）采用时分复用多路访问技术。基带传输速率为1Mbit/s，采用数据包的形式按时隙（Time Slot）传送数据，每时隙0.625ms（不排除将来可能采用更高的传输速率）。每个蓝牙设备在自己的时隙中发送数据，这在一定程度上可有效避免无线通信中的“碰撞”和“隐藏终端”等问题。

3.3　低功耗蓝牙（iBeacon）及蓝牙4.0协议

低功耗蓝牙（Bluetooth Low Energy，BLE）作为一种无线连接技术在过去3年爆炸性发展。目前为数百万个电子装置提供低功率连线功能，例如智能手表、健身追踪器、智能手机配件和医疗监测器。通过即将推出的技术改进，BLE将更加广泛地运用在新一代消费性电子产品与新兴物联网中。

由于蓝牙4.0协议拥有极低的运行和待机功耗，使用一粒纽扣电池甚至可连续工作数年之久；同时还具有低成本、跨厂商互操作性、3ms低延迟、AES－128加密等诸多特色，大大扩展了蓝牙技术的应用范围。所以，目前很多蓝牙厂商也都推出了符合蓝牙4.0版本的低功耗协议的蓝牙芯片。本节将介绍低功耗蓝牙的概念、工作原理，以及蓝牙4.0低功耗部分协议的技术原理、协议架构；同时将介绍基于低功耗蓝牙技术的iBeacon新功能，使得读者对低功耗蓝牙和iBeacon都可以有更深入的了解。

3.3.1　什么是低功耗蓝牙和iBeacon

Beacon是一种低成本的硬件设备，小到可以贴在墙上或者工作台上，可通过低功耗蓝牙传输信息或者将信息直接推送给智能手机或平板电脑。它们将改变零售商、大型活动组织者、交通系统、企业和教育机构与身处室内的人的沟通方式。用户还可以把Beacon部署在家庭自动化系统中。

低功耗蓝牙（BLE）是发布在2010年的蓝牙4.0规范的一部分，它由Nokia发起于2006年，虽然合并到蓝牙技术，但它是与经典蓝牙不同的一组协议，并且设备不向后兼容。因此现在有3种蓝牙设备：①蓝牙：仅支持经典模式；②智能蓝牙过渡（Bluetooth Smart Ready）：支持经典模式和低功耗（Low Energy，LE）模式；③智能蓝牙：仅支持LE模式。

低功耗蓝牙的主要关注点理所当然在低功耗上。例如一些Beacon在一块纽扣电池下（电池通常不更换，除非当Beacon停止工作时，才需要更换）可以持续两年传输信号。低功耗蓝牙同经典蓝牙都使用相同的频谱范围（2.4～2.4835GHz）。每个信道的频宽为1MHz。蓝牙4.0使用2MHz间距，可容纳40个信道。第一个信道始于2402MHz，每1MHz一个信道，至2480MHz。具备适配跳频（Adaptive Frequency－Hopping，AFH）功能，通常每秒跳

1600次。低功耗蓝牙有更低的传输速率，尽管它的本意不是传输大量数据，而是进行发现和简单通信。在理论范围，低功耗蓝牙和经典蓝牙信号都可以最远达到100m。

iBeacon是苹果公司2013年9月发布的移动设备用OS（iOS7）上配备的新功能。其工作方式是，配备有低功耗蓝牙（BLE）通信功能的设备使用BLE技术向周围发送自己特有的ID，接收到该ID的应用软件会根据该ID采取一些行动。比如，在店铺里设置iBeacon通信模块的话，便可让iPhone和iPad上运行一资讯告知服务器，或者由服务器向顾客发送折扣券及进店积分。此外，还可以在家电发生故障或停止工作时可以使用iBeacon向应用软件发送信息。

3.3.2　低功耗蓝牙如何工作

低功耗蓝牙有两种工作状态：广播状态和连接状态。

广播状态：广播是单向的被发现机制，想要被发现的设备可以每20ms～10s传输一个数据包。时间间隔越短，电池寿命也越短，但设备发现速度越快。发送的数据包通常可以加长至47B，由以下构成：

报头	访问地址	广播信道协议数据单元	CRC
1B	4B	2～39B	3B

广播信道协议数据单元（Protocol Data Unit，PDU）：PDU有它自己的头部（2B，负载的大小和它的类型以及设备是否支持连接等）和实际的数据负载（最长至37B）。负载的头部后6B是设备的MAC地址，实际的数据最长有31B，结构如图3-18所示。

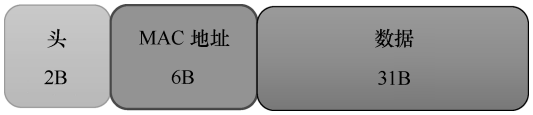


图3-18　PDU结构

低功耗蓝牙可以处于一个非连接广播模式（所有的信息都被包含在广播中），但有时也可以允许连接（通常为允许）。

连接状态：设备被发现之后，可以建立一个连接。对于每一个服务特性，它都可以去读取低功耗蓝牙提供的数据，即每一个特性提供一些可以被读取或被写的值。例如一个智能调温器可以使用一个服务特性读取当前温度、湿度（作为特性服务），而使用另一个服务特性去设置期望的温度。

低功耗蓝牙与iBeacon：iBeacon的核心技术即为低功耗蓝牙（BLE），具体而言，利用了BLE中名为“通告帧”（Advertising）的广播帧。通告帧是定期发送的帧，只要是支持BLE的设备就可以接收到。

iBeacon的数据主要由4部分构成，分别是UUID（Universally Unique Identifier，通用唯一识别符）、Major、Minor、Measured Power。

- UUID规定为ISO/IEC11578：1996标准的128位标识符。
- Major和Minor由iBeacon发布者自行设定，都是16位的标识符。比如，连锁店可以在Major中写入区域资讯，可在Minor中写入个别店铺的ID等。另外，在家电中嵌入iBeacon功能时，可以用Major表示产品型号，用Minor表示错误代码，用来向外部通知故障。
- Measured Power是iBeacon模块与接收器之间相距1m时的参考接收信号强度标识（Received Signal Strength Indicator，RSSI）。接收器根据该RSSI与接收信号的强度来推算发送模块与接收器的距离。

iBeacon 利用以上数据格式就可以进行有效信息的传递。

3.3.3　低功耗蓝牙协议

LE 协议的底层与基础蓝牙协议底层基本相似，但在主机端，针对传感器网络应用推出了属性协议（ATT）以及通用属性配置（GATT），具体协议分层结构如图 3-19 所示。

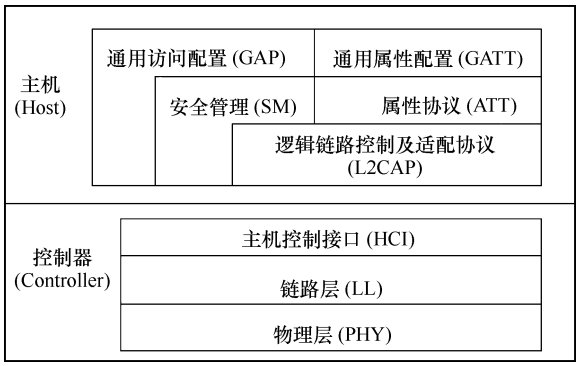


图 3-19　协议分层结构图

其中，基于逻辑链路控制与适配协议（即 L2CAP 以上）的部分可在主机端实现，这一部分可称为主机端部分，HCI 层以下部分可称为芯片控制器层也可简称底层协议。下面对每层协议做一下介绍。

（1）物理层

物理层采用调频技术减少干扰与信号衰减，从 2.402 ~ 2.480 GHz 均匀分为 40 个信道，每个信道宽 2MHz；使用 GFSK 调制解调方式；输出功率为 0.01 ~ 10mW；传输速率为 1Mbit/s。提供 3 个固定的广播信道，广播数据用于建立连接以及发现设备，这样使得建立连接的时间可以压缩到 3ms 左右，大大提高了设备建立连接的效率。另外它提供了 37 个数据信道采用自适应调频技术发送数据。

（2）链路层

链路层功能是执行一些基带协议底层数据包管理协议。链路层设备主要有待机、发起、扫描、连接、广播等 5 种工作状态，状态转换图如图 3-20 所示。

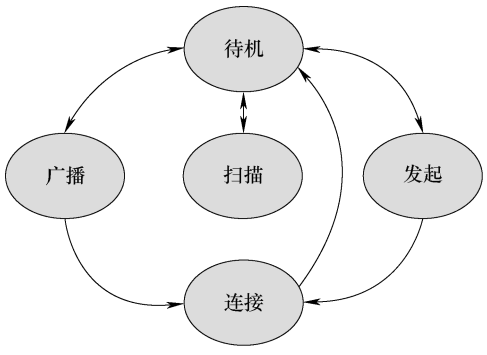


图 3-20　状态转换图

待机状态不发送和不接收任何包，任何状态都可以进入待机状态。

广播状态在广播信道发送广播包并且监听可能的响应包，广播状态可以由待机状态进入。

扫描状态将会监听广播信道包，扫描状态可以从待机状态进入。

发起状态将会监听从特定设备发出的广播包并且发起连接请求作为响应，发起状态可从待机状态进入。

连接状态可以从发起状态或者广播状态进入，在连接状态下有主从两种角色。

当从发起状态进入连接状态时，发起连接请求，将会是主设备，当从广播状态进入连接状态时，将会是从设备。

链路层主要有两种重要的事件操作：扫描与建立连接。

设备扫描有被动扫描和主动扫描两种。被动扫描是通过被动接收广播包得到设备信息。被动扫描过程如图 3-21 所示。

主动扫描是通过发送扫描请求得到扫描回应后获取设备信息。主动扫描过程如图 3-22 所示。

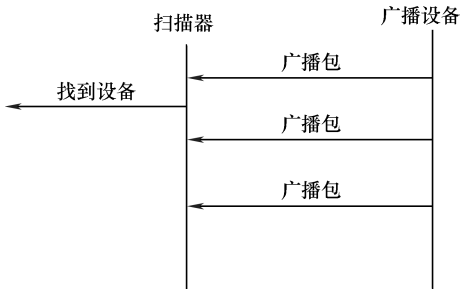


图 3-21　被动扫描

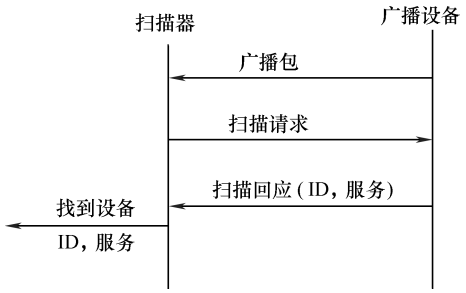


图 3-22　主动扫描

而建立连接的过程是通过发送连接请求包来建立设备连接。建立连接过程如图 3-23 所示。

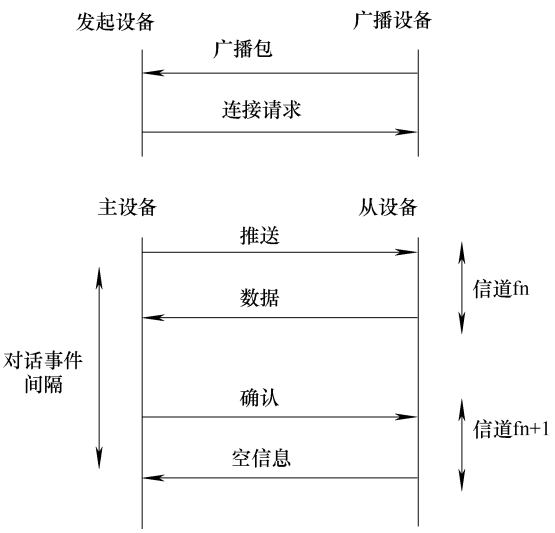


图 3-23　建立连接流程图

（3）主机控制接口层

主机控制接口与标准蓝牙技术相同，提供了主机与控制器层的通信方式与命令事件格式，重用标准蓝牙传输层接口如 UART（Universal Asynchronous Receiver/Transmitter，通用异步收发传输器）接口、USB 接口等。

（4）逻辑链路控制与适配协议层

与标准蓝牙技术相同，为上层提供了数据封装业务，提供端到端的逻辑数据通信。

（5）安全管理层

定义了配对和密钥分发方法，提供其他层协议接口来安全地建立连接以及交换数据。安全管理层不涉及具体的 BLE 安全算法，只是提供一些接口，节省功耗以及降低复杂性，具体安全算法可以通过在底层硬件实现。

（6）通用接入层

定义了通用的接口，供应用层调用底层模块（比如设备发现），建立连接相关的业务，同时封装了安全设置相关的 API。

（7）属性协议层

属性协议允许设备以“属性”的形式向另外的设备暴露它的某些数据。在 ATT 协议里，暴露属性的称为 Server 端，另外一端称为 Client。

（8）通用属性配置

GATT 层是一种具体使用属性协议的应用框架。GATT 定义了属性协议应用的架构。在 BLE 协议中，应用的数据片段被称为“特征”，而 BLE 中两个设备之间的数据通信就是通过 GATT 子过程来处理的。

3.3.4　iBeacon 功能

一套 iBeacon 的部署由一个或多个在一定范围内发射传输它们唯一的识别码 iBeacon 的信标设备组成。接收设备上的软件可以查找 iBeacon 并实现多种功能，比如通知用户；接收设备也可以通过连接 iBeacons 从 iBeacon 的通用属性配置服务来得到自己想要的信息。

1）定位：在区域内（主要是室内）设置 iBeacon 基站，通过手持蓝牙终端接收到 iBeacon 基站发送的与位置相关的 UUID 号和 RSSI 值，通过加权的三环定位算法即可定位人员在室内的坐标位置。

此定位方法具有功耗小、时延低、传输距离远的特点，最大限度地满足了高精度室内定位技术的要求。一般所有的基站都均匀地分布在所需定位的室内空间中。

2）测距：iBeacon 的传输距离分为 3 个不同的范围，最近 immediate（cm 级）、中距 near（1m 以内）和远距 far（大于 1m）。

当用户进入、退出或者在区域内徘徊时，iBeacon 的广播有能力进行传播，根据用户和 iBeacon 基站的距离，基站可以得到用户的距离信息，并且这 3 个距离范围可以相互交互。

3.3.5　低功耗蓝牙（iBeacon）的优势与劣势

表 3-5 为典型蓝牙与低功耗蓝牙的对比。

表 3-5　典型蓝牙与低功耗蓝牙对比

技 术 规 范	典型蓝牙 BT	低功耗蓝牙 BLE
无线电频率	2.4GHz	2.4GHz
距离	10/100m	30m
空中传输数据速率	1～3Mbit/s	1Mbit/s
应用吞吐量	0.7～2.1Mbit/s	0.2Mbit/s
安全	64/128bit 及用户自定义的应用层	128bitAES 及用户自定义的应用层
健壮性	自动适应快速调频，FEC，快速 ACK	自动适应快速调频
响应延迟	约 100ms	6ms
发送数据的总时间	100ms	<6ms
政府监管	全球	全球
认证机构	蓝牙技术联盟（Bluetooth SIG）	蓝牙技术联盟（Bluetooth SIG）
语言能力	有	无
网络拓扑	分散网	Star－bus
耗电量	1（作为参考）	0.01～0.5（视使用情况而定）
最大操作电流	<30mA	<15mA
主要用途	手机、游戏机、耳机、stereo audio streaming、汽车和 PC 等	手机、游戏机、PC、表、体育健身、医疗保健、智能穿戴设备、汽车和家用电子等

相比传统蓝牙，最新的低功耗蓝牙广播距离增加了，可达30m；耗能大幅减少，广播端仅靠一枚纽扣电池就可以坚持数年不间断工作；频段切换频繁，蓝牙广播在繁忙的2.4G ISM频段，快速跳频就会更少被干扰。

iBeacon要想实现超越Wi-Fi的室内定位精度的效果，广播端需要大量作为蓝牙基站的iBeacon硬件盒子，因为蓝牙使用的2.4G ISM频段本身易受干扰，测距不太精确，iBeacon直接测距不准，需要房间里有多个iBeacon广播点并且拓扑合理。信号不稳定，需要通过时间平滑，或者多个iBeacon互相验证纠正。要做到定位精度高、反应快需要相当的积累。根据联合测试结果，在拓扑合理、算法适当的情况下，每20m^{2}部署1个iBeacon的情况下，定位精度才可以保持在cm级别。

除了iBeacon广播端部署成本的问题，iBeacon要想实现定位，信号接收端也有要求，由于iBeacon是基于最新的Bluetooth 4.0 LE标准。相比之下，几乎所有的智能手机都可以接收到Wi-Fi信号，而且Wi-Fi热点目前已具有相当规模，可以直接拿来用，唯一需要的是更新Wi-Fi热点MAC物理地址和真实地理地址的映射数据库。

iBeacon本身不会自动推送定制信息，信息推送是手机应用里的定制功能，只有客户安装了某个应用，客户才能在某个iBeacon网络收到定制信息。

iBeacon要实现室内定位，面临架设成本高，基础设施不完善；实现LBS消息推送，条件苛刻，不现实；无线支付目前又有安全上的问题等缺点，所以iBeacon想要得到推广和应用，需要技术标准协议，以及软硬件上的全方位改造。

3.3.6　低功耗蓝牙的未来走向

从目前的情况来看，BLE技术已经为需要低功率无线连线的装置提供了优异的方案。然而，BLE的能源效率甚至将变得更高，且蓝牙4.1的改进项目将可让此技术更加容易用于设计新一代的无线装置和智慧型物件，进而组成物联网。

即使蓝牙4.1拥有这些改进项目，但仍可向下相容于传统的装置，包括：

1）支援多重角色。链路层与双模式拓扑的改变能让双模式装置同时当作Smart Ready分享器以及Smart装置。

2）高效率资料交换。在逻辑链路控制与适配协（L2CAP）中新增连线导向通道，能让BLE装置之间的大量资料传输更加有效率，同时减少了负担。

3）改善连线。工程师在建立和维护蓝牙连线时将享有更多的灵活性，包括自动重新连线。

4）IP架构连线。新的核心规格新增专用的L2CAP通道，打造了IPv6通信的技术基础，借此为物联网铺路。

3.4　UWB

UWB（Ultra-Wide Band，超宽带）技术具有系统复杂度低、发射功率谱密度低、对信道衰落不敏感、低截获能力、定位精度高等优点。尤其适用于室内等密集多径场所的高速无线接入，非常适用于建立一个高效的无线局域网。基于此，UWB技术不仅可以缓解传统的无线技术在工业环境的通信质量下降问题，而且增加了带宽，解决了传统无线技术传输速率

低，不能适应工业网络化控制系统向多媒体信息传输及监测、控制、故障诊断等多功能一体化方向发展的要求。因此建立基于 UWB 的网络化控制系统的体系结构，使控制网络系统实现定位、信息识别、控制、监测及诊断等一体化，形成真正意义的物联网具有重大的实际应用价值和意义。

3.4.1　UWB 的概念

3.4.1.1　UWB 技术介绍

UWB 技术凭借其超宽的信号带宽、较低的发射功耗以及高数据传输速率等特点，被认为是最有发展前景的无线电技术之一。近年来随着“泛在无线通信”概念的提出，无线局域网、无线个域网和无线体域网等短距离无线应用逐渐渗透到人们的生活当中。UWB 技术正是定位于短距离无线通信这一广阔的应用领域，特别是最近物联网应用的兴起，UWB 技术可以作为物联网的基础通信技术之一，实现不同设备之间的互联互通。同时 UWB 技术还可以应用于精确定位、雷达跟踪等领域，成为目前学术研究和业界关注的重点技术。

UWB 无线通信的历史可以追溯到 20 世纪 50 年代，早期的超宽带系统利用占用频带极宽的超短基带脉冲进行通信，主要应用于军用的雷达以及低截获率/低侦测率的通信系统。2002 年 4 月，美国联邦通信委员会（FCC）发布了民用 UWB 设备使用频谱和功率的初步规定。规定中将相对带宽大于 0.2 或在传输的任何时刻带宽大于 500MHz 的通信系统称为 UWB 系统。FCC 对 UWB 系统所使用的频谱范围规定为 3.1 ~ 10.6GHz，发射机的有效各向同性发射功率不得高于 -41dBm/MHz，如图 3-24 所示。

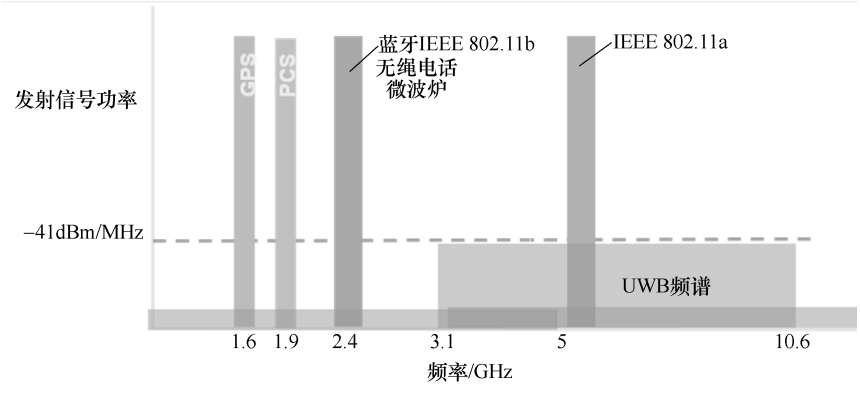


图 3-24　FCC 规定的室内 UWB 发射功率和频谱限制

FCC 关于“超宽带”的定义是：信号的相对带宽（信号频谱的带宽与其中心频率之比，又称相对带宽）大于等于 20%，或者绝对带宽大于等于 500MHz。显然此定义没有界定信号的时域波形特征，因此，有多种方式产生超宽带信号。其中，传统而且典型的方法是利用纳秒级的窄脉冲（又称为冲激脉冲，Impulse）的宽频谱特性来实现，直接发射经过调制的窄脉冲，无需正弦载波，通常将其称为冲激无线电（Impulse Radio，IR）。当 IR 的带宽达到超宽带定义的要求时，称为超宽带冲激无线电（UltraWideBand ImpulSe Radio，IR-UWB），其信号调制主要是对脉冲的幅度和脉冲在时间轴上的位置偏移进行调制。此外，因为 IR-UWB

发射非连续的脉冲串，因此很适合运用跳时（Time-Hopping）技术（事实上，也正是IR-UWB的发展推动了近几年来跳时技术的进步）。另一类的超宽带无线技术仍然基于正弦载波的概念发射连续波，其超宽带的实现可以采用扩展频谱技术或者提高数据传输速率进而提高射频带宽，典型的例子是IEEE 802.15.3a高速WPAN的多频带（Multi-Band，MB）超宽带物理层提案，它的基本特点是将FCC规定的3.1～10.6GHz带宽划分为多个满足超宽带定义的子带（大于500MHz），在每个子带上采用正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）技术。

超宽带无线通信应用大体上可以分为两类，一类是短距离高速应用，数据传输速率可以高达数百Mbit/s，主要是构建短距离高速WPAN、家庭无限多媒体网络以及替代高速短程有线连接，如无线USB和DVD等，典型的通信距离是10m；另一类中长距离（几十米以上）低速率应用，通常数据传输速率为1Mbit/s量级，主要应用于无线传感器网络和低速率连接。超宽带无线通信的网络形式主要是自组织（Ad-Hoc）网络。就对应标准而言，高速率应用对于IEEE 802.15.3，低速率应用对应于IEEE 802.15.4。此外，值得一提的是，超宽带冲击无线电具有特别的军事应用特色，因为发射的是窄脉冲串，因而功率谱很低，具有很好的低截获率特性，这正是超宽带技术首先在军事领域得到关注的原因所在。在军事应用上，超宽带无线通信的距离可达十几千米。

3.4.1.2　UWB的特点

超宽带系统的主要性能特点及技术优势表现在以下几个方面：

1）超宽带带来了全新的通信方式及频谱管理模式。多年来，传统的无线通信技术大都是基于正弦载波的，而消耗大量发射功率的载波本身并不传送信息，真正用来传送信息的是调制信号，即用某种调制方式对载频进行调制。而超宽带系统可以采用无载波方式，即不使用正弦载波信号，直接调制超短窄脉冲，从而产生一个数吉赫兹（GHz）量级的大带宽。这种传输方式上的革命性变化将带来一种崭新的无线通信方式。同时，作为一种与其他现存传统无线技术共享频带的无线通信技术，对于目前日益紧张的、有限的频谱资源，超宽带技术有其独特的优势，全球频谱规划组织也对其表示高度关注和支持。所以，超宽带不仅仅只是一项革命性的技术，它更是一段免许可证的频谱资源。目前FCC开放的频段是3.1～1.6GHz，UWB可共用7.5GHz的频带。

2）抗多径能力强：UWB发射的是持续时间极短的单周期脉冲，且占空比极低，多径信号在时间上是可分离的，因此具有很强的抗多径能力。多径衰落一直是传统无线通信难以解决的问题，而UWB信号由于带宽达数吉赫兹（GHz），具有高分辨率，能分辨出时延达纳秒级的多径信号，而恰好室内等多径场合的多径时延一般也是纳秒级的。这样，UWB系统在接收端可以实现多径信号的分集接收。UWB信号的抗多径衰落的固有鲁棒性特别适合于室内等多径、密集场合的无线通信应用。但UWB信号极高的多径分辨率也导致信号能量产生严重的时间弥散（频率选择性衰落），接收机必须通过牺牲复杂度（增加分集阶数）以便捕获足够的信号能量。这将对接收机设计提出严峻挑战。在实际的UWB系统设计中，必须折中考虑信号带宽和接收机复杂度，得到理想的性价比。

3）定位精确：冲激脉冲具有很高的定位精度和穿透能力，采用超宽带无线电通信，很容易将定位与通信合一，在室内和地下进行精确定位。信号的距离分辨力与信号的带宽成正比。由于信号的超宽带特性，UWB系统的距离分辨精度是其他系统的成百上千倍。UWB信

号脉冲宽度在纳秒级，其对应的距离分辨能力可高达厘米级，这是其他窄带系统所无法比拟的。这使得超宽带系统在完成通信的同时还能实现准确定位跟踪，定位与通信功能的融合极大地扩展了系统的应用范围。

4）保密性强：UWB 信号一般把信号能量弥散在极宽的频带范围内，功率谱密度低于自然的电子噪声，采用编码对脉冲参数进行伪随机化后，脉冲的检测将更加困难。由于 UWB 信号本身巨大的带宽及 FCC 对 UWB 系统的功率限制，使 UWB 系统相对于传统窄带系统的功率谱密度非常低。低功率谱密度使信号不易被截获，具有一定的保密性，同时使对其他窄带系统的干扰可以很小。

5）UWB 具有超高速、超大容量、抗截获性好等诸多优点，超宽带的低功耗特点对于用便携式电池供电的系统长时间工作是非常重要的。UWB 以非常宽的频率带宽来换取高速的数据传输，在 10m 的传输范围内，信号传输速率可达 500Mbit/s。

6）系统结构简单，成本低，易数字化。UWB 通过发送纳秒级脉冲来传输数据信号，其发射机直接用脉冲小型激励天线，不需要功放与混频器；同时在接收端，也不需要中频处理。UWB 系统发射和接收的是超短窄脉冲，无需采用正弦载波而直接进行调制，接收机利用相关器能直接完成信号检测。这样，收发信机不需要复杂的载频调制解调电路和滤波器等，它只需要一种数字方式来产生超短窄脉冲。因此，这可以大大降低系统复杂度，减小收发信机的体积和功耗，易于数字化和采用软件无线电技术。实际上随着半导体技术的发展和新型脉冲产生技术的不断涌现，已经有公司将这种系统集成到单芯片上。

3.4.1.3　UWB 的应用前景

UWB 技术自问世以来，收到了广大研究者的关注，在理论研究和应用研究方面取得了显著的成果。首先来看一下研究方面的一些成果。美国 Xtreme Spectrum 公司能提供在各种无线设备之间传输音频、视频的 UWB 芯片组，它采用双相解调技术和 IEEE 802.15.3MAC 协议，传输速率达到 100Mbit/s，因此 Intel 称 UWB 为无线 USB。Time Domain 公司利用 UWB PPM 技术，开发了两代 PulsOn 芯片，第三代商用 PulsOn 芯片也即将问世。2003 年 1 月，Philips 和 GA 签订了一个备忘录，利用 Philips 在 BiCOMS 的优势和 GA 的 UWB 技术联合开发速率达到 480Mbit/s 的 UWB 芯片组，并支持 IEEE 802.15.3a 标准。Pulse Link 公司在 2003 年第一季度推出了传输速率达 400Mbit/s 的 UWB 芯片组。新加坡的 Cellonics 公司开发了基于非线性动态理论的新技术，它只需要使用一个电感器和一个二极管就可以实现数字调制解调器，不需要混频器、振荡器和锁相环。该技术可以改善 UWB 接收设计中的相关接收，而且简单、成本低，功率也低。美国 Discrete Time 公司开发了多频段 UWB 技术，它采用了不同频段发送信息而不是发射单个脉冲。与单频段 UWB 相比，多频段 UWB 系统的每段内可以用较低的速率发射信息，这降低了 UWB 的成本，具有较好的自适应性，可以与 IEEE 802.11a 共存。Intel、Cisco、Sony 等公司都准备进入无线数据通信市场，无线家用网络将会是 UWB 主流市场。对短距离高速 WPAN，UWB 有希望成为一项可行和有竞争力的无线技术，有能力支持以用户为中心的个人无线通信世界。

总之，UWB 的应用领域十分广泛，总结起来有 3 个方面：雷达成像系统（包括穿地雷达、墙中成像雷达、穿墙成像雷达、医学成像系统、监视系统等）、高速无线通信系统、精确测量定位系统（包括车载雷达、精密测量和传感定位系统）。在雷达成像应用中，主要以 UWB 穿墙成像雷达为主。目前国外已有用于军事、抢险、反恐、资源探测方面的 UWB 穿墙

成像雷达产品，这类产品主要依据的是 FCC 制定的频谱限值要求，最大平均等效全向发射功率（Effective Isotropic Radiated Power，EIRP）不超过 -41.3dBm/MHz，工作频段在 2GHz 以上。UWB 穿墙成像技术产品往往都是利用持续时间极为短暂的 UWB 信号脉冲穿过一定厚度的墙壁，通过设置在成像设备上的信息屏幕，获取墙壁另一侧的物体（运动）信息。此外，大地探测雷达也可以应用 UWB 技术，其工作原理与穿墙雷达是相仿的。在高速无线通信应用中，UWB 可以作为一种短距离高速传输的无线接入手段，非常适合支持无线个域网的应用。UWB 将通过支持无线 USB 的应用，取代传统的 USB 电缆，使无线高速 USB 应用成为可能。UWB 可应用于移动通信、计算机及其外设、消费电子、信息安全等诸多方面，如家用高清电视图像传送、数字家庭宽带无线连接、消费电子中高速数据传输、高清图片及视频显示、汽车视频与媒体中心等。在精确定位应用中，UWB 由于其高分辨率，在精确测量定位系统中得到了广泛应用，汽车防碰雷达系统（车载 UWB 雷达）就是一个典型的例子。车载 UWB 雷达主要应用在 24GHz 频段。

3.4.2　UWB 的架构及研究现状

3.4.2.1　UWB 无线传输系统的基本模型

UWB 系统的基本模型主要由发射部分、无线信道和接收部分构成，与传统的无线发射、接收机结构相比，UWB 的发射、接收机结构相对简单，易于实现，因为脉冲产生器只需产生大约 100mV 的电压就能满足发射要求，因而发射端不需要功率放大器，只需产生满足带宽要求的极窄脉冲即可，在接收端，天线收集的信号先通过低噪声放大器，再通过一个匹配滤波器和相关接收机恢复出期望信号。UWB 无线传输的基本模型如图 3-25 所示。

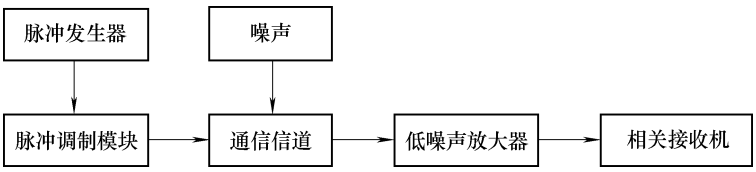


图 3-25　UWB 传输系统的基本模型

3.4.2.2　UWB 的研究现状

UWB 在 10m 以内的范围实现无线传输，是应用于无线个域网（WPAN）的一种近距离无线通信技术。众所周知，IEEE 802.15.3a 从 2003 年开始对 UWB 的技术方案进行标准化。在 UWB 物理层技术实现中，存在两种主流的技术方案：基于正交频分复用（OFDM）技术的多频带 OFDM（MB-OFDM）方案、基于 CDMA 技术的直接序列 CDMA（DS-CDMA）方案。

CDMA 技术广泛应用于 2G 和 3G 移动通信系统，在 UWB 系统中使用的 CDMA 技术与在传统通信系统中使用的 CDMA 技术没有本质的区别，只是使用了很高的码片速率，以获得符合 UWB 技术标准的超宽带宽。OFDM 则是应用于 E3G、B3G 的核心技术，具有频谱效率高、抗多径干扰和抗窄带干扰能力强等优点。

直接序列扩频超宽带技术（DS-UWB）主要是由飞思卡尔（Freescale）半导体公司支持的方案。MB-OFDM 方案则是由 WiMEDIa 联盟支持的。两种标准一直以来都处于激烈争论

中，评价 DS-CDMA 和 MB-OFDM 在技术层面上孰优孰劣，对方案的最终妥协是无益的。在 IEEE 802.15.3a 内部虽然经过多次投票表决，始终无法淘汰其中一种标准，取得统一。最终在 2006 年 1 月份召开的 IEEE 802 会议上，IEEE 802.15.3a 经过投票，解散了该任务组，UWB 在 IEEE 的标准化进程被终止。

UWB 的 MAC 层协议支持分布式网络拓扑结构和资源管理，不需要中心控制器，即支持 Ad-Hoc 或 Mesh 组网，支持同步和异步业务、支持低成本的设备实现以及多个等级的节电模式。协议规定网络以微微网为基本单元，其中的主设备被称为微微网协调者（PNC）。PNC 负责提供同步时钟、QoS 控制、省电模式和接入控制。作为一个 Ad-Hoc 网络，微微网只有在需要通信时才存在，通信结束，网络也随之消失。网内的其他设备为从设备。WPAN 网络的数据交换在 WPAN 设备之间直接进行，但网络的控制信息由 PNC 发出。

像大家熟知的 Wi-Fi、WiMax 联盟一样，WiMedia 联盟的重要使命就是建立 WPAN 认证流程和规范，进行认证以确保设备的互操作性，推动 UWB 技术在全球范围的应用。WiMedia 联盟由英特尔、TI、松下、三星、诺基亚、富士通等著名公司和许多消费电子公司所组成，自成立几年来，已经拥有非常广泛的成员。

WiMedia 联盟定义的 UWB 协议分层如图 3-26 所示。前面已经提到物理层存在 MB-OFDM 和 DS-UWB 两个分支，WiMedia 目前主要采用 MB-OFDM 方式。为了支持多种应用，如无线 USB、无线 IEEE1394 等，WiMedia 联盟在物理层和 MAC 层之上定义了协议适配层（Protocol Adapter Layer，PAL）。

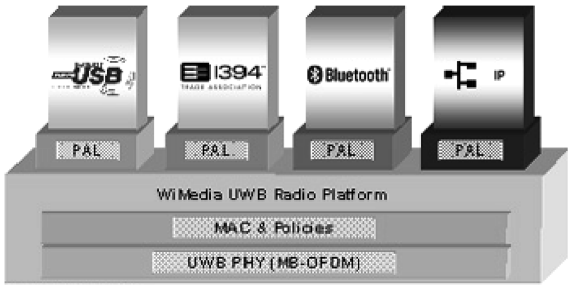


图 3-26　UWB 协议分层

WiMedia 联盟已经发布了物理层认证规范和兼容性测试平台，并且开展了多次物理层兼容性测试，主要 UWB 芯片和设备商均参加了兼容性测试。随着产品的逐步成熟，WiMedia 联盟将正式开展 UWB 的设备认证工作。

3.4.3　UWB 与物联网结合的关键技术

UWB 技术具有巨大的诱惑力，同时又向我们提出了很多的挑战。虽然 FCC 对 UWB 的发射功率、通信距离做了严格的限制，但它毕竟与现存的大多数通信系统工作在同一频段，相互之间的干扰问题将不得不考虑。要实现该技术用途的广泛性，许多关键技术有待于解决。

（1）规则与标准

UWB 一项革命性的新技术，需要制定各种规则与标准来保证 UWB 系统与目前运行系统

之间的兼容性和不同厂商 UWB 产品之间的兼容性。UWB 要获得成功首先要有一套广为接受的物理层（PHY）和媒体接入控制（MAC）协议标准。UWB 技术与（Ad-Hoc 网的结合使得 UWB 系统容量变得很大，因此在 Ad-Hoc 网的管理层上也要制定相应的标准来保证各个移动节点接入的灵活性和各个产品之间的兼容性。

基于 UWB 技术的无线 Ad-Hoc 网在网络构成和路由寻找过程中，利用 UWB 技术的精确定位能力能准确地测量出节点之间的距离，再通过节点间的信息交互可以逐步算出网络的地理拓扑结构图。但该地理拓扑图并不能作为路由选择的唯一依据。由于 UWB 在距离、速率和功率上的互换性，给路由的选择带来了极大的灵活性。采用 UWB 技术后，需要研究一种具有无线资源管理功能的路由算法，综合考虑跳数、传输速率和发送功率等因素，使整个网络的无线资源的利用率达到最优，网络的全局运行成本最低。其中 Ad-Hoc 网络的动态路由协议是设计 Ad-Hoc 网络的关键，它要求有一个高度自适应的路由机制来处理网络拓扑结构的变化，以实现 Ad-Hoc 网与主干网的多跳接入和无缝接入。而现有的路由技术不适用于 Ad-Hoc 网络。如何把多个无线 Ad-Hoc 网连成一个大网以及如何与 Internet 相结合，是当今热点问题之一。

（2）信号的选择

UWB 信号的形式主要有两种：跳时（TH）信号和直接序列（DS）信号。TH-UWB 采用瞬时开关技术来产生短脉冲或只有很少几个过零点的波形，直接将能量扩展到很宽的频带内。脉冲由专用宽带天线，以每秒几十至几百兆赫的高速率发射，这些脉冲在时间上以随机或伪随机间隔分布。对这些脉冲进行时间编码就可以实现多址通信。DS-UWB 采用 Gbit/s 的速率发射的高占空比宽带脉冲，该脉冲序列以每数百 Mbit/s 的速率对数据进行编码，多个编码脉冲表示一个 bit，编码增益能提供抗多径干扰能力，在短距离范围内，DS-UWB 能提供极高的数据传输率。这两种信号在各种环境中的优缺点还有待于进一步研究与实验。

UWB 虽然具有抗多径衰落的能力，但它还是受到多径衰落的影响。例如，当传播距离和天线高度之比过大时，视距信号和反射信号到达的时差可能小于发射脉冲的持续时间，这时多径干扰将不可避免。因此要对 UWB 系统的最大传输速率做出严格限制，使得信号的周期尽可能长一点，确保在下一个脉冲发射之前目前正在传输的脉冲所引起的多径分量基本消失，以减少传输脉冲之间的干扰；同时 UWB 信号的周期又不能太短，否则在一个脉冲传输过程中信道的时变效应就不能忽略。

（3）抗干扰技术

UWB 采用的是频谱重叠技术，容易对其他同频系统产生干扰。UWB 的发射功率虽然很小，但它的瞬时峰值功率还是比较大的，因此有必要采取一定的优化措施，例如自适应功率控制、占空比优化等，以减少对其他通信系统的干扰。另一方面，由于 UWB 系统传输功率很低，且大部分工作在工业区、商业区或者住宅区等一些环境恶劣的场合，容易受到噪声和其他同频无线电的干扰。如何解决 UWB 和其他无线电系统的兼容问题是目前 UWB 的一个重要课题。

（4）调制、接收技术

UWB 原先用在军事上，大容量、多用户不是它的主要目的。但在商业通信中大容量、多用户恰恰是它的主要问题，而 UWB 信道的时域特殊性需要一个合适的调制技术和编码方

案来提高系统的用户容量。

理想的 UWB 接收机是 RAKE 接收机，但它的复杂性随着多径数的增加呈指数上升，因此一般采用的是次最佳 RAKE 接收机。这种次最佳 RAKE 接收机的性能又是任何？是否存在其他更好的接收机结构？这些都有待于进一步的研究。根据 Q. Li 和 L. Rusch 的研究，自适应多用户检测接收机能集聚多径能量，在克服符号间干扰和码间干扰等方面要比4个和8个支路的 RAKE 接收机好得多，特别是在抗宽带干扰方面，这种接收机具有更多的优越性。

UWB 信号覆盖范围宽，频率弥散效应明显。在频段的低端和高端信号有着不同的失真、频散及损耗。另外高速器件的成本要比低速器件高得多。采用信道分割技术可以有效地克服这些问题。通过信道的分割技术还能避免与无线 LAN 使用的 5GHz 频带的干扰，不同区域可分配不同的波段，确保信号的轻松传输。

在 UWB 产品的天线设计方面，要求是微型、在各种条件下能正常工作（例如靠近物体或放在身边），具有超宽频带和一定增益。而 UWB 信号的带宽很宽，根据自由空间传播定理，频段的高端和低端增益相差大约 11dB，所以实现高效的 UWB 天线，尤其在尺寸很小时，困难重重。

（5）信道特性

UWB 不同于窄带无线通信，它在调制、编码、功率控制、天线设计等方面有着许多特殊性。在研究 UWB 通信技术的时候急切需要一个合适的、贴近于现实的 UWB 信道模型来公正地评价该技术的物理性能。令人遗憾的是至今人们对 UWB 的信道特性，特别是 UWB 信道的时变特性，还不十分清楚，我们还没有足够多的实验数据来建立一个完整的信道模型。

（6）集成电路的开发

UWB 系统的带宽比窄带系统高出了几十倍，实现 UWB 宽带集成电路和高速非线性器件方面，器件的宽带特性是其技术瓶颈所在，它们的开发成功与否是 UWB 技术得以发展和应用的关键因素。

3.4.4　UWB 的发展趋势

UWB 具有带宽高、抗干扰能力强的特点，是物联网重要的通信手段。UWB 除了上一节介绍的关键技术之外，还有一些新的方向，如 UWB 与认知无线电（Cognitiver Radio，CR）结合的认知超宽带和基于协作模式的 UWB 定位研究。

3.4.4.1　认知超宽带系统

CR 是一种智能的无线电技术，它具有学习能力，能与周围环境交互信息，以感知和利用在该空间的可用频谱，并限制和降低冲突的发生。CR 与 UWB 都是提高频谱利用率的技术手段，所以 CR 与 UWB 结合，具有广阔的应用场景。认知超宽带是一种基于频谱感知的具有自适应发射功率谱密度和灵活波形的新型超宽带系统。该系统的基本原理主要是利用 CR 能够感知周围频谱环境和 UWB 系统易于数字化软件化的特性，依据感知得到的频谱信息和动态频谱分配策略来自适应地构建 UWB 系统的频谱结构，并生成相应的频谱灵活的自适应脉冲波形，根据信道的状态信息进行自适应的发射与接收。

3.4.4.2　基于协作模式的 UWB 定位技术

目前在反恐、应急、救援等应用中，室内定位是一个关注的热点。室内无法利用 GPS、北斗等卫星定位系统，需要采用新的技术实现室内定位。UWB 凭借其准确的定位优势，采用协作模式与 GPS 等室外定位系统结合，实现全方位立体化的定位。美国军方正在研究 UWB 室内定位系统，以部分已知坐标节点为参考，通过协议定位算法获得室内节点位置的经纬度坐标。

参 考 文 献

[1] Shahin Farahani. ZigBee Wireless Networks and Transceivers [M]. 1st ed. MA: Newnes, 2008.

[2] Jean-Philippe Uasseur. Interconnecting Smart Objects with IP [M]. 1st ed. MA: Morgan Kanfmann, 2010.

[3] George Aggelou. Wireless Mesh Networking with 802.16, 802.11 and ZigBee [M]. 1st ed. New York: Mc Graw Hill, 2009.

[4] 刘辉. ZigBee 无线传感器网络的设计及应用 [D]. 苏州：苏州大学，2007.

[5] 张顺扬. ZigBee 无线传感器网络研究及仿真 [D]. 广州：广州工业大学，2008.

[6] 吴飞. 基于 ZigBee 无线传感器网络的研究 [D]. 太原：太原理工大学，2010.

[7] 庞娜. 网状结构 ZigBee 无线传感器网络研究 [D]. 长春：吉林大学，2010.

[8] 邓永红. 详解蓝牙技术 [J]. 有线电视技术，2005（5）.

[9] 王一强，孙罡. UWB 超宽带技术研究及应用 [J]. 通信技术，2009（3）：70-73.

[10] 王忠思，黄辉，邵晓. UWB 无线通信关键技术及应用分析 [J]. 通信电源技术，2009，26（4）：42-45.

[11] 卜格鸿，喻文芳. 蓝牙（Bluetooth）技术及其应用 [J]. 装备指挥技术学院学报，2002，13（5）：92-95.

[12] 闫文婷. 基于蓝牙技术的数据传输的研究与实现 [D]. 南京：南京理工大学，2004.

[13] 周翔. UWB 无线通信的国内外发展及研究应用现状 [J]. 南京职业技术学院学报，2005，5（4）：37-38.

第 4 章　传输层——网络接入技术

如今已经存在的各种有线无线通信网络，能够满足高带宽、远距离传输的要求。将现有通信网用来承载物联网感知信息，需要不同的接入技术来支持。接入网处于物联网传输层汇聚网和承载网之间，实现感知数据从汇聚网到承载网的接入。

物联网的接入方式是多种多样的，各种网关设备是很重要的部件：它们将多种接入手段整合起来，统一接入到通信网络中，并且可满足局部区域短距离通信的接入需求，实现与公共网络的连接，同时完成转发、控制、信令交换和编解码等功能，而终端管理、安全认证等功能保证了物联网业务的质量和安全。

结合物联网的特点，网络接入技术不再是传统的通信网中的接入技术。本章介绍的接入技术都是结合了物联网的种种特点的接入方式，主要采用 6LoWPAN、M2M 及全 IP 融合架构。

6LoWPAN 是物联网无线接入中的一项重要技术。6LoWPAN 是使用 IPv6 的低功率无线个人局域网，该技术结合了 IEEE 802. 15. 4 无线通信协议和 IPv6 技术的优点，解决了窄带宽无线网络中的低功率、有限处理能力的嵌入式设备使用 IPv6 的困难，实现了短距离通信到 IPv6 的接入。

M2M 接入技术是目前物联网一个重要的接入方式，是物联网中承上启下、融会贯通的平台，同时也是一种经济、可靠的组网方法。现阶段物联网的发展还处于初级阶段，M2M 由于跨越了物联网的应用层和感知层，是无线通信和信息技术的整合，它可用于双向通信，如远距离收集信息、设置参数和发送指令，M2M 技术广泛用于安全监测、远程医疗、货物跟踪、自动售货机等。

全 IP 融合技术是通过全 IP 无缝集成物联网和其他各种接入方式，诸如宽带、移动互联网现有的无线系统，将其都集成到 IP 层中 ，从而通过一种网络基础设施提供所有通信服务，这样将带来诸多好处，如节省网络成本，增强网络的可扩展性和灵活性，提高网络运作效率等。但物联网时代的数据量巨大，各种物体设备都需接入网络，而传统的 IP 地址协议空间不足以满足传感网的巨大需求。全 IP 融合技术和 IPv6 协议可以很好地解决这一问题。对传感网而言，IPv6 协议提供的巨大地址空间，以及 IPv6 协议支持的移动性等特点非常适合与其结合发展。

4. 1　6LoWPAN

6LoWPAN 是实现无线嵌入式网络的重点。IPv6 是 20 世纪 90 年代 IETF（互联网工程任务组）设计的用于替代 IPv4 的下一代互联网 IP，用来解决迅速增长的互联网需求。6LoWPAN 技术结合了 IEEE 802. 15. 4 无线通信协议和 IPv6 技术的优点。它采用的是 IEEE802. 15. 4 规定的物理层和 MAC 层，不同之处在于 6LoWPAN 技术在网络层上使用 IETF 规定的 IPv6。

在物联网中，信息采集最基本和最重要的方式之一就是传感器，每个传感器都具有数据采集、简单的数据处理、短距离无线通信和自动组网的能力。大量传感器节点组成传感器网络。随着传感器与无线网络技术的迅速发展，需要进行处理和传输的数据量也急剧增加。为了实现对物体智能控制的目标，人们将大量的传感器节点接入互联网。而传统的IP地址协议空间不足以满足传感器网络的巨大需求。IPv6协议可以很好地解决这一问题。在这种背景下，2004年11月IETF正式成立了6LoWPAN协议工作组，即基于IPv6协议的低功耗无线个人局域网工作组，该工作组致力于研究如何解决IPv6数据包在IEEE 802.15.4上传输问题。规定6LoWRAN技术在物理层采取IEEE 802.15.4，MAC层以上采取IPv6协议栈。

4.1.1　无线嵌入式设备网络对网络协议的挑战

功率和频宽比：电池供电的无线设备需要保持很低的频宽比，降低设备功率，并准备随时访问网络。

多播：嵌入式无线电技术，例如IEEE 802.15.4，并不特定支持多播，在这样一个网络中，泛洪式传输对功率和带宽都是一种极大的浪费。多播对IPv6的操作而言是极为重要的。

网格拓扑：嵌入式无线电技术的应用主要受益于多条网格组网以获得要求的覆盖范围和有效的开销。

带宽和帧大小：低功率无线嵌入式无线电技术通常有有限的带宽（在20～250kbit/s）和帧长度（40～200B）。在网格拓扑结构中，随着信道共享技术的使用，带宽进一步降低，并随着多跳转发快速减少。IEEE 802.15.4标准有127B的帧长度，layer-2净负载字节长度只有72B。IPv6标准中的最大帧长为1280B，因此需要进行划分。

可靠性：标准互联网协议不对低功率无线网络进行优化。例如，TCP无法区分丢包的原因是因为拥挤还是因为失去了无线连接。发生在无线网络嵌入式网络进一步的不可靠是因为节点的无法读入、能量耗尽和休眠占空比。

为了解决这些问题，IETF建立6LoWPAN的工作小组，并专门让无线嵌入式设备和网络可以使用IPv6。IPv6设计的特点有一个简单的头结构，并具有分级寻址模型，因而适用于在无线嵌入式网络中使用6LoWPAN。此外，通过为这些网络创建一个专门的标准组，6LoWPAN中一个很小的IPv6堆就可以兼顾最小的设备。最后，通过进行特别针对6LoWPAN的邻居发现协议版本的设计，可以将低功率无限网格网络的特性纳入考虑之中。结果是将6LoWPAN有效扩展到无线嵌入式领域，从而使端到端IP网络和特点得到广泛应用。

4.1.2　6LoWPAN的技术优势

无线嵌入式网络使得很多应用变得可能。然而这些应用程序大量使用的专有技术使其难以融入更大的网络和并且很难更好地提供基于互联网的服务。这一问题可以通过使用IP解决，IP整合各种不同应用使它们互相融合，如图4-1所示。IP的好处包括：

1）普及性。IP技术被众多的人接受。作为下一代互联网核心技术的IPv6，在LoWPAN网络中使用也更易于被大众接受。

2）适用性。基于IP的设备不需要翻译网关或授权书就可以很容易连接到其他的IP网络。

3）兼容性。IP 网络对现有的网络基础设施兼容。

4）开放性。IP 是开放性协议，随着标准化进程和文件对公众的开放，IP 技术在一个开放和自由的环境中越来越具体，从而产生了大量相关的创新。

5）更广阔的地址空间。单从数字上来说，IPv6 所拥有的地址容量是 IPv4 的约 8×10^{28} 倍，达到 $2^{128} - 1$ 个。这不但解决了网络地址资源数量的问题，同时也为除计算机外的设备连入互联网在数量限制上扫清了障碍。满足了部署大规模、高密度 LoWPAN 网络设备的需求。

6）IPv6 支持无状态自动地址配置。IPv6 采用了无状态地址分配的方案来解决高效率海量地址分配的问题。其基本思想是网络侧不管理 IPv6 地址的状态。节点设备连接到网络中后，将自动选择接口地址（通过算法生成 IPv6 地址的后 64 位），并加上前缀地址，作为节点的本地链路地址。

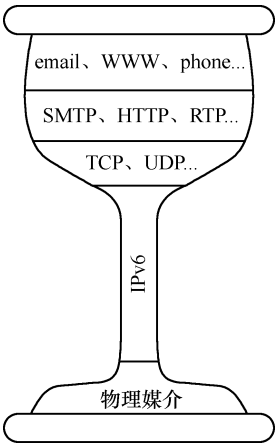


图 4-1　原 IP 架构

由此可见，IPv6 技术在 6LoWPAN 上的应用具有广阔的发展空间，从而使得大规模 6LoWPAN 的实现成为可能。与传统的 IP 网络直接通信需要很多互联网协议，通常需要一个操作系统来处理这些协议的复杂性和可维护性。传统的互联网协议要求对嵌入式设备的主要原因：

1）安全：IPv6 包括可选的支持 IP 安全认证和加密，并且网络服务通常利用安全接口或运输层安全机制。这些技术有时候会太复杂，特别是对简单的嵌入式设备。

2）网络服务：互联网网络服务取决于网络服务，主要是传输控制协议（Transmission Control Protocol，TCP）、HTTP、SOAP（Simple Object Access Protocol，简单对象访问协议）和复杂传输类型的 XML 等。

3）管理：基于简单网络管理协议（Simple Network Management Protocol，SNMP）的管理和网络服务经常是低效和复杂的。

4）帧长度：现在的网络协定需要足够的帧长度，大量应用协议对带宽有很高要求。

4.1.3　6LoWPAN 的历史和标准

6LoWPAN 是由互联网工程任务组（IETF）定义的一系列标准，它发展并兼容所有核心网络的标准和架构。6LoWPAN 的简单技术定义是：通过一个适配层和优化的相关协议，6LoWPAN 标准使 IPv6 能够高效地在简单的嵌入式设备的低功耗、低速率无线网络中应用。

虽然嵌入式 IP 已经有很长的历史了，6LoWPAN IETF 的工作小组于 2005 年才正式开始。20 世纪 90 年代，摩尔法则假定指出计算和通信能力的迅速提高，可以使得任何嵌入式设备都能够实现 IP。虽然这个假定有一部分是真实的，而且物联网发展速度极快，但是廉价、低功耗的微控制器和低功耗的无线网络无线电技术并没有得到应用。绝大多数简单的嵌入式设备还利用记忆有限的 8 位、16 位微控制器，因为 8 位、16 位微控制器功耗低、廉价、小巧。与此同时，无线科技的物理权衡导致了短程、低功率的无线电有限的数据传输速率、帧长度和占空比，在 IEEE 802.15.4 标准中就是这样。最小化网络协议的早期作品采用低功率微控制器和无线技术，包括瑞典计算机科学学院的 μIP 技术和无线通信中心的 NanoIP 技术。

IEEE 802.15.4 标准在 2003 年发布是 6LoWPAN 标准化的最主要因素。第一次全球广泛支持的低功率，无线嵌入式通信标准变为现实（IEEE802.15.4）。这个新标准的普及给因特网社区适应这种 IP 无线嵌入式链接的标准必要的鼓舞。

2007 年第一个 6LoWPAN 标准发布，RFC4919 指定了原始标准的基本需求和初始目标，接着 RFC4944 具体说明了 6LoWPAN 的格式和功能。通过实验和研究工作，6LoWPAN 工作小组对头压缩、邻居发现、使用场景和路由要求等方面进行了改进。2008 年，新 IETF 低功耗，低损耗网络路由工作小组成立。这个工作小组致力于研究低功耗、无线、不可靠网络中的路由要求和解决方案。虽然不是限制在 6LoWPAN 中使用，但在 6LoWPAN 中使用是一个主要的目标。

2008 年，ISA 开始无线工业自动化系统的标准化：SP100.11a（也称为 ISA100），它是基于 6LoWPAN 的。图 4-2 给出了相关标准组织、联盟之间的关系。开放空间联盟（Open Geospatial Consortium，OGC）规定基于 IP 的感应研究和应用的解决方案。2007 ~ 2008 年，6LoWPAN 工作组陆续发布了一些草案，包括 6LoWPAN 数据包格式、6LoWPAN 协议体系架构、路由协议、IPv6 邻居发现技术及 6LoWPAN 协议应用场景等。2009 年，欧洲电信标准协会（European Telecommunication Standards Institute，ETSI）成立了一个 M2M 的工作组，包括兼容 6LoWPAN 的端到端 IP 架构。

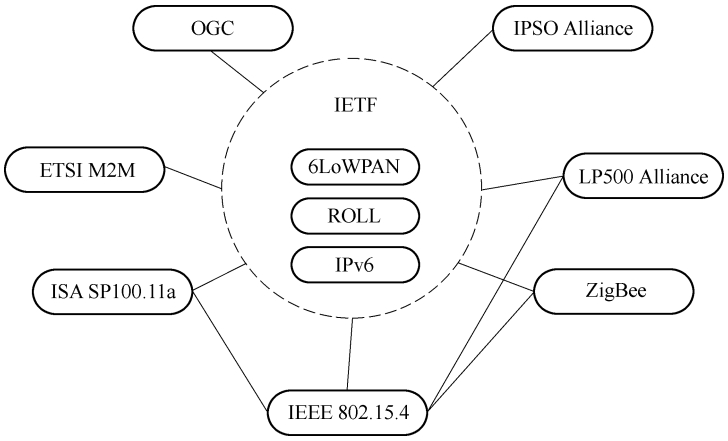


图 4-2　6LoWPAN 与各标准、联盟的关系

4.1.4　6LoWPAN 架构

如图 4-3 中展示了 3 种不同的 LoWPAN：简单型 LoWPAN、扩展型 LoWPAN、自组织型 LoWPAN。一个 LoWPAN 是 6LoWPAN 节点的集合，这些节点具有相同的 IPv6 地址前缀（IPv6 地址中前 64 位），这意味着在 LoWPAN 中无论哪个节点的 IPv6 地址都保持一样。自组织型 LoWPAN 不需要连接到互联网，可以在没有互联网基础设施的情况下运行。简单型的 LoWPAN 通过一个 LoWPAN 边缘路由器连接到另一个 IP 网络。图中展示了一个回程连接（例如点对点 GPRS），但这也可以是中枢网络连接（共享的）。扩展型 LoWPAN 包含了 LoWPAN 中心（例如以太网）连接的多边缘路由器。

LoWPAN 通过边缘路由器连接到其他的 IP 网络。边缘路由器起着非常重要的作用，因

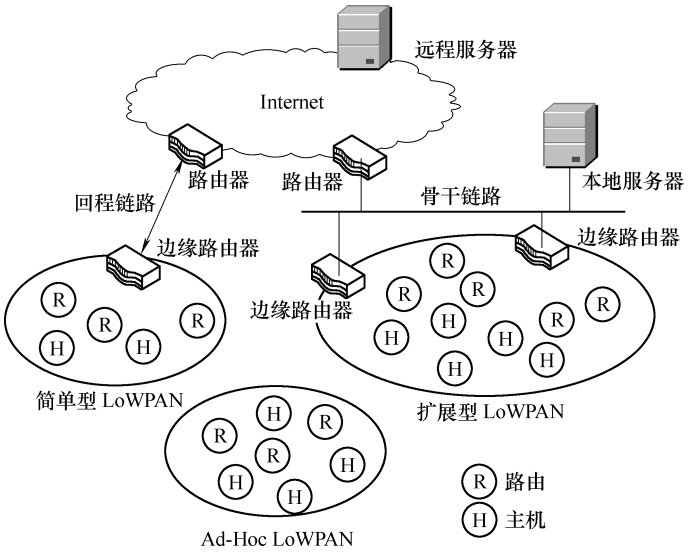


图 4-3　6LoWPAN 架构

为在进行 6LoWPAN 压缩和邻居发现时，它可以连接内外网络。如果 LoWPAN 连接到一个 IPv4 网络，边缘路由器也能够处理与 IPv4 网络的互联。边缘路由器有典型的相关 IT 管理解决方案的管理特性。如果多个边缘路由器共享一个共同的骨干链接，它们能被相同的 LoWPAN 支持。

LoWPAN 由主节点或路由节点与一个或者更多的边缘路由器组成。一个 LoWPAN 节点接口具有相同的 IPv6 前缀，IPv6 前缀被分配给边缘路由器和主机。为了方便有效的网络操作，节点在边缘路由器进行注册。这些操作是邻居发现的一部分，这是 IPv6 的一个重要基本原理。

邻居发现定义了在相同链接中主机和路由器的相互作用。在同一时间内 LoWPAN 节点可以参与多个 LoWPAN（称为 multi-homing），并且边缘路由器之间可以达到容错性。LoWPAN 中的节点可以在边缘路由器之间甚至不同 LoWPAN 之间自由移动。由于没有物理变化的无线通信信道也可以改变网络拓扑结构。

如同正常 IP 节点间通信一样，LoWPAN 节点和其他 IP 网络节点之间的通信是以一种端到端的方式进行的。每一个 LoWPAN 节点都由一个 IPv6 地址唯一确定，并且可以发送和接受 IPv6 数据包，简单型 LoWPAN 和扩展型 LoWPAN 节点可以借助边缘路由器的服务器互相通信。由于 LoWPAN 节点的有效负荷和处理能力严格受限，应用协议经常在 UDP 负载中设计一个简单的二进制格式。

简单型 LoWPAN 和扩展型 LoWPAN 的主要不同在于 LoWPAN 中的多边缘路由器的存在，它们拥有共同的 IPv6 前缀和主干链接。多重 LoWPAN 可以与其他部分交叠（即使是在同样的信道中）。当节点从一个 LoWPAN 移动到另一个 LoWPAN 时，节点的 IPv6 地址会发生变化。简单 LoWPAN 通过回程链路连接到互联网。

网络调度时，根据网络管理需求，一般优先考虑多重简单型 LoWPAN 而不是回程链接中的扩展型 LoWPAN。

在扩展型 LoWPAN 结构中，如图 4-3 右侧，多个边缘路由器共享一个共同的骨干链

接和通过拥有同样的 IPv6 的前缀合作，卸载的大多数邻居发现消息来骨干链接。这大大简化了 LoWPAN 节点操作，因为 IPv6 地址在扩展型 LoWPAN 和运动的边缘路由器之间是稳定的。

边缘路由器代表 IPv6 节点对外进行转发。对 LoWPAN 外面的 IP 节点而言，不管它们的接入点在哪里，LoWPAN 节点总是可以接入的。这使得大企业也可以建立 6LoWPAN 基础设施。运行起来和 WLAN（Wi-Fi）接入点的基础设施相似，只是接入点第 3 层代替第 2 层。

6LoWPAN 不需要基础架构操作，但也可以作为 Ad-Hoc LoWPAN 进行操作。在这种拓扑结构中，一个路由器必需配置为一个简化的边缘路由器，实现两个基本功能：生成一个独特的本地单播地址（Unique Local Unicast Address，ULA），以及实现 6LoWPAN 邻居发现注册功能。

4.1.5　6LoWPAN 协议栈

为了实现无线传感器与 IP 网络的无缝互联，6LoWPAN 协议栈的架构如图 4-4 所示。该体系结构分别包括了 IEEE 802.15.4 物理层、IEEE 802.15.4 媒体访问控制层（Medium Access Control，MAC）层、6LoWPAN 适配层，IPv6，6LoWPAN 传输层（UDP，ICMP）以及应用层。图 4-4 把 IPv6 协议栈与 6LoWPAN 协议栈进行了比较，一个典型的 IP 协议栈相应的 5 层网络模型。由于互联网协议将大量不同的链路层技术与多个传输应用协议联系起来，互联网模型有时被称为“柳腰”模型。

6LoWPAN 中的 IPv6 协议栈与普通 IP 协议栈的区别如图 4-5 所示。

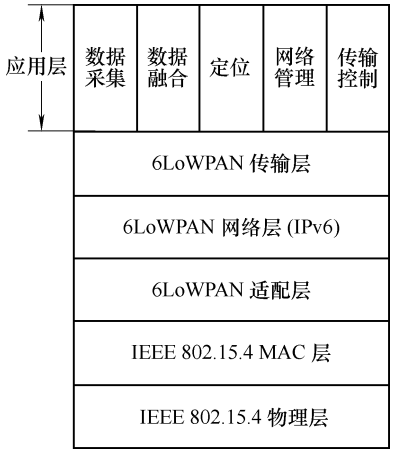


图 4-4　6LoWPAN 协议的体系结构

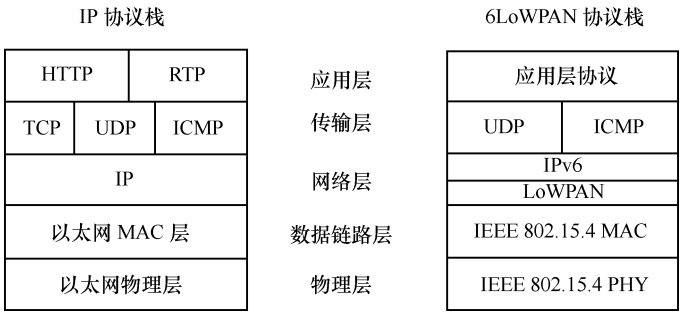


图 4-5　IP 和 6LoWPAN 协议栈区别

一个简单的 6LoWPAN 中的 IPv6 协议栈（也称为 6LoWPAN 协议栈）与普通 IP 协议栈基本相同，在以下几个方面有不同之处：

首先，6LoWPAN 仅支持 IPv6，在 IEEE 802.15.4 和（RFC4944）里面类似的链路层中，LoWPAN 适配层是定义在 IPv6 之上的优化。实际上，嵌入式设备实现 6LoWPAN 协议栈经常同 IPv6 一起对 LoWPAN 进行配置，因此它们作为网络层的一部分一起展示。

其次，在传输协议方面。最常见的6LoWPAN传输协议是用户数据协议（User Datagram Protocol，UDP），它也可以按照LoWPAN格式进行压缩。因为性能、效率和复杂性的问题，6LoWPAN的传输控制协议（TCP）不常用。互联网控制消息协议（ICMPv6）用来进行信息控制。

LoWPAN格式和全IPv6之间的转换由边缘路由器完成。这转换对双向都是透明、高效的。在边缘路由器中的LoWPAN转换是作为进行6LoWPAN网络接口驱动的一部分，并且对IPv6协议栈本身通常是透明的。

4.1.6　6LoWPAN链路层

IP的最重要功能之一是互联各种异构网络使之成为一个单一的互操作的网络。这同样适用于6LoWPAN和嵌入式网络，那里有许多无线（也有有线）链路层技术。嵌入式网络的针对性应用比典型个人计算机网络需要更广泛的通信解决方案，个人应用几乎普遍地使用以太网和Wi-Fi。幸运的是在嵌入式网络应用领域里，IEEE 802.15.4标准是最常见的2.4GHz无线技术，并已经被用来作为6LoWPAN发展基础。其他6LoWPAN技术包括GHz以下无线电、远程遥测链接和平坦功率通信，见表4-1。

为了能够在互联网协议下工作，链路层应当具有一些特点满足要求。这些特点包括框架、寻址、纠错、长度指示、可靠性、广播以及合理的帧长度。6LoWPAN的设计是为了可以使用一种特殊类型的链接，具有一套的链接的要求和建议。

链路层支持6LoWPAN最基本的要求是框架、单播传输和寻址。寻址需要区分同一链接中的节点，并形成IPv6地址。它强烈建议一个链接支持唯一的默认地址情况下，从而能够支持无边界的自动配置。多址接入链接应该提供广播服务。IPv6标准而不是6LoWPAN标准要求能够提供多播服务，只要满足广播就足够了。IPv6需要最大传输单元（Maximum Transmission Unit，MTU）是一个链接1280B，这一要求6LoWPAN满足，因为它支持6LoWPAN适配层的划分。一个链接应该提供至少30B长的有效负载长度，最好是大于60B。虽然UDP和ICMP包括一个简单的16位校验，建议链路层也进行纠错检查。最后，因为IPsec对6LoWPAN而言，并非总是很实用的，强烈建议连接点具有强大的加密和认证能力。2006年的版本的IEEE 802.15.4标准中不包括“下一个协议标识符”，这使得检测负载中的协议十分困难。

接下来的部分介绍了用于6LoWPAN的3种链路层技术：IEEE 802.15.4，GHz以下的ISM带宽无线电和低速功率线通信。

IEEE 802.15.4标准描述了低速率无线个人局域网的物理层和MAC协议，属于IEEE 802.15工作组。IEEE 802.15.4定义了两个物理层标准，分别是2.4GHz和868/915MHz物理层。两个物理层都基于直接序列扩频（Direct Sequence Spread Spectrum，DSSS），使用相同的物理层数据包格式，在868/915MHz、2.4GHz的ISM频段上，数据传输速率最高可达250kbit/s。2.4GHz频段采用的是O-QPSK调制，868/915MHz频段采用BPSK调制。第一个版本的标准于2003年发布，2006年修订。最近IEEE 802.15.4a标准发布，扩展IEEE 802.15.4有两个新的物理层标准：分别是2.4GHz物理层和3.1～10.6GHz的超宽带物理层两个物理层都基于直接序列扩频，使用相同的物理层数据包格式，区别在于工作频率、调制技术、扩频码片长度和传输速率。

表 4-1　IEEE 802.15.4 标准所期望达到的特性

速　　率	250kbit/s（2.4 GHz）和 20 kbit/s（868MHz/915MHz）
电池寿命	通过采用不对称能耗节点以及无电池运作等优化手段，延长电池寿命
传输时延	10～50ms 或 1s
通信距离	一般 10cm～10m，最多 100m
网络节点数	最多 65534 个
复杂度	低于现有标准（如 IEEE 802.11）
MAC 层的网络控制方式	星形或对等网络

（1）IEEE 802.15.4 网络构成和网络拓扑

IEEE 802.15.4 支持两种拓扑：单跳星形或多跳对等拓扑（见图 3-3 及图 3-5）。

最简单的一种是星形网，只有一个网络协调器，连接多个从设备。为了降低系统成本，定义了两种物理设备：完整功能设备（Full Function Device，FFD）和部分功能设备（Reduced Function Device，RFD）。FFD 支持各种拓扑结构，可以作为网络协调器，可以与任何其他设备对话。RFD 仅支持星形结构，不能作为网络协调器，只能与网络协调器对话，但是实现非常简单。在星形网中只有网络协调器是 FFD，其他均为 RFD。另一种网络结构是对等网络，它的覆盖范围很大，有成千上万个节点。

（2）IEEE 802.15.4 网络的工作模式和数据传送方式

IEEE 802.15.4 支持两种工作模式：信标使能（Beacon-enabled）和无信标使能（Non-beaconenabled）模式。

信标使能模式中，Coordinator 定期广播信标，以达到相关设备实现同步及其他目的。在无信标使能模式中，Coordinator 不定期广播信标，而是在设备主动向它请求信标时再向它单播信标。

IEEE 802.15.4 网络数据传送方式有 3 种：直接数据传输、间接数据传输和有保护时隙数据传输。数据可以在协调者和设备之间进行传输，也可以在对等网络中从一方到另一方。

（3）IEEE 802.15.4 的技术特点

1）允许传输的报文长度较短。MAC 层允许的最大报文长度为 127B，除去 MAC 头部 25B 后，仅剩下 102B 的 MAC 数据。

2）支持两种地址。长度为 64bit 的标准 EUI-64 长 MAC 地址以及长度仅为 16bit 的短 MAC 地址，可以视协议实现选用两种地址。

3）带宽低。在不同的工作频率下 IEEE 802.15.4 协议提供不同的数据速率：250kbit/s（2.4GHz），40kbit/s（915MHz），20kbit/s（868MHz）。

4）网络拓扑简单，可以在拓扑中进行多跳路由的操作。

5）低功耗。一般运行 IEEE 802.15.4 的节点都要求使用低功耗的硬件设备，使用电池供电。

4.1.7　6LoWPAN 寻址

6LoWPAN 中 IP 寻址同任何 IPv6 网络中都相同，类似于以太网络中的寻址。IPv6 地址

是由 6LoWPAN 的前缀和无线网络接口链路层地址自动形成的。6LoWPAN 中的寻址方式的不同之处在于低功耗的无线技术支持链路层寻址，链路层地址和 IPv6 地址之间的直接映射用于进行压缩。

IPv6 地址长 128bit，前 64 位为前缀部分，后 64 位是接口的标识符。无边界地址自动配置，用来形成 IPv6 链路层地址的无线通信接口的接口标识符。为了压缩和简化，6LoWPAN 网络假定 ID 直接映射到链路层地址，因此可以避免地址分辨的需要。6LoWPAN 中 IPv6 地址的格式由前缀和链路层地址组成，这样可以获得高的压缩比。

4.1.8　6LoWPAN 适配层

IPv6 协议作为流行的网络层协议大多部署在路由器、PC 等计算资源较为丰富的设备上；而无线传感器节点采用 IEEE 802.15.4 标准，大多运行在计算资源稀缺的无线设备上。由于两者在设计出发点上的不同，导致了 IPv6 协议不能像构架到以太网那样直接地构架到 IEEE 802.15.4 MAC 层上，需要一定的机制来协调这两层协议之间的差异。在无线传感器网络超轻量化 IPv6 协议栈研究项目的实现中，在 IPv6 层和 MAC 层之间引入了适配层来屏蔽 MAC 层的差异，来解决 6LoWPAN 遇到的若干问题。图 4-6 为 6LoWPAN 适配层的功能模块示意图，适配层的主要功能有：

1）6LoWPAN 支持树状和网状等点对点的多跳拓扑。适配层为 6LoWPAN 提供网络拓扑构建、地址分配和 MAC 层路由等服务。在多跳拓扑中，中间的节点作为适配层报文的转发者，为其他节点转发数据报文。

2）IEEE 802.15.4 标准定义的 MAC 层的最大 MTU 为 102B，而 IPv6 协议要求的最小 MTU 为 1280B。适配层对 IPv6 报文头部进行压缩和解压缩，并且对超过 102B 的报文进行分片和重组。

3）与以太网不同，IEEE 802.15.4 不支持组播，由适配层为 IPv6 提供组播的支持。

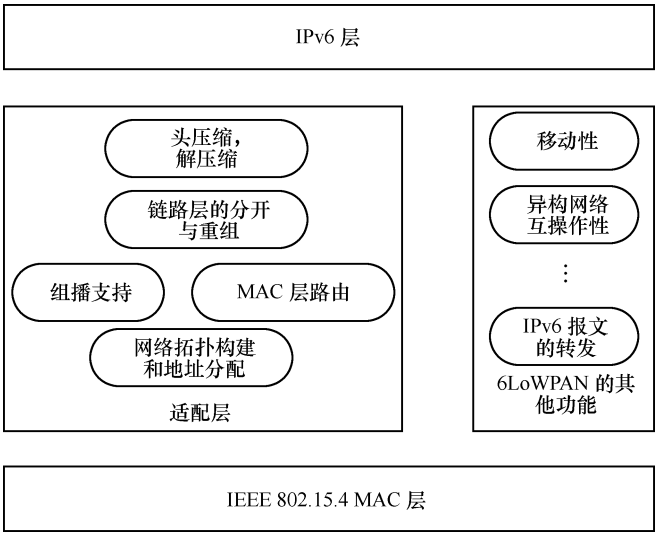


图 4-6　6LoWPAN 适配层的功能模块

4.2　M2M 接入方法

机器对机器通信（Machine-to-Machine Communication，简称 M2M）正伴随着第三代移动通信系统的运营成为中国电信产业发展的焦点。M2M 是基于特定行业终端，以公共无线网络为接入手段，为客户提供机器到机器的通信解决方案，满足客户对生产过程监控、指挥调度、远程数据采集和测量、远程诊断等方面的信息化需求。M2M 不是简单的数据在机器和机器之间的传输，更重要的是，它是机器和机器之间的一种智能化、交互式的通信，具有广泛的应用前景。目前 M2M 应用已经在我国电力、交通、智能家居、物流行业、企业安防以及金融等多个行业中均有相应应用，已被正式纳入国家《信息产业科技发展“十一五”规划及 2020 年中长期规划纲要》的重点扶持项目中。

物联网是把所有物品通过射频识别等信息传感设备与互联网连接起来，实现智能识别和管理，是继计算机、互联网与移动通信之后的又一次信息产业浪潮。从智慧地球到感知中国，无论物联网的概念如何扩展和延伸，其最基本的物物之间感知和通信是不可替代的关键技术。

M2M 技术是物联网实现的关键，是无线通信和信息技术的整合，用于双向通信，适用范围较广，可以结合 GSM/GPRS/UMTS 等远距离传输技术，同样也可以结合 Wi-Fi、Blue-Tooth、ZigBee、RFID 和 UWB 等近距离连接技术，应用在各种领域。

运营商角度定义：M2M 是基于特定行业终端，以 SMS/USSD/GPRS/CDMA 等为接入手段，为集团客户提供机器到机器的解决方案，满足客户会生产过程监控、指挥调度、远程数据采集和测量、远程诊断等当面的信息化需求。图 4-7 是 M2M 与物联网关系示意图。

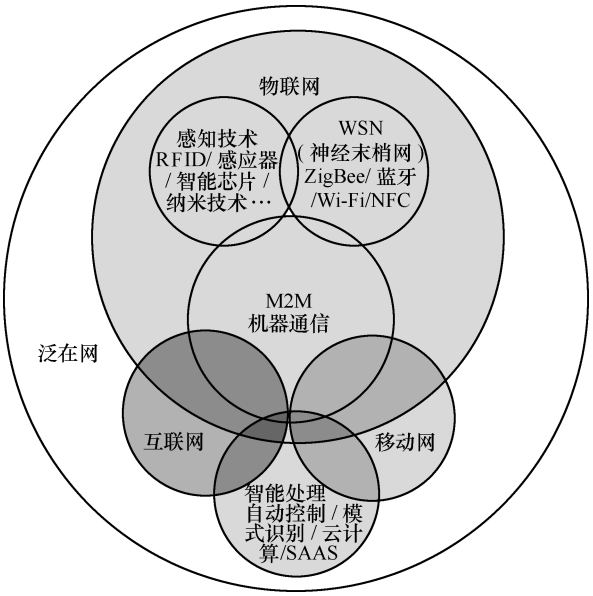


图 4-7　M2M 与物联网关系示意图

通过收集、电话、计算机、传真机等机器设备之间的通信来实现人与人的交流，这对我们来说是习以为常的。物联网是“网络一切”。机器与机器之间的对话成为切入物联网的关键。M2M 正是解决机器开口说话的关键技术，其宗旨是增强所有机器设备的通信和网络能力。但目前绝大多数的机器和传感器不具备本地或远程的通信和联网能力。机器的互连，通信方式的选择，数据的整合成为 M2M 技术的关键。

M2M 不是简单的数据在机器和机器之间的传输，更重要的是，它是机器和机器之间的一种智能化、交互式的通信。也就是说，即使人们没有实时发出信号，机器也会根据既定程序主动进行通信，并根据所得到的数据智能化地做出选择，对相关设备发出正确的指令。可以说，智能化、交互式成为了 M2M 有别于其他应用的典型特征，这一特征下的机器也被赋予了更多的“思想”和“智慧”。

随着我国社会经济的不断发展和市场竞争的日益深化，各行各业都希望通过加快自身信息化建设，提高工作效率，降低生产和运行成本，全面增强市场竞争力。M2M 技术综合了通信和网络技术，将遍布在人们日常生活中间的机器设备连接成网络，使这些设备变得更加“智能”，从而可以提供丰富的应用，给日常生活、工业生产等的方式带来新一轮的变革。在当今世界上，机器的数量至少是人的数量的 4 倍，因此 M2M 具有巨大的市场潜力，未来通信的主体将是 M2M 通信。由于无需布线，覆盖范围广，移动网络是 M2M 信息承载和传送最广泛、最有市场前景的技术。随着移动通信网络带宽的不断提高和终端的日益多样化，数据业务能力不断提高，这将促使 M2M 应用的发展进一步加快，有专家断言，在未来的 3G 时代，“机与机”产生的数据通信流量最终将超过“人与人”和“人与机”产生的通信流量。ITU 在描述未来业务时认为，NGN 应是一个电信级和企业级的全业务网，能满足新的通信需求，其中首次强调了要为大量的机器服务。而 M2M 与移动技术的结合，有可能带来杀手业务，促进 3G 和 NGN 的发展。一句话，M2M 是移动通信系统争夺的下一个的巨大市场。

在我国，工业网络化是工业化和信息化融合的大方向，工业控制需要实现智能化、远程化、实时化和自动化，M2M 正好填补这一缺口；同时，未来 LTE 网络建设带来的无线宽带突破，更为 M2M 服务的发展提供了更佳的承载基础——高数据传输速率、IP 网络支持、泛在移动性。3GPP（3rd Generation Partnership Project）作为移动通信网络及技术的国际标准化机构，从 2005 年就开始关注基于 GSM 及 UMTS 网络的 M2M 通信。传统的 3GPP 蜂窝通信系统主要以 H2H（Human to Human）应用作为目标进行优化，并对 VoIP、FTP、TCP、HTTP、流媒体等业务应用提供 QoS（Quality of Service）保障，而 M2M 的业务特征和 QoS 要求与 H2H 有明显差异，主要表现在低数据传输速率、低占空比、不同的延迟要求；从终端使用场景和分布的差异来看，传统蜂窝通信系统针对 H2H 终端的典型分布位置和密度进行优化，如手机的典型无线环境和单位面积内的数量，而 M2M 终端的使用环境和数量密度均与 H2H 有明显差异，主要表现为 M2M 网络部署的地理范围比传统手机网络更为广泛，在单位面积内，M2M 终端可能有“海量”的存在。正是因为以上差异，3GPP 专门发起了多个研究工作组，分别从网络、业务层面、接入网、核心网对 M2M 通信的网络模型、业务特征以及基于未来 3GPP 网络的 M2M 增强技术进行了系统的研究。

4.2.1 概述

4.2.1.1 M2M研究背景

M2M这个理念在20世纪90年代就出现了，但是仅仅停留在理论阶段。2000年以后，随着移动通信技术的发展，以移动通信技术实现机器设备的联网成为可能。2002年左右M2M业务就在市场上出现，并在随后的几年迅速发展成为了众多通信设备商和电信运营商的关注焦点。目前全球的机器数量远远地超过了人的数量，由此，我们可以预见M2M技术良好的市场前景。

目前国外尤其欧美地区发展M2M已经有六七年的时间，形成了比较成熟的产业链，并应用到了各行各业中。很多通信设备商、软件商、运营商从中受益，M2M已经成为通信产业新的增长点。其中运营商因为语音市场饱和，格外关注机器通信领域，据OVUM预测，到2010年M2M业务收入将占到电信运营商总收入的20%。

我国目前M2M市场才起步，以运营商推动为主，产业链存在很多空白，因此很有必要研究全球M2M市场的发展状况，以对我国M2M市场的发展进行更好的规划。

4.2.1.2 M2M的概念

M2M是一种通信理念，也是机器之间建立连接的所有技术和手段的总称。通信网络技术的出现和发展，给我们的社会生活面貌带来了翻天覆地的变化，人与人之间可以更加快捷地沟通，信息的交流更顺畅。但是到目前为止，除了计算机和其他一些IT设备外，很多普通机器设备几乎不具备联网和通信的能力，例如家用电器、各种交通运输工具、各种自动售货机、工厂的机器设备等。而M2M的核心目标就是使生活中所有的机器设备都具备联网和通信的能力。M2M技术具有非常重要的意义，有着广阔的市场前景，它正在推动着社会生产和生活方式的重大变革。与此同时，M2M不只是简单地远程测量，还具有远程控制功能，用户可以在读取远程数据的同时对其进行操控。M2M不只是人到机器设备的远程通信，而且还包括及机器与机器之间的通信和相互沟通，而反映到人的交互界面可能就只有一个结果。M2M不是一种新的技术，而是在现有的基础上的一种新的应用，很多应用比如远程测量和GPS已经存在了很多年，但近些年由于移动通信技术的发展才被加上M2M的名称。M2M不只是基于移动通信技术的，无线传感器网络RFID等短距离无线通信技术甚至有线网络都可以成为连接机器的手段。

4.2.1.3 M2M系统在物联网中的作用

M2M（Machine to Machine）是指机器（尤其是指传感器）之间建立连接的所有技术和手段的总称。而“物联网”是在“互联网概念”的基础上，将其用户端延伸和扩展到任何物品与物品之间，进行信息交换和通信的一种网络概念。其定义是：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。物联网的最底层末端传感器网络所采集的数据最终要传输到物联网的应用层，而M2M系统正好是跨越了物联网的应用层和感知层，完成了将感知层的数据经过融合处理后传输到物联网的应用层，起着承上启下、融会贯通的作用。

现阶段物联网的发展还处于初级阶段，M2M 由于跨越了物联网的应用层和感知层，是无线通信和信息技术的整合，它可用于双向通信，如远距离收集信息、设置参数和发送指令，因此 M2M 技术可以用于安全监测、远程医疗、货物跟踪、自动售货机等。因此，M2M 通信系统是目前物联网应用中一个重要的通信模式，是物联网中承上启下、融会贯通的平台，同时也是一种经济、可靠的组网方法。

4.2.1.4　M2M 业务运营碰到的主要问题

M2M 业务潜力巨大，运营商已经试验或者开展的 M2M 业务只是 M2M 应用的一小部分，可以说，M2M 业务仍处于起步阶段。因此，在看到 M2M 业务潜在巨大市场的同时，我们也看到了 M2M 业务发展存在的许多问题。

（1）缺乏完整的标准体系

由于国内目前尚未形成统一的 M2M 技术标准规范，甚至业界对 M2M 概念的理解也不尽相同，这将是 M2M 业务发展的最大障碍。目前，各个 M2M 业务提供商根据各行业的应用特点及用户需求，进行终端定制，这种模式造成终端难以大规模生产、成本较高、模块接口复杂。此外，不同的 M2M 终端之间进行通信，需要统一的通信协议，让不同行业的机器具有共同的“语言”，这些将是 M2M 的应用基础。

（2）商业模式不清晰，未形成共赢的规模化产业链

M2M 作为一项复杂的应用，涉及应用开发商、系统集成商、网络运营商、终端制造商及最终用户等各个环节，以及与人们生活相关的各个行业。目前，M2M 应用开发商数量众多，规模较小，且各自为战，针对具体业务的开发系统各不相同，开发成本较高；系统集成商只是针对具体某个行业进行系统提供，多个系统和多个行业之间很难进行互联互通；网络运营商正沦为提供通信的管道，客户黏性低、转网成本低，尚未发挥其在产业链中的主导地位作用 M2M 终端耦合度低，附加值低，同质化竞争严重；用户对 M2M 业务认识还比较模糊，由于 M2M 业务多数是以具体行业应用程序来命名，大多数用户对此类业务并不称其为 M2M 业务。可见，涉及 M2M 业务的各个环节不能很好地协调，还没建立一套完整的产业链，也没有形成成熟的商业模式。

4.2.2　M2M 对蜂窝系统的优化需求

由于 M2M 与 H2H（Human to Human）通信在一些方面（比如数据量、数据传输速率、延迟等）有着很大的差异，因此需要对现有的蜂窝系统进行优化来满足 M2M 的通信要求，具体原因如下：

1）业务特征的差异；

2）以往的蜂窝通信系统针对 H2H 业务进行优化，比如 VoIP、FTP、TCP、HTTP、流媒体等业务；

3）M2M 业务特征和 QoS 要求与 H2H 有明显的差异，比如低数据传输速率、低占空比、不同的延迟要求；

4）终端使用场景和分布差异；

5）以往的蜂窝通信系统针对 H2H 终端的典型分布位置和密度进行优化，比如手机的典型无线环境和单位面积内的数量；

6）M2M 终端的使用环境和数量密度与 H2H 有明显差异，比如传感器网络的使用地域

比手机更为广泛，在单位面积内 M2M 终端可能大量地存在。

4.2.2.1　增强网络能力

在网络层，3GPP 主要在 M2M 结构上做了改进来支持在网络中支持大规模的 M2M 设备部署 M2M 服务需求。

基于 MTC（Machine Type Communication，机器类型通信）设备和 MTC 服务器之间的端到端的应用使用的是 3GPP 系统提供的服务。3GPP 系统提供专门针对 MTC 优化的传输和通信服务，包括 3GPP 承载服务、IMS、SMS。如图 4-8 所示，MTC 设备通过 MTCu 接口连接到 3GPP 网络，如 UTRAN、E-UTRAN、GERAN、I-WLAN 等。MTC 设备通过由 PLMN 提供的 3GPP 承载服务、SMS 以及 IMS 与 MTC 服务器或者其他 MTC 设备进行通信。MTC 服务器是一个实体，它通过 MTCi/MTCsms 接口连接到 3GPP 网络，然后与 MTC 设备进行通信。另外 MTC 服务器这个实体可以在操作域内也可以在操作域之外。

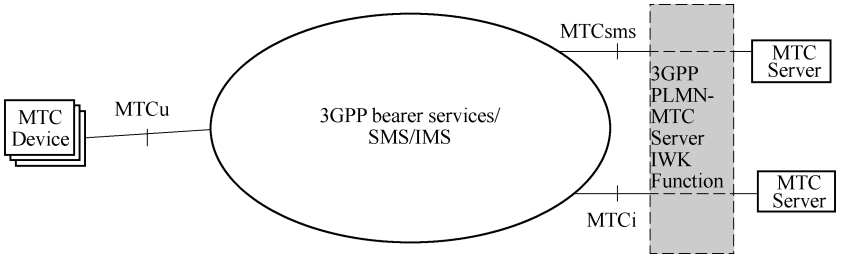


图 4-8　针对 MTC 的 3GPP 架构

图 4-8 中的接口定义如下：

1）MTCu：它是 MTC 设备接入 3GPP 网络的接口，完成用户层和控制层数据的传输。MTCu 接口可以基于 Uu、Um、Ww 和 LTE-Uu 接口来设计。

2）MTCi：它是 MTC 服务器接入 3GPP 网络的接口，并且通过 3GPP 的承载服务/IMS 来和 MTC 设备进行通信。它可以基于 Gi、Sgi 以及 Wi 接口来设计。

3）MTCsms：它是 MTC 服务器通过 3GPP 承载服务/SMS 接入 3GPP 网络的接口。

4.2.2.2　增强接入能力

1）研究各种 MTC 通信应用的典型业务流量特性，定义新的流量模型。

2）针对 SA1 工作组定义的 MTC 需求，研究对 UTRA 和 EUTRA 的改进。

3）研究针对大量的低功耗、低复杂度 MTC 设备的优化的 RAN 资源使用。

4）最大限度地重用当前的系统设计，尽可能减少修改，以限制 M2M 优化带来的额外成本和复杂度。

4.2.3　M2M 模型及系统架构

4.2.3.1　中国移动 M2M 模型及系统架构

1. M2M 系统结构图

M2M 系统分为 3 层，为应用层、网络传输层和设备终端层，如图 4-9 所示。应用层提供各种平台和用户界面以及数据的存储功能，应用层通过中间件与网络传输层相连，通过无线网络传输数据到设备终端。当机器设备有通信需求时，会通过通信模块和外部硬件发送数

据信号，通过通信网络传输到相应的 M2M 网关，然后进行业务分析和处理，最终到达用户界面，人们可以对数据进行读取，也可以远程操控机器设备。应用层的业务服务器也可以实现机器之间的互相通信，来完成总体的任务。

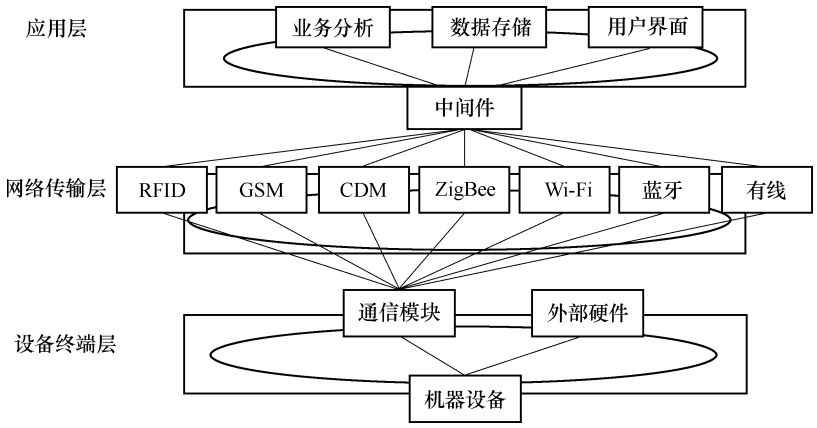


图 4-9　M2M 系统结构与技术体系

（1）设备终端层

设备终端层包括通信模块以及控制系统等。通信模块产品按照通信标准来分可分为移动通信模块、ZigBee 模块、WLAN 模块、RFID 模块、蓝牙模块、GPS 模块以及网络模块等，外部硬件包括从传感器收集数据的 I/O 设备、完成协议转换功能将数据发送到通信网络的连接、控制系统、传感器，以及调制解调器、天线、线缆等设备。设备终端层的作用是通过无线通信技术发送机器设备的数据到通信网络，最终传送服务器和用户。而用户可以通过通信网络传送控制指令到目标通信终端，然后通过控制系统对设备进行远程控制和操作。

（2）网络传输层

通信传输层即用来传输数据的通信网络。从技术上来分，通信网络包括：广域网（无线移动通信网络、卫星通信网络、Internet、公众电话网）、局域网（以太网、WLAN、Bluetooth）、个域网（ZigBee、传感器网络）等。

（3）应用层

应用层包括中间件、业务分析、数据存储、用户界面等部分。其中数据存储用来临时或者永久存储应用系统内部的数据，业务分析面向数据和应用，提供信息处理和决策，用户界面提供用户远程监测和管理的界面。

中间件包括两部分：M2M 网关、数据收集/集成部件。网关是 M2M 系统中的“翻译员”，它获取来自通信网络的数据，将数据传送给信息处理系统。主要的功能是完成不同的通信协议之间的转换。数据收集/集成部件是为了将数据变成有价值的信息，对原始数据进行不同加工和处理，并将结果呈献给需要这些信息的观察者和决策者。

2. 网元功能描述

M2M 业务系统结构图如图 4-10 所示。

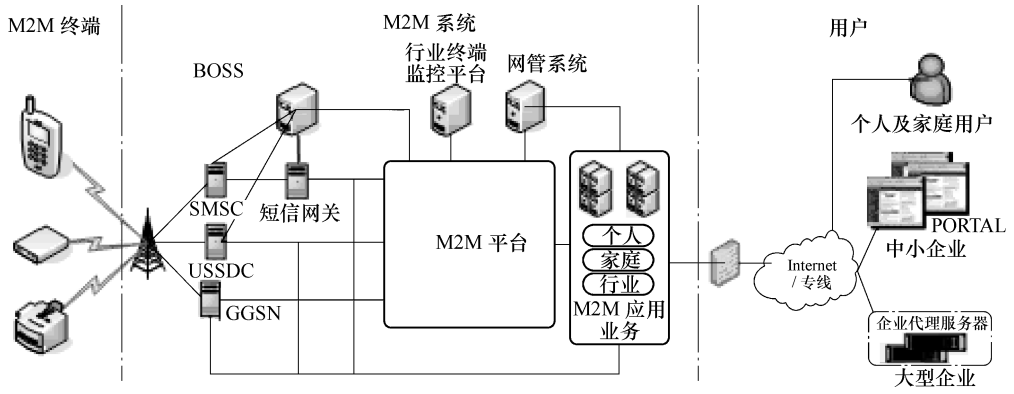


图 4-10　M2M 业务系统结构

M2M 终端：M2M 终端基于 WMMP 并具有以下功能：接收远程 M2M 平台激活指令、本地故障告警、数据通信、远程升级、数据统计以及端到端的通信交互功能。

M2M 平台：为 M2M 应用服务的客户提供统一的 M2M 终端管理、终端设备鉴权，并对目前短信网关尚未实现的接入方式进行鉴权。支持多种网络接入方式，提供标准化的接口使得数据传输简单直接。提供数据路由、监控，用户鉴权、计费等管理功能。

M2M 应用业务平台：为 M2M 应用服务客户提供各类 M2M 应用服务业务，由多个 M2M 应用业务平台构成，主要包括个人、家庭、行业三大类 M2M 应用业务平台。

短信网关：由行业应用网关或移动梦网网关组成，与短信中心等业务中心或业务网关连接，提供通信能力，负责短信等通信接续过程中的业务鉴权、设置黑白名单、EC/SI 签约关系/黑白名单导入。行业网关产生短信等通信原始使用话单，送给 BOSS 计费。

USSDC：负责建立 M2M 终端与 M2M 平台的 USSD 通信。

GGSN：负责建立 M2M 终端与 M2M 平台的 GPRS 通信，提供数据路由、地址分配及必要的网间安全机制。

BOSS：与短信网关、M2M 平台相连，完成客户管理、业务受理、计费结算和收费功能。对 EC/SI 提供的业务进行数据配置和管理，支持签约关系受理功能，支持通过 HTTP/FTP 接口与行业网关、M2M 平台、EC/SI 进行签约关系以及黑白名单等同步的功能。

行业终端监控平台：M2M 平台提供 FTP 目录，将每月统计文件存放在 FTP 目录，供行业终端监控平台下载，以同步 M2M 平台的终端管理数据。

网管系统：网管系统与平台网络管理模块通信，完成配置管理、性能管理、故障管理、安全管理及系统自身管理等功能。

4.2.3.2　ETSI 系统结构图

ETSI 的 M2M 功能结构主要是用来利用 IP 承载的基础网络（包括 3GPP、TISPAN 以及 3GPP2 系统）。同时 M2M 功能结构也支持特定的非 IP 服务（SMS、CSD 等）。M2M 系统结构包括 M2M 设备域和网络与应用域，如图 4-11 所示。

M2M 设备域由以下几部分组成。

1）M2M 设备：M2M 设备主要是利用 M2M 服务能力和网络域的功能函数来运行 M2M 应用。M2M 设备域到 M2M 核心网的连接方式主要有以下两种连接方式：

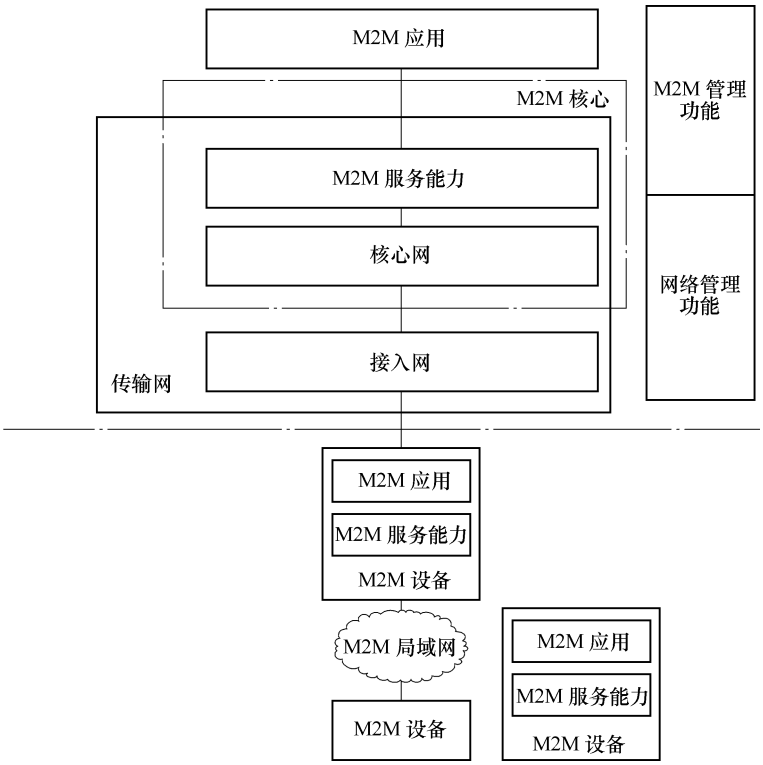


图 4-11　系统结构

① 直接连接：M2M 设备通过接入网连接到网络和应用域。M2M 设备主要执行以下几种过程，比如注册、鉴权、认证、管理、提供网络与应用域。M2M 设备还可以让其他对于网络与应用域不可见的设备连接到自己本身。

② 利用网关作为网络代理：M2M 设备通过 M2M 网关连接到网络与应用域。M2M 设备通过局域网的方式连接到 M2M 网关。这样 M2M 网关就是网络和应用域面向连接到它的 M2M 设备的一个代理。M2M 网关会执行一些过程，比如鉴权、认证、注册、管理以及代理连接到这个网关的 M2M 设备向网络与应用域提供服务。M2M 设备可以通过多个网关并联或者串联的方式连接到网络域。

2）M2M 局域网：可以通过 M2M 局域网让 M2M 设备连接到 M2M 网关。包括个人局域网（比如 IEEE 802.15x、ZigBee、蓝牙、IETF ROLL、ISA100.11a 等）、局域网（比如：PLC、M-BUS、Wireless MBUS 和 KNX）。

3）M2M 网关：M2M 网关主要作用是利用 M2M 服务能力来保证 M2M 设备连接到网络与应用域，而且 M2M 网关还可以运行 M2M 应用。

M2M 网络与应用域由以下几部分组成：

1）接入网：接入网允许 M2M 设备域与核心网通信。主要包括：xDSL、HFC、PLC、Satellite、GERAN、UTRAN、eUTRAN、W-LAN 和 WiMax。

2）传输网：允许在网络与应用域内传输数据。

3）M2M 核心：由核心网和服务能力组成。

① 核心网：主要提供以下服务。

- 以最低限度和其他潜在的连接方式进行 IP 连接；
- 服务和网络控制功能；
- 与其他网络的互联；
- 漫游。

不同的核心网可以提供不同的服务能力集合，比如有的核心网包括 3GPP CNS、ETSI TISPAN CN 和 3GPP2 CN。

② M2M 服务能力。

- 提供 M2M 功能函数，这些函数可以被不同的应用共享；
- 通过一系列的开放接口开放功能；
- 应用核心网功能。

4.2.4 核心网针对 M2M 的优化

（1）基于群组的优化

为了满足操作者的需求，M2M 设备可以以组为单位来进行管理控制。这种优化可以提供一种简单的模式来控制/升级/收费 M2M 设备，这种模式可以减少多余的信号来防止冲突。而且当 M2M 设备数目很大时，采用这种基于群组的优化策略可以节省大量的网络资源。M2M 设备的分组可以按照区域、按照设备特性以及设备的从属来划分，M2M 设备的分组方式是很灵活的。而且，每个 M2M 设备对于网络来说是可见的。

（2）M2M 设备与一个或者多个 M2M 服务器通信

M2M 订阅者允许一个或者多个 M2M 服务器通过公众陆地移动电话网（Public Land Mobile Network，PLMN）与 M2M 设备进行通信，这种通信方式经过优化用于 M2M 通信。为了使 M2M 设备和 M2M 服务器能够进行通信，需要满足以下要求：

1）M2M 订阅者可以利用 M2M 设备与一个或者多个 M2M 服务器进行通信。

2）PLMN 应该允许 M2M 设备和服务器进行交互，或者由 M2M 设备和 M2M 服务器发起会话。

3）在 M2M 设备与 M2M 服务器通信之前，PLMN 可以对 M2M 设备进行鉴权、认证。

4）可以唯一地标记 M2M 设备。

5）可以唯一地标记 M2M 设备组。

（3）IPv4 寻址技术

对于一些 M2M 应用来说，需要 M2M 服务器作为 M2M 设备域 M2M 服务器通信的发起者，但是由于 IPv4 地址空间有限，M2M 设备被分配了私有的非路由可达的 IPv4 地址，因此 M2M 设备对于 M2M 服务器是不可达的。

因此，系统应该提供一种机制，使得在公共地址空间的 M2M 服务器可以成功地发送消息给在私有 IPv4 地址空间的 M2M 设备，这个机制应该满足一下要求：

1）这种机制是可以升级的。

2）这种机制应该最小化由 MNO 和 M2M 使用者要求的配置。

3）这种机制应该最小化 M2M 服务器初始化 M2M 设备的所需的消息交互。

4）这种机制应该最小化其他额外的用户层面的潜在因素。

5）这种机制应该最小化任何对于 M2M 设备安全方面的威胁。

（4）在线少量数据传输

具有在线少量数据传输的 M2M 设备可以频繁地发送或者接收少量的数据。传输的数据量会根据每个 M2M 系统的不同而不同。对于少量在线数据传输，我们可以认为只要应用程序需要就可以随时传输。以下功能是在线少量数据传输所要求的：

1）当一个 M2M 设备连接或者被激活时，必须非常有效地进行少量数据传输。

2）少量数据传输的定义应该在每次业务订阅时进行配置。

（5）离线少量数据传输

具有离线少量数据传输功能的 M2M 设备可以不频繁地发送或者接受少量的数据。传输的数据量会根据每个 M2M 系统的不同而不同。对于离线少量数据传输，M2M 应用能够知道 M2M 设备是否可以通信以及进行少量数据传输，或者当设备不可以通信时，仍然可以传输数据。对于少量数据传输需要以下功能：

1）当一个 M2M 设备连接或者被激活时，必须非常有效地进行少量数据传输。

2）少量数据传输的定义应该在每次业务订阅时进行配置。

（6）低移动性

对于 M2M 的低移动性，有以下使用场景：

1）不频繁地移动，但是在很小的范围内移动，比如家庭健康监测。

2）不频繁地移动，但是在很大的范围内移动，比如移动销售终端。

3）不频繁地移动，在固定的位置，如水位、水温等的测量。

M2M 设备的低移动性会降低低移动性 M2M 设备的资源利用，节省大量的资源。

（7）M2M 订阅

M2M 的特征是由订阅来控制的，任何 M2M 特征的订阅的使用都是在订阅特征的时候被默认激活。同时，基于操作者的权限，也应该允许让 M2M 订阅者来激活未被订阅的 M2M 特性或者关闭已经订阅的 M2M 特性。这种激活/关闭机制已经超出了 3GPP 的范围。

关于 M2M 订阅，需要以下相关的要求：

1）M2M 解决方法应该能够向 PLMN 提供 M2M 订阅并且允许一个或者更多的 M2M 设备来共享这种订阅。

2）每个 M2M 设备都应该与一种 M2M 订阅相关联并且有一种设备订阅（包括用于鉴权的安全证书）。

3）一种 M2M 订阅需要表明被 M2M 设备订阅的特性共享这次订阅。

4）它应使全体 MTC 的设备共享同一 MTC 的订阅以使用所有已订阅的 MTC 的特点属于这个订阅。

（8）M2M 设备触发器

对于许多 M2M 应用来说，M2M 设备与服务器之间有一种数据轮询模型。这是因为每个 M2M 用户都想控制与 M2M 的通信并且不允许 M2M 设备来随机接入 M2M 服务器。另外，在一些应用场合，M2M 设备启动时，M2M 服务器可能偶尔需要从 M2M 设备轮询数据。对于那些不是经常连接到网络的 M2M 的设备来说，基于服务器触发指示，来触发 M2M 设备附加或者建立一个 PDP/PDN 连接是非常有利的。为了触发 M2M 设备需要满足以下要求：

1）PLMN 应该能够触发 M2M 设备来发起与服务器的通信，这次通信是基于服务器触发

指示的。

2）M2M 设备应该可以接收网络的触发指示而且只接收到触发指示时可以建立与 M2M 的服务器的通信。

（9）M2M 监视

M2M 设备可能会被部署到高风险的地区，比如被破坏的可能性或者通行模块被盗窃。对于那些 M2M 设备，网络最好可以监测和报告那些可能的事件（包括位置信息），比如破坏或者盗窃通信模块。为了满足 M2M 监视，必须满足以下要求：

1）尽量让用户配置监视的活动，比如，监测 M2M 设备与 UICC(Universal Integrated Circuit Card，通用集成电路卡）的联系，M2M 功能的错位，附着点的变化，连接的断开等。

2）M2M 用户可以配置网络将要执行的动作。

3）网络可以检测到监视的事件。

4）网络可以向 M2M 用户或者 M2M 服务器报告监视的活动。

5）可以配置在连接的实际最大损失和 M2M 订阅的探测之间的最大时间。

4.2.5　M2M 的通信管道

4.2.5.1　基于蜂窝移动通信

如图 4-12 所示，在这种通信管道中，终端包括 M2M 设备或者网关需要安装 SIM 卡模块，这样可以将 M2M 应用服务器和网络连接起来。主要利用现有的移动电信网完成 M2M 的数据传输，当然在现有的蜂窝移动通信网中会设有特定的接口供 M2M 传输使用。

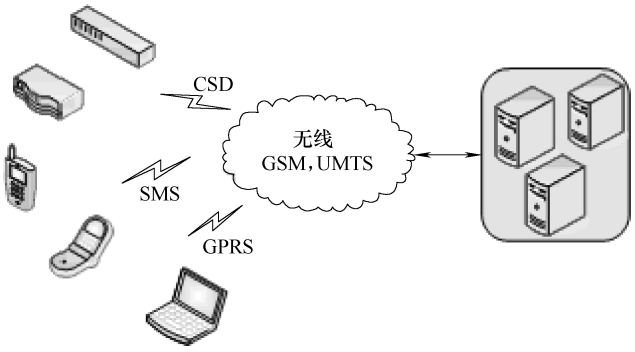


图 4-12　M2M 基于蜂窝移动通信管道

4.2.5.2　基于其他无线技术

这些通信技术包括卫星通信、IEEE 802.11x、蓝牙、ZigBee（IEEE 802.15）、RFID 等无线通信技术，这些技术主要是完成无线传感器网络的部署，然后让无线传感器网络作为 M2M 重要的补充接入方式。

无线传感器网络的国际标准具有的特征：

1）基于 IEEE 802.15.4 的低速 WPAN 技术。

2）868MHz/2.4GHz。

3）具有低功耗、低成本、近距离等特点。

4）支持 star、tree、mesh 等组网方式。

5）已有量产成熟的芯片。

国内标准特点有：

1）CWPAN 标准组已经和 IEEE 802.15.4c 融合并正式批准为 IEEE 802.15.4-2009。

2）工作在 780MHz 的中国频段。

4.2.6　核心网对 M2M 业务的支持优化

4.2.6.1　设备标识资源

现在 H2H 终端采用 IMEI、IMSI、MSISDN、IPv4 地址作为设备标识的资源，以 IMSI 为例，IMSI 号码为 15 位，由 3 位 MCC 国家码、3 位 MNC 网络标识码、9 位设备标识码组成。其资源对于 H2H 终端应该是足够的，全球的手机用户包括各类软终端目前还远不到 10 亿用户。但如果资源与 M2M 终端共用，就非常紧张。据预测，M2M 终端在未来将是 H2H 终端的 5～10 倍，如此庞大的数量采用现有的资源肯定是远远不够的。

MTC（Machine Type Communication，机器类型通信）设备标识应能唯一标识一个 M2M 终端，可采用 IMSI、MSISDN、IP addr、IMPU/IMPI 等。随着 M2M 应用日益广泛，设备标识资源短缺问题必将日益突出，国际各标准组织（如 ITU、3GPP）也在积极寻求解决方案，设备标识资源不足的问题对核心网的影响需要引起足够的关注。

4.2.6.2　核心网负荷

当大量终端比较集中地接入网络时，对无线、核心网都将构成比较大的负荷，拥塞难免会发生，也会增加人与人之间通信的故障率。

核心网负荷包括控制面负荷与媒体面负荷，可以想象，当大规模的 M2M 设备同时接入到核心网，同时发送数据到 M2M 应用平台，核心网会遭受非常大的负荷冲击。一方面，核心网的移动性管理网元需要同时处理终端的接入控制，频繁进行附着、激活、业务请求、创建承载等信令交互，会造成控制面负荷过载的发生。同时，当数据交互同时发生时，大量的 M2M 终端通过核心网的媒体网关与同一个远程服务器进行数据通信，这就可能造成媒体网关数据拥塞，特别是媒体网关到远程服务器的 IP 通道会造成数据阻塞，引起媒体面过载的发生。

举例来说，当长江水位上涨到警戒水位时，大量水位监控器会向长江防洪指挥中心的远程服务器发送监控数据，部分检测点可能还会上传实时图像，这类突发的接入与数据传输是 M2M 应用的特点之一，这对核心网的信令面与媒体面的负荷冲击是瞬间的，对核心网通信的可靠性及健壮性造成相当大的影响，需要从技术层面规避这种瞬间负荷对网络的冲击。

目前标准组织也提出了一些方案，如采用随机数接入机制，采用定时接入机制，对组内最大负荷进行限制等方法等来减小瞬间负荷对核心网的冲击。

4.2.6.3　核心网安全

随着 M2M 终端的日益增多，M2M 终端通信安全问题也引起了各运营商的重视。对于 MTC 系统优化的通信安全性应不低于非 MTC 通信的安全性，如端到端连接安全、组认证安全等。M2M 通信安全是多方面的，有终端接入鉴权安全、端到端通信安全、数据安全等多方面。在终端接入鉴权安全方面，需要防止 M2M 终端接入认证信息被恶意盗用，如 H2H 终端盗用 M2M 终端的 USIM 接入到核心网，影响与远程 MTC 服务器的数据通信安全。

端到端通信链路安全方面，现有的机制很多，如采用类似 VPN 的机制建立 IPsec 隧道等方式。在归属域，M2M 终端与 MTC 服务器之间的端到端安全通过归属网络信任域进行保证，但当 M2M 终端漫游到其他运营商的网络时，M2M 终端与 MTC 服务器通过运营商网络的非信任域进行通信，端到端安全无法保证，需要制定相应的安全机制。

4.2.6.4　终端管理和计费

MTC 上下文中的标识需要扩展，网络同时还需要识别 M2M 设备组的标识。可采用 OMA DM 的机制对 M2M 终端进行远程管理，远程更新软件，配置 M2M 终端的初始化参数等。MTC 计费需要进行优化，避免大规模 M2M 终端进行数据通信产生的 CDR 对网络的冲击。计费可以考虑按组进行计费，为属于同一组的 M2M 设备提供更简单的计费机制，或采用某种策略不生成设备的计费话单等各类灵活的计费方式。

针对 M2M 终端多样化的特点，对 M2M 终端也进行必要的分类，并针对不同类型进行优化。M2M 终端主要类型可分为低移动性、低数据量、监控类、时间控制类、组管理类等。对于低移动性与低数据量类设备，需要提高网络资源利用率，降低对设备的移动性管理；对于监控类设备，需要网络对各类监控时间实现实时监控，若发现异常事件需要及时汇报给用户及管理后台，同时对设备进行一定的网络接入限制措施；对于组管理类，需要进一步优化组计费、组管理、组策略等组优化方案。

4.2.6.5　其他方面

M2M 不同的应用对核心网都有特定的需求，如在测量监控的应用中，需要对测量设备进行实时控制，在现有网络中因 IPv4 地址限制原因，采用 NAT 进行内外网地址转换，将导致实时控制的时间延迟问题。

一些 M2M 应用中，M2M 终端可能安装在无人值守的区域，如森林防火、水位监控、空气质量检测类终端，网络需要为这类终端提供防盗检测，一旦发现终端异常移动，网络需要对这类终端进行必要的限制，并及时通知到远程服务器及用户进行异常处理。

对于一个高可用性的场景，如动物监控、儿童走失监控、煤气监控、楼宇监控等，需要终端是低耗能设备，对核心网而言，可能需要提供低耗电移动性控制策略，如延长 Paging、TAU 时间等措施，保证 M2M 终端的电池使用时间持久。

4.2.7　WMMP 通信协议概述

WMMP（Wireless M2M Protocol）是为实现 M2M 业务中 M2M 终端与 M2M 平台之间、M2M 终端之间、M2M 平台与 M2M 应用平台之间的数据通信过程而设计的应用层协议，主要作用是为了实现推进机器通信协议统一，降低运营成本的目的，其体系如图 4-13 所示。

WMMP 由 M2M 平台与 M2M 终端接口协议（WMMP-T）和 M2M 平台与 M2M 应用接口协议（WMMP-A）两部分协议组成。WMMP-T 完成 M2M 平台与 M2M 终端之间的数据通信，以及 M2M 终端之间借助 M2M 平台转发、路由所实现的端到端数据通信。WMMP-A 完成 M2M 平台与 M2M 应用之间的数据通信，以及 M2M 终端与 M2M 应用之间借助 M2M 平台转发、路由所实现的端到端数据通信。

WMMP 的功能架构如图 4-14 所示。WMMP 的核心是其可扩展的协议栈及报文结构，而在其外层是由 WMMP 核心衍生的与通信机制无关的接入方式和安全机制。在此基础之上，由内向外依次为 WMMP 的 M2M 终端管理功能和 WMMP 的 M2M 应用扩展功能。

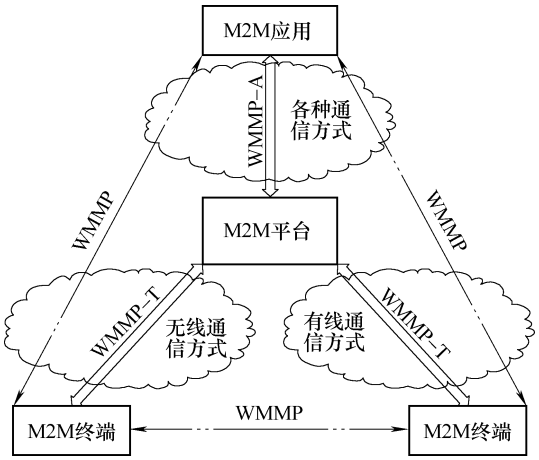


图 4-13　WMMP 体系

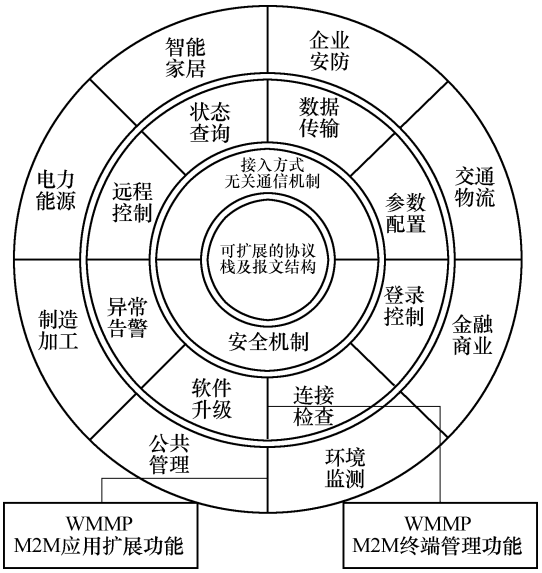


图 4-14　WMMP 的功能架构

在上图中 WMMP 的终端管理功能包括异常警告、软件升级、连接检查、登录控制、参数配置、数据传输、状态查询、远程控制。WMMP 应用扩展功能包括智能家居、企业安防、交通物流、金融商业、环境监测、公共管理、制造加工、电力能源等行业应用。

WMMP 对用户的价值体现在：

1）满足无人值守机器终端的基本管理需求，提供电信级的终端管理能力。

2）通过扩展协议的方式满足行业用户差异化的需求，提供 WebService 接口，降低应用开发难度。

3）提供了端到端通信的服务保障能力，有效提高业务质量。

4）提供了业务快速开发和规模运营的基础，降低用户业务使用成本。

基本功能：提供端到端电信级机器通信、终端管理、业务安全等基本功能。

扩展功能：屏蔽了不同行业之间的差异，通过扩展协议即可满足行业用户差异化需求。

M2M 平台与应用系统接口协议是 WMMP 的一部分（WMMP-A），它对 M2M 平台与终端的接口规范进行了封装，对应用系统提供了对 M2M 终端进行监控管理的能力。同时，通过本协议，M2M 终端与 M2M 应用之间可以通过 M2M 平台传递业务流程，实现定制化的 M2M 应用。

（1）基本协议

双方的消息交互采用 SOAP（Simple Object Access Protocol，简单对象访问协议）接口。这是一个可以运行在任何传输协议上的轻量级协议，它包含 3 个方面：XML-envelop 为描述信息内容和如何处理内容定义了框架；将程序对象编码成为 XML 对象的规则；执行远程调用（Remote Procedure Call，RPC）的约定。

（2）接口描述

本协议支持两种连接方式：

1）基于 HTTP 的标准 WEB Service 方式。应用系统和 M2M 平台采用 WSDL（Web Serv-

ices Description Language）来对接口进行描述。WSDL是用来定义Web服务的属性以及如何调用它的一种XML。一个完整的WSDL服务描述是由一个服务接口和一个服务实现文档组成的。通过查阅Web服务的WSDL文档，开发者可以知道Web提供了哪些方法和如何用正确的参数调用它们。因为WSDL包含了对服务接口的完整描述，所以我们可以使用它来创建能简化服务访问的存根，该存根为一段Java代码（假设使用Java），它自动生成了访问Web服务的类。如果我们需要访问Web服务，只需调用该类中对应的方法即可，而不用在客户端程序中再写入配置信息。要求通信双方作为Web Service服务端时，应实现HTTP会话的超时机制。即一定时间内，如果客户端没有新的HTTP请求，则服务端主动断开连接。会话维持的时间要求可配置。

2）长连接。应用系统可以选择采用长连接和M2M平台交互，以提高效率。消息格式的定义和Web Service方式一致。

（3）消息格式

所有的协议数据单元（PDU）由如下表的消息头和消息体组成：

PDU组成	描　　述
Message Header	消息头
Message BODY	消息体
Message HASH	消息摘要，计算方法为： MD5［消息头+3DES（消息体）+用户名+密码］

消息头和消息体在xml中的表现形式如下：

```
<? xml version = "1.0" encoding = "UTF-8"? >
< MsgName >
< Head >
< Attribute1 > 消息头属性一 </Attribute1 >
< Attribute2 > 消息头属性二 </Attribute2 >
< Attribute3 > 消息头属性三 </Attribute3 >
</Head >
< BODY > 加密后的消息体 </BODY >
< HASH > 消息摘要 </HASH >
</MsgName >
```

未加密的消息体也是一个完整的xml文件，如下例所示：

```
<? xml version = "1.0"? >
< BODY >
< Attribute1 > 消息体属性一 </Attribute1 >
< Attribute2 > 消息体属性二 </Attribute2 >
< Attribute3 > 消息体属性三 </Attribute3 >
</BODY >
< HASH > 消息摘要 </HASH >
```

本规范报文为文本格式，对于二进制内容，应进行 BASE64 编码。

加密后的消息体通过 BASE64 编码放入 BODY 标签。

（4）消息的安全性

1）数据安全。

本规范采用 3DES 算法对数据进行加密。M2M 平台与应用之间的交互消息均要求携带摘要字段，算法如下：MD5[消息头 +3DES(消息体) + 用户名 + 密码]。

其中用户名和密码由 M2M 平台为应用分配，应用发往 M2M 平台的消息以及 M2M 平台发往应用的消息，均要求用上述算法计算摘要。

应用系统和 M2M 平台的交互包含两种密钥：

① 基础密钥，不同的 M2M 应用系统由 M2M 平台分配不同的基础密钥；M2M 平台负责统一分配和保存所有的 M2M 应用系统密钥。M2M 应用系统的密钥通过 Email 的方式由 M2M 平台发送给各 M2M 应用系统。

② 会话密钥，应用系统与 M2M 平台的每次会话均由 M2M 平台分配会话密钥。一次会话只允许持续一定的时间，如果超出该时间，应用系统必须重新登录，分配新的会话密钥。否则 M2M 平台将拒绝应用系统的消息。

基础密钥用于应用向平台登录启动新会话时加密消息体，以及 M2M 平台返回会话密钥时用于加密消息体。应用系统需要先在 M2M 平台登录，登录消息包含 M2M 平台分配的用户名和密码，并用基础密钥加密（3DES 算法）。M2M 平台为本次会话分配会话密钥，并用基础密钥加密后返回给应用系统。然后在会话中，双方用会话密钥加密和解密消息体。

消息交互流程如图 4-15 所示。

应用系统首先通过 TAppLoginReq 在 M2M 平台进行登录，由 M2M 平台分配并返回会话密钥。在后续的消息交互的数据包中，双方通过会话密钥加密消息体。

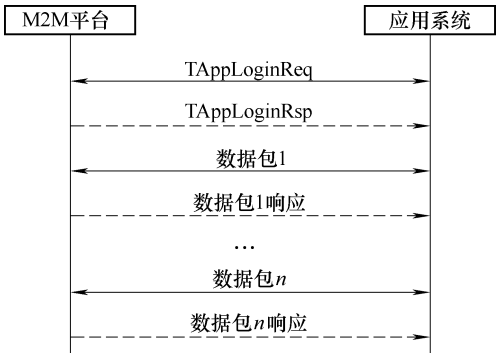


图 4-15　消息交互流程

2）网络安全。

M2M 平台接口采用如下的手段保证和 M2M 应用系统之间通信的网络安全：IP 鉴权及业务 ID 控制列表。

① M2M 应用系统接入 M2M 平台时需提供其业务系统出访 IP 和 URL（根据其业务特性确定）。

② M2M 平台为 M2M 应用系统的每一个业务分配一个全局唯一的业务 ID。

③ M2M 平台侧防火墙配置安全策略，只有有效的 IP 和业务 ID 才能够访问 M2M 平台。

④ M2M 应用系统端配置相应策略，以拒绝非 M2M 平台的接口调用。

⑤ 建议 M2M 应用系统和 M2M 平台之间采用 VPN 通道。

4.2.8　M2M 技术的发展趋势

（1）移动通信技术将成为主流，短距离通信技术将成为补充

移动通信可以实现全球的设备监控和联网，是实现 M2M 最理想的方式，目前也已经有

不少的基于移动通信的 M2M 业务。但可以预见到在未来的几年移动通信模块成本和网络建设费用仍然居高不下，为每一台机器或者每一个物品配备移动通信的模块仍不现实。在这种情况下，短距离通信将成为扩展移动通信 M2M 的重要手段，尤其在一些特定的应用中。RFID、无线传感器等短距离通信技术与移动通信网络的无缝连接将成为未来 M2M 应用的重要趋势，这也为网络融合以及“网络一切”理念创造了机遇。RFID、蓝牙可以直接与移动通信模块连接，也可以通过无线传感器网络连接到移动通信模块，如图 4-16 所示。同时，也不排除有新的专门针对 M2M 应用的通信技术产生，能代替现有的各有优点或者缺点的技术。而有线网络和 Wi-Fi 技术由于其高速率和高稳定性的优势，将在一些特殊的领域继续存在。

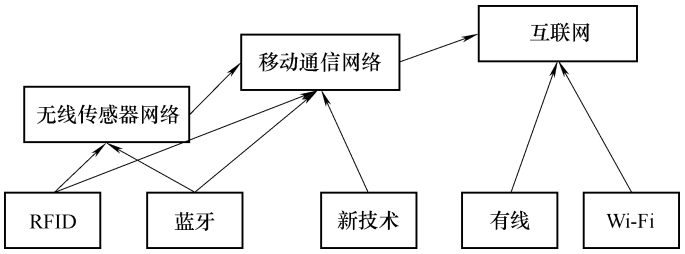


图 4-16　未来 M2M 技术结构

（2）无线通信技术和 M2M 产业的发展将推动 M2M 标准化

M2M 行业数据标准制定目前已经有初步的成果，虽然影响力还不大。随着 M2M 产业链的整合以及 M2M 业务领域的不断扩大，相信 M2M 的数据标准、体系结构标准、设备接口标准、安全标准、测试标准将不断地完善和融合，最终形成统一的标准体系。届时，整个标准体系不止包括移动通信 M2M，还将包括短距离通信技术及应用。

（3）无线升级通信终端软件将成为提高经营效率的重要手段

随着 M2M 通信终端和模块的大规模应用，通信终端软件升级将成为困扰 M2M 服务提供商的一个难题。标准化以后，当需要业务更新的时候通常只要更新通信模块的软件和应用设备软件即可，应用设备和服务器一般集中在 M2M 服务提供商和运营商那里，更新很容易，但通信模块和终端的软件升级则需要派遣专业人员提供现场支持，当终端分布在很大的区域内或者数目众多的时候，就会严重降低经营效率。DOTA（Download Over The Air，空中下载）和 FOTA（Firmware Over The Air，空中存储）技术目前已经在手机中实现了广泛的应用，Ovum 预测，未来的两年手机 FOTA 软件将迅速发展。M2M 通信对 FOTA 技术需求比手机应用更强烈，因此虽然目前这项技术在 M2M 领域还涉及比较少，但相信随着 M2M 产业的发展，越来越多的 M2M 厂商会注重这项技术在 M2M 中的作用。

4.2.9　M2M 应用前景

4.2.9.1　视频监控

（1）视频监控 M2M 应用概述

安全防范监控系统是通过传输设备传输视频信号，并从摄像到图像显示和记录构成独立完整的系统。它能实时、形象、真实地反映被监控对象，不但极大地延长了人眼的观察距离，而且扩大了人眼的机能，它可以在恶劣的环境下代替人工进行长时间监视，让人能够看到被监视现场实际发生的一切情况，并通过录像机记录下来。同时报警系统设备对非法入侵进行报警，产生的报警信号输入报警主机，报警主机触发监控系统录像并记录。

安全防范适合于监控网点分散、数量多的大型监控项目，需要建立集中管理模式的监控

项目，需要整合 PC 式、嵌入式主机，以及网络视频服务器的网络监控项目。需要实现多用户、多部门、多级别的权限控制的监控项目。需要简化网络监控操作的项目，监控中心需要组建电视墙、进行报警集中管理的项目，前端网点无人值守、需要通过网络集中监控的项目。需要进行集中存储及流媒体转发功能的项目应用领域：金融行业（各银行网点、信用社、邮政储蓄的远程集中联网监控）、公安、交通系统（城市道路监控、高速路监控、城市治安联防监控、“数字城管”“平安城市”监控系统）、教育系统（考场监控、校园保安监控、远程教学等）、油田、煤矿系统（油井、输油管道、矿井的远程集中联网监控）、电信、水利、电力行业（机房、无人值守基站的联网监控）、跨省市的大型企、事业单位、连锁经营店铺等，娱乐商业场所（歌舞厅、网吧、酒吧、夜总会）以及军队、医院等。

移动视频监控作为目前最重要的视频监控类业务应用，它利用高带宽的无线接入，支持在任一地点上传现场图像、在任一位置接收远方图像，并和固定网视频监控系统融合实现监控在时间、地点等方面的全覆盖。移动视频监控是一种具有高端和差异化特色的典型 3G 多媒体应用，可广泛服务于应急指挥、公交监控、家庭监控、公共多媒体服务等领域，从而在原有监控系统的基础上扩大视频监控的应用环境和使用方式，给用户更友好、更便捷、更贴身的业务体验。

在我国，电信运营商从 2004 年开始进入安全监控领域，现在已处于一个快速发展期。目前中国电信推出的视频监控业务品牌是“全球眼”，中国联通推出的品牌是“宽视界”和“神眼”（原中国网通建设，现统一划入中国联通）。另外，中国移动、中国联通也已建设了少量的移动视频监控系统。随着运营商的重组完成和 3G 牌照的发放，中国电信、中国移动和中国联通已全部成为固定网 + 移动 3G 的全业务运营商，视频监控系统将以固定网和移动融合为主题快速建设，业务也将得到迅速发展。

（2）视频监控 M2M 应用方案

安全防护中的最重要的应用就是视频监控业务，电信运营商通过构建视频监控业务运营系统，即可开展相关的业务和应用。因此，视频监控业务应该具备固定网移动融合、可运营、可管理、可运维、高可靠性、开放性和标准化等特点。

视频监控系统应该充分考虑电信级平台架构、新业务功能支持、大容量组网、综合网管、电信级存储、系统和运营安全等方面的内容。系统基于 NGN 体系，采用模块化结构设计，提供电信级的可运营系统，可提供面向不同客户群、固定网和移动融合的多样化视频监控应用。

同时，系统应该支持不同用户之间的交叉访问，实现不同行业用户的按需访问；具备开放性和扩展性，可引入产业链内的不同厂家，共同丰富业务应用、促进业务发展；通过统一的运维支撑平台，可提高运维效率、降低运维成本。整个系统具备电信级可靠性和安全，可承载用户不断增长的业务需求。

视频监控主要有 3 种技术：模拟视频监控技术、数字视频监控技术和网络视频监控技术。

1）在模拟视频监控系统中，图像的传输、交换以及存储均基于模拟信号处理技术。模拟视频监控在图像还原效果方面具有一定优势，但是，传输距离有限、工程布线复杂、信号易受干扰、应用不灵活、无法集中管理等缺陷限制其只适合于提供末端接入。

2）数字视频监控引入了先进的数字信号处理技术，利用 MPEG-4、H. 264 等高效视频编码技术，监控图像能够以较低的带宽占用实现在各类现有数字传输网上的远距离传输。但是其体现的主要是信号处理技术上的变革，不涉及体系结构。这导致目前的数字视频监控系统在组网方式上千差万别，且无法互通。

3）网络视频监控以数字信号处理为基础，通过参考并借鉴先进、成熟的通信网体系架构，采用网络化的方式实现信号的传输、交换、控制、录像存储以及点播回放，并通过设立强大的中心业务平台，实现对系统内所有编解码设备及录像存储设备的统一管理与集中控制。网络视频监控体现的不仅仅是技术的革新，更重要的是架构的革新。

随着技术的发展以及市场需求进一步趋广，视频监控市场正快速发展，传统的模拟监控市场逐步萎缩，而数字监控逐步成为主流，网络监控稳步增长。网络视频监控的出现弥补了模拟和数字视频监控的不足，利用 TCP/IP 网络，实现了远程监控和低成本扩展监控范围，使得视频监控可以向很多领域渗透。网络化将是视频监控市场重要的发展趋势。

伴随着 3G 移动网络技术的飞速发展，无线视频监控已进入飞速发展的时代。3G 的启动将促使安防监控从 PC 的有线视频监控走向手机的无线视频监控，通过手机实现远程视频监控将成为网络视频监控的主流。无线视频监控将成为 3G 业务的“杀手级”应用。用户可通过 3G 手机对监控区域进行监控。同时，3G 监控前端具备专业的无线远程监控功能，当出现盗贼入侵、意外失火或是煤气泄漏等状况，它会根据指令把报警信息、或拍摄到的实时视频画面发送到用户手机上，让用户及时获悉并做出处理。同时，利用高带宽的 3G 网络作为承载，可以接入安防系统中的摄像头等设备，将视频、音频信息通过 3G 网络传送到控制平台，并由控制平台做进一步的分析和处理。

4. 2. 9. 2　智能交通

（1）智能交通 M2M 应用概述

在现代城市的发展过程中，交通问题越来越引起人们的关注。随着城市车辆的增加，人、车、路三者关系的协调，已成为交通管理部门所面临的重要问题。城市道路的畅通，采用有效的控制措施，最大限度地提高道路的使用效率是城市道路交通控制的重要内容。

智能交通是指采用电子计算机技术、电子技术和现代通信技术，使车辆和道路智能化，以实现安全快速的道路交通环境，从而达到缓解道路交通拥堵、减少交通事故、节约交通能源、减轻驾驶疲劳的目的。

20 世纪 60 年代末，美国开始智能交通方面的研究，之后，欧洲、日本等也相继加入这一行列。经过 30 多年的发展，美国、欧洲、日本成为世界智能交通研究的三大基地。事实证明，智能交通可以大幅度提高交通网络的运行效率，是解决交通拥挤最经济有效的办法。它蕴涵着巨大的社会与经济效益，是目前世界各国交通领域竞相研究和开发的热点。

（2）智能交通 M2M 应用方案

一个典型的智能交通系统如图 4-17 所示，系统分为 GPS/GLONASS 卫星定位系统、移动车载终端、无线网络和 ITS 控制中心组成。

车载终端由控制器模块、GPS 模块、无线模块及视频图像处理设备等组成，控制器模块通过 RS232 接口与 GPS 模块、无线模块、视频图像处理设备相连。

车载终端通过 GPS 模块接收导航卫星网络的测距信息，将车辆的经度、纬度、速度、

时间等信息传给微控制器；通过视频图像设备采集车辆状态信息。

微控制器通过 GPS 模块与监控中心进行双向的信息交互，完成相应的功能。

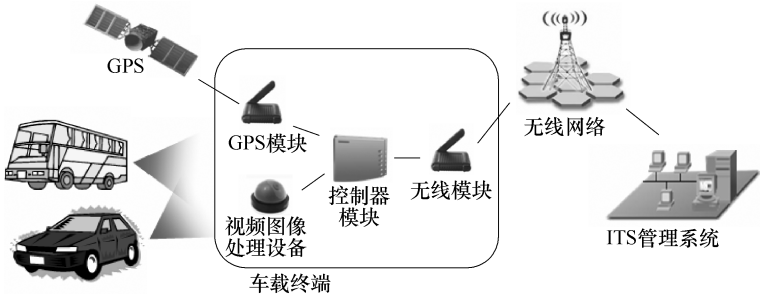


图 4-17　典型智能交通系统

一个完整的智能交通系统可以具体分为如下部分：

1）数据采集部分——负责采集位置及视频数据；

2）传输部分——传输数据的通道；

3）ITS 管理平台。

4.3　全 IP 融合与 IPv6 以及 IPv9

IP 规定了计算机在因特网上进行通信时应当遵守的规则，计算机系统只要遵守 IP 就可以与因特网互联互通，正因为有了 IP，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。网络大融合已成为当今世界电信发展的一大主题，无论是固定网还是移动网，核心网还是接入网都在朝这个大方向发展，而 IP 技术是其中采用的首选技术。全 IP 网络是一种非常有前景的物联网接入方案，通过全 IP 无缝集成物联网和其他各种接入方式，诸如宽带、移动因特网和现有的无线系统，将其都集成到 IP 层中，从而通过一种网络基础设施提供所有通信服务，这样将带来诸多好处，如节省网络成本，增强网络的可扩展性和灵活性，提高网络运作效率，创造新的收入机会等。

目前，全 IP 过渡问题的研究正在进行之中，通信设备制造商、运营商都卷入到了这股热潮之中，它已成为下一阶段通信技术发展的主要研究方向之一。全 IP 网络架构的物联网集智能传感网、智能控制网、智能安全网的特性于一体，真正做到将识别、定位、跟踪、监控、管理等智能化融合，从而也更易于将所有需实现远程互操作的人和物直接连到现有网络诸如国际互联网上，从而从中找到商业模式，引发新的经济生长点。

随着全球经济和信息化浪潮的持续发展，下一步，世界上所有的人，以及万物都可能融入到这个网络化的世界中，形成更为广阔的数字化海洋。可以预见的是，未来网络化的技术如果仍然是 IP，那么下一代网络所容纳的巨大节点数量，将远远超越现有 IPv4 地址空间容量，因此，这个网络化的世界的引擎将要升级到下一代互联网技术——以 IPv6 地址为基础标识的 IP 网络技术。在 IPv6 巨大容量的包容下，世界上人人都可拥有全球唯一的地址，实现更为公平的普遍通信服务，使得家庭、城市以及地球上的万物将可以逐步数字化和 IP 化，融入到这个新的网络中来，城市以及人类生活变得高度智能化。

与之相应，物联网作为“物物相连的互联网”，真要把物和物连接起来，除了需要这样

那样的传感器，首先要给它们每个都贴上一个标签，也就是每个物品都有个自己的 IP 地址，这样用户才可以通过网络访问物体。但是目前的 IPv4 受制于资源空间耗竭，已经无法提供更多的 IP 地址，而 IPv6 可以让人们拥有几乎无限大的地址空间，这使得全世界的人使用的手机、家电、汽车甚至鞋子等上网都成为可能，这样就能构筑一个人人有 IP、物物都联网的物联网世界。因此，IPv6 技术是物联网底层技术条件的基础，没有 IPv6 物联网就无从谈起。

对于物联网而言，无论是远程通信，还是近距离通信，为了满足 IP 地址需求量的空前提升，都必须尽快过渡到 IPv6。物联网的远程通信需求，将推动现有移动或者固定网络向 IPv6 的商用化演进。物联网应用，主要以公众无线网络为载体，大多使用 2G、3G 网络来实现远程通信，同时也有部分应用采用了固定光纤接入方式，根据不同的应用场景选择不同的接入方式。而现有的 2G、3G 网络，分组域核心网设备 GGSN/PDSN 均需要尽快升级支持给终端分配 IPv6 地址，同时分组域核心网设备与骨干承载网络之间需要尽快实现 IPv6 组网和路由。对于固定接入方式而言，接入路由器和骨干及城域承载网络也需要尽快完成向 IPv6 的升级，以满足快速业务接入的要求。

在近距离通信领域，主流技术也开始支持 IPv6。常用的近距离无线通信技术有 IEEE 802.11b、IEEE 802.15.4（ZigBee）、Bluetooth、UWB、RFID、IrDA 等。其中，ZigBee 作为一种近距离、低复杂度、低功耗、低数据传输速率、低成本的双向无线通信技术，完整的协议栈只有 32KB，可以嵌入各种设备中，同时支持地理定位功能，因而成为构建近距离无线传感网的主流技术。当前，ZigBee 已在其智能电网的最新标准规范中加入了对 IPv6 协议的支持。

精简 IPv6 适配于物联网是当前面临的主要问题，作为下一代网络协议，IPv6 凭借着丰富的地址资源以及支持动态路由机制等优势，能够满足物联网对通信网络在地址、网络自组织以及扩展性等诸多方面的要求。然而，在物联网中应用 IPv6，并不能简单地“拿来就用”，而是需要进行一次适配。

IPv6 不能够直接应用到传感器设备中，而是需要对 IPv6 协议栈和路由机制进行相应的精简，以满足对网络低功耗、低存储容量和低传送速率的要求。由于 IPv6 协议栈过于庞大复杂，并不匹配物联网中互联对象，尤其是智能小物体的特点，因此虽然 IPv6 可为每一个传感器分配一个独立的 IP 地址，但传感器网需要和外网之间进行一次转换，起到 IP 地址压缩和简化翻译的功能。

目前，相关标准化组织已开始积极推动精简 IPv6 协议栈的工作。例如，IETF 已成立了 6LowPAN 和 RoLL 两个工作组进行相关技术标准的研究工作。相比较传统方式，能支持更大的节点组网，但对传感器节点功耗、存储、处理器能力要求更高，因而成本要更高。另外，目前基于 IEEE 802.15.4 的网络射频芯片还有待进一步的开发来支持精简 IPv6 协议栈。

总体上，物联网应用 IPv6 可按照“三步走”策略来实施。首先，承载网支持 IPv6；其次，智能终端、网关逐步应用 IPv6；最后，智能小物体（传感器节点）逐步应用 IPv6。目前，一些网络设备商的产品，包括骨干和接入路由器、移动网络分组域设备等，已经可以完全满足第一和第二阶段商用部署的要求，同时他们在积极跟踪第三阶段智能小物体应用 IPv6 的要求，包括技术标准和商用产品两大领域。我们有理由相信，在 IPv6 的积极适配与

广泛应用下，物联网产业有望实现真正的大繁荣。

IPv6 协议的引入使得大量、多样化的终端更容易接入 IP 网，并在安全性和终端移动性方面都有了很大的增强。基于 IPv6 的物联网，可以在 IP 层上对数据包进行高强度的安全处理，使用 AH 报头、ESP 报头来保护 IP 通信安全，其安全机制更加完善；同时，终端移动性也更有利于监测物品的实时位置。从而，IPv6 将促进物联网向着更便捷、更安全的方向发展，IPv6 技术使大量、多样化的终端更容易接入 IP 网，并在安全性和终端移动性方面都有了很大的增强，其应用必将促进物联网向着更便捷、更安全的方向发展。

IPv6 虽然号称“能给世界上的每粒沙子分配地址”，但地址资源掌握在他国手中，我国实际能分得的地址数量尚未可知。事实上，IPv4 虽然可以为网络分配约 42 亿个 IP 地址，但美国占据了地址总量的 74%，而我国分到使用权的地址数不到美国公开地址的 10%。

目前尚有另一种 IP 演进策略即 IPv9，IPv9 协议是指 0 ~ 9 阿拉伯数字网络作虚拟 IP 地址，并将十进制作为文本的表示方法，即一种便于找到网上用户的使用方法；为提高效率和方便终端用户，其中有一部分地址可直接作域名使用；同时，由于采用了将原有计算机网、有线广播电视网和电信网的业务进行分类编码，因此，又称“新一代安全可靠信息综合网协议”。IPv4 和 IPv6 都采用十六进制技术，而 IPv9 采用十进制技术，能分配的地址量是 IPv6 的 8 倍。IPv9 协议的主要特点：

1）采用了定长不定位的方法，可以减少网络开销，就像电话一样可以不定长使用。

2）采用特定的加密机制。加密算法控制权掌握在我国手中，因此网络特别安全。

3）采用了绝对码类和长流码的 TCP/ID/IP，解决声音和图像在分组交换电路传输的矛盾。

4）可以直接将 IP 地址当成域名使用，特别适合 E164，用于手机和家庭上网。

5）有紧急类别可以解决在战争和国家紧急情况下的线路畅通。

6）由于实现点对点线路，因此对用户的隐私权加强了。

7）特别适合无线网络传输。

虽然 IPv9 设计一种具有全新报头结构的互联网通信协议，但当前问题在于这种全新协议不能与现有网络兼容，IPv9 迟迟不能大量部署，耗资巨大，很大一部分原因也在于此。

参 考 文 献

[1] Zach Shelby, Carsten Bormann. 6LoWPAN: The Wireless Embedded Internet [M]. 1st ed United Kingdom: Wiley, 2009.

[2] Rajeev S. Koodli, Charles E. Perkins. Mobile Inter-Networking with IPv6 1st ed. New Jersey: Wiley, 2007.

[3] 孙燚. 6LoWPAN 无线传感器网络与 BACnet 网络的集成技术研究 [D]. 重庆：重庆大学, 2009.

[4] 李堃. 基于 6LoWPAN 的 IPv6 无线传感器网络的研究与实现 [D]. 南京：南京航空航天大学, 2008.

[5] 中国通信标准化协会. 移动 M2M 业务研究报告. 2009.

[6] 工业和信息化部电信研究院, M2M 业务应用市场研究, 2009.

[7] 十进制网络工作组. ICS 35. 100. 70：数字域名规范 [Z]. http：//202. 38. 64. 40/ ~ syang/ IPv9/

[8] 张永晖, 蒋新华, 林漳希. IPv6 与 IPv9 的比较 [J]. 计算机工程, 2006, 32(4)：116-118.

[9] ETSI TS 102690 V <0. 62 > (2010-07). Machine-to-Machine Communications (M2M)：Functional Architecture.

[10] Jean-Philippe Vassear, Interconnecting smart Objects with IP [M]. 1st ed. MA：Morgan Kanfmann. 2010.

第 5 章　传输层——承载网技术

物联网的到来，其大规模信息交互与无线传输为主的特点，使物联网成为各种资源需求的大户。数据传输需要网络，现今我们已经拥有完备的通信网络设施，在物联网时代我们可以借助通信网的现有设施，再针对物联网的特性加以一定的优化和改造就可以为物联网所用。所以，如何将现在存在的各种网络与物联网结合起来是一个十分重要的问题。

由于物联网和通信网有着很显著的差别，所以物联网的承载如何与通信网结合是一个需要重点考虑的问题。物联网发展对目前通信网形成新的挑战。

首先，物联网的业务规模是移动通信业无法比拟的。据美国研究机构 Forrester 预测，到 2020 年物物互联业务与现有人与人的通信互联比例将达 30∶1，即可能从 60 亿人口扩展 500 亿乃至上万亿的机器和物体。因此，当物联网正式实现，有超过 500 亿以上的终端需要通过无线方式连接在一起，其对各种网络资源的需求，尤其是对网络容量和带宽的需求将大大超越通信网已有的设计与承载能力。

有专家分析，物联网的应用目前一般是小流量的 M2M 应用。比如路灯管理、水质监测等，所需要传输的数据量很小，原有的 2G/3G 网络就可以实现对这些数据量的支撑；还有人认为，目前物联网涉及的控制、计费、支付，实际上都不会占用大量带宽，目前有充足的资源支撑建设物联网。但是，应该看到，随着物联网的发展，在不远的将来，物联网将会出现有大量占用高带宽的应用。以物联网的视频应用为例，视频感知是物联网的一个典型应用。就目前而言，就已经存在了不少这样的例子：如远程专家诊断、远程医疗培训已经成为智慧医疗应用的一个必然组成部分；在智能电网中，输电线路远程视频监控系统、电网抢修视频采集和调度指挥；在智慧城市中，几乎所有的城市都可以看到城市视频安全监管等。比如平安城市中公共交通等以视频图像为主的监控业务。而物联网的信息传输中，视频传输要求是最高的，也是占用频谱最多的业务。以北京的公交系统视频监控业务为例，目前北京市有 3 万多辆公交车，如果每辆公交车上面布设 4 个摄像头，则 3 万辆公交车的数据总量预计将达到约 180Gbit/s，而且对图像的连续性和实时性有较高要求。未来将会有更多的大数据量和高带宽要求的业务涌现。所以其传输的带宽需求绝不是目前的通信网可以轻松承载的。

其次，移动蜂窝网络着重考虑用户数量，而物联网数据流量具有突发特性，可能会造成大量用户堆积在热点区域，引发网络拥塞或者是资源分配不平衡的问题。这些都会造成物联网的需求方式和规划方式有别于已有通信网通信。

第三，目前，通信网络是针对人与人通信设计的，它对不同用户申请的语音业务可以进行设置，从而进行控制并保障其质量；而物联网业务主要是数据业务，物联网业务在网络传输中只有有权和无权之分。而对于有权用户，其用户等级是相同的，网络只对信息进行尽力而为的处理。因此，网络不能针对物联网业务特性进行有效的识别和控制，而且当大量物联网终端接入后，网络的效率也将大幅降低。

因此，物联网的发展必然造成对通信网的巨大压力和挑战。

5.1　物联网承载网发展阶段

利用通信网络进行物联网信息承载时，根据物联网的特性，可以分为3个不同的阶段。

混同承载阶段：在物联网发展初期，业务量不是特别大的情况下，由于现有网络不能区分人与人的通信、物与物的通信，直接采用现有网络承载物联网业务，不需要对网络做大的改动，主要通过终端侧的配置以及对终端的管理，缓解网络的压力。

区别承载阶段：当物联网发展到一定阶段，物联网应用规模的增加对网络资源（如号码资源、传输资源）造成较大压力，这时需要对网络进行部分改造，使得网络侧能够区别物与物的通信还是人与人的通信，并且针对不同情况采取不同策略，缓解网络压力，保障业务质量。

独立承载阶段：在物联网业务规模化后，物联网大量的数据信息传输将成为一个重点考虑的因素。如果完全按照之前的传输模式在现有的传输系统中传输将产生与其他通信相互干扰的问题。此时应该考虑到物联网独有的特性，对网络做出必要的改变，使得网络能够适应物联网信息的传输。

5.2　物联网当前的混同承载

当前正处于物联网发展初期，业务量不是特别大的情况下，直接采用现有网络承载物联网业务，不需要对网络做大的改动。在混同承载阶段，互联网和物联网的共同点是技术基础是相同的，不管是互联网还是物联网最后都会基于一个分组数据。但是两者的承载网和业务网是分离的。由于互联网和物联网对于网络的要求不同，而且各自的网络组织形态和功能要求也不一样，物联网系统需要很高的实时性、安全可信性、资源保证性等，这些和互联网有很大的差别。

5.2.1　物联网业务对承载网的要求

我们可以了解到，各种不同的物联网业务对QoS要求也不相同（见表5-1）。

表5-1　各种不同的物联网业务对QoS要求

	时　延	误 码 率	上行传输速率
数据采集类业务	不敏感	高	不高
会话类业务	敏感	不高	高
交互类业务	敏感	高	不高
流媒体类业务	不敏感	高	高

而不同的承载网络所能够提供的业务能力也是各不相同，我们可以针对不同类型的业务选择不同的网络进行承载，见表5-2。

表 5-2　不同承载网络的技术指标

	EDGE	TD-SCDMA	WLAN
下行理论传输速率/(bit/s)	473k	2.8M(HSDPA)	11M(IEEE 802.11b)
下行传输速率/(bit/s)	100～150k	1～1.6M（HSDPA）	600k～1M
上行传输速率	30～40k	60k 左右	600k～1M
时延	较长	一般	一般
误码率	同环境有关	同环境有关	较好

目前，EDGE（Enhanced Data Rate for GSM Evolution，增强型数据速率 GSM 演进技术）网络覆盖率较高，可以作为目前的物联网承载网络。

WLAN 的特点是传输速率较高，但它的覆盖面不广，移动性也不好，所以适用范围相对较窄。

5.2.2　3G + WLAN 是目前承载物联网的较佳模式

WLAN 要承担起物联网传输与承载的重任必然面临许多新的挑战。

首先，WLAN 要实现技术创新。一方面，WLAN 要向更高传输速率演进，IEEE 802.11n 的 320Mbit/s 传输速率是必需的要求，业界甚至提出在 60GHz 频段实现 7Gbit/s 的传输速率的设想。另一方面，实现 WLAN 技术的升级，在天线技术、服务质量（QoS）保障技术、多点传播软件技术以及无线信号收发技术方面不断改进，进一步提高可靠性和传输质量。

对 WLAN 的第二个挑战是频谱资源的紧缺。按照预测，我国到 2020 年，在设定的小区内 150 人同时使用 WLAN，其传输速率为 200kbit/s，每用户忙时呼叫次数为 0.15，每户平均呼叫时长为 3000s 的情况下，上下行共需 2516MHz 频率。而 WLAN 用于物联网，在一个小区内的物品或设备数量可能远远多于 150 个，而且在承载某些视频业务时其实时在线的比例更高，频谱需求也将超过 2516MHz，成为名副其实的用频“大户”。而我国至今在非授权的 2.4GHz 和 5.8GHz 频段为 WLAN 分配了 208.5MHz 频率，与到 2020 年 WLAN 人与人通信所需频率尚存巨大缺口，如果加上物联网的频谱需求，其频率缺口更大。

对 WLAN 的挑战之三是安全隐患。由于 WLAN 使用非授权频谱，特别是目前的 2.4GHz 频段，集中了大量无线电业务，WLAN 要与点对点或点对多点扩频微波系统、蓝牙、RFID、无绳电话，甚至微波炉共享频谱，而没有频率保护的规定。试验证明，无绳电话、蓝牙设备，特别是微波炉对 WLAN 的干扰最大，常使 WLAN 数据传输出现丢码、错码，不但传输速率下降，严重时甚至中断几秒及数分钟，当然 QoS 保证也无从谈起。

如果单纯以 3G 广域网实现局域物联网的承载与传输，将对 3G 传输网的带宽和控制形成较大压力；而凭借 WLAN 在局域范围内实现对异构传感网数据的汇聚、处理与传输，将发挥 WLAN 传输速率高、组网结构简单、建设方便快捷等特点，会使物联网用户获得高速、方便与丰富的使用体验。在广域感知阶段，会产生一些基于无线传感器网络技术的公共节点，这些公共节点作为物联网基础设施的基本组成部分，必然要实现广域管理，这时 3G/4G 将发挥其广域网的统一协议、寻址、鉴权、认证等优势。但是，要实现无线传感器网络公共节点，WLAN 是不可或缺的环节。

3G + WLAN 的出现是为 3G 人与人的通信而设计和存在的，但其特有的组网模式却可在

物联网的承载与传输中大显优势。在 WLAN 技术演进和逐步解决频谱需求的过程中，物联网无疑为 3G + WLAN 的发展增添了新动力。

5.2.3　TD-SCDMA 为物联网发展加速

物联网业务以上行流量为主，而目前中国移动 EDGE 最大上行带宽仅为 60kbit/s，限制了视频传输高频数据采集类的大带宽应用。TD-SCDMA 是我国具有自主知识产权的第三代移动通信技术，第三代移动通信无法延续 2G 以语音为业务核心的发展模式，其业务重点将转向数据业务和互联网业务。TD-SCDMA 上行传输速率达到 128kbit/s，TD-SCDMA 作为物联网承载平台，有很大的发展空间。它可以为我们的农业、共有监控、公共安全、城市管理、远程医疗、智能家具、智能交通，环境检测等方面服务。

在煤炭行业的应用包括瓦斯的传感器、通风的传感器、电力监控的传感器，通过 TD 的网络和地下的工业网络，提供综合管理平台，为地层的勘测，为煤炭行业的安全方面，包括提高工业效率方面提供全面的解决方案。传感器在煤炭方面的应用，在中国物联网应用里处于领先的地位，目前超过 50 种类型，超过 1000 个应用规模。

服务于智能城市的解决方案，包括电子商务、购物导引、智能监控、信息采集等，通过传感器和 TD 网络，后台的管理系统，形成一体化的解决方案。

TD 推动物联网发展，不仅体现在提高生产效率方面，也体现在提高人民的生活水平上。我国在推动物联网的过程中，更应该重视自己国家的核心技术，更应该重视标准化工作。在今后如果可以推动 TD 技术和物联网在重点行业和领域的广泛应用，包括能源、交通、智慧城市、民生服务等重点行业和领域，就会与供应商、制造商形成共赢的局面。

5.3　物联网未来的区别承载

当物联网发展到一定阶段，物联网应用规模的增加对网络资源（如号码资源、传输资源）造成较大压力，这时需要对网络进行部分改造，物联网承载网进入区别承载阶段。LTE 网络是可以提供高达百兆 bit/s 以上的带宽，支持更多的用户，传输速率目前可以与家庭的宽带相媲美。LTE 同时作为新一代的无线宽带业务和现在的 3G 相比在网络优势和成本上有很大的优势。所以在区别承载阶段，LTE、LTE-A、光通信等网络通过部分改造，可以承载物联网不同类型的业务，并可以全面兼容其他业务，给用户提供更多的选择。

5.3.1　LTE 与物联网

5.3.1.1　LTE 简介

LTE 是为适应时代需求而提出的新的移动宽带接入标准，为此 3GPP 规定了 LTE 系统的各项技术指标并引入了多项核心新技术。LTE（Long Term Evolution）项目是 3GPP 对通用移动通信系统（UMTS）技术的长期演进，始于 2004 年 3GPP 的多伦多会议。

LTE 并非人们普遍误解的 4G 技术，而是 3G 与 4G 技术之间的一个过渡，是 3.9G 的全球标准，与 3G 相比，LTE 具有如下技术特征：

1）通信速率有了提高，下行峰值传输速率为 100Mbit/s、上行为 50Mbit/s。

2）频谱效率提高了：下行链路 5（bit/s）/Hz，（3～4 倍于 R6 版本的 HSDPA）；上行链

路2.5（bit/s）/Hz。

3）以分组域业务为主要目标，系统在整体架构上将基于分组交换。

4）QoS保证：通过系统设计和严格的QoS机制，保证实时业务（如VoIP）的服务质量。

5）系统部署灵活，能够支持1.25~20MHz的多种系统带宽，并支持“paired”和“unpaired”的频谱分配，保证了将来在系统部署上的灵活性。

6）降低无线网络时延。

7）增加了小区边界传输速率，在保持目前基站位置不变的情况下增加小区边界传输速率。

8）强调向下兼容，支持已有的3G系统和非3GPP规范系统的协同运作。

LTE技术也分为TDD-LTE和FDD-LTE两种。

LTE系统引入的核心新技术总结如下。

（1）OFDM/OFDMA

LTE中的传输技术采用OFDM技术，其原理是将高速数据流通过串/并变换，分配到传输速率较低的若干个相互正交的子信道中进行并行传输。由于每个子信道中的符号周期会相对增加，因此可以减小由无线信道的多径时延扩展产生的时间弥散性对系统造成的影响。

LTE规定了下行采用OFDMA，上行采用SC-FDMA的多址方案，这保证了使用不同频谱资源用户间的正交性。LTE系统对OFDM子载波的调度方式也更加灵活，具有集中式和分布式两种，并灵活地在这两种方式间相互转化。上行除了采用这种调度机制之外，还可以采用竞争（Contention）机制。

（2）MIMO

MIMO技术是提高系统传输速率的主要手段，LTE系统分别支持适应于宏小区、微小区、热点等各种环境的MIMO技术。基本的MIMO模型是下行2×2，上行1×2天线阵列，LTE发展后期会支持4×4的天线配置。目前，下行MIMO模式包括波束成形、发射分集和空间复用，这3种模式适用于不同的信噪比条件并可以相互转化。波束成形和发射分集适用于信噪比条件不高的场景中，用于小区边缘用户有利于提高小区的覆盖范围；空间复用模式适用于信噪比较高的场景中，用于提高用户的峰值传输速率。在空间复用模式中同时发射的码流数量最大可达4；空间复用模式还包括SU-MIMO（单用户）和MU-MIMO（多用户），两种模式之间的切换由eNodeB决定。上行MIMO模式中根据是否需要eNodeB的反馈信息，分别设置开环或闭环的传输模式。

（3）E-MBMS

3GPP提出的广播组播业务不仅实现了网络资源的共享，还提高了空中接口资源的利用率。LTE系统的增强型广播组播业务（Enhanced Multimedia Broadcast/Multicast Service，E-MBMS）不仅实现了纯文本低传输速率的消息类组播和广播，更重要的是实现了高速多媒体业务的组播和广播。为此，对UTRA做出了相应的改动：增加了广播组播业务中心网元（BM-SC），主要负责建立、控制核心网中的MBMS的传输承载，MBMS传输的调度和传送，向终端设备提供业务通知；定义了相关逻辑信道用于支持E-MBMS。

从业务模式上，MBMS定义了两种模式，即广播模式和组播模式。这两种模式在业务需求上不同，导致其业务建立的流程也不同。

5.3.1.2　物联网技术与 LTE 技术的结合

现在移动通信网是覆盖面积最广阔的通信网，如果能够实现物联网和移动通信网的融合，那么物与物之间的通信将成为现实。如果给每一个物都贴上一个标签，还有遍布各地的读写器，物与物之间通信的容量非常大，现有的 GSM 和 3G 通信技术都不足以提供这么大的通信容量，采用频谱效率非常高的 LTE 技术是解决这个问题的一个方案。

LTE 技术可以在 20MHz 频谱带宽上提供下行 100Mbit/s、上行 50Mbit/s 的峰值传输速率，具有非常高的频谱效率。在组网方面，以 LTE 为代表的 4G 能够真正实现无线接入技术(包括局域网、无线局域网、家用局域网和自组织网络等)，移动网络和有线宽带技术的融合，使得 LTE 系统能够真正提供“无所不在”的服务。

未来物联网通信主体的数量将是人的数量的百倍以上，目前的 IPv4 地址濒临耗尽，而 IPv6 在地址空间上大大增加，可以满足物联网应用对 IP 地址日益增长的需求。IPv4 实现的只是人机对话，而 IPv6 则扩展到任意事物之间的对话，它不仅可以为人类服务，还将服务于众多硬件设备，如家用电器、传感器、远程照相机和汽车等。IPv6 为物联网的应用提供了充足的地址资源，而 LTE 系统又支持 IPv6 协议，可以允许容纳足够多的终端。

5.3.1.3　采用 LTE 技术的物联网体系结构

物联网技术采用以 LTE 为代表的 4G 移动通信技术作为承载网是未来的发展趋势。图 5-1给出了一种基于 LTE 技术的物联网体系结构，该体系结构主要包括 3 个部分：国家传感信息中心、LTE 核心传输网和综合接入网。

国家传感信息中心，也叫“感知中国”中心，包括 ONS 服务器、EPC-IS 服务器和内部中间件。由于标签中只存储了产品的 EPC，计算机需要一些将 EPC 匹配到相应产品信息的方法。ONS 服务器就是一个物联网的名称解析服务器，被用来定位物联网对应的 EPC-IS 服务器。EPC-IS 服务器就是一种物联网信息发布服务器，提供了一个模块化、可扩展的数据和服务接口，使得相关数据可以在企业内部和企业之间共享。EPC-IS 服务器主要包括客户端模块、数据存储模块和数据查询模块 3 个部分。内部的中间件负责提供一个服务器与 LTE 核心网的接口，收集 EPC 数据，还可以集成防火墙的功能。大型企业也可以建立自己的 EPC-IS 服务器。

LTE 核心传输网主要负责数据的可靠传输，和原有的物联网架构中的互联网作用类似，主要包括基站和移动管理实体两部分。移动管理实体中的网关设备适合将多种接入手段整合起来，统一接入到电信网络的关键设备，网关可满足局部区域短距离通信的接入需求，实现与公共网络的连接，同时完成转发控制信令交换和编解码等功能，而终端管理安全认证等功能保证了物联网业务的质量和安全。

综合接入网部分支持不同的终端接入。图 5-1 中 LTE 收发信机只提供收信息和发信息的功能，应用模式和图 2-1 的物联网 EPC 系统工作示意图相同。综合接入网可以把无线传感器网络直接通过具有读写器、中间件功能的智能站接入 LTE 系统，此智能站可以收集所辖范围内的标签数据和传感器数据。也可以把读写器、中间件直接集成到 LTE 手机里，现在手机已经非常普及，如果手机都具有读写器功能，可以大大增加收集标签的地域范围。还可以通过手机、笔记本电脑等各种终端进行查询和更新 EPC-IS 服务器产品信息。

目前的物联网和 LTE 系统尚处于初级阶段，在成本标准和规模化方面还有待完善。LTE

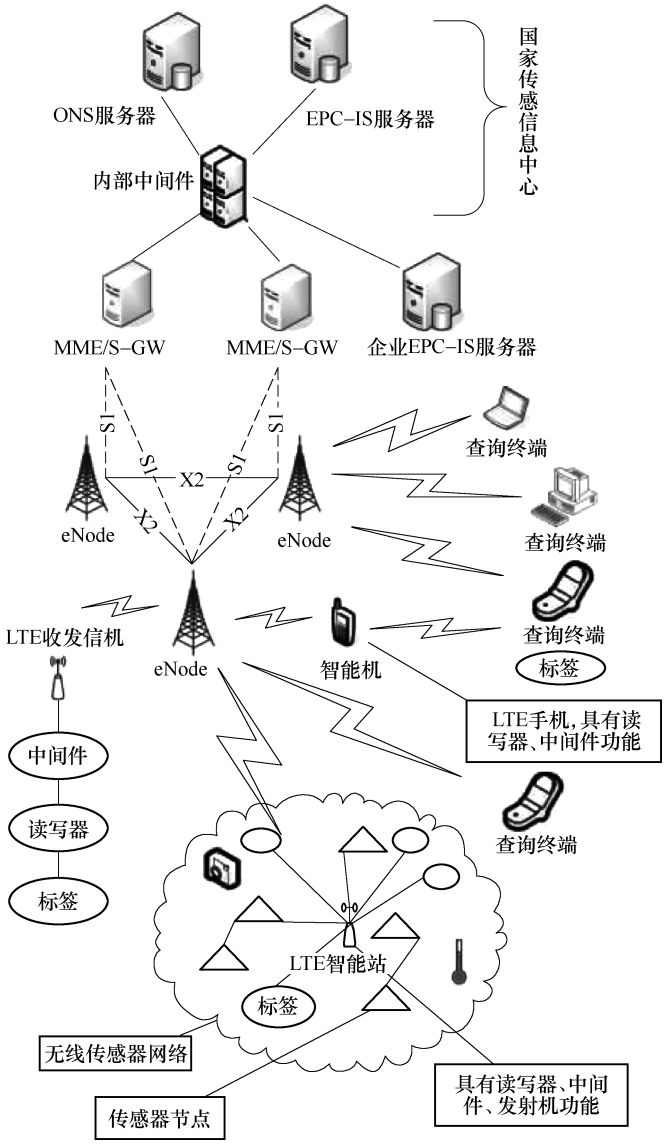


图5-1　基于LTE系统的物联网架构

可以成为物联网背后的有力技术支撑，更高速的网络带宽使得所有局部细小的传感器网络能够有机联系在一起，其传输的数据有文本语音及视频等多种形式的选择，LTE网络的建成让互联网从技术角度不再受限，可以根据各行业间的不同要求孵化出适合的行业终端和应用。移动通信网与物联网的结合，将极大地延伸传统通信业的领域，使人与人的通信延伸到物与物的通信、人与物的通信。

5.3.2　LTE-A与物联网

5.3.2.1　LTE-A简介

LTE-A是LTE-Advanced的简称，是LTE技术的后续演进。LTE俗称3.9G，这说明

LTE 的技术指标已经与 4G 非常接近了。LTE 与 4G 相比较，除最大带宽、上行峰值传输速率两个指标略低于 4G 要求外，其他技术指标都已经达到了 4G 标准的要求。而将 LTE 正式带入 4G 的 LTE-A 的技术整体设计则远超过了 4G 的最小需求。在 2008 年 6 月，3GPP 完成了 LTE-A 的技术需求报告，提出了 LTE-A 的最小需求：下行峰值传输速率为 1Gbit，上行峰值传输速率 500Mbit，上下行峰值频谱利用率分别达到 15Mbit/Hz 和 30Mbit/Hz。这些参数已经远高于 ITU 的最小技术需求指标，具有明显的优势。

为了满足 IMT-Advanced（4G）的各种需求指标，3GPP 针对 LTE-Advanced（LTE-A）提出了几个关键技术，包括载波聚合、多点协作、接力传输、多天线增强等。

（1）载波聚合

LTE-A 支持连续载波聚合以及频带内和频带间的非连续载波聚合，最大聚合带宽可达 100MHz。为了在 LTE-A 商用初期能有效利用载波，既保证 LTE 终端能够接入 LTE-A 系统，每个载波应能够配置成与 LTE 后向兼容的载波，然而也不排除设计仅被 LTE-A 系统使用的载波。

目前 3GPP 根据运营商的需求识别出了 12 种载波聚合的应用场景，其中 4 种作为近期重点分别涉及 FDD 和 TDD 的连续和非连续载波聚合场景。在 LTE-A 的研究阶段，载波聚合的相关研究重点包括连续载波聚合的频谱利用率提升，上下行非对称的载波聚合场景的控制信道的设计等。

（2）多点协作

多点协作分为多点协调调度和多点联合处理两大类，分别适用于不同的应用场景，互相之间不能完全取代。多点协调调度的研究主要是集中在和多天线波束成形相结合的解决方案上。

在 3GPP 最近针对 ITU 的初步评估中，多点协作技术是唯一能在基站四天线配置条件下满足所有场景的需求指标的技术，并同时明显改进上行和下行的系统性能，因此多点协作的标准化进度成为 3GPP 提交的 4G 候选方案和面向 ITU 评估的重中之重。

（3）接力传输

未来移动通信系统在传统蜂窝网的基础上需要对城市热点地区容量优化，并且需要扩展地铁及农村的覆盖。

目前在 3GPP 的标准化工作集中在低功率可以部署在电线杆或者外墙上的带内回程的接力传输上，其体积小重量轻，易于选址。一般来说，带内回程的接力传输相比传统的微波回程的接力传输性能要低，但带内回程不需要 LTE 频谱之外的回程频段而进一步节省费用，因此两者各自有其市场需求和应用场景。

（4）多天线增强

鉴于日益珍贵的频率资源，多天线技术通过扩展空间的传输维度成倍地提高信道容量而被多种标准广泛采纳。

受限于发射天线高度对信道的影响，LTE-A 系统上行和下行多天线增强的重点有所区别。在 LTE 系统的多种下行多天线模式基础上，LTE-A 要求支持的下行最高多天线配置规格为 8×8，同时多用户空分复用的增强被认为是标准化的重点。LTE-A 相对于 LTE 系统的上行增强主要集中在如何利用终端的多个功率放大器，利用上行发射分集来增强覆盖，上行空间复用来提高上行峰值传输速率等。

（5）OFDM

OFDM 由多载波调制（Multi-Carrier Modulation，MCM）发展而来，OFDM 技术是多载波传输方案的实现方式之一，它的调制和解调是分别基于快速傅里叶反变换（IFFT）和快速傅里叶变换（FFT）来实现的，是实现复杂度最低、应用最广的一种多载波传输方案。在传统的频分复用系统中，各载波上的信号频谱是没有重叠的，以便接收端利用传统的滤波器分离和提取不同载波上的信号。OFDM 系统是将数据符号调制在传输速率相对较低的、相互之间具有正交性的多个并行子载波上进行传输。它允许子载波频谱部分重叠，接收端利用各子载波间的正交性恢复发送的数据。因此，OFDM 系统具有更高的频谱利用率。同时，在 OFDM 符号之间插入循环前缀，可以消除由于多径效应而引起的符号间干扰，能避免在多径信道环境下因保护间隔的插入而影响子载波之间的正交性。这使得 OFDM 系统非常适用于多径无线信道环境。

OFDM 的优点在于抗多径衰落的能力强，频谱效率高，OFDM 将信道划分为若干子信道，而每个子信道内部都可以认为是平坦衰落的，可采用基于 IFFT/FFT 的 OFDM 快速实现方法，在频率选择性信道中，OFDM 接收机的复杂度比带均衡器的单载波系统简单。与其他宽带接入技术不同，OFDM 可运行在不连续的频带上，这将有利于多用户的分配和分集效果的应用等。但 OFDM 技术对频偏和相位噪声比较敏感，而且峰值平均功率比（Peak to Average Power Rate，PAPR）大。

（6）无线中继

LTE 系统容量要求很高，这样的容量需要较高的频段。为了满足下一代移动通信系统的高传输速率的要求，LTE-A 技术引入了无线中继技术。用户终端可以通过中间接入点中继接入网络来获得带宽服务，减小了无线链路的空间损耗，增大了信噪比，进而提高了边缘用户信道容量。无线中继技术包括 Repeaters 和 Relay。

Repeaters 是在接到母基站的射频信号后，在射频上直接转发，在终端和基站都是不可见，而且并不关心目的终端是否在其覆盖范围，因此它的作用只是放大器而已。它的作用仅限于增加覆盖，并不能提高容量。

Relay 技术是在原有站点的基础上，通过增加一些新的 Relay 站（或称中继节点、中继站），加大站点和天线的分布密度。这些新增 Relay 节点和原有基站（母基站）都通过无线连接，和传输网络之间没有有线的连接，下行数据先到达母基站，然后再传给 Relay 节点，Relay 节点再传输至终端用户，上行则反之。这种方法拉近了天线和终端用户的距离，可以改善终端的链路质量，从而提高系统的频谱效率和用户数据传输速率。

（7）自组织网络

为了通过有效的运维成本（Operational Expenditure，OPEX）和 LTE 网络参数和结构复杂化的压力，3GPP 借用自组织网络的概念，在 R8 提出一种新运维策略。该策略将 eNodeB 作为自组织网络节点，在其中添加自组织功能模块，完成蜂窝无线网络自配置（Self-configuration）、自优化（Self-optimization）和自操作（Self-operation）。作为 LTE 的特性，SON（Self-Organiged Network，自组织网络）已经在 R8 引入需求，R9 完成自愈性、自优化能力的讨论。

LTE 自组织网络与传统 IP 互联网自组织不同在于，LTE 要求自组织节点可以互联之外，可以对网络进行自优化和自操作。

5.3.2.2　LTE-A 的演进

LTE-Advanced 与 4G 进程相互协同。2008 年 3 月 ITU-R 发出通函，向各成员征集 4G 候选技术提案，正式启动了 4G 标准化工作。在 2009 年 7 月初结束的 ITU-RWP5D(International Telecommunications Union-Radio Communications Sector Working Party 5D）的迪拜会议上，ITU 确定了 4G 最小需求，包括小区频谱效率、峰值频谱效率、频谱带宽等 8 个技术指标，这将成为衡量一个候选技术是否能成为 4G 技术的关键指标。

而 3GPP 将以独立成员的身份向 ITU 提交面向 4G 技术的 LTE-Advanced（LTE-A）。从 2008 年 3 月开始，3GPP 就展开了面向 4G 的研究工作，并制定了详尽的时间表，与 ITU 的时间流程紧密契合。在 ITU-RWP5D 的时间表中有两个关键的时间点：在 2009 年 10 月 WP5D 第 6 次会议结束 4G 候选技术方案的征集，2010 年 10 月 WP5D 第 9 次会议确定 4G 技术框架和主要技术特性，确定 4G 技术方案。围绕这两个时间点，3GPP 对其工作进行了部署，已经于 2008 年 9 月向 ITU-RWP5D 提交了 LTE-A 的最初版本，并分别于 2009 年 5 月和 2009 年 9 月提交完整版和最终版。

2009 年 10 月 14 日至 21 日，国际电信联盟在德国德累斯顿举行 ITU-R WP5D 工作组第 6 次会议，LTE-Advanced 入围，包含 TDD 和 FDD 两种制式。

2010 年 10 月 20 日，国际电信联盟无线通信部门（ITU-R）第 5 研究组国际移动通信工作组（WP5D）第 9 次会议在重庆确定 LTE-Advanced 和 IEEE 802.16m 为新一代移动通信（4G）国际标准。国际电信联盟于 2011 年底前完成 4G 国际标准建议书编制工作，2012 年初正式批准发布 4G 国际标准建议书。

5.3.2.3　LTE-A 与物联网的结合——D2D

物联网需要自动控制信息、传感射频识别、无线通信及计算机技术等，物联网的研究将带动整个产业链的发展，LTE-A 作为最有潜力承载新一代无线通信各种需求和业务的系统，对 LTE-A 网络中设备间（Device To Device，D2D）通信的研究有着非常重要的作用。由于 LTE-A 系统是在分组交换域中运行的，它可以提供基于互联网连接性、主要会话发起协议（Session Initiation Protocol，SIP）和 IP 的 D2D 连接性。基于 SIP 和 IP 的 D2D 连接性有利于给运营商提供 D2D 连接性控制，以及用一些升级软件功能来适合运营商的基础设施。D2D 通信使新业务有机会实现，而且减小短距离数据集中对等通信中 eNode 的负荷，比起 3G 扩频蜂窝和 OFDM 无线局域网，LTE-A 资源管理更快速，而且产生更高的时频分辨率。这可以允许使用没有分配的时频资源，或者由于受 eNode 控制功率受限而部分重复使用分配给 D2D 通信的资源。

图 5-2 给出了在目前 LTE-A 网络结构基础上实现 D2D 通信增加的功能块。为了达到这个目的，移动管理实体（Mobility Management Entity，MME）提供 SIP 和 IP 的连接，MME 与服务网关或公用数据网（Public Data Network，PDN）网关协商获取用户设备（User Equipment，UE）的 IP 地址，因此 MME 在 IP 地址功能体。为了这个目的，移动管理实体（MME）提供 SIP（Session Initiation Protocol）和 IP 连接性，MME 同服务网关、订阅信息、公用数据网络网关协商为用户设备（UE）获取 IP 地址。MME 在 IP 地址，订阅信息，SSIP presence 业务和 SAE（System Architecture Evolution）网络认证之间扮演一个绑定者的角色。所有这些表明 D2D 会话初始请求（像 SIP 邀请）应该发送到 MME 然后 MME 可以发起一个 D2D 无线承载的建立和一个给 D2D 终端设备的 IP 地址传送。D2D 通信的 IP 地址可以同本

地子网区域一起被创建，与本地断点的解决类似。在 UE 端 D2D 链路上像 IP 一样的连接性向高层协议栈（TCP/IP 和用户数据报协议（User Datagram Protocol，UDP）/IP）提供无缝操作，而且它使蜂窝和 D2D 联网的移动过程变得容易。

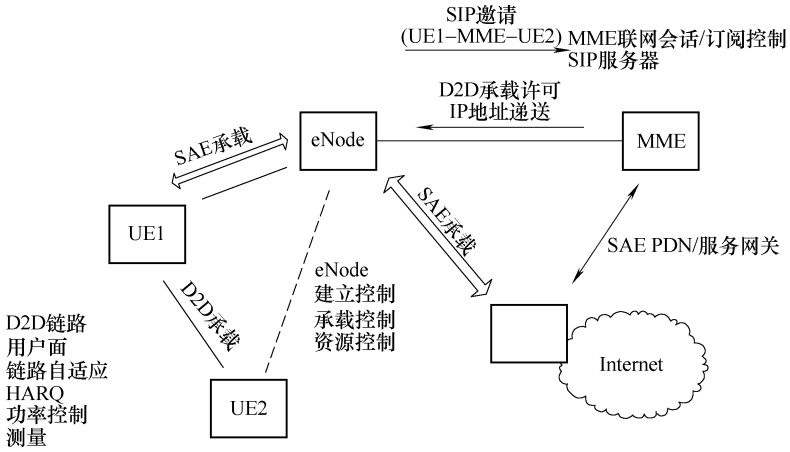


图 5-2　LTE-A 网络结构基础上实现 D2D 通信

下面介绍要实现 D2D 操作需要的一些功能块。

1. 无线身份标识和承载建立

在通过无线网络身份（Temporary Mobile Subscriber Identity，TMSI）或 IP 地址找到 D2D 的终端 UE 后，MME 将无线资源的本地控制授权给基站（eNode），基站也服务于 D2D 设备的蜂窝无线连接。因此，MME 的额外复杂度会受限，D2D 链路本身可以根据 LTE-A 无线原则运转。eNode 可以通过使用小区无线网络临时标识符（Cell Radio Network Temporary Identifier，C-RNTI）作为 UE 在小区中唯一的身份来保持对 UE 的控制，从一对一的关系映射到 LTE-A 逻辑信道的蜂窝承载身份标识，可以同样被逻辑信道上具有 D2D 承载身份标识的新指示取代。逻辑信道身份识别作为和 LTE-A 蜂窝类似的信令单元，现在可以被分配用来服务一个蜂窝逻辑信道或一个 D2D 逻辑信道。

2. 用户面

D2D 连接上的信息交换单元为 IP 包，重复使用 IP 数据报可以给像 TCP/IP 或 UDP/IP 的高层协议栈提供 IP 级的兼容性，而 TCP/IP 或 UDP/IP 显然可以用于蜂窝或者 D2D 通信。使用 UDP 端口可以避免 TCP 的 D2D 链路无线容量变化引起的主要问题，而链路无线容量变化是由于慢的起始和拥塞控制算法导致的。D2D 链路中内部相互连接网络路径上容量的 TCP 探测不是必需的，链路容量在对等实体上直接可用。因为层 2 协议提供可靠传输，且 D2D 中 TCP 重传在对等实体上有完整的重传信息，所以 TCP 重传也不是必需的。

UDP 提供分段和依次发送窗口等最重要的特性。UDP 段接收窗口用作处理通过无线协议的快速重传及提供到应用的依次发送。如果 UDP 段的长度变化不足以调整来适应 D2D 无线容量的变化，就应该考虑 UDP 段的无线层分段，这个会增加无线协议开销和分段的复杂度。

3. 干扰管理

蜂窝环境中具有 D2D 链路的干扰管理是一个重要问题。因为来自 D2D 链路的干扰会降低蜂窝容量和效率。LTE-A 在 1ms 子帧的短时隙 180kHz 的物理资源块（Physical Resource Block，PRB）的灵活频率分配上进行调度。因此，D2D 链路可以找到短时隙和频率比例，在蜂窝网络中不引入有害干扰而实现通信。类似问题会在感知无线电中观察到。最早的蜂窝和 D2D 通信间干扰协调的方法是给 D2D 分配专用的 PRB，这些资源是依据临时需求动态调整的 D2D 通信的专用资源，可能会导致可用资源使用效率降低；而当 D2D 链路重复使用分配给蜂窝链路相同 PRB 时，效率会提高。为了控制使用相同资源时 D2D 到蜂窝网络的干扰，我们建议 eNode 能够控制 D2D 发射机的最大发射功率。此外，在蜂窝网络中，eNode 使用上行或下行资源或两者兼有给 D2D 连接分配资源。当 D2D 作为 LTE-A 网络的一个底层实体，以频分复用或者时分复用方式工作时，干扰协调机制没有根本的不同。但是，当 D2D 复用蜂窝网络的上下行资源时，需要不同干扰协调机制在 D2D 链路中，没有清晰的上下行定义。

1）D2D 与蜂窝网络共享上行资源的干扰协调，在蜂窝上行传输中，eNode 是受到来自所有 D2D 发射机干扰的受害接收机。由于 D2D 连接中的 UE 仍然由服务 eNode 控制，它可以限制 D2D 发射机的最大发射功率。特别地，对于 D2D 通信的设备，UE 可以使用功率控制信息。D2D 发射机的发射功率可以通过功率回退值减小，这个功率回退值，通过 D2D 发射机的发射功率与蜂窝功率控制决定的发射功率相比得到。对于蜂窝用户的上行传输 eNode 可以额外地申请提高功率来确保蜂窝上行的信干燥比（Signal To Interference Noise Ratio，SINR）符合目标 SINR 要求。

2）D2D 与蜂窝网络共享下行资源的干扰协调，下行蜂窝网络的蜂窝接收机的实际位置取决于 eNode 的短期调度。因此，每次受害接收机可以是任何被服务的 UE。在建立一个 D2D 连接后，eNode 可以设定 D2D 的发射功率来限定对蜂窝网络的干扰。可以通过长期观察不同 D2D 功率水平对蜂窝链路质量的影响，找到合适的 D2D 发射功率水平。此外，eNode 可以确保在和 D2D 连接占用同样资源上被调度的蜂窝用户在传播条件下是独立的。例如，eNode 可能同室外蜂窝用户一起调度室内 D2D 连接。

4. 链路自适应

链路自适应通过自适应地改变 SINR 和误块率（Block Error Rate，BLER），以达到最大化效率的目标。链路自适应还可以通过调制编码速率选择和自动请求（Automated Repeat Request，ARQ）重传的方法实现。调制编码的瞬间选择可以部分基于信道探测测量，部分基于缓冲中指示比特数的缓冲状态信息。因为 D2D 资源上的 BLER 可以改变，这个改变主要取决于 D2D 的链路是在专用的资源上运行还是重复使用蜂窝资源，所以在链路自适应中，HARQ（Hybrid-ARQ）是必需的特征。与蜂窝链路相比，BLER 操作点可以更高，而且更高的变化可以被容忍。HARQ 怎样运行和服务于 D2D 的 HARQ 种类的细节是尚未解决的研究问题。应该在多天线配置方面对传输形式的自适应做进一步研究，分析预编码（Precoding）或者波束成形（Beamforming）是否会提供增益。

5. 信道测量

LTE-A 中的信道测量在低开销和多时频资源块分辨率的时频配置上有很好的特性。对于重复间隙里的探测用参考符号（Sounding Reference Symbol，SRS）仅仅占用一个符号的位

置。因此，测量接收机通过整合全时频上的探测序列，获得全带宽信道信息除了探测用参考符号，解调用参考符号（Demodulation Reference Symbol，DRS）也可用作信道测量，尽管解调用参考符号主要用于 LTE-A 中的信道估计、均衡、解调和解码，但 DRS 和 SRS 的结构对于 D2D 链路也是可用的。

6. 移动性

D2D 通信的距离是受限制的，当 D2D 运行对蜂窝网络有可容忍的影响时，不同场景下多大的 D2D 距离是可行的应该进行进一步研究。由于距离受限，D2D 无线可以设计为固定的链路。然而，它也应该支持有限的移动性。如果可行，默认的移动情况是将 IP 连接从 D2D 链路切换到蜂窝链路或者相反在无线意义上，这个可以通过 eNode 管理的一个公共的 C-RNTI 实现，在 IP 意义上，这个可以基于拥有多个有效 IP 地址来实现，可以允许用户面路由选择到一个 D2D 链路或者蜂窝网络的 IP 隧道，通过 IP 地址的流量的区分是唯一的且很容易由 UE 管理。

结合 LTE-A 的物联网技术，将引领人类走向新的 IT 时代。正由于物联网及 LTE-A 系统的有效结合和发展潜力，因此针对其架构分析具有重要意义。

5.3.3　物联网与光通信技术

5.3.3.1　概述

自 20 世纪 70 年代光纤商用化以来，光纤通信技术的发展已日渐成熟。20 世纪 90 年代后，随着光纤放大器和波分复用技术的迅速发展，光纤通信的通信距离和通信容量得到迅速拓展。目前单一波长的传输容量已从 2.5Gbit/s、10Gbit/s 发展到 40Gbit/s，单波道 160Gbit/s 传输技术的研究也已开展。从 1280～1625nm 的广阔的光频范围都能实现低损耗、低色散传输，使传输容量几百倍，几千倍甚至上万倍的增长，这一技术成果将带来巨大的经济效益，在一根光纤上同时传送千万路电话已从梦想变为现实。

在物联网迅速发展过程中，需要完成各种信号的会聚、接入、传输，并形成全国性的物联网，光纤通信将有很大的应用前景，不论是移动网还是传统固定电话网，从长远发展趋势看，最终将走向泛在网，从物联网应用的承载需求看，通信网或者说泛在网的技术发展完全能够承载物联网的需求。物联网涉及海量的数据集合和泛在的网络要求，即要求在空间上无所不在，时间上随时随地。传感网所承载的业务状态多数是近距离通信，而通信网特别是光纤通信网络能承载更高的带宽，适合长距离传输，非常适宜物联网应用的拓展。现有通信网络核心层传输技术正在向大容量 IP 化和智能化发展，从物联网的角度来看，还应更加智能化，包括自动配置障碍自动诊断和分析路由自动调度适配、资源分配更智能化等。网络接入层传输技术的发展趋势是光接入网络。目前各大运营商都已建设 FTTx（Fiber-to-the-x，光纤接入），它具有 QoS（服务质量）保障和更丰富的接入能力，能够满足 M2M 多种高速媒体流传送。

光纤不仅容量巨大而且价格低廉。光纤传输有许多突出的优点：频带宽、损耗低、重量轻、抗干扰能力强、保真度高、工作性能可靠、成本低。

目前，大容量光纤通信技术已经应用到了电信网、计算机网、广播电视网之中。这对于物联网的发展也具有十分重要的意义。

5.3.3.2　PON 技术

1. PON（Passive Optical Network，无源光纤网络）的标准发展

PON 系统首先出现在 20 世纪 90 年代初，1996 年 ITU-T 完成了对 G.982 的标准化。与此同时，以 ATM 为基础的 PON（APON）发展迅速，1998 年 ITU-T 正式通过了 G.983.1 建议，该建议对 APON 系统进行了详尽的规范。1999 年 ITU-T 推出了 G.983.2 建议即 APON 的光网络终端（ONT）管理和控制接口规范。ITU（International Telecommunications Union）和 FSAN（Full Servier ACCESS Network）联盟采纳了 ATM 标准，把它作为在 PON 第二层的帧封装标准，能为商业用户、家庭用户提供包括 IP 数据、视频、音频等综合业务，形成了 APON 的标准（文档号 ITU-TRecG.983）。但是 APON 存在着一系列的问题，比如带宽有限、带宽损失大、数据包开销大、协议转换麻烦、技术复杂、设备昂贵、多厂家互操作性差等。随着以太网技术的异军突起，APON 技术一直没有得到大规模应用。

随着互联网的高速发展，用户网络带宽的要求不断提高，各种新的宽带接入技术已经成为研究的热点。在这种背景下，IEEE 于 2000 年底成立了 EFM 工作组（Ethernet inThe First Mile Study Group），试图引入一种新的接入技术标准 Ethernet PON（Ethernet Passive Optical Network，EPON）。2004 年 IEEE 802.3EFM 工作组发布了 EPON 标准 IEEE 802.3ah，2005 年并入 IEEE 802.3ah-2005 标准。EPON 利用 PON（无源光网络）的拓扑结构实现以太网的接入，它基于高速以太网平台和 TDM 时分 MAC（媒体访问控制）方式，能够提供多种综合业务的宽带接入，但其承载 TDM 业务和语音业务的效果不理想，较难满足电信级的 QoS 要求。

除了 EPON 标准，另外一个主要标准则为 ITU-T 的 GPON（Gigabit-Capable PON）标准，GPON 最早由 FSAN 组织于 2002 年 9 月提出，ITU-T 在此基础上于 2003 年 3 月完成了 ITU-TG.984.1 和 G.984.2 的制定，2004 年 2 月和 6 月完成了 G.984.3 的标准化，从而最终形成了 GPON 的标准族。GPON 技术是最新一代宽带无源光综合接入标准，其无论编码效率、汇聚层效率、承载协议率和业务适配效率都最高，具有高带宽、高效率、大覆盖范围、用户接口丰富等众多优点，被大多数运营商视为实现接入网业务宽带化，综合化改造的理想技术。

2. GPON 和 EPON 技术对比

GPON 和 EPON 技术各有特点，表 5-3 为对这两种技术做出重点对比。

表 5-3　GPON 和 EPON 技术的对比

项　　目	GPON	EPON
相关标准组织	ITU-T G.984 标准组	IEEE 802.3ah 工作组
支持的速率等级	上行 155Mbit/s，622Mbit/s，1.25Gbit/s 或 2.5Gbit/s 下行 1.25Gbit/s 或 2.5Gbit/s	上下行对称 1.25Gbit/s
支持的 ODN 等级	Class A、B、C	Class A、B
上下行可用带宽（传输 IP 业务）	1100Mbit/s	760～860Mbit/s

（续）

项　　目	GPON	EPON
协议和封装格式	ATM 或 CFP 封装格式	基于 IEEE 802.3 协议的封装格式
同步方式	第 125μs 下行同步标识	时钟标签法
测距方式	数字开窗法	时钟标签法
业务能力	ATM、TDM、以太网	以太网
成本	略高	低
QoS 保证	容易	难

1）GPON 支持多种速率等级，可以支持上下行不对称速率，上行不一定要达到1.25Gbit/s以上的速率，EPON 则只支持对称 1.25Gbit/s 的单一速率。

2）EPON 支持 ClassA 和 B 的 ODN 等级，GPON 可支持 ClassA、B 和 C，因此 GPON 可支持高达 128 的分路比和长达 20km 的传输距离。2009 年日本市场大量使用的分路比为1:32。

3）单从协议上比较，GPON 标准是以 G.984.3 体系结构为基础，而 EPON 则是以 IEEE 802.3ah 协议为基础。

4）ITU 在制定 GPON 标准过程中沿用了 APON 标准 G.983 的很多概念，与 EFM 制定的 GEPON 标准相比其标准更完善。但由于其增加了 TC 子层，因此也相应增加了一定的开销。

5）GPON 标准规定 TC 子层可以采用 ATM 和 GFP 两种封装方式，其中 GFP 封装方式适于承载 IP 等基于包的高层协议，对于为了支持 ATM 业务而定义的 ATM 封装方式在以 Ethernet 为基础的 GPON 系统中可以省略 ATM 业务或者单独开发。

6）EPON 在 Ethernet 上承载 TDM 业务的技术并不成熟，较难满足电信级的 QoS 要求，因此 EPON 为了能够承载 TDM 业务和语音业务必须设计新的 MAC 机制并增加新的软硬件。而 GPON 由于其设计的 TC 子层结构和 ATM 封装方式，能够比较容易地支持 TDM 业务和语音业务。

7）相对较低的成本令 EPON 较早开始大规模商用。

8）GPON 在效率及 QoS 上具有明显优势。

综上所述，GPON 在上下行带宽、距离/分光比均比 EPON 有优势，并且能良好地承载 TDM 业务和语音业务；虽然，目前，GPON 设备单价比 EPON 略高，但随着 GPON 产业链的日益成熟，这种价格差距将很快消失。

5.4　三网融合

物联网时代，当大量终端比较集中地接入网络时，同时发送数据到物联网应用平台，核心网会遭受非常大的负荷冲击。对无线、核心网都将构成比较大的负荷，拥塞难免会发生，也会增加人与人之间通信的故障率。一方面，核心网的移动性管理网元需要同时处理终端的接入控制，频繁进行附着、激活、业务请求、创建承载等信令交互，会造成控制面负荷过载

的发生。同时，当数据交互同时发生时，大量的物联网终端通过核心网的媒体网关与同一个远程服务器进行数据通信，这就可能造成媒体网关数据拥塞，特别是媒体网关到远程服务器的IP通道会造成数据阻塞，引起媒体面过载的发生。

物联网实质是一个由感知层、网络层和应用层共同构成的庞大的社会信息系统。物联网的发展更多地取决于网络的发展，物联网的很多应用都需要网络来支撑，三网融合为物联网的发展提供了条件，为物联网进入家庭搭建互联奠定了基础。

三网融合的驱动力是信息化服务。信息化服务已经广泛地渗透到人们的工作、生活之中。物联网正是以家庭信息服务为目标，致力于实现用户对生活品质的不断追求，因而具有了庞大的市场和产业空间。典型的应用包括远程学习、教育、保健、娱乐、智能家居、家庭安保等。技术的发展使未来的电信网、广电网和互联网都可以向数字、双向、多功能、智能、全业务方向发展，能够为物联网提供安全、高速和宽带的信息传输服务。因此，物联网的发展非常契合三网融合的理念。

物联网为三网融合提供了应用切入点，电信、电视等运营商都纷纷想从物联网产业的广阔发展空间中分一杯羹，除了提供基础的网络服务，还想利用各自的服务手段、技术手段、公信力和客户群在物联网发展中扮演关键的重要角色，成为海量数据处理和信息管理服务提供商。

5.4.1　三网融合综述

5.4.1.1　什么是三网融合

三网融合是指通过技术改造将电信网、互联网和广播电视网络技术相互融合，使得三大系统相互兼容，让它们的高层应用业务进行融合，目的是能够在同一个网络上同时开展语音、数据和视频等多种不同业务。三网融合之后每个网络都能够提供包括语音、数据、图像等综合多媒体的通信业务。三网融合并不是指三大网络简单的物理合一，而是指三个网络中业务的融合。三网融合的目标是整合各类网络资源，形成具有业务融合能力的网络基础设施，如图5-3所示。

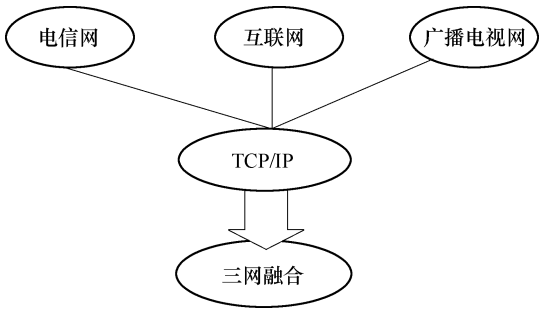


图5-3　三网融合示意图

物联网中，由于大量物体需要接入网络，业务量剧增，数据量也大大增加，三网融合对于物联网核心网的建设十分重要。物联网通过各种不同的接入方式将感知层获取的数据信息接入到网络中，庞大的数据流和复杂的数据系统需要一个互相融合的网络来支持系统对数据的传输和操作。

作为信息产业发展的基础，广播电视网、电信网与互联网的三网融合则是现代信息技术发展的必然趋势，并且已经日渐成为人们关注的网络领域技术变革的热点。

广播电视网是全国最大的公众信息网络，贯通全国和各省市首府及其大部分的城镇，拥有用户终端数超过1亿户。宽带双向光纤同轴电缆混合网（Hybrid Fiber-Coax，HFC）入户技术可在有线电视的同轴电缆上，利用频分技术，同时实现看电视、打电话、上网，且互不

干扰。虽然我国的有线电视网是世界上用户规模最大的有线电视网，但由于其发展不均衡，全国各地网络分配网带宽不一，使用器材离散性大等诸多原因，因而也只有在对现有网络进行不同程度的升级改造之后，才有进一步拓展广播电视业务以外的其他增值业务的可能。

电信网是以电话网为基础逐步发展起来，目前信息到户主要是双绞线，通过交换机与骨干网相连。电话网是最早进行数字化的，传输方式逐步向光纤到户发展，传输协议从准同步体系（Plesynchronous Digital Hierarchy，PDH）到同步体系（Synchronous Digital Hierarchy，SDH）进而到非同步转移模式（Asynchronous Transfer Mode，ATM）发展，但由于发展的不均衡，尚不能做到全网传输和交换的数字化。

虽然有非对称用户线路（Asgmmetric Digital Subscriber Line，ADSL）和高速用户环路（Very-high-bit-rate Digital Subscriber Loop，VDSL）等方式，速率可以从几 Mbit/s 到几十 Mbit/s，但 ADSL 和 VDSL 的高速率对于电缆介质的传输距离和线路质量有着严格的要求。可以说，整个网络的流通能力受到双绞线传输容量这一瓶颈的抑制，这将是电信业务网一个难以逾越的障碍。

计算机网最早是从局域网发展起来的，远程网络是在国际互联网大规模发展后才迅速进入平常百姓家庭的，早先主要取决于电信网实现用户接入，同样受入户双绞线传输容量的限制。但随着 TCP\IP 的推广应用，架构于 IP 之上的软交换、IPTV 技术应用日趋成熟，在计算机网络实现语音、数据、视频的混合传输已经成为现实。而在接入层面，LAN、FTTX、PON、Wi-Fi、WiMax 等新技术层出不穷，发展极快，目前 FTTB/C + LAN 接入技术已经成为家庭宽带接入的优选方案。

5.4.1.2　三网融合的表现形式

三网融合已经在我们生活中有了很多应用，其中，手机电视、VoIP、下一代广播电视网等几个方面是比较为大家所熟知的。

手机电视（MobileTV），百度百科给出的解释是：“利用具有操作系统和流媒体视频功能的智能手机以及现在支持 RTSP（Real Time Streaming Protocol，实时流传输协议）的非智能机都可以观看电视的业务。”简单来说就是在手机上实现观看电视节目的功能。手机可以接收电视卫星发射的信号，可以接收到各大电视台的信号，方便人们随时随地看电视。

VoIP（Voice overIP）即 IP 电话（Internet Protocol Phone），是利用 IP 网络实现语音通信的一种先进通信手段，是一种完全基于 IP 网络的语音传输技术。与传统电话不同的是它的资费极低，甚至很多是免费的。因为 IP 电话的语音信号走的是互联网，互联网通信的一大特点就是低费用。它利用语音网关，软交换平台，网守等设备将模拟信号数字化，然后将数据压缩成数据包，通过 IP 网络传输到语音的目的地址。目的地址接收到数据包后，将数据重组，解压缩后再还原成模拟信号。这样，一次完整的通话过程就在 IP 网络中实现了。IP 电话存在的缺点是安全性不高，语音质量取决于当时网络环境的好坏，通话质量无法得到保证。

5.4.1.3　三网融合的优点

三网融合之后，带来的不仅是用户对多业务需求的满足，还有对网络资源的节省。甚至将引起人们生活方式的改变。

1. 资源节省方面

不仅有利于简化网络，降低网络管理复杂度，降低维护成本，极大地减少基础建设投入，而且还可以使不同的独立专业网络转变为综合性网络，提升网络性能，充分利用网络资源。

2. 业务方面

不仅继承了原有的网络语音、数据、视频等业务，而且通过网络融合，衍生了更加丰富多彩的增值业务，极大地拓展了业务提供的范围。并且能够提供的业务由单一业务向文字、语音、数据、图像、视频等多媒体综合业务转化。

三网融合打破了电信、广电运营商在各自领域长期的垄断地位，使资费变得更低。

5.4.2　三网融合的研究现状和发展趋势

5.4.2.1　国外现状

对国外而言，他们并没有三网这一概念，但是如同我国的三网融合工作中实际进行的工作一样，西方各国也通过各种方式打破了电信运营商和有线电视网运营商的独立运营模式，美国、法国、日本等陆续出台相应的立法，来促进广播电视业和电信业务的激烈竞争，以繁荣信息业。各国也早都意识到各大不同运营商独立进行的网络建设造成的资源资金的浪费和网络的重复性搭建，也不利于信息业的长远发展。进行网络融合不仅可以节约资源，避免资源浪费，也可以满足人们日益增长的对于多种业务的不断增长的要求。各国也已经先后放松对互联网、有线电视公司、电信运营商之间的管制，创造环境以方便它们之间的相互融合、相互竞争。

微软、索尼等世界知名IT企业，已经把“网络融合”作为发展的业务重点而加以大力推进。国际上，TCI、Nynex、CEY等有线电视网络公司和AT&T、Spring等通信公司以及Microsoft、Oracle、IBM等计算机软硬件公司都在三网融合这方面进行了相关的研究工作，并且有的公司已经有相应的产品问世。

美国这一IT强国，在这方面也是具有领先的水平，他们的电信和通信业市场开放较早，竞争更为成熟和充分，领先于很多国家进行了网络融合这方面的探索和尝试。1993年，美国提出信息高速公路计划，带来了席卷全球的信息化浪潮，1996年，美国电信法的颁布，为有线电视的发展开辟了广阔的前景。美国研究出一系列新技术并投入应用，如电缆调制解调器、非对称数字用户线路（ADSL）、无线有线电视技术等，彻底改变了有线电视的应用范围，改变了人们对有线电视的传统观念，可以说在网络融合这一场现代化高科技竞争之中，美国已经处于领先地位。

5.4.2.2　国内现状

我国是提出“三网融合”的国家，政府对这方面十分关注，正是由于意识到各不同运营商独立进行的网络建设造成的资源资金的浪费这一事实，着眼于信息业的长远发展，我国提出了“三网融合”这一技术概念。希望能够依靠网络融合节约资源、避免资源浪费，并且可以满足人们日益增长的对于多种业务的不断增长的要求。

我国已经推出了IP电话、数字电视、网络电视、手机网络等日常生活各方面的应用，并且普及率很高，也已经得到了广大消费者的认同和赞赏。政府工作、公共安全、平安家居、工业监测等方面也开始应用三网融合技术。现在我们的手机可以听广播、看电视、上网

等，进行多种业务；在互联网上我们可以看网络电视，可以打 IP 电话，这些都是三网融合带来的产物。

5.4.2.3　发展趋势

三网融合的应用无处不在，范围涉及家居、交通、工业、农业、商业、政府工作、军事化等各个方面，必定能够得到良好的发展。我们已经实现了手机看电视、上网，互联网上看电视，打电话。我们不难预见：以后的电视也可以打电话、上网。三者之间会形成相互交叉，形成你中有我、我中有你的格局。

例如，未来，我们可以用电视遥控器打电话，在手机上看电视剧，随需选择网络和终端，只要拉一条线、接入一张网，甚至可能完全通过无线接入的方式就能通信、看电视、上网等各种应用需求。而对于物流行业来说，以后客户发货可以随时随地用手机迅速查到合适的物流公司，并立即下单，物流公司可以通过手机视频看到客户的货的大致情况，并立即决定派什么样的车去提货，发完货以后，客户也能随时自主追踪货物状态，直到货物安全到达最终用户手里。

5.4.3　三网融合的网络架构

当前各主要网络都支持 TCP/IP 标准协议。因此我们以该协议作为核心协议，进行多网络的融合。TCP 不仅仅是一个通信协议，也不仅仅是一个 API（Application Programming Interface，应用程序编程接口），它是由多个数据通信协议组成的套件。虽然该套件中有许多协议，但传输控制协议（TCP）和互联网协议（IP）是其中最重要的两个协议，所以套件以它们的名字来命名，并称为 TCP/IP 簇，简称 TCP/IP。

目前计算机网使用的协议绝大部分是 TCP/IP。TCP/IP 是 1969 年在美国的 ARPANet（Advanced Research Project Agency Network）网上开始研制的，最初的目的是分组交换。TCP/IP 历经三十多年的发展，逐渐得以完善和成熟，并成为网络市场中事实上的网络通信协议标准，TCP/IP 是一组用于实现网络互连的通信协议。互联网网络体系结构以 TCP/IP 为核心。基于 TCP/IP 的参考模型将协议分成四个层次，它们分别是：应用层、网际互连层、传输层（主机到主机）和网络访问层。

1）应用层：应用层对应于 OSI（Open System Interconnect，开放式系统互联）参考模型的高层，为用户提供所需要的各种服务，例如：FTP（File Transfer Protocol，文本传输协议）、Telnet、DNS（Domain Name System，域名系统）、SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）等。

2）传输层：传输层对应于 OSI 参考模型的传输层，为应用层实体提供端到端的通信功能。该层定义了两个主要的协议：传输控制协议（TCP）和用户数据报协议（UDP）。TCP 提供的是一种可靠的、面向连接的数据传输服务；而 UDP 提供的是不可靠的、无连接的数据传输服务。

3）网际互联层：网际互联层对应于 OSI 参考模型的网络层，主要解决主机到主机的通信问题。该层有 4 个主要协议：网际协议（Internet Protocol，IP）、地址解析协议（Address Resolution Protocol，ARP）、互联网组管理协议（Internet Group Management Protocol，IGMP）和互联网控制报文协议（Internet Control Message Protocol，ICMP）。IP 是网际互联层最重要的协议，它提供的是一个不可靠、无连接的数据传递服务。

4）网络访问层：网络访问层与 OSI 参考模型中的物理层和数据链路层相对应。事实上，TCP/IP 本身并未定义该层的协议，而由参与互连的各网络使用自己的物理层和数据链路层协议，然后与 TCP/IP 的网络访问层进行连接。其结构如图 5-4 所示。

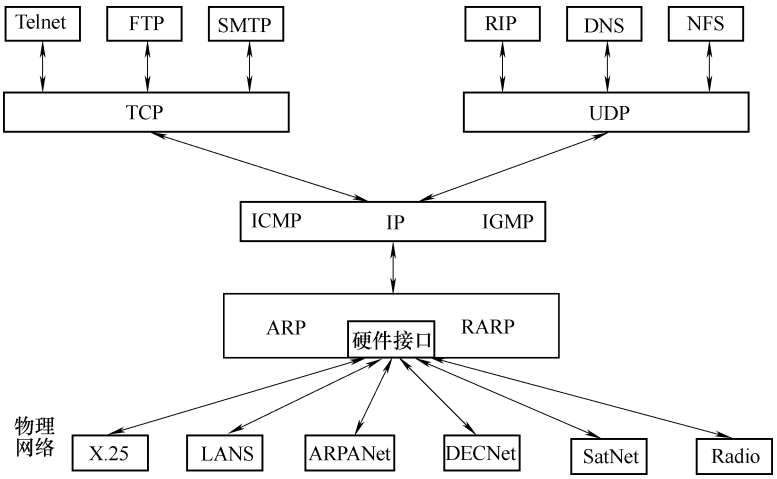


图 5-4　TCP/IP 协议族

三网融合后的网络架构如图 5-5 所示，电信网、互联网、广播电视网相互融合，它们的物理层将所有资源进行共享，并将所有的信息资源对所有业务经营者共享，融合之后三大网络的功能基本相同，通过多种接入方式达到对多种业务的统一服务。

不同网络的数据在 IP 层融合。长途电话的语音数据根据协议标准形成 IP 包，IP 包使用相应的链路层协议可以在以太网、有线电视网等任意的网络中传输。最后到达网关，该网关根据相应协议将数据转成 PSTN 中的信令和语音数据发送给相应的接收端，最终实现提供多种业务的目的。

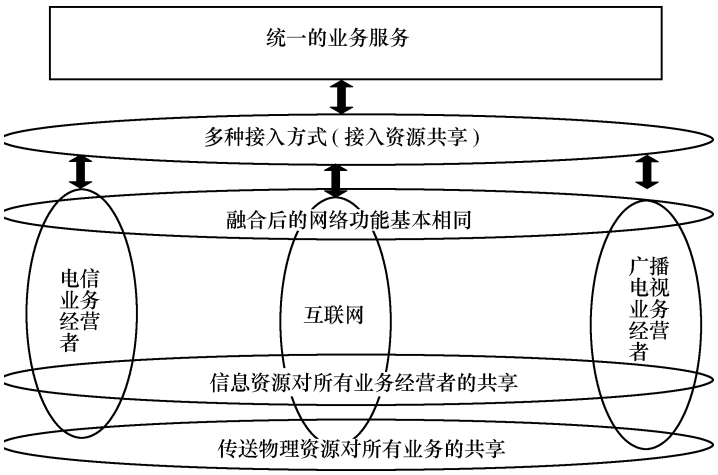


图 5-5　三网融合网络架构

5.4.4　三网融合的技术条件

5.4.4.1　数字通信技术

具有统一的数据流模式是三大网络之间能够进行业务融合的前提条件。数字通信技术对语音、图像以及其他类型的数据信号编码，使它们成为0/1数字符号。所有业务通过数字化都统一成0/1比特流。这样不论是语音信号、数据信号、图像信号还是视频信号等都可以通过不同的网络来进行传输、交换、处理，达到网络融合的目的。

5.4.4.2　大容量光纤通信技术

三网融合的目的是为了更好地提供各种业务。随着业务量增多，业务种类也变得更纷繁复杂。随之带来的趋势就是网络的业务量会不断增大，网络中传输的数据量也变得很庞大。尤其是在物联网这一领域的应用之中，大数据量传输处理能力更是一个必要条件。大数据传输量在传输时需要更大的带宽。大容量光纤通信技术刚好满足了这一要求，成了在三网融合技术里传输介质的最佳选择。

我们知道，光纤不仅容量巨大而且价格低廉。光纤传输有许多突出的优点：频带宽、损耗低、重量轻、抗干扰能力强、保真度高、工作性能可靠和成本低等。

目前，大容量光纤通信技术已经应用到了电信网、互联网、广播电视网之中，这十分有利于三网融合的进展。

5.4.4.3　IP技术

三网融合，要对网络资源进行综合调度和管理，不仅需要将不同种类型的业务数据格式统一成数字信号，在传输过程中还需要各种网络之间具有统一的规则和传输协议。IP技术满足了这种需求。TCP/IP是互联网的基本思想：TCP/IP能够抽象和屏蔽硬件细节，向用户提供通用的网络服务。在低层网络技术与高层应用程序之间采用TCP/IP，网络传输更为快捷方便。由于提供了统一的IP地址，从而屏蔽了下层物理网络地址的差异性，统一了异种网络地址，保证了异种网络的互通。可以将多种业务、多种硬件环境、多种通信协议综合统一起来。

为了满足网络融合产生的IP地址需求量的增大，产生了IPv6技术。IPv6巨大的地址空间和灵活的分配地址方式都十分适合网络融合中各种网络适合的通信方式之间的相互转换，并且在物联网这一特殊领域发挥着重要作用。

全IP技术在物联网中也将扮演重要角色，也是三网融合的一个技术趋势。

三网融合的关键技术有很多。技术的发展是三网融合最主要的推动力量。网络技术正逐渐趋向一致，逐渐向IP汇聚已成为下一步发展的主导趋势，特别是IP技术、光通信技术和数字技术、接入网技术、软件技术等重大技术的进展，为三网融合铺平了道路，三网融合正是这些技术合力的结果。

5.4.5　电力线通信及四网合一

电力线通信（Power Line Communication，PLC）是指利用现有电力线，通过载波方式将模拟或者数字信号进行高速传输的技术。它具有高可靠性、低成本等优点，是一种应用较为普遍的通信方式。

物联网的承载网具有传输数据量庞大、传输距离远的特点，如果将物联网和电力线通信

技术相结合，在现有电路上采取智能嫁接技术，可以对大量终端进行控制和管理，市场潜力巨大，另外又十分环保节能。电力线通信技术将成为物联网新技术的有益补充，具有广泛的应用前景。

传统电力显示给用电设备传送电能，而不是用来传送数据的，所以电力线对数据传输有许多限制。电力网设计的初衷是传送 50Hz 或 60Hz 的电力。使用这种介质在较高的频率上传送数据有一些技术上的挑战。各个国家的电源线栅格结构、室内布线和接地方式不尽一致，甚至在一个国家内都不相同。电力线信道是一个刺耳的噪声传输媒质，是一种很难建模、具有频率选择性、受到多色背景噪声损害及周期和非周期性脉冲噪声影响的信道。

建立高速、双向、实时、集成的通信系统是实现智能电网的基础，没有这样的通信系统，任何智能电网的特征都无法实现，因为智能电网的数据获取、保护和控制都需要这样的通信系统的支持，因此建立这样的通信系统是迈向智能电网的第一步。同时，通信系统要和电网一样深入千家万户，这样就形成了两张紧密联系的网络——电网和通信网络，只有这样才能实现智能电网的目标和主要特征。作为智能电网的标志性技术之一，电力光纤到户是在普通低压入户电线中加入光结，把电线打造成一条信息共享的“高速路”。在这条“高速路”上，既可输送电能，也可搭载互联网和电信、广播电视信号，从而实现四网融合的功能。现代通信的方式主要有：互联网、光纤通信、电力线通信、无线通信等。由电力线网络发展起来的通信方式覆盖广、安全性高，正受到越来越多的关注。在克服了标准统一及通信质量等问题后，很有可能在智能电网中大有所为。

宽带电力线通信（Broadband over Power Line Communication），简称 BPL，是指带宽限定在 2～30MHz 之间、通信速率通常在 1Mbit/s 以上的电力线载波通信。宽带电力线通信技术指利用现有电力线，无需重新布线就可以实现数据、视频等信号的传输，终端上只要插上电源插头，就可以实现互联网接入、电视信号接收、电话拨打，最终实现四网合一。

集互联网、电视、电话及电力传输于一体的“四网合一”宽带电力线通信（BPL）新技术，是一种利用现有的电力线作为信息传输媒介，通过载波方式传输模拟或数字信号的通信技术，是一种全新的通信手段，其优势明显。可直接利用现有的电力线，而无需重新布线、成本低廉、应用范围广。同时，由于成功地解决了 BPL 载波通信的防雷、抗干扰、抗衰减、信号安全隔离、信号分离和信号注入等技术难题，不仅可以自动对抗来自其他电器对通信的信号干扰，在用电高峰期也能正常使用，也保证了通信的安全性和保密性。

电力基础设施将通过加载数字设备和芯片技术升级为人类创新生产和生活的重要设施，电力系统的通信和信息等服务完全可能与传统业务平分秋色，与此同时将实现有插座的地方就有信息互动，电力产业将实现工业革命以来最重要的大跨度转型。BPL 解决了信息高速公路的末端接入问题，可满足智能电网用电环节信息化、自动化、互动化的需求。

5.4.5.1　电力线信道特性分析

电力线主要是用来传输电能的，并不是理想的通信信道。由于电力线通信信道具有明显的时变性和随机性，目前对其研究大都停留在实测的水平上，没有精确的理论分析和数学模型。分析电力线信道特性，需要考虑 3 方面的问题。

（1）噪声特性

低压电力线信道内的噪声分为 4 类。

1）背景噪声时时存在。其频谱占据了整个通信带宽，所以扩展信号频谱并不能提供任

何增益。经测量发现背景噪声的主要来源是交直流两用电动机。不过背景噪声很少能够达到最高功率水平，而且将与传输信号一起被用户配电网络所衰减。

2）随机脉冲噪声：闪电和负载的开关操作，都会产生随机脉冲噪声，而且每一个脉冲噪声都将影响一个很宽的频带。脉冲噪声3种主要参数是幅度、宽度和到达间歇时间。脉冲幅度和脉冲宽度一起给出了脉冲能量。宽度影响到在给定速率下的数据位数，而到达间歇时间则影响脉冲噪声发生的频率。在特性恶劣的信道中，常使用扩频（Spread Spectrum，SS）和前向纠错编码（Forward Error Correction，FEC）和交织技术来降低误码率。

3）与工频同步的谐波噪声：由工频电压触发的可控硅整流器产生。因其开关频率与电源频率同步，故产生了一系列不同幅度不同频率的谐波噪声。

4）与工频无关的谐波噪声：又称为周期异步噪声，一般是由电视接收机和计算机显示器产生。脉冲的重复频率依赖于电视机和显示器的扫描频率标准，而对高分辨率和图像偏移质量的追求将使这些频率越来越高。

（2）衰减特性

高频信号在电力线上的衰减，是低压电力线通信遇到的又一个实际困难。电力线是用来传输50Hz电能的，并非为通信专门设计。另外，由于低压电网线路分支很多，各种不同性质的负载在网络的任意位置随机地连接或断开，使通信系统所要求的最基本的阻抗匹配都很难做到，信号时常会遇到反射、驻波等种种复杂现象的干扰，因此，其衰减特性非常复杂，具有很强的时变性。这种衰减与通信距离、信号频率等都有密切关系。

低压电网衰减特性的一些定性规律。

1）除了短距离传输外，即使接收机与发射机同相，信号衰减仍可达到或超过20dB；

2）当频率上升时，信号衰减随之增大，但这种变化并不是单调的；

3）在某些特定的频率点上，有可能发生深度衰减；

4）电力网上电力负载的变化会极大地影响信号的衰减。不同的节点间，甚至同一对节点在不同时间，其衰减值都相差很大。

（3）阻抗特性

电力线的阻抗主要由电力线上接入负载的阻抗特性所决定。正是由于接入负载阻抗的不确定性和时变性，引起了电力线阻抗的不稳定。

测量结果表明：低压电力线上的输入阻抗与所传输的信号频率密切相关。总体上，阻抗随着频率增加而增加，但某些局部又出现所谓的阻抗低谷区。其原因是电力线连接有各种复杂的负载。这些负载及电力线本身组合成许多谐振回路，在谐振频率及其附近频率上，形成低阻抗区，从而造成了在局部频率段内，阻抗随着频率增加而减小的现象。同时，由于负载在电力线上随机地连接或断开，所以在不同时间，电力线的输入阻抗会发生较大幅度的改变。其结果，在同一频率下测量的阻抗有很大的波动。

如果输出阻抗不能较好地与线路阻抗相匹配，则信号能量不能有效输出，实际耦合到电力线上的信号能量就会很小，产生较大的耦合损耗。

5.4.5.2　IEEE 电力线通信标准

对于消费者来说，目前已经可在某些时间利用多种技术实现到室内和在室内的宽带连接。在这些技术中，电力线通信对于提供宽带连接是一个极好的候选对象，因为它是一种既存的基础设施。这一设施比任何其他有线设施更普遍地渗透到千家万户，从而可使每一件电

力线设备变成增值服务的目标。因此，可以考虑把电力线通信作为其他方法不可替代的、在未来大量应用的宽带连接技术。宽带电力线通信不能被采纳的最根本的障碍是由于缺乏一个全球认可的标准化组织制订的国际技术标准，幸好，这一障碍通过 IEEE P1901 标准联合工作组的工作，将很快被消除。成立于 2005 年 6 月的联合工作组，2009 年已经进入到关键工作阶段。

自从 2005 年 6 月工作组成立以来，业界对电力线通信技术的兴趣大为增加，现在工作组已囊括了跨整个电力线通信价值链的 50 多个实体。按照 IEEE P1901 工作组的工作范围，电力线通信标准将使用低于 100MHz 的传输频率，该频率范围将可用于所有级别的电力线通信设备，包括用于最前/最后一英里（到互联网最前设备距离 <1500m）连接宽带服务的设备，以及建筑物内的局域网和其他的数据分发（设备间距 <100m）应用，且物理层数据率大于 100Mbit/s。

P1901 工作组的工作范围只限于物理层和国际标准化组织开放系统互联基本参考模型所定义的数据链路层的媒体接入子层。

2005 年 6 月 IEEE P1901 工作组正式成立，9 月便确定了总的工作流程。同时，一个分组开始制订一整套统一的功能和技术要求，并在 IEEE 通信学会电力线通信技术委员会某些成员的协助下，研究了信道和噪声模型以及拓扑描述，其结果被批准列入到通告的附录中。此后几年的进展形成了 3 个不同簇的数百项功能和技术要求：

室内（IH）——该簇要求涉及使用结构中的低压线缆承载数字内容；

接入（AC）——该簇要求涉及在馈到室内的中低压电力线上的宽带内容传输；

共存（CX）——该簇要求侧重于使电力线通信设备相互兼容的要求，即使是基于不同技术的设备。

室内簇的功能和技术要求主要针对将住房或办公室的电力线用作数字通信介质的问题。接入簇包括的功能和技术要求针对将多媒体服务通过电力线送给居民，以及发挥电力实际功效的问题。共存簇包含的功能和技术要求针对如何控制非互通设备能共享信道而不引起相互之间有害的干扰。在共存簇中定义共存协议，该协议确定通用资源的共享机制，由此来决定非 IEEE 1901 设备彼此之间以及它们与 IEEE 1901 设备之间的信道共享。除这 3 个簇之外，P1901 工作组还开始把自己的工作扩展到运输领域的通信能力（如飞机、舰船、火车、汽车等）。

2007 年 2 月，工作组批准了一整套作为电力线通信基础标准所确定的功能和技术要求，并发出征求建议书，以征求满足所批准的功能和技术要求的系统技术解决方案。截至 2007 年 6 月，总共收到 12 份建议，每簇 4 份。2008 年 4 月，每一簇只剩下一个被选定的技术建议。

5.4.5.3　PLC 系统

图 5-6 为典型的 PLC 系统示意图。在配电变压器低压出线端安装 PLC 主站，将电力线高频信号和传统的光缆等宽带信号进行互相转换。PLC 主站的一侧通过电容或电感耦合器连接电力电缆，注入和提取高频 PLC 信号；另一侧通过传统通信方式，如光纤、CATV、ADSL 等连接至互联网用户侧，用户的计算机通过以太网接口或 USB 接口与 PLC 调制解调器相连，普通话机通过 RJ-11 接口连至 PLC 调制解调器，而 PLC 调制解调器直接插入墙上插座。如果 PLC 高频信号衰减较大或干扰较大，可以在适当的地点加装中继器以放大信号。

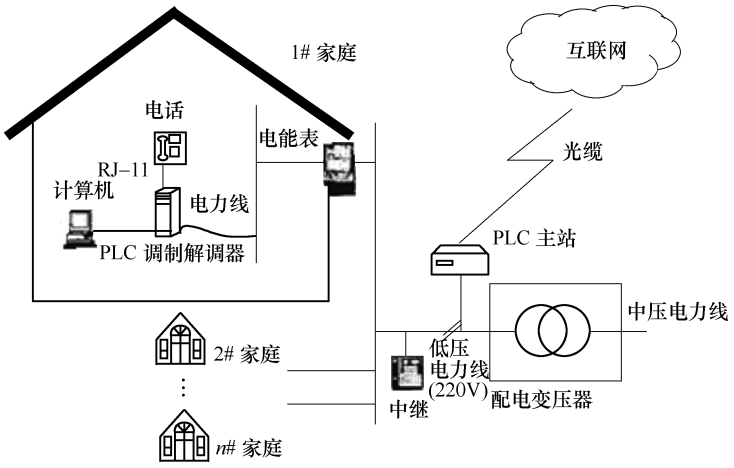


图 5-6　PLC 系统示意图

PLC 与其他接入方式的比较见表 5-4。目前最常用的接入方法可分为：以电话线为基础的 Modem 接入、ISDN 接入、ADSL 接入和以利用四通八达的有线电视网络为基础的 Cable Modem 接入、以卫星直拨网络为基础的 Direct PLC 接入等。另外还可以利用电力线上网，最有前途的应该是高速光纤直接到户专线接入。

表 5-4　几种接入方式的比较

通信方式	速率/(bit/s)	可否同线传输语音	物理介质	评　价
调制解调器	56k	否	双绞线	标准化程度高、应用广泛、接入速度低
ISDN	128k	是	双绞线	电话和数据传输共享，费用较普通电话线稍贵，接入速度稳定但偏低
ADSL	下行 8M 上行 2M	是	双绞线	不干扰普通电话使用，频带专用，接入速度快，非对称传输，频宽受距离限制，费用较高，局端设备较贵
PLC 宽带接入	2 ~ 45M	是	电力线	分布广泛，无需新线，接入方便，共享带宽，费用低，电力线接入部分采用一点对多点结构，与局端连接采用点对点结构，未达到大规模商用阶段，标准不统一
光纤宽带	接入 10G 以上	是	光纤和超五类线缆	用户接入带宽高，可达 10Mbit/s 或 100Mbit/s，可靠性高，性能稳定需要建设完善的光纤网络，建设成本高

与其他接入技术比较，电力线宽带接入网络具有以下优势：

1）充分利用现有的低压配电网络基础设施，无需任何布线。

2）电力线是覆盖范围最广的网络，它的规模是其他任何网络无法比拟的。

3）PLC 能够提供高速的传输，可为用户提供高速互联网访问服务、语音服务，从而为用户上网和打电话增加了新的选择，有利于其他电信服务商改善服务、降低价格。

4）PLC 是家居自动化的主力军。在家里的任何位置，只要连接到房间内的任何电源插座上，就可立即拥有 PLC 带来的高速网络享受。

5）PLC 属于即插即用，不用烦琐的拨号过程，接入电源就等于接入网络。

5.4.5.4　PLC 技术在物联网中的应用案例：智能家庭

1）无线遥控：只要一个遥控器，就可以在家里任何地方遥控家里所有楼上楼下、隔房的灯和电器；而且无需频繁更换各种遥控器，就能实现对多种红外家电的遥控功能；轻按场景按钮，就能轻松实现“会客”“就餐”和“影院”等灯光和电器的组合场景。

2）定时控制：卧室的窗帘准时自动拉开、微波炉（电饭煲）定时烹饪、音响自动关机，轻按门厅口的“全关”键，所有的灯和电器全部熄灭，安防系统自动布防。外出旅游时，可设置主人在家的虚拟场景，防范小偷入侵。

3）互联网传输：国外通过实际网络的实验证明，PLC 可以获得 6MHz 的带宽，在同时传送 3 个低速率或 3 个中等速率多媒体流的情况下没有分组丢失和抖动。PLC 网络除了完成智能家庭中的内部通信外，将来还能不用拨号就可接至互联网。各户的 PLC 网关可以安装在其熔丝盒里。网关可能连接一个或几个用来增强信号强度的中继器。对于低压电力通信技术还有很多需要完善的部分，相信今后还会在家居智能化方面有更大的突破，发展出更多的功能。

综上所述，推进家庭自动化的最现实最经济的途径就是把这项电力线通信技术与网络、微控制器相结合。即以电力线为物理媒介，把分布在住宅各个角落的微控制器和家电 PC 连成一个网络。这样，电力线和信号线合一，无需布设信号线；人们原来使用和维护电器的习惯都不受影响，家电无需增加双绞线、红外等接口，只要在内部配备电力线载波通信芯片，再更新程序就行了，对老式家电的改造也很容易；载波速度慢是电力线通信的一个缺点，但家电的信息量小，就基本上可忽略这一因素。因此电力线载波通信技术就能在家居智能化应用上得以实现，特别是在中速率传输应用方面，因其具有可靠性高、造价低廉优点，可以与“蓝牙”相媲美。

5.5　NGN、NGB、NGI 与三网融合

5.5.1　三网的现状、问题和发展趋势

5.5.1.1　电信网

我国工业和信息化部 2010 年 10 月 21 日发布的数据显示，我国电话用户数已经达到 11.3 亿，其中手机用户达到 8.3 亿，使用固定电话用户总数为 3 亿户。我国的电信网具有以下特点：电路交换网；服务质量保证；恒定、对称的话路量，64kbit/s 带宽，效率低，成本高。

具有了以上特点，电信网拥有一些其他网络无法具备的优势：电信网有强大而覆盖面广的传输网，基本已经完成了城乡完全覆盖；由于电信网起步很早，内部管理严格；具有大型网络设计、运营经验；与用户有长期的服务关系，在计费管理方面有很充足的经验。

但是电信网也存在自身的不足之处，主要问题在于以下几点：

1）我国电话业务还处在大发展阶段，但在 5～10 年内业务量将让位给数据业务。

2）电信的最大资产——铜缆接入网价值与日递减。

3）以 ATM 为基础的 B-ISDN 体系由于 IP 的崛起而失败。

根据以上存在的问题，电信运营商也做出了针对性的策略调整：首先是在体制和概念上

进行转变；其次，进行了电路交换与分组交换之间的转变；而且，引入了宽带接入技术。

5.5.1.2　有线电视网

目前全世界有线电视用户9.4亿，2010年3月21日在2010年CCBN主题报告会上，统计数据显示目前我国有线电视用户数已超过1.74亿，在数量上是美国有线电视用户的2.5倍，是世界第一大规模。主要的优势有：

1）普及率高；电视比电话的普及率更高，每个家庭都拥有一台或者几台电视机。

2）接入带宽最宽；有线电视网网络接入带宽有专门的频段。

3）掌握重要的信息源，且处在高度严格的管制之下。

4）通过Cable Modem用户共享10～30Mbit/s。

5）低廉的包月租费。

6）有利于数字电视的开播。

但是目前我国有线电视网还存在很多问题，目前三网融合的主要问题在于广播电视网络这一领域。主要问题在于：

1）网络分散、各自为政，无统一严格的技术标准和网络规划。

2）基本上没有形成全国网。

3）现有网络多为单向网络，为双向通信必须改造。

4）网络质量较差，可靠性较低。

5）技术上还存在一定问题，并且技术上无国际标准。

6）缺乏通信方面的知识和运行经验，且实力有限。

针对以上问题，为了解决好三网融合这一战略大局，广电网也制定了以下一些策略：首先，需要建立全国性的、统一的SDH网，形成以SDH+HFC+电缆调制解调器为特征的基本框架。然后与IP技术结合，抢占IP市场，再逐步进军电话业务和其他多媒体业务。

5.5.1.3　互联网

互联网作为三网融合的网络主力和依托，是十分重要的一个领域。全世界用户数已超过15亿，我国用户数已超过4亿，2010年第一季度，我国移动互联网用户数目达到2.06亿。互联网本身具有以下一些优势：

1）无连接IP分组交换网形式。

2）效率高，成本低，信令、计费和网管简单，带宽不固定，成本基于带宽或流量，与距离和时间无关。

3）TCP/IP是目前唯一可为三大网络共同接受的通信协议，没有电信铜缆和交换电路的包袱，技术更新块，成本低。以太网已经渗透到接入网、城域网，乃至广域网。

但是互联网也存在很多问题，主要问题有以下几点：

缺乏大型网络与电话业务方面的技术和运行经验；对全网没有有效的控制管理能力；端到端性能无法保障；实时业务质量目前无法保证。

5.5.2　下一代网络

5.5.2.1　NGN的产生

对传统电信网络的改造和升级，以适应新技术和新应用，如怎样处理数据拥塞、怎样增加通信带宽、怎样保证传输质量、怎样对多类终端的综合接入已经成为运营商们所必须面对

的问题。

目前电信业务发展的主要特点：

1）新业务的不断出现，数据业务的快速发展，通信量急剧上升。

2）计算机技术的发展和计算机互联需求的增加，使得基于 IP 和 ATM 的分组交换网日益发展壮大。

3）新的语言压缩技术已经可以将话音信号压缩在低于 64kbit/s 的信道上传输，并已在 IP 电话、移动通信系统中得到广泛的应用。

一方面，传统的电信网络越来越难以适应现代信息交换和传输的需求。另一方面，基于 IP 的网络通信有着惊人的增长速度，IP 业务的高速增长推动着分组交换和传输技术的不断进步，各种光通信技术的应用使得光纤的容量大大的增加，也推动了交换设备的升级。

在这样的一个背景下，下一代的网络（NGN）应运而生，基于 TDM 的 PSTN 电话网和分组交换网融合，形成可以传递包括语音、数据、视频、多媒体信息在内的新一代网络。

5.5.2.2　下一代网络的定义

欧洲电信标准化委员会（European Telecommunication Standards Institute，ETSI）认为：NGN 只是在电信和信息领域用来指代业务基础设施变化的一个代名词，它包括了针对 PSTN/ISDN/GSM Phase 2 以后的所有网络的发展趋势。

国际电联（ITU-T）NGN 标准化小组提出：NGN 应是 PSTN、移动通信网和分组网（ATM/IP）的融合，未来网络应在统一的分组网上支持各种业务。

所谓 NGN 是一个非常松散定义的术语，泛指一个不同于目前一代的、大量采用创新技术、以 IP 为中心，同时可以支持语音、数据和多媒体业务的融合网络。一方面，NGN 不是现有电信网和 IP 网的简单延伸和叠加，而应是两者融合的结果，所涉及的也不仅仅是单项节点技术和网络技术，而是整个网络的框架，是一种整体网络解决方案。另一方面，NGN 的出现和发展不是革命，而是演进，即在继承现有的网络优势基础上实现的平滑过渡。

NGN 主要是以 ATM/IP 特别是 IP 为基础的分组网，然而，从传统的电路交换网到分组网将是一个长期的渐进过程，因而 10～15 年的主要任务是同时支持这两种网络，解决这两网之间的互通以及各自业务和应用的互操作性，在其中，软交换技术将是完成这一过渡的关键技术。

从基础传送网层面来看，以 WDM 为基础的光网络将是理想的大容量网络，然而主要基于点对点通信的 WDM 尽管容量有余，但组网灵活性欠佳，而能实现光层灵活联网功能的光联网将是理想的下一代光网络的传送平台。

总之，NGN 将是以软交换为核心，光联网和分组传送技术为基础的开放式融合网络。

5.5.2.3　NGN 特点

NGN 是可以提供语音、数据、多媒体在内的各种通信业务的综合、开放的网络体系，其主要特征：

- 分组网
- 控制在承载、呼叫/会话和应用/业务之间分离
- 业务提供与网络分离与开放接口的提供分离
- 基于业务模块，提供范围更广的服务
- 具有端到端 QoS 和透明性的带宽能力

■ 通过开放式接口与传统网络互通
■ 通用移动性
■ 用户可以无限制地访问业务提供商
■ 各种不同的识别机制，可以解析到 IP 地址
■ 基于固定和移动的融合业务
■ 业务相关的功能与底层的传输技术无关

1）开放性：划分为几个模块，每个模块能独立发展，互不干涉，又能组成一个整体，部件间的协议接口标准化，有利于设备间，包括异构网的互联互通的问题。

2）业务驱动：业务与呼叫控制分离、呼叫控制与承载控制分离。

通过这两者的分离实现相对独立的业务体系，允许业务与网络独立发展，提供开放的 API，支持不同带宽、实时的或非实时的各种媒体业务的使用，使得业务和应用有较大的灵活性。

3）多用户。NGN 综合了固定电话网、移动电话网和 IP 网络的优势，使得模拟用户、移动用户、ADSL 用户、ISDN 用户、IP 窄带网络用户、IP 宽带网络用户甚至通过卫星接入的用户都能作为 NGN 中的一员相互通信。

4）高性能。NGN 具有高速物理层、链路层和网络层，网络层使用统一的 IP 实现业务融合，链路层趋于采用电信级分组节点，传送层从点对点趋于光联网，提供巨大而廉价的网络带宽和网络成本、可持续发展的网络结构、透明支持任何业务和信号，接入层采用多元化的宽带无缝接入技术，大大提高了用户业务的灵活性和服务质量。

5.5.2.4　NGN 的体系结构

NGN 总体发展方向主要是应用分组化的基础设施，ITU-T 提出了 NGN 的垂直参考配置模型—NGN 体系框架，如图 5-7 所示，按照设备功能可划分为 4 个主要层次：

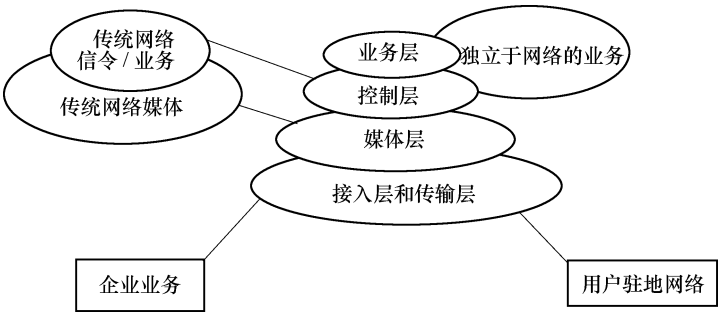


图 5-7　NGN 体系结构

1）接入层和传输层：由媒体网关、各种接入方式组成，媒体网关负责适配语音和其他媒体流到分组传输网。

2）媒体层：负责将各种各样的用户信息格式转换为适合在网络上传输的格式，如将语音信号分割成 ATM 信元或 IP 包。

3）控制层：主要由媒体网关/软交换控制和 IP 业务交换功能组成，完成业务逻辑的具体执行，包含了呼叫控制、资源管理、接续控制和路由等操作，实现各种信令协议的互通和转换，是 NGN 核心和中枢，负责业务功能与呼叫控制的分离，业务功能与承载功能的分离。

4）业务层：负责与各种增值业务控制逻辑相应的网络管理及服务，完成增值业务处理

（业务生成、业务逻辑定义和业务编程接口、业务认证和计费等）。

5.5.2.5　支撑 NGN 的关键技术

以软交换为核心，IP/ATM 为骨干网的 NGN 是一种融合的网络，除软交换技术、媒体网关技术和信令网关技术外，列举几种支撑 NGN 的关键技术。

1）IPv6：扩大了地址空间，提高了网络的整体吞吐量、服务质量，安全性有了更好的保证，支持即插即用和移动性，实现多播功能。

2）宽带接入：VDSL、EPON 等。

3）城域网：城域光网（Metropolitan Optical Network，MON）是基于 WDM，在光层上进行操作的城域网，是一个扩展性非常好的并能适应未来透明、灵活、可靠的平台，可提供动态的、基于标准的多协议支持，同时具有高效配置、高生存能力和综合网络管理的能力。

4）4G 移动通信系统：最高传输速率高达或超过 100Mbit/s；可在不同的接入技术之间进行漫游与互通。

5）IP 终端：开发出适应于多种上网的 IP 终端。

6）网络安全技术：采用强安全性的网络协议（例如 IPv6）；对关键的网元、网站、数据中心设置真正的冗余、分集和保护。

5.5.3　下一代广播电视网

下一代广播电视网（Next Generation Broadcast，NGB）是以自主知识产权技术标准为核心的、可同时传输数字信号和模拟信号的、具备双向交互、组播、推送播存和广播 4 种工作模式的、可管可控可信的、全程全网的宽带交互式网络。

下一代广播电视网采用广播和交换技术相结合的扁平式网络体制，以可保证服务质量的大规模汇聚接入技术为基础，具有开放式业务支撑架构，承载网对业务透明，服务提供机制引入透明计算模式以保证可信度，家庭用户终端的外延形态是智慧家庭网络，家庭物联网是其内在的自然属性。

5.5.3.1　NGB 的架构

NGB 涵盖 3 个部分：业务部分、承载部分和管理部分，如图 5-8 所示。

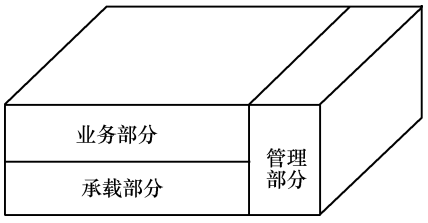


图 5-8　NGB 3 部分

NGB 的业务部分将包含 3 个层次：NGB 业务支撑层、NGB 业务运营层、NGB 业务提供层，如图 5-9 所示。

NGB 的承载部分包括由有线和无线一体化支撑，单向广播和双向交互融合的新型泛在网络。总纵向体系包括 4 个层次：NGB 互通骨干层、NGB 城域骨干层、NGB 接入层、NGB 终端层，如图 5-10 所示。

5.5.3.2　NGB 的功能特点

可漫游：NGB 服务系统可以实现用户在漫游状态下接入广播电视网，并使用与归属地完全一致的服务。

可扩展：NGB 完全基于分布式的架构来构建，在网络承载、业务系统、管理系统方面都可以根据需要进行扩展，足用户数目不断增长和业务及管理需求不断变化的需要。

可运营：NGB 将构建完善的用户管理、运营支撑、互通监管、互通结算等业务运营和

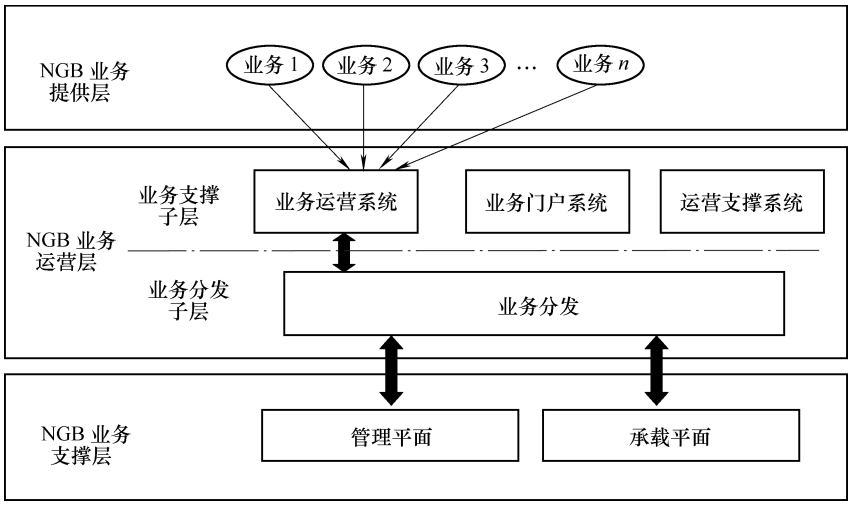


图 5-9　NGB 业务体系结构

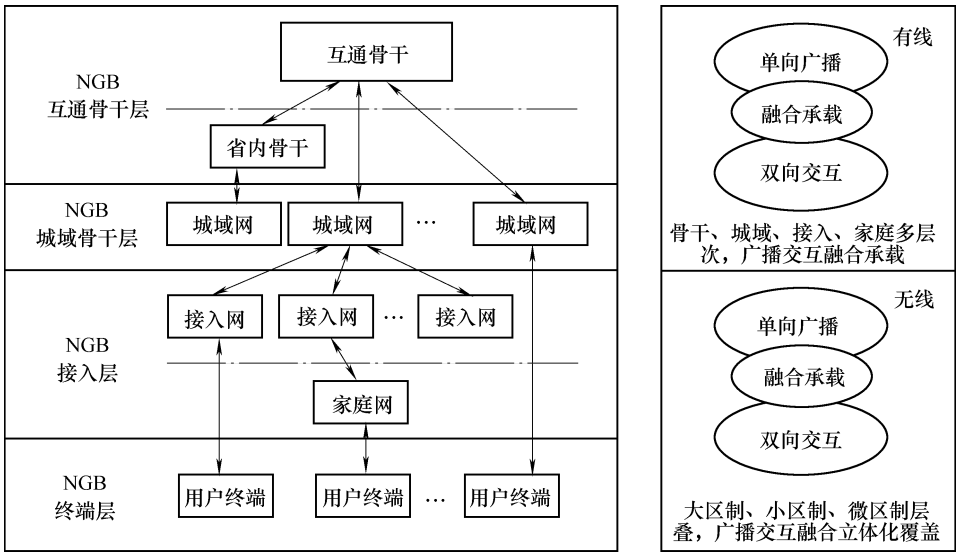


图 5-10　NGB 承载体系结构

运营管理体系，使得广播电视网真正实现可运营。

可联网：NGB 将采用开放的分布式架构，各地的运营网络都可以根据需要进行业务的互联互通，这将有利于自的优势资源，互通有无，并利于实现业务的规模化运营，打造健康的产业环境。

可互通：NGB 还将实现与互联网、通信网等外部网络的互通，在业务融合和互通的基础上实现渐进式发展。

5.5.4　下一代互联网

NGI 是 Next Generation Internet 的缩写，这个由美国克林顿政府支持开发的项目，目标

是将连接速率提高至当时互联网速率的100倍到1000倍。突破网络瓶颈的限制，解决交换机、路由器和局域网络之间的兼容问题。

时至今日，NGI在诸多方面都取得了长足进展，例如无损失及低损失数据压缩技术（MP3与MP4）降低了音、视频信息传输对带宽的需求，速度更快、成本更低的接入技术也大量涌现，从而使Web视频已成为各类新型应用系统及操作系统的常备应用组件之一。下一代互联网协议的IPv6等也为NGI的发展奠定了坚实的基础。IPv6是由互联网工程工作小组研发的最新IP技术，旨在取代已沿用了20年之久的IPv4，它可以大大增加IP地址的数量和安全性能。

5.5.4.1　下一代互联网的三个计划

下一代互联网几个基本计划几乎是并行提出和进行的，它们是：白宫下一代互联网NGI倡议，美国国家科学基金会（NSF）超高带宽网络服务（The Very high-speed Backbone Network Service，VBNS），高等院校与企业合作的Internet 2。

超高带宽网络服务（VBNS）：1995年，美国国家科学基金会就VBNS与美国世界通信公司（MCI）签订5年合作协议，VBNS于1995年4月起投入运行，连接5个超级计算机中心和100所大学及研究机构。到2000年VBNS主干速率将升级到2.5Gbit/s。

Internet 2：1996年10月1日，美国一些科研机构和34所大学代表在芝加哥聚会，提出开发新一代互联网，取名“Internet 2”，以提供高速互联网服务的设想。1997年9月，高级互联网开发合作组成立，以管理Internet 2和帮助其他联合组织。Internet 2的建立不是为取代互联网，也不是为普通用户新建另一个网络，而是用于教育和科研。

白宫下一代互联网：Internet 2提出之后，美国政府随即于10月6日宣布白宫NGI这一多机构倡议。1997年，研究机构已经演示了5种“前期应用”。NGI计划的研究工作主要涉及协议，开发部署、高端试验网以及应用演示。其中某些目标会通过Internet 2或VBNS来实现。NGI计划在3个倡议计划中是最领先的。它的一个关键目标是开发和演示两个试验网，要在端到端的速率方面分别比目前的互联网快100倍和1000倍，即达到100Mbit/s和1Gbit/s。

5.5.4.2　下一代互联网的目标

下一代互联网具有广泛的应用前景，支持医疗保健、国家安全、远程教学、能源研究、生物医学、环境监测、制造工程以及紧急情况下的应急反应和危机管理等，它有直接和应用两个方面目标。

直接目标：

1）使连接各大学和国家实验室的高速网络的传输速率比现有互联网快100～1000倍，其速率可在1s内传输一部大英百科全书。

2）推动下一代互联网技术的实验研究，如研究一些技术使互联网能提供高质量的会议电视等实时服务。

3）开展新的应用以满足国家重点项目的需要。

应用目标：

1）在医疗保健方面要让人们得到最好的诊断医疗，分享医学的最新成果。

2）在教育方面要通过虚拟图书馆和虚拟实验室提高教学质量。

3）在环境监测上通过虚拟世界为各方面提供服务；在工程上通过各种造型系统和模拟

系统缩短新产品的开发时间。

4）在科研方面要通过 NGI 进行大范围的协作，以提高科研效率等。

5.5.5　三网融合与物联网

三网融合技术能够很好地解决物联网中各种问题。通过将电信网络、互联网和广播电视网络技术相互融合，使得三大系统相互兼容，让它们的高层应用业务进行融合，使能够在同一个网络上同时开展语音、数据和视频等多种不同业务。三网融合之后每个网络都能够提供包括语音、数据、图像等综合多媒体的通信业务。三网融合并不是指三大网络的简单的物理合一，而是指三个网络中业务的融合。三网融合的目标是整合各类网络资源，形成具有业务融合能力的网络基础设施。

并且物联网的产业化，需要芯片商、传感设备商、系统解决方案厂商、移动运营商等上下游厂商通力合作，加强广电、电信、交通等部门的合作，是探索未来商业模式的重要切入口。三网融合将是物联网发展以及实现更广泛应用的重大契机和平台，是物联网发展的重要动力，将为打破“行业壁垒”提供示范。

参 考 文 献

[1] 宁祥峰，张春业，万伟，等. 基于 LTE 系统的物联网架构的研究与设计［J］. 计算机应用，2010，30（6）：6-10.

[2] 杜少凤，韩玉楠，王亚峰，等. 物联网体系结构及 LTE-A 在物联网中系统架构的探讨分析［J］. 现代电信科技，2010（8）：61-66.

[3] 曹青. 光通信技术在物联网发展中的应用探讨［J］. 江苏通信，2011（1）：36-38.

[4] 肖净敏. 三网融合中的接入网复用技术的研究［D］. 北京：华北电力大学，2009.

[5] 林学技. 三网融合之接入网技术研究［D］. 北京：北京邮电大学，2010.

[6] 陆治国. 三网融合的实现探究［D］. 青岛：中国海洋大学，2007.

[7] 陈超逸. 基于“三网融合”的中国数字电视发展战略研究［D］. 天津：天津大学，2009.

[8] 徐锦. 多网融合技术研究及其在远程教育系统中的应用［D］. 杭州：浙江工业大学，2008.

[9] 刘继军. 国内电力载波通信芯片技术及市场［J］. 电器工业，2010（12）：61-65.

[10] 周霞. 基于电力载波通信的物联网应用研究［J］. 数字技术与应用，2010（9）：4.

[11] 张瑞玲，皇甫昱. 电力线通信（PLC）技术应用研究［J］. 商丘职业技术学院学报，2007，29（6）：62-64.

[12] 刘爱军，王向军，刘雁征. 电力线通信在智能家庭中的应用［J］. 商业文化，2008（11）：129.

[13] 刘应华，刘桥. 智能电网中宽带电力线通信技术的研究［J］. 科技信息，2010（34）：421.

第 6 章　支撑及应用技术

物联网支撑技术包括中间件技术、对象名称解析服务（Object Name Service，ONS）、实体标记语言（Physical Markup Language，PML）、智能技术和云计算等技术。

中间件技术：中间件系统是位于感知设备和物联网应用之间，可以对感知设备采集的数据进行校对、过滤、汇集等处理过程，有效地减少发送到应用程序的数据的冗余度以及提高数据的正确性，在物联网中起着很重要的作用。

对象名称解析服务：对象名称解析服务（ONS）将一个 EPC 映射到一个或者多个 IP/URI，在这些 IP/URI 中可以查找到关于这个物品的更多的详细信息，通常对应这一个 EPCIS。ONS 是联系前台中间件软件和后台 EPCIS 服务器的网络枢纽。运行在本地服务器中的 ONS 帮助本地服务器吸收标签读写器侦测到的全球信息，而且还可以将 EPC 关联到这些物品相关的 Web 站点或者其他互联网资源。

实体标记语言：它将为工商业中的软件开发、数据存储和分析工具提供一个描述自然实体、过程和环境的标准化方法，并能够提供一种动态的环境，使与物体相关的静态的、暂态的、动态的和统计加工过的数据在此环境中可以交换。PML 可广泛应用在存货跟踪、事务自动处理、供应链管理、机器操纵和物对物通信等方面，在物联网中扮演着重要的角色。

嵌入式智能：嵌入式智能系统是集软硬件于一体的、可独立工作的计算机系统，在物联网的一些应用场景中，需要一些传感器实现对周围环境和监测目标的自动化监测和控制，这就需要嵌入式智能来实现。

云计算：从信息和设备的量化方面来看，物联网使用了数量惊人的传感器，采集到惊人的数据量，通过无线传感器网络、宽带互联网进行传输和汇聚；从质的方面来看，使用了海量数据存储设施、高性能的处理设施和先进的处理算法对这些数据进行处理分析、挖掘，从而可以更加迅速、准确、智能地对物理世界进行管理和控制。因此，人们可以更加精细、动态地管理生产和生活，达到智能的状态，提高资源利用率和生产力水平。可以看出，云计算凭借其强大的处理能力、存储能力和极高的性能价格比，很自然地就会成为物联网的后台支撑平台。

6.1　中间件

当代计算机技术发展迅速，同时各种各样的应用软件需要在不同的应用平台之间进行移植，或者多种应用软件在一个平台下协同工作，这就需要保证平台和应用系统之间数据传递的可靠性、高效性，同时保证系统的协同性。为了实现这个要求，我们需要一种基于软硬件平台，对高层应用软件进行支持的软件系统，中间件技术就是在这个大环境下应运而生。

6.1.1　中间件的概念

中间件是位于平台（操作系统和硬件）和应用程序之间的通用服务，针对不同的操作

系统和硬件平台，它们可以有符合接口和协议规范的多种实现。除了操作系统、数据库外，凡是能批量生产、高度复用的软件都算是中间件。国际商业机器（IBM）公司、Oracle 公司和微软公司等都是引领中间件潮流的生产商；SAP 公司等大型企业资源计划（ERP）应用软件厂商的产品也是基于中间件架构的；国内的用友软件股份有限公司、金蝶国际软件集团有限公司等软件厂商也都有中间件部门或者分公司。欧洲联盟 Hydra 物联网中间件计划的技术框架，值得我们国内借鉴。具体讲，中间件屏蔽了底层操作系统的复杂性，使程序开发人员面对一个简单而又统一的开发环境，减少了程序设计的复杂性，将注意力集中在自己的业务上，不必再为程序在不同软件的一致性而重复地工作，从而大大减少了技术上的负担。中间件技术具有以下特点：满足大量应用的需要；运行于多种硬件和 OS 平台；支持分布式计算，提供跨网络、硬件和 OS 平台的透明性的应用或者服务的交互功能；支持标准协议。

6.1.2　中间件的发展现状及分类

6.1.2.1　国内外中间件的发展现状

在包括物联网软件在内的软件领域，美国长期引领潮流，基本上垄断了世界市场，欧洲联盟早已看到了软件和中间件在物联网产业链中的重要性，从 2005 年开始资助 Hydra 项目，这是一个研发物联网中间件和“网络化嵌入式系统软件”的组织，已取得不少成果。目前在我国有很多传感器、传感网、RFID 研究中心及产业（生产）基地，也有很多人呼吁建立物联网标准，唯独没有物联网软件和中间件研发基地和组织，这种现象令人忧虑，如果我国的物联网集成软件技术一直处于滞后的状况，必将影响我国物联网战略的实施。中央提出了重点发展软件产业和电子芯片产业，明确将软件产业列为战略性新兴产业，这也为发展我国的物联网中间件提供了机遇。国内的物联网技术应用处于刚起步阶段，成功的应用案例比较少见，相比国外存在着比较大的差距。虽然我国的物联网产业有政府的大力宣传和扶持，成立了以无锡为代表的物联网技术研发基地，但物联网的整个产业链还没完全形成，尤其是在物联网应用集成技术方面还很薄弱。物联网作为一个汇集了数据采集、数据传输、数据处理、业务应用技术的集成化概念，其应用的关键问题也是集成问题，通过有效的技术集成将上述各层次的技术整合在一起，形成完整的数据采集、数据传输、数据处理、数据应用通道，才能实现物联网的真正应用。深圳远望谷信息技术股份有限公司和 IBM 公司联手开发了 RFID 中间件适配层软件，青岛海尔集团、南京瑞福智能科技有限公司也做过这方面的尝试。

6.1.2.2　中间件的分类

中间件所包括的范围十分广泛，针对不同的应用需求涌现出多种各具特色的中间件产品。但至今中间件还没有一个比较精确的定义，因此，在不同的角度或不同的层次上，对中间件的分类也会有所不同。由于中间件需要屏蔽分布环境中异构的操作系统和网络协议，它必须能够提供分布环境下的通信服务，我们将这种通信服务称之为平台。基于目的和实现机制的不同，我们将平台分为以下主要几类：远程过程调用中间件；面向消息中间件；对象请求代理中间件；事务处理监控中间件。

它们可向上提供不同形式的通信服务，包括同步、排队、订阅发布、广播等，在这些基本的通信平台之上，可构筑各种框架，为应用程序提供不同领域内的服务，如事务处理监控

器、分布数据访问、对象事务管理器（Object Transaction Manager，OTM）等。平台为上层应用屏蔽了异构平台的差异，而其上的框架又定义了相应领域内的应用的系统结构、标准的服务组件等，用户只需告诉框架所关心的事件，然后提供处理这些事件的代码。当事件发生时，框架则会调用用户的代码。用户代码不用调用框架，用户程序也不必关心框架结构、执行流程、对系统级 API 的调用等，所有这些由框架负责完成。因此，基于中间件开发的应用具有良好的可扩充性、易管理性、高可用性和可移植性。

1. 远程过程调用中间件

远程过程调用是一种广泛使用的分布式应用程序处理方法。一个应用程序使用 RPC 来“远程”执行一个位于不同地址空间里的过程，并且从效果上看和执行本地调用相同。事实上，一个 RPC 应用分为两个部分：server 和 client。server 提供一个或多个远程过程；client 向 server 发出远程调用。server 和 client 可以位于同一台计算机，也可以位于不同的计算机，甚至运行在不同的操作系统之上。它们通过网络进行通信。相应的 stub 和运行支持提供数据转换和通信服务，从而屏蔽不同的操作系统和网络协议。在这里 RPC 通信是同步的。采用线程可以进行异步调用。

在 RPC 模型中，client 和 server 只要具备了相应的 RPC 接口，并且具有 RPC 运行支持，就可以完成相应的互操作，而不必限制于特定的 server。因此，RPC 为 client/server 分布式计算提供了有力的支持。同时，远程过程调用 RPC 所提供的是基于过程的服务访问，client 与 server 进行直接连接，没有中间机构来处理请求，因此也具有一定的局限性。比如，RPC 通常需要一些网络细节以定位 server；在 client 发出请求的同时，要求 server 必须是活动的等。

2. 面向消息中间件

MOM 指的是利用高效可靠的消息传递机制进行平台无关的数据交流，并基于数据通信来进行分布式系统的集成。通过提供消息传递和消息排队模型，它可在分布环境下扩展进程间的通信，并支持多通信协议、语言、应用程序、硬件和软件平台。目前流行的 MOM 中间件产品有 IBM 的 MQSeries、BEA 的 MessageQ 等。消息传递和排队技术有以下 3 个主要特点：

1）通信程序可在不同的时间运行：程序不在网络上直接相互通话，而是间接地将消息放入消息队列，因为程序间没有直接的联系，所以它们不必同时运行。消息放入适当的队列时，目标程序甚至根本不需要正在运行；即使目标程序在运行，也不意味着要立即处理该消息。

2）对应用程序的结构没有约束：在复杂的应用场合中，通信程序之间不仅可以是一对一的关系，还可以是一对多和多对一方式，甚至是上述多种方式的组合。多种通信方式的构造并没有增加应用程序的复杂性。

3）程序与网络复杂性相隔离：程序将消息放入消息队列或从消息队列中取出消息来进行通信，与此关联的全部活动，比如维护消息队列、维护程序和队列之间的关系、处理网络的重新启动和在网络中移动消息等是 MOM 的任务，程序不直接与其他程序通话，并且它们不涉及网络通信的复杂性。

3. 对象请求代理中间件

随着对象技术与分布式计算技术的发展，两者相互结合形成了分布对象计算，并发展为当今软件技术的主流方向。1990 年底，对象管理集团 OMG 首次推出对象管理结构（Object

Management Architecture，OMA），对象请求代理（ORB）是这个模型的核心组件。它的作用在于提供一个通信框架，透明地在异构的分布计算环境中传递对象请求。CORBA 规范包括了 ORB 的所有标准接口。1991 年推出的 CORBA 1.1 定义了接口描述语言 OMG IDL 和支持 client/server 对象在具体的 ORB 上进行互操作的 API。CORBA 2.0 规范描述的是不同厂商提供的 ORB 之间的互操作。

ORB 是对象总线，它在 CORBA 规范中处于核心地位，定义异构环境下对象透明地发送请求和接收响应的基本机制，是建立对象之间 client/server 关系的中间件。ORB 拦截请求调用，并负责找到可以实现请求的对象、传送参数、调用相应的方法、返回结果等。client 对象并不知道同 server 对象通信、激活或存储 server 对象的机制，也不必知道 server 对象位于何处、它是用何种语言实现的、使用什么操作系统或其他不属于对象接口的系统成分。

值得指出的是 client 和 server 角色只是用来协调对象之间的相互作用，根据相应的场合，ORB 上的对象可以是 client，也可以是 server，甚至兼有两者。当对象发出一个请求时，它是处于 client 角色；当它在接收请求时，它就处于 server 角色。大部分的对象都是既扮演 client 角色又扮演 server 角色。另外由于 ORB 负责对象请求的传送和 server 的管理，client 和 server 之间并不直接连接，因此，与 RPC 所支持的单纯的 client/server 结构相比，ORB 可以支持更加复杂的结构。

4. 事务处理监控中间件

事务处理监控（TPM）最早出现在大型机上，为其提供支持大规模事务处理的可靠运行环境。随着分布计算技术的发展，分布应用系统对大规模的事务处理提出了需求，比如商业活动中大量的关键事务处理。事务处理监控介于 client 和 server 之间，进行事务管理与协调、负载平衡、失败恢复等，以提高系统的整体性能。它可以被看作是事务处理应用程序的“操作系统”。总体上来说，事务处理监控有以下功能：

1）进程管理，包括启动 server 进程、为其分配任务、监控其执行并对负载进行平衡。

2）事务管理，即保证在其监控下的事务处理的原则性、一致性、独立性和持久性。

3）通信管理，为 client 和 server 之间提供了多种通信机制，包括请求响应、会话、排队、订阅发布和广播等。

事务处理监控能够为大量的 client 提供服务，比如飞机订票系统。如果 server 为每一个 client 都分配其所需要的资源的话，那么 server 将不堪重负。但实际上，在同一时刻并不是所有的 client 都需要请求服务，而一旦某个 client 请求了服务，它希望得到快速的响应。事务处理监控在操作系统之上提供一组服务，对 client 请求进行管理并为其分配相应的服务进程，使 server 在有限的系统资源下能够高效地为大规模的客户提供服务。

根据应用对象的不同，中间件还可以分为 RFID 中间件、嵌入式中间件、数字电视中间件、通用中间件、M2M 物联网中间件等。

6.1.3 中间件技术在物联网中的应用

物联网中间件是业务应用程序和底层数据获取设备之间的桥梁，它是封装数据管理、设备管理、事件管理的中心，是物联网应用集成的核心部件，所以在物联网产业链中占有重要的地位。目前，物联网中间件最主要的代表是 RFID 中间件，其他的还有嵌入式中间件、数字电视中间件、通用中间件、M2M 物联网中间件等。下面重点介绍一下 RFID 中间件。

物联网的中间件处于物联网的集成服务器端或者感知层、传输层的嵌入式设备中。服务器端中间件成为物联网业务基础中间件，一般都是基于传统的中间件（应用服务器、ESB/MQ 等）构建，加入设备连接和图形化组态展示等模块；嵌入式中间件是一些支持不同通信协议的模块和运行环境。中间件的特点在于它固化了很多通用的功能，但在具体的应用中多半需要二次开发来实现个性化的行业业务需求，因此所有物联网中间件都提供了快速开发（Rapid Application Develop，RAD）工具。

6.1.3.1　RFID 中间件

物联网是把所有的物体通过各种网络连接起来，实现任何物体、任何人、任何时间、任何地点的智能化识别、信息交换与管理。从技术架构上来看，物联网可分为感知层、网络层、应用层。在这里中间件平台实现各种传感器和 RFID 硬件设备与应用系统之间数据传输、过滤、数据格式转换的一种中间程序，它降低了应用开发的难度，使得开发者不需要直接按面对底层架构，而通过中间件进行调用。在物联网中，软件是灵魂，中间件技术就是灵魂的核心。

如图 6-1 所示为 EPC 物联网系统，EPC 系统是一个非常先进、综合和复杂的系统，其最终目标是为每一个单品建立全球的、开放的标识标准。它主要由 EPC 标签、读写器、SAVANT（RFID 中间件）、对象名解析服务（ONS）、信息服务（EPCIS）5 部分组成。而物联网中的中间件 SAVANT 在架构中起着关键部件的作用，SAVANT 扮演 RFID 标签和应用程序之间的中介角色，从应用程序端使用中间件所提供一组通用的应用程序接口（Application Programming Interface，API），即能连到 RFID 读写器，读取 RFID 标签数据。这样一来，即使存储 RFID 标签数据的数据库软件或后端应用程序增加或改由其他软件取代，或者读写 RFID 读写器种类增加等情况发生时，应用端不需修改也能处理，省去多对多连接的维护复杂性问题。由此可见，SAVANT 是衔接相关硬件设备和业务应用的桥梁，主要实现屏蔽异构性、实现互操作和信息的预处理等。

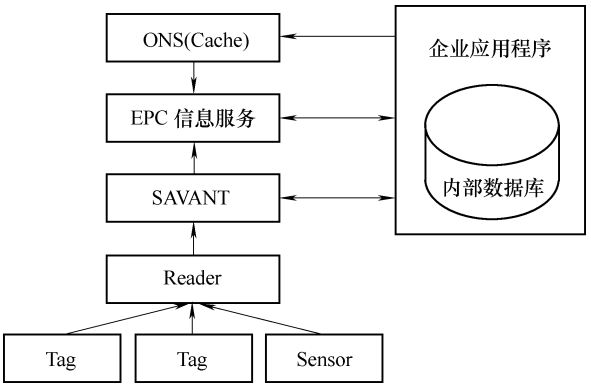


图 6-1　物联网网络结构

（1）屏蔽异构性

异构性表现在计算机的软硬件之间的异构性，包括硬件（CPU 和指令集、硬件结构、驱动程序等）、操作系统（不同操作系统的 API 和开发环境）、数据库（不同的存储和访问格式）等。造成异构的原因源自市场竞争、技术升级以及保护投资等因素。物联网中的异构性主要体现在以下几方面：

1）物联网中底层的信息采集设备种类众多，如传感器、RFID、二维码、摄像头以及 GPS 等，这些信息采集设备及其网关拥有不同的硬件结构、驱动程序、操作系统等。

2）不同的设备所采集的数据格式不同，这就需要中间件将所有这些数据进行格式转化，以便应用系统可直接处理这些数据。

（2）实现互操作

在物联网中，同一个信息采集设备所采集的信息可能要供给多个应用系统，不同的应用系统之间的数据也需要相互共享和互通。但是因为异构性，不同应用系统所产生的数据结果取决于计算环境，使得各种不同软件之间在不同平台之间不能移植，或者移植非常困难。而且，因为网络协议和通信机制的不同，这些系统之间还不能有效地相互集成。通过中间件可建立一个通用平台，实现各应用系统、应用平台之间的互操作。

（3）数据的预处理

物联网的感知层将采集海量的信息，如果把这些信息直接传输给应用系统，那么应用系统对于处理这些信息将不堪重负，甚至面临崩溃的危险。而且应用系统想要得到的并不是这些原始数据，而是对其有意义的综合性信息。这就需要中间件平台将这些海量信息进行过滤，融合成有意义的事件再传给应用系统。

SAVANT是一个物联网中的中间件，它的主要作用是用来加工和处理来自一个或者多个解读器的所有信息和事件流，它是处在阅读器和计算机互联网之间的一种中间件系统，对标签解读器和企业应用程序的连接起着纽带的作用，代表应用程序提供一系列的计算功能。为了减少发往信息网络系统的数据量以及防止错误识读、漏读或者多读信息，SAVANT会对标签数据进行过滤、分组、计数。中间件（SAVANT）是物联网的神经系统，是一种企业通用的管理EPC数据架构。它可以被灵活地安装在商店、本地配送中心，区域或者全国范围内的数据中心，来实现对数据的捕获、监控和传送，减少从阅读器传往工厂应用的数据量。这种分布式的结构可以简化物联网管理，提高运行效率。同时，中间件还可提供与其他RFID支撑软件系统进行互操作等功能。此外，中间件还定义了阅读器和应用两个接口。中间件如图6-2所示。

中间件应该具备两个关键特征：首先要为上层的应用层服务，这是一个基本条件；此外，又必须连接到操作系统的层面，并且保持运行工作状态。中间件研究的领域和范围很广，涉及多个行业，也涉及多个不同的研究方向，比如应用服务器、应用集成架构与技术、门户技术、工作流技术、企业级应用基础软件平台体系架构、移动中间件技术和物联网中间件技术等领域。

1. RFID中间件（SAVANT）的组成

通常情况下，物联网中的中间件具有的模块包括读写器接口、事件管理器、应用程序接口、目标信息服务和对象名解析服务等，如图6-3所示。

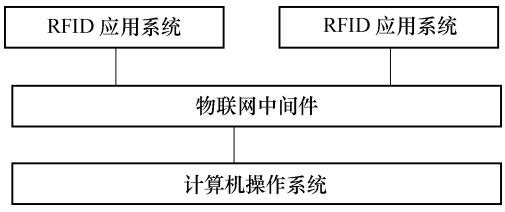


图6-2　中间件示意图

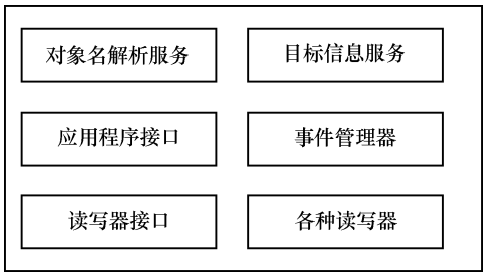


图6-3　物联网中间件模块结构

各个模块描述如下：

1）读写器接口：物联网中间件需要具备集成各种形式的读写器的功能。协议处理器确保使中间件能够通过各种网络方案连接到 RFID 读写器，作为 RFID 标准化制定主体的 EPC-global 组织负责制定并推广描述 RFID 读写器与应用程序间通过普通接口相互作用的规范。

2）事件管理器：事件管理器用来对来自于读写器接口的 RFID 时间数据进行过滤、聚合和排序的操作，并且再通告数据与外部系统相关联的内容。

3）应用程序接口：应用程序接口的作用是使外部应用程序系统能够控制读写器。服务器端的接收器接收应用程序的系统指令，它提供一些通信功能。

4）目标信息服务：目标信息服务由两个部分组成：一个是目标存储库，用于存储于标签物体有关的信息，使得这些信息用于以后的查询；另一个是为目标存储库提供目标存储管理的信息接口服务引擎。

5）对象名解析服务：对象名解析服务是一种目录服务，它能使每个带标签产品分配的唯一编码与一个或者多个拥有关于产品更多信息的目标信息服务的网络定位地址相匹配。

2. RFID 中间件（SAVANT）的主要功能

中间件的主要功能是数据过滤、数据聚合、信息传递，具体介绍如下。

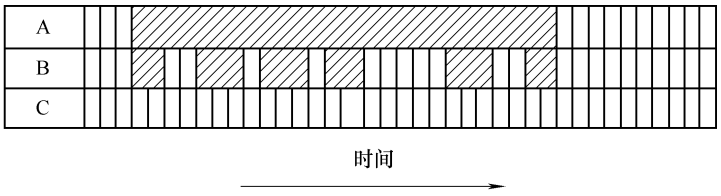
（1）数据过滤

SAVANT 接收来自读写器的海量 EPC 数据，这些数据存在大量的冗余信息，并且也存在一些错读的信息。所以要对数据进行过滤，消除冗余数据，过滤掉“无用”信息以便传送给应用程序或上级 SAVANT“有用”的信息。冗余数据包括在短期内同一台读写器对同一个数据进行重复上报，如在仓储管理中，对固定不动的货物重复上报，在进货、出货的过程中，重复检测到相同物品；多台临近的读写器对相同数据都进行上报，读写器存在一定的漏检率，这和阅读器天线的摆放位置、物品离阅读器远近、物品的质地都有关系。通常为了保证读取率，可能会在同一个地方相邻摆放多台阅读器，这样多台读写器将监测到的物品上报时，可能会出现重复。除上述问题外，很多情况下用户可能还希望得到某些特定货物的信息、新出现的货物信息、消失的货物信息或者只是某些地方的读写器读到的货物信息。用户在使用数据时，希望最小化冗余，尽量得到靠近需求的准确数据，这就要靠 SAVANT 来解决。对于冗余信息的解决办法是设置各种过滤器处理。可用的过滤器有很多种，典型的过滤器有 4 种：产品过滤器、时间过滤器、EPC 码过滤器和平滑过滤器。产品过滤器只发送与某一产品或制造商相关的产品信息，也就是说，过滤器只发送某一范围或方式的 EPC 数据。时间过滤器可以根据时间记录来过滤事件，例如，一个时间过滤器可能只发送最近 10min 内的事件。EPC 码过滤器可以只发送符合某个规则的 EPC 码。平滑过滤器负责处理那些出错的情况，包括漏读和错读。根据实际需要过滤器可以像拼装玩具一样被一个接一个地拼接起来，以获得期望的事件。例如，一个平滑过滤器可以和一个产品过滤器结合，将对反盗窃应用程序感兴趣的事件分离出来。

（2）数据聚合

从读写器接收的原始 RFID 数据流都是些简单零散的单一信息，为了给应用程序或者其他的 RFID 中间件提供有意义的信息，需要对 RFID 数据进行聚合处理。可以采用复杂事件处理（Complex Event Processing，CEP）技术来对 RFID 数据进行处理以得到有意义的事件信

息。复杂事件处理是一个新兴的技术领域，用于处理大量的简单事件，并从其中整理出有价值的事件，可帮助人们通过分析诸如此类的简单事件，并通过推断得出复杂事件，把简单事件转化为有价值的事件，从中获取可操作的信息。在这里，利用数据聚合将原始的 RFID 数据流简化成更有意义的复杂事件，如一个标签在读写器识读范围内的首次出现及它随后的消失，如图 6-4 所示。通过分析一定数量的简单数据就可以判断标签进入事件和离开事件。聚合可以用来解决临时错误读取所带来的问题从而实现数据平滑。聚合类型见表 6-1。



说明：A 行画面的斜线部分显示了当待检测标签被人放入阅读器范围后理论上能够被检测到的时间段。B 行的画面斜线部分则显示了读写器检测到标签的实际时间段。C 行显示了假定的标签状态及到达和离开时间

图 6-4　进入事件、离开事件示意图

表 6-1　聚合类型

聚 合 类 型	描　　述
进入离开	这种类型的聚合将对标签一定数量的读取，简化标签进入和离开识读范围
计数	只记录范围内有多少标签数据而不关心标签的具体内容
通道	标签是否要通过某个位置，如 door
虚拟读写器	几个读写器之间可以通过组合形成一个虚拟读写器，当这几个读写器读入数据时只需记录一次

（3）信息传递

经过过滤和聚合处理后的 RFID 数据需要传递给那些对它感兴趣的实体，如企业应用程序、EPC 信息服务系统或者其他 RFID 中间件，这里采用消息服务机制来传递 RFID 信息。RFID 中间件是一种面向消息（MOM）的中间件，信息以消息的形式从一个程序传送到另一个或多个程序。信息可以以异步的方式传送，所以传送者不必等待回应。面向消息的中间件包含的功能不仅是传递信息，还必须包括解释数据、安全性、数据广播、错误恢复、定位网络资源、找出符合成本的路径、消息与要求的优先次序以及延伸的除错工具等服务。通过 J2EE 平台中的 Java 消息服务（JMS）实现 RFID 中间件与企业应用程序或者其他 SAVANT 的消息传递的结构如图 6-5 所示。这里采用 JMS 的发布/订阅模式，RFID 中间件发布给一个主题发布消息，企业应用程序和其他的一个或者多个 SAVANT 都可以订购该主题消息。其中的消息是物联网的专用语言——物理标记语言（PML）格式。这样一来，即使存储 RFID 标签信息的数据库软件或增加后端应用程序或改由其他软件取代，或者增加 RFID 读写器种类等情况发生，应用端都不需要修改也能进行数据的处理，省去了多对多连接的维护复杂性问题。

3. RFID 中间件（SAVANT）体系结构

在实际应用中，我们给每件产品加上 RFID 标签后，在产品的生产、运输和销售过

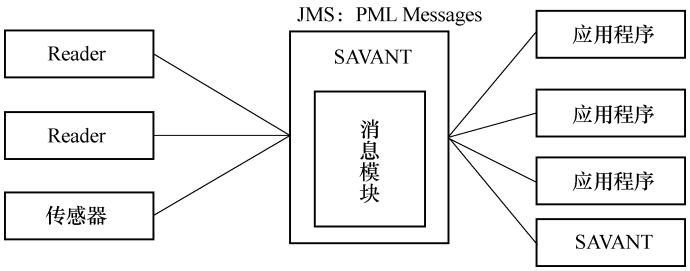


图 6-5　SAVANT 消息传递结构

程中，不同地理位置的读写器将会不停地采集到产品电子编码的数据流，SAVANT 位于读写器和信息网络的中间位置，处理来自读写器获得的所有信息和事件流。Auto-ID 中心提出的 SAVANT 的技术体系结构是一种通用的管理 EPC 数据的架构，它是具有一系列特定属性的“程序模块”或者“服务”，并且被集成在一起来满足不同用户的特定需求。这些程序模块设计可以支持不同群体对模块的扩展。SAVANT 连接标签识读器和企业应用程序，代表着应用程序提供一系列的计算功能，如在将数据送往应用系统之前，需要过滤、汇总、计算标签数据，压缩数据容量，减少网络流量。SAVANT 向上层转发它所关注的某些事件或者事件摘要，并且能够有效地防止错误识读、漏读和重读。由于不同的客户应用程序对 EPC 处理的需求各不相同，为了应对应用程序的各种改进和变动，SAVANT 的构造中除了包含标准的模块外，还具有某些特定的程序模块或者服务，以供用户集成并满足他们的具体需求。图 6-6 描述了 SAVANT 的组件与其他应用程序的通信状况。

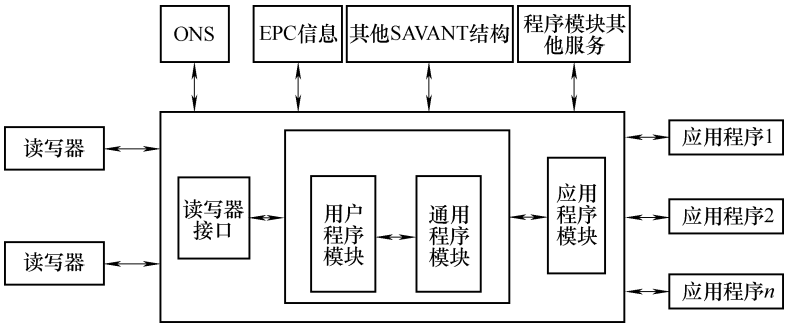


图 6-6　SAVANT 体系结构

SAVANT 为程序模块的集成器，程序模块通过两个接口与外界交互：读写器和应用程序接口。其中读写器接口提供与 RFID 读写器的连接方法；应用程序接口将 SAVANT 和外部应用程序链接起来，这些应用程序通常是现有的企业运行的应用系统程序，或为新的 EPC 应用程序，或为其他的 SAVANT 系统。应用程序接口是程序模块与外部应用的通用接口，在必要时，应用程序接口能采用 SAVANT 服务器本地协议与以前的扩展服务进行通信，或者采用与读写器协议类似的分层方法实现，其中高层定义命令与抽象语法底层实现了具体语法与协议的绑定。除了 SAVANT 定义的两个外部接口（读写器接口和应用程序接口）外，程序模块之间用它们自己定义的 API 函数交互。

SAVANT通常安装在商店、仓库、制造车间、运输车辆、本地配送中心、区域乃至全国性的数据中心，以实现对数据的捕获、监控和传送。典型的EPC SAVANT系统呈树形结构，现存在的一种典型的中间件（SAVANT）系统架构如图6-7所示。

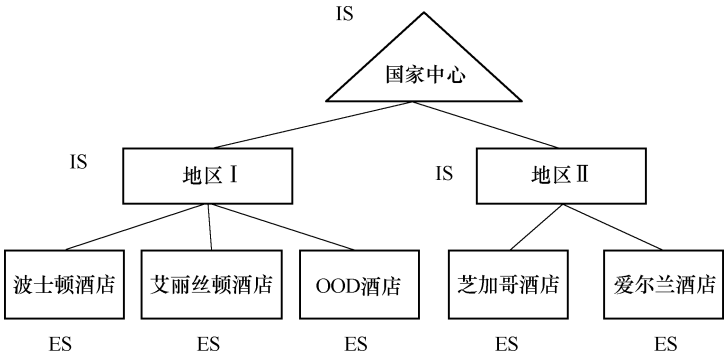


图6-7　SAVANT的系统架构

这种结构的叶节点叫作Edge SAVANT（ES），树的分支节点叫作Internal SAVANT（IS）。“ES”由它们在网络中的逻辑位置而得名，它们始终处在SAVANT分布式网络结构的最底层，EPC数据只有通过ES才能进入物联网的系统中。它直接与RFID读写器连接，从标签中采集EPC数据，连续地捕获、监视存储数据，并且向其他的EPC SAVANT传送。每次识读EPC SAVANT都要保存一些信息，例如标签的EPC码、扫描标签的读写器码、识读时间以及与EPC不相关的一些信息，如读写器的地理位置和观测到的温度等。在EPC SAVANT的逻辑等级中“IS”指内部节点，是“ES的父节点或者上级”，它除了从下属节点采集数据外，还负责EPC的数据合计。

SAVNAT的程序模块可以由Auto-ID标准委员会定义，或者由用户和第三方生产商来定义。Auto-ID标准委员会定义的模块叫作标准程序模块。这些标准模块需要应用在SAVANT的所有应用实例中。其他模块可以根据用户定义包含或者不包含在一些具体实例中，这些叫作可选程序模块。主要介绍3个必需的标准程序模块：事件管理系统（Event Management System，EMS）、实时内存事件数据库（Real-time In-Memory Event Database，RIED）和任务管理系统（Task Management System，TMS）。

（1）事件管理系统（EMS）

EMS配置在“ES”端，用于收集读取的标签信息，其主要功能是：

1）能够允许不同类型的读写器将信息写入到适配器；

2）从读写器收集标准格式的EPC数据；

3）允许过滤器对EPC数据进行过滤处理；

4）将处理后的数据写入RIED或本地数据库，或通过HTTP/JMS/SOAP广播到远程服务器。

对事件进行缓冲，使得数据记录器，数据过滤器和适配器能够互不干扰地工作。当事件产生并传递给适配器后，被编入一个队列，从这个队列，事件自动转寄到过滤器，根据不同过滤器的定义，将不同的事件过滤出来，如时间过滤器只允许特定时间标记的事件通过。数据记录器将事件存储到数据库或者将事件传递到某种网络连接，如Socket、http等。图6-8示意了一个EMS中不同类型的读写器、队列、不同类型的过滤器和不同类型的记录器系统

工作过程。

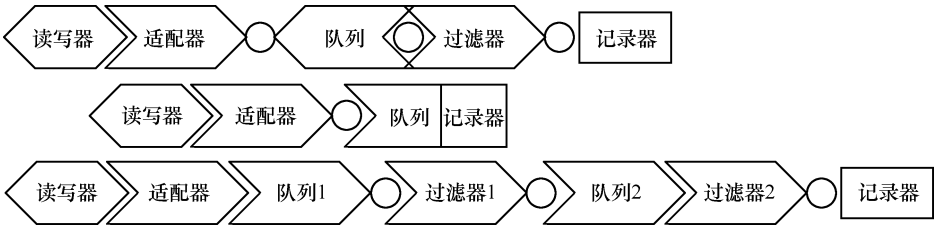


图 6-8　SAVANT 事件处理过程

（2）实时内存事件数据库（RIED）

它是 SAVANT 特有的一种存储容器和优化的数据库，为满足 SAVANT 在逻辑网络中的数据传输速度要求而设立，用以存储“边缘 EPC SAVANT”的事件信息，维护来自读写器的信息，并提供过滤和提供记录时间的框架。记录器要将事件记录到数据库，但数据库通常不能在 1s 内处理上千个事物，因此需要由 RIED 提供与数据库通信的接口，以解决访问速度匹配。应用程序一般使用 JDBC 或用本地接口访问 RIED。RIED 提供诸如 SELECT、UPDATE、INSERT、DELETE 等 SQL 操作，支持定义在 SQL92 中的子集，RIED 同时还提供快照功能，以维护数据库不同时间的数据快照。RIED 的模型如图 6-9 所示，由 8 个组件构成。

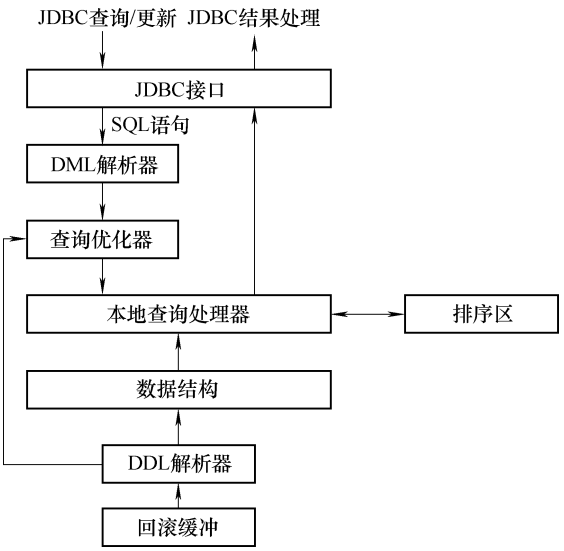


图 6-9　RIED 的模型图

1）JDBC 接口：使远程的机器能使用标准的 SQL 查询访问 RIED，并使用标准的 URL 定位 RIED；

2）DML 解析器：解析 SQL 数据修改语言，包括标准 SQL 命令，是整个 SQL92 DML 规范的子集；

3）查询优化器：将 DML 解析器的输出转化为 RIED 可查询的执行计划，定义的搜索路径用来找到一个有效的执行计划；

4）本地查询处理器：处理直接来自应用程序（或 SQL 解析器）的执行计划；

5）排序区：为本地查询处理器执行排序、分组和连接操作，采用哈希表来进行链接和分组操作，使用高效排序算法进行排序操作；

6）数据结构：采用“有效线程安全持久数据结构”来存储不同的数据快照，该数据结构实现持久创建新的数据快照，这种数据结构在 RIED 的实时操作中是必需的；

7）DDL 解析器：DDL 解析器处理计划定义文档和初始化内存模型中的不同数据结构，还提供查找定义在 DDL 中的查询路径功能；

8）回滚缓冲：RIED 中执行的事物可提交或者回滚，该缓冲保持所有更新直至事物提交。

（3）任务管理系统（TMS）

EPC SAVANT 使用定制的任务来执行数据管理和数据监控，通常，一个任务可被看作多任务系统的一个线程，TMS 的功能恰似操作系统的任务管理，它把由外部应用程序定制的任务转为 SAVANT 可执行的程序，写入任务进度表，使 SAVANT 具有多任务执行功能。SAVANT 支持的任务有 3 种类型：一次性任务、循环性任务和永久性任务。

另外，TMS 还要提供通常多任务操作系统所不具有的特性。如：

1）具有时间段任务的外部接口；

2）从冗余的类服务器中随机选择加载 Java 虚拟机的类库；

3）调度程序维护任务的持久化信息数据，在 SAVANT 瘫痪或任务瘫痪后能实现重启。

TMS 简化了分布式 EPC SAVANT 的维护。企业用户只需通过保障类服务器上的任务的更新及与更新相关 SAVANT 上的调度任务，就可维护 EPC SAVANT，但硬件和核心软件必须定期更新，如 OS（Operating System）和 Java 虚拟机。

为 TMS 编写的任务可访问所有 EPC SAVANT 的工具。TMS 任务可执行各种企业应用操作，如数据收集，发送或收集另一 EPC SAVANT 的产品信息；PML 查询，查询 ONS、PML 服务器随机动态/静态产品实例信息；远程任务调度，调度或删除另一 EPC SAVANT 上的任务；告警职员，在一些定义的事件（如货架缺货、失窃、物品过期等）发生时，向相关人员发送告警；远程更新，发送产品信息给远程的供应链管理系统。

6.1.3.2　嵌入式中间件

嵌入式应用系统通常由嵌入式硬件平台、设备驱动程序、嵌入式操作系统和嵌入式应用程序组成。嵌入式硬件平台由具体应用硬件和接口设备构成；设备驱动程序实现应用功能与接口设备的信息软件；嵌入式操作系统运行硬件平台上，实现系统资源的管理；应用程序是根据应用需求来实现其功能的具体应用软件。应用程序在确定的操作系统平台上运行，通过调用操作系统的功能和硬件设备驱动程序，以及进行数据信息处理来实现其应用功能目标，嵌入式应用系统的基本结构如图 6-10 所示，从软件分层结构来看，是典型的 2 层结构体系，即“应用—实现”。

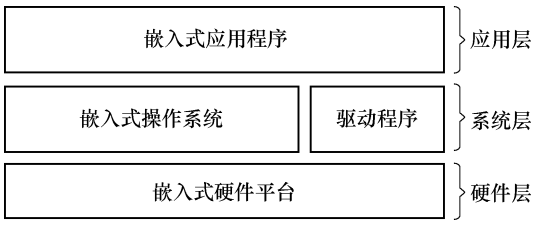


图 6-10　嵌入式应用系统结构

由于各种嵌入式应用目标的差异，以及使用的嵌入式操作系统的不同，具有同样功能的嵌入式应用程序（比如 I/O 接口数据采集、数据显示等），需要针对特定的嵌入式操作系统编程，应用开发者不但要关注具体应用的问题，而且要花费大量的精力去了解下层平台的特性，并解决所处平台之间的差异，而且编制的应用程序不能直接移植到其他操作系统上运行，使嵌入式应用程序的开发成为瓶颈。为了能够实现对嵌入式应用产品的快速开发，适应市场需求，就需要解决应用程序在不同嵌入式操作系统上实现移植和编程代码的重用性问题。因此在这里引入了面向应用编程的中间件技术，研究探索一条实现嵌入式应用程序开发的快捷途径，实现应用程序的可移植性和代码的重用性，提高物联网中嵌入式应用产品的开发效率和开发速度。

1. 嵌入式中间件的架构

嵌入式中间件由于是针对嵌入式系统的特点和资源条件进行设计的，与普通的 PC 或 Server 的中间件体系结构是有很大差异的。嵌入式中间件是介于嵌入式应用程序和操作系统、硬件平台之间的一个中间层次，它与操作系统类型和硬件平台结构无直接关系，对应用程序使用什么样的语言来实现也没有要求，它为应用程序提供一个统一规范的编程接口或请求管理机制，应用程序只需通过功能调用或请求响应来实现其应用功能。具体的嵌入式应用产品，其功能需求目标各不相同，对软硬件接口功能的要求也有差异，通过定义一组面向应用编程的，具有标准应用程序接口，为嵌入式应用软件的开发，建立一个能够在不同操作系统平台和硬件平台上运行的具有层次结构好、模块化程度高的通用扩展接口，形成一个嵌入式中间件的基本架构。要实现这一目标，必须要做到两点，建立一个标准化的面向应用编程的接口规范，为应用程序提供直接透明的系统调用功能和操作系统的功能扩展；将标准化的编程接口，构建成为能够满足多种硬件平台、独立于操作系统、代码可移植和重用的开发工具集，即应用编程中间件。是解决在不同的嵌入式平台上，实现应用程序的移植性和互操作以及编程代码的重用性等问题的有效途径。面向应用编程嵌入式中间件的结构如图6-11所示，按软件分层结构的划分，属于 4 层体系结构，即“应用—中间件—实现—硬件”。

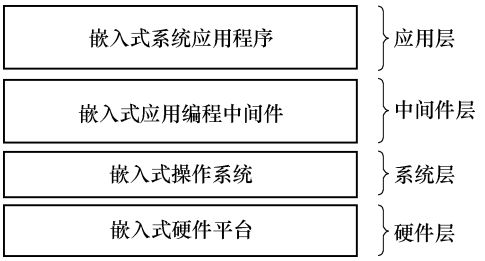


图 6-11　嵌入式中间件结构

在对嵌入式操作系统的应用中，针对嵌入式操作系统具有可裁减、可封装的特性，分析明确了构建面向应用编程的嵌入式中间件的技术路线之后，关键在于实现对中间件的方法，将应用的各种功能需求抽象出来，建立一个标准化的面向应用编程的接口规范，屏蔽操作系统的底层具体细节，特别是能够屏蔽不同的操作系统之间的差异。通过调用规范的系统功能调用接口，能够大幅度地降低开发难度，提高应用程序的可移植性、可维护性和可继承性。作为嵌入式的操作系统，通常是由一个基本的内核组成，为用户提供任务管理、内存管理、文件管理和设备驱动等基本功能，根据具体的应用需求进行相应的扩充，例如 Linux 和 Win-CE 都是如此。将操作系统扩展层功能和系统调用功能设计成为界于应用程序和操作系统之外的一个嵌入式中间层，使其对应用程序具有通用的功能调用编程接口，对操作系统或硬件具有实现其功能调用的硬件设备驱动和资源协调功能，这就使得在进行应用软件设计时，仅需要关心为实现硬件设备驱动和资源协调所对应的功能调用编程接口，不需要了解设备驱动和资源协调具体的操作步骤和控制机理，这就降低了嵌入式应用程序的编程难度，应用开发过程变得快捷，程序代码的复用程度提高。

2. 嵌入式中间件的架构设计

面向应用编程的嵌入式中间件设计思路，主要是参考 POSIX（Portable Operating System Interface，可移植操作系统接口）的结构原理和 MinimumCORBA 规范的设计思想来进行构建的。POSIX 定义了操作系统应为应用程序提供规范的接口和系统调用集的方法；MinimumCORBA 提出了分布式应用的互操作性、平台无关性、语言无关性的中间件设计方法；同时采用编程组件（Component）技术来实现面向应用编程组件库的设计。

要构建嵌入式中间件，可以通过两种模式来实现，一是将应用编程中间件与操作系统基

本内核进行编译封装，形成一个虚拟的嵌入式操作系统、实现应用程序与操作系统直接功能调用，这种方式具有与操作系统耦合度紧密，运行效率较高，但对操作系统的依赖程度过大，不能完全独立于操作系统，对不同的操作系统需要进行大量的优化修改工作。另一种模式是将应用编程中间作为一个独立的软件包运行，形成一个包含标准应用编程接口功能的管理协调运行环境、实现应用程序与操作系统之间代理调度机制。这种方式具有与操作系统独立开来，可以运行在不同的操作系统平台上，但对不同的操作系统，需要对与操作系统交互的接口调度机制进行优化和改进工作。

（1）虚拟操作系统（Virtual Operating System，VOS）模式

在应用程序与操作系统之间构建具有 POSIX 标准的面向应用编程接口，在嵌入式操作系统基本功能接口的基础上，对这些接口功能采取先实现一个最小的操作系统内核，然后根据应用具体要求，对操作系统进行相应的应用功能扩充，形成一个既包括操作系统基本功能调用，又具有操作系统应用功能扩展的独立于操作系统内核的 1 个嵌入式中间层，然后对中间层和操作系统内核进行封装，形成 1 个虚拟操作系统（VOS）的中间件。

该中间层的基本功能和扩展功能就可以作为通用编程接口函数提供给应用编程人员直接调用。当用户程序需要访问系统的硬件资源（如建立数据通信、I/O 数据采集，输出驱动控制等）时，采用接口驱动功能模式；用户程序发出系统功能调用申请，中间件层接收到请求后，根据请求的实现目标，向操作系统提交服务需求，操作系统协调硬件资源后，向用户程序返回所需的信息。虚拟操作系统的中间件结构如图 6-12 所示。

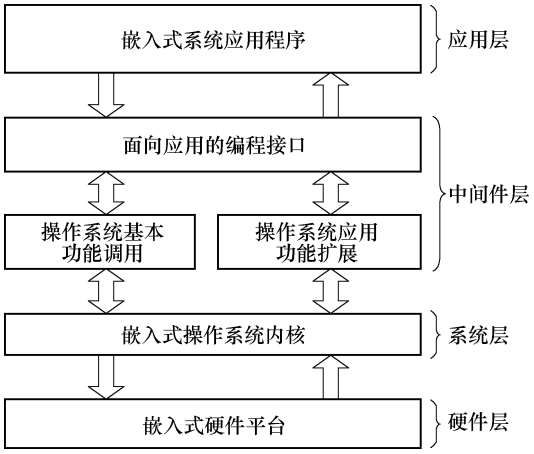


图 6-12　虚拟操作系统的中间件结构

（2）组件调用代理模式

将嵌入式应用涉及的设备驱动、功能调用以及相关应用编程接口用组件的形式表现出来，形成标准化的面向应用编程组件库（Application Programming Component，APC），同时在应用程序端建立起组件调用的代理机制，在操作系统端构建功能组件调用管理机制。形成一个具有独立运行管理功能的中间件层，由这个中间件层来实现应用程序与嵌入式操作系统之间的请求代理和功能调度，从而完全实现了应用程序的可移植性、可维护性和可继承性，同时也实现了对不同操作系统能够直接进行底层系统功能调用。当应用程序要实现 1 个应用功能时，将应用请求发送给中间件，中间件根据应用程序请求，通过调用代理机制，代理执行面向应用编程组件，来实现对操作系统的功能调用，完成嵌入式应用功能，并将结果信息通过调用代理机制返回给应用程序。组件调用代理中间件结构如图 6-13 所示。

6.1.3.3　数字电视中间件

数字电视中间件是数字电视机顶盒的软件平台，为数字电视的应用提供运行环境和软件接口，即位于数字电视内部操作系统与应用程序之间的软件部分，它以应用程序接口（API）的形式存在。数字电视机顶盒不仅要接收数字化传输的视音频节目，还要接收大量

的数据，同时数字电视还要实现交互功能，这就要求数字电视机顶盒具有一定的信息处理能力和网络通信能力。面对大量涌现的数据业务和交互业务，一个通用的软件平台是必需的。采用中间件系统，可以跨越硬件、技术等复杂的内容，让数字电视应用软件开发商用统一的方法定制具有自己特色的应用软件，从而在提高开发效率、减少开发成本的同时能够跟上技术的发展，将应用的开发变得更加简捷，使产品的开放性和可移植性更强。图 6-14 描述了中间件在数字电视软件体系结构中的位置。

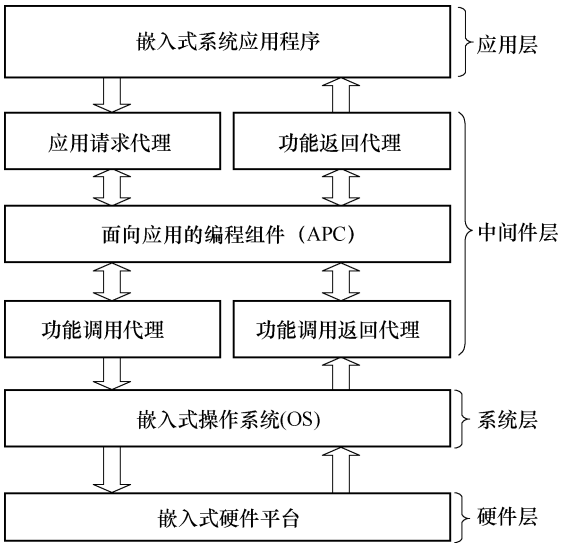


图 6-13　组件代理调用中间件结构

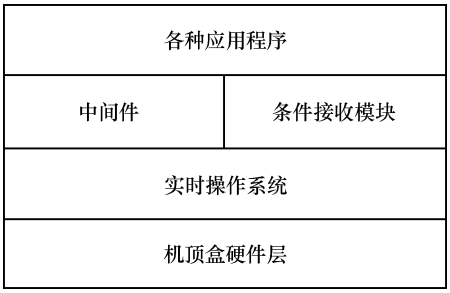


图 6-14　中间件在数字电视软件体系结构中的位置

目前，比较成熟的商用中间件产品有 OpenTV 的 EN2，Liberate 的 TV Navigator for DTV，Enreach 的 EnreachTV for DTV，CanalPlus 的 Media Highway 以及 NDS 的 NDS Core 等，我国已经有一定市场份额的中间件生产厂商主要有 Canal Plus、NDS 和 OpenTV 等几家。法国 Canal Plus 的 Media Highway 是欧洲中间件系统的代表，其最早采用的编程语言是一种解释执行的私有语言，后来，Canal Plus 采用 Java 语言和标准的数据下载协议 DSMCC Object Carousel（即 DSMCC 对象轮盘传输），重新进行系统设计和制定编程接口，成功地将 Java 引入数字电视机顶盒中。Canal Plus 的中间件产品在欧洲有广阔的市场。英国 NDS 的中间件解决方案主要是基于 HTML，利用 HTML 网页浏览器能实现一定的互动性，目前，NDS 正在研究基于 Java 的解决方案。OpenTV 是国际上极负盛名的中间件生产厂商，它采用的编程语言是 C 语言，也是解释执行的。

1. 数字电视中间件的特点

从数字电视中间件系统结构来看，中间件所处的位置决定了其软件系统的构成具有如下特点：

1）交互性：支持双向交互和不许回转的本地交互，能支持有低端的基本业务到高端的交互业务。

2）移植性：就是要求中间件软件具有平台无关性，一方面能够独立运行于任何硬件平台，另一方面它所提供的驱动层的接口能够在大多数硬件平台上使用。

3）稳定性：一个成功的平台在技术和市场上必须具有稳定的生命周期，基本的业务平台应稳定持续而且具有良好的可扩展能力。

4）采用通用的 API：采用统一的应用程序接口方式，要支持实时流的应用、下载和本地存储等；广播商和应用提供商能够自己开发应用；支持业务数据提取；使用户终端制造商能够以体现自身特点的方式使用。

2. 数字电视中间件的系统结构

由于 Java 技术已经成为国内外数字电视中间件标准中选用的核心技术之一，目前国内外成熟的数字电视中间件产品几乎无一例外地采用了 Java 技术。因为 Java 语言具有跨平台性、安全性、可扩展性、易用性，并且 Sun 公司提供了 Java 的开放源代码。基于 Java 语言的应用软件能够在不同的设备上运行，无论是用户使用的 PC，还是数字机顶盒，Java 技术都为交互式数字电视的开发提供了方便。

我国制定的数字电视中间件标准明确指出，中间件系统要求采用 Java 虚拟机，并且提供 Java 应用程序接口，使用 Java 语言编制交互式使用。根据该标准，结合有线数字机顶盒的硬件环境和操作系统的特征，借鉴国内外中间件产品，有人提出了一种基于有线机顶盒的数字电视中间件的实现方案，该方案采用了 Java 技术，使用 J2ME 中的连接设备配置（Connected Device Configuration，CDC）、个人简表，使用 JavaTV API，方案如图 6-15 所示。

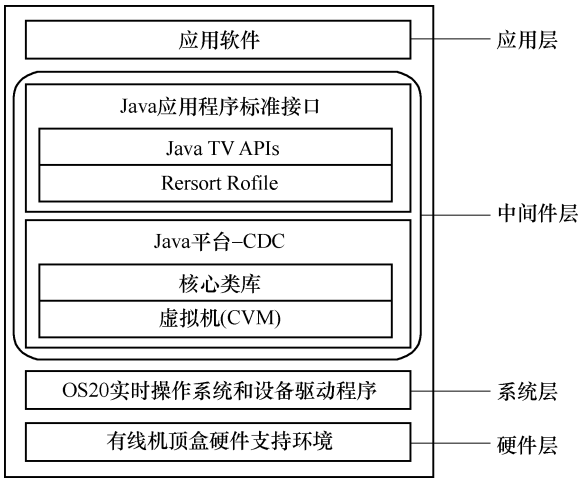


图 6-15　基于有线机顶盒的中间件设计方案

1）硬件层：此层是有线机顶盒的硬件环境，主要采用 ST 公司的 Sti5516 芯片，CPU 为 ST20-C2。

2）系统层：此层包括 OS20 实时操作系统和设备驱动程序。OS20 为 Java 平台（CDC）的虚拟机和类库的运行提供系统级的支持。设备驱动程序控制硬件设备，为个人简表和 Java TVAPI 提供支持。

3）中间件层：此层包括 Java 平台（CDC）和 Java 应用程序的接口，它为 Java 应用程序的运行提供了完整的 Java 环境。其中 Java 应用程序标准接口包括个人简表和 Java TV API。

4）应用层：此层利用中间件层提供的标准接口开发丰富的 Java 应用软件，向用户提供交互式电视节目。

6.2　对象名称解析服务

EPC 标签由于其存储容量相对较小而只存储了二进制 EPC 编码，未能存储其相关的商品信息（如产地、制造日期、保质期等）。如何利用现有的 EPC 编码来查找其商品相应的信息成为人们急需解决的问题。通过分析现有的互联网，我们通过 DNS 便能够顺利浏览各个网站的信息而无需记忆其站点的 IP 地址，类似地，利用 DNS 来构建 ONS，可以很好地解决这个问题。

6.2.1　ONS 的体系结构

由图 6-16 可见，ONS 的作用是将一两个 EPC 映射到一个或者多个 URI，通过这些 URI 我们可以查到在 EPCIS（或 Web）服务器上关于此产品的其他详细信息。这里，ONS 存有制造商位置的记录，而 DNS 则是到达 EPCIS 服务器位置的记录，所以 ONS 设计运行在 DNS 之上。

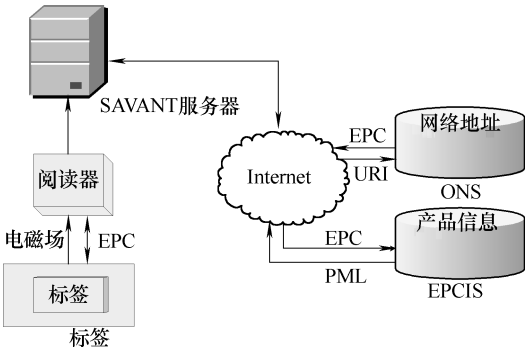


图 6-16　EPC 网络图

与 DNS 相似，ONS 系统的层次也是分布式的，主要由根 ONS、ONS 服务器、本地 ONS、本地缓存（Cache）及映射信息组成，其结构如图 6-17 所示。

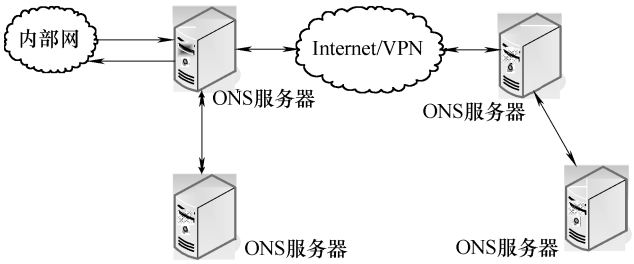


图 6-17　ONS 系统结构图

图中，根 ONS 服务器处于 ONS 层中的最高层，它拥有 EPC 名字空间的最高层域名，因此基本上所有的 ONS 查询都要经过它。ONS 也相当重要，它用于回应本地的 ONS 查询，并返回查询成功的 URI。ONS 本地缓存则是将经常、最近查询的 URI 保存起来，以减少对外的查询次数。作为 ONS 查询的第一站，其作用是极大地提高了查询效率并且减少了 ONS 服务

器的压力。而映射信息则是ONS系统所提供服务的实际内容，它指定了EPC编码与相关的URI映射关系，并且分布存储在不同层次的各个ONS服务器中。这样，ONS系统便是最大限度地利用现有的互联网体系结构中的DNS系统，节省了大量的重复投资。

6.2.2　ONS的工作过程

1）阅读器读取RFID标签，以二进制的格式获取EPC编码。

（01 00000000110000010010 01001001000011001 00100010101011011001010l）这是以一个64位的EPC代码为例。

2）所采集到的EPC传送到本地服务器。

（01 00000000011 0000010010 010010010000110010010001010101101100l0101）。

3）将二进制的EPC编码转换为整数并在头部添加“urn:epc”。转换为URI格式urn:epc:1.1554.37401.2272661。

4）ONS将URI被转换位域名格式，其方法为

清除urn:epc1.1554.37401.2272661；

清除EPC序列号1.155437401；

颠倒数列37401.1554.1；

添加“.nsroot.org”37401.1554.1.onstoot.org。

ONS生成并且提取正确的URL（该过程可能需要远程ONS），并且将此URL发送到本地服务器。

5）本地服务器通过已经或取得URL和所需要的EPCIS连接。

6.2.3　ONS的安全分析

ONS服务器是ONS系统的核心，可以向ONS客户端提供ONS查询服务。如果查询成功，则返回此EPC对应的URI，并在返回信息所经过的所有ONS服务器及ONS客户端的缓存中保存该映射信息，以备下一次查询时使用。根ONS服务器位于ONS层次结构的最顶层，拥有EPC名称空间中的最高层域名。在大多数情况下，ONS查询请求不会到达根ONS服务器，但是当ONS客户端从本地缓存或上一级ONS服务器中查不到所需的信息时，则将该查询请求转发给根ONS，从根ONS开始逐级查询。目前，根ONS服务器的域名为epc.objid.net，根ONS服务器及配套的发现服务系统由EPCglobal委托给美国Verisign（威瑞信）公司进行运维和管理。

由于ONS与DNS之间存在的这种内在联系，这就使得ONS的部署很容易实现，没有必要单独开发和维护一套独立的系统。另一方面，由于DNS存在的软件漏洞、缓存中毒、域名劫持、DDoS攻击等安全问题在ONS中同样存在，影响了EPC系统的可靠性和安全性。除此之外，EPC物联网中使用的RFID技术存在安全问题。例如，当对物品标签中的EPC信息进行采集时，EPC标签和读写器之间采用无线射频信号进行通信，在采集数据的过程中将EPC信息暴露到四周的空气中，此时如果EPC信息在交给SAVANT之前被窃取或篡改，将会给物品真实“身份”的识别带来隐患。为解决ONS遇到的安全问题，除借鉴DNS安全管理中的成功经验外，还可以有针对性地采用一些安全技术和措施，如ONS服务器在加入根ONS服务器时需要进行认证，在ONS中部署DNSSEC（域名系统安全扩展）等。针对RFID

系统存在的安全问题，可以通过综合运用数据加密、信道扰码、电磁屏蔽等技术，对标签中的 EPC 数据、读写器与标签之间的通信、计算机系统中 EPC 信息的存储及 EPC 信息在互联网中的传输进行安全管理。

目前，由于 EPC 物联网在全球正处于发展阶段，出于信息安全、知识产权等各方面的因素，相关标准尚未得到各个国家的普遍认可和执行，ONS 等 EPC 物联网中的关键基础设施架构还未在全球范围内铺开，大量的技术研究主要在局域范围内进行，重点集中在 EPC 标签、RFID 中间件等方面，针对基于互联网的 EPC 物联网的研究和应用相对较少，网络安全、查询优化、名字空间规划、动态 ONS 等。可以预计，今后对 ONS 的要求也会不断地提高。

6.3　实体标记语言

6.3.1　PML 概述

世界上的事物千千万万，未来的 EPC 物联网也将会庞大无比；自然物体会发生一系列事件，而附着的 EPC 标签里面也只是存储了 EPC 代码一串数字字符而已。如何利用 EPC 代码在物联网中实时传输这些 EPC 代码所代表的自然物体所发生的事件信息，EPC 物联网通信语言的问题值得我们去思考。我们发现现有的可扩展标示语言（XML）是一种简单的数据存储语言，它仅仅展示数据且极其简单，任何应用程序都可对其进行读写，这使得它很快成为了计算机网络中数据交换的唯一公共语言。XML 描述网络上的数据内容及结构的标准，对数据赋予上下文相关功能。它的这些特点非常适合于物联网中的信息传输。为此，在 XML 语言的基础上发展了更适合于物联网的 PML。在 2.1.1 节分析物联网中的信息流通情况，从图 2-1 中可以发现 PML 是 SAVANT、EPCIS、应用程序、ONS 之间相互表述和传递 EPC 相关信息的共同语言，它定义了在 EPC 物联网中所有的信息传输方式。从图 2-1 还可以看到，在整个 EPC 物联网上，物品信息流动过程是这样的。阅读器扫描到 EPC 标签后，将读取的标签信息及传感器信息传递给 SAVANT，经 SAVANT 过滤冗余信息等处理后通过 ONS 送到 EPC 信息服务器。企业应用软件可通过 ONS 访问 EPC 信息服务器获取到此产品的相应信息，也可通过 SAVANT 经过安全认证后访问企业伙伴的产品信息。物联网上所有信息皆以 PML 文件格式来传送，其中 PML 文件可能还包括了一些实时的时间信息、传感器信息。

图 6-18 所示为 PML 的组成结构图，它是一个标准词汇集，主要包含了两个不同的词汇、PML 核及 SAVANT 扩充。如果需要的话，PML 还能扩展更多的其他词汇。

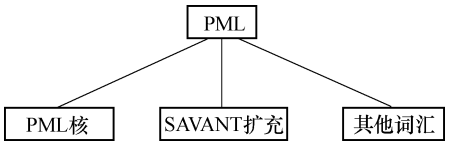


图 6-18　PML 结构图

6.3.2　PML 的设计

现实生活中的产品丰富多样，很难用一个统一的语言来客观描述每一个物体。然而，自然物体都有着共同的特性，如体积、重量；企业个人交易时有着时间、空间上的共性。自然物体的一些相关信息（如生产地、保质期）不会变化。同时 EPC 物联网是建立在现有的互

联网上的。为此，作为描述物体信息载体的 PML，其设计有着独特的要求。

（1）开发技术

PML 首先使用现有的标准（如 XML、TCP/IP）来规范语法和数据传输，并利用现有工具来设计编制 PML 应用程序。PML 需提供一种简单的规范，通过默认的方案，使方案无需进行转换，即能可靠传输和翻译。PML 对所有的数据元素提供单一的表示方法，如有多个对数据类型的编码方法，PML 仅仅选择其中的一种，如日期编码。

（2）数据存储和管理

PML 只是用在信息发送时对信息区分的方法，实际内容可以任意格式放在服务器（SQL 数据库或者数据表中），即不必一定以 PML 格式存储信息。企业应用程序将以现有的格式和程序来维护数据，如 Aaplet 可以从互联网上通过 ONS 来选取必需的数据，为便于传输，数据将按照 PML 规范重新进行格式化。这个过程与 DHTML 相似，也是按照用户的输入将一个 HTML 页面重新格式化。此外，一个 PML“文件”可能是多个不同来源的文件和传送过程的集合，因为物理环境所固有的分布式特点，使得 PML“文件”可以在实际中从不同的位置整合多个 PML 片段。

（3）设计策略

现将 PML 分为 PML CORE（PML 核）与 PMLExtension（PML 扩展）两个部分进行研究，如图 6-19 所示。

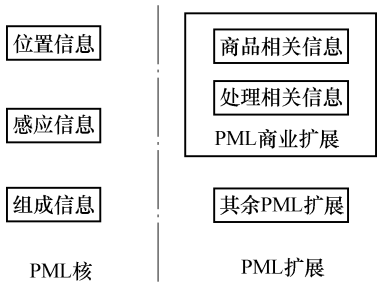


图 6-19　PML 与 PML 扩展

PML 核用统一的标准词汇将 Auto-ID 底层设备获取的信息分发出去，比如位置信息、组成信息和其他感应信息。由于此层面的数据在自动识别前不可用，所以必须通过研发 PML 核来表示这些数据。PML 扩展用于将 Auto-ID 底层设备所不能产生的信息和其他来源的信息进行整合。第一种实施的 PML 扩展包括多样的编排和流程标准，使数据交换在组织内部和组之间发生。

PML 核主要集中于直接由 Auto-ID 底层设备所生成的数据，它主要描述包含特定实例和独立于行业的信息。特定实例是条件与事实相关联，事实（如一个位置）只对一个可自动识别的对象有效，而不是对一个分类下的物体有效。独立于行业的条件指出数据建模的方式：即它不取决于指定对象所参与的行业或业务流程。对于 PML 商业扩展，提供的大部分信息对一个分类下的所有物体均可用，大多数信息内容高度取决于实际行业，例如高科技汗液组成部分的技术数据都远比其他行业通用。这个扩展在很大程度上是针对用户特定类别并与它所需要的应用相适应，目前 PML 扩展框架的焦点集中在现有的电子商务标准上，扩展部分可以覆盖到不同的领域。

至此，PML 设计便提供了一个描述自然实体、过程环境的统一标准，可供工业和商业中软件开发、数据存储和分析工具之用，同时还提供一种动态环境，使物体相关的静态的、暂时的动态的和统计加工过的数据实现互相交换。

6.3.3　PML 的应用举例

EPC 物联网系统的一个最大好处在于自动跟踪物体的流动情况，这对企业的生产及管理有着很大的帮助。图 6-20 所示为 PML 信息在 EPC 系统中的流通情况，可以看出 PML 最

主要的作用是作为 EPC 系统中各个不同部分的一个公共接口，即 SAVANT、第三方应用程序、存储商品相关数据的 PML 服务器之间的共同通信语言。现考察具体实际应用情况。

图 6-21 所示为某冰箱企业的生产示意图，一辆装有冰箱的卡车从仓库中开出，在其仓库门口处的阅读器读到了贴在冰箱上的 EPC 标签，此时阅读器将读取到的 EPC 代码传送给上一级 SAVANT 系统。SAVANT 系统收到的 EPC 代码后，生成一 PML 文件，发送至 EPCIS 服务器或者企业的管理软件，通知这一批货物已经出仓了。此时 PML 文件如图 6-22 所示。

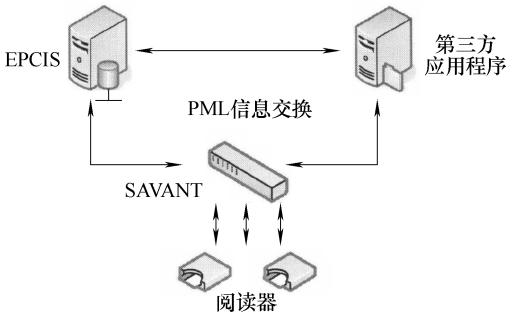


图 6-20　PML 作为 EPC 系统的公共接口

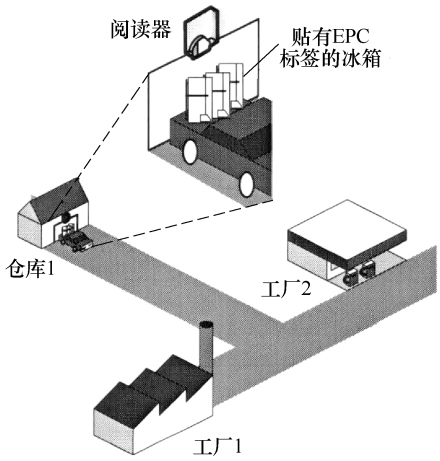


图 6-21　某冰箱企业生产示意图

图 6-22 中的 PML 文件简单、灵活、多样，并且是人眼也可阅读、易理解的。这里对该 PML 文档中的主要内容做一扼要说明。

```
<pmlcore:Observation>
    <pmlcore:DataTime>20070712150434</pmlcore:DateTime>
        <pmlcore:Tag><pmluid:ID>urn:epc:1.3.42.356</pmluid:ID>
            <pmlcore:Data>
                <pmlcore:XML>
                    <EEPROM xmlns="http://tag.example.org/">
                    <FamilyCode>12</FamilyCode>
                    <ApplicationIdentifier>123</ApplicationIdentifier>
                    <Block1>FFA0456F</Block1>
                    <Block2>58433791</Block2>
                    </EEPROM>
                </pmlcore:XML>
            </pmlcore:Data>
        </pmlcore:Tag>
</pmlcore:Observation>
```

图 6-22　PML 文档一例

1）在文档中，PML 元素在一个开始标签（注意，这里的标签不是 RFID 标签）和一个结束标签之间。例如 < pmlcore：Observation > 和 < /pmlcore：Observation > 等。

2）< pmlcore：Tag > < pmluid：ID > urn：epc：1：3. 24. 356 < /pmluid：ID > 指 RFID 标签中的 EPC 编码，其版本号为 1，域名管理．对象分类．序列号为 3. 24. 356，由相应 EPC 编码的二进制数据转换成的十进制数。URN 为统一资源名称（Uniform Resource Name），指

资源名称为 EPC。

3）文档中有层次关系，注意相应信息标示所属的层次。文档中所有的标签都含有前缀“<”及后缀“>”。PML 核简洁明了，所有的 PML 核标签都能够很容易地理解。同时 PML 独立于传输协议及数据存储格式，且不需其所有者的认证或处理工具。在 SAVANT 将 PML 文件传送给 EPCIS 或企业应用软件后，这时候企业管理人员可能要查询某些信息。

这里我们为便于理解，将其 PML 信息形象地绘制成一副三维空间图像，如图 6-23 所示，坐标轴名称分别为时间（戳）、物体 EPC 代码、地理位置。由于阅读器一般都事先固定好，地理位置便可用阅读器的 ID 号来表示。

下面就是对 PML 文件信息进行查询了。采用下列查询语句：SELECT COUNT（EPCno）from EPC_DB where Timestamp =“200707012”Reader-No =“Rd_ID_2”，这里只是简单地采用 SQL 中的 COUNT 函数。但是实际的情况远远要比这个复杂得多，可能需要跨地区、时间，综合多个 EPCIS 才能得到所需的信息。可以预见，PML 的应用随着 EPC 的发展将会非常广泛，进入所有行业领域。

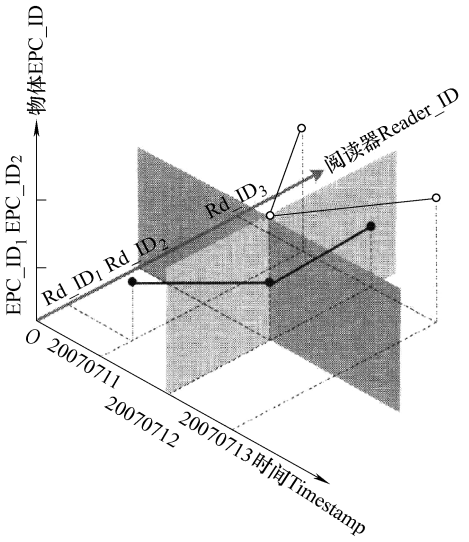


图 6-23　冰箱流动情况查询

信息化是 21 世纪各行业的重要发展趋势，电子商务、电子政务、远程医疗、远程教育等基于网络技术的应用发展迅速。高度网络化的 EPC 物联网系统，意在构造一个全球统一标识的物品信息系统，它将在超市、仓储、货运、交通、溯源跟踪、防伪防盗等众多领域和行业中获得广泛的应用和推广。物联网中的信息载体采用 PML，同其他任何语言一样，PML 不是一个单一的标准语言，它应随着时代的变化而发展。

6.4　物联网智能

物联网智能是将人工智能技术服务于物联网络的技术，是将人工智能的理论方法和技术通过具有智能处理功能的软件部署在网络服务器中去，服务于接入物联网的物品设备和人。物联网智能化也要研究解决 3 个层次的问题：网络思维，具体讲是网络思维、网络学习、网络诊断等；网络感知让网络像人一样能感觉到气味、颜色、触觉；网络行为，研究网络模拟、延伸和扩展人的智能行为（例如智能监测、智能控制等行为）。

将人工智能技术的研究成果应用到物联网中去，将单一机器的智能处理技术应用到物联网的智能处理是实现物联网的智能化的必经之路，也是物联网技术的核心。物联网智能化的目的是在更广的空间范围内集中、规模化地利用智能化的网络来处理或管理社会的一些基础设施或行业服务，从而达到整个社会管理智能化的目的。

（1）智能物联网概念

智能物联网能够对接入物联网的物品设备产生的信息实现自动识别和处理判断，并能将

处理结果反馈给接入的物品设备，同时能根据处理结果对物品设备进行某种操作指令的下达，使接入的物品设备做出某种动作响应，而整个处理过程无需人类的参与。

物联网就是以实现智能化识别、定位、跟踪、监控和管理的一种网络来定义。但是在目前的实际应用过程中，往往忽略了物联网的智能化本质。也就是说，物联的核心技术是智能化，而不仅仅是接入的传感器、网络传输或者是哪个行业的应用。

（2）智能物联网的实现途径

要实现物联网智能化，就必须让人工智能成为物联网的大脑智能化物联网中必要的构成要素，为智能化感知终端、传输网络、具有人工智能的数据处理服务器提供智能管理。可以理解为把若干个智能机器人进行了分布式部署，将智能机器人的传感器、动作部件放在远端，而将智能机器人的大脑作为大型数据处理服务器放在网络上，从而实现多个智能机器协同处理控制远端的传感器或动作部件的目的。无论是物联网的使用者还是接入物联网的设备，都可以通过互联网来接收和发送数据，充分利用了互联网的数据共享特性。

（3）物联网中的人工智能技术

物联网中需要来自人工智能技术的研究成果。如问题求解、逻辑推理证明、专家系统、数据挖掘、模式识别、自动推理、机器学习、智能控制等技术。通过对这些技术的应用，使物联网具有人工智能机器的特性，从而实现物联网智能处理数据的能力。特别是在智能物联网发展初期，专家系统、智能控制应该首先被应用到物联网中去，使物联网拥有最基本的智能特性。

物联网专家系统是指在物联网上存在一类具有专门知识和经验的计算机智能程序系统或智能机器设备（服务器），通过网络化部署的专家系统来实现物联网数据的基本智能处理，以实现对物联网用户提供智能化专家服务功能。物联网专家系统的特点是实现对多用户的专家服务，其决策数据来源于物联网智能终端的采集数据。

在物联网的应用中，控制将是物联网的主要环节，如何在物联网中实现智能控制将是物联网发展的关键。将智能控制技术移植到物联网领域将极大丰富物联网的应用价值，接入物联网的设备将接受来自物联网的操作指令，实现无人参与的自我管理和操作。

在物联网的智能控制应用中智能控制指令主要来自接入物联网的某一个用户或某一类用户，以实现该类用户的无人值守工作。

6.5　物联网中的大数据分析

我们现在处于大数据时代，各种数据通过传感器产生，也有在网上直接产生的，互联网一分钟可以产生非常多的东西，如苹果商城下载 2 万余次，一分钟内上传 10 万条新微博，全世界物联网上以及虚拟网络上，产生了大量的数据。国外的数据量不一定比中国大，淘宝 2014 年双十一发生 912 亿元交易额，新浪微博晚上 100 万以上的响应请求，中国联通改制详细记录客户的上网记录一秒钟有 83 万条。虚拟运行管理产生的数据量更大，企业资源管理客户关系管理等现在也是大数据，企业本身也是每时每刻在产生大量数据。2012 年国际数据公司发布了数字世界 2020，指出在 2005 年由机器产生的数据占到数据总量的 11%，2020 将增加到 42%。

物联网产生的大数据与一般的大数据有不同的特点。物联网的数据是异构的、多样性的、非结构和有噪声的，更大的不同是它的高增长率。物联网的数据有明显的颗粒性，其数

据通常带有时间、位置、环境和行为等信息。物联网数据可以说也是社交数据，但不是人与人的交往信息，而是物与物，物与人的社会合作信息。物联网的混搭将使物联网的数据变得更有用，将物联网感知的数据与通过社会媒体获得的数据结合，也就是人跟机器的社会联网，将使决策更科学。

6.5.1　物联网与大数据

物联网时代的数据主要分为感知数据和社交网络数据两种。目前来说，网络上的数据量还是大于机器感知到的数据量，但是到2015年，随着传感设备的不断普及，以及感知数据的逐渐集中，它的数据量将开始超过网络数据，最终将发展到网络数据的2倍，这种变化趋势是不可阻挡的。

物联网主要包括3方面的内容：感知层、网络层以及应用层，其中感知层所产生的数据量最多。物联网中的应用层往往是对感知层中数据的处理以及加工，通过应用层，物联网能够很好地实现感知层中数据的智能化以及商业化，与此同时，也能够进一步挖掘物联网中不同用户的喜好，进而为满足不同用户的商业需求奠定基础。可以说，物联网中的应用层是物联网最具有商业价值的内容。总而言之，物联网产生了大数据，大数据反过来推动了物联网的发展，二者相辅相成，共同发展，从这一层面上讲，物联网产业的本质内涵就是广泛地应用大数据分析与处理手段来实现智能化的管理与运营。

那么物联网大数据呈现出哪些特点？数据之间也是有区别的，最基本的数据类型是结构化数据，就是数据库可读的数据，这也是最容易被处理的。其次是相当多的可被处理的非结构化数据，比如新闻、微博等。此外最多的是那些大量的目前还不能被处理的非结构化数据，最典型的就是目前各种碎片化物联网应用中的数据，可能采集上来的数据中有的没有被有效利用。

产生大量休眠数据的原因在于3点：第一点是处理速度，有这样一个说法，如果数据采集后几秒内没有被处理，那么数据就已经失去价值，如果几分钟之后还没有被处理，那么数据就已经没有价值了。第二点原因是处理成本，尽管人们希望及时地处理数据，但是由于数据太分散，或者计算能力不足，以及网络延迟等原因，在缺少更高速的处理器和更宽的网络带宽时，就难以实现实时处理。第三点产生休眠数据的原因是认知能力，有些数据尽管可以采集上来，但是却不知道该如何利用，将来也许有用，那么这样的数据也会成为休眠数据。

现在谈论的大数据大多是指互联网中的大数据。而物联网中的大数据和互联网中的有何不同，最根本的一个区别就是现在所研究的大数据，大多是指历史的数据，也就是在已经产生的数据中去搜索，或做关联分析。但是在交通、电网以及公共安全等智慧城市的各种应用中，物联网的大数据更多是指未来的数据。我们并不知道明天的交通状况如何，也不知道下一季度工业用电的峰值，只知道传感器会持续不断地给我们提供数据，这些数据会在未来以一种典型的流数据的形式到来，我们需要在最短的时间内对这些流数据进行处理、分析、存储和分发。因此物联网大数据的研究内容和传统的互联网大数据有很大不同，需要在架构和核心技术上取得突破，需要在旧商业模式基础上技术创新，还需要根据新技术建立新的应用商业模式。

6.5.2　海云协同模型

海云数据系统是中国科学院“面向感知中国的新一代信息技术”战略性先导科技专项

“海云数据系统关键技术研究与系统研制”课题研究的重要内容。其目标是研制面向海量数据存储与挖掘的互联网服务平台，为“海云创新实验环境”用户提供大规模数据存储、处理、挖掘与可视化分析服务，创新数据挖掘互联网服务模式。海云协同模型就来自于中国科学院“面向感知中国的新一代信息技术研究”战略性先导科技专项“海云数据系统关键技术研究与系统研制”课题。

物联网系统尤其是移动物联网系统由数十亿的无线传感组件构成，这些组件时刻执行着感知、收集和处理具有不同类型数据的任务，可以预见，随着时间的推移，这些物联网应用将推动数据空间达到更大的规模。在物联网系统中，人和设备（从智能手机到可穿戴智能设备，从安装在汽车里的智能传感器到宇宙飞船）紧密互联，从这数十亿互联的组件中产生的大量传感数据将形成一个巨大的数据海洋，从而加速了大数据的出现。从如此大量的数据中提取有价值的信息来提高日常生活质量和办公效率是信息科技发展的必然需求。

在物联网系统应用场景中，对于利用大数据解决实际问题这一现实需求，我们都面临着以下这几方面的挑战。

1）需要新的系统架构来管理整个信息空间的大数据的生命周期。

2）需要新的协同机制来判断具有不同实际需求的任务，然后将这些任务指派到相应的端系统执行。

3）需要新的存储和计算技术来完成对大数据的存储和分析工作，从而进一步地挖掘大数据的潜在价值来生成按需获取的服务信息，同时确保服务信息的实时响应。

鉴于以上挑战的存在，接下来将详细介绍这种创新的物联网大数据管理解决方案，即面向物联网大数据管理的海云协同模型。

物联网系统具有显著的异构性、混杂性和超大规模等特性。异构性表现在不同的制造商、不同的拥有者、不同的类型以及不同范畴的对象网络共存于物联网中；混杂性表现在网络形态、组成、场景、服务和应用等多个方面；超大规模性表现在物联网系统是物理世界与信息空间的深度融合，是全球范围的人、机、物的互联。所有这些物联网系统的特性决定了物联网传感数据也具有异构性、混杂性、实时感知和超大规模等特性。这些特性决定了众多不同的物联网大数据应用场景中大数据处理任务的异构性和需求的多样性，这些任务的异构性和需求的多样性要求物联网大数据管理系统必须采用不同的新技术来处理具有不同格式的大数据，而现有的针对特定数据类型和业务的系统在架构上已经难以满足如此多样化的需求。这意味着我们需要设计新的系统架构，不仅要满足实时响应服务依赖较少数据和计算资源任务的需求，而且能满足依赖大量数据和计算资源但不要求实时响应服务的需求。

基于以上实际需求，这里提出了面向物联网大数据管理的海云协同模型，图 6-24 为模型的整体架构。

如图 6-24 所示，海云协同模型的核心为定义了 3 种不同的服务请求类型，即：海端实时响应服务请求、云端实时响应服务请求和云端大数据分析与挖掘服务请求。

6.5.2.1　海端实时响应服务请求

如图 6-24 所示，海端实时响应服务判定器用于判断服务请求是否属于要求强实时服务响应的请求类型，并且这种请求只需依赖较少的数据量和计算量，但却要求很强的响应实时性。本文所讨论的海云协同模型中，响应这种服务请求的计算任务被定义为海端实时响应任务。

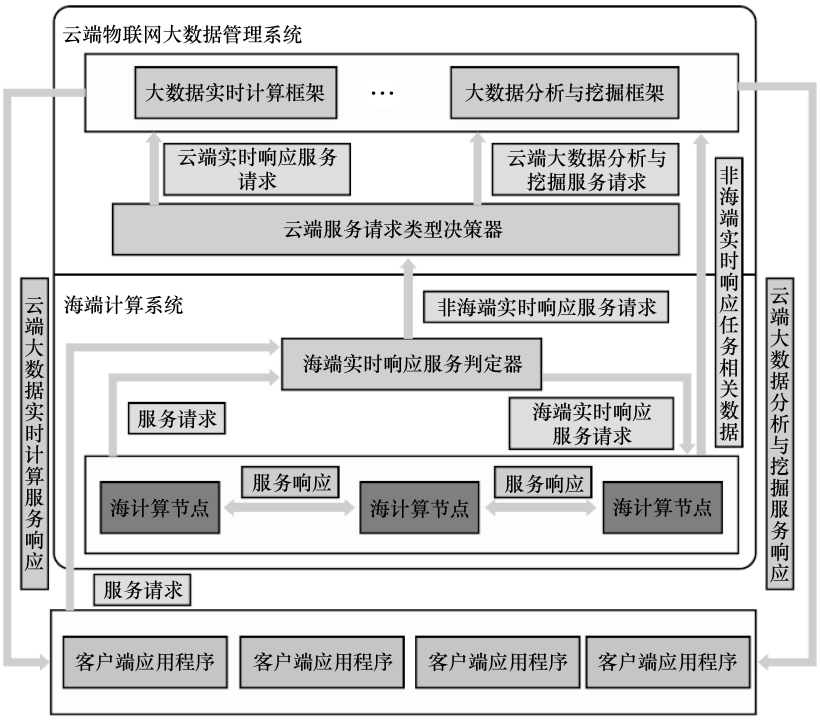


图 6-24　海云协同模型整体架构图

例如车联网系统中车辆碰撞预警系统。在车辆碰撞预警系统中，当安装在车辆上的无线传感器感知到有其他车辆进入自身周围的特定范围内并且有可能发生碰撞时，会利用动态自组织网络技术与其他车辆组成一个动态临时网络，并且实时发送一条碰撞预警信息给其他车辆，以避免发生碰撞。碰撞危险解除后，传感器会将此次预警过程中的数据信息发送到云端物联网大数据管理系统，为道路整改或者交通流量控制等方案的设计提供有用的历史参考数据。这些方案的设计，可能需要经过大量的历史数据分析和挖掘以得出较好的方案，因此这种碰撞预警发生的时间、地点、周边交通状况等数据信息将会变得很有价值。

自组网请求信息和碰撞预警信息只承载很少的数据量，并且可以在动态局部自组网中快速发送，同时海端实时响应服务判定器也会在这个局部动态自组网中实现，以降低与云端服务器交互而带来的网络负载，从而保证服务响应的高效实时性。如果服务请求属于这种类型，则完成服务响应的计算任务将直接在位于本地的物联网计算节点中执行，并实时给予其他本地计算节点或客户端应用程序以服务响应，这种响应是秒级甚至是毫秒级的。

这里所讨论的海云协同模型中，这种本地物联网计算节点被称为海计算节点，而完成这种服务请求任务的计算过程被称为海计算，在车辆碰撞预警系统中，安装在车辆上的无线传感器就充当了海计算节点。

6.5.2.2　云端实时响应服务请求

如果服务请求不属于海端实时响应服务请求，则服务请求会被发送至云端物联网大数据管理系统，由云端服务请求类型决策器来判断服务请求的类型。此时会有两种判定的服务请求类型：云端实时响应服务请求和云端大数据分析与挖掘服务请求。

云端实时响应服务请求是指那些既要求实时响应同时又依赖较多的数据和计算资源的服务请求，例如实时路径导航，实时交通拥堵状况查询等服务请求，这些应用请求可能来自用户智能手机上的客户端应用程序，实时路径导航需要依赖用户当前的位置和地图数据来实时计算出导航路线并且推送到客户端应用程序，这需要 GPS 定位数据和地图数据，并且经过一系列计算来完成导航。对于低功耗的海计算节点（通常为无线传感器节点），其计算和存储能力显然不能负荷这样的计算任务，因此这类服务请求会被发送到云端计算系统进行实时计算（通常采用基于分布式系统的实时流计算技术）。

6.5.2.3　云端大数据分析与挖掘服务请求

云端大数据分析与挖掘服务请求是指那些依赖海量数据和计算资源才能完成响应的服务请求（通常为海量的数据和复杂的数学模型，如某种机器学习模型或者数据挖掘方法）。这些大数据的分析和挖掘工作是一个长期的工作，因此没有实时性的要求，从而可以在云端分布式计算系统中以离线的方式进行。在需要分析和挖掘结果时，利用大数据可视化工具呈现分析结果并且推送到客户端程序。

例如利用出租车公司的历史载客数据，分析出租车乘客的区域密度分布以指导出租车公司进行车辆分布规划；利用电子商务网站的用户历史购物数据分析用户的潜在购物兴趣，从而向用户推荐相关商品，促成潜在的购物行为；利用大量的历史天气数据来预测未来的天气情况；利用历史路况信息和道路交通事故历史数据挖掘出有用的知识信息，给道路整改方案和交通流量控制方案的设计提供有价值的参考等。

6.5.2.4　海云协同模型的协同机制

海云协同模型协同机制的核心在于如何确定服务请求的类型，下面介绍海云系统模型协同机制的运行原理。

1）在海云协同模型中定义了一组服务请求类型集，这组服务请求类型集是一组特定的服务请求类型和处理这个服务请求所需计算任务的映射集。

2）当客户端服务请求被提交到服务请求类型决策器时（海端实时响应服务判定器和云端服务请求类型决策器），决策器会解析出描述服务请求的类型标识符。

3）服务请求类型决策器利用解析到的服务请求类型标识符，搜索已定义的服务请求类型集来确定所需的计算任务。

4）服务请求类型决策器把所确定的计算任务提交到相应的计算模块（海计算节点、大数据实时计算框架、大数据分析与挖掘框架）执行。

5）计算模块在完成计算任务后把结果以服务的形式推送给服务请求客户端（海计算节点、客户端应用程序），完成对服务请求的响应。

6.5.2.5　海端计算系统

在物联网系统中存在实时数据感知和处理任务以及实时响应型服务请求，将这种类型的数据处理和服务响应任务都提交到云端执行会消耗时间和网络带宽。一方面由于物联网系统中实时感应数据异构且庞大，另一方面是由于实时响应服务的高度实时性要求，例如车辆碰撞预警系统中的实时服务响应。因此，海端计算系统的核心在于本地数据存储和计算，即在本地无线传感器节点中完成对实时感知数据的存储和处理工作，从而确保无线传感器节点之间的实时服务响应。

例如：安装有无线传感器节点的一辆汽车正在靠近一个交通事故现场，此时服务响应信

息为一条交通事故预警信息，提醒车辆提前减速慢行，绕开事故现场。海端计算系统的核心设计理念在于，在类似车辆碰撞预警系统的实际应用场景中，预警信息的产生并不需要依赖物联网系统的全局感知数据，而仅仅只是和事故现场车辆状态有关的局部传感信息，因此这些局部传感信息的处理完全可以独立于云端物联网大数据管理系统而在传感器自身完成。图6-25为海端计算系统的详细架构。

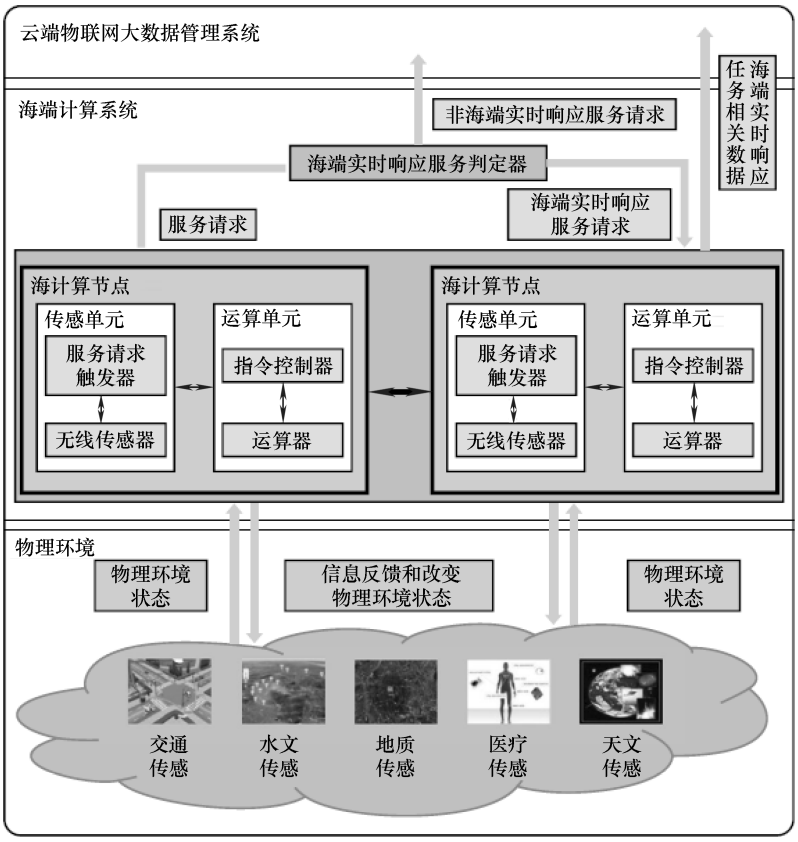


图6-25　海端计算系统框架

如图6-25所示，海计算节点由传感单元和运算单元构成，传感单元负责感知和存储物联网传感数据，而运算单元负责完成海端实时响应服务所需的数据处理和服务消息生成以及推送等任务，传感单元和运算单元协同完成海端动态自组织网络的构建以及海端实时服务响应等任务，即海计算。

由于物联网应用的多样化，物联网系统将呈现一个可扩展的分布式的结构，因此海端计算系统不仅降低了网络流量的负载，同时海端计算系统的高度自治性将给物联网系统的扩展带来架构上的灵活性。必须强调，在海端计算系统中，由于海计算节点负责完成局部感知数据的存储和计算任务，因此设计具有更强存储和计算能力的无线传感器是海计算问题的重要部分。增强无线传感器的性能，属于电子设计的范畴，不在本节的讨论范围之内。

6.5.2.6　云端物联网大数据管理系统

在海云协同模型中，海端计算系统针对那些依赖局部感知、本地存储和本地计算并且要

求高实时性服务响应的物联网应用给出了解决方案。而云端物联网大数据管理系统的设计则是针对那些依赖全局感知、云端存储和海量复杂计算的物联网应用。

在这些复杂的依赖海量数据和计算的应用中，海量感知数据有可能包括服务于交通流量预测的道路状况数据流；服务于病人状态监控和病情预测的医疗传感数据；服务于物流跟踪和客户兴趣分析的物流和商品零售感知数据流等。

海量的复杂计算则可能包括利用大数据实时流计算技术实时计算出用户请求的最佳导航路径并推送给请求客户端；建立可行的机器学习模型利用大量的历史路况数据作为训练集来预测未来某个时间段的交通流量；利用 Apriori 算法或 FP-Tree 算法等数据挖掘方法从大量的电子商务网站交易记录中提取关联规则等。

因此，设计高效的物联网大数据存取组件（如分布式存储系统 Amazon S3、Google Bigtable 和 HDFS 等），提出新的面向物联网大数据的实时计算技术，提出高效的面向物联网大数据分析和挖掘方法来满足上述实际应用的多样化需求，是设计云端物联网大数据管理系统的核心问题。

近年来，云计算受到了业界的高度关注并且成为分布式计算、资源共享、按需服务获取等问题的通用解决方案。Open Stack 是一个提供了基础设施即服务（Infrastructure as a Service，IaaS）的软件项目，由控制了大量计算、存储和网络资源的一系列相互作用的组件构成。由于 HDFS 和 MapReduce 编程模型的功能强大，Hadoop 已经成为大规模数据分析问题的首选工具。因此，使用 Open Stack 和 Hadoop 计算框架来构建云端物联网大数据管理系统，图 6-26 为其系统架构。

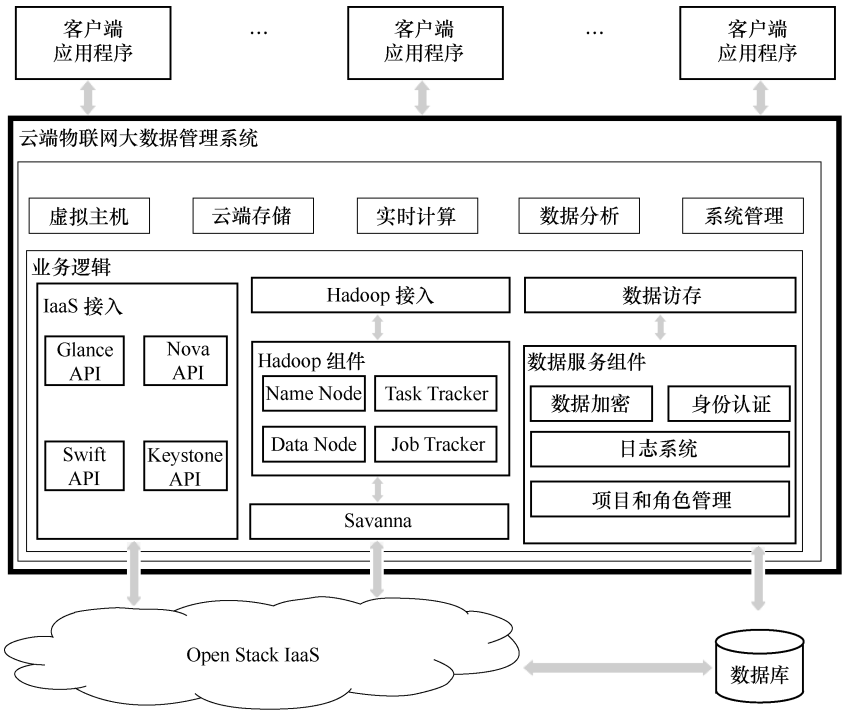


图 6-26　云端物联网大数据管理系统架构

云端系统实现了一系列旨在处理和响应云端服务请求（云端实时响应服务请求和云端大数据分析与挖掘服务请求）的服务组件。虚拟主机服务组件向终端用户共享了云端系统的硬件和软件资源，从而终端用户可以按需使用云端系统服务集群的计算和存储资源，完成数据和计算密集型大数据处理任务（天气预测等科学计算）；云存储服务组件提供大数据的快速存取服务，这些数据包括路况实时监测数据、交通事故相关数据等实时流数据和海量电子商务网站交易数据、历史天气数据和历史路况数据等，云存储服务组件由 Open Stack 的分布式对象存储系统 Swift 实现。

实时计算服务组件执行云端实时服务响应请求所需的计算任务，包括实时路径导航服务请求等。数据分析服务组件使用一系列工具组件（数据集成和清理工具、大数据挖掘和机器学习算法库等）来执行云端大数据分析与挖掘服务请求所需的计算任务，实时计算服务组件和数据分析服务组件都由 Hadoop 计算框架实现。最后，系统管理服务组件执行与系统管理、服务租用和计费等业务相关的一系列服务。

综上所述，云端系统实现的所有服务组件都是基于 Open Stack 和 Hadoop 搭建的，因此，在服务组件集之下是一组获取 Open Stack 和 Hadoop 核心服务的访问组件（即 Glance API、Nova API、Swift API、Key Stone API 以及 Hadoop 接入组件）。数据访存模块和数据服务组件是一组实现用户认证、数据加密、系统服务计费等功能的系统支持组件。云端系统架构的最底层是 Open Stack IaaS 的核心组件以及用于用户认证、服务计费等服务的数据库系统。

6.6　云计算

物联网运营平台的功能和性能需求，发现其在以下几个方面显现出了云计算特征。

（1）对资源有大规模、海量需求

未来物联网运营平台需要存储数以亿计的传感器设备在不同时间采集的海量信息，并对这些信息进行汇总、拆分、统计、备份，这需要弹性增长的存储资源和大规模的并行计算能力。

（2）资源负载变化大

有些行业应用的峰值负载、闲时负载和正常负载之间差距明显，例如无线 POS 刷卡应用在白天较忙，而在夜晚较空闲。不同行业应用的资源负载不同，例如低频次应用一般 10min 以上甚至 1 天采集、处理一次数据，而高频次应用会要求 30s 采集、处理一次数据。另外，同一行业应用由于是面向多个用户提供服务的，因此存在负载错峰的可行性，例如居民电力抄表可以分时分区上报数据。

（3）以服务方式提供计算能力

虽然不同行业应用的业务流程和功能存在较大差异，但从物联网运营角度来看，其计算控制需求是相同的，都需要对采集的数据进行分析处理，因此可以将这部分功能从行业密切相关的流程中剥离出来，包装成面向不同行业的服务，以平台服务方式提供给客户，客户只要满足服务接口要求，就能享受到这些服务能力。例如可以在物联网运营平台实现一个大气污染监控的计算模型，并暴露服务接口，行业应用调用这个接口就能够获得监控数据分析结果。

可以说云计算与物联网平台有着天然的联系，所以很自然地针对物联网运营平台的云计

算特征，考虑引入云计算技术构建物联网运营平台。

6.6.1　云计算概述

传统模式下，企业建立一套 IT 系统不仅仅需要购买硬件等基础设施，还要买软件的许可证，需要专门的人员维护。当企业的规模扩大时还要继续升级各种软硬件设施以满足需要。对于企业来说，计算机等硬件和软件本身并非他们真正需要的，它们仅仅是完成工作、提高效率的工具而已。对个人来说，我们想正常使用计算机需要安装许多软件，而许多软件都是收费的，对不经常使用该软件的用户来说购买是非常不划算的。可不可以有这样的服务，能够提供我们需要的所有软件供我们租用？这样我们只需要在用时付少量“租金”即可“租用”到这些软件服务，为我们节省许多购买软硬件的资金。

我们每天都要用电，但我们不是每家自备发电机，它由电厂集中提供；我们每天都要用自来水，但我们不是每家都有井，它由自来水厂集中提供。这种模式极大地节约了资源，方便了我们的生活。面对计算机给我们带来的困扰，我们可不可以像使用水和电一样使用计算机资源？这些想法最终导致了云计算的产生。云计算的最终目标是将计算、服务和应用作为一种公共设施提供给公众，使人们能够像使用水、电、煤气和电话那样使用计算机资源。

云计算是由分布式计算（Distributed Computing）、并行计算（Parallel Computing）、网格计算（Grid Computing）发展来的，是一种新兴的商业计算模型。目前，对于云计算的认识在不断地发展变化，云计算仍没有普遍一致的定义。

作为一种商业计算模型，云计算是基于网络将计算任务分布在大量计算机构成的资源池中，使用户能够借助网络按需获取计算力、存储空间和信息服务。

狭义的云计算指的是厂商通过分布式计算和虚拟化技术搭建数据中心或超级计算机，以免费或按需租用方式向技术开发者或者企业客户提供数据存储、分析以及科学计算等服务，比如亚马逊数据仓库出租生意。

广义的云计算指厂商通过建立网络服务器集群，向各种不同类型客户提供在线软件服务、硬件租借、数据存储、计算分析等不同类型的服务。广义的云计算包括了更多的厂商和服务类型，例如国内用友、金蝶等管理软件厂商推出的在线财务软件。

通俗地理解是，云计算的“云”就是存在于互联网上的服务器集群上的资源，它包括硬件资源（服务器、存储器、CPU 等）和软件资源（如应用软件、集成开发环境等），本地计算机只需要通过互联网发送一个需求信息，远端就会有成千上万的计算机为你提供需要的资源并将结果返回到本地，所有的处理都在云计算提供商所提供的计算机群来完成。云计算将所有的计算资源集中起来，并由软件实现自动管理，无需人为参与。这使得应用提供者无需为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

有人打了个比方：这就好比是从古老的单台发电机模式转向了电厂集中供电的模式。它意味着计算能力也可以作为一种商品进行流通，就像煤气、水电一样，取用方便，费用低廉。最大的不同在于，它是通过互联网进行传输的。

云计算是并行计算、分布式计算和网格计算的发展，或者说是这些计算机科学概念的商业实现。云计算是虚拟化（Virtualization）、公用计算（Utility Computing）、IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）等概念混合演进并跃升的结果。总体来说，云计算可以算作是网格计算的一个商业演化版。

6.6.2　云计算的特点

（1）超大规模

“云”具有相当的规模，Amazon、IBM、微软、Yahoo 等的“云”均拥有几十万台服务器。企业私有云一般拥有成百上千台服务器。“云”能赋予用户前所未有的计算能力。

（2）虚拟化

云计算支持用户在任意位置、使用各种终端获取应用服务。所请求的资源来自“云”，而不是固定的有形实体。应用在“云”中某处运行，但实际上用户无需了解、也不用担心应用运行的具体位置。只需要一台笔记本或者一部手机，就可以通过网络服务来实现我们需要的一切，甚至包括超级计算这样的任务。

（3）高可靠性

“云”使用了数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性，使用云计算比使用本地计算机可靠。

（4）通用性

云计算不针对特定的应用，在“云”的支撑下可以构造出千变万化的应用，同一个“云”可以同时支撑不同的应用运行。

（5）高可扩展性

“云”的规模可以动态伸缩，满足应用和用户规模增长的需要。

（6）按需服务

“云”是一个庞大的资源池，你按需购买；云可以像自来水、电、煤气那样计费。

（7）极其廉价

由于“云”的特殊容错措施，因此可以采用极其廉价的节点来构成云。“云”的自动化集中式管理使大量企业无需负担日益高昂的数据中心管理成本，“云”的通用性使资源的利用率较之传统系统大幅提升，因此用户可以充分享受“云”的低成本优势，经常只要花费几百美元、几天时间就能完成以前需要数万美元、数月时间才能完成的任务。云计算可以彻底改变人们未来的生活，但同时也要重视环境问题，这样才能真正为人类进步做贡献，而不是简单的技术提升。

（8）潜在的危险性

云计算服务除了提供计算服务外，还提供了存储服务。但是云计算服务当前垄断在私人机构（企业）手中，而他们仅仅能够提供商业信用。对于政府机构、商业机构（特别像银行这样持有敏感数据的商业机构）对于选择云计算服务应保持足够的警惕。一旦商业用户大规模使用私人机构提供的云计算服务，无论其技术优势有多强，都不可避免地让这些私人机构以“数据（信息）”的重要性挟制整个社会。对于信息社会而言，“信息”是至关重要的。另一方面，云计算中的数据对于数据所有者以外的其他用户云计算用户是保密的，但是对于提供云计算的商业机构而言确实毫无秘密可言。所有这些潜在的危险，是商业机构和政府机构选择云计算服务、特别是国外机构提供的云计算服务时，不得不考虑的一个重要的前提。

6.6.3　云计算的分类

云计算按照服务类型大致可以分为3类：将基础设施作为服务（IaaS）、将平台作为服务（PaaS）和将软件作为服务（SaaS），如图6-27所示。

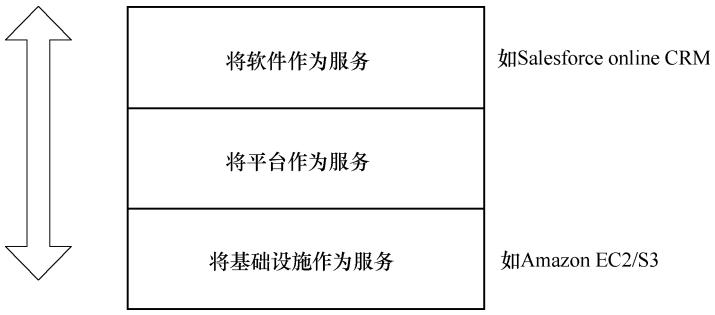


图6-27　云计算服务类型

IaaS将硬件设备等基础资源封装成服务供用户使用，如Amazon云计算（Amazon Web-Services，AWS）的弹性计算云EC2和简单存储服务S3。在IaaS环境中，用户相当于在使用裸机和磁盘，既可以让它运行Windows操作系统，也可以让它运行Linux操作系统，因而几乎可以做任何想做的事情，但用户必须考虑如何才能让多台机器协同工作起来。AWS提供了在节点之间互通消息的接口简单队列服务（Simple Queue Service，SQS）。IaaS最大优势在于它允许用户动态申请或释放节点，按使用量计费。运行IaaS的服务器规模达到几十万台之多，用户因而可以认为能够申请的资源几乎是无限的。而IaaS是由公众共享的，因而具有更高的资源使用效率。PaaS对资源的抽象层次更进一层，它提供用户应用程序的运行环境，微软的云计算操作系统Microsoft Windows Azure可大致归入这一类。PaaS自身负责资源的动态扩展和容错管理，用户应用程序不必过多考虑节点间的配合问题。但与此同时，用户的自主权降低，必须使用特定的编程环境并遵照特定的编程模型。这有点像在高性能集群计算机里进行MPI编程，只适用于解决某些特定的计算问题。

SaaS的针对性更强，它将某些特定应用软件功能封装成服务，如Salesforce公司提供的在线客户关系管理（Client Relationship Management，CRM）服务。SaaS既不像PaaS一样提供计算或存储资源类型的服务，也不像IaaS一样提供运行用户自定义应用程序的环境，它只提供某些专门用途的服务供应用调用。需要指出的是，随着云计算的深化发展，不同云计算解决方案之间相互渗透融合，同一种产品往往横跨两种以上类型。

6.6.4　云计算体系结构及其技术

6.6.4.1　云计算体系结构

云计算至少作为虚拟化的一种延伸，影响范围已经越来越大。但是，目前云计算还不能支持复杂的企业环境。因此云计算架构呼之欲出，经验表明，在云计算走向成熟之前，我们更应该关注系统云计算架构的细节。基于对现有的一些云计算产品的分析和个人一些经验，总结出一套云计算体系结构，如图6-28所示。云计算的体系结构主要包括云端用户、管理系统、部署工具、资源监控、服务目录、资源监控、服务器集群。

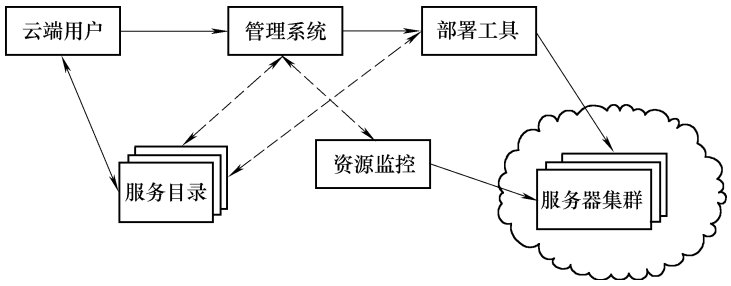


图 6-28　云计算体系结构

（1）云端用户

提供云用户请求服务的交互界面，用户通过 Web 浏览器可以注册、登录及定制服务、配置和管理用户。主要有以下几种技术：

1）HTML：标准的 Web 页面技术，现在主要以 HTML4 为主，但是将要推出的 HTML5 会在很多方面推动 Web 页面的发展，比如视频和本地存储等方面。

2）JavaScript：一种用于 Web 页面的动态语言，通过 JavaScript，能够极大地丰富 Web 页面的功能。

3）CSS：主要用于控制 Web 页面的外观，而且能使页面的内容与其表现形式之间优雅地分离。

4）Flash：业界最常用的 RIA（Rich Internet Applications，富互联网应用）技术，能够在现阶段提供 HTML 等技术所无法提供的基于 Web 的富应用，而且在用户体验方面，非常不错。

5）Silverlight：来自微软公司的 RIA 技术，虽然其现在市场占有率稍逊于 Flash，但由于其可以使用 C#来进行编程，所以对开发者非常友好。

（2）服务目录

用户在取得相应权限后可以选择或定制的服务列表。它在下面的基础设施层所提供资源的基础上提供了多种服务，比如缓存服务和 REST 服务等，而且这些服务既可用于支撑云端用户，也可以直接让用户调用，并主要有 5 种技术：

1）REST：通过 REST 技术，能够非常方便和优雅地将中间件层所支撑的部分服务提供给调用者。

2）多租户：就是能让一个单独的应用实例可以为多个组织服务，而且保持良好的隔离性和安全性，并且通过这种技术，能有效地降低应用的购置和维护成本。

3）并行处理：为了处理海量的数据，需要利用庞大的 X86 集群进行规模巨大的并行处理。

4）应用服务器：在原有的应用服务器的基础上为云计算做了一定程度的优化。

5）分布式缓存：通过分布式缓存技术，不仅能有效地降低对后台服务器的压力，而且还能加快相应的反应速度，最著名的分布式缓存例子莫过于 Memcached。

（3）管理系统和部署工具

提供管理和服务，能管理云用户，能对用户授权、认证、登录进行管理，并可以管理可

用计算资源和服务，接收用户发送的请求，根据用户请求并转发到相应的应用程序，调度资源智能地部署资源和应用，动态地部署、配置和回收资源。主要有下面这6个方面。

1）账号管理：通过良好的账号管理技术，能够在安全的条件下方便用户登录，并方便管理员对账号的管理。

2）SLA监控：对各个层次运行的虚拟机，服务和应用等进行性能方面的监控，以使它们都能在满足预先设定的SLA（Service Level Agreement，服务等级协议）的情况下运行。

3）计费管理：也就是对每个用户所消耗的资源等进行统计，来准确地向用户索取费用。

4）安全管理：对数据、应用和账号等IT资源采取全面保护，使其免受犯罪分子和恶意程序的侵害。

5）负载均衡：通过将流量分发给一个应用或者服务的多个实例来应对突发情况。

6）运维管理：主要是使运维操作尽可能地专业和自动化，从而降低云计算中心的运维成本。

（4）资源监控

监控和计量云系统资源的使用情况，以便做出迅速反应，完成节点同步配置、负载均衡配置和资源监控，确保资源能顺利分配合适的用户。

（5）服务器集群

虚拟的或物理的服务器，由管理系统管理，负责高并发量的用户请求处理、大运算量的计算处理、用户Web应用服务，云数据存储时采用相应数据切割算法，采用并行方式上传和下载大容量数据，主要有4种技术：

1）虚拟化：也可以理解它为基础设施层的“多租户”，因为通过虚拟化技术，能够在一个物理服务器上生成多个虚拟机，并且能在这些虚拟机之间实现全面的隔离，这样不仅能降低服务器的购置成本，而且还能同时降低服务器的运维成本，成熟的X86虚拟化技术有VMware的ESX和开源的Xen。

2）分布式存储：为了承载海量的数据，同时也要保证这些数据的可管理性，所以需要一整套分布式的存储系统。

3）关系型数据库：基本是在原有的关系型数据库的基础上做了扩展和管理等方面的优化，使其在云中更适应。

4）NoSQL：为了满足一些关系数据库所无法满足的目标，比如支撑海量的数据等，一些公司特地设计一批不是基于关系模型的数据库。

用户可通过云用户端从列表选择所需服务，其请求通过管理系统调度相应的资源，并通过部署工具分发请求、配置Web应用。

6.6.4.2　云计算的关键技术

云计算系统运用了许多技术，其中以编程模型、海量数据管理技术、海量数据存储技术、虚拟化技术、云计算平台管理技术最为关键。

（1）编程模型

MapReduce是Google开发的Java、Python、C++编程模型，它是一种简化的分布式编程模型和高效的任务调度模型，用于大规模数据集（大于1TB）的并行运算。严格的编程模型使云计算环境下的编程十分简单。MapReduce模式的思想是将要执行的问题分解成

Map（映射）和 Reduce（化简）的方式，先通过 Map 程序将数据切割成不相关的区块，分配（调度）给大量计算机处理，达到分布式运算的效果，再通过 Reduce 程序将结果汇总输出。

（2）海量数据分布存储技术

云计算系统由大量服务器组成，同时为大量用户服务，因此云计算系统采用分布式存储的方式存储数据，用冗余存储的方式保证数据的可靠性。云计算系统中广泛使用的数据存储系统是 Google 的 GFS 和 Hadoop 团队开发的 GFS 的开源实现 HDFS。GFS 即 Google 文件系统（Google File System），是一个可扩展的分布式文件系统，用于大型的、分布式的、对大量数据进行访问的应用。GFS 的设计思想不同于传统的文件系统，是针对大规模数据处理和 Google 应用特性而设计的。它运行于廉价的普通硬件上，但可以提供容错功能。它可以给大量的用户提供总体性能较高的服务。一个 GFS 集群由一个主服务器（master server）和大量的块服务器（chunk server）构成，并被许多客户（client）访问。主服务器存储文件系统的元数据包括名字空间、访问控制信息、从文件到块的映射以及块的当前位置，它也控制系统范围的活动。主服务器定期通过 HeartBeat 消息与每一个块服务器通信，给块服务器传递指令并收集它的状态。GFS 中的文件被切分为 64MB 的块并以冗余存储，每份数据在系统中保存 3 个以上备份。客户与主服务器的交换只限于对元数据的操作，所有数据方面的通信都直接和块服务器联系，这大大提高了系统的效率，防止主服务器负载过重。

（3）海量数据管理技术

云计算需要对分布的、海量的数据进行处理、分析，因此，数据管理技术必须能够高效地管理大量的数据。云计算系统中的数据管理技术主要是 Google 的 BT（Big Table）数据管理技术和 Hadoop 团队开发的开源数据管理模块 HBase。BT 是建立在 GFS、Scheduler、Lock Service 和 Map Reduce 之上的一个大型的分布式数据库，与传统的关系数据库不同，它把所有数据都作为对象来处理，形成一个巨大的表格，用来分布存储大规模结构化数据 Google 的很多项目使用 BT 来存储数据，包括网页查询，Google Earth 和 Google 金融。这些应用程序对 BT 的要求各不相同：数据大小（从 URL 到网页到卫星图像）不同，反应速度不同（从后端的大批处理到实时数据服务）。对于不同的要求，BT 都成功地提供了灵活高效的服务。

（4）虚拟化技术

通过虚拟化技术可实现软件应用与底层硬件相隔离，它包括将单个资源划分成多个虚拟资源的裂分模式，也包括将多个资源整合成一个虚拟资源的聚合模式。虚拟化技术根据对象可分成存储虚拟化、计算虚拟化、网络虚拟化等，计算虚拟化又分为系统级虚拟化、应用级虚拟化和桌面虚拟化。

（5）云计算平台管理技术

云计算资源规模庞大，服务器数量众多并分布在不同的地点，同时运行着数百种应用，如何有效地管理这些服务器，保证整个系统提供不间断的服务是巨大的挑战。云计算系统的平台管理技术能够使大量的服务器协同工作，方便地进行业务部署和开通，快速发现和恢复系统故障，通过自动化、智能化的手段实现大规模系统的可靠运营。

6.7　物联网中的数据挖掘

面对物联网中海量的信息，不能原地停留在采集信息的层面，因为采集到的信息往往是分散的，不具有关联性，如若不集中处理，难以发现有价值的规律信息。再者，集中处理后的数据不进行决策分析也不能为服务人群提供有效合理的建议。准确地提取有用的信息并快速做出最优决策正是用户所渴求的，这就需要在物联网的基础上进一步结合数据挖掘（Data Mining）技术的强大支撑和决策支持系统的辅助决策，提高物联网面向用户的效率。

物联网中数据挖掘技术的应用大大方便了信息的收集和管理。物联网中的感知识别层和传输层通过其相关技术将大量信息传输到综合应用层，在综合应用层利用数据挖掘技术首先对数据进行预处理，经过数据准备、数据选择、数据完整性及一致性检查，冗余滤除，数据变换等操作对数据进行层层“过滤”和筛选，再选择合适的数据挖掘算法从数据中提取有价值的数据或规则。

互联网将信息互联互通，物联网将现实世界的物体通过传感器和互联网连接起来，并通过云存储、云计算实现云服务。物联网具有行业应用的特征，依赖云计算对采集到的各行各业、数据格式各不相同的海量数据进行整合、管理和存储，并在整个物联网中提供数据挖掘服务，实现预测、决策，进而反向控制这些传感网络，达到控制物联网中客观事物运动和发展进程的目的。数据挖掘是决策支持和过程控制的重要技术支撑手段，它是物联网中的重要一环。物联网中的数据挖掘已经从传统意义上的数据统计分析、潜在模式的发现与挖掘，转向物联网中不可缺少的工具和环节。

6.7.1　物联网与数据挖掘

6.7.1.1　数据挖掘技术简介

数据挖掘技术也叫作知识发现，所谓数据挖掘就是从大量数据中发现对人们有价值的概念、模式和规律等，它是一个揭示出隐含的、先前未知的并有潜在价值的信息的过程。它是一门交叉科学，主要涉及数据库技术、人工智能、机器学习、统计学、信息检索和模式识别等领域，有十分广阔的应用前景。随着物联网的发展，数据挖掘技术也必然会在物联网中得到广泛运用。一个完整的数据挖掘过程，是个很庞大的系统，主要结构如图 6-29 所示，主要分为以下几个部分：

1）确定业务对象。在进行数据挖掘之前，最重要的一步就是要明确业务问题并且弄清数据挖掘的目的，然后再找数据的来源。数据挖掘的来源很多，只要具备大量数据的来源都可以进行挖掘，虽然最后的结构是不可预测的，但要探索的问题必须是可以预见的，否则进行数据挖掘时是不会成功的。

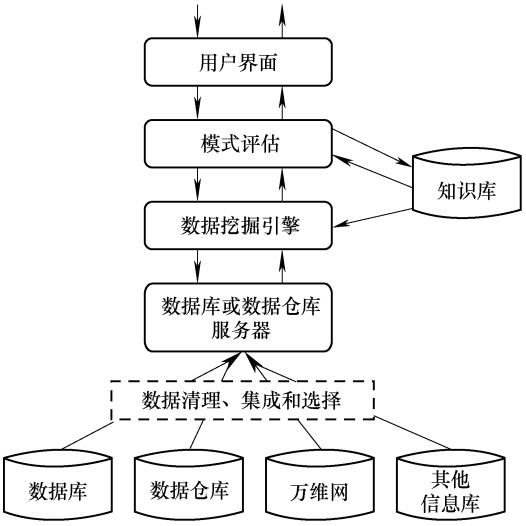


图 6-29　数据挖掘系统结构

2）数据预处理。由于数据的来源很多，其中包含很多的数据信息，在确定了数据来源后，必须首先对数据信息进行数据预处理。数据预处理一般包括数据清理、数据集成、数据变换和数据规约4个处理过程。

3）数据的转换。将数据转换成一个分析模型，这个分析模型是针对挖掘算法建立的，建立一个真正适合挖掘算法的分析模型是数据挖掘成功的关键。

4）数据挖掘过程。对所得到的经过转换的数据进行挖掘，除了进行完善并选择合适的挖掘算法外，其余一切工作都能自动地完成。

5）模式评估。解释并评估结果，其使用的分析方法一般应视数据挖掘操作而定，通常会用到可视化技术。根据某种兴趣度量，识别表示知识的真正有用的模式。

6）知识的同化。使用可视化和知识表示技术，向用户提供挖掘的知识。

7）用户界面。最后需要将数据挖掘的结果展示给用户，提供给用户适当的操作界面进行操作，以得到相关的结果。

6.7.1.2　物联网中的大数据应用

可以将物联网的数据挖掘分为4个模块，包括：感知层、传输层、数据层、数据挖掘服务层，如图6-30所示。

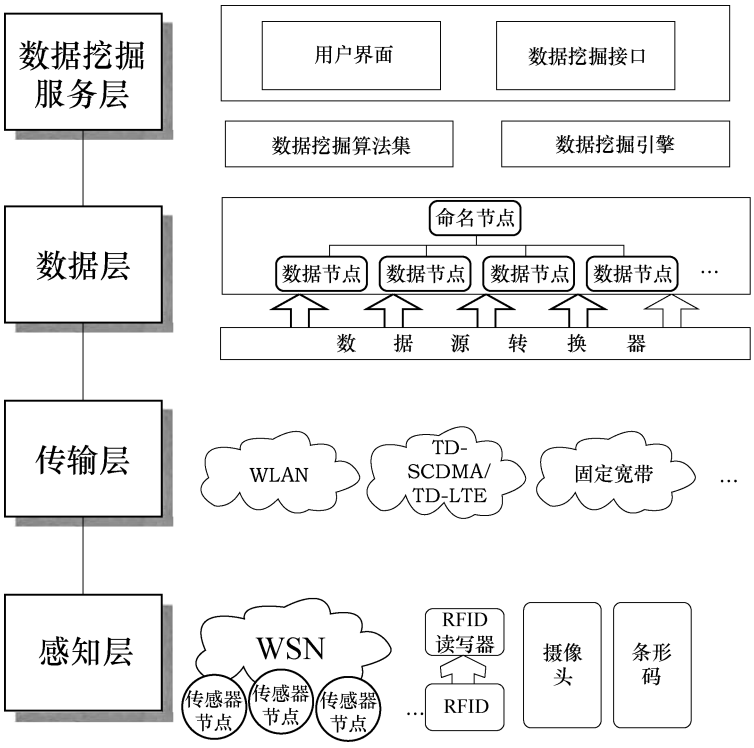


图6-30　物联网数据挖掘架构

（1）物联网感知层

感知层的作用主要是在目标区域内布置大量的采集节点，这些节点通过传感器、摄像头或其他仪器仪表来采集物联网数据，其中这些数据在物联网感知层内会存在通信，即存在无线传感器网络，通过这些网络汇聚数据到汇聚节点，然后对数据进行汇总、存储并且通过传

输层最终传输到云平台数据中心。

（2）传输层

传输层主要是集传感器网络、无线网络、有线网络等多种网络形态于一体的高速、无缝、可靠的数据传输网络，能够灵活快速地将感知数据传输至云计算数据中心，实现更加全面的互通互联；将各类监测设备进行联网数据传输，实现物联网中监测设备的网络化高速数据传输。

（3）数据层

数据层对于整个物联网数据挖掘平台是至关重要的，由于我们已经提到了物联网数据的异构性、海量性等特点，因此在数据层如何解决物联网这些数据存储及处理的问题决定了物联网数据挖掘平台的可行性和性能。数据层主要包括两个重要模块：数据源转换模块、分布式存储模块。数据源转换模块主要用于物联网中异构数据的转换，分布式存储模块主要结合了 Hadoop 平台的文件系统 HDFS，采用分布式方式存储物联网海量数据。

由于在物联网中，不同的对象会由不同的数据类型来表示，甚至相同的对象都会用不同的数据来表示，因此数据源转换器的作用主要是来解决物联网数据异构性，它不仅可以保证数据存储的完整性，还能保证数据挖掘的顺利进行。数据源转换模块相当于数据层与感知层中各个监测设备的接口，并完成数据包解码以及按相应数据模型使分布式存储模块存储的都是有效并且完整的数据。

（4）数据挖掘服务层

数据挖掘服务层主要包括数据准备模块、数据挖掘引擎模块以及用户模块。数据准备模块主要包含了对于数据的清理、变换、数据规约等；数据挖掘引擎模块主要包含数据挖掘算法集和模式评估等；用户模块主要包含数据挖掘知识的可视化表示。根据知识挖掘的类型不同，数据挖掘引擎模块可以包括的功能主要有特征、区分、关联、聚类、局外者、趋势和演化分析、偏差分析、类似性分析等。提供这些功能的关键在于数据挖掘引擎模块中算法集提供各种功能的算法，而在 Hadoop 平台中数据挖掘算法需要对传统经典数据挖掘算法进行改进，即进行算法并行化处理。

用户模块是整个物联网数据挖掘平台直接面向使用人员的部分，所以应该具有良好的友好性，用户可以通过界面操作进行数据挖掘任务，并能够得到可以被理解的知识。为了增强平台的可移植性，在用户服务底层模块增加开放接口，从而可以使第三方调用物联网数据挖掘平台的功能，使物联网应用更加丰富。

6.7.2　物联网数据挖掘的关键问题

6.7.2.1　物联网系统中数据的特点

1）数据量大。每个物联网系统均拥有成千上万甚至更多的传感设备，这些传感设备不断向数据中心传输采集到的数据。数据中心不仅要存储当前接收到的数据，同时需要保存历史数据，用以支持对象的状态跟踪、数据统计分析及数据挖掘。因此，物联网系统中数据挖掘任务面临的第一个关键问题是数据量大。

2）数据类型复杂。物联网系统监控的对象种类繁多，包括交通、生物、森林、建筑等。不同监控对象所采集的信息各不相同，例如交通系统中需要采集视频信息，医学监控系统需要采集诸如脉搏、血压等生理信息以及医学立体影响信息等。可见物联网系统采集的数

据类型复杂，包括文本类型、图像类型、视频类型等。

3）数据具有异构性。物联网系统中包含多种传感终端，如 GPS 传感终端、RFID 传感终端、视频传感终端、无线传感器等。不同的传感终端采集到的数据的格式和语义均不相同。数据的异构性为数据存储与挖掘增加难度。

4）高度动态性。每个时刻都有不同的传感终端添加到物联网中或者从物联网中移除。随着传感器节点的增加，其采集到的数据要插入到数据库中。同样当一个传感器节点从物联网中移除后，数据库不应再记录该传感器节点采集到的数据。一个物联网系统含有大量的传感器节点，每个传感器节点动态变化频繁，因此物联网系统中的数据具有高度动态性。

5）时空特性。物联网系统的传感终端分布在不同地区，每个传感终端采集到的数据均反映该时刻监控对象的状态及其他信息。感知数据在特定时间和特定空间内才有意义，如果不在这个地点或过了这个时间，数据的意义可能就不大了。因此，复杂的时空特性是物联网系统中数据的一个显著特点。

6）不完整性。物联网系统的传感终端在无人监控状态下工作，每个传感终端随时可能受到自然因素或者人为因素的攻击，包括雷电破坏、人工恶意破坏等，导致传感终端数据接收不完整。另一方面，尽管传感终端可以被广泛地部署在不同地理位置，但是依然无法覆盖每一个角落，因此空间数据收集不完整也是物联网系统数据的特点之一。

6.7.2.2　物联网对数据挖掘的要求

1）实时高效数据挖掘。物联网系统中任何一个控制端均需要对环境进行实时分析并做出正确决策。因此实时、高效是物联网系统对数据挖掘最为关键的要求之一。

2）分布式数据挖掘。物联网计算设备和数据随机分布，必须采用分布式并行数据挖掘。

3）数据质量控制。多源、多模态、多媒体、多格式数据的存储与管理是控制数据质量、获得真实结果的重要保证。

4）决策控制。挖掘出的模式、规则、特征指标用于预测、决策和控制。

5）挖掘任务。主要包括数据抽取、分类预测、聚类、关联规则发现等。

6.7.2.3　物联网环境数据挖掘存在的挑战

1）数据挖掘算法的选择。选择合适的算法，并采取适当的并行策略，才能提高并行效率。因此算法的设计变得非常重要，参数的调节变得必不可少，而且参数的调节直接影响最终的结果。

2）不确定性。首先数据挖掘任务的描述具有不确定性，数据采集和预处理也带有很多的不确定性；其次是数据挖掘方法和结果有不确定性；最后由于每个用户所关注的最终的挖掘目标不一样，这就导致了对挖掘结果的评价也有不确定性。不确定性是数据挖掘在物联网系统中面临的最大挑战。

3）可信性与安全性。在云计算环境下做数据挖掘会导致数据挖掘云服务软件可信性问题。首先是服务的正确性和服务的安全性；其次是服务的质量，服务质量由可用、可靠和高性能这 3 个方面来度量。

6.7.3　基于云计算的物联网数据挖掘模型

基于云计算的物联网数据挖掘模型构架分为五层，分别是物联网数据接入层、数据集成

层、数据挖掘平台层、业务控制层和交互层，如图 6-31 所示。

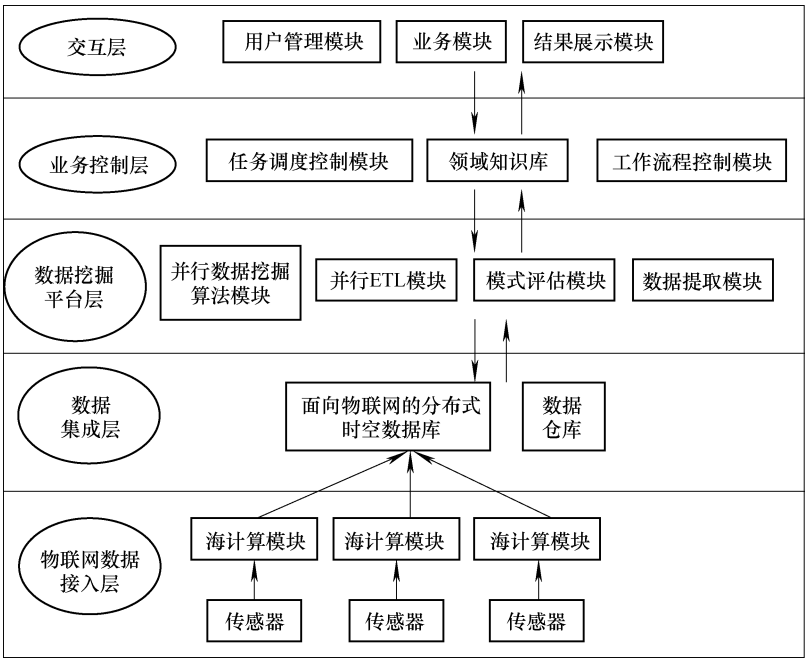


图 6-31　基于云计算的物联网数据挖掘模型框架

6. 7. 3. 1　结构层次

（1）物联网数据接入层

物联网接入层实现数据采集、提取关键数据、将关键数据传输到数据集成层的作用。物联网数据接入层包括各种传感终端，如 GPS 传感终端、RFID 传感终端、视频传感终端、无线传感器等。利用这些传感终端监控现实世界对象，采集反应监控对象的状态及其他信息并发送到相应的海计算节点。采集的数据包括文本数据、图像数据和视频数据等。海计算节点对传感数据进行预处理，提取关键数据并传输到数据集成层，即面向物联网的分布式时空数据库。

（2）数据集成层

数据集成层存储物联网系统传感终端采集到的关键数据，为数据挖掘提供数据源。面向物联网的分布式时空数据库存储物联网系统的关键数据，并为数据仓库的构造提供数据源。数据仓库中的数据是按照主题来组织的，存储的数据可以从历史的观点提供信息，面对多数据源，经过清晰和转换后的数据仓库可以为数据挖掘提供面向历史的发现知识的数据环境。

（3）数据挖掘平台层

数据挖掘平台层是整个构架的核心之一，提供数据挖掘阶段业务需要的各个模块，并具有较细的粒度。如数据预处理、模式评估、数据挖掘等功能模块。这一层的主要任务是实现各种任务过程中算法的并行化，并将挖掘结果返回给业务控制层。

（4）业务控制层

这一层提供业务逻辑并实现对各种业务流程的控制和调度。根据用户提交的业务请求，任务调度控制模块结合领域知识库指导工作流程控制模块控制和调度数据挖掘平台层的多个

模块来完成挖掘任务，并将挖掘结果返回给交互层。

（5）交互层

这一层主要提供系统和用户之间的接口。通过提供具有良好表现形式的图形界面，使得用户可以登录系统定制各种细粒度的业务，查看或者保存各种输出结果。

6.7.3.2　功能模块

（1）物联网数据接入层模块

海计算模块：海计算模块包含大量海计算节点。主要用以存储传感终端采集的各种数据，并对数据进行预处理，主要包括去除噪声数据和重复数据，处理不完整数据，识别并提取关键数据，统一数据格式。最后将预处理后的关键数据传输给数据集成层。在物联网数据接入层对数据进行预处理有利于节省网络带宽，同时有利于数据集成层的存储和进一步应用。

（2）数据挖掘平台层模块

并行数据挖掘算法模块：为数据挖掘各种任务提供并行算法。作为数据挖掘引擎，包含一个能够提供各种基于云计算进行并行数据挖掘算法的库，用于完成各种数据挖掘任务。

并行 ETL 模块：对数据进行预处理。输入的数据来源于面向物联网的分布式时空数据库与数据仓库，为数据挖掘过程进行数据清理、提取、转换和加载。

模式评估模块：对产生的模式进行评估。符合用户要求的结果存入领域知识库，领域知识库可以辅助业务控制逻辑指导数据挖掘过程。

数据提取模块：根据挖掘任务的不同，在面向物联网的时空数据库或数据仓库中提取相关的数据。

（3）业务控制层模块

任务调度控制模块：响应上层的业务模块，对完成业务所需的子业务进行调用和管理，并通过调用底层模块完成业务。

工作流程控制模块：对业务状态进行监控和管理。可将具体的信息参数返回给本层的任务调度控制模块。

（4）交互层

用户管理模块：实现用户身份的识别以及相应权限的设置，同时也包括对用户登录或者注销等常用的管理。

业务模块：实现细粒度的用户业务需求的提交。用户提交的各种业务通过业务模块得到。

结果展示模块：实现用户对业务结果的查看、分析和保存等功能。用来将系统的返回结果交付给用户。

参 考 文 献

[1] 徐力今. 数字电视中间件的研究与模型设计 [J]. 有线电视技术，2005（14）：46-50.

[2] 陈焕经，王振强. 数字电视中间件综述 [J] . 中国有线电视，2003（11）：15-17.

[3] 张春红，裘晓峰，夏海伦，等. 物联网技术与应用 [M]. 北京：人民邮电出版社，2011.

[4] 甘勇，郑富娥，吉星，等. RFID 中间件关键技术研究 [J]. 电子技术与应用，2007（9）：130-132.

[5] 贺平，蒋亚军，赵会群 . EPC 系统的 Savant 中间件技术及其设计实现 [J]. 计算机工程与应用，2006

（09）：221-225.
[6] 李巡生，陈光，保云，等. 面向应用编程的嵌入式中间件技术实现途径 [J]. 云南大学学报：自然科学版，2007，29（S2）：162-166.
[7] 王学峰. 物联网与人工智能 [J]. 数字通信世界，2011（04）：77-79.
[8] 张福生，边杏宾. 物联网中间件技术是物联网产业链的重要环节 [J]. 科技创新与生产力，2011（3）：41-43.
[9] 董立峰. RFID 中间件技术在物联网中的应用及研究 [J]. 科技信息，2010（10）：74-75.
[10] 陈峥，刘慧，宫雪. 物联网之 SAVANT 体系结构的分析研究 [J]. 物流科技，2006（07）：18-21.
[11] 单承赣，焦宗东，张琦 . EPC 物联网中的“信使”——ONS [J]. 中国电子商情（RFID 技术与应用），2007（3）：17-18.
[12] 陈宝震，焦宗东. 物联网中的通信语言 PML [J]. 中国电子商情（RFID 技术与应用），2007 (5)：43-46.
[13] 胡清，詹宜巨，黄小虎. 基于 RFID 企业物联网及中间件技术研究 [J]. 微计算机信息，2009，25（7-2）：158-160.
[14] 秦滔. 物联网与 RFID 中间件探讨 [J]. 电脑与信息技术，2010，18（4）：17-19.
[15] 阴琳芳，龚华明. 中间件技术在物联网中的应用探讨 [J]. 科技广场，2010（11）：36-38.
[16] 马延珂. 数字电视中间件技术 [J]. 北京广播学院学报自然科学版，2003，10（1）：13-17.

第 7 章　物联网业务支撑平台

7.1　物联网业务

物联网是指通过信息传感设备，按照约定的协议，把任何物品与信息网络连接起来，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。物联网将机器的通信延伸到物与物之间的通信，将有限的信息采集提升到信息的全面感知，将移动通信技术扩展为多种通信技术的结合，并最终将以机器通信为核心的服务发展到以物理世界信息化为核心的服务，在更多的应用领域中衍生出丰富多彩的物联网应用。

物联网业务可以广泛地应用到众多的行业中，包括车辆、电力、金融、环保、石油、个人与企业安防、水文、军事、消防、气象、煤炭、农业与林业、电梯等。

7.1.1　物联网的业务介绍

在物联网业务应用的行业中，当前优先看好的是智能电网、公交运输、面向个人和企业的安防、金融这几个行业的物联网应用。至2009 年9 月日本 KDDI 已售出约200 万台物联网通信模块，其中 50% 的终端已在用。KDDI 的物联网业务针对的两个主要行业市场分别为车辆管理（占到总量的 50%，主要销售给汽车制造企业）和儿童定位（占到总量的 10%，销售给保安服务公司，不面向最终用户）。KDDI 的物联网业务策略为：聚焦在提供优质完善的通信服务，收取通信费用，而不提供行业应用服务；定制嵌入式通信模块，嵌入到各种行业终端和应用，实现对产业价值链的把握。法国电信是欧洲第一家提供完整端到端物联网方案的电信运营商，已拥有超过 110 万户的物联网 UIM 终端。法国电信拥有的两个物联网业务品牌分别为数据通道服务“物联网 data”、管理和应用服务“物联网 Connect”：3 个物联网应用产品子品牌分别为基于定位的车辆综合管理“Fleet Link”、基于定位的个人管理“Lone Work”以及提供移动网定位服务的“Cell ID”。Sprint 已经通过 ODI（Open Device Initiative，主动设备开放）计划认证了 160 名厂商的物联网终端设备，这些终端设备被广泛应用到智能抄表、无线 POS 机、车载管理等多个行业领域内。Sprint 在 2009 年年中与物联网虚拟运营商 DataSmart 签订多年战略合作关系，由 DataSmart 向 Sprint 客户提供完整的端到端解决方案（包括终端测试、应用试用、开发支撑、资费方案、终端管理等）。2009 年 7 月 Verizon Wireless 与高通宣布建立一家专门提供物联网产品的合资公司，将利用高通多样的物联网解决方案，同时充分利用 Verizon Wireless 先进的连接技术与专业的设备认证技术，为包括医疗保健、制造业、公共事业、消费品等各种细分市场提供相关服务。目前，中国移动物联网终端数已经超过 300 万，主要集中在电力、交通和金融行业，截至 2009 年 6 月中国移动已在全国 31 个省、市、自治区开通了物联网业务，相继推出了“车务通”“电梯卫士”“消防监控系统”“爱贝通”和“关爱通”这 5 项物联网应用，在接下来的 5 年平均增长率

将可能达到60%以上。中国移动在2007年前后就在重庆建立了物联网运营支撑中心，负责全国物联网产品的研发、物联网平台的建设等工作。至2010年年底，中国电信的物联网用户数已接近100万。

7.1.2　物联网的业务分类

物联网的分类有多种，如按照接入方式、应用类型等方式进行分类。一种简单粗略的分类方法是类似于计算机网络划分为专用网网络和公众网络，我们可以从物联网的用户范围不同，划分为公众物联网和专用物联网两种。公众物联网是指为满足大众生活和信息的需求提供的物联网服务，而专用物联网就是满足企业、团体或个人特色应用需求，有针对性地提供的专业性的物联网业务应用。专用物联网可以利用公众网络（如：Internet）、专网（局域网、企业网络或移动通信互联网中公用网络中的专享资源）等进行信息传送。

目前可以纳入物联网范围的应用很多，在此，我们大致按照技术特征可以大致把物联网的业务分为4类，分别是：身份相关业务、信息汇聚型业务、协同感知型业务、泛在服务。

现在业界有一种认识，认为从信息汇聚，到协同感知，再到泛在聚合是物联网的必然发展趋势，但是并不是所有物联网的业务都会发展到泛在聚合的阶段。很多应用和服务只要求信息汇聚，但是这些信息是封闭的、机密的、只对小部分群体有效，这种服务和应用在现实中很难实现泛在汇聚。

7.1.2.1　身份相关业务

身份相关业务类应用主要是利用射频标志（如RFID）、二维码、条码等可以标识身份的技术，并基于身份所提供的各类服务。按照终端是去识别其他身份信息，还是被识别可以分为主动模式和被动模式，按照服务是提供给个人还是提供给企业，又可以分为个人应用和企业业务两大类。

对于不同的应用实现的方式可能各有不同，一般方法是：在物上贴上RFID标签，读写设备通过读取RFID标签中的信息，尤其是ID信息，通过这个ID信息向物联网名称解析服务器请求以获取该ID所对应的进一步详细信息的统一资源标志符（Uniform Resource Identifier，URI），读写设备通过这个统一资源标志符进行进一步的信息获取。

7.1.2.2　信息汇聚型业务

信息汇聚型业务主要是由物联网终端采集、处理、经通信网络上报数据，由物联网平台处理，提交给具体的应用和服务，由物联网平台统一对物联网终端、数据、应用和服务，以及第三方进行统一管理。具体的应用类型，如自动抄表、电梯管理、物流、交通管理等。

信息汇聚型业务的具体架构如图7-1所示。整个系统主要由机器到机器（M2M）终端、网络、平台、应用以及运营系统构成，下图中的通信网络是用移动通信网络进行说明的，固定网也可以作为其数据传送通道。移动通信网络是信息传送的载体，可以采用各种通信方式进行传送，如：短信、彩信、IP等。

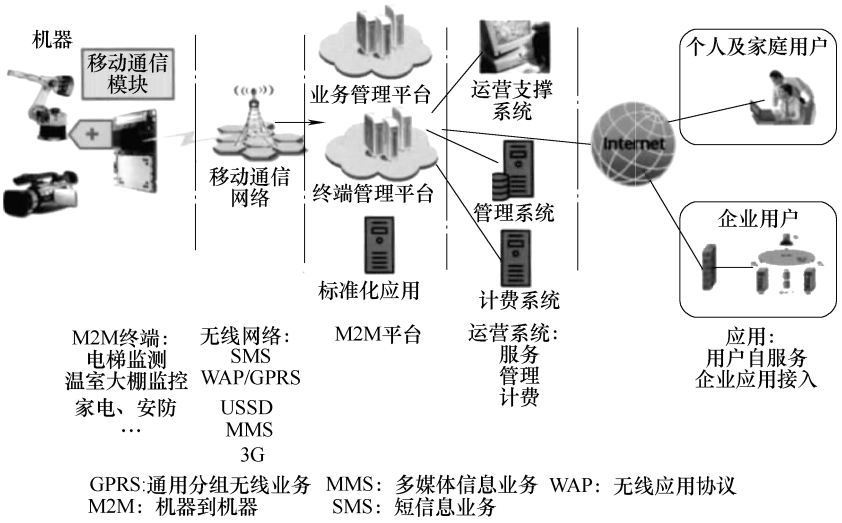


图 7-1　信息汇聚型业务

在架构中，如果进一步考虑适应不同的网络、考虑接入更大终端数量，以及便于将物联网服务更便利地提供给企业用户，可以分别考虑引入物联网接入网关设备和物联网应用行业网关设备，接入网关设备可以支持物联网终端的汇聚和对不同网络的支持，尤其对网络地址转换（Network Address Translation，NAT）穿越的支持；行业网关设备将物联网服务或者服务的接口，以行业网关方式提供给企业，有点类似现在的短信网关之类的设备。

7.1.2.3　协同感知型业务

在信息汇聚型业务中，物联网的终端只要接受物联网平台管理，执行数据采集、简单处理、上报、接受管理等功能，物联网的终端之间不需要进行通信。

随着物联网的发展，物联网应用应该能够担负起更为重要的任务、更为复杂的业务和服务。这类服务需要物联网终端之间、物联网终端和人之间执行更为复杂的通信，同时，这种通信能力在可靠性、时延等方面可能有更高要求，对物联网终端的智能化要求也更为突出，这样，才能满足协同处理的要求。

这类应用非常具体的内容，如应用场景、需求、架构、通信协议之类，从长远来看，协同感知型业务是物联网发展的趋势。

7.1.2.4　泛在服务

泛在服务以无所不在、无所不包、无所不能为基本特征，以实现在任何时间、任何地点、任何人、任何物都能顺畅地通信为目标，是人类通信服务的极致。

未来的泛在服务会不会以互联网为载体。通过将现实世界中的“物”的信息融入到互联网上，让“物”通过互联网更好地被更多的用户所共享，这不仅是物联网的飞跃，也是互联网的一个重要发展。同时，在可管可控的电信网络中，也将“物”纳入统一管理，支持物与人、物与物之间的直接通信，支持更广泛范围内的信息共享，电信网和物联网的融合也将是一个重要方向。

在电信网范围内对这方面的研究处于初步阶段，2009 年 9 月，ITU-T 通过了 Y.2002

(Y. NGN-UbiNet)，这也是对泛在网络的一个初步研究，给出了泛在网的愿景。

“5C+5Any”是泛在网络的关键特征，5C分别是：融合、内容、计算、通信、连接；5Any分别是：任意时间、任意地点、任意服务、任意网络、任意对象。

总体含义是：通过底层的全连通的、可靠的、智能的网络，以及融合的内容技术、微技术和生命技术，将通信服务扩展到教育、智能建筑、供应链、健康医疗、日常生活、灾害管理、安全服务、运输等行业，并为人们提供更好的服务，让人们享受信息通信的便利，让信息通信改变人们的生活，更好地服务于人们的生活。

7.2　物联网业务系统架构

根据应用场景的不同，现阶段物联网应用主要分为3类：RFID相关应用、基于传感网络的应用，以及M2M两化融合相关应用，从而实现物联网典型的“管、控、营一体化”功能化应用场景。本节将从业务系统架构角度分别描绘三大类应用的典型场景。

7.2.1　基于RFID的应用架构

电子标签可能是3类技术体系中最灵活的能够把“物”改变成为“智能物”的设备，它的主要应用是给移动和非移动资产贴上标签，实现各种跟踪和管理。按瑞士ETH Fleisch教授的划分，RFID是穿孔卡、键盘和条码等应用技术的延伸，它比条码等技术自动化程度高，但它们都属于提高“输入”效率的技术，也都应该属于物联网应用技术范畴。Auto-ID中心的EPCGlobal体系就是针对所有可电子化的编码方式的，而不只是针对RFID。RFID只是编码的一种载体，此外还有其他基于物理、化学过程的载体，例如同方试金石公司的防伪技术。EPCGlobal提出了Auto-ID系统的五大技术组成，分别是EPC（电子产品码）标签、RFID标签阅读器、ALE中间件实现信息的过滤和采集、EPCIS信息服务系统，以及信息发现服务（包括ONS和PML）。由于该体系从一开始就让世界各大洲的从业人员充分参与，EPCGlobal标准（架构图见图7-2）得到了较广泛认同，这里不再对其标准体系架构赘述。

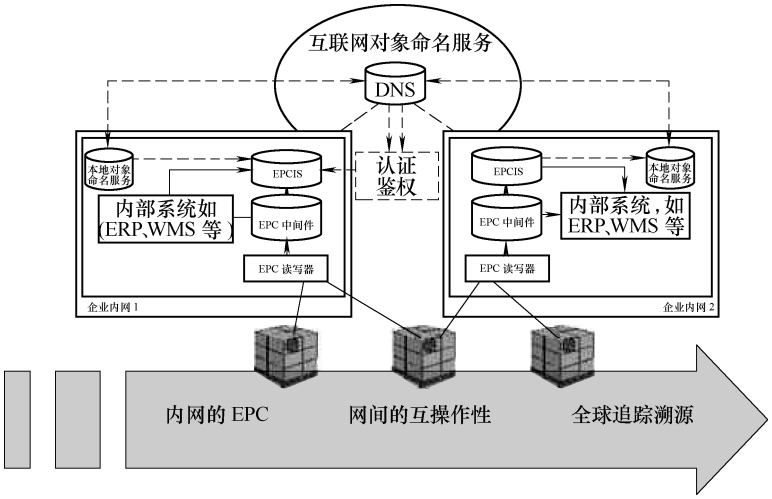


图7-2　EPCGlobal标准架构图

ONS（即对象命名服务）主要处理电子产品码与对应的 EPCIS 信息服务器地址的查询和映射管理（见图 7-3），类似于互联网络中已经很成熟的域名解析服务（DNS）。在设计 ONS 规范时，EPCGlobal 组织要求必须结合现有互联网基础设施和相关规范进行，这显然是一个正确的决定。于是 ONS 基本上按 DNS 的原理实现，甚至采用了 DNS 的现有基础设施，现今全球 ONS 服务也是 EPCGlobal 委由世界最大的 DNS 营运商 VeriSign 营运。

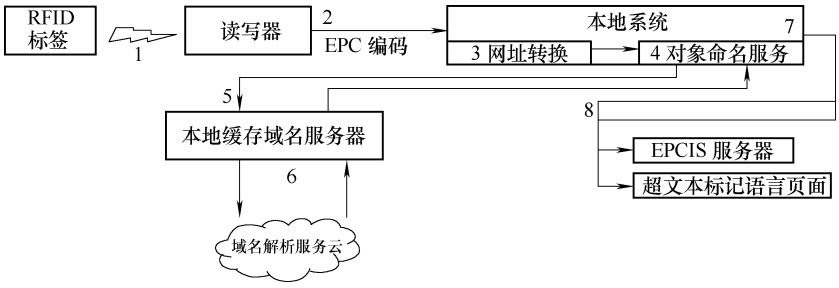


图 7-3　ONS 服务原理

EPC 识别只是“标签”，所有关于产品有用的信息都用一种新型的标准的 XML——PML 来描述，PML 的作用就像互联网的基本语言 HTML 一样。

有了 ONS 和 PML，以 RFID 为主的 EPC 系统才真正从 Network of Things 走向了 Internet of Things（物联网）。基于 ONS 和 PML，企业对 RFID 技术的应用将由企业内部的闭环应用过渡到供应链的开环应用上，实现真正的“物联网”。ONS 和 PML 作为物联网框架下的关键技术，有着广泛的应用前景。相比之下，传感网和 M2M 从业群体的技术架构还没有完全上升到 ONS/PML 这样同等的“物联网”技术体系高度，这大概也就是 Auto-ID 人群认为物联网概念是他们首创的主要原因吧。笔者认为，在走向物联网的道路上，传感网和 M2M 群体应该借鉴和直接采用 ONS/PML 技术体系。

7.2.2　基于传感网络的应用架构

当人们谈论传感网络的时候，一般主要是指无线传感器网络（WSN），此外还有视觉传感器网络（Visual Sensor Networks，VSN）以及人体传感器网络（Body Sensor Networks，BSN）等其他传感网，这里我们也主要讨论 WSN。

WSN 由分布在自由空间里的一组“自治的”无线传感器组成，共同协作完成对特定周边环境状况的监控，包括温度、湿度、化学成分、压力、声音、位移、振动、污染颗粒等。WSN 中的一个节点（或叫 Mote）一般由一个无线收发器、一个微控制器和一个电源组成，形成自治重构（Ad-Hoc 或 Self-Configuring）网络，包括无线网状网（Mesh Networks）和移动自重构网（MANET）等。无线传感器网络目前还是计算机和通信专业的学者们一个非常活跃的研究领域，十多年前 IBM（苏黎世研究中心）、微软等大企业就开始投入巨资研究传感网，但商业收效甚微，所以大企业已经基本不再投入做纯 WSN 研究（哈佛大学 Welsh 教授语），WSN 的研究主要还是在大学和国立研究机构。

WSN 的研究大多还专注于网络底层（包括非 IP 的 ZigBee、TinyOS 和基于 IP 的 6LoWPAN 等），以及电源的持久性等问题，按照其目前的发展，笔者认为 WSN 离真正的“物联网”还有一定距离，对像 EPCGlobal 中 ONS 和 PML 等物联网层面的问题研究还不够。

另外，WSN 的研究者们太热衷于无线技术，忽略了感知层用有线现场总线和传输层用长距离无线通信的组合。从实用和商业推广的角度，这个组合早已经达到稳定和大规模应用的水平。

7.2.3　基于 M2M 的应用架构

业界认同的 M2M 理念和技术架构覆盖的范围应该是最广泛的，包含了 EPCGlobal 和 WSN 的部分内容，也覆盖了有线和无线两种通信方式，一个典型的 M2M 系统由图 7-4 所示的几个部分组成。

图 7-4　典型的 M2M 系统

M2M 也覆盖和拓展了工业信息化（两化融合）中传统的 SCADA（Supervisory Control And Data Acquisition，数据采集与监视控制）系统。SCADA 系统在工业、建筑、能源、设施管理等领域和现在的 M2M 系统一样，行使设备数据收集和远程监控监测的工作。乍一看，M2M 和 SCADA 似乎是一样的，但由于 M2M 基于互联网等新技术，有很多标准化的东西（如 XML、WebServices/SOA 等）做基础，它和传统的 SCADA 是有区别的，好多 SCADA 系统基本上还是基于陈旧的 C/S 架构。

M2M 有 MVNE（Mobile Virtual Network Enabler，移动虚拟网络提供商）和 MVNO（Mobile Virtual Network Operator，移动虚拟网络运营商）两种业务模式，MVNO 业务模式在中国还未形成（或政策不允许），但在美国早已经存在，JasperWireless、Aeris 等公司一直在做基于 SaaS 营运的 M2M 业务 MVNO，也就是 MMO（M2M Mobile Operator）。由于 M2M/智慧地球最近的发展催生了许多新的机遇，美国各大营运商如 Verizon、ATT 等以前都不直接做 M2M 业务，最近都纷纷成立了 M2M 业务部门，直接开展 M2M 业务，例如 AT&T 和 Amazon 合作直接支撑其 Kindle 电子阅读器无线接入服务。结果迫使一些原来的 MVNO 成了 MVNE，JasperWireless 就是例子，ATT&T 正好采用了 JasperWireless 平台。

7.3　物联网业务支撑参考平台

7.3.1　业务平台需求分析

创新的物联网应用通常需要使用到多个异构接入网络的基本功能，为此，物联网的业务

平台特征需求可以归纳如下：

（1）自主自治

由于物联网由数量庞大的异构接入网络组成，任何运营商都不能够事无巨细地管理和控制如此大量的设备。所以，物联网的业务平台应当具有更多的自主性，能够最大程度地自管理、自配置、自修复，并根据环境变化自发调整自己的行为。这种自主并不意味着让网络完全独立于人的干预而运行，而是指网络能够按照人的利益和偏好去完成自发的控制过程，从而最终实现业务的开发、部署和实施。

（2）自适应

作为一个通用的业务平台，物联网业务平台将面临更多的变化。这种变化既包括下层基础网络能力的变化，又包括上层应用开发需求的变化。业务平台需要应对产业链的多个环节。为了延长整个业务平台的生命周期，业务平台内部结构需要有相应的适应环境变化的能力。

（3）智能感知

为了具备足够的智能，平台需要具有足够感知的能力，必须能够感知用户的状态和周围的环境，从而根据这些信息调整对业务逻辑判断、业务调用等行为。用户的相关信息是非常丰富的，包括物理位置、生理状况、心理状态、个人历史信息、日常行为习惯等。如何获取需要的信息是智能感知计算实现时的关键技术点。不同的内容来自于各种分布式的数据源，因此业务平台需要对这些信息进行收集和管理，并运用一些相关的推理决策机制对这些原始数据进行评估和分析。

（4）安全可信

业务平台所处的网络是以多种无线网络接入互联网实现的异构集成网络。开放的无线网络使得恶意攻击者能够随时随地以任意方式对网络发起攻击。此外，这种以用户需求为中心主动向用户提供服务的方式，决定了平台中必定存储着大量的个人隐私以及保密性很强的一些信息，这样的一些信息一旦被人恶意地加以利用或是散布都将给国家的安全和社会的稳定带来强烈的冲击和影响。因而，要求业务平台提供基于认证和信任的安全机制、个人隐私的保护机制等安全可信保证。

物联网业务应用作为信息产业新的经济增长点，核心的运营支撑平台必须服务于产业链上的各参与方，包括物联网运营商、业务提供商以及用户等，通过运营支撑平台的推广与合作，广泛发展物联网业务，推动物联网市场快速增长，从而形成共赢的良性产业生态环境。

从物联网运营的角度，首先，物联网业务运营支撑平台能够对原有语音、彩信、短信等电信业务能力进行封装，提供开放接口，从而降低业务创新的难度。其次，平台需要具备透明的认证鉴权、接入计费、网管、业务支撑等功能，同时为所有的物联网业务者提供统一的运营维护、管理界面。再次，平台必须提供不同行业应用系统、社会公共服务系统（120、110 和 119 等）的接入，实现行业信息的整合，提供大量数据的存储、分析和挖掘，具有云计算的能力。还有，该平台需要具有开放、灵活、异构的架构，不但能够与传感器网络、移动接入以及宽带接入网络等无缝集成，而且能够与现有的运营商已有的承载网和业务网无缝集成，平台具备可扩展性、易融合性等。此外，平台必须具备完善的管理能力，实现统一的合作伙伴的管理、统一的用户管理、统一的业务产品管理、统一的订购管理、统一的认证鉴权管理等。

从业务提供者的角度，希望专注于业务应用的开发，关注业务数据和业务流程的处理，期望简单、快速的业务开发环境，不希望分散精力处理不同的传感器、不同的电信能力以及不同的门户系统。首先，平台需要对提交的物联网业务开发需求，自动匹配适合的传感器资源，并经传感器与业务平台进行对应登记注册。其次，提供标准的开发接口、开发传感器与平台的交互界面，编写详细的数据上传、下载、存储以及其他等业务交互流程，并根据需要，激活比如语音、视频、短信、计费、网管、故障、告警等其他的工作流。此外，平台需要为每个业务应用提供用户统计、业务统计、计费统计等功能，提供符合自身业务需要的门户。

从物联网业务的使用者角度，由于物联网本身具有的复杂性、普遍性，因此每个用户可能有多个物联网应用，有多种方式接入，客户希望可以像使用水和电一样方便地接入使用物联网业务，有自己的业务申请注册管理界面、有自己的费用结算、充值划账界面，有自己的鉴权管理、委托管理、查询统计、多种提醒等功能。

7.3.2　物联网业务运营支撑平台方案举例

7.3.2.1　平台框架

在对物联网业务运营支撑平台建设的需求分析的基础上，结合传统电信运营企业面临的挑战，一种典型的物联网业务运营支撑平台的架构如图 7-5 所示。

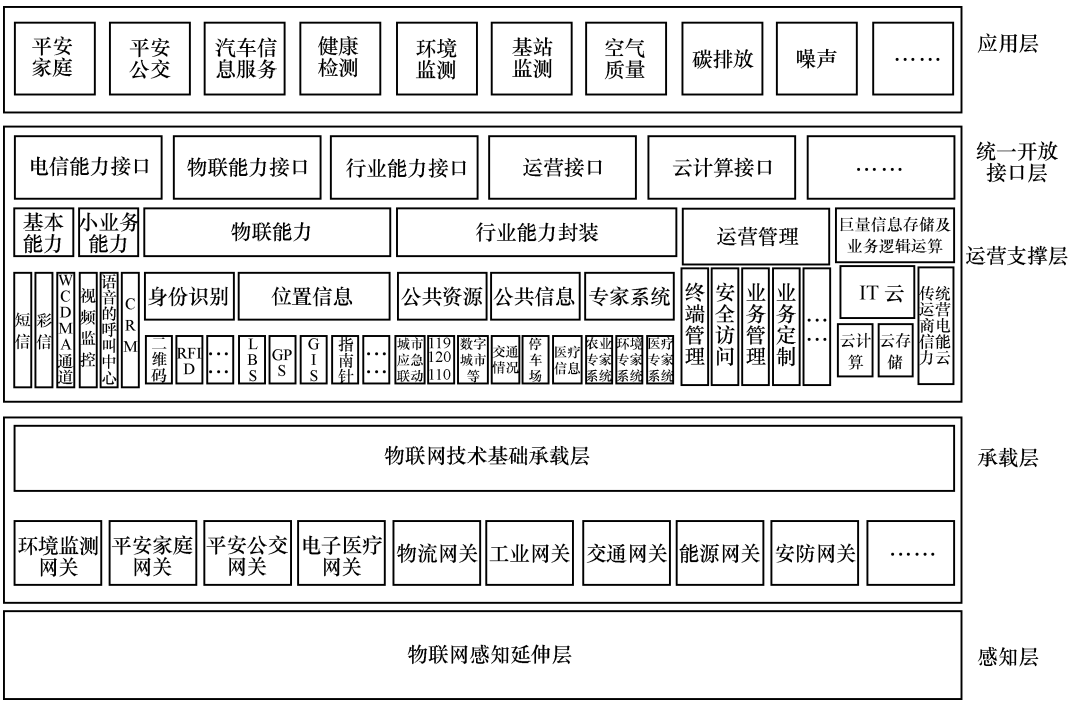


图 7-5　物联网业务运营支撑平台的架构图

整个系统采用开放分层结构来实现，自下而上包括感知层、承载层、运营支撑层、统一开放接口层以及应用层等，其中，无线传感器网络、RFID 读写器、M2M 终端设备，构成物联网的感知层；运营商提供的网络资源，包括 GSM、WCDMA 以及 3G 网络和有线网络，构

成网络传输层，实现感知层信息的上传以及应用层信息的下达；结合运营商的业务运营支撑环境，构成物联网的运营支撑层。平台通过标准化协议引入物联网终端和应用，并提供鉴权、计费、业务管理、业务受理等功能；各种行业应用构成物联网的应用层，它们通过开放接口调用各种能力，满足业务需求。

考虑物联网应用的数据存储，数据运算都比目前的互联网高几个数量级，因此设计该平台需要考虑在传统 IT 系统的基础之上，融合云计算的方案，以增强平台的计算能力、扩展能力。利用云计算解决了运营商大量闲置的计算和存储能力的问题，为适应业务量的弹性增长、降低应用部署成本提供了重要的技术手段。

物联网的应用会用到大量的电信能力，比如短信、彩信、定位、呼叫中心等，也可能用到第三方的服务和资源。通过该平台，实现业务能力的汇聚和开放，大大降低开发难度，为物联网的飞速发展奠定基础，是物联网未来实现信息智能化处理的普遍架构形式。在此基础上，实现机器到机器、机器到人、人到机器的互动与协作，实现物联网应用的融合。

7.3.2.2　对外接口设计

如图 7-6 所示，物联网业务运营支撑平台总共包括六大接口。其中，与终端设备的接口主要完成对物联网终端的接入；应用系统接口主要为上层应用系统提供标准接口，为各行业应用系统提供基于面向服务的功能调用；管理接口主要提供客户签约信息，其中包括客户信息、所开通移动 M2M 的 SIM 卡信息，用户业务信息，用户账户信息等；计费接口主要记录物联网感知终端接入平台的各种计费数据，并与计费系统的互通；网管接口主要提供与管理分析平台系统的接口，实现与告警、监控、性能分析等功能系统的接口；业务能力接口主要提供与短信中心、彩信中心的接口，通过此接口终端就可以通过短信与终端接入平台进行短信互通。

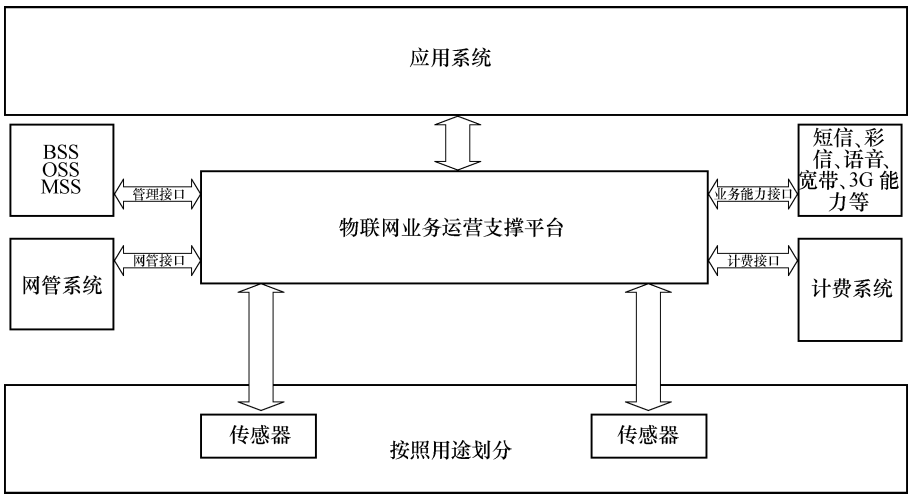


图 7-6　物联网业务运营支撑平台接口

7.3.2.3　关键模块

根据物联网业务运营的特点，物联网业务运营支撑平台需要包括 4 个核心模块以及 4 个边缘模块等关键组件，如图 7-7 所示。

4 个核心模块分别为安全访问控制模块、终端管理模块、业务管理模块以及业务定制模块。其中安全访问控制模块主要是针对号码资源管理、SIM 个人化、密钥管理和鉴权访问控

制；终端管理模块主要是对物联网终端的注册、状态和监控管理；业务管理模块主要是针对业务集成和全网应用以及各级应用管理；业务定制模块主要考虑对各行业的二次开发和增值业务管理。

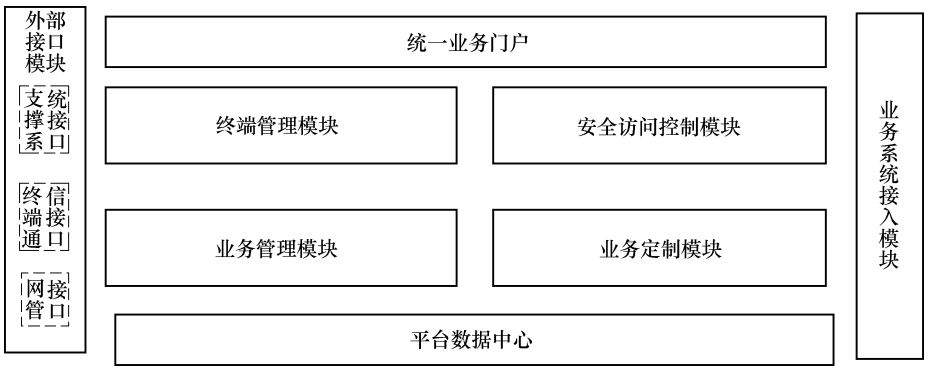


图 7-7　关键模块分布图

除此之外，还需要 4 个边缘模块提供业务信息的接入、展示、存储和反馈等，分别为业务系统接入模块、统一业务门户、外部接口模块以及平台数据中心等。其中统一业务接入模块主要提供对业务的接入、鉴权以及计费等模型，可为运营商、应用提供商、用户三者提供基于统一共用的计费模型，可以各自获取关注的计费信息，对接入和鉴权也采用统一的模型进行处理；统一的门户提供统一的运营商门户、应用提供者门户以及用户门户，各个不同使用者的门户功能按照各自需求不同提供不同配置；统一的对外接口将为传感网提供统一的接入管理接口，对电信能力提供统一的接入，对支撑系统提供统一的集成以及对行业系统和社会公众系统提供统一的集成等；统一的数据中心将针对不同业务应用系统的数据提供存储，并在此基础上进行深入的业务数据挖掘，挖掘关联行业的应用，从而推出更多的行业融合增值业务。

7.4　电信运营商在物联网业务发展中的策略

在物联网方面，电信运营商应坚持合作与开放，联合产业链各方共同克服面临的问题和困难，推动物联网的发展。

7.4.1　广泛开展产业合作，积极整合产业链资源

从“完善物联网产业链、建设物联网运营支撑平台、推动物联网相关标准制订、加快 IPv4 向 IPv6 的演进、构建云计算平台”等环节入手，与产业链各方共同努力推动物联网的发展。

积极介入物联网领域的研发和标准化工作，努力成为中国物联网产业的主力军。要高度重视物联网应用的标准化工作，规范化与标准化是物联网规模化推广和降低应用成本的关键。

如前文所述，物联网基本架构分为感知层、传输层和应用层，涉及的技术范围非常广泛，运营商很难对所有的技术都深入研究，物联网的发展要依靠产业链各界共同合作推进，

因此对于不同层应当采取不同的策略。

1. 感知层——用

感知层的无线传感器网络技术标准众多，无论国际还是国内，都有相当数量的科研机构和专业公司在研究，部分无线传感器网络技术已经具备一定规模，有成熟的产业链，电信营商至少在现阶段没有必要对感知层的无线承载、通信协议、自组网算法等方面进行深入的研究。对感知层的研究应当围绕“用”开展，以传感网和通信网的结合为切入点，关注异构网络如何实现协同工作以及如何实现可管理的感知网。

2. 传输层——建

传输层包含了接入网络和接入单元，接入网络即通信网络，要以电信运营商为主进行建设和优化。现有的通信网络是以承载人与人的通信为主的，其设计和建设都是围绕着人的通信模式，进入物联网发展的时代，不但会产生大量的通信节点，而且这些节点的通信特征与人的通信截然不同，必然对网络带来压力。同时，对物联网节点的管理也对通信网络提出了很多新问题。通信网会向着“能支撑物联网应用规模有序发展”的目标演进，在充分利用现有网络资源的原则下，根据业务量的增加，分阶段、逐步进行网络改造。

混同承载阶段：在业务发展初期，业务量不是特别大的情况下，直接采用现有网络承载物联网业务，网络不做大的改动，网络参数基本不变。由于现有网络不能区分人与人的通信、物与物的通信，主要通过终端侧的配置以及对终端的管理，缓解网络的压力。

区别承载阶段：业务发展中期，物联网应用规模的增加对网络资源（如号码资源、传输资源）造成较大压力，这时需要对网络进行部分改造，使得网络侧能区别物与物的通信，采取不同策略，缓解网络压力，保障业务质量。

独立承载阶段：在物联网业务规模化后，将产生与其他通信相互干扰的问题，同时也出现了大量对通信 SLA 要求较高的物联网应用，可考虑逐步采用物理/逻辑隔离的网络承载物联网业务，如建设独立的接入网，在核心网中划分专门的互联子网等。接入单元是将感知的数据传送到通信网的关键设备，运营商需要进行掌控，根据网络的要求和用户的需求，引导设备生产厂商进行开发，并积极推动产业链发展。

3. 应用层——汇

应用层包括了中间件和应用。中间件层面，运营商可以充分发挥优势，将结合网络的运营能力开放出来，提供给应用集成，为用户提供更好的服务。

应用是物联网发展的基础，物联网的发展要依赖应用的驱动，然而物联网应用非常丰富，涉及行业众多，深入到每个行业，其总量也许并不是非常大，但这些行业加起来占有的比重却非常高，长尾效应明显。因此需要从行业市场和垂直市场两个方面分别制定策略，对于行业市场，采取与产业链合作，鼓励合作伙伴积极推进；电信运营商则更多关注垂直市场层面，发挥运营优势，开发标准化应用，可适用于多个行业，如全球眼视频监控应用、定位应用等，这些垂直市场的标准化应用又可以作为物联网的基础能力，通过中间件方式提供。

7.4.2　选取具体行业进行重点突破

由于初期存在盈利模式和运营经验不足的客观约束，因此要结合政府所引导发展的重点

行业和领域进行重点突破，成功后再进行大规模的复制推广。下面电信运营商物联网业务规划的 3 点建议：

1. 通过政府采购带动物联网产业发展

我国政府的规模比较大，政府机关、医院、学校、大型国企、社会团体的采购都通过政府采购完成。政府及其有关部门对物联网产品实行采购，不但推动物联网初期发展，也可以得到多方面的效益，众所周知，物联网的应用在环保、交通、司法、医疗等多方面会大大推动社会发展，因此，政府采购物联网产品不但是支持物联网的发展，同时也是建设智能社会的一项举措。

对于电信运营商而言，如何有效抓住政府这一关键用户，与政府一同承担建设智能社会的社会责任，成为业务发展初期的重中之重。

首先，运营商应该以国家战略政策为导向，选取重点业务推向政府用户，例如目前全球都在热切关注环保问题，通过这一契机推广污水、空气监控等智能环保业务会得到政府支持，又如当前很多城市的交通问题尤为突出，此时推出智能公交站台、车管专家等智能交通也是明智之举。其次，物联网业务应该大力发展自主创新业务，增强运营商的研发资源，为我国物联网业务良性发展提供技术储备。

物联网发展初期离不开政府的支持，通过政府采购来带动物联网产业的发展，选举重点业务进行突破，大力发展自主创新，物联网业务才能得到稳步发展。

2. 选取具体行业进行重点突破

政府用户通过强大的影响力来推动物联网产业初期的发展，而个人用户的预期利润也是有限的，因此行业用户是一个重点赢利点。

电信运营商在挖掘行业用户的过程中，可以选取具体行业进行重点突破，以物流园为例，物流本应是高端服务业，而目前我国物流业信息化和技术水平发展比较滞后，因此物流业可以借助物联网，构建统一信息平台，形成物畅其流、快捷准时的服务体系，成为真正的高端服务产业。电信运营商针对这样的行业，推出物流信息化业务，抓住行业用户这一盈利较大的群体，积极研究行业特点，把行业特点与物联网产品结合，物联网业务才能争取到一个较大的赢利点。

3. 为集团客户定制解决方案，突出解决方案的针对性

集团客户是一个全新又庞大的市场，有独立的客户需求和市场特征。电信运营商早在基础移动业务中就运用过为用户定制业务的方式。随着物联网不断发展，运营商通过网络、移动优势，有针对性地为集团客户定制解决方案，例如为企业提供一卡通系统、考勤管理系统、门禁管理系统等解决方案，突出解决方案的针对性，寻求及构建良好的商务模式，从而使集团客户信息化消费成为运营商的重要业务，物联网业务才能大大拓展其市场。

7.4.3　开展有针对性的部署和差异化应用服务

一是充分考虑自身网络的优势和特征，切入特定的行业应用；二是打造整合在统一品牌下的标准化产品，并在各地分公司结合当地实际将标准化产品与个性化应用相结合进行推广；三是要逐步拓展行业应用辐射下的公众服务和自服务管理领域，使已有的大规模公众客户和企业自身首先成为物联网的使用者和推广者。

7.4.4 M2M 市场发展策略建议

1. 加强宣传，培育 M2M 市场

目前国内 M2M 认知度还不高，建议从信息化和网络融合的角度加大宣传力度，宣传 M2M 业务的优势和意义，以增加潜在的客户群。可以由运营商、设备商、集成商等联合起来成立 M2M 产业联盟，并定期组织 M2M 发展论坛进行应用讨论。

2. 瞄准产业链空白，大力发展中小企业

目前我国 M2M 发展才起步，市场机会很多。政府应当鼓励中小企业学习 Telit、Wyless 等新兴企业的经验，抓住机遇，瞄准我国目前的 M2M 产业链的空白，成为行业新兴的管理咨询提供商、外部硬件提供商、M2M 服务商或者应用设备软件提供商等。尤其外部硬件商和应用设备软件商，随着国内电信运营商对 M2M 重视的提高，会有大量合作开发的机会，例如 Telenor 在制定车辆信息通信解决方案的过程中，采用了 Telit 的通信模块和 Airbiquity 的通信平台。

3. 继续由运营商主导整个 M2M 产业链

国内 M2M 产业目前仍然比较零散，缺乏主导力量，需要电信运营商来牵头，组织系统集成商、设备商和软件商建立统一的接入标准及运营平台，这样产业链的其他环节才能有机会发展。单靠企业信息化无法支撑整个 M2M 产业链，必须上升到运营商和行业的高度才能推动 M2M 市场发展和产业链整合。

建议已经拥有 M2M 应用平台并推出相关业务的电信运营商参考 Orange 的经营策略，加大宣传力度，并针对行业客户进行个性化解决方案的制定，来拓展国内纵向市场。建议目前没有 M2M 应用平台建设打算的电信运营商仿照 AT&T，以提供网络连接给 M2M 服务商的形式参与到 M2M 市场中，等机会成熟了再进行自己的业务开发。

参 考 文 献

[1] 马华兴. 解惑3G业务：概念、实现和规划 [M]. 北京：北京邮电大学出版社，2006.

[2] 解冲锋，孙颖，高歆雅. 物联网与电信网融合策略探讨 [J]. 电信科学，2009（12）：9-12.

[3] 中兴通讯. 定制化开发建设统一的 M2M [N]. 中国电子报. 2009 年 006 版.

[4] ITU-T Y.2002 (Y.NGN-UbiNet). Overview of ubiquitous netw orking and of its s upport in NGN [S]. 2009.

[5] K Traub, G Allgaird. EPCglobal Architecture Framework, 2005.

[6] 7R Murty, A Gosain, M Tierney, A Brody… Citysense：A vision for an urban-scale wireless networking testbed psu. edu - Proceedings of the …, 2008 - Citeseer.

[7] 胡昌玮，周光涛，唐雄燕. 物联网业务运营支撑平台的方案研究 [J]. 信息通信技术，2010（2）：52-57.

[8] 马慧子. 移动运营商物联网业务规划研究 [C]. 中国通信学会通信管理委员会 2010 年学术研讨会，2010：33-37.

[9] 于明，胡前笑，周伟杰. 运营商 M2M 技术与业务发展策略研究 [J]. 通信世界 2009（40）：B6-B7.

第 8 章　安全与管理

2009 年以来，“智慧地球”概念炙手可热，物联网有关内容大量在人们的视野中出现。然而，随着物联网发展进入物物互联阶段，由于其设备数量庞大、复杂多元、缺少有效监控、节点资源有限、结构动态离散，安全问题日渐突出，除面对互联网和移动通信网络的传统网络安全挑战之外，还存在着一些特殊安全挑战，如果不未雨绸缪，必将阻碍其发展进程。因此，虽然物联网的应用，可以使人与物的交互更加方便，给人们带来诸多便利，在物联网的应用中，如果网络安全没有保证，那么个人隐私、物品信息等随时有可能被泄露。而且如果网络不安全，物联网的应用为黑客提供了远程控制他人物品、甚至操纵城市供电系统，夺去机场管理权的可能性。不可否认，物联网在信息安全方面存在很多问题。根据物联网的上述特点，除了面对一些通信网络的传统网络安全问题之外，还存在着一些与已有移动网络安全不同的特殊安全问题，这是由于物联网是由大量的设备构成，而相对缺乏人的管理和智能控制所造成的。

8.1　物联网的安全体系结构

在我国，随着人们对物联网理解的不断加深，物联网的内涵进一步明朗。在 2009 年的百家讲坛上，时任中国移动总裁王建宙指出，物联网应该具备 3 个特征：一是安全感知；二是可靠传递；三是智能处理。尽管对物联网概念还有一些其他的不同描述，但内涵基本相同。因此我们在分析物联网的安全性时，也相应地将其分为 3 个逻辑层，即感知层、传输层和处理层。除此之外，在物联网的综合应用方面还应该有一个应用层，它是对智能处理后的信息的利用。在某些框架中，尽管智能处理应该与应用层被作为同一个逻辑层进行处理，但是从信息安全角度考虑，将应用层独立出来更容易建立安全架构。

其实针对物联网的几个逻辑层，目前已经有很多针对性的密码技术和解决方案。但需要说明的是，物联网作为一个应用整体，各个层独立的安全措施不足以提供可靠的安全保障。而且物联网与几个逻辑层所对应的基础设施之间还存在很多本质的区别。最基本的区别可以从以下几点看到：

1）已有的对传感器网络（感知层）、互联网（传输层）、移动网（传输层）、安全多方计算、云计算（处理层）等一些安全解决方案在物联网环境可能不再适用。首先，物联网所对应的传感网的数量和终端物体的规模是单个传感网所无法相比的；其次，物联网所连接的终端设备或器件的处理能力将有很大差异，它们之间可能需要相互作用；最后，物联网所处理的数据量将比现在的互联网和移动网都大得多。

2）即使分别保证感知层、传输层和处理层的安全，也不能保证物联网的安全。这是因为物联网是融几个层于一体的大系统，许多安全问题来源于系统整合；物联网的数据共享对安全性提出了更高的要求；物联网的应用将对安全提出了新要求，比如隐私保护不属于任一层的安全需求，但却是许多物联网应用的安全需求。鉴于以上诸原因，对物联网的发展需要

重新规划并制定可持续发展的安全架构，使物联网在发展和应用过程中，其安全防护措施能够不断完善。

物联网一般分为3个层次：感知层、传输层和应用层。这种分层结构，决定了物联网安全机制的设计应当建立在各层技术特点和面临的安全威胁的基础之上。同时，基于物联网的三层体系结构，在这里我将物联网的安全分为4个层次感知层、网络层、处理层和应用层，如图8-1所示。物联网安全的核心是感知信息的安全采集、传输、处理和应用，物联网的安全模型可以描述为：安全的信息感知、可靠的数据传送和安全的信息操控。

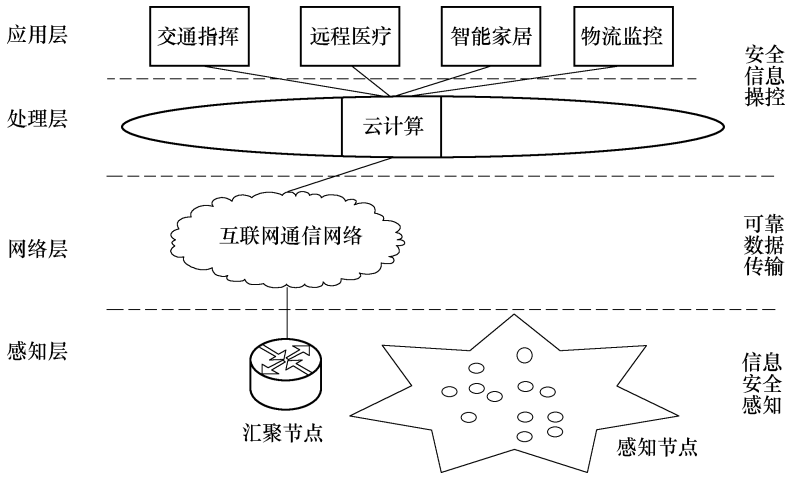


图8-1　物联网安全体系结构

随着基于RFID技术的物联网快速推广和应用，其数据安全问题在某些领域甚至已经超出了原有计算机信息系统的安全边界，成为了一个广泛关注的问题。主要原因如下：

1）标签计算能力弱：RFID标签在计算能力和功耗方面具有特有的局限性，RFID标签的存储空间极其有限，如最便宜的存储标签只有64～128位的ROM，尽可以容纳唯一的标识符。由于标签本身的成本有限，标签自身比较难以具备足够的安全能力、极容易被攻击者操控，恶意用户可能会利用合法的阅读器或者自行构造一个阅读器，直接与标签进行通信、读取、篡改甚至删除标签内所存储的数据。在没有足够信任的安全机构保护下，标签的安全性、有效性、完整性、可用性、真实性都得不到保障。

2）无线网络的脆弱性：标签层和读写器层采用无线射频信号进行通信，在通信过程中没有任何物理或者可见的接触（通过电磁波的形式进行），而无线网络固有的脆弱性使得RFID系统很容易受到各种形式的攻击。这给应用系统的数据采集提供灵活性和方便性的同时也使传递的信息暴露于大庭广众之下。

3）业务应用的隐私安全：在传统的网络中，网络层的安全和业务层的安全是相互独立的，而物联网中网络连接和业务使用是紧密结合的，物联网中传输信息的安全性和隐私性问题也成了制约物联网进一步发展的重要因素。根据RFID的物联网系统结构，我们把物联网的威胁和攻击分为两类：一类是针对物联网系统中的实体的威胁，主要是针对标签层、读写器层和应用系统层的攻击；一类是针对物联网中传输过程的威胁，包括射频通信层以及互联网层的通信威胁。

8.2　感知层安全需求和安全策略

在讨论安全问题之前，首先要了解什么是感知层。感知层的任务是全面感知外界信息，或者说是原始信息收集器。该层的典型设备包括 RFID 装置、各类传感器（如红外、超声、温度、湿度、速度等）、图像捕捉装置（摄像头）、全球定位系统（GPS）、激光扫描仪等。这些设备收集的信息通常具有明确的应用目的，因此传统上这些信息直接被处理并应用，如公路摄像头捕捉的图像信息直接用于交通监控。但是在物联网应用中，多种类型的感知信息可能会同时处理，综合利用，甚至不同感应信息的结果将影响其他控制调节行为，如湿度的感应结果可能会影响到温度或光照控制的调节。同时，物联网应用强调的是信息共享，这是物联网区别于传感网的最大特点之一。比如交通监控录像信息可能还同时被用于公安侦破、城市改造规划设计、城市环境监测等。于是，如何处理这些感知信息将直接影响到信息的有效应用。为了使同样的信息被不同应用领域有效使用，应该有综合处理平台，这就是物联网的智能处理层，因此这些感知信息需要传输到一个处理平台。

在考虑感知信息进入传输层之前，我们把传感网络本身（包括上述各种感知器件构成的网络）看作感知的部分。感知信息要通过一个或多个与外界网连接的传感节点，称之为网关节点（sink 或 gateway），所有与传感网内部节点的通信都需要经过网关节点与外界联系。在物联网的传感层，本节以传感网为例分析感知层的安全需求和策略。

8.2.1　感知层的安全挑战和安全需求

在物联网中，为了节约人力成本，在感知层大量使用传感器来标识物品设备，由人或者机器来操控它们来完成一些复杂的、危险的和机械的工作。在这种情况下，物理网中的这些物品设备多数是部署在无人监控的地点工作的，那么攻击者可以轻易接触到这些设备，针对这些设备或者它们上面的传感器进行干扰或者伪装成合法的传感器，如果国家的一些重要机构取决于物联网时，攻击者可以通过对传感器本体进行干扰，从而达到影响其表示设备的正常运行。例如，电力部门是国民经济发展的重要部门，在远距离输电过程中，有许多变电设备可通过物联网进行远程操控。在无人变电站附近，攻击者可非法使用红外装置来干扰这些设备上的传感器。如果攻击者更改设备的相关参数，后果不堪设想。而传感器通常情况下，功能简单、携带能量少，这使得它们无法拥有复杂的安全保护能力，而物联网涉及的通信网络多种多样，它们的数据传输和消息也没有特定的标准，所以没法提供统一的安全保护体系。

一般情况下，感知层采用射频识别（RFID）技术，节点之间是无线传播。攻击者很容易在节点之间的传播信号中获取敏感信息，从而伪造信号。例如：身份证系统中，攻击者可以通过感知节点间的信号交流，来获取机密信息、用户隐私，甚至可以据此伪造身份，其后果不言而喻，危害巨大。如果安置物品上的标签或读写设备设备（如物流、门禁系统）信号受到恶意干扰，很容易造成重要物品损失。

综上所述，感知层可能遇到的安全挑战包括下列情况：

1）传感网的网关节点被敌手控制，则安全性全部丢失；

2）传感网的普通节点被敌手控制（敌手掌握节点密钥）；

3）传感网的普通节点被敌手捕获（但由于没有得到节点密钥，而没有被控制）；

4）传感网的节点（普通节点或网关节点）受来自于网络的 DOS 攻击；

5）接入到物联网的超大量传感节点的标识、识别、认证和控制问题。

敌手捕获网关节点不等于控制该节点，一个传感网的网关节点实际被敌手控制的可能性很小，因为需要掌握该节点的密钥（与传感网内部节点通信的密钥或与远程信息处理平台共享的密钥），而这是很困难的。如果敌手掌握了一个网关节点与传感网内部节点的共享密钥，那么他就可以控制传感网的网关节点，并由此获得通过该网关节点传出的所有信息。但如果敌手不知道该网关节点与远程信息处理平台的共享密钥，那么他不能篡改发送的信息，只能阻止部分或全部信息的发送，但这样容易被远程信息处理平台觉察到。因此，若能识别一个被敌手控制的传感网，便可以降低甚至避免由敌手控制的传感网传来的虚假信息所造成的损失。

传感网遇到比较普遍的情况是某些普通网络节点被敌手控制而发起的攻击，传感网与这些普通节点交互的所有信息都被敌手获取。敌手的目的可能不仅仅是被动窃听，还通过所控制的网络节点传输一些错误数据。因此，传感网的安全需求应包括对恶意节点行为的判断和对这些节点的阻断，以及在阻断一些恶意节点（假定这些被阻断的节点分布是随机的）后，网络的连通性如何保障。

对传感网络分析（很难说是否为攻击行为，因为有别于主动攻击网络的行为）更为常见的情况是敌手捕获一些网络节点，不需要解析它们的预置密钥或通信密钥（这种解析需要代价和时间），只需要鉴别节点种类，比如检查节点是用于检测温度、湿度还是噪声等。有时候这种分析对敌手是很有用的。因此安全的传感网络应该有保护其工作类型的安全机制。既然传感网最终要接入其他外在网络，包括互联网，那么就难免受到来自外在网络的攻击。目前能预期到的主要攻击除了非法访问外，应该是拒绝服务（DoS）攻击了。因为传感网节点的通常资源（计算和通信能力）有限，所以对抗 DoS 攻击的能力比较脆弱，在互联网环境里不被识别为 DoS 攻击的访问就可能使传感网瘫痪，因此，传感网的安全应该包括节点抗 DoS 攻击的能力。考虑到外部访问可能直接针对传感网内部的某个节点（如远程控制启动或关闭红外装置），而传感网内部普通节点的资源一般比网关节点更小，因此，网络抗 DoS 攻击的能力应包括网关节点和普通节点两种情况。

传感网接入互联网或其他类型网络所带来的问题不仅仅是传感网如何对抗外来攻击的问题，更重要的是如何与外部设备相互认证的问题，而认证过程又需要特别考虑传感网资源的有限性，因此认证机制需要的计算和通信代价都必须尽可能小。此外，对外部互联网来说，其所连接的不同传感网的数量可能是一个庞大的数字，如何区分这些传感网及其内部节点，有效地识别它们，是安全机制能够建立的前提。

针对上述的挑战，感知层的安全总体需求可以总结为如下几点：

1）机密性：多数传感网内部不需要认证和密钥管理，如统一部署的共享一个密钥的传感网；

2）密钥协商：部分传感网内部节点进行数据传输前需要预先协商会话密钥；

3）节点认证：个别传感网（特别当传感数据共享时）需要节点认证，确保非法节点不能接入；

4）信誉评估：一些重要传感网需要对可能被敌手控制的节点行为进行评估，以降低敌

手入侵后的危害（某种程度上相当于入侵检测）；

5）安全路由：几乎所有传感网内部都需要不同的安全路由技术。

8.2.2　感知层的安全策略

了解了传感网的安全威胁，就容易建立合理的安全架构。在传感网内部，需要有效的密钥管理机制，用于保障传感网内部通信的安全。传感网内部的安全路由、联通性解决方案等都可以相对独立地使用。由于传感网类型的多样性，很难统一要求有哪些安全服务，但机密性和认证性都是必要的。机密性需要在通信时建立一个临时会话密钥，而认证性可以通过对称密码或非对称密码方案解决。使用对称密码的认证方案需要预置节点间的共享密钥，在效率上也比较高，消耗网络节点的资源较少，许多传感网都选用此方案；而使用非对称密码技术的传感网一般具有较好的计算和通信能力，并且对安全性要求更高。在认证的基础上完成密钥协商是建立会话密钥的必要步骤。安全路由和入侵检测等也是传感网应具有的性能。

由于传感网的安全一般不涉及其他网络的安全，因此是相对较独立的问题，有些已有的安全解决方案在物联网环境中也同样适用。但由于物联网环境中传感网遭受外部攻击的机会增大，因此用于独立传感网的传统安全解决方案需要提升安全等级后才能使用，也就是说在安全的要求上更高，这仅仅是量的要求，没有质的变化。相应地，传感网的安全需求所涉及的密码技术包括轻量级密码算法、轻量级密码协议、可设定安全等级的密码技术等。

8.2.3　具体案例：RFID 安全问题及策略

虽然 RFID 由于频段相容等等多种原因还没有形成统一的行业标准，但是已经有越来越多的 RFID 产品被广泛应用于零售、物流、仓储、生产制造、自动收费、动物识别和图书馆管理等领域。同时在 RFID 的应用中也面临一个不可忽视的安全问题，RFID 标签、网络和数据等各个环节都存在安全隐患。例如：消费物品的 RFID 标签可能被用于追踪，侵犯人们的位置隐私；贴有标签的商品带有销售数据可能被商业间谍充分利用；隐私侵犯者通过重写标签以篡改物品信息等。接下来的内容详细介绍了 RFID 系统中存在的各种安全问题、产生的原因以及解决策略，并分析各种策略的优缺点，最后提出解决 RFID 安全问题新的思路。

8.2.3.1　RFID 系统面临的安全攻击

针对 RFID 系统的主要安全攻击可简单地分为主动攻击和被动攻击两种类型。

主动攻击包括：

1）对获得的 RFID 标签实体，通过物理手段在实验室环境中去除芯片封装，使用微探针获取敏感信号，进而进行目标 RFID 标签重构的复杂攻击。

2）通过软件，利用微处理器的通用通信接口，通过扫描 RFID 标签和响应阅读器的探询，寻求安全协议、加密算法以及它们实现过程中的弱点，进而删除 RFID 标签内容或篡改可重写 RFID 标签内容的攻击。

3）通过干扰广播、阻塞信道或其他手段，产生异常的应用环境，使合法处理器产生故障，拒绝服务的攻击等。

被动攻击主要包括：

1）通过采用窃听技术，分析微处理器正常工作过程中产生的各种电磁特征，来获得

RFID 标签和阅读器之间或其他 RFID 通信设备之间的通信数据。

2）通过阅读器等窃听设备，跟踪商品流通动态等。

主动攻击和被动攻击都会使 RFID 应用系统承受巨大的安全风险。

主动攻击通过物理或软件方法篡改标签内容，以及通过删除标签内容及干扰广播、阻塞信道等方法来扰乱合法处理器的正常工作，是影响 RFID 应用系统正常使用的重要安全因素。尽管被动攻击不改变 RFID 标签中的内容，也不影响 RFID 应用系统的正常工作，但它是获取 RFID 信息、个人隐私和物品流通信息的重要手段，也是 RFID 系统应用的重要安全隐患。

8.2.3.2　主要解决策略

RFID 安全和隐私保护与成本之间是相互制约的。根据自动识别（Auto－ID）中心的试验数据，在设计 5 美分标签时，集成电路芯片的成本不应该超过 2 美分，这使集成电路门电路数量限制在了 7.5～15 kB。一个 96 bit 的 EPC 芯片需要 5～10 kB 的门电路，因此用于安全和隐私保护的门电路数量不能超过 2.5～5 kB，使得现有密码技术难以应用。优秀的 RFID 安全技术解决方案应该是平衡安全、隐私保护与成本的最佳方案。

现有的 RFID 安全和隐私技术可以分为两大类：一类是通过物理方法阻止标签与阅读器之间通信，另一类是通过逻辑方法增加标签安全机制。

1. *物理方法*

（1）杀死（Kill）标签

原理是使标签丧失功能，从而阻止对标签及其携带物的跟踪，如在超市买单时的处理。但是，Kill 命令使标签失去了它本身应有的优点。如商品在卖出后，标签上的信息将不再可用，不便于日后的售后服务以及用户对产品信息的进一步了解。另外，若 Kill 识别序列号（PIN）一旦泄露，可能导致恶意者对超市商品的偷盗。

（2）法拉第网罩

根据电磁场理论，由传导材料构成的容器（如法拉第网罩）可以屏蔽无线电波。使得外部的无线电信号不能进入法拉第网罩，反之亦然。把标签放进由传导材料构成的容器可以阻止标签被扫描，即被动标签接收不到信号，不能获得能量，主动标签发射的信号不能发出。因此，利用法拉第网罩可以阻止隐私侵犯者扫描标签获取信息。比如，当货币嵌入 RFID 标签后，可利用法拉第网罩原理阻止隐私侵犯者扫描，避免他人知道你包里有多少钱。

（3）主动干扰

主动干扰无线电信号是另一种屏蔽标签的方法。标签用户可以通过一个设备主动广播无线电信号用于阻止或破坏附近的 RFID 阅读器的操作。但这种方法可能导致非法干扰，使附近其他合法的 RFID 系统受到干扰，严重的是，它可能阻断附近其他无线系统。

（4）阻止标签

原理是通过采用一个特殊的阻止标签干扰防碰撞算法来实现，阅读器读取命令每次总是获得相同的应答数据，从而保护标签。

2. *逻辑方法*

（1）哈希（Hash）锁方案

Hash 锁是一种更完善的抵制标签未授权访问的安全与隐私技术。整个方案只需要采用 Hash 函数，因此成本很低。方案原理是阅读器存储每个标签的访问密钥 K，对应标签存储

的元身份（MetaID），其中 MetaID = Hash（K）。标签接收到阅读器的访问请求后发送 MetaID 作为响应，阅读器通过查询获得与标签 MetaID 对应的密钥 K 并发送给标签，标签通过 Hash 函数计算阅读器发送的密钥 K，检查 Hash（K）是否与 MetaID 相同，相同则解锁，发送标签真实 ID 给阅读器。

（2）随机 Hash 锁方案

作为 Hash 锁的扩展，随机 Hash 锁解决了标签位置隐私问题。采用随机 Hash 锁方案，阅读器每次访问标签的输出信息都不同。

随机 Hash 锁原理是标签包含 Hash 函数和随机数发生器，后台服务器数据库存储所有标签 ID。阅读器请求访问标签，标签接收到访问请求后，由 Hash 函数计算标签 ID 与随机数 r（由随机数发生器生成）的 Hash 值。标签发送数据给请求的阅读器，同时阅读器发送给后台服务器数据库，后台服务器数据库穷举搜索所有标签 ID 和 r 的 Hash 值，判断是否为对应标签 ID。标签接收到阅读器发送的 ID 后解锁。

尽管 Hash 函数可以在低成本的情况下完成，但要集成随机数发生器到计算能力有限的低成本被动标签，却是很困难的。其次，随机 Hash 锁仅解决了标签位置隐私问题，一旦标签的秘密信息被截获，隐私侵犯者可以获得访问控制权，通过信息回溯得到标签历史记录，推断标签持有者隐私。后台服务器数据库的解码操作是通过穷举搜索的，需要对所有的标签进行穷举搜索和 Hash 函数计算，因此存在拒绝服务攻击。

（3）Hash 链方案

作为 Hash 方法的一个扩展，为了解决可跟踪性，标签使用了一个 Hash 函数在每次阅读器访问后自动更新标识符，实现前向安全性。Hash 链与之前的 Hash 方案相比主要优点是提供了前向安全性。然而，它并不能阻止重放攻击。并且该方案每次识别时需要进行穷举搜索，比较后台数据库每个标签，一旦标签规模扩大，后端服务器的计算负担将急剧增大。因此 Hash 链方案存在着所有标签自更新标识符方案的通用缺点，难以大规模扩展，同时，因为需要穷举搜索，所以存在拒绝服务攻击。

（4）匿名 ID 方案

采用匿名 ID，隐私侵犯者即使在消息传递过程中截获标签信息也不能获得标签的真实 ID。该方案通过第三方数据加密装置采用公钥加密、私钥加密或者添加随机数生成匿名标签 ID。虽然标签信息只需要采用随机读取存储器（RAM）存储，成本较低，但数据加密装置与高级加密算法都将导致系统的成本增加。因标签 ID 加密以后仍具有固定输出，因此，使得标签的跟踪成为可能，存在标签位置隐私问题。并且，该方案的实施前提是阅读器与后台服务器的通信建立在可信通道上。

（5）重加密方案

该方案采用公钥加密。标签可以在用户请求下通过第三方数据加密装置定期对标签数据进行重写。因采用公钥加密，大量的计算负载超出了标签的能力，通常这个过程由阅读器来处理。该方案存在的最大缺陷是标签的数据必须经常重写，否则，即使加密标签 ID 固定的输出也将导致标签定位隐私泄露。与匿名 ID 方案相似，标签数据加密装置与公钥加密将导致系统成本的增加，使得大规模的应用受到限制，并且经常地重复加密操作也给实际操作带来困难。

RFID 标签已逐步进入到我们的日常生产和生活中，同时，也给我们带来了许多新的安

全和隐私问题。由于对低成本 RFID 标签的追求，使得现有的密码技术难以应用。如何根据 RFID 标签有限的计算资源，设计出安全有效的安全技术解决方案，仍然是一个具有相当挑战性的课题。为了有效地保护数据安全和个人隐私，引导 RFID 的合理应用和健康发展，还需要建立和制订完善的 RFID 安全与隐私保护法规、政策。

8.3　传输层的安全需求和安全策略

物联网的传输层主要用于把感知层收集到的信息安全可靠地传输到信息处理层，然后根据不同的应用需求进行信息处理，即传输层主要是网络基础设施，包括互联网、移动网和一些专业网（如国家电力专用网、广播电视网）等。在信息传输过程中，可能经过一个或多个不同架构的网络进行信息交接。例如，普通电话座机与手机之间的通话就是一个典型的跨网络架构的信息传输实例。在信息传输过程中跨网络传输是很正常的，在物联网环境中这一现象更突出，而且很可能在正常而普通的事件中产生信息安全隐患。

此外，尽管物联网的传输层应当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，而且以集群的方式存在，因此会导致数据传输时，由于大量机器的数据发送而造成网络拥塞。而且，现在通信网络是面向连接的工作方式，而物联网的广泛应用必须解决地址空间缺乏和网络安全标准等问题，从目前的现状看物联网对其核心技术的要求，特别是在可信、可知、可管、可控制等方面，远远高于目前的 IP 网络所提供的能力，因此认为物联网必定会为其核心网络采用数据分组技术。

此外现有的通信网络安全架构均是从人的通信角度设计的，并不完全适用于机器间的通信，使用现有的互联网安全体制会割裂物联网机器间的逻辑联系。庞大且多样化的物联网核心网络必然需要一个强大而统一的安全管理平台，否则对物联网中各种物品设备的日志等安全信息的管理将成为新的问题，并且由此可能会割裂网络之间的信任关系。

8.3.1　传输层的安全挑战和安全需求

网络环境目前遇到前所未有的安全挑战，而物联网传输层所处的网络环境也存在安全挑战，甚至是更高的挑战。同时，由于不同架构的网络需要相互连通，因此在跨网络架构的安全认证等方面会面临更大挑战。初步分析认为，物联网传输层将会遇到下列安全挑战。

1）DoS 攻击、DDoS 攻击；

2）假冒攻击、中间人攻击等；

3）跨异构网络的网络攻击。

在物联网发展过程中，目前的互联网或者下一代互联网将是物联网传输层的核心载体，多数信息要经过互联网传输。互联网遇到的 DoS 攻击和 DDoS 攻击仍然存在，因此需要有更好的防范措施和灾难恢复机制。考虑到物联网所连接的终端设备性能和对网络需求的巨大差异，因此很难设计通用的安全方案，而应针对不同网络性能和网络需求有不同的防范措施。在传输层，异构网络的信息交换将成为安全性的脆弱点，特别在网络认证方面，难免存在中间人攻击和其他类型的攻击（如异步攻击、合谋攻击等）。这些攻击都需要有更高的安全防护措施。如果仅考虑互联网和移动网以及其他一些专用网络，则物联网传输层对安全的需求

可以概括为以下几点：

1）数据机密性：需要保证数据在传输过程中不泄露其内容。

2）数据完整性：需要保证数据在传输过程中不被非法篡改，或非法篡改的数据容易被检测出。

3）数据流机密性：某些应用场景需要对数据流量信息进行保密，目前只能提供有限的数据流机密性。

4）DDoS 攻击的检测与预防：DDoS 攻击是网络中最常见的攻击现象，在物联网中将会更突出。物联网中需要解决的问题还包括如何对脆弱节点的 DDoS 攻击进行防护。

5）移动网中认证与密钥协商（Authentication and Key Agreement，AKA）机制的一致性或兼容性、跨域认证和跨网络认证（基于 IMSI）：不同无线网络所使用的不同 AKA 机制对跨网认证带来不利。这一问题亟待解决。

8.3.2　传输层的安全策略

传输层的安全机制可分为端到端机密性和节点到节点机密性。对于端到端机密性，需要建立如下安全机制：端到端认证机制、端到端密钥协商机制、密钥管理机制和机密性算法选取机制等。在这些安全机制中，根据需要可以增加数据完整性服务。对于节点到节点机密性，需要节点间的认证和密钥协商协议，这类协议要重点考虑效率因素。机密性算法的选取和数据完整性服务则可以根据需求选取或省略。考虑到跨网络架构的安全需求，需要建立不同网络环境的认证衔接机制。另外，根据应用层的不同需求，网络传输模式可能区分为单播通信、多播通信和广播通信，针对不同类型的通信模式也应该有相应的认证机制和机密性保护机制。简言之，传输层的安全架构主要包括如下几个方面：

1）节点认证、数据机密性、完整性、数据流机密性、DDoS 攻击的检测与预防。

2）移动网中 AKA 机制的一致性或兼容性、跨域认证和跨网络认证（基于 IMSI）。

3）相应密码技术。密钥管理（密钥基础设施 PKI 和密钥协商）、端对端加密和节点对节点加密、密码算法和协议等。

4）多播和广播通信的认证性、机密性和完整性安全机制。

8.3.3　M2M 安全问题及策略

现代网络计算与硬件技术的发展为 M2M 技术的发展提供了有力的支持，M2M 技术的前景似乎一片光明，但是在实际上，要想很好地发展 M2M 技术还存在一系列问题，其中最主要的就是 M2M 系统的安全问题。

8.3.3.1　M2M 系统安全问题分析

从 M2M 系统的网络架构来看，具体可以分为节点、网络传输载体及数据处理中心 3 个部分，其具体结构如图 8-2 所示。节点主要负责的工作是对各项资料的收集，并将收集到的资料传送到后台数据处理中心。通常情况下，节点的设置因为考虑成本的因素并不会加入太多的功能，而是将大部分功能交给后台控制中心；网络传输载体的主要作用是负责将节点收集的资料传输到数据处理中心；数据处理中心的主要作用是完成所有数据的分析处理工作，并向节点下发一些简单的指令。

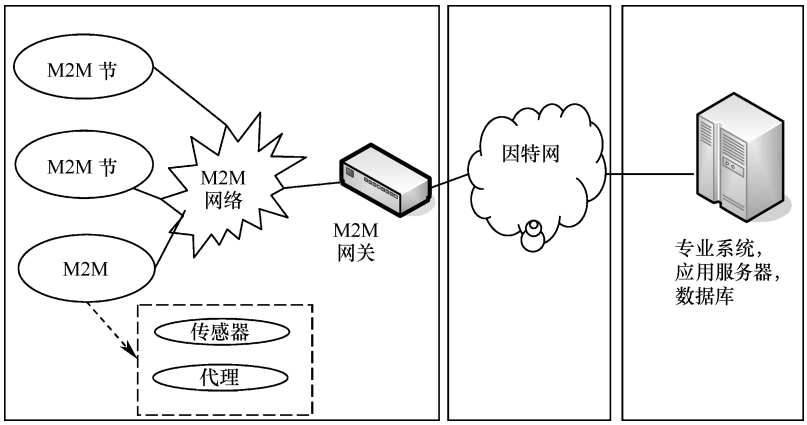


图 8-2　M2M 系统的网络结构

（1）M2M 系统节点

M2M 节点所涉及的安全问题，最重要的就是 M2M 节点通信时的安全性。无论是节点之间的通信还是节点与数据处理中心之间的通信，都应该保证通信过程中数据传输的安全性，避免被不法分子所利用。比较直接的解决方法是对数据进行加密，但是密钥的管理具备一定的难度，尤其是在 M2M 系统中通常会存在大量节点，这就导致数据在传输过程中，需要使用数量庞大的密钥，而且由于成本的限制，通常情况下，每个节点所能存储的数据是非常有限的，这就使数据加密这一方式难以有效应用到实际工作中。

另外，节点收集资料的可靠性也是当前所面临的主要问题之一。节点通常利用传感器对数据资料进行采集，在这一过程中，通常有两种原因容易造成数据的采集错误，第一种是 M2M 节点本身硬件的故障所导致的，第二种原因是黑客入侵传感器后，对传感器的数据交换进行控制，导致传感器执行错误的指令所造成的。M2M 节点的感测数据如果发生错误，容易导致整个系统的错误运行并下发错误的指令，危害人类的生活。

（2）网络传输载体

网络传输载体的主要作用是实现节点与数据处理中心的数据交换。在这一过程中，常见的安全威胁包括两种，一种是阻断服务攻击，这类威胁主要容易造成通信的中断，导致节点与数据处理中心无法进行及时通信，严重影响 M2M 系统的工作效率。另一中是中间人攻击，这种威胁通常容易造成数据泄漏、丢失以及遭到窜改的危险，影响 M2M 系统数据的可靠性，导致系统执行错误的指令。

（3）数据处理中心

数据处理中心的主要任务是负责对节点数据的汇总、整理及分析，并在此基础上做出自动化智能决策。通常情况下，数据处理中心会设置在云端服务器或者某个机房中，由专人进行管理和维护。在这一过程中主要涉及服务器的安全问题，如果处理不好，就容易导致整个系统的瘫痪。

8.3.3.2　M2M 系统安全措施

在 M2M 系统中，如果想要保证系统的安全稳定运行，就必须要全方位做好系统的安全防护措施，如果其中的任意一个环节出现漏洞，都会影响到整个系统的正常运行，下面提出

了几点针对 M2M 系统所实施的安全措施。

（1）基于身份识别的密码系统

因为 M2M 系统通常包含大量的物品，因此在考虑到密钥更新以及硬件成本的情况下，对称式密钥系统并非是较好的安全措施。在 M2M 系统中，因为所涉及的物品过多，如果使用密钥进行管理就容易导致整个网络达到效能瓶颈，对整个 M2M 系统的运行效率产生较大影响。基于身份识别的密码技术通过为每个物品附加一个独立的 ID，在任意物品之间需要进行通信时，只需要知道对方的 ID 就可以透过公用密钥建立彼此之间的密钥，保证通信的安全。

（2）成对监督机制

通常情况下，传感器的程序都是通过刻录在 ROM 里面进行执行的，因为内存只提供了读取的权限，攻击者不太可能对内存进行修改，因此，其要想对节点进行攻击，通常是对节点的 ROM 进行修改，并让修改后的 ROM 程序在传感器中执行，从而实现对整个系统的攻击。要想解决这一问题，最好的办法就是从节点的硬件入手，让攻击者无法对 ROM 进行修改。在攻击者对 ROM 进行修改的过程中，被修改的这一节点就会处于瘫痪的状态。通过在 M2M 系统中应用成对监督机制来实现对各个节点的监控，通过建立各个节点之间的相互监督机制，当某个节点在停止运行后，它所对应的监督节点就会做出响应，并向数据处理中心进行汇报，以此来实现对每一个节点运行状态的监控，从而实现对攻击者修改 ROM 这一威胁的防护。

（3）错误数据侦测过滤机制

如果节点将错误的数据信息发送给数据处理中心，就容易导致系统做出错误的决策。因此，保证节点发送数据的准确性至关重要，数据服务中心在进行数据分析处理的过程中，需要对当前节点数据及附近的多个节点的数据进行评估，因为邻近的节点通常所采集的数据差异性较小，如果数据处理中心发现某个节点的数据与邻近节点数据的平均值产生较大差异，那么该数据将被系统所过滤，从而保证各节点数据的准确性，为系统的决策提供准确的依据。

除了上述措施之外，针对一些客观因素所导致的 M2M 系统安全问题，如供电故障、网络系统故障等问题，需要与电力、电信等多部门进行联合解决，从而保证 M2M 系统安全稳定的运行。

8.4　应用层的安全需求和安全策略

应用层是信息到达智能处理平台的处理过程，包括如何从网络中接收信息。在从网络中接收信息的过程中，需要判断哪些信息是真正有用的信息，哪些是垃圾信息甚至是恶意信息。在来自于网络的信息中，有些属于一般性数据，用于某些应用过程的输入，而有些可能是操作指令。在这些操作指令中，又有一些可能是多种原因造成的错误指令（如指令发出者的操作失误、网络传输错误、得到恶意修改等），或者是攻击者的恶意指令。如何通过密码技术等手段甄别出真正有用的信息，又如何识别并有效防范恶意信息和指令带来的威胁是物联网应用层的重大安全挑战。

8.4.1　应用层的安全挑战和安全需求

物联网应用层的重要特征是智能，智能的技术实现少不了自动处理技术，其目的是使处理过程方便迅速，而非智能的处理手段可能无法应对海量数据。但自动过程对恶意数据特别是恶意指令信息的判断能力是有限的，而智能也仅限于按照一定规则进行过滤和判断，攻击者很容易避开这些规则，正如垃圾邮件过滤一样，这么多年来一直是一个棘手的问题。因此应用层的安全挑战包括如下几个方面：

1）来自于超大量终端的海量数据的识别和处理；

2）智能变为低能；

3）自动变为失控（可控性是信息安全的重要指标之一）；

4）灾难控制和恢复；

5）非法人为干预（内部攻击）；

6）设备（特别是移动设备）的丢失。

物联网时代需要处理的信息是海量的，需要处理的平台也是分布式的。当不同性质的数据通过一个处理平台处理时，该平台需要多个功能各异的处理平台协同合作。但首先应该知道将哪些数据分配到哪个处理平台，因此数据类别分类是必需的。同时，安全的要求使得许多信息都是以加密形式存在的，因此如何快速有效地处理海量加密数据是智能处理阶段遇到的一个重大挑战。

计算技术的智能处理过程较人类的智力来说还是有本质的区别，但计算机的智能判断在速度上是人类智力判断所无法比拟的，由此，期望物联网环境的智能处理在智能水平上不断提高，而且不能用人的智力去代替。也就是说，只要智能处理过程存在，就可能让攻击者有机会躲过智能处理过程的识别和过滤，从而达到攻击目的。在这种情况下，智能与低能相当。因此，物联网的传输层需要高智能的处理机制。

如果智能水平很高，那么可以有效识别并自动处理恶意数据和指令。但再好的智能也存在失误的情况，特别在物联网环境中，即使失误概率非常小，因为自动处理过程的数据量非常庞大，因此失误的情况还是很多。在处理发生失误而使攻击者攻击成功后，如何将攻击所造成的损失降低到最小程度，并尽快从灾难中恢复到正常工作状态，是物联网智能应用层的另一重要问题，也是一个重大挑战，因为在技术上没有最好，只有更好。

智能应用层虽然使用智能的自动处理手段，但还是允许人为干预，而且是必需的。人为干预可能发生在智能处理过程无法做出正确判断的时候，也可能发生在智能处理过程有关键中间结果或最终结果的时候，还可能发生在其他任何原因而需要人为干预的时候。人为干预的目的是为了应用层更好地工作，但也有例外，那就是实施人为干预的人试图实施恶意行为时。来自于人的恶意行为具有很大的不可预测性，防范措施除了技术辅助手段外，更多地需要依靠管理手段。因此，物联网应用层的信息保障还需要科学管理手段。

智能处理平台的大小不同，大的可以是高性能工作站，小的可以是移动设备，如手机等。工作站的威胁是内部人员恶意操作，而移动设备的一个重大威胁是丢失。由于移动设备不仅是信息处理平台，而且其本身通常携带大量重要机密信息，因此，如何降低作为处理平台的移动设备丢失所造成的损失是重要的安全挑战之一。

8.4.2　应用层的安全策略

为了满足物联网智能应用层的基本安全需求，需要如下的安全机制。

1）可靠的认证机制和密钥管理方案；
2）高强度数据机密性和完整性服务；
3）可靠的密钥管理机制，包括 PKI 和对称密钥的有机结合机制；
4）可靠的高智能处理手段；
5）入侵检测和病毒检测；
6）恶意指令分析和预防，访问控制及灾难恢复机制；
7）保密日志跟踪和行为分析，恶意行为模型的建立；
8）密文查询、秘密数据挖掘、安全多方计算、安全云计算技术等；
9）移动设备文件（包括秘密文件）的可备份和恢复；
10）移动设备识别、定位和追踪机制。

8.4.3　云计算安全问题

8.4.3.1　云计算安全问题概述

云计算本身是一个复杂的系统，云计算的安全需求散布在云计算的各个层次、各个环节。以下分别从云服务提供商、云服务用户的角度探讨云计算的安全需求。

对于云服务提供商，需要解决以下问题：①如何保证云服务平台、数据中心这样的复杂系统能长时间安全运行，并在故障发生时能及时隔离故障，将影响降到最低；②对于云计算数据中心这样引人注目的存在，如何应对由此引来的数量众多的网络黑客；③面对参差不齐的用户，如何对他们进行有效的安全管理，并能鉴别和屏蔽恶意用户。

对于云服务用户，有以下安全需求：①如何在现有云计算服务还不能确保稳定的情况下尽量让运行在云环境上的应用稳定、安全、可用；②如何保证自己在云端的数据安全、完整、可用，且商业机密不被泄露。

虽然云计算的架构层次还没有统一的标准，但大体可以抽象为 5 层，从底向上分别为：物理资源层、资源抽象与控制层、资源架构层、开发平台层、应用服务层。其中资源架构层、开发平台层、应用服务层分别对应云计算的 3 种服务模式：基础设施即服务（Infrastructure as a Service，IaaS）模式、平台即服务（Platform as a Service，PaaS）模式和软件即服务（Software as a Service，SaaS）。下面按该层次详细分析其中的安全问题。

1）物理资源层安全。本层安全问题包括硬件安全和软件安全两个方面，与传统软硬件安全问题基本相同，硬件方面包括物理设备本身的问题如硬件故障和电源故障等，还包括设备的物理环境、物理访问和电磁辐射造成信息泄露等安全问题；软件方面包括病毒攻击、网络入侵等安全问题。

2）资源抽象与控制层安全。本层主要涉及虚拟化带来的各种安全挑战。虚拟化是云计算中最重要的技术之一，也是云计算的重要标志，然而，虚拟化的结果却使许多传统的安全防护手段失效，引发了诸如虚拟机逃逸、远程管理缺陷、迁移攻击、虚拟机通信等安全问题。

3）资源架构层安全。本层提供基本的分布式资源服务，用户面临的主要安全问题包

括：存储安全、数据完整性、冗余备份和审计计费安全等。

4）开发平台层安全。本层为应用程序开发者提供程序的开发环境、运行环境和运营环境，同时还提供数据库、用户界面、负载均衡等服务支持。用户面临的安全问题包括安全设计、安全编程、安全测试和安全发布等问题。

5）应用服务层安全。本层中云计算运营商通过互联网向用户提供软件服务，这些软件的开发、测试、运行、维护、升级由应用程序提供者负责。用户面临的安全问题包括身份认证与访问控制、安全单点登录、数据与隐私保护等。

8.4.3.2　云计算应用中存在的安全问题

前面已经提到，互联网时代中传统的安全威胁在云计算服务中同样存在。2009 年，云安全联盟（CloudSecurity Alliance，CSA）发布《云计算关键领域安全指南》并更新到版本 2.1。该指南主要从攻击者的角度总结出云计算环境可能面临的 12 个关键安全域。之后 CSA 又发布了一份云计算安全风险简明报告，将安全指南浓缩为 7 个最常见、危害程度最大的安全威胁。下面，按照从低到高、由内及外等层次一一列出。

1）基础设施共享问题：攻击者获取 laaS 供应商的非隔离共享基础设施的不受控制访问权；

2）未知的风险：未知的安全漏洞、软件版本、安全实践、代码更新等；

3）不安全的接口和 API：接口质量和安全没有得到保障以及第三方插件的安全；

4）账户或服务劫持：攻击者获得云服务用户的凭据，导致云服务客户端问题；

5）数据丢失或泄漏：云中不断增长的数据交互放大了数据丢失或泄漏的风险；

6）不怀好意的内部人员：从组织内部发起攻击，如果公司使用了云服务，威胁将会进一步放大；

7）滥用和恶意使用云计算：利用云服务发送垃圾邮件或传播恶意代码等恶意活动。

较早时间，美国信息技术研究和咨询公司 Gartner 也发布了《云计算安全风险评估》报告。该报告主要从云服务提供商的安全能力角度及其潜在情况或事件下受威胁程度提出云计算环境下的安全风险，主要包括：

1）特权用户接入：供应商的管理员处理敏感信息的风险；

2）可审查性：供应商拒绝外部审计和安全认证的风险；

3）数据位置：数据存储位置未知的隐私风险；

4）数据隔离：共享资源的多租户数据隔离；

5）数据恢复：供应商的数据备份和恢复能力；

6）调查支持：供应商对不恰当或非法行为难以提供取证支持；

7）长期生存性：服务稳定性、持续性及其迁移。

如果仅从字面上简单理解云计算的安全威胁和安全风险，上面列出的条目在互联网时代的 IDC（Internet Data Center，互联网数据中心）就都已经出现，并且传统的安全模型和防御体系也有较为完善的理论指导和实践方案，在物理层面、系统层面、网络层面、甚至 Web 应用层面已经有了比较成熟的安全产品。那么是否可以完全照搬这些互联网安全解决方案而直接运用到云计算体系中吗？答案是否定的。下面，我们从云计算安全模型和关键技术等方面进行说明。

8.4.3.3　云计算安全模型介绍

由于当前正处于从传统互联网或者IT应用环境向云计算应用发展的关键时期，统一规划和整体考虑云计算安全离不开云计算安全模型的指导。所谓云计算安全模型，就是从安全管控的角度建立的云计算模型，用以描述不同属性组合的云服务架构，并实现云服务架构到安全架构之间的映射，为风险识别、安全控制和技术实现提供依据。信息安全领域已经开始着手从不同角度建立云计算安全模型，虽然存在争议，也缺乏大规模实践的验证，但在学术界和产业界的共同推动下，这些来自各方的云计算安全模型正在为云计算应用安全做着有益的探索。

（1）CSA模型

当前，美国国家标准与技术研究所（National Institute of Standards and Technology，NIST）给出的3种服务模型已经被广泛接受并成为业内的事实规范。这3种服务模式包括：基础设施即服务（IaaS）模式、平台即服务（PaaS）模式和软件即服务（SaaS）模式。例如亚马逊公司提供的以亚马逊网络服务（AWS）为框架的服务器、存储、带宽、数据库，以及信息接口的资源服务模式，就是比较典型的IaaS模式；而微软公司的Azure服务平台提供一系列可供开发的操作系统，也可看作是一种PaaS服务模式。

根据其所属层次的不同，针对上述3类服务模式，CSA提出了基于基本云服务的层次性及其依赖关系的安全参考模型，如图8-3所示。该模型主要反映了从云服务模型到安全控制模型的映射。该安全模型的突出特点是提供商所在的等级越低，云计算用户所要自行承担的安全能力和管理职责就越多。进而言之，CSA模型是可以允许用户有条件获取所需安全配置信息以及运行状态信息的，也允许用户部署实施自有专用安全管理软件来保证自己数据的安全。

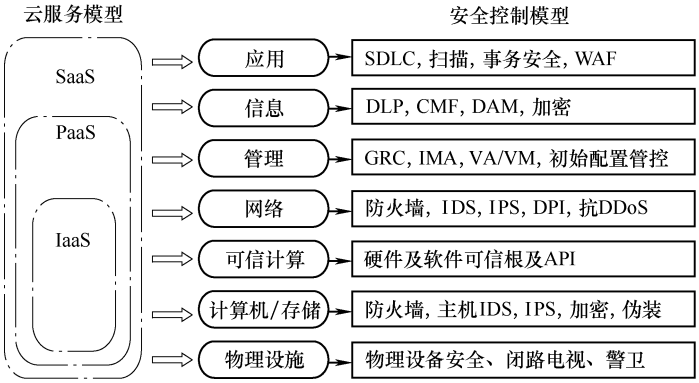


图8-3　CSA云计算参考模型

（2）企业界模型

在国内，一些大型的IT设备制造企业也不约而同地推出了云计算整体解决方案以及相关云计算安全服务模型。与CSA模型不同的是，这些云计算安全模型更加偏重于具体的产品解决方案，而没有上升到理论层面。虽然在具体工程中已经有实践应用，但是基本上还是采用传统网络安全技术作为主要的防御力量，在针对云计算应用的响应速度、系统规模等方面的安全要求依旧没有本质上的突破。图8-4描述了一个简约的、面向工程的云计算安全

模型。

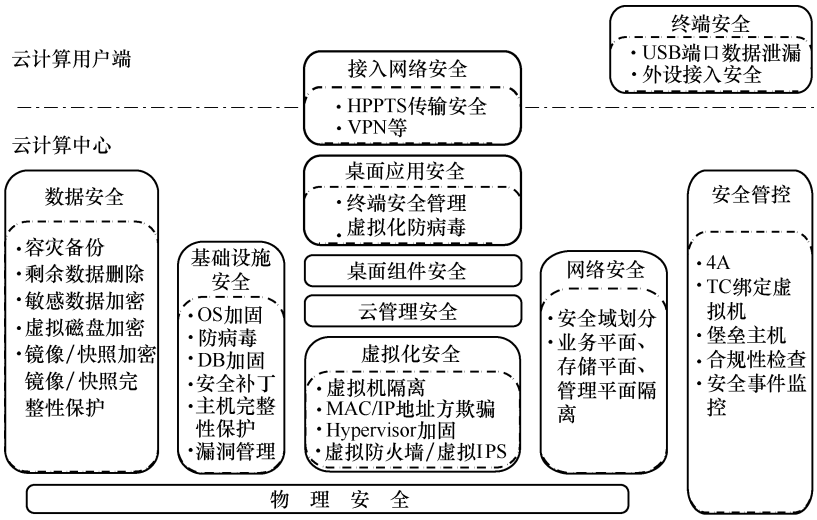


图 8-4　国内 IT 企业云计算安全模型

（3）其他模型

我国的一些科研机构也发布了相关的云计算的安全模型。在中科院软件所提出的模型中，整个云计算安全技术模型被分为 3 个部分：云计算用户端安全对象、云计算安全服务体系和云安全标准体系。另外，还有 Jericho Forum 提出的安全协同模型。它从数据的物理位置、云计算技术和服务的所有关系状态、应用资源和服务时的边界状态、云服务的运行和管理者 4 个影响安全协同的维度上分了 16 种可能的云计算形态。当然，还有很多云计算安全模型都在探索和验证中，但是这些模型都把技术关注点更多地放在用户数据安全与隐私保护；各层次资源的提供者、管理者、使用者的安全防护措施的统一；云计算安全监管体系的建立等方面，这也从另外角度说明了采用传统专一严格为原则搭建的安全模型已经不合时宜了。

8.4.3.4　云计算中的关键安全技术

由于在云计算应用场景中，传统的安全威胁，如网络病毒、漏洞入侵、内部泄漏、网络攻击等依旧存在，因此这些安全威胁仍需要使用防病毒软件、入侵检测、4A、抗 DDoS 等技术或者安全设备去实现对云的保护。而与此同时，云计算的逐步应用正直接或者间接影响信息安全领域的进程，一些新兴的安全技术也在慢慢兴起。下面，我们简单列举一些云计算安全中使用到的一些关键技术。

（1）主机虚拟化安全

从现在产业趋势来看，由于 IaaS 模式技术相对成熟，因此从 IaaS 着手整合计算、存储、网络资源，再逐步发展 PaaS、SaaS 等其他各种云服务能力已经是云计算服务建设的主流思路。而基于虚拟化技术的弹性计算，正是 IaaS 的基础，因此主机虚拟化安全是 IaaS 建设方案中需要重点考虑的问题。在主机虚拟化中，Hypervisor 和虚拟机这两个最主要的部分的安全性是最为重要的。

虚拟机管理器 Hypervisor 是用来运行虚拟机的内核，代替传统操作系统管理着底层物理

硬件，是服务器虚拟化的核心环节，其安全性直接关系到上层的虚拟机安全。如果虚拟机管理器的安全机制不健全，被某个恶意虚拟机其漏洞或者某个协议端口获取了高级别的运行等级，就可以比操作系统更高的硬件调配权限，从而给其他客户带来极大的安全隐患。

在 IaaS 中，一台物理机器往往被划分为多台虚拟机器进行使用。由于同一物理服务器的虚拟机之间可以相互访问，而不需要经过之外的防火墙与交换机等设备，因此虚拟机之间的攻击变得更加容易。如何保证同一物理机上不同虚拟机之间的资源隔离，包括 CPU 调度、内存虚拟化、VLAN、I/O 设备虚拟化，是当前 IaaS 模式下首要解决的安全技术问题。

（2）海量用户的身份认证

在互联网时代的大型数据业务系统中，大量用户的身份认证和接入管理往往采用强制认证方式，例如指纹认证、USB Key 认证、动态密码认证等。但是在这种身份认证和管理主要是基于系统自身对于用户身份的不信任作为主要思想而设计的。在云计算时代，因为用户更加关心的云计算提供商是否按照 SLA 实施双方约定好的访问控制策略，所以在云计算模式下，研究者开始关注如何通过身份认证来保证用户自身资源或者信息数据等不会被提供商或者他人滥用。当前比较可行的解决方案就是引入第三方 CA 中心，由后者提供为双方所接受的私钥。

（3）隐私保护与数据安全

用户隐私保护和数据安全主要包括各类信息的物理隔离或者虚拟化环境下的隔离；基于身份的物理或者虚拟安全边界访问控制；数据的异地容灾与备份以及数据恢复；数据的加密传输和加密存储；剩余信息保护等。在云计算应用中，数据量规模之巨已经远远超出传统大型 IDC 数据规模，同时不同用户对于隐私和数据安全的敏感度也各不相同。这里，我们主要讲一下用户最常面临和关心的加密传输和加密存储。

在云计算应用环境下，数据传输加密可以选择在链路层、网络层、传输层、甚至应用层等层面实现。主要的技术措施包括 IPSec VPN、SSL 等 VPN 技术，保证用户数据在网络传输中的机密性、完整性和可用性。对于云存储类服务，一般的提供商都支持对数据进行加密存储，防止数据被他人非法窥探。一般会采用效能较高的对称加密算法，如 AES、3DES 等国际通用算法，或我国国有商密算法 SCB2 等。在云计算中，如网盘等虚拟存储的应用也是非常常见的。在这种情况下，如果只是对退租用户 VM 磁盘中文件做简单的删除，而下一次将磁盘空间（逻辑卷）重新分配给其他租户时，就可能会被恶意租户使用数据恢复软件读出磁盘数据，而导致先前租户的数据泄漏。因此在进行存储资源回收时，需要使用软件技术对逻辑卷的每一个物理位进行清“零”覆写，保证磁盘空间重新分配给其他租户时不能通过软件方式恢复其原有数据。

（4）其他一些安全技术措施

当然，在云计算应用环境中，还有其他一些安全技术。例如 PaaS 服务商提供的开发平台以 API 方式提供各种编程环境，就可能由于 API 接口质量和安全没有得到保障而带来平台的平台可靠性、平台可用性、平台完整性等一系列安全问题。目前的技术解决方案有平台升级和 Parley—X 保护等。再例如 SaaS 模式主要面临的安全问题就是软件漏洞，因此主要的解决技术仍然是软件补丁、版本升级等。

科研人员也在不断研究以用户为中心的、而非以云计算提供商为中心的信任模型。一些安全公司也在研发基于客户端的隐私或者用户数据管理工具，帮助用户控制自己的敏感信息

在云端的存储和使用。

8.4.3.5 云计算安全的解决方案

除了学术界，产业界对云计算的安全问题非常重视，并为云计算服务和平台开发了若干安全机制，各类云计算安全产品与方案不断涌现。

（1）微软

微软的云计算平台叫作 Windows Azure。在 Azure 上，微软通过采用强化底层安全技术性能，使用所提出的 Sydney 安全机制，以及在硬件层面上提升访问权限安全等系列技术措施为用户提供一个可信任的云，从私密性、数据删除、完整性、可用性和可靠性 5 个方面保证云安全。

（2）亚马逊

亚马逊是互联网上最大的在线零售商，但是同时也为独立开发人员以及开发商提供云计算服务平台。亚马逊是最早提供远程云计算平台服务的公司，他们的云计算平台称为弹性计算云（Elastic ComputeCloud，EC2）。亚马逊从主机系统的操作系统、虚拟实例操作系统、防火墙以及 API 呼叫多个层次为 EC2 提供安全，目的就是防止亚马逊 EC2 中的数据被未经认可的系统或用户拦截，并在不牺牲用户要求的配置灵活性的基础上提供最大限度的安全保障。

（3）其他解决方案

Sun 公司发布开源的云计算安全工具可为 Amazon 的 EC2、S3 以及虚拟私有云平台提供安全保护。Yahoo 的开源云计算平台 Hadoop 也推出安全版本，引入 kerberos 安全认证技术，对共享敏感数据的用户加以认证与访问控制，阻止非法用户对 Hadoop clusters 的非授权访问。McAfee 公司发布了一个基于云的电子邮件网关 McAfeeSaaS Email Security & Archiving Suite，能完成实时监控和分析传入的邮件流量，同时可以隐藏关键的邮件传输网关。EMC、Intel、Vmware 等公司联合宣布了一个“可信云体系架构”的合作项目，并提出了一个概念证明系统。

参 考 文 献

[1] 叶青. 物联网安全问题技术分析 [J]. 网络安全技术与应用，2010（10）：32-33.

[2] 武传坤. 物联网安全架构初探 [J]. 战略与决策研究，2010，25（4）：411-419.

[3] 肖毅. 物联网安全管理技术研究 [J]. 通信技术，2011，44（1）：69-71.

[4] 彭朋，韩伟力，赵一鸣，等. 基于 RFID 的物联网的安全需求研究 [J]. 计算机安全，2011（1）：75-79.

[5] 吴同. 浅折物联网的安全问题 [J]. 网络安全技术与应用，2010（08）：7-9.

[6] 孙其博，刘杰，黎羴，等. 物联网：概念、架构与关键技术研究综述 [J]. 北京邮电大学学报，2010，33（3）：1-9.

[7] 杨庚，许建，陈伟，等，物联网安全特征与关键技术 [J]. 南京邮电大学学报（自然科学版），2010，30（4）：20-29.

[8] 刘利民，肖德宝，李琳，等. 物联网感知层中 RFID 的信息安全对策研究 [J]. 武汉理工大学学报，2010，32（20）：79-82.

[9] 潘晓勇，张蕾，樊学会. 使用数字证书增强 RFID 系统的通信安全性 [J]. 电子科技，2010，23（11）：123-125.

第 9 章　物联网典型行业应用

9.1　物联网应用的背景及发展趋势

9.1.1　应用背景

各国政府对物联网的发展和应用十分重视，纷纷出台战略指导规划。美国总统奥巴马就任总统后，积极回应了 IBM 公司提出的“智慧地球”概念，并将物联网计划升级为国家战略；日本政府在 2004 年推出了基于物联网的国家信息化战略 u-Japan（泛在网络计划），其理念是以人为本，实现所有人与人、物与物、人与物之间的连接；韩国于 2006 年把 u-Korea 战略修订为 u-IT839 计划，更加强调泛在网络技术的应用，使“服务-基础设施-技术创新产品”三者融合更加紧密，并于 2009 年 10 月制定了《物联网基础设施构建基本规划》，将物联网市场确定为新增长动力；欧盟推出了《欧盟物联网行动计划》（Internet of Things – An action plan for Europe），在医疗专用序列码、智能电子材料系统等应用方面做出了尝试。

我国物联网的发展与全球同处于起步阶段。2009 年提出“感知中国”的概念。2010 年政府工作报告中将物联网正式列为中国五大新兴战略性产业。据不完全统计，2010 年我国物联网产业市场规模接近 2000 亿，而 2011 年其产业规模超过 2600 亿元人民币，2012 年物联网产业规模达到 3650 亿元，同比增长 38.6%，2015 年我国物联网产值已超过 5000 亿元。物联网受到全社会极大的关注与重视，许多省市、产业、行业，也开始着手制定物联网的相关规划。

物联网标准是国际物联网技术竞争的制高点。发达国家通过政府和企业共同努力，加大发展传感器节点核心芯片、嵌入式操作系统、智能计算等核心技术的支持力度，同时加快标准制定和产业化进程，在国际竞争中占据了有利的位置。工业和信息化部制定的《物联网“十二五”发展规划》，明确提出了物联网是我国新一代信息技术自主创新突破的重点方向，在芯片、传感器、近距离传输、海量数据处理以及综合集成、应用等领域，尽快提升技术创新能力，解决处于产业链低端、核心技术受制于人的状况。2013 年国务院发布的《国家重大科技基础设施建设中长期规划（2012—2030 年）》中，物联网产业成为其中的规划之一。因此，研究物联网相关的关键技术具有重大的现实意义。

物联网应用涉及国民经济和人类社会生活的方方面面，因此，“物联网”被称为是继计算机和互联网之后的第三次信息技术革命。信息时代，物联网无处不在。由于物联网具有实时性和交互性的特点，在本章中，作者将介绍几个物联网最新的典型应用，对其核心思想和主要技术进行介绍。

9.1.2　发展趋势

未来几年是我国物联网相关产业以及应用迅速发展的时期。以物联网为代表的信息网络

产业成为新兴战略性产业之一，成为推动产业升级、迈向信息社会的“发动机”。物联网终端将快速发展，呈现多样化、智能化的特点。物联网时代的通信主体由人扩展到物，物联网终端是用于表征真实世界物体、实现物体智能化的设备。随着物理世界中的物体逐步成为通信对象，必将产生大量的、各式各样的物联网终端，使得物体具有通信能力，实现人与物、物与物之间的通信。另一方面，随着技术的进步，低功耗和小体积的传感器将大量出现，而且其感知能力更加全面，为物联网的规模化发展提供了基础。而且随着手机日趋智能、接口更加丰富，手机传感器种类和数量将更加快速增长、应用也日趋多样；未来手机不仅可以控制自身的传感器，还可以通过接入传感器网络，控制网络内的传感器，获取一定区域内的数据，应用场景会更加丰富，有力地推动了物联网的发展。与现有通信网相比，物联网在 anytime、anyone、anywhere 的基础上，又拓展到了 anything。人们不再局限于网络的虚拟交流，有人与人，也包括机器与人、人与机器、机器对机器之间广泛的通信和信息的交流。因此，物联网时代的网络将是传感器网、通信网和互联网的融合，即无所不在的泛在网络。

随着物联网关键技术的不断发展和产业链的不断成熟，物联网的应用将呈现多样化、泛在化的趋势。首先，物联网发展将以行业用户的需求为主要推动力，以需求创造应用，通过应用推动需求，从而促进标准的制定、行业的发展。放眼未来几年，全球物联网终端将会更为广泛应用于各产业，其中以工业、交通、能源及安防等产业最具成长潜力。其次，随着物联网产业的不断发展，物联网应用将逐步从行业应用向个人应用、家庭应用拓展，物联网将会使我们的生活变得“聪明”和“善解人意”，通过芯片自动读取信息，并通过互联网进行传递，物品会自动获取信息并进行传递，使得信息的处理—获取—传递整个过程有机地联系在了一起，对人类生产力又是一次重大的解放。

9.2　O2O 室内商场应用

O2O 即 Online to Offline，是指线上营销、线上购买带动线下经营和线下消费，也即把线上的消费者带到现实的商店中去——在线支付购买线下的商品和服务，再到线下去享受服务。其核心就是通过打折、提供信息、服务等方式，把线下商店的信息推送给互联网用户，从而把他们带到现实的商店中去——消费者在线支付购买线下的商品和服务，再到线下去享受服务。即将线下商务的机会与互联网结合在了一起，让互联网成为线下交易的前台。这样很快达到规模。在这个过程中三方实现互惠合作。

线下商家：降低了线下商家对店铺地理位置的依赖，减少了租金方面的支出；持续深入地进行情感联络，进而进行精准营销。

消费者：O2O 提供了丰富、全面、及时的商家折扣信息，能够快捷筛选订购适宜的商品或服务，且价格实惠。

O2O 平台：带来大规模高黏度的消费者，进而能争取到更多的商家资源。本地化程度较高的垂直网站借助 O2O 模式，还能为商家提供其他增值服务。

Local 是移动商业新模式的地理基础。通过基于位置的服务，空间使用者不仅可通过时间，亦可利用地理坐标对商务信息进行筛选，空间管理者可以精确定位每位需要与之互动的空间使用者。因此，在 Mobile 技术的支撑下，商家可以使用用户签到数据进行深度数据挖掘，收集用户的生活半径、口味喜好、消费水平及消费习惯等信息，然后针对性地提供与位

置相关的各种信息服务。

9.2.1　概述

人们80%以上的时间处于室内环境，随着社会现代化建设的不断发展，大型建筑的日益增多，室内位置服务的需求正不断增加。商业及个人位置服务、时空大数据挖掘、应急救援、安全监控、大型场馆管理、特殊人群监护等领域都需要使用准确的室内定位信息，特别是在应对紧急疏散等应急场景时，室内定位信息更是显得尤为重要。随着室内位置服务的需求日益迫切，位置服务正开始由室外导航向室内外无缝导航进行转变。

目前的室内定位技术主要依托手机上的通信系统，如无线保真（Wi-Fi）与蓝牙（iBeacon）等。机场、商场等为实现室内位置服务，进行了Wi-Fi与蓝牙网络建设，一方面通过手机客户端应用（APP）向用户提供与位置相关的位置服务，一方面自己统计客流情况，进行数据分析，优化自身的商业业态，为客户提供更好的服务。

9.2.2　室内位置服务典型应用

在线离线/线上到线下模式（O2O）行业被普遍认为是下一个万亿元规模的市场。商业广场受电子商户冲击极大，智能商场的变革已势在必行。统计表明，2012年和2013年互联网所产生的流量等于自互联网诞生以来一直到2011年所产生的数据量总和。互联网产生了大数据，而移动互联网和物联网进一步推动数据的暴涨，网络中心体现去中心化，大数据促进了信息融合和产业跨界结合，大数据引发了更多新业态的出现。因此需要利用多业态大数据挖掘技术推动相关产业的发展，而位置信息正是其中的核心信息，在数据精准推送、个人导航与地图查询、消费行为模式分析等方面都必不可少，是联系用户与商家的重要纽带。

依靠新的互联网技术与空间数据结合，发展业态的融合服务，将为用户创造前所未有的购物体验，为传统商业提供商业智能（Business Intelligence，BI）分析，实现线上线下的有效互动。就用户而言空间数据信息可以让用户在商场中不再迷茫，准确的位置、地图与电商信息将把用户与其最适合的商品轻松地串联在一起；而就商场而言，空间数据将闭合现有商业BI分析中的最后一环，彻底打通空间位置、消费及会员信息的三大线下数据的交叉分析渠道，为商场决策提供最准确的支持，使商场能与用户之间碰撞出更精彩的火花。

9.2.2.1　Wi-Fi室内定位系统

在该系统中，商场部署Wi-Fi网络，由AP探测手机的信号强度，将其上报至接入控制器（Access Controller，AC）。AC将汇聚的AP探测信息交互至本地位置控制器（Location Controller，LC），由LC进行协议解析，转换为标准定位信息报文，LC将信息报文发送给定位服务器（Positioning Server，PS），PS进行位置解算后将位置信息用于提供服务，并存入数据库，进行大数据分析，如图9-1所示。

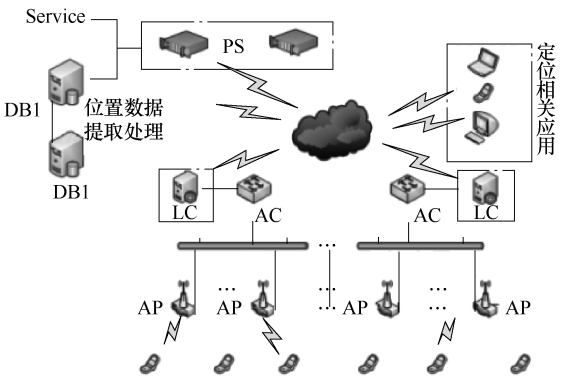


图9-1　Wi-Fi室内定位系统示意图

9.2.2.2　iBeacon 室内定位系统

许多商场已经开始建设 iBeacon 定位系统，在商场安装 iBeacon 节点，为手机提供更精确的定位服务。iBeacon 定位系统对网络要求相对较低，节点部署好后由手机 APP 通过系统的标准接口获取手机检测的 iBeacon 信号强度，然后通过通信网将信息回传到 LC，由 LC 进行定位，再将定位结果回传给手机。

9.2.2.3　O2O 商场位置服务

O2O 室内位置服务主要分 3 个步骤。

第一步：数据采集

数据采集包括 Wi-Fi 网络建设、生成室内地图、建立室内定位系统，如图 9-2 所示。

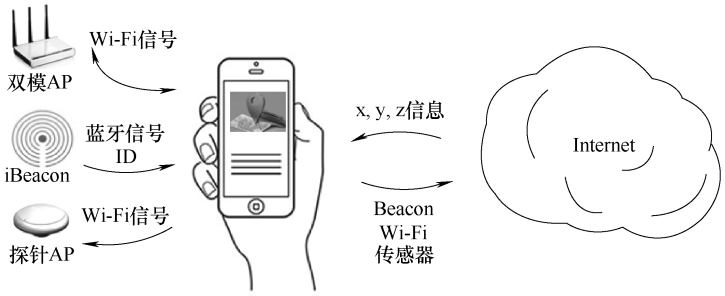


图 9-2　数据采集示意图

基于 Wi-Fi 的网络或是 iBeacon 对顾客进行室内定位，不需要终端用户使用 APP 或是接入网络，只要开启 Wi-Fi 或者 iBeacon，就能对其进行定位，是实现客流统计分析、空间大数据挖掘等的数据来源。

室内定位系统建设的整体方案如图 9-3 所示。

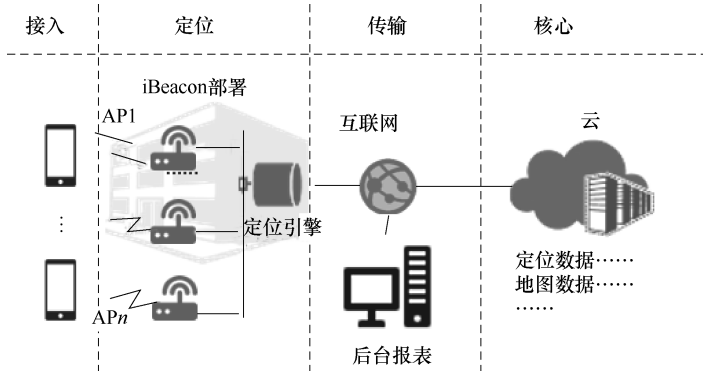


图 9-3　室内定位系统建设的整体方案

第二步：位置数据分析

除了为消费者提供导航以外，还可以记录消费者位置数据，绘制空间地图，使室内信息与定位数据无缝结合，进一步实现客流统计分析、空间大数据挖掘等。地图还可以记录位置信息变化的全部过程，提供店铺调整前后效果比较等数据分析依据。

图 9-4 所示为人员分布情况，图中的刷新时间 5s，不同颜色代表不同类型的人员，黑色点代表顾客，灰色点代表店员。

图 9-4　实时客流位置分布图

第三步：业务应用

汇总消费者信息，针对消费者偏好进行精准营销、及时调整销售方案。

商家得到如表 9-1 所示的数据，就可以对客户的到访频次、品牌的驻留时长、消费能力、购物习惯变化和社交圈等有详细了解，并对客户进行分类，根据不同用户的类型像客户的用户端推送其感兴趣的消息，从而提高销售量和用户对商家的好感度。

表 9-1　客流统计项目

	功能验收分项	数据展示方式要求		
		数据表	图　表	地　图
广场客流整体统计	每天每时段到场顾客总数	√	√	
	每天每时段到场有效顾客总数（按驻留总时长设定）	√	√	
客流量分层统计	每层楼的客流统计	√	√	√
	每位顾客逛了多少层楼的统计	√		
	按顾客逛的楼层数聚类统计	√	√	
	自定义顾客逛的层数对顾客进行查询	√		
客流分店铺统计	每个店铺客流总人数	√	√	√
	每位顾客逛了多少个店铺	√		
	按顾客逛的店铺数聚类统计	√	√	
	自定义顾客逛的店铺数对顾客进行查询	√		
顾客到访频次统计	每位顾客某天、每周、每月到购物中心的频次	√		
	每位顾客某天、每周、每月到商铺的频次	√		
客流密度热图	每个位置点上顾客的驻留时长，地图可视化呈现			√
	区分店铺、公共区、楼层，有效顾客平均逗留时长	√	√	√
客户实时位置图	实时监控场馆内顾客数量与分布			√
	针对某个客户进行首末次进店全路径跟踪	√	√	√

（续）

	功能验收分项	数据展示方式要求		
		数据表	图　表	地　图
店铺客流排名表	根据店铺的客流量进行排名，可查看前10名、前20名等，可自定义范围	√		
店铺驻留时间排名表	根据店铺有效顾客的平均驻留时长（排除路过顾客）进行排名	√		
活跃客户统计	购物中心的活跃客户：每月（季度）多次到场且每次逛了多家店铺的顾客数及比例，条件可自定义	√		
	某商铺的活跃客户：每月多次到店铺且有一定逗留时长的顾客数，条件可自定义	√		
新增客户统计	每天、每周、每月、每季度等环比新增客户数	√	√	

9.2.3　室内位置服务平台

室内位置服务平台基于空间数据信息进行数据分析与服务，平台主要包括4个层面：感知层、数据层、处理层和服务层，如图9-5所示。

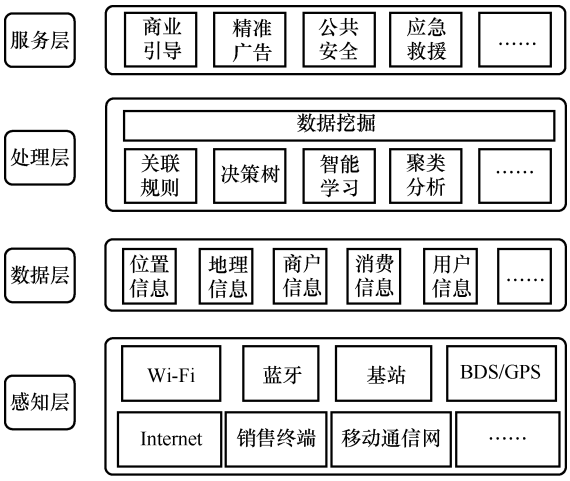


图9-5　室内位置平台分层结构

感知层：主要包括定位数据感知设备及其他数据感知设备。定位数据感知设备包括如Wi-Fi、蓝牙、基站、北斗卫星导航系统及全球定位系统（GPS）等可用于定位的传感器；其他数据感知设备包括互联网（Internet）、销售点情报管理系统、移动通信基站等感知用户、商户、消费等信息的手段。

数据层：主要包括由感知层获取的位置信息、地理信息、商户信息、消费信息、用户信息等多业态信息，构成大数据融合服务的基础。

处理层：主要利用关联规则、决策树、智能学习、聚类分析等方法，对多业态信息进行大数据挖掘，分析各信息的内在关系，为用户按需提供个性化服务与精准推送。

服务层：利用大数据挖掘的结果进行商业引导、精准广告、公共安全、应急救援等应用。用户通过手机、公共电子屏等方式获取服务信息。

9.2.4　室内定位技术

9.2.4.1　Wi-Fi 定位

Wi-Fi 网络侧定位：Wi-Fi 网络侧定位可适用于所有手机用户，常用于统计分析，也可用于精度与实时性要求较低的终端导航定位应用。该模式由 Wi-Fi 网络中的各个接入点检测打开 Wi-Fi 的手机设备，通过多个 AP 对同一手机探测到的信号强度，对手机进行定位。该模式定位精度一般在 5～8m，系统延时 2～5s。

Wi-Fi 终端侧定位：Wi-Fi 终端侧定位系统由手机探测 Wi-Fi 网络中的多个 AP 的信号强度进行定位。该方式定位精度可达 3～5m，定位延时 1s 以内。但由于 iOS 系统不支持 APP 获取 Wi-Fi 的相关信息，因此该种方式能适用于安卓系统手机，不能用于 iPhone 手机，成为制约该方式应用的主要瓶颈。

9.2.4.2　iBeacon 定位

iBeacon 是苹果公司制定的专用于蓝牙定位的一种协议技术，安卓系统也兼容了该技术。iPhone 4S 以上且采用 iOS 7 以上系统的 iPhone 用户、具有蓝牙 4.0 以上硬件及安卓 4.3 以上系统的安卓用户均可采用该方式定位。iBeacon 成本较低，可以在 6～10m 的间距进行高密度部署，定位精度，定位延时 1s 以内。

9.3　iBeacon 应用——智能图书馆

9.3.1　智能图书馆系统架构

1. 软件架构

本架构分为 4 层，分别是传感器接入层、位置传感网数据处理层、位置传感网服务引擎和位置传感网应用层，如图 9-6 所示。

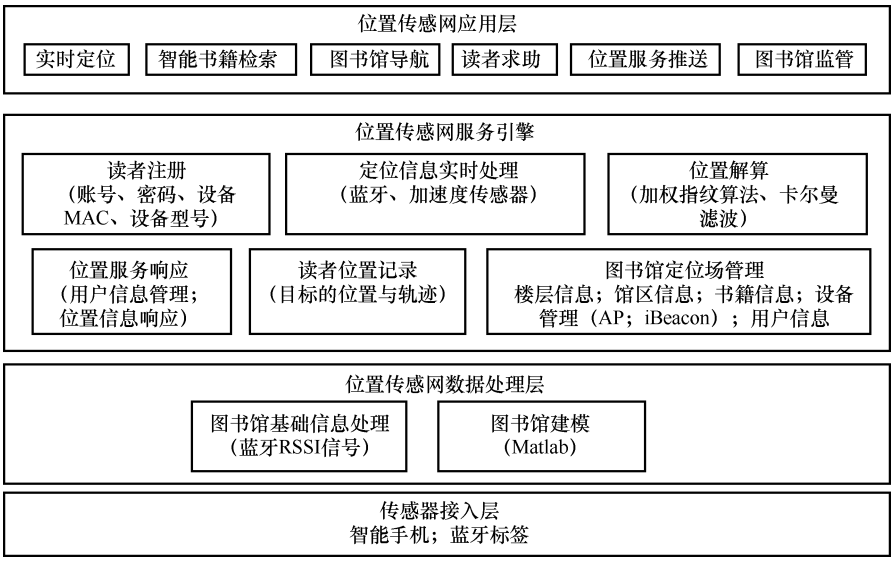


图 9-6　智能图书馆系统软件架构

2. 硬件部署

图9-7所示为智能图书馆系统硬件部署。系统的硬件分为5类：蓝牙iBeacon基站、读者终端、智能图书馆后台服务器、管理员终端、3D监管终端。

图9-7　智能图书馆系统硬件部署

（1）蓝牙iBeacon基站

蓝牙iBeacon基站作为智能图书馆定位的基础硬件设备，用于发送蓝牙RSSI信号，与移动终端进行通信。

（2）读者终端

采集RSSI信号，通过加权指纹算法与卡尔曼滤波算法实时计算出当前坐标，参照指纹信息库，解算出读者位置，向服务器发送服务请求来获取相应的位置服务。

（3）智能图书馆后台服务器

存储、管理与转发系统内的数据。

（4）管理员终端

当读者发送求助请求时，管理员终端能实时显示出需要帮助的读者所在的位置以及读者的求助内容。其他功能与读者端类似。

（5）3D监管终端

实时显示图书馆的运行情况，包括读者状态与馆区状态。

9.3.2　定位传感网

传感器网络部署在图书馆室内空间，具有位置感知能力。通过室内外位置传感网构建定位场，待定位目标与定位场相互作用，位置服务网关（LBS－GW）获取相关信息后，由实时定位引擎（RTLS）计算产生待定位目标的位置信息。

定位设备分为手持终端和蓝牙信号发射基站两部分。手持终端被定位人员携带即可，蓝牙信号发射基站将被有序地部署在图书馆各层的阅览室、书库、自习室和报告厅等场所。最终需要根据定位效果确定以及调整蓝牙信号发射基站部署规模，每40m^{2}布置一蓝牙信号发射基站。

室内地图语义指事先已在 Oracle 数据库存储的地图数据库信息，主要为地图属性，例如门是可通过的，窗户是不可通过的。然后可以方便地将存储在服务器数据库中的语义数据提取出来加以使用。图 9-8 所示为智能图书馆定位流程。

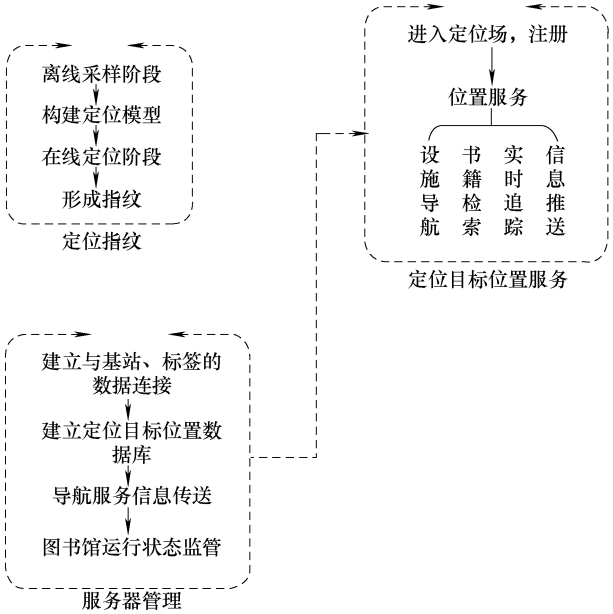


图 9-8　智能图书馆定位流程

9.3.3　图书馆 LBS 位置服务

LBS 提供的与位置相关的服务如下。

1. 实时定位与服务推送

空间位置感知设计目标是当读者持智能手机进入图书馆时，打开导航 APP，显示读者的空间位置。当读者经过某个设施的附近，系统界面下方将会自动推送该设施的相应介绍和使用状态。

2. 智能书籍检索

在书籍检索界面输入图书名搜索图书时，系统界面会显示书籍所在的位置，并引导读者至相应馆区，实现高效的书籍检索服务。

3. 馆区导航

系统能够将用户导航至图书馆中，当读者使用导航时，选择想要到达的馆区，系统界面即可显示到达该馆区的导航路径。

4. 手机客户端应用

在用户端，则通过 APP 向用户提供一体化的服务。APP 通过地图与位置信息，将商场的一系列服务串联起来，典型功能包括以下几项。

看地图：查询地图，搜索兴趣点。

定位导航：用户对自己进行定位，并获取导航路线。

反向寻车：在停车后记录自己的停车位置，离开商场时进行导航，准确寻找自己的

车位。

优惠推送：根据位置信息与大数据分析平台得到的客户偏好进行优惠信息推送。

商品查询：查询商品相关信息。利用位置信息可将距离较近的商品列表放在前面，便于查找。

移动支付：基于位置进行手机支付。将位置信息与顾客需要付款的店铺绑定，可使用户更加便捷地付款。

会员卡：顾客在办理会员卡时可在手机上一键操作，然后 APP 根据顾客的定位信息，自动接入所在店铺的会员系统。

9.4　可穿戴设备

9.4.1　可穿戴设备定义

可穿戴设备也称可穿戴计算设备，目前并没有统一的概念定义。麻省理工学院对可穿戴计算设备的定义是计算机科技结合多媒体和无线传播以不突显异物感的输入或输出仪器（如首饰、眼镜或衣服）连接个人局域网络、侦测特定情境或成为私人智慧助理，进而成为使用者在行进动作中处理信息的工具。

可穿戴设备通常以人体为载体，通过便携式穿戴，实现对应的业务功能。可穿戴设备与人体的交互形态主要基于人体能力和设备内置能力配合实现，是计算“以人为本、人机合一”理念的产物。基于这些定义，可穿戴设备可理解为基于人体自然能力之上的，借助计算机科技实现对应业务功能的设备。人体自然能力指人类本体与生俱来的能力，如动手能力、行走能力、语言能力、眼睛转动能力、心脏脉搏跳动能力、大脑神经思维能力等；这里的计算机科技指基于人体能力或环境能力通过内置传感器、集成芯片功能实现对应的信息智能交互功能。

具体而言，穿戴式智能设备是应用穿戴式技术对日常穿戴进行智能化设计，开发出可以穿戴的设备的总称，如眼镜、手套、手表、服饰及鞋等。

而广义的穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分功能，例如智能手表或智能眼镜等，以及只专注于某一类应用功能，需要和其他设备如智能手机配合使用，如各类进行体征监测的智能手环、智能首饰等。随着技术的进步以及用户需求的变迁，可穿戴式智能设备的形态与应用热点也在不断变化。

穿戴式技术在国际计算机学术界和工业界一直都备受关注，只不过由于造价成本高和技术复杂，很多相关设备仅仅停留在概念领域。随着移动互联网的发展、技术进步和高性能低功耗处理芯片的推出等，部分穿戴式设备已经从概念化走向商用化，新式穿戴式设备不断传出，谷歌、苹果、微软、索尼、奥林巴斯、摩托罗拉等诸多科技公司也都开始在这个全新的领域深入探索。

9.4.2　可穿戴设备分类

目前行业尚未对可穿戴设备分类给出明确的界定方式，可以按照可穿戴设备的物理形态、业务应用形态和通信类型进行划分。

9.4.2.1　按照物理形态分类

按照设备物理形态可分为眼镜、手表、手环、手套、项链、挂件、头箍等类型。

1）眼镜。以谷歌眼镜为代表的可穿戴设备是可穿戴概念的最早践行者，镜片集成显示屏幕实现内容的展示功能，镜框内置的芯片、智能操作系统等实现应用的运行、数据存储、网络交互、自然语言的交互等功能。通过开放 SDK 程序包，开发者可开发个性化的应用并运行在眼镜上。

2）手表。手表是传统穿戴式设备，在手表内集成计算芯片和智能操作系统，并通过手表显示屏实现内容的呈现和交互，实现程序的运算是可穿戴设备对手表的理解。目前三星、苹果等电子厂商均在智能手表领域有对应的产品。

3）手环。在手环上集成传感器感知功能芯片，通过内置小型显示器实现数据的呈现功能，手环的应用主要集中在健康领域。例如通过人体感知实现睡眠管理等。

4）手套。手套是不太成功的可穿戴设备，市场上可见的手套类型设备包含两类：一种是手套上集成传感器实现动作信息的感应功能，以实现精细化的控制操作；另一种是通过近距离的通信功能和手机绑定，实现耳机功能。

5）项链。项链类设备常见于宠物类应用中，一般以吊坠的方式集成芯片和操作系统，实现定位和通信的功能。应用以平台提供网页或 APP 的方式进行操作。某些项链里面还集成了语音功能，可监控设备周围环境声音。

6）挂件。通过挂件内集成传感芯片、计算芯片和显示屏幕，实现交互功能。一般用于健康领域，如通过内置陀螺仪、定位芯片、加速度传感器等通过对运动轨迹、步伐的统计，计算出运动的能量消耗，给出健康提醒反馈。

7）头箍。头箍类设备更多的是偏概念类设备，目前尚不成熟，其原理是内置芯片感知大脑活跃度，并根据活跃度实现控制输出。目前主要在一些简单的游戏中使用。

9.4.2.2　按照应用类型分类

按照设备应用类型可分为健康类应用、安全类应用、游戏类应用等类型。

1）健康类。健康类应用设备主要指应用形态以满足人们健康需求为主，包含医疗相关设备和健身运动类相关设备。医疗可穿戴设备如测心率的腕表等，健身运动类设备如计步器等。

2）安全类。安全类应用设备主要是基于位置地点或范围识别的安全类应用设备，如基于手环或项链识别佩戴者当前所处的地理位置的设备；通过蓝牙近距离通信技术实现钱包防窃、小物件识别等设备。

3）游戏类。游戏类应用设备包含微软 Kinect 体感设备等，主要满足娱乐需求。

9.4.2.3　按照通信类型分类

设备按照与网络的结合方式包含几类：直接和互联网结合、通过中转介质和互联网结合、与智能设备结合。

1）直接通信。通过内置的移动通信芯片，如 GPRS、CDMA、Wi-Fi 等实现和网络的通信功能。

2）间接通信。间接通信借助智能终端的通信能力，设备以蓝牙、红外、ZigBee 等短程通信协议和智能设备结合，智能终端作为数据节点进行通信。智能终端内置 APP 或者基于网络的程序借助云平台侧数据和处理逻辑实现应用的呈现。

3）端到端连接。设备以蓝牙、红外、ZigBee 等短程通信协议和智能设备结合，智能终端内置 APP 实现业务的呈现。

9.4.3　可穿戴技术关键技术

各种可穿戴设备的功能虽不尽相同，但大部分都是由各类传感器实现数据的收集再配合不同的算法完成的，下面是各类智能可穿戴设备的主要技术。

9.4.3.1　传感器技术

1. 重力传感器

智能手环运动监测功能通过重力传感器实现。重力传感器已是一种很成熟的技术，手机也早有应用，比如现在智能手机的屏幕翻转功能，就是通过重力传感器来实现的。传感器通过判断人运动的动作得到一些基础数据，再结合用户之前输入的个人身体体征的基本信息，根据一些特定算法，得到针对个人的个性化监测数据，诸如运动步数、距离以及消耗的热量等，从而判断运动的频率和强度。由于每个人运动随个人身体体征的不同而产生不同的效果，因而用户在使用手环进行监测前需要在 APP 中录入自己的性别、年龄、身高、体重等信息，信息自动同步到手环中，通过传感器监测运动动作，经过特定算法最终实现运动监测的功能。

睡眠监测也通过相同的传感器技术实现。人的睡眠按照脑电波信号可分为 5 个阶段：入睡期、浅睡期、熟睡期、深睡期、快速动眼期（Rapid Eyes Movement，REM）。在不同阶段，人的脑电波可以迅速改变。有意思的是，重力传感器并不具备直接探测脑电波的功能，所以它是将人在睡眠中动作的幅度和频率作为衡量睡眠的标准，来判断睡眠处于哪个阶段；手环的智能闹钟功能，会在快速动眼期将用户唤醒。

2. NFC（Near Field Communication，近场通信）技术

NFC 技术主要实现名片传送、开锁解锁、信息交换等功能，只要手机支持 NFC 技术，通过触碰对方的手机就可以将个人联系方式或者网址链接等信息传送过去。此外，还可以对手机应用程序进行加密解锁，设备与手机一接触，就可以解锁，来保护隐私。

NFC 技术即近场无线通信技术，是一种短距离的高频无线通信技术，允许电子设备之间进行非接触式点对点数据传输。NFC 芯片相当于一个天线，与手机后面的芯片接触时，通过电磁传递能量的原理，将手机上微小的电流传感到介质的芯片上，然后用电流去驱动芯片上的电路，进而将信号传输出来。NFC 技术前身叫作 RFID 技术，此前更多地被用于生产、物流、资产管理等领域，比如物流领域中给货物贴上标签，然后用来采集货物信息或者判断是否丢失等。在智能手机出现之后，手机厂商开始将其定义了一个频段然后应用在手机上。

3. 脑电波传感

Brain Link 运用的最核心技术是脑电波传感技术。此技术原用于医疗和军事领域，如医疗中对儿童多动症的治疗等。以往这些应用技术由于成本太高以及用户体验较差，所以无法在大众消费市场中推广。现在对传感器、芯片，包括微机电的技术进行改进，使之体积缩小、成本降低，从而使得这样的技术可以在大众电子消费市场里推动，通过方便易戴的头箍形式实现。

以往的脑电波的传感要通过很多个传感头来实现，约有 16 位或者 64 位，传感器上需要

涂抹导胶，医院的相关设备需要专业的医生为患者佩戴，佩戴过程需要耗时四十多分钟。现在将传感器的材料变成金属的传感器，采用干电极，不需要涂抹任何的导胶，同时传感头的数目减少为3个，这样，用户通过设备说明书即可自行操作，简单方便且用户体验更佳。

4. GPS + LBS 结合定位

定位技术通过 GPS 卫星定位技术和 LBS 基站定位双结合的技术实现。GPS 卫星定位准确、稳定，但是受到天气和位置的影响比较大，当遇到天气不佳或者位置不利的情况，就会受到很大影响，甚至无法进行定位。LBS 基站定位系统是通过电信移动运营商的网络获取移动终端用户的位置信息，在电子地图平台的支持下的一种位置服务，其使用方便，成本低，只要用户手机有信号即可定位，不受天气和位置的影响。但是其定位精度同位置技术站的数量相关，误差在 50 ~ 500m 之间，在偏远地区或者手机信号不佳的地区，会产生比较大的定位误差。将两种定位技术相结合，优势互补，为用户提供更精准的定位。

9.4.3.2　可穿戴计算技术

1. System on Chip 体系结构设计技术

该设计技术可把计算机的硬件集成到一个芯片里，这样计算机可以做得很小而且有利于降低功耗、提高速度，尤其是可以降低成本缩短生产周期。

2. 微小计算机多端口高性能 I/O 设计技术

可穿戴计算设备的主机是微小型的，但却要与多达十几部的外部设备相连，因此要求微小型计算机拥有足够多数量的接口，而且要有很高的 I/O 处理能力。

3. 无线自组网络技术

可穿戴计算设备系统要伴随人的活动并作为一个移动节点随时上网，多个这样的节点将构成一个特殊的网络，称之为自组网，这类网络没有固定的路由器，各节点以任意方式移动并动态连接，每个节点都可以充当路由器，且所具有的自动重组功能还可以提高网络的抗毁能力。这类网络具有以下特点：动态变化的拓扑结构，受限且经常变化的带宽，可能出现的非对称连接，终端受限的操作，分布式控制的网络。

4. 嵌入式操作系统技术

现存的微机操作系统可以用于可穿戴计算机系统，但由于可穿戴计算机系统的体积和存储空间十分有限，所以，操作系统应尽量压缩到专用的程度，并提高实时性。因此需要使用嵌入式操作系统，这类系统常常是实时的和微内核的，并具有极强的处理多外设的能力。

5. 移动数据库技术

可穿戴计算机系统在移动中上网，移动中访问数据库，这类移动式的数据库管理技术将有别于固定的数据库管理，移动数据库需满足以下4个目标：可用性与可伸缩性；可移动性——移动中访问或移动中更新；可串行性——支持可串行的并发事务处理；收敛性——系统总能收敛到一致状态。

6. 人机交互技术

可穿戴计算机系统实际上是一个实时的信息处理系统，又是一个人机结合、以人为本的集合体，人际关系更加和谐自然，因此人机交互技术是可穿戴计算机系统的关键技术，它应解决了人与计算机之间的交互问题以及人通过这种交互提高对周围实物店感知的能力。

7. 基于蓝牙的无线传输技术

可以想象当多达几十个模块分布于人体之上，它们之间的连线将是十分沉重的负担，而

且是一个不可靠因素，而利用蓝牙可代替这些线。

8. 外部设备选择与设计技术

可穿戴计算机系统除了主机之外，就是大量的外部设备，设备的选择与设计至关重要。其中主要包括输入类设备、输出类设备和电源等。对这些设备的要求是：具有高性能指标，小体积低功耗，符合人体特征，有利于健康，安全可靠。

9.4.4 已发布智能可穿戴设备

1. Google Glass& 微软眼镜

Google Glass 内置 GPS、动作传感器、摄像头等，可以指路、好友互动、拍照和拍摄视频，并与 Google 其他服务紧密集成，更增加了现实体验感。

微软眼镜命名为“Monocle”，该智能眼镜可以在观看实况比赛过程中，为用户提供相关的数据信息，增强现场体验感。

2. Nike + 和 iWatch

Nike + 和 iWatch 为智能运动手环。Nike + 是一系列可穿戴设备和应用，主要为用户提供运动记录和数据分享等功能，产品包括：Nike + SportWatch GPS、Nike + Running 应用程序、Nike + SportBand 等；iWatch 所能实现的是简单的数据通信和中转。

3. 小米智能鞋和 Heapsylon

小米智能鞋是由小米公司推出，该智能鞋能与小米手机连接在一起，不仅可以测算路线，还可以测算出跑步时的心率等情况；Heapsylon 则是可以测量跑步者的步数、步距、速度和消耗热量的智能袜子。

9.4.5 可穿戴设备存在的问题及发展方向

1. 存在问题

智能可穿戴设备领域仍处在发展的初级阶段，相应的产业链、商业模式等都没有成型。目前，主要存在以下问题。

（1）多为智能手机“配件”，独立性不强

大部分的智能可穿戴设备都是智能手机的辅助工具，一部分是对智能手机功能的拓展，一部分是对智能手机功能的平移。如小米智能手环，仅仅是对智能手机部分功能的平移。通过蓝牙连接后，小米手环可为用户提供闹钟叫醒、睡眠测试、运动记录等功能，只是作为智能手机（安卓系统）的辅助外设，失去了独立存在的必要性。另一方面，智能可穿戴设备的硬件设计、生产需要对接多个合作伙伴和厂商，其整个过程市场极其烦琐；同时由于智能可穿戴设备作为智能手机的“配件”存在，需要和代工厂合作，内部审核流程复杂，模具评审时间长，在一定程度上延长了智能可穿戴设备的研发周期。

（2）功能尚不完善，专属应用较少

随着智能可穿戴设备市场的不断发展壮大，逐步形成了一个新的智能可穿戴设备的 APP 市场，但目前智能可穿戴设备功能尚不完善，专属应用较少。整个智能可穿戴设备市场呈现生态环境高度碎片化，市场上的各种智能可穿戴设备，由于各自运行的平台不同，使得开发商/ 研发者很难开发出适应多种设备的应用软件。

（3）以数据为中心，用户体验差

大部分的智能可穿戴设备都强调以数据为中心，实现与第三方数据的有效对接，主要集中在对各种数据进行分析、处理和综合等，以期为用户提供更多、更可靠的数据和分析。但是由于不同的健康大数据服务平台进行数据整合的方式、标准各不相同，导致数据标准多样化，不同平台间的数据不能互通，在一定程度上忽略了人机交互设计和用户体验。智能可穿戴设备功能应用于用户的常规需求贴合度较低，不能满足用户对于智能可穿戴设备的期望。

（4）电池技术亟待升级

智能可穿戴设备的电池使用时间一直是影响使用体验的重要问题。功耗、电池寿命都是阻碍智能可穿戴设备市场发展的因素，但是新的电池产品的研发及快速充电技术的研发进展缓慢，虽然在电池研发领域已经有所突破，但是受限于成本等问题，还未能大规模商用。

（5）费用昂贵，渗透率低

在目前已经发布的智能可穿戴设备中，Google Glass 为一流产品，但是其价格的高昂使其不能被中低收入水平的用户接受。但是，随着技术的进步，智能可穿戴设备的价格将会出现一定程度的下滑。

2. *发展方向*

虽然智能可穿戴设备存在以上诸多问题，但是该领域的发展势头却不可阻挡。主要表现在以下几个方面。

（1）硬件

智能可穿戴设备未来硬件的发展方向主要集中在电池和充电技术、屏幕和处理器 3 个方面。在研究柔性薄膜电池技术、非接触式充电技术等的同时，提高智能可穿戴设备屏幕的曲度、柔韧性和分辨率；并且研发低功耗处理器，使智能可穿戴设备在实现人机交互的同时，更注重用户体验。

（2）软件生态系统

随着智能可穿戴设备市场的蓬勃发展，智能可穿戴设备的产品类型将呈现整合与细分并行的发展趋势，不断整合新的应用和服务，力求为用户打造一体化的智能可穿戴体验；构建良好的软件生态系统，解决智能可穿戴设备领域的跨平台的操作。

（3）大数据及云服务

未来的智能可穿戴设备将进一步整合传感器采集的数据与云服务，同时整合第三方服务机构，为用户提供基于大数据的个性定制化服务。

9.5　智能硬件

9.5.1　物联网在智能硬件中的应用

智能硬件是继智能手机之后的一个科技概念，通过软硬件结合的方式，对传统设备进行改造，进而让其拥有智能化的功能。智能化之后，硬件具备连接的能力，实现互联网服务的加载，形成“云 + 端”的典型架构，具备了大数据等附加价值。改造对象可以是电子设备，也可以是以前没有电子化的设备。涉及领域包括可穿戴设备、智能家居、互联网智能硬件、虚拟现实设备等。其涉及的主流产品大致包括以下几类：一是记录运动、睡眠等行为的手环类产品；二是控制家用电器的开关类产品；三是基于位置信息的定位产品；四是测量体重、

血压等信息的健康类产品；五是智能化的家居、娱乐、外设产品。

经历了“链接人与服务”到“链接人与设备”的过程，互联网巨头纷纷进入智能硬件市场，推出了智能硬件产品，以及不同角度的平台化切入。

智能硬件正在慢慢走入我们的生活，不仅仅是各大商家需要适应新时代的潮流，我们也应该在这个大环境下跟随潮流，尽自己的一份力量，同时也应注意保护好自己的信息安全。

9.5.2　智能硬件的典型应用

9.5.2.1　智能手表简介

智能手表，是将手表内置智能化系统、搭载智能手机系统而连接于网络以实现多功能，能实现同步手机中的电话、短信、邮件、照片、音乐等功能。

智能手表采用的主要技术为：微处理器（或单片机）+电源方案（电池+电源管理芯片）+通信+传感器。微处理器或单片机负责设备的计算和管理，电池以及电源管理芯片负责整个设备的供电，通信方案使用 NFC 和蓝牙，传感器根据功能需求选择加速度、陀螺仪、指南针以及心率监测等。

9.5.2.2　智能电视简介

智能电视是基于互联网浪潮冲击形成的新产品，其目的是带给用户更便捷的体验，打破遥控器对传统电视的束缚，实现了带走看、分类看、多屏看和随时看四大功能。智能电视具有全开放式平台，搭载了操作系统，用户在欣赏普通电视内容的同时，可自行安装和卸载各类应用软件，是持续对功能进行扩充和升级的新电视产品。智能电视能够不断给用户带来有别于使用有线数字电视接收机的丰富的个性化体验。

智能电视的关键技术包括芯片技术、显示技术、操作系统、软件与应用、联网技术和人机交互技术，这里选取与物联网有关的进行简介。

芯片技术：高集成度，多核是主流。智能电视需要既能完成传统电视的解码显示功能，又能运行操作系统和众多应用，因此芯片设计上两方面均要兼顾。智能电视芯片主要有单芯片和双芯片两种设计方案，早期设计多以双芯片为主，目前国内智能电视芯片主要以单芯片为主。单芯片方案一方面有成本优势，另一方面降低了智能电视的设计和研发难度。

操作系统：操作系统是智能电视的核心部分，一直以来都是各企业大力研发，投入最多的一个项目。因为电视智能化实现的前提就是要有强大的操作系统，目前已上市的智能电视使用的操作系可大体分为4类，即 Android、Windows、iOS 及 Linux 企业自建系统。

联网技术：①Wi－FiDisplay 技术，影像的压缩/解压处理及管理数据流的传输层等利用 Wi－FiDisplay 处理，同时将延迟的时间降低到0.01ms 以下，非常适用设备间将高清影像进行随时 & 可靠的传输；②WiGig 技术，使用60GHz 频段，是一种传输速率可达到7Gbit/s 的短距离无线技术，是普通 Wi-Fi 速率的10倍以上，非常适合传输高清图像和大容量文件。

人机交互技术：传统遥控器输入效率很低，已经不能满足要求。智能语音和体感遥控是未来人机交互的发展方向。

9.5.2.3　智能路由器简介

智能路由器就是智能化管理的路由器。智能路由器具有独立的操作系统，用户可自行安装、控制带宽、上网加速、过滤视频广告等，远不局限于无线上网的功能。比如它将一个单一功能性的产品变成了一个平台，在这个平台上面，可以安装 APP 插件来增加新的功能。

此外，智能路由器的“智能”还要体现在用户体验上，这里不得不说到的是智能路由器提供的移动终端配置功能，用户可以通过手机或 PAD 通过第三方软件轻松对家中的路由器进行设置。无论路由器发展到什么地步，这些用户体验都是无线路由器中的“智能”所在。

纵观现有包括智能路由器在内的各种家用路由器设备，其功能大致可以分为 3 个层次。第一个层次是最基本的网络功能，例如 WLAN 及有线接入、有线或 3G 连接互联网、支持 PPPoE 拨号、支持 DHCP 及 NAT、接入加密及控制等，普通家用路由器大多只提供这一层次的功能；第二个层次是在普通路由器上提供一些扩展功能，例如网络存储、离线下载、蹭网检测、应用加速等；更高一个层次是在路由器上提供应用平台，用户可以自行下载并安装所需要的应用，具有更大的灵活性和可扩展性。基于路由器的功能分层，智能路由器是指具备一定的操作系统，在传统路由器的基本网络功能之外，能够提供存储、安全、下载等更多扩展功能的路由器产品，更进一步的智能路由器可具备应用平台，支持 APP 自由扩展安装。

要具备第二层次和第三层次的功能，意味着需要有一定的操作系统支持。目前路由器上使用的操作系统也可以分为 3 类：一是 WLAN 芯片厂商提供的开发套件 SDK；二是 VxWorks、eCos 等嵌入式实时操作系统；三是 OpenWRT、DD－WRT、Tomato 等开源路由器操作系统。普通路由器主要使用前两类系统，但也有一些所谓的“极客”会在某些型号的普通路由器上安装第三类系统以增强路由器功能；而智能路由器则多基于第三类操作系统开发，尤其是 OpenWRT。从这个意义上说，智能路由器是将原先极客们自行改造的路由器商品化、大众化，降低了普通用户使用的门槛。

除了功能上的差异，智能路由器的配置也普遍更高一些。除了在无线侧选择支持 802.11ac 为主外，CPU 主频、RAM 内存容量等参数也都更高，这也是路由器智能化的基础。在提高配置的同时，智能路由器产品的价格相对于同级别的产品反而相对更低，这也是很多用户关注智能路由器的一个重要原因。

其实智能路由器的出现，就是将原来一些偏极客的功能（例如对路由器进行刷新的第三方固件、DD-wrt、tomato 和 penwrt 等常用的针对路由的嵌入式 Linux 系统）带给普通大众。另外，在智能路由器中一些方便用户生活的功能也添加了进来，例如各类应用商店的加速功能、下载加速、脱机下载等功能在用户每天的生活中都是息息相关的，这些更为融合了时下的移动互联网的需求元素。

9.6　车联网

9.6.1　车联网概述

9.6.1.1　车联网基本概念

车联网是指综合应用射频识别（RFID）、全球定位系统、车用信息采集、道路环境信息感知等信息传感设备，对人/车/路的静、动态信息进行采集、识别、传输、融合和利用，从而能够将人/车/路与互联网连接。车联网技术是结合移动通信、环保、节能、安全等发展起来的融合性技术，可以实现车与车、车与路、车与人、车与传感设备等交互，实现车辆与公众网络通信的动态移动通信系统。

随着移动互联网、车联网及物联网的发展，一个智能汽车的时代正在到来，无线通信技术与汽车电子技术整合的趋势正在加速，通过配备车联网产品，汽车等移动交通工具摇身一变成为一个移动网络，从而让用户享受到无处不在的信息服务。

9.6.1.2　车联网与物联网的联系

国际电信联盟（ITU）给物联网的定义是，物联网主要解决物品到物品（Thing to Thing，T2T），人到物品（Human to Thing，H2T），人到人（Human to Human，H2H）之间的互连。定义中特别指出，H2T 和 H2H 中的 H（human）指的是通过通用装置而非个人计算机实现互连的人。通过物联网，可以构建无处不在的网络，实现任何时间、任何地点，互连任何物品的需求。

由此可见，车联网是物联网络的一部分。当物联网中互连的对象都是车辆以及一些道路基础设施时，物联网就成为了车联网。物联网的范畴要比车联网大得多，车联网只是物联网的一种特定应用。然而，要真正全面实现物联网，尚存在一些困难，比如全球标准不统一、部署成本过高、技术尚不够完善、安全性等问题。相比之下，车联网的实现就具有更高的可行性了。车联网的研究过程中需要借鉴物联网的研究成果和研究思路，同时，车联网的研究成果也将丰富发展物联网的研究工作。

与物联网相比，车联网有一些自己的特点。

1）车联网当中的网络节点以车辆为主，这就决定了车联网的高动态特性。与一般的物联网相比，车联网中的汽车节点移动速度更快、拓扑变化更频繁、路径的寿命更短。

2）与一般的物联网相比，车联网中的汽车节点间的通信受到的干扰因素更多，包括路边的建筑物、天气状况、道路交通状况、汽车的相对行驶速度等。

3）车联网中受到车辆运动情况、道路分布状况等因素的影响，网络的连通性不稳定，这在一定程度上限制了车联网的推广使用。

4）车辆中有稳定的电源供电，网络工作时一般没有能量方面的限制；车辆中有较大的承载空间，可以装备较高性能的车载计算机以及一些必要的外部辅助设备，如 GPS、GIS 等。

5）车联网对网络的安全性、可靠性以及稳定性要求更高。车联网的应用过程中，不能够像互联网一样出现一些不安全、不可靠的事件，否则可能会造成巨大的生命财产损失，引起车辆行驶的混乱。

9.6.2　自动驾驶与车联网

1. 自动驾驶汽车嵌入车联网

自动驾驶汽车采用以可见光网络为基础的车联网，车联网由标准的无限车联设备、中央信息系统两部分组成。固定在汽车和道路上的标准无限车联设备通过实时发射和接收可见光信号，实现自动驾驶汽车和中央信息系统之间的信息交流和共享。标准的无限车联设备包括发射和接收两部分，实现发射和接收光信号的功能。发射部分由白光 LED 光源和信号处理单元组成，发射的调制光为可见光且发射角较大，对人眼的损害很小，因此发射部分可以具有较大的发射功率，提高了可见光通信的可靠性。接收部分包括光电检测器和信号处理单元，光电检测器将接收到的光信号转换为电信号，信号处理单元对电信号进行放大和处理后送至中央信息系统进行处理，处理结果以相同的方式反向传送给无人驾驶汽车，最终实现信

息的交流和共享。其工作过程示意图如图9-9所示。

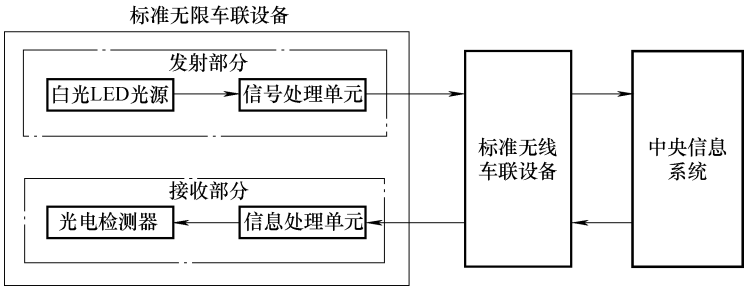


图9-9　自动驾驶汽车嵌入车联网

2. 基于车联网自动驾驶汽车的应用设计

基于车联网的自动驾驶汽车在道路环境中运行应用示意图如图9-10所示，在自动驾驶汽车行驶的过程中，标准的无线车联设备将车辆运行状态、车辆位置和目的地等信息发送给中央信息系统；集成了白光LED阵列的交通信号灯接收无人驾驶汽车的信息，同时将该信息传递给中央信息系统；中央信息系统对车辆当前的运行环境、行驶路线、车辆状态等信息进行分析处理，以判定车辆的运行安全性。

中央信息系统根据接收到的信息经过车联网计算云算出车流量等道路信息，然后通过白光LED交通信号灯将道路信息发送到车辆。自动驾驶汽车根据该信息设计规划出车辆的最优路线，缓解交通堵塞。当发生交通事故时，自动驾驶汽车可通过车联网将事故地点、伤员情况等重要数据自动上传到中央信息系统，以便交警和救护人员进行支援和救助工作。

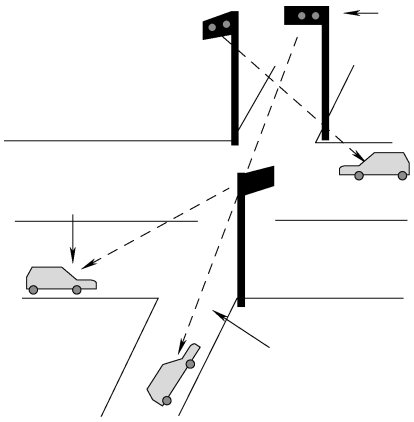


图9-10　自动驾驶汽车在道路环境中运行应用示意图

9.6.3　车联网关键技术

RFID：RFID是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，识别工作无须人工干预。当前，RFID技术已经应用于一些领域中，如物流与供应链管理、不停车收费系统等。RFID应用于车联网的主要优势是该技术可以识别高速运动的多个物体，可以容易地实现车联网中节点间的数据传输。在车联网中，建议采用有源RFID技术实现通信，有源RFID可以提供更远的读写距离，并且可以实现主动感知，这一点对于车联网来说比较重要。与其他一些传输技术相比，RFID还具有数据存储量大、小巧轻便、使用寿命长、防水防磁、安全性好等优点。

中间件技术：中间件技术是当前软件研发领域中的核心技术，在物联网领域，同样需要重视物联网RFID中间件的研发。RFID中间件是实现RFID硬件设备与应用系统之间数据传输、过滤、数据格式转换的一种中间程序，将RFID读写器读取的各种数据信息，经过中间件提取、解密、过滤、格式转换、导入车联网的应用程序中，并通过应用系统反应在用户界面上，供车联网用户使用。针对车联网中的不同应用，可以开发不同的RFID中间件，如车

辆路径导航中间件、紧急事件处理中间件、车辆辅助驾驶中间件、交通信号控制中间件等。每种中间件的开发都需要参照车联网应用服务的要求和标准进行。中间件技术降低了应用开发的难度，提高了开发效率。

协议研发：车联网没有采用传统的TCP/IP参考模型，这就决定需要研发新的适用于车联网的网络协议栈。新协议的研发也应参考OSI网络分层的思想，依据车联网的体系结构逐层进行探讨。新协议的研发应该引入当前的最新研究成果，同时结合车联网的实际特点，注重协议的运行效率。车联网还需要接入Internet，这就需要研究协议转换的问题，使得车联网中的数据与Internet中的数据实现互通。当然，车联网中的网络协议也包括网络控制、数据安全传输等方面的内容。

智能技术：车联网应该是一种智能化的新型网络，需要在车联网中采用一些先进的智能技术。通过使用智能技术，可以使车辆具备一定的智能性，能够主动感知环境的变化、实时交通状况甚至是驾驶员的需求等。智能技术研究的主要内容包括人工智能理论、智能控制系统、信号处理识别、信息融合等方面的内容。被寄予重望的汽车无人驾驶、交通智能导航等应用都要以智能技术的运用为基础。

安全可靠性：构建安全、可靠的物联网应用系统是当前研究的一个热点及难点技术，安全性和可靠性将决定车联网的推广普及程度。物（车）联网的开放性、包容性和匿名性带来了一些不可避免的安全隐患，物（车）联网的复杂恶劣的应用环境对可靠性提出了极高的要求。车联网应该具有防御网络攻击、保护个人隐私和确保数据传输准确等方面的能力。

9.7　自动驾驶

自动驾驶汽车就是无人驾驶汽车，也称为智能汽车。它是仿人驾驶的，分三步进行：首先由装在驾驶室的摄像机和图像识别系统辨别驾驶环境；其次车载主控计算机和相应的路径规划软件决定是沿车道前进还是换道准备超车；最后自动驾驶系统向方向盘、油门和制动控制器发出动作指令。

20世纪80年代以来，智能控制理论与技术在交通运输工程中越来越多地被应用。在这一背景下，自动驾驶汽车的提出是十分必然的。智能汽车是一种高新技术密集的新型汽车，是目前主流汽车的换代产品。

9.7.1　自动驾驶简介

根据自动驾驶汽车依靠人工智能、视觉计算、雷达、监控装置和全球定位系统协同合作，让电脑可以在没有任何人类主动的操作下，自动安全地操作机动车辆。

根据这个定义，自动驾驶其实已经有了一定程度的实际应用。判断自动驾驶的核心在于主动式的操作，而根据其主动介入的程度，自动驾驶可以分为下列4个阶段。

第一阶段是驾驶员辅助系统，驾驶员辅助系统能通过为驾驶员采集关键信息，为危险的驾驶行为发出警告，相关技术有车道偏离警告、正面碰撞警告和盲点报警系统。目前这些技术已相当成熟并得到了广泛的应用，配备上述功能的车型价格已经下探至30万元以内。

第二阶段是半自动驾驶，当特定情况发生而驾驶员不能及时做出恰当措施时，半自动系统能让在汽车主动进行特定操作，例如紧急自动制动、紧急车道辅助。目前此类功能主要配

置在豪华车型上，但价格已经有了迅速下滑的趋势。

第三阶段是高度自动驾驶。该系统能在驾驶员监控的情况下，让汽车自主控制行驶，驾驶员可以随时夺回控制权。2015 年美国 CES 中的一辆经过改造的奥迪 A7 通过此技术行驶了 900km 由旧金山到达拉斯维加斯参展，并且速度可达 90km/h。但此技术目前仅出现在试验车型中，尚未量产。6 月 11 日特斯拉公告将会在月底公测可以进行自动驾驶的 mode S，但没有披露具体细节。

第四阶段：完全自动驾驶，这也是自动驾驶的终极阶段。在无需驾驶员操作的情况下，汽车可以完全自主行驶。Google 无人汽车便是定位于此，目前行驶距离已超过 30 万 mile[⊖]，但仅能实现特定场景下的低速行驶。

第一、二阶段已经实现，第三阶段接近商用，第四阶段也已呈现雏形。因此有理由相信，无人驾驶的汽车将会在未来的几年内得以商用。

实现无人驾驶的必要条件之一就是汽车能够通过遍布全车的各种传感器迅速采集到与之相关的车内、外的海量信息并高速处理。这些车辆信息被分析和处理后，可以根据计算主动的选择主动操作。

9.7.2　自动驾驶的应用场景

自动驾驶汽车的研究，可以归纳为 3 个方面：高速公路环境、城市环境和特殊环境下的无人驾驶系统。就具体研究内容而言，各个方面相互重叠，只是技术的侧重点不同。

1. 高速公路环境下的无人驾驶系统

这类系统将使用在环境限定为具有良好标志的结构化高速公路上，主要完成道路标志线跟踪和车辆识别等功能。这些研究把精力集中在简单结构化环境下的高速自动驾驶上，其目标是实现进入高速公路之后的全自动驾驶。尽管这样的应用定位有一定的局限性，但它的确解决了现代社会中最为常见、危险，也是最为枯燥的驾驶环节的驾驶任务。

2. 城市环境下的无人驾驶系统

与高速环境研究相比，城市环境下的无人驾驶由于速度较慢，因此更安全可靠，应用前景更好。短期内，可作为城市大容量公共交通（如地铁等）的一种补充，解决城市区域交通问题，例如大型活动场所、公园、校园、工业园、机场等。但是，城市环境也更为复杂，对感知和控制算法提出了更高的要求。城市环境中的无人自动驾驶将成为下一阶段研究重点。例如，美国国防部“大挑战”比赛 2007 年已采用城市环境。目前这类环境的应用已经进入到小范围推广阶段，但其大范围应用目前仍存在一定困难，例如可靠性问题、多车调度和协调问题、与其他交通参与者的交互问题、成本问题、商业模型等。

3. 特殊环境下的无人驾驶系统

无人驾驶汽车研究走在前列的国家，一直都很重视其在军事和其他一些特殊条件下的应用。但其关键技术和基于高速公路和城市环境的车辆是一致的，只是在性能要求上的侧重点不一样。例如，车辆的可靠性、对恶劣环境的适应性是在特殊环境下考虑的首要问题，也是在未来推广应用要重点解决的问题。

⊖ 1mile（英里）=1609.344m，后同。

9.7.3　Google 自动驾驶汽车原理

自动驾驶系统的核心是车顶上的激光测距仪，它能够提供精细的 3D 地图数据，自动驾驶汽车会把激光测到的数据和高分辨率的地图相结合，做出不同的数据模型，以便汽车能够识别障碍，遵守交通规则。

另外，在汽车的前后保险杠上有 4 个雷达，用于探测周边情况；后视镜的附近有一个摄像机，以检测交通灯情况；一个 GPS、一个惯性测试单元、一个车轮编码器，用来确定位置，跟踪其运动情况。

自动驾驶汽车依赖于非常精确的地图来确定位置，因为只是用 GPS 技术会出现偏差。在自动驾驶汽车上路之前，Google 的工程师会驾车收集路况数据，因此，自动驾驶汽车能够将实时的数据和记录的数据进行比较，这有助于它将行人和路旁的物体分辨开来。图 9-11 所示为 Google 自动驾驶汽车原理图。

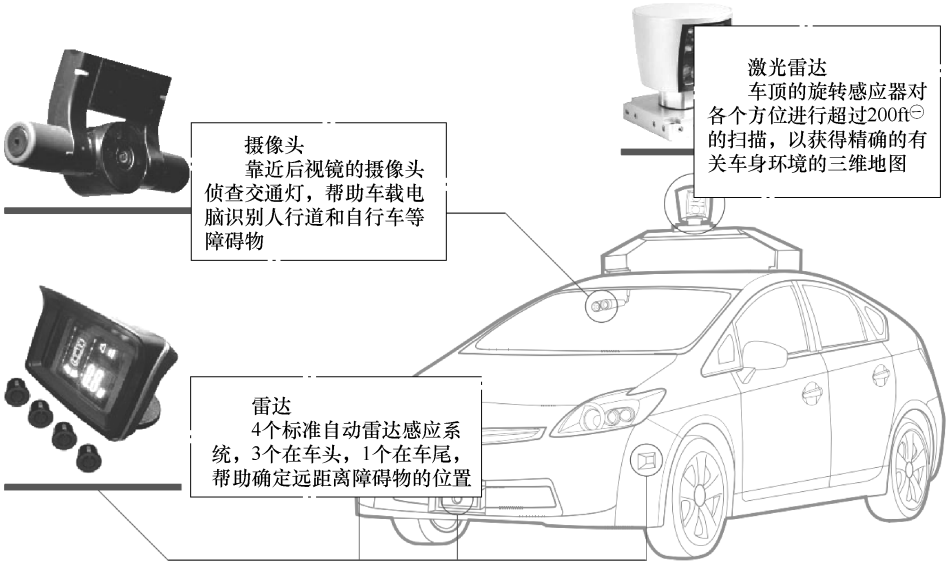


图 9-11　Google 自动驾驶汽车原理图

自动驾驶汽车也必须具有某种人工智能。比如在交通灯变绿色时，汽车开始拐弯，但这时有路人走过，它将会让路。另一个例子是，在十字路口，它会根据规则让其他车先过，如果其他车辆没有反应，它将往前行进一点，以表明自己的意图。

9.7.4　自动驾驶存在的问题

自动驾驶系统有两大关键技术，即车辆定位和车辆控制技术。车辆定位是汽车自动驾驶的基础，目前常用的技术包括磁导航和视觉导航等。其中，磁导航是目前最成熟可靠的方案，它的最大优点是不受天气等自然条件的限制。但是，磁导航需要在路面铺设一定数量的导航设备，系统实施过程比较复杂，且不易维护。视觉导航就不存在这个问题，视觉导航的

⊖ 1ft（英尺）=0.3048m，后同。

优点是车载主控计算机可以在试样车偏离目标车道前，事先知道并预防发生，同时当在高速公路行驶时，不需要对现有的道路结构做变化。其缺点是，当天气条件差，如风沙、大雾致使能见度过低或路上的交通标志不清晰时，视觉导航就会失效。但由于视觉导航对基础设施的要求较低，是最有前景的定位方法。解决视觉导航过程中存在的问题，首先需要精度极高的视觉导航仪，其次是增强交通标志被识别的功能。

车辆的控制技术是汽车自动驾驶的核心，主要包括车速控制和方向控制等几个部分。汽车自动驾驶系统的控制是一个典型的预瞄准控制行为，自动驾驶系统找到当前道路环境下的预瞄点，向油门和方向控制器发出动作指令。但在复杂的道路文通中，就存在一定的问题。比如说，在自动驾驶系统向油门和方向控制器发出动作指令后，汽车预瞄点的前方突然有行人横穿马路，对于这种突发事件，就需要自动驾驶系统有临时更改发出的动作指令的功能，重新设定行驶路线。汽车可以通过数学函数进行计算，算出汽车以何种速度行进不会撞上上述任何有着一定速度的事物。这需要设计极其准确的函数，还需要计算机反应极其敏捷，在几 μs 里就可以判断形势、纳入计算，并得出汽车速度、方向的结论。

9.8　物联网在医疗保健中的应用

9.8.1　医疗保健物联网应用概述

改革开放 20 年以来，我国在基础建设方面取得了重大飞跃，人均居住面积、交通运输条件以及通信传输网络等都得到了有效改善和显著提高。有权威机构的调查报告显示，参照国际社会的发展规律，伴随生活质量的不断提高，今后十年内，社会及公众的发展需求将由基础设施建设向更高层次的消费及服务转移，其中需求最为突出的几个方面当首推医疗条件、健康投入及教育水平等。

除却医疗技术及医疗体制的种种制约，落后的医用通信手段也大大制约了医院、医生和各种先进医用设备的作用时间和空间，大医院之拥挤、医疗资源之缺乏以及由此直接导致的医药费之昂贵等一系列就医难的问题已引起全社会的广泛关注。随着我国人口老龄化问题的日益严重，家庭医疗监护将成为普遍的社会需求。在患者和医院及医疗工作人员之间建立高速信息网络，是以改善医用通信条件为手段解决上述问题的有效可行的重要方法之一。

用传感技术和现代通信技术将病人的监护范围从医院内扩展到通信网络可以到达的任何地方，从而实现病人与诊所、诊所与医院或医院间医疗信息的传送。医生通过网络全程监护患者的病程（包括突发病变），并给予他们必要的指导和及时处理，而患者则通过网络在家里、公共场所或社区医院得到大医院的救治和指导。远程监护提供一种通过对被监护者生理参数进行连续监测研究远地对象生理功能的方法，缩短了医生和病人之间的距离，医生可以根据这些远地传来的生理信息为患者提供及时的医疗服务，远程监护系统不仅能提高老人的生活质量，而且能够及时捕捉老人的发病先兆，结合重要生理参数的远程监护，可以提高老年人的家庭护理水平。这对于患者获得高水平的医疗服务及在紧急情况时的急救支援，具有重要意义。

远程监护系统是顺应信息社会发展和人们对医疗保健的需求而产生和发展起来的。随着信息技术的不断发展，其形式将更加多样，无线、移动和传感技术融合而成的微型化无线智

能传感网络必将为远程监护系统的发展带来新的突破。无线医疗具有实时、移动、价廉、人性化和可推广等特点，拥有巨大的潜在市场需求，能够给科研开发、产业增长、企业发展带来巨大的空间。

9.8.2　医疗保健物联网应用方案

无线传感器网络技术、短距离通信技术（IEEE802.11a/b/g、ZigBee、Wi-Fi）、蜂窝移动通信网（GPRS/CDMA/3G）、互联网技术等先进通信技术的发展，为实现基于物联网的医疗保健应用方案提供了坚实的技术基础。物联网在医疗保健上的应用，将会带动医疗设备的微型化和网络化，同时促进医疗模式向预防为主的方向发展。

图9-12中描述了一种可扩展的多层次网络式远程医疗监护系统结构。系统由监护终端设备和无线专用传感器节点构成了一个微型监护网络。医疗传感器节点用来测量各种人体生理指标，如体温、血压、血糖、血氧、心电、脑电、脉搏等，传感器还可以对某些医疗设备的状况或者治疗过程情况进行动态监测。传感器节点将采集到的数据，通过无线通信方式将数据发送至监护终端设备，再由监护终端上的通信装置将数据传输至服务器终端设备上，如通过Internet可以将数据传输至远程医疗监护中心，由专业医护人员对数据进行观察，提供必要的咨询服务和医疗指导，实现远程医疗。

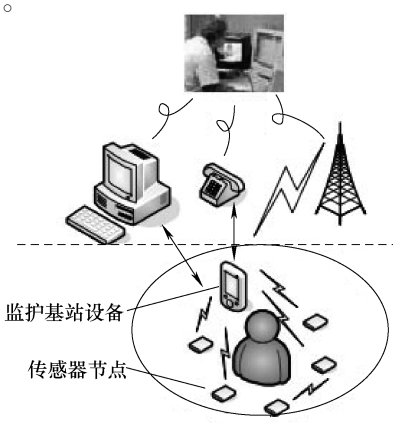


图9-12　通用医疗监护系统

一个完整的远程医疗监护物联网系统可以具体分为如下部分：

1）传感器部分，负责对病人生理参数（如心电图、心跳、呼吸、脉搏等）进行采集。

2）传输网络部分，传输数据的通道，包括数据在传感器和个人终端间的传输通道，个人终端和服务器间的传输通道。

3）远程医疗业务平台。

4）远程医疗业务提供方。

远程医疗监护物联网系统应该具有如下特点：

1）实时采集传输，实时采集病人的心电、呼吸、体温、心率等医用信息，传输和存储到数据库；

2）实时监控报警，实时数据自动分析和预警，为预防和治疗提供参考，紧急情况及时传递到远程医疗中心，并通知病人家属和主治医生，为突发事件赢得宝贵的抢救时间；

3）无线数据传输，提供可选的多种无线通信方式，为病人提供24h连续的生理信息的监护，患者可以自由移动；

4）实时诊断分析，医护人员可以实时调取病人医疗数据，结合电子病历，对病情做出分析和诊断，医生的指令可以发回到监护仪，指导治疗和救助；

5）紧急求助服务，病人主动请求定位最近的医护人员为患者提供及时的救助服务；

6）辅助医疗管理，提供辅助的医疗管理手段，记录病人请求、医护人员提供服务的相关工作记录。

根据不同应用场景的需求，可以对传感器节点进行不同设置并采用不同覆盖范围的网络

技术，逐级形成家庭社区医疗监护网络、医院监护网络，乃至整个城市和全国的医疗监护网络。

9.8.2.1　应用模式

医疗保健物联网应用方案主要可以根据应用场景和功能的不同划分为两种模式，分别是家庭社区远程医疗监护系统和医院临床无线医疗监护系统。

（1）家庭社区远程医疗监护系统

家庭社区远程医疗监护系统以前期预防为主要目的，对患有心血管等慢性疾病的病人在家庭、社区医院等环境中进行身体健康参数的实时监测，远程医生随时可对病人进行指导，发现异常时进行及时的医疗监护。这样一方面节省了大型专科医院稀缺的医疗资源，减少了庞大的医疗支出费用，同时又在保证个人生命安全的基础上，为病人就医提供了便利。

一个适用于家庭社区环境的典型远程医疗监护物联网系统如图 9-13 所示。系统分为以下几部分：

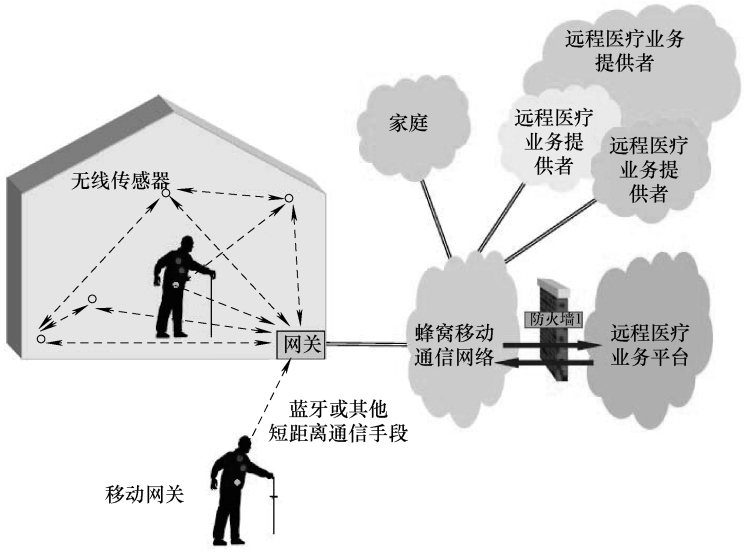


图 9-13　家庭远程医疗监护系统

1）用户便携终端，包括客户端，一般为 PC、便携电脑、PDA、甚至手机等，具有采集、存储、显示、传输、预处理、报警等功能，其中 PDA 和手机是目前最有发展潜力的个人终端。

2）服务器端为设于医院监护中心或家庭护理专家处的专业服务器，可提供详细的疾病诊断及分析，并提供专业医疗指导，反馈最佳医疗措施。

3）网络部分。

其中用户便携终端负责数据采集、本地监测、病人定位和数据发送，其工作方式可以是无线或有线，电源方式为有线或电池供电。服务器端由信息采集服务器、数据库服务器及监控管理终端等组成。信息采集服务器负责接收远程发来的心电数据和位置数据，实现对病人的远程监控，同时以 Web 服务的标准格式为医生提供一个历史数据检索、查看和诊断的平台。医生在医生工作站和医生终端上通过标准的浏览器即可实现对病人数据的实时访问。

其中网络部分通过移动网络与其他网络互联；移动网络在其中起到了枢纽和控制的功能；其中用户便携终端包含了常见的传感器，主要用于测量身体参数和室内外环境，除了人体参数外，还可以实现如体重、人体和环境温度等参数的测量，并自动通过无线网络技术，上传到终端，实现参数的实时监测。另外，家庭社区主要针对慢性疾病进行监护，个人监护设备不应对病人的日常生活进行限制，因此要求有很好的便携性。

家庭社区远程医疗监护系统通过现有的通信技术，在家庭环境中对人体和环境参数进行综合测量，从而实现护理和保健的统一。

（2）医院临床无线医疗监护系统

医院临床无线医疗监护系统在医院范围内利用各种传感器对病人的各项生理指标进行监护和监测。系统可以采用先进的传感器技术和无线通信技术，替代固定监护设备的复杂电缆连接，摆脱传统设备体积大、功耗大、不便于携带等缺陷，使得患者能够在不被限制移动的情况下接受监护，满足当今实时、连续、长时间检测病人生命参数的医疗监护需求。

在该应用模式下，系统仍旧可以沿用通用的远程医疗系统模型，利用无线数据传输的方式，传递医疗传感器与监护控制仪器之间的信息，减少监护设备与医疗传感器之间的联系，使得被监护人能够拥有较多的活动空间，获得准确的测量指标，满足病人的日常生活需要。同时，在医院病房内建立无线检测网络，很多项测试可以在病床上完成，极大地方便了病人就诊过程，并加强医院的信息化管理和工作效率。

系统需要同时支持床旁重患监护和移动病患监护。系统可分为：

1）生理数据采集终端，具有采集、存储、显示、传输、预处理、报警等功能，根据病人病情的需要，可分为固定型和移动型终端两种。

2）病房监护终端，作为病房内数据采集的中心控制和接入节点，收集病人的生理数据，支持本地监测，同时将数据发送至远程服务器终端。

3）远程服务器终端为设于医院监护中心的专业服务器，可提供详细的疾病诊断及分析，并提供专业医疗指导，反馈最佳医疗措施。

4）网络部分。

其中，生理数据采集终端和病房监护终端构成病房范围内的数据采集传输网络，可根据移动性的需求，采用无线或有线的方式进行连接，实现病房内多用户数据采集和病人定位，同时也方便医生和护士在病房内对病人的情况进行检查和监测。远程服务器由信息采集服务器、数据库服务器及监控管理终端等组成。信息采集服务器，负责接收远程发来的心电数据和位置数据，实现对病人的远程监控，同时以 Web 服务的标准格式为医生提供一个历史数据检索、查看和诊断的平台。医生在医生工作站和医生终端上通过标准的浏览器即可实现对病人数据的实时访问。

9.8.2.2　应用前景

由于无线监测系统技术的先进性以及应用模式的独特性，将给医疗服务带来巨大的变化，临床无线监护和个人远程监护将成为最先实现的应用模式。无线远程医疗系统的适用范围很广，包括远程急救、远程心脏病学、远程放射学、远程心理学、远程监护（包括偏远地区的医疗中心、家庭监护及远程或孤立点的个人监护）。监护的信号包括生物信号如 ECG、血压、温度、SpO_2、CO_2、医学图像或视频信号、电子病历（EPR）及音频信号等。

在医院临床无线监护应用模式中，系统可用于各种心律失常、缺血性心脏病、传导障

碍、各科病人的手术中监护和手术后观察等各项监测，提供实时无线的监测手段，为医疗安全提供新的保障，缓解 ICU 的资源紧张；系统也可用于危重症患者的长、短途转运过程中的监护。另外，对心律失常患者在院外观察药物疗效及病情监测也具有临床意义。

在个人远程监护应用模式中，系统可预防和减少某些病恶性事件发生，它对几类人群具有重要意义：一是对亚健康人群的心脏日常监护和保健护理具有积极作用，是日常工作繁忙、工作高度紧张、精神压力较大、缺少运动的各界人士（企业高层人士、高科技工作者、政府重要公职人员）自我监护的理想工具；二是有助于疾病患者的长期病情监测；三是随时及频繁就医有困难的患者和中老年患者；四是从事特殊行业并患有心律失常且伴有临床症状的人群。

当无线远程医疗系统发展成为一个成熟的医疗产品时，传统的医疗模式将被打破，一种全新的基于互联网的医疗监护体系将会形成——它以医院为核心，面向社区、家庭与个人，通过互联网联系组成一个有机整体，保证人们无论在医院内外甚至偏远地区均能得到及时、有效、专业的医疗诊断和治疗，从而大大提高医疗水平，使人们的生活质量越来越高。

9.8.2.3　主要参数指标

根据无线医疗保健系统的测量参数的种类以及要求，可以分为中等数据量和高数据量，如表 9-2 和表 9-3 所示。

表 9-2　中等数据量业务参数

参　　数	物联网节点	物联网汇聚节点
业务 burst 数据率/（bit/s）	若干	若干
每个业务 burst 数据量/bit	若干	若干
业务发生频率	s ~ m 量级不等	s ~ m 量级不等
延迟要求	s 量级	s 量级
节点密度	十位数量级	十位数量级

表 9-3　高数据量业务参数

参　　数	物联网节点	物联网汇聚节点
业务 burst 数据率/（bit/s）	若干	若干
每个业务 burst 数据量/bit	若干	若干
业务发生频率	s ~ m 量级不等	s ~ m 量级不等
延迟要求	s ~ m 量级	s ~ m 量级
节点密度	百位数量级	十位数量级

9.9　库存管理

库存管理作为企业生产、计划和控制的基础，为企业的生产管理和成本控制提供重要依据。基于云会计的物联网和大数据技术能为企业搜集、分析、处理前端数据，对企业科学、高效的库存管理提供支持。在分析大数据时代云会计对企业库存管理在管理成本、控制系统和管理水平等方面影响的基础上，结合大数据、云会计和物联网的技术特征，构建了一个包

括物联网、云会计平台、大数据分析中心、库存管理等核心组成模块的企业库存管理框架模型，详细阐述了入库、调拨、出库等库存管理环节的运作方式。

云会计因其成本低、效率高、易于拓展、可定制性强等优势受到了中小企业的广泛关注。基于企业的云会计平台，通过物联网可实现物品的实时智能化识别、定位、跟踪、监控和管理，为企业进行大数据决策积累海量数据。库存管理是企业物料管理的核心，需要及时准确地反映各种物料的仓储、流向情况。云会计、物联网等技术的发展确保了企业获取货物的实时信息，而大数据分析中心则为企业做出科学合理的库存管理决策提供了技术支持。

综观现有研究发现，物联网、云计算核心技术在库存管理方面的研究已经逐步展开，但同时涉及大数据、物联网、云会计的库存管理研究文献相对还比较匮乏。实际上，大数据、云会计、物联网技术在企业物料数据的搜集、分析、处理及其同行业与相关行业的数据检索方面有着很大的优势。本节在分析大数据时代云会计对企业库存管理影响的基础上，融合大数据、云会计和物联网技术于企业的库存管理应用，构建了大数据时代基于云会计的企业库存管理框架模型，并详细阐述了库存管理入库、调拨和出库环节的具体运作方式。

9.9.1　大数据时代云会计对库存管理的影响

在大数据时代，云会计可以满足企业尤其是中小企业对于会计信息化低成本、高效率、操作简单、信息方便获取的需求，这必然会对企业库存管理的管理成本、存货控制及管理水平产生较大的影响。

1. 云会计使库存管理的成本更低廉

库存管理的目标之一是在保证生产或销售经营需要的前提下最大限度地降低库存成本，即对库存合理布局，减少调拨次数。存货不足不能及时满足生产和销售的需要会给企业带来损失，而存货过多将导致存储成本增加，进而影响企业利益。如何对库存管理的成本进行控制对企业的生产经营至关重要。以物联网技术为前端、大数据分析中心为后端的云会计平台，能够在时空分离的环境下预测或获取企业不同区域的仓储信息和客户订货信息，以减少企业的库存管理成本。基于云会计平台，企业能够搜集、分析货物的实时信息，动态了解各仓库的实时库存情况。仓储管理部门在获得大数据分析中心提供的库存数据与客户偏好数据的基础上，能够做到对各仓库库存合理布局，减少调拨次数，节约库存管理成本。

2. 云会计使存货控制系统更精确

为提高企业整体运作效率，很多企业对存货管理采用了 ABC 控制系统或即时制（Just In Tine，JIT）库存控制系统。在 ABC 控制系统中，如何准确区分 ABC 三类存货并进行分类控制是企业需要解决的重要问题。JIT 管理强调只在使用存货之前才要求供应商送货，从而将存货数量减到最小，实现物资供应、生产、销售连续同步运动。这种方式在提高生产效率、减少存储成本的同时需要考虑到与供应商协同接洽的问题。大数据、云会计技术的应用，能够提高企业 ABC 控制系统或即时制控制系统的运行效果。

在企业的云会计平台上，通过对自身以往所有各种类型存货数据的大数据分析，以及参考同行业、相关行业的历史数据，可以对 ABC 三类存货进行更为科学合理的区分，使 ABC 控制系统更加精确。面对即时制更加严格的要求，企业需要考虑到存货的计划需求、与供应商关系、准备成本和电子数据等方面，一旦存货预警就会产生生产线、销售线告急的情况，将为企业带来巨大损失。物联网与大数据技术的发展为解决 JIT 控制面临的问题提供了解决

方案。由供应商提供的存货都带有唯一的产品电子代码，企业和供应商可以通过物联网同时获得存货的使用情况，在数据显示该批存货需要补充时，物联网得到传感信息的反馈及时提醒企业补给，通知供应商做好供货准备，并给出下一订货批量的预计时间及数量要求。这样就加强了企业与供应商的信息沟通与交流，使 JIT 控制系统得到更好的实施。

3. 云会计使库存管理更智能

由于各个地区消费者的需求偏好往往存在差异，使得企业在全国布局的仓库库存往往在商品的类型、数量等方面不尽相同。基于云会计平台，通过前端的物联网，企业可以获取各个区域仓库的存货情况。针对库存调拨，通过后端的数据中心进行大数据分析，可以选择在最优的仓库之间进行商品的调配，并根据对调拨结果的分析就以后的商品库存分配进行优化。消费者在网上购买商品时，云会计平台会自动选择就近且有货的库存点进行智能化发货。在存货的运输与存储过程中会涉及安全问题，尤其是对于高价值的存货，其一旦损失将会对企业造成严重影响。云会计平台下物联网技术的运用，可以做到存货信息流和物流的统一、对存货流向形成监控，具有极强的监测功能。存货信息能够实时反映在云会计平台上，即便出现货物丢失情况，企业也能够即时采取措施应对，确保企业存货的安全性。

9.9.2　大数据时代基于云会计的库存管理框架模型构建

库存管理及时准确地反映各种物资的仓储和流向情况，可以为企业的生产管理和成本控制提供依据。通过对货物的各种信息进行即时的采集、分析和处理，可以使企业实时动态的库存管理成为现实。在云会计平台上，前端的物联网技术能够实时采集数据，后端的大数据分析中心对数据进行分析与处理，为企业的库存管理决策提供支持。在分析大数据时代云会计对企业库存管理在成本、控制、管理水平等方面影响的基础上，结合大数据、云会计和物联网的技术特征，考虑企业当前主要的库存管理需求，本文建立了由云会计平台、大数据分析中心、库存管理等核心模块组成的大数据时代基于云会计的企业库存管理框架模型，如图 9-14所示。

在图 9-14 中，企业库存管理决策所需的库房信息，如仓库信息、货位信息、物料信息和出入库信息等，可以通过物联网技术借助云会计平台进行实时搜集；决策所需的其他大数据源，可以通过互联网、移动互联网、社会化网络等多种媒介，借助云会计平台从企业内部、交易所、事务所、外部市场、银行等获取。同时，经由大数据处理技术和方法（Hadoop、Storm、Pentaho BI 等）规范所获取数据，并通过 ODS、DW/DM、OLAP 等数据挖掘与数据分析技术提取企业进行库存管理决策所需的财务与非财务数据。大数据分析中心对企业库存管理的入库信息、调拨信息、出库信息进行分析，以此来支撑库存管理模块，为采购入库、库房调拨、销售出库阶段实时、准确的决策提供了依据。

1. 采购入库

在采购入库阶段，由大数据分析中心结合企业生产情况、外部环境等因素对采购计划、采购数量、采购时间、物流过程等相关采购流程的影响，就公司所接订单、产品或服务的生产周期以及交货的时间等进行分析，并针对企业历史数据的分析以及对供应商信用程度、产品质量、产品价格等的综合分析，制定出合格供应商名册向企业推荐最优供应商。采购部门则根据分析结果按照企业需求制定出科学的采购计划与选择适合并满意的供应商。完成供应商选择之后要进行签订采购合同、发出订购单，供应商确认订购单、根据订单交货等步骤，

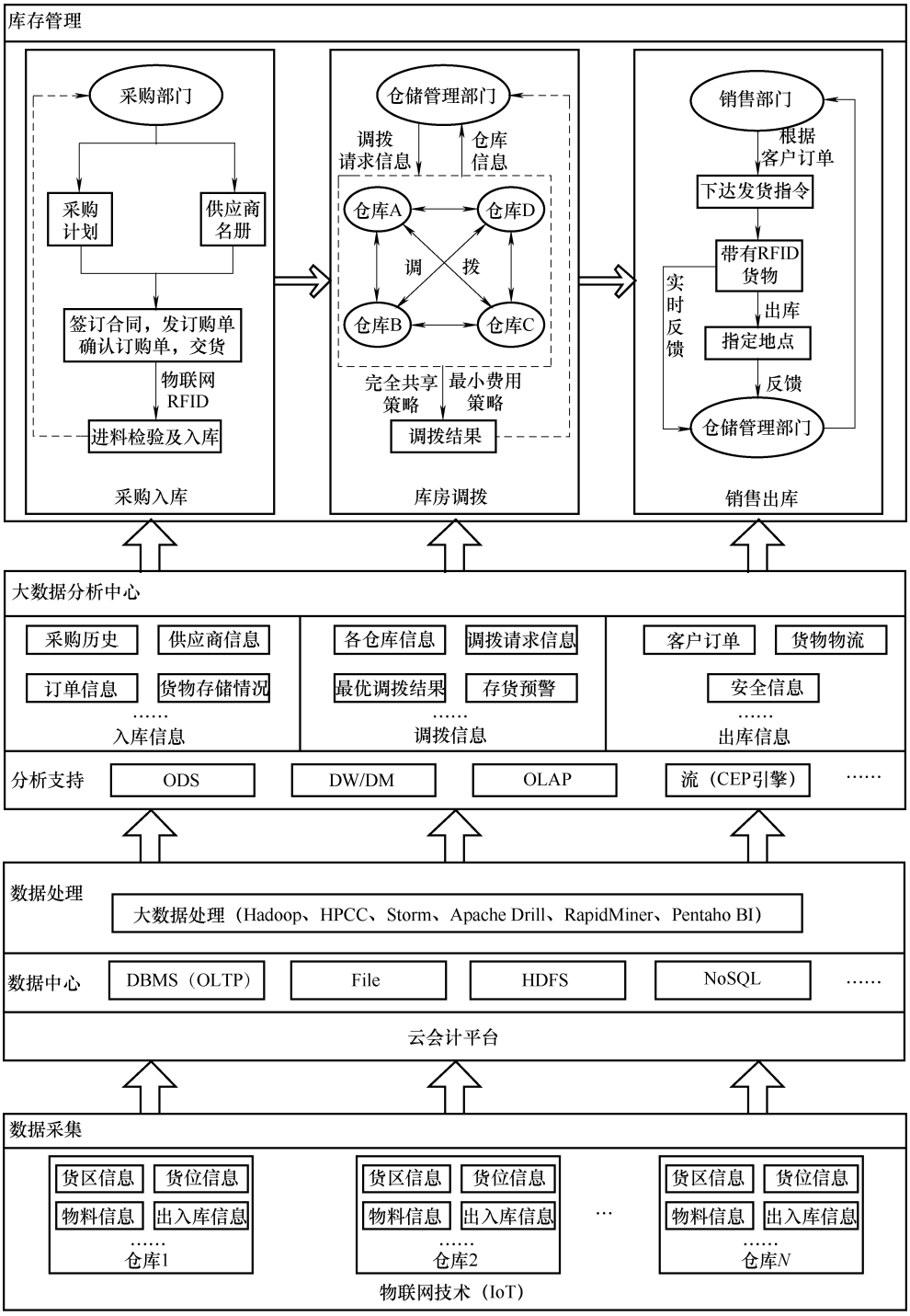


图 9-14　大数据时代基于云会计的库存管理框架模型

这一过程需注意明确合同内容，明晰产品信息与双方责任。在最后一个部分即进料检验及入库阶段，由射频识别技术（RFID）识别出产品的品牌、规格、型号以及供应商的检验合格标识（在物联网技术下，产品都带有唯一电子标签）之后方可入库，若有检验不合格者，根据标签自带的生产信息退回至供应商处，并根据采购合同的条款或退换货物或进行赔付，退换后的货物同样要进行这一系列的检验过程，直到合格后入库。

2. 库房调拨

在库房调拨阶段，模型采用完全共享策略，即某仓库库存水平一旦无法满足当前订单，而采用调拨方式可满足时，可从其他点调拨，要求调拨点的当前库存能满足需求点的订单需求量。由于云会计前端的物联网可以得到企业各仓库的库存信息，这样在任何仓库发生存货预警时，都可以向后端的大数据分析中心实时反馈请求调拨信息。对请求调拨信息进行分析之后，按照最小费用策略确定存货的调拨点与调拨量，并向该仓库发布调拨信息，以此在各仓库间完成存货的相互补给。在各仓库不能满足库存需要或者调拨成本过高时，库存信息将直接向总部反馈，由总部完成存货的分配。最后将调拨结果经由大数据分析中心向仓储管理部门进行汇报。

基于云会计的库存调拨模块将企业的分布式库存连成了一个有机整体，不再是单独的仓库管理，可满足大中型企业库存实时性的问题，便于整体优化及一体化管理。大数据分析中心为各仓库的信息共享提供了技术支撑，物联网技术的运用为掌握各仓库的实时信息提供了有力保障，可为企业节省时间与成本。

3. 销售出库

针对企业的销售出库，销售部门根据经由大数据分析中心分析之后的客户订单向指定的仓库下达发货指令，当指定仓库接收到发货指令之后，带有 RFID 的货物将被发往指定地点，同时，货物的地理位置信息与其他信息等由带 RFID 技术的物联网通过大数据分析中心向仓储管理部门实时反馈，以确保货物的安全以及了解物流信息。在货物到达指定地点后，将会再次向大数据分析中心反馈信息，并向仓储管理部门与销售部门发送货物安全送达的信息，从而完成整个出库过程。

大数据已成为企业新型的战略资产和企业核心竞争力的重要基础，可为企业的经营决策提供重要的支持。大数据、云会计和物联网技术能为企业搜集、分析、处理前端数据，并获取到同行业与相关行业的数据信息，这必然会对企业传统的库存管理方式产生较大的影响。

参 考 文 献

[1] 中国通信标准化协会. 移动 M2M 业务研究报告. 2009. 8.
[2] 张丹，李业德. 浅谈物联网的应用 [J]. 科技信息，2010（35）：88.
[3] 李野，王晶波，董利波，等. 物联网在智能交通中的应用研究 [J]. 移动通信，2010（15）：30-34.
[4] 钱彬，莫日宏. 物联网技术在智能电网中的应用 [J]. 新材料产业，2010（12）：51-53.
[5] 姬珠珠. 车联网：城市交通的智慧之光 [J]. 交通世界，2010（18）：34-39.

地址：北京市百万庄大街22号
邮政编码：100037

电话服务
服务咨询热线：010-88361066
读者购书热线：010-68326294
010-88379203
网络服务
机工官网：www.cmpbook.com
机工官博：weibo.com/cmp1952
金书网：www.golden-book.com
教育服务网：www.cmpedu.com


机械工业出版社微信公众号


E视界
传播电类内容提升专业知识


科技电眼
关注电类行业动向 聚焦前沿科技

上架指导 工业技术／通信工程／物联网
ISBN 978-7-111-55124-9
策划编辑◎朱林

定价：49.00元