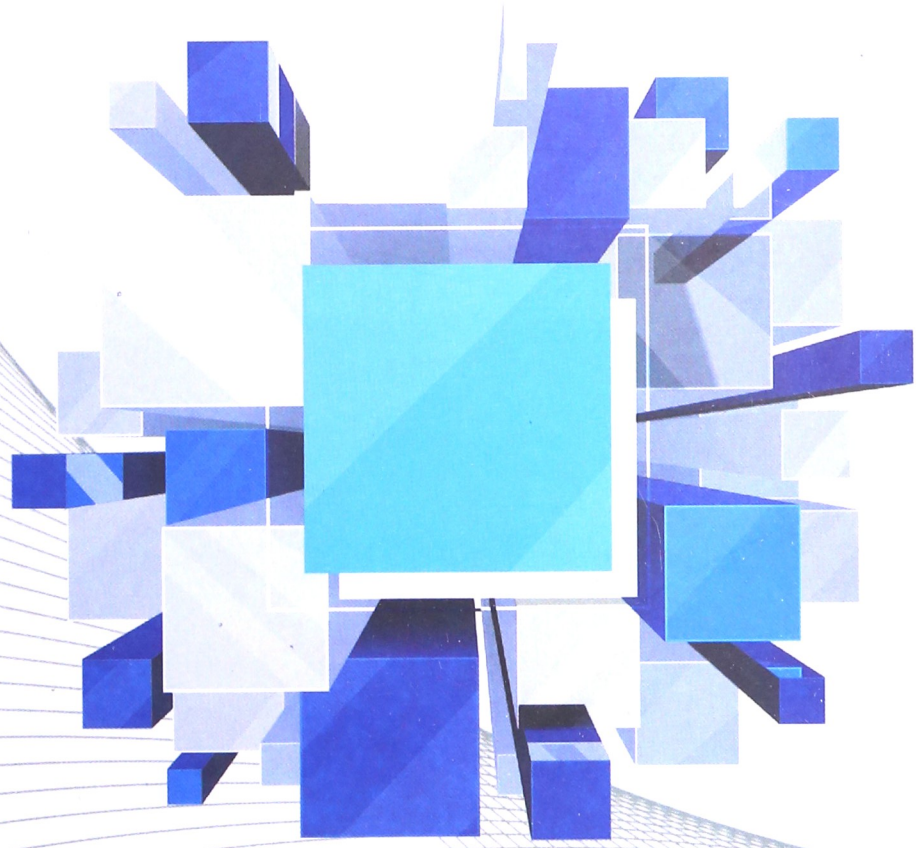
中国电子学会物联网专家委员会推荐

普通高等教育物联网工程专业“十二五”规划教材

物联网信息安全

Information Security in the Internet of Things

于旭 梅文 编著



西安电子科技大学出版社
http://www.xduph.com

中国电子学会物联网专家委员会推荐

普通高等教育物联网工程专业“十二五”规划教材

物联网信息安全

于 旭 梅 文 编著

西安电子科技大学出版社

内 容 简 介

本书较为全面地讲述了物联网信息安全的基本知识、技术体系以及相关理论。全书共分 8 章。第 1 章重点介绍了物联网的基本概念以及物联网中所存在的安全问题。第 2 章对与物联网信息安全领域联系较紧密的数学知识进行了讲解。第 3 章从终端节点、感知网络、通信网络、应用和控制管理等不同层面指出了物联网各部分的安全问题。第 4 章对物联网身份认证、访问控制和安全审计进行了详细的描述。第 5 章重点给出了数字签名的概念和几种典型的数字签名方案，并对数字证书技术进行了简要的介绍。第 6 章针对物联网的路由安全问题进行了介绍，重点分析了无线传感器网络和 Ad hoc 网络中的路由安全问题。第 7 章对容侵容错技术、网络入侵检测技术以及虚拟专用网技术进行了介绍。第 8 章对物联网中的数据安全和隐私保护技术进行了全面的介绍。

本书可作为高等学校物联网工程专业及其他相关专业高年级本科生及研究生的教材，还可作为企业管理者、科研人员、高等院校教师等了解物联网安全知识的参考用书。

图书在版编目(CIP)数据

物联网信息安全/于旭，梅文编著. —西安：西安电子科技大学出版社，2014.1
普通高等教育物联网工程专业“十二五”规划教材
ISBN 978-7-5606-3286-5

Ⅰ. ① 物… Ⅱ. ① 于… ② 梅… Ⅲ. ① 互联网络—信息安全—高等学校—教材
Ⅳ. ① TP393.4

中国版本图书馆 CIP 数据核字(2014)第 009826 号

策　　划　毛红兵
责任编辑　毛红兵　郑瑞涛
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西天意印务有限责任公司
版　　次　2014 年 1 月第 1 版　2014 年 1 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　12
字　　数　275 千字
印　　数　1～3000 册
定　　价　21.00 元
ISBN 978-7-5606-3286-5/TP
XDUP　3578001-1

前　言

互联网信息安全是一个关系国家安全和主权、社会稳定、民族文化继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快变得越来越突出。网络信息安全是涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，它主要研究如何使网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

近些年，随着物联网概念的普及，物联网在人们的生产、生活中起着越来越重要的作用。2009 年 8 月温家宝总理提出“感知中国”，物联网被正式列为国家五大新兴战略性产业之一，写入“政府工作报告”。物联网在中国受到了全社会极大的关注，其受关注程度是其他国家无法比拟的。物联网的信息安全也越来越引起人们的关注，成为研究的热点内容。由于物联网包含了很多传统互联网所没有的内容，其信息安全问题也更为复杂。

本书针对物联网信息安全进行了较为系统的介绍，主要内容包括物联网身份认证、访问控制、安全审计技术、数字签名、数字证书、物联网安全路由协议、网络入侵检测、网络入侵防御、容侵容错技术、虚拟专用网技术、数据安全和隐私保护等。

全书共分 8 章，其中第 1、3 章由梅文编写，第 2、4、5、6、7、8 章由于旭编写。

在本书付梓之际，特别要感谢青岛科技大学物联网信息工程教研室主任——曾宪武副教授，他对本书提出了很多建设性的意见和建议。另外，本书在编写过程中还得到了李峻羽先生的支持，在此向他表示感谢。此外，还要感谢青岛科技大学信息科学技术学院的领导对本书出版所给予的全力支持。

由于物联网信息安全是一个全新的领域，近些年发展很快，文中疏漏和不当之处在所难免，敬请读者指正。

作　者

2013 年 7 月于青岛

目　录

第1章

概 要

1.1 引 言

1.1.1 物联网及物联网安全系统的定义

1. 物联网的定义

物联网(Internet of Things，IOT)，顾名思义，就是将所有物体连接在一起的网络。物体通过二维码、射频识别(Radio Frequency Identification，RFID)、传感器等信息感知设备与网络连接起来，进行信息交换和通信，实现智能化识别、定位、跟踪、监控和管理。在物联网时代，现实的“万物”与虚拟的“网络”将融合为“物联网”，现实的任何物体(包括人)在网络中都有与之对应的“标志”，最终的物联网就是虚拟的、数字化的现实物理空间。

更详细的物联网定义如下。

1) 中国定义

物联网是一个基于互联网、传统电信网等信息载体，让所有能够被独立寻址的普通物理对象实现互联、互通的网络，它具有普通对象设备化、自治终端互联化和普适服务智能化三个重要特征。

物联网指的是将无处不在(Ubiquitous)的末端设备(Devices)和设施(Facilities)，包括具备“内在智能”的传感器、移动终端、工业系统、楼控系统、家庭智能设施、视频监控系统等和“外在使能”(Enabled)的，如贴上 RFID 标签的各种资产(Assets)、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”(Mote)，通过各种无线或有线、长距离或短距离的通信网络实现互联、互通(Machine to Machine，M2M，机器对机器)、应用大集成(Grand Integration)，以及基于云计算的 SaaS(Software as a Service，软件即服务)营运等模式，提供安全可控乃至个性化的实时在线监测、定位追溯、报警联动、调度指挥、预案管理、远程控制、安全防范、远程维保、在线升级、统计报表、决策支持、领导桌面(集中展示的 Cockpit Dashboard)等管理和服务功能，实现对“万物”的“高效、节能、安全、环保”的“管、控、营”一体化。

2) 欧盟定义

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一道，构成未来互联网。

2．物联网安全的概念

物联网作为最近几年提出的一个新的概念，预示了互联网技术发展的新方向，即虚拟网络与现实世界的结合。但物联网不是对现有技术的颠覆性革命，而是对现有技术的聚合应用。物联网的核心和基础是网络，是在现有网络基础上延伸和扩展的，因此物联网也同传统互联网技术一样面对安全问题。同时，物联网还存在着一些与已有互联网安全不同的特殊安全问题：物联网中的“物”的信息量比“互联网”时代大很多；物联网的感知设备计算能力、通信能力、存储能力及能量等都受限，不能应用传统互联网的复杂安全技术；现实世界的“物”都连网，通过网络可感知及控制交通、能源、家居等，与人们的日常生活密切相关，安全呈现大众化、平民化的特征，安全事故的危害和影响巨大；物联网安全与成本的矛盾十分突出。

我国是对物联网研究较早的国家之一，物联网的初步应用也正在进入产业化进程。可以肯定物联网的发展是下一代互联网技术发展的必然产物，物联网的出现可能会在很大程度上改变现代社会的运行方式，极大地方便人们的生活，同时将会在新的社会运行体制中产生新的社会问题。互联网发展的初始阶段并未将信息系统安全作为重点考虑，从系统构架上来看缺少了非常重要的一部分，尽管现在信息安全技术在网络架构各个层次上均有进展，但由于系统设计之初的缺陷，补救措施仍然难以满足信息系统安全的现实需求。物联网现在尚处于定义模糊、方向不明确的初始阶段，如果在建设物联网伊始，我们没有将信息系统安全作为系统的重要组成部分去发展研究，那么后果将不堪设想。在互联网时代，信息安全带来的危害发生在虚拟世界，结束于虚拟世界，最大的危害是社会经济的损失；然而在物联网时代，由于虚拟世界与现实世界的结合，信息安全造成的危害将直接威胁到我们生存的现实环境。因此物联网的安全体系建设，应与物联网技术的发展同步，以政府为主导，制定系统、规范的体系结构，建立合理的安全机制，在保证物联网信息安全的基础上，稳步发展物联网技术，避免重蹈互联网发展的覆辙，尽量避免新技术带来对社会的不利冲击。信息安全等级保护工作是公安部对互联网时代信息安全体系建设做出的一个重要贡献，随着物联网技术革新的到来，如何将信息安全等级保护合理科学地移植到物联网体系结构中，必将成为一个重要的研究课题，同时也是物联网发展的先决条件。

在互联网中，先系统后安全的思路使安全问题层出不穷，因而物联网在应用之初，就必须同时考虑应用和安全，将两者从一开始就紧密结合，系统地考虑感知、网络和应用的安全；物联网时代的安全与信息将不再是分离的，物联网安全不再是“打补丁”，而是要给用户提供“安全的信息”。

3. 物联网信息安全的特点

(1) 安全威胁由网络世界延伸到物质世界。物联网可以将洗衣机、电视、碎纸机、电灯、微波炉等家用电器连接成网络，并能通过网络进行远程操作，但威胁也随之而来。未来的信息安全威胁将不仅仅停留在网络安全的范畴，而是走进我们的生活，形成对物理空间的安全威胁。例如，黑客可以通过物联网对电冰箱发起攻击，使其超频工作，导致毁机。因此，物联网极大地加大了我们应对互联网安全防范的范围和治理的难度。

(2) 安全威胁由网络扩展到众多节点。许多大型项目的传感节点都具有暴露性或被定位性，为外来入侵者提供了场所和机会。物联网感知层嵌入了 RFID 芯片，不仅能方便物品的主人所感知，同时其他人也能跟踪或截获其感知信息，特别是当成千上万条被感知的信息同时通过无线网络进行传输时，节点的安全性相当低，要让其得到强大而有效的安全保护是很困难的。

(3) 安全威胁由物联网自身放大到云计算服务体系。随着大规模传感器和电子标签的应用，势必面临传感器节点测量或感知到的海量数据如何处理的问题，云计算技术当仁不让地成为物联网发展的技术支撑和服务支撑。但云计算将核心的计算部分放置到一个中央服务器的集群中，这些集群受控于一个组织或某个网络巨头之门下，若这个集群出了故障，将对所有连接的客户造成损害。

任何一个新的信息系统出现都会伴生着信息安全问题，物联网也不可避免。物联网安全问题重点表现在如果物联网出现了被攻击、数据被篡改等问题，并致使其出现了与所期望的功能不一致的情况，或者不再发挥其应有的功能，那么依赖于物联网的控制结果将会出现灾难性的问题，如工厂停产或出现错误的操控结果。

1.1.2 物联网系统安全研究的重要性

物联网产业蒸蒸日上，然而在繁荣的景象背后，其安全危机正日渐显现。因为网络本身是存在安全隐患的，分布随机的传感信息网络、无处不在的无线网络更是为各种网络攻击提供了广阔的“土壤”。物联网面临的安全隐患比互联网更加严峻，而且物联网的普及越广，不安全的后果越严重，如果处理不好，整个国家的经济和安全都将面临威胁。

物联网将经济社会活动、战略性基础设施资源和人们的生活全面地架构在全球互联、互通的网络上，所有的活动和设施理论上透明化，一旦遭受攻击，其安全和隐私将面临巨大的威胁，甚至可能引发电网瘫痪、交通失控、工厂停产等恶性后果。因此实现信息安全和网络安全是物联网大规模应用的必要条件，也是物联网应用系统成熟的重要标志。

随着物联网建设的加快，物联网的安全问题必然成为制约其全面发展的重要因素。在物联网发展的高级阶段，由于其场景中的实体均具有一定的感知、计算和执行能力，广泛存在的这些感知设备将会对国家基础、社会和个人信息安全构成新的威胁：一方面，由于物联网具有网络技术种类上兼容和业务范围上无限扩展的特点，因此当大到国家电网数据小到个人病例情况都接到看似无边界的物联网时，将可能导致更多的公众个人信息在任何时候、任何地方被非法获取；另一方面，随着国家重要的基础行业和社会关键服务领域(如电力、医疗等)都依赖于物联网和感知业务，国家基础领域的动态信息将可能被窃取。所有的这些问题使得物联网安全上升到国家层面，成为影响国家发展和社会稳定的重要因素。

物联网相较于传统网络，其感知节点大都部署在无人监控的环境，具有能力脆弱、资

源受限等特点，并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台，传统网络的安全措施不足以提供可靠的安全保障，因此物联网的安全问题具有特殊性。所以在解决物联网的安全问题时，必须根据物联网本身的特点设计相关的安全机制。

物联网的安全问题和互联网的安全问题一样，永远都会是一个被广泛关注的话题。由于物联网连接和处理的对象主要是机器或物的相关数据，其“所有权”特性导致物联网的信息安全要求比以处理“文本”为主的互联网更高，对“隐私权”保护的要求也更高。此外还有可信度问题，包括防伪和防 DoS(Denial of Services，拒绝服务)攻击，因此要特别关注物联网的安全问题。

从物联网未来的发展来看，当全世界互联成一个超级系统时，系统的安全将直接关系到国家的安全，我们需要高度重视，面对挑战制定对策。物联网系统的安全和一般 IT 系统的安全基本一样，主要有八个尺度：读取控制、隐私保护、用户认证、不可抵赖性、数据保密性、通信层安全性、数据完整性、随时可用性，前四项主要处在物联网 DCM 三层架构的应用层，后四项主要位于传输层和感知层，其中“隐私权”和“可信度”(数据完整性和保密性)问题在物联网体系中尤其受关注。如果从物联网系统体系架构的各个层面仔细分析，我们会发现现有的安全体系基本上可以满足物联网应用的需求，尤其在物联网的初级和中级发展阶段。

物联网应用特有(比一般 IT 系统更易受侵扰)的安全问题有如下几种：

(1) Skimming(掠过)：在末端设备或 RFID 持卡人不知情的情况下，信息被读取。

(2) Eavesdropping(偷听)：在一个通道的中间，信息被截取。

(3) Spoofing(欺骗)：伪造、复制设备数据，冒名输入到系统中。

(4) Cloning(克隆)：克隆末端设备，冒名顶替。

(5) Killing(杀掉)：损坏或盗走末端设备。

(6) Jamming(干扰)：伪造数据，造成设备阻塞不可用。

(7) Shielding(屏蔽)：用机械手段屏蔽电信号，让末端无法连接。

针对上述问题，物联网发展的中、高级阶段将面临如下五大特有(在一般 IT 安全问题之上)的信息安全挑战：

(1) 四大类(有线长、短距离和无线长、短距离)网络相互连接组成的异构、多级、分布式网络导致统一的安全体系难以实现“桥接”和过渡。

(2) 设备大小不一、存储和处理能力的不一致导致安全信息，如 PKI(Public Key Infrastructure，公钥基础设施)、Credentials 等的传递和处理难以统一。

(3) 设备可能无人值守、丢失、处于运动状态、连接时断时续、可信度差，种种这些因素增加了信息安全系统设计和实施的复杂度。

(4) 在保证一个智能物件能被数量庞大甚至未知的其他设备识别和接受的同时，又要保证其信息传递的安全性和隐私性。

(5) 用户单一服务器 SaaS 模式对安全框架的设计提出了更高的要求。对于上述问题的研究和产品开发，目前国内外都还处于起步阶段，在 WSN(Wireless Sensor Network，无线传感器网络)和 RFID 领域有一些针对性的研发工作，统一标准的物联网安全体系的问题目前还没提上议事日程，比物联网统一数据标准的问题更滞后。

1.2 物联网的结构

1.2.1 物联网的基础结构

物联网理论上分为三层，从上往下依次为：应用层，各种应用程序；网络层，通过网络进行数据传输，如 Internet；感知层，信息采集设备及物理链路层，如 RFID、ZigBee(一种低速短距离传输的无线网络协定)等。图 1-1 是物联网的基础结构示意图，图 1-2 是物联网各层的关系图。

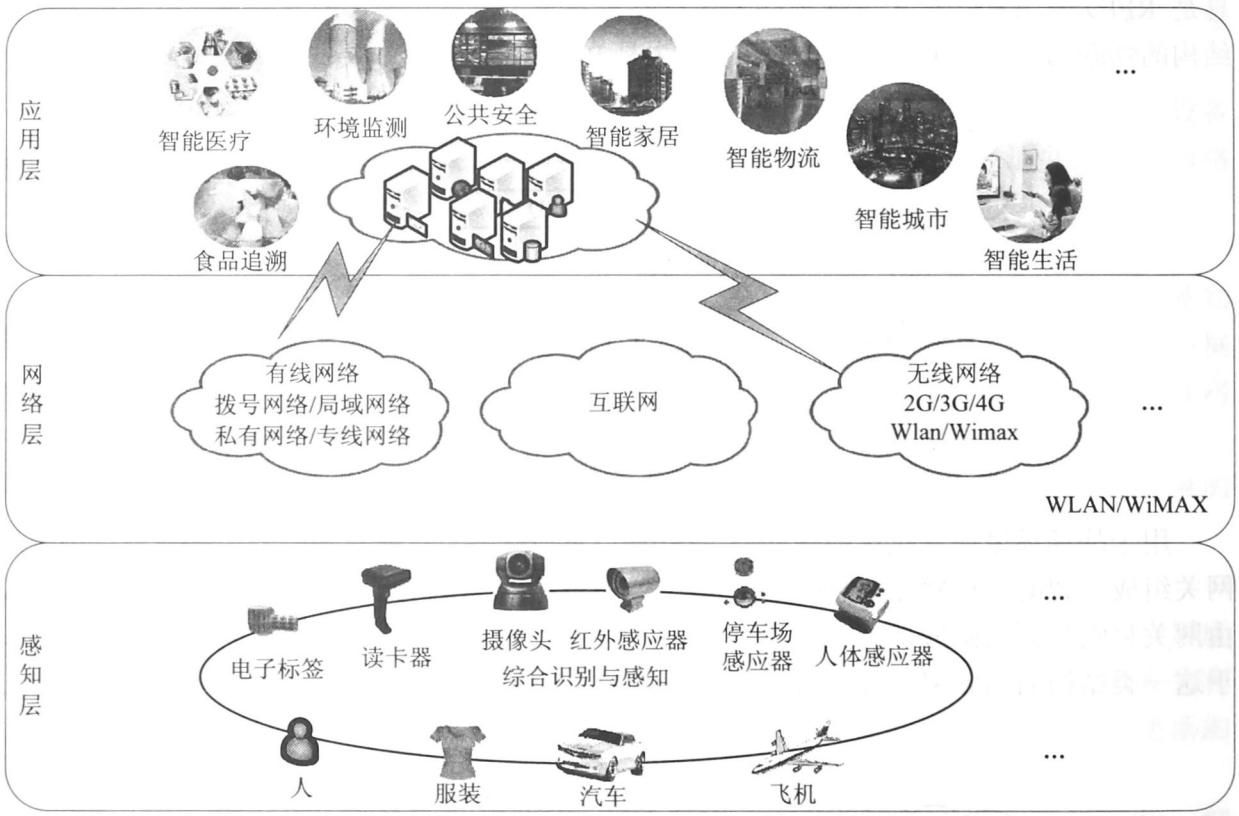


图 1-1 物联网的基础结构示意图

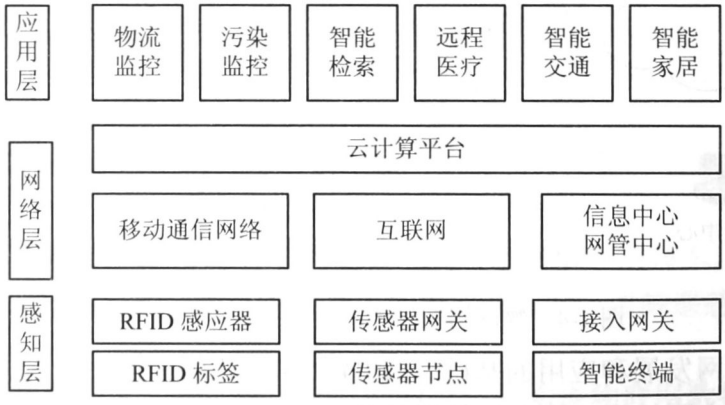


图 1-2 物联网各层的关系图

1．感知层

感知层包括传感器等数据采集设备，是数据接入到网关之前的传感器网络。感知层由数据采集子层、短距离通信技术和协同信息处理子层组成。数据采集子层通过各种类型的传感器获取物理世界中发生的物理事件和数据信息，如各种物理量、标识、音频和视频多媒体数据等。物联网的数据采集涉及传感器、RFID、多媒体信息采集、二维码和实时定位等技术。短距离通信技术和协同信息处理子层将采集到的数据在局部范围内进行协同处理，以提高信息的精度，降低信息冗余度，并通过具有自组织能力的短距离传感网接入广域承载网络。

对于目前关注和应用较多的 RFID 网络来说，张贴或安装在设备上的 RFID 标签和用来识别 RFID 信息的扫描仪、感应器属于物联网的感知层。在这一类物联网中被检测的信息是 RFID 标签的内容，高速公路不停车收费系统、超市仓储管理系统等都是基于这一类结构的物联网，称为 RFID 感应式。图 1-3 是 RFID 感应式感知层的简单结构。

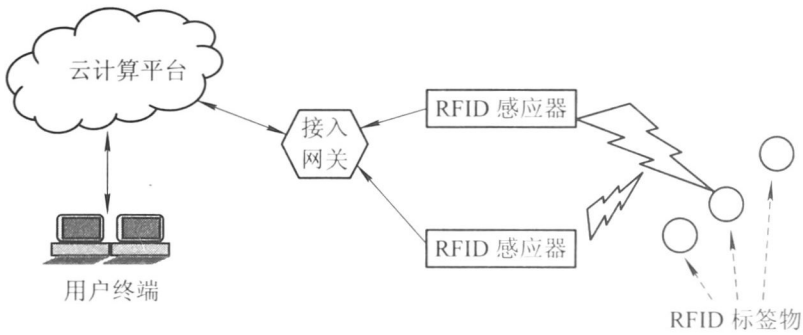


图 1-3　物联网感知层的结构——RFID 感应式

用于战场环境信息收集的智能微尘(Smart Dust)网络，其感知层由智能传感节点和接入网关组成。智能节点感知信息(温度、湿度、图像等)，并自行组网传递到上层网关接入点，由网关将收集到的感应信息通过网络层提交到后台处理。环境监控、污染监控等应用是基于这一类结构的物联网，称为自组多跳式。图 1-4 是自组多跳式感知层的一个例子。

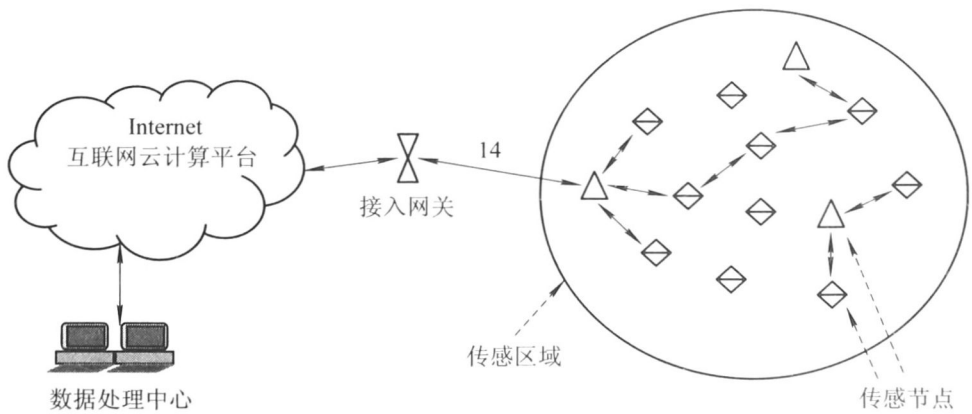


图 1-4　物联网感知层的结构——自组多跳式

感知层是物联网发展和应用的基础，RFID 技术、传感和控制技术、短距离无线通信技术是感知层涉及的主要技术，其中又包括芯片研发、通信协议研究、RFID 材料、智能节点

供电等细分技术。通信协议的研究机构主要有伯克利大学等，西安优势微电子的“唐芯一号”是国内自主研发的首片短距离物联网通信芯片，Perpetuum 公司针对无线节点的自主供电已经研发出通过采集振动能供电的产品，而 Powermat 公司也推出了一种无线充电平台。

2．网络层

网络层主要关注来自于感知层的、经过初步处理的数据经由各类网络的传输问题，这涉及智能路由器、不同网络传输协议的互通、自组织通信等多种网络技术。

物联网的网络层建立在现有的移动通信网和互联网基础上，它将来自感知层的各类信息通过基础承载网络传输到应用层，这些承载网络包括移动通信网、互联网、卫星网、广电网、行业专网及其形成的融合网络等。根据应用需求，物联网的网络层可作为透传的网络层，也可升级以满足未来不同内容传输的要求。经过 10 余年的快速发展，移动通信、互联网等技术已比较成熟，在物联网的早期阶段基本能够满足物联网中数据传输的需要。

物联网通过各种接入设备与移动通信网和互联网相连，如手机付费系统中由刷卡设备将内置手机的 RFID 信息采集并上传到互联网，网络层完成后台鉴权认证并从银行网络划账。

网络层还具有信息存储查询、网络管理等功能。

网络层中的感知数据管理与处理技术是实现以数据为中心的物联网的核心技术。感知数据管理与处理技术包括传感网数据的存储、查询、分析、挖掘、理解以及基于感知数据决策和行为的理论和技术。云计算平台作为海量感知数据的存储、分析平台，将是物联网网络层的重要组成部分，也是应用层众多应用的基础。

在产业链中，通信网络运营商将在物联网网络层占据重要的地位，而正在高速发展的云计算平台将是物联网发展的又一助力。

3．应用层

物联网的应用层利用经过分析处理的感知数据，为用户提供丰富的特定服务。应用层主要包括服务支撑层和应用子集层。物联网的核心功能是对信息资源进行采集、开发和利用。服务支撑层的主要功能是根据底层采集的数据，形成与业务需求相适应、实时更新的动态数据资源库。

物联网的应用可分为监控型(物流监控、污染监控)、查询型(智能检索、远程抄表)、控制型(智能交通、智能家居、路灯控制)、扫描型(手机钱包、高速公路不停车收费)等。

应用层是物联网发展的目的，软件开发、智能控制技术将会为用户提供丰富多彩的物联网应用。各种行业和家庭应用的开发将会推动物联网的普及，也给整个物联网产业链带来利润。

另外从物联网技术的体系结构角度解读物联网，可以将支持物联网的技术分为四个层次：感知技术、传输技术、支撑技术与应用技术。

(1) 感知技术。感知技术是指能够用于物联网底层感知信息的技术，它包括 RFID 与 RFID 读写技术、传感器与传感器网络、机器人智能感知技术、遥测遥感技术以及 IC 卡与条形码技术等。

(2) 传输技术。传输技术是指能够汇聚感知数据，并实现物联网数据传输的技术，它

包括互联网技术、地面无线传输技术以及卫星通信技术等。

(3) 支撑技术。支撑技术是指用于物联网数据处理和利用的技术，它包括云计算与高性能计算技术、智能技术、数据库与数据挖掘技术、GIS(Geography Information System，地理信息系统)/GPS(Global Positioning System，全球定位系统)技术、通信技术以及微电子技术等。

(4) 应用技术。应用技术是指用于直接支持物联网应用系统运行的技术，它包括物联网信息共享交互平台技术、物联网数据存储技术以及各种行业物联网应用系统。

1.2.2 物联网的体系架构

体系架构是指导具体系统设计的首要前提。物联网涉及面广，包含多种业务需求、运营模式、技术体制、信息需求和产品形态均不同的应用系统，因此统一、系统的业务体系结构才能够满足物联网全面实时感知、多目标业务、异构技术体制融合等需求。各业务应用领域可以对业务类型进行细分，比如细分为绿色农业、工业监控、公共安全、城市管理、远程医疗、智能家居、智能交通和环境监测等各类不同的业务服务，根据业务需求的不同，对业务、服务、数据资源、共性支撑、网络和感知层的各项技术进行裁剪，形成不同的解决方案，这可以承担一部分程序和人机交互功能。应用层将为各类业务提供统一的信息资源支撑，建立并实时更新可重复使用的信息资源库和应用服务资源库，使得各类业务服务可以根据用户的需求随需组合，这就使得物联网的应用系统对业务的适应能力明显提高。应用层能够提升对应用系统资源的重用度，为快速构建新的物联网应用奠定基础，以满足在物联网环境中复杂多变的网络资源应用需求和服务。

除此之外，物联网还需要信息安全、物联网管理、服务质量管理等公共技术支撑，这些技术支撑以采用现有标准为主。在各层之间，信息不是单向传递，而是有交互、控制的。所传递的信息多种多样，其中最为关键的是围绕物品信息，完成海量数据采集、标识解析、传输、智能处理等各个环节，与各业务领域应用融合，完成各业务功能。因此物联网的系统架构和标准体系是一个紧密关联的整体，这决定了物联网研究的方向和领域。

物联网的感知环节具有很强的异构性，为实现异构信息之间的互联、互通与互操作，未来的物联网需要以一个开放的、分层的、可扩展的网络体系结构为框架。目前，国内的研究人员在描述物联网的体系框架时，多采用 ITU-T 在 Y.2002 建议中描述的 USN(泛在传感器网络)高层架构作为基础，自下而上分为底层传感器网络、泛在传感器网络接入网络、泛在传感器网络基础骨干网络、泛在传感器网络中间件、泛在传感器网络应用平台五个层次。图 1-5 是 USN 架构的示意图。

物联网的整个结构可分为射频识别系统和信息网络系统两部分。射频识别系统主要由标签和读写器组成，两者通过 RFID 空中接口通信，读写器获取产品标识后，通过 Internet 或其他通信方式将产品标识上传至信息网络系统的中间件，然后通过 ONS(Object Name Service，对象名服务)解析获取产品的对象名称，继而通过 EPC(Electronic Product Code，电子产品码)信息服务的各种接口获得产品信息的各种相关服务。整个信息系统的运行都会借助 Internet 的网络系统，利用在 Internet 基础上发展出的通信协议和描述语言。因此我们可以说物联网是架构在 Internet 基础上关于各种物理产品信息服务的总和。从应用角度来看，物联网中三个层次值得关注，也就是说，物联网由三部分组成：一是传感网络，它以二维