第 1 章 物联网系统的安全体系

1.1 物联网系统的起源与发展

物联网系统的应用领域很广，物联网系统在家庭中的典型应用是智能家居（smart home 或 home automation）。因此，不妨从分析智能家居的美妙功能开始介绍物联网。如图 1-1 所示，所谓智能家居，就是通过物联网技术将家庭中的各种设备（如音 / 视频设备、照明设备、窗帘控制设备、空调、安防设备、计算机、家庭影院系统、网络家电等）连接到一起，组成一个智能化的家居系统，提供灯光控制、风扇控制、空调控制、厨房设备控制、浴室设备控制、安全防盗报警、主人身体健康状况监测、家居环境监测、可编程家电控制等多种功能和手段。与普通家居相比，智能家居除了具有传统的居住功能，还兼备了智能建筑、网络通信、智能家电等自动化功能，提供智能的全方位的家居服务。

图 1-1　智能家居示意图

下面让我们描绘一下应用物联网技术的智能家居的美好生活——在杨柳轻飘、百花盛开的春天，你可以在美梦醒来之前，就已经让智能茶壶自动为你热好牛奶、红茶或咖啡，或者让智能榨汁机自动为你榨好苹果汁，让智能煎锅自动为你煎好鸡蛋，或者让智能电饭锅做好营养丰富的早餐；当你享受早餐时，可以让智能电视自动为你播放当天的新闻，或者让智能音响设备自动播放美妙的音乐；你可以让智能淋水器根据当天阳光的照射量自动为种植的花草淋上适量的水；你还可以让扫地机器人自动打扫你的房间。

在阳光灿烂、酷热难熬的夏天，当你忙碌了一天，可以在下班回到家之前，遥控家中的空调开始工作；也可以遥控智能高压锅开始熬汤，遥控电饭锅开始煮饭；也许你打算

品尝美酒，你可以在回家的路上到商店购买一瓶美酒，只要简单地用手机扫描一下电子标签，就可以识别这瓶酒的真伪；当你的汽车快回到家门口的时候，车库会“聪明”地认出你，自动为你打开大门；当你迈进客厅的时候，智能电视自动为你播放喜爱的节目。

在风和日丽、心旷神怡的秋天，当你和家人回到家前，可以遥控打开家里的智能窗户和智能窗帘，达到通风和更换室内新鲜空气的目的；你还可以让智能机器人陪伴你的孩子，一起玩猜谜语游戏，教孩子背诵《三字经》或者唐诗，或者给孩子讲生动有趣的故事。

在寒风凛凛、风雪交加的冬天，当你准备离开家去上班的时候，智能机器人会给你说明当前户外实际的气温，提醒你要及时穿上御寒衣服，以免受寒生病；你只要提前用遥控器简单地发出一条指令，就可以指挥停在户外的汽车化雪解冻……

以上这些美好的设想，都可以用物联网技术轻易地实现。

比尔·盖茨的智能家居，就是物联网技术应用的一个典型案例。这幢豪宅位于美国华盛顿湖东岸，依山傍水，修建于 20 世纪 90 年代，从设计、施工到建成，整整花了七年时间，耗资 6000 万美元。整幢建筑物共铺设了长达 80 千米的光纤和电缆，家中几乎所有的设施都通过网络连接在一起。大门外安装有天气感知器，可以根据各项天气指标通知户内的空调系统调节室内的温度和湿度，主人在回家途中只要用手机发布指令，家中的浴缸就开始放水调温，为主人洗澡做好准备。更为奇妙的是，每一位来访的客人都可以领到一个含有电子标签的胸针，胸针中存放了每位客人对灯光的亮度和颜色、电视频道、室内的通风、温度、湿度、音乐、绘画等的个人喜好。当客人走进某个房间时，电子标签就会通过传感系统与房间中的设备交换信息，所有设备自动将环境调整到使客人最舒适、最满意的状况。

物联网的应用，可以大大改善人们的工作和生活，帮助人们更好地实现对一切智能物体的远程管理，让人们轻松地做到“运筹帷幄之中，决胜千里之外”。

早在 1991 年，美国麻省理工学院（MIT）的凯文·阿什顿（Kevin Ashton）教授，就已经提出了物联网的概念。

1995 年，比尔·盖茨在其著作《未来之路》一书中也提及了物联网，但当时并未引起人们的广泛重视。

1999 年，美国麻省理工学院建立了自动识别中心（Auto-ID），提出“万物皆可通过网络互连”，阐明了物联网的基本概念。早期的物联网是基于射频识别（Radio Frequency Identification，RFID）技术的物流网络。

2004 年，日本总务省提出 u-Japan 计划，该战略力求实现人与人、物与物、人与物之间的连接，希望将日本建设成一个随时、随地、任何物体、任何人均可连接的泛在网络社会。

2005 年，国际电信联盟电信标准化部（International Telecommunication Union-Telecommunication Standardization Sector，ITU-T）在突尼斯举行的信息社会世界峰会（World Summit on Information Society，WSIS）上正式确定了“物联网”的概念，并随后发布了《ITU 互联网报告 2005：物联网》（*ITU Internet Reports 2005: the Internet of Things*），介绍了物联网的特征、相关的技术、面临的挑战和未来的市场机遇，声称在未来 10 年左右时间里，物联网将得到大规模应用，革命性地改变世界的面貌。

2006 年，韩国确立了 u-Korea 计划，该计划旨在建立无所不在的社会（ubiquitous

society），在民众的生活环境里建设智能型网络（如 IPv6、BcN、USN）和各种新型应用（如 DMB、Telematics、RFID），让民众可以随时随地享有科技智慧服务。

2006 年 3 月，欧盟召开“从 RFID 到物联网”会议，对物联网做了进一步的描述。

2008 年，在法国召开的欧洲物联网大会的重要议题包括未来互联网和物联网的挑战、物联网中的隐私权、物联网在主要工业部门中的影响等内容。

2008 年 7 月，美国国家情报委员会发表的《2025 年对美国利益潜在影响的 6 种关键技术》报告将“物联网”技术列入其中，认为物联网技术存在裂变性的影响能力，将对人类社会的生产和生活产生巨大的影响。

“智慧地球”概念最初是美国的 IBM 公司提出的，2009 年被上台伊始的美国总统奥巴马积极回应，物联网被提升为一种战略性新技术，全面纳入到智能电网、智能交通、建筑节能和医疗保健制度改革等经济刺激计划中。IBM 公司的“智慧地球”市场战略在美国获得广泛关注，随后迅速推广到全球范围。

2009 年，时任美国总统奥巴马响应 IBM 公司“智慧地球”的战略，提出了“感知地球”的概念。

2009 年 6 月 10 日，中国科学院发布了《创新 2050：科学技术与中国的未来，中国至 2050 年信息科技发展路线图》系列报告，描述了物联网的发展路线图。

2009 年 8 月，时任中国总理温家宝在视察中国科学院无锡物联网产业研究所时，对物联网应用也提出了“感知中国”的理念，由此推动了物联网概念在中国的重视。

2009 年，欧盟执委会发表了欧洲物联网行动计划，描绘了物联网技术的应用前景，提出欧盟政府要加强对物联网的管理，促进物联网的发展。

2009 年 12 月 15 日，欧洲物联网项目总体协调组发布了《物联网战略研究路线图》，将物联网研究分为感知、宏观架构、通信、组网、软件平台及中间件、硬件、情报提炼、搜索引擎、能源管理、安全 10 个层面，系统地提出了物联网战略研究的关键技术和路径。

2010 年 6 月，欧盟委员会推出了《数字议程》（*Digital Agenda*）五年行动计划，该议程是《欧盟 2020 战略》七项旗舰举措之一，明确了利用 ICT 帮助实现欧盟 2020 战略目标的使能作用。

2012 年 2 月，中国工信部发布了《物联网“十二五”发展规划》，将超高频和微波 RFID 标签、智能传感器明确为支持重点，并明确在九大领域开展示范工程。

2012 年 5 月，国务院审议通过的《“十二五”国家战略性新兴产业发展规划》明确将物联网作为重要任务和重大工程。

近年来，由于世界各国政府的重视和发展，全球物联网行业呈现快速发展的趋势，应用领域快速扩张，大数据、人工智能、云计算、区块链等新技术与物联网系统快速融合。

1.2　物联网系统的定义与特征

1.2.1　物联网系统的定义

物联网是一个综合性的智能网络系统，有许多种不同的定义。各个领域的专家和学者们都先后提出了自己的定义，众说纷纭、各抒己见。这些定义是专家和学者们基于个人研

究角度提出来的。在本书中，编者选择了最具代表性的几种定义供读者们参考。

（1）物联网是实现物体与物体连接的互连网络。英语中“物联网”一词为 Internet of Things（IoT），可以翻译成物与物的互联网。

（2）美国麻省理工学院的自动识别中心（Auto-ID）指出：物联网把所有的物品通过射频识别和条形码等信息传感设备，与互联网紧密地连接起来，实现智能化的识别和管理。

（3）物联网指将各种信息传感设备，如射频识别装置、红外感应器、全球定位系统、激光扫描器与互联网结合起来。其目的是把所有物品连接在一起。

（4）物联网经过接口与无线网络（也含固定网络）连接，使物体与物体之间及人与物体之间实现沟通与对话。

（5）中国电信对物联网的定义：物联网是基于特定的终端，以有线或无线等接入手段，为集团和家庭客户提供机器到机器、机器到人的解决方案，满足客户对生产过程、家居生活监控、指挥调度、远程数据采集和测量、远程诊疗等方面的信息化需求。

以上 5 种对物联网的定义都具有一定的局限性，目前比较准确的是 2005 年由国际电信联盟给出的定义：物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备，按照约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

物联网有狭义与广义之分，狭义的物联网指物与物之间的连接和信息交换；广义的物联网不仅包括物与物的信息交换，还包括人与物、人与人之间的泛在连接和信息交换。广义的物联网是一种基于泛在网及其多制式、多系统、多终端等的综合网络。

在广义物联网中不仅包括机器到机器（Machine to Machine，M2M），也包括机器到人（Machine to Person，M2P）、人到人（Person to Person，P2P）、人到机器（Person to Machine，P2M）之间广泛的通信和信息的交流。而在这个物联网中的机器（Machine，M），被定义为可以获取信息的各种终端，包括各类无线传感器、RFID 读写器、智能手机、个人计算机（Personal Computer，PC）、平板电脑、摄像头、电子望远镜、卫星定位设备（GPS）等。

物联网系统可以感知到人类需要的各种信息终端（即传感器），这些信息终端都被连接到泛在网上。这里所说的泛在网，几乎囊括了当代各种信息通信网络，不仅仅包括固定互联网和移动互联网，还包括电话通信网、移动通信网、广播电视网和各种其他专用网络。并基于这些网络的整合将各种智能终端与人紧密联系在一起，构成了一个在任何时间、任何地点都可以取得服务的物联网。总之，物联网的最终目的是为人类提供各种现代化服务。

1.2.2 物联网系统的特征

根据物联网系统实现的功能来进行分析，物联网系统具备以下四个特征。

（1）全面感知：可以利用 RFID、无线传感器、条形码、二维码等识别设备随时随地获取物体的信息。

（2）可靠传输：通过各种接入网络与互联网的融合，可以实时、可靠、准确地传输物

体的信息。

（3）智能处理：可以利用云计算、模糊识别等各种智能计算技术，对海量的物体信息进行分析和处理，对物体实施智能化的控制。

（4）综合应用：可以根据各个行业、各种业务的具体特点，形成各种单独的业务应用方案，或者整个行业及系统的应用方案。

1.3　物联网系统的体系结构

物联网系统的体系结构如图 1-2 所示。

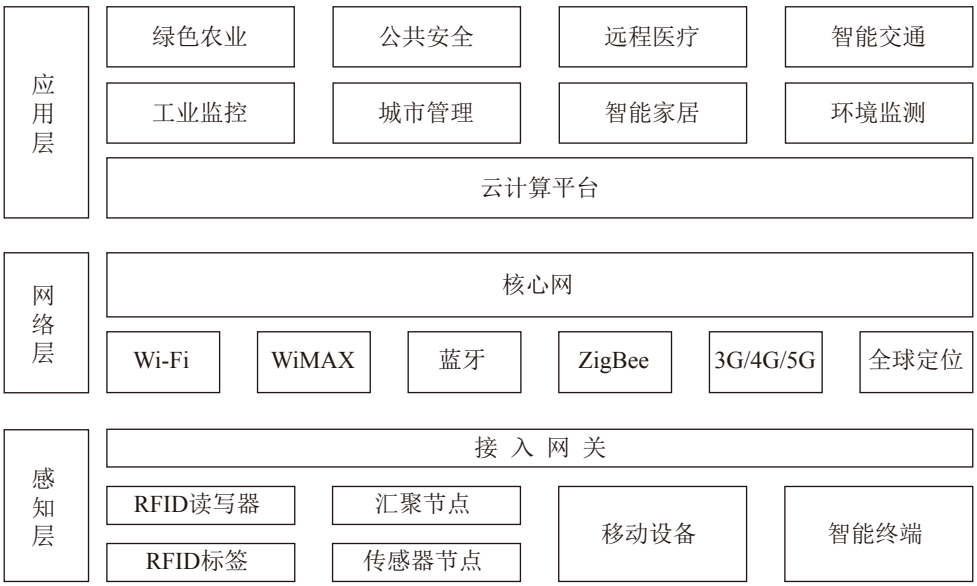

图 1-2　物联网系统的体系结构

到目前为止，物联网系统的体系结构还没有统一的标准。在本书中，我们采用业界广泛认可的体系结构，将物联网系统分为三个层次：感知层、网络层、应用层。

下面将对感知层、网络层、应用层这三层的结构及功能进行简要分析。

1.3.1　感知层

感知层由传感器节点和接入网关等组成，传感器感知外部世界的温度、湿度、声音和图像等信息，并传送到上层的接入网关，由接入网关将收集到的信息通过网络层提交到后台处理。当后台对数据处理完毕后，发送执行命令到相应的执行机构，完成对被控对象或被测对象的控制参数调整，或者发出某种信号以实现远程监控。

感知层是物联网技术发展和应用的基础，涉及 RFID、近距离无线通信技术、传感器技术、无线传感器网络等技术。

1. RFID

RFID 全称为 Radio Frequency Identification，即射频识别技术，又称为无线射频识

别，是一种近距离无线通信技术，通过无线电信号识别特定目标并读写相关数据，而无须在识别系统与特定目标之间建立机械或光学接触。RFID 常用的工作频率可分为低频（125 ～ 134.2kHz）、高频（13.56MHz）、超高频和微波等。RFID 读写器也分为移动式和固定式两类。RFID 技术的应用很广泛，在图书馆、门禁系统、食品安全等领域都有广泛的应用。

粘贴或者安装在物品上的 RFID 标签，以及用来识别 RFID 信息的读写器等，都属于物联网的感知层。在感知层中，被检测的信息是 RFID 标签中与它所粘贴的物品对应的物品身份标识。高速公路不停车收费系统、超市仓储管理系统等都是 RFID 的典型应用案例。

2. 近场通信

近场通信（Near Field Communication，NFC，也称为近距离无线通信）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，在 10cm（3.9in）内交换数据。NFC 技术由免接触式 RFID 技术演变而来，由飞利浦公司和索尼公司共同开发推广，是一种非接触式识别和互连技术，可以在移动设备、消费类电子产品、个人计算机和智能控件工具间进行近场通信。

近场通信是一种短距高频的无线电技术，在 13.56MHz 频率下运行于 20cm 距离内。其传输速度有 106kb/s、212kb/s 或者 424kb/s 三种。目前近场通信已通过成为 ISO/IEC IS 18092 国际标准、EMCA-340 标准与 ETSI TS 102 190 标准。NFC 采用主动和被动两种读取模式。

3. 传感器技术

传感器技术（sensor technology）是实现测试与自动控制的重要技术。在物联网感知层中，传感器的主要特征是能准确传递和检测出被测对象某一形态的信息，并将其转换成另一形态的信息。具体地，传感器指那些对被测对象的某一确定的信息具有感受（或响应）与检出能力，并使之按照一定规律转换成与之对应的可输出信号的元器件或装置。如果没有传感器对被测对象的原始信息进行准确可靠的捕获和转换，一切准确的测试与控制都将无法实现。

4. 无线传感器网络

无线传感器网络实现了数据的采集、处理和传输三种功能。它与通信技术和计算机技术并称信息技术的三大支柱。

无线传感器网络（Wireless Sensor Network，WSN）是由大量静止的或移动的传感器以自组织和多跳的方式构成的无线网络。它以协作方式感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给物联网的所有者。

无线传感器网络具有众多不同类型的传感器，可以探测包括地震、电磁、温度、湿度、风力、噪声、光强度、大气压强、土壤成分，移动物体的形状、大小、运动速度和方向等周边环境下多种多样的现象。其潜在的应用领域包括军事、航空、防爆、救灾、环境、医疗、保健、家居、工业、商业等。

1.3.2　网络层

在物联网的体系架构中，网络层位于中间，它向下与感知层相连接，向上则与应用层相连接，高效、稳定、实时、安全地传输上层与下层之间的数据。

网络层是物联网的“神经中枢”和“大脑”，用于实现信息传递和处理。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等。

网络层的主要功能是传输和预处理感知层所获得的数据。这些数据可以通过移动通信网、互联网、企业内部网、各类专线网、局域网、城域网等进行传输。特别是在三网（有线电话网、有线电视网、光纤网）融合后，有线电视网也能承担物联网网络层的功能，有利于物联网的快速推进。网络层所需要的关键技术包括核心网技术、近场技术和移动通信技术等。

物联网网络层构建在现有互联网等通信网络基础之上。物联网通过各种接入设备与互联网相连。例如，手机付费系统中由刷卡设备将内置手机的 RFID 信息采集上传到互联网，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，包括传感网数据的存储、查询、分析、挖掘和理解，以及基于感知数据决策的理论与技术。

1.3.3　应用层

应用层位于物联网体系结构的最上层。应用层与各种不同的行业相结合，实现广泛智能化。应用层是物联网与行业专业技术的深度融合，与行业需求结合，实现行业智能化，这类似人的社会分工，最终构成人类社会。

在各层之间，信息不是单向传递的，也有交互、控制等，所传递的信息多种多样，其中最关键是物品信息，包括在特定应用系统范围内能唯一标识物品的识别码和物品的静态与动态信息。

云计算平台作为海量感知数据的存储、分析平台，是物联网的重要组成部分，也是应用层众多应用的基础支撑。在产业链中，通信网络运营商和云计算平台提供商将在物联网中占据重要地位。

应用层主要根据行业特点，借助物联网的技术手段，开发各类的行业应用解决方案，将物联网的优势与行业的生产经营、信息化管理、组织调度结合起来，形成各类的物联网解决方案，构建智能化的行业应用。

例如，交通行业涉及智能交通技术；电力行业涉及智能电网技术；物流行业涉及智慧物流技术等。

物联网在各行业的应用还涉及系统集成技术、资源打包技术等。

物联网应用层利用经过分析处理的感知数据，为各行业的用户提供丰富的特定服务。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推动物联网的普及，给整个物联网产业链带来利润。

1.4 物联网的关键技术

1.4.1 RFID 技术

射频识别（RFID）是一种基于近场通信的识别技术，可以通过无线电信号识别特定目标并读写相关数据，而无须在识别系统与特定目标之间建立机械或者光学接触。RFID 的系统结构如图 1-3 所示。

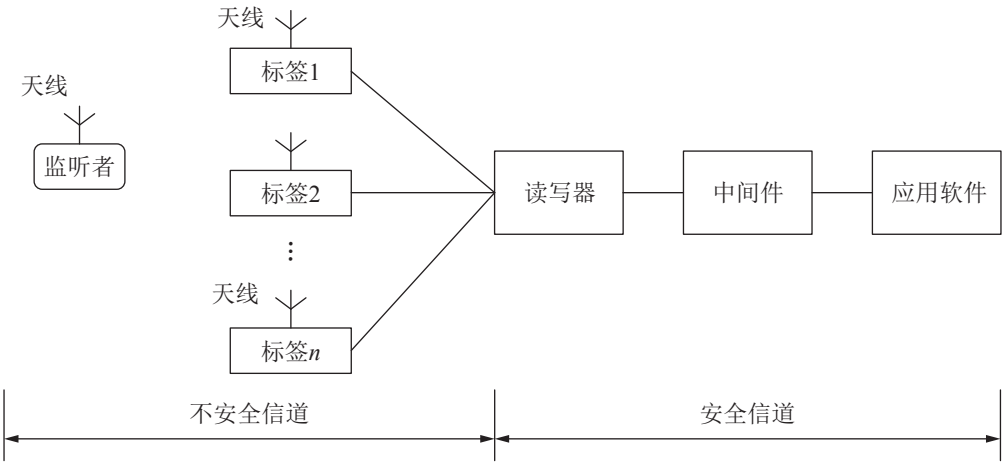

图 1-3　RFID 的系统结构

RFID 技术把电信号调制成某个制定频率的电磁波，把数据从附着在物品上的电子标签上传送出去，以自动辨识与追踪该物品。某些电子标签在工作时，能够从读写器发出的电磁场中得到能量，并不需要电池；也有些电子标签本身配有电源，并可以主动发出无线电波。电子标签包含了物品的相关信息，在几米之内就可以被读写器感知。与条形码不同，RFID 标签不需要处在读写器视线范围内，因此也可以嵌入被追踪物品之内。

从系统结构上分析，一套完整的 RFID 系统，由电子标签、读写器、中间件和应用软件等部分组成。

1. 电子标签

电子标签由天线、耦合元件及芯片组成。在 RFID 系统中，通常用电子标签作为物品的应答器，每个电子标签具有唯一的电子编码，粘贴或附着在物体上，用于标识物品。天线是将 RFID 标签的数据信息传递给读写器的设备。RFID 天线可分为标签天线和读写器天线两种类型。

2. 读写器

读写器（reader）由天线、耦合元件和芯片组成，是读取（写入）标签信息的设备，

分为手持式或固定式两种类型。读写器发射某一特定频率的无线电波，将能量传送给标签，用以驱动电子标签中的电路，从而将其内部的数据送出。此时，读写器便按照次序接收这些数据，并发送给中间件做相应的处理。

3. 中间件

中间件（middleware）位于读写器与应用软件之间，是一种面向消息的、可以接收应用软件端发送的请求，并同时与一个或者多个读写器交互通信，在接收和处理数据后向应用软件返回处理结果的特殊软件。

4. 应用软件

顾名思义，应用软件是工作在应用层的软件，主要用于进一步处理收集的数据，并使其为人们所使用。应用软件系统是计算机的后台处理系统，计算机通过有线或无线网络与阅读器相连，获取电子标签的内部信息，对读取的数据进行筛选和分析，并进行后台处理。

RFID 技术的基本工作原理并不复杂：标签进入磁场后，接收读写器发出的射频信号，凭借感应电流所获得的能量发送存储在芯片中的产品信息（无源标签或被动标签），或者由标签主动发送某一频率的信号（有源标签或主动标签），读写器读取信息并解码后，送至计算机系统进行相关数据处理。

以 RFID 读写器与电子标签之间的通信及能量感应方式来划分，应用软件大致可以分为感应耦合式（inductive coupling）及后向散射耦合式（backscatter coupling）两种类型。一般低频的 RFID 多采用第一种方式，而较高频的 RFID 多采用第二种方式。

根据使用的结构和技术不同，读写器可以是读出设备，也可以是读写设备。它是 RFID 系统的信息控制和处理中心。读写器通常由耦合模块、收发模块、控制模块和接口单元组成。读写器和电子标签之间一般采用半双工通信方式进行信息交换，同时通过耦合给无源电子标签提供能量和时序。在实际应用中，则进一步通过以太网（Ethernet）或无线局域网（Wireless Local Area Network，WLAN）等实现对物体识别信息的采集、处理及远程传送等管理功能。

许多行业都可以应用射频识别技术。例如，将 RFID 电子标签粘贴在一辆正在生产中的汽车上，生产厂家便可以追踪此车的生产进度；将电子标签粘贴在产品上，仓库就可以追踪该产品所在的位置；将电子标签附于牲畜与宠物上，可以方便地识别牲畜与宠物的身份。此外，RFID 身份识别也可以使企业员工能够进入紧闭的大门；汽车上的 RFID 标签可以用于收费路段或停车场的自动缴费。

1.4.2　无线传感器网络技术

1. 无线传感器网络的定义

无线传感器网络是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自组织网络。其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息，并发送给观察者。传感器、感知对象和观察者构成了无线传感器网络的

三个要素。

近年来，微机电系统（Micro-Electro-Mechanism System，MEMS）、片上系统（SoC）、无线通信和低功耗嵌入式技术飞速发展，孕育出无线传感器网络（WSN），并以其低功耗、低成本、分布式和自组织的特点带来了信息感知的一场变革。

正如互联网使计算机能够访问各种数字信息，而可以不管其保存到什么位置一样，无线传感器网络能扩展人们与现实世界进行远程交互的能力。它甚至被人们称为一种全新类型的计算机系统，因为它具有区别于过去硬件的可以到处散布的和集体感知与分析的能力。

2. 无线传感器网络的结构

无线传感器网络的结构如图 1-4 所示。

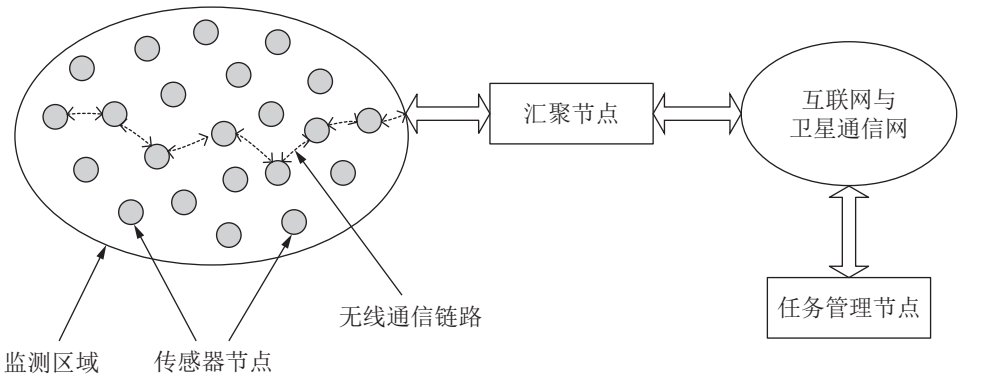

图 1-4　无线传感器网络的结构

无线传感器网络系统通常包括传感器节点（sensor）、汇聚节点（sink）和任务管理节点（coordinator）。

大量传感器节点随机部署在监测区域内部或附近，能够通过自组织方式构成网络。传感器节点监测的数据沿着其他传感器节点逐跳地进行传输，在传输过程中监测数据可能被多个节点处理，经过多跳后路由到汇聚节点，最后通过互联网或卫星通信网到达任务管理节点。用户通过任务管理节点对传感器网络进行配置和管理，发布监测任务，以及收集监测数据。

（1）传感器节点。传感器节点处理能力、存储能力和通信能力相对较弱，通过小容量电池供电。从网络功能上看，每个传感器节点除了进行本地信息收集和数据处理外，还要对其他节点转发来的数据进行存储、管理和融合，并与其他节点协作完成一些特定任务。

（2）汇聚节点。汇聚节点的处理能力、存储能力和通信能力相对较强，是连接传感器网络与 Internet 等外部网络的网关，用以实现两种协议间的转换，同时向传感器节点发布来自管理节点的监测任务，并把 WSN 收集到的数据转发到外部网络。汇聚节点既可以是一个具有增强功能的传感器节点，有足够的能量供给和更多的内存与计算资源，Flash 和 SRAM 中的所有信息传输到计算机中，通过汇编软件，可方便地把获取的信息转换成汇编文件格式，从而分析出传感节点所存储的程序代码、路由协议及密钥等机密信息，同时还可以修改程序代码，并加载到传感器节点中。

（3）任务管理节点。任务管理节点用于动态地管理整个无线传感器网络。无线传感器网络的所有者通过任务管理节点访问无线传感器网络的资源。

1.4.3　M2M 技术

M2M 平台的系统结构如图 1-5 所示。

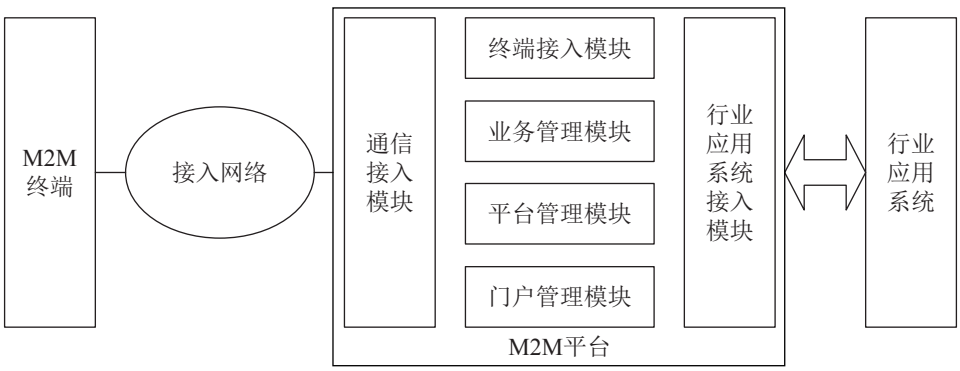

图 1-5　M2M 平台的系统结构

M2M 是“机器对机器通信”的英文简称，主要指通过“通信网络”传递信息从而实现机器对机器的数据交换，也就是通过通信网络实现机器之间的互连互通。移动通信网络由于其网络的特殊性，终端侧不需要人工布线，可以提供移动性支撑，有利于节约成本，并可以满足危险环境下的通信需求，使得以移动通信网络作为承载的 M2M 服务得到了业界的广泛关注。

通信接入模块主要实现平台与 M2M 终端的通信连接，包括实现各种有线接入网络、无线接入网络的通信功能，如 3G/4G/5G、Wi-Fi、WiMAX、ADSL 等。

终端接入模块主要实现平台对终端接入的认证管理、连接保持及流量控制功能。在终端接入时，通过平台可以完成包括报文收发、报文认证、终端流控和协议适配等功能；在终端接入后，平台将完成终端注册、终端登录、终端退出及终端注销等功能。此外终端接入模块还实现终端信息查询、状态监测、故障管理、参数查询和配置、远程控制和终端操作任务管理等功能。该模块中需要实现不同运营商的 M2M 终端接入协议，如中国移动通信企业标准无线机器通信协议（Wireless Machine-to-Machine Protocol，WMMP）、中国电信技术规范 M2M 终端监测控制协议（M2M Device Management Protocol，MDMP），以实现与 M2M 终端的数据交互。

业务管理模块主要实现对终端和应用基本信息的维护，对相应的行业应用业务的受理、计费及下单等。

平台管理模块主要完成 M2M 业务系统正常运行所需的基础数据管理、操作员账号管理、系统安全管理等功能。

门户管理模块提供人性化的 Web 登录界面，供平台管理员、业务管理员、企业客户、终端厂商、服务提供商等完成终端管理、应用管理、系统管理等功能。

行业应用系统接入模块实现平台与行业应用系统的对接，为行业应用系统提供终端管理服务和行业应用数据转发服务，包括应用接入的建立和维护、流量控制、终端管理请求

处理、应用数据转发请求处理等基本功能。

由以上分析可以看出，M2M 平台涉及的技术主要包括门户管理技术、通信接入技术、安全管理技术、流量控制技术和数据库管理技术等。

M2M 与社会的发展和人们的生活、工作密切相关，其应用遍布各个领域，如交通领域（交通监控、定位导航）、电力领域（远程抄表和负载监控）、农业领域（大棚监控、动物溯源）、智慧城市（电梯监控、路灯控制）、安全领域（城市和企业安防）、环保领域（污染监控、水土检测）和智能家居（老人和儿童看护、智能安防）等。

1.4.4 基于 IPv6 协议的下一代互联网

1. IPv6 的基本概念

基于 IPv6 协议的下一代互联网是物联网的核心网络。IPv6 是 Internet Protocol Version 6 的缩写，即互联网协议第 6 版。IPv6 是互联网工程任务组（Internet Engineering Task Force，IETF）发布的用于替代现行 IP 协议（IPv4）的下一代 IP 协议。

目前，国际互联网（Internet）广泛使用的是 IPv4 技术，IPv4 技术最大问题是网络地址资源有限。理论上，IPv4 可以编址 1600 万个网络、40 亿台主机。但采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数目大打折扣。IPv4 地址已于 2011 年 2 月 3 日分配完毕，其中，北美占有 IPv4 全部地址的 3/4，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国截至 2010 年 6 月 IPv4 地址数量达到 2.5 亿个，远远落后于 4.2 亿网民的需求。IPv4 地址资源的不足，严重地制约了中国及其他国家互联网技术的应用和发展。

一方面 IPv4 地址资源数量有限，另一方面随着电子技术及网络技术的发展，物联网将进入人们的日常生活，需要海量的 IP 地址资源。在这样的需求下，IPv6 应运而生。单从数量级上看，IPv6 所拥有的地址容量约为 IPv4 的 8×10^{28} 倍，达到 2^{128} 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接入网络在数量限制上扫清了障碍。

如果说 IPv4 实现的只是人机对话，那么 IPv6 则扩展到任意事物之间的对话，它不仅可以为人类服务，还可以为众多硬件设备服务，如家用电器、传感器、远程照相机、汽车等。它将使无时不在、无处不在的深入社会每个角落的真正的物联网成为可能，并带来无可估量的经济利益。

2. IPv6 技术的优势

与 IPv4 技术相比，IPv6 技术具有以下几个优势。

（1）IPv6 具有更大的地址空间。

IPv4 中规定 IP 地址长度为 32 位，最大地址个数为 2^{32} 个；而 IPv6 中 IP 地址的长度为 128 位，即最大地址个数为 2^{128} 个。与 32 位地址空间相比，其地址空间增加了（$2^{128}-2^{32}$）个。

目前，IPv4 采用 32 位二进制数地址长度，约有 43 亿个 IP 地址，而 IPv6 采用 128 位二进制数地址长度，具有海量的地址资源。地址的丰富将完全突破在 IPv4 互联网应用上

的种种限制。

以智慧家庭为例，家中每一个传感器、每一台家电都可以有一个独立的 IP 地址，可以真正形成一个智慧家庭。

IPv6 在地址空间上的优势在很大程度上解决了 IPv4 互联网存在的问题，这也成为国际互联网从 IPv4 向 IPv6 演进的重要动力。

（2）IPv6 使用更小的路由表。

IPv6 的地址分配一开始就遵循聚类（aggregation）的原则，这使得路由器能在路由表中用一条记录（entry）表示一个子网，大大缩短了路由器中路由表的长度，提高了路由器转发数据包的速度。

（3）IPv6 增强了对多媒体应用的支持。

IPv6 增加了增强的组播（multicast）支持，以及对流的控制（flow control），这使得基于 IPv6 的网络在多媒体应用方面有良好的发展前景，为服务质量（Quality of Service，QoS）控制提供了良好的网络平台。

（4）对自动配置的支持。

IPv6 技术增加了对自动配置（auto configuration）的支持。这是对动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）的改进和扩展，使得网络（尤其是局域网）的管理更加方便和快捷。

（5）IPv6 具有更高的安全性。

在 IPv6 网络中，用户可以对网络层的数据进行加密并对 IP 报文进行校验，在 IPv6 的加密与鉴别选项提供了分组的保密性与完整性，极大地增强了网络的安全性。

（6）允许扩充。

如果新的技术或应用需要时，IPv6 允许协议进行扩充。

（7）更好的头部格式。

IPv6 使用新的头部格式，其选项与基本头部分开，如果需要，可将选项插入到基本头部与上层数据之间。这简化和加速了路由选择过程，因为大多数的选项不需要由路由选择。

（8）实现附加的功能。

IPv6 可以通过一些新的选项来实现附加功能。

3. IPv6 的关键技术

（1）IPv6 DNS 技术。IPv6 DNS 体系结构与 IPv4 DNS 体系结构相同，都是统一采用树状结构的域名空间。在从 IPv4 向 IPv6 的演进阶段，正在访问的域名可以对应多个 IPv4 和 IPv6 地址，未来，随着 IPv6 网络的普及，IPv6 地址将逐渐取代 IPv4 地址。

（2）IPv6 路由技术。IPv6 路由查找的原理与 IPv4 一样，均遵循最长地址匹配原则，选择最优路由还允许地址过滤、聚合、注射操作。原来的 IPv4 IGP 和 BGP 的路由技术，如 RIP、ISIS、OSPFv2 和 BGP-4 动态路由协议一直延续到 IPv6 网络中，新的版本分别是 RIPng、ISISv6、OSPFv3，BGP4+。

（3）IPv6 安全技术。与 IPv4 相比，IPv6 并没有提供新的安全技术，但 IPv6 协议可以通过 128 字节的 IPSec 报文头包、ICMP 地址解析和其他安全机制来提高安全性。

1.4.5 无线通信网络

无线通信网络主要包括无线局域网（Wi-Fi）、无线城域网（WiMAX）、紫蜂技术（ZigBee）、蓝牙技术、红外通信技术和 5G 移动通信等技术。

1. Wi-Fi 技术

无线保真（Wireless Fidelity，Wi-Fi）技术是通过在互联网连接基础上，安装无线访问点来实现的。这个访问点对无线信号做短距离传输，一般仅覆盖 100m 以内的范围。当一台支持 Wi-Fi 的设备（如智能手机、平板电脑等）遇到一个无线接入点时，该设备可以用无线方式连接到这个无线局域网。大部分无线接入点布置在公共区域，如机场、咖啡店、餐厅、旅馆、书店、校园等。许多家庭和办公室也拥有 Wi-Fi 网络。虽然有些无线接入点是免费的，但是大部分稳定的公共 Wi-Fi 网络都是由私人互联网服务提供商（Internet Service Provider，ISP）提供的，因此当用户连接到无线接入点时也许商家会收取一定费用。

2. WiMAX 技术

全球微波互连接入（World Interoperability for Microwave Access，WiMAX），也称为无线城域网或 802.16。WiMAX 是一种新兴的宽带无线接入技术，能提供面向整个城市的无线互联网高速连接服务，数据传输距离最远可达 50km。WiMAX 还具有 QoS 保障、传输速率高、业务丰富多样等优点。WiMAX 技术的起点较高，它同时采用了 OFDM/OFDMA、AAS、MIMO 等先进的通信技术。

随着 WiMAX 技术的发展，可以逐步实现宽带业务的移动化，而 5G 移动通信技术则可以实现移动业务的宽带化，这两种技术的融合程度会越来越高。

WiMAX 系统的结构如图 1-6 所示。

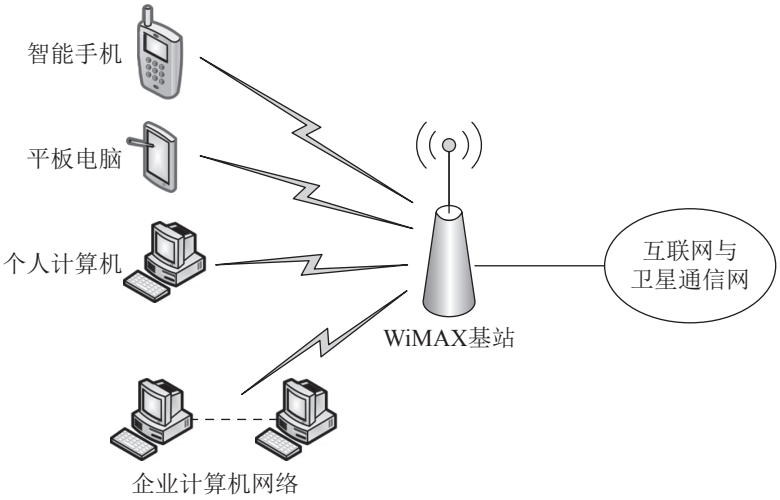

图 1-6　WiMAX 系统的结构

3. ZigBee 技术

紫蜂（ZigBee）是一种近距离、低复杂度、低功耗、低速率、低成本的无线通信技术，主要用于距离短、功耗低且传输速率不高的各种电子设备之间进行数据传输，以及典

型的有周期性数据、间歇性数据和低反应时间数据传输的应用。

与移动通信的 CDMA 网或 GSM 网络不同的是，ZigBee 网络主要为工业现场自动化控制数据传输而建立，因此具有简单、使用方便、工作可靠、价格低的特点。而移动通信网主要是为语音通信而建立的，每个基站价值一般在百万元人民币以上，而每个 ZigBee“基站”却不到一千元人民币。每个 ZigBee 网络节点不仅本身可以作为监控对象，如其所连接的传感器直接进行数据采集和监控，还可以自动中转其他网络节点传过来的数据资料。除此之外，每一个 ZigBee 网络节点（FFD）还可在自己信号覆盖范围内，和多个不承担网络信息中转任务的孤立的子节点（RFD）进行无线连接。

4. 蓝牙技术

蓝牙（Bluetooth）技术，是一种支持设备短距离（一般 10m 内）通信的无线电技术。能在移动电话、PDA、无线耳机、笔记本计算机、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 Internet 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、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（Industrial，Science，Medicine，即工业、科学、医学）频段。其数据速率为 1Mb/s。采用时分双工传输方案实现全双工传输。

5. 红外通信技术

红外通信技术利用 950nm 近红外波段的红外线作为传递信息的媒体，即通信信道。简言之，红外通信的实质就是对二进制数字信号进行调制与解调，以便利用红外信道进行传输；红外通信接口就是针对红外信道的调制解调器。发送端将基带二进制信号调制为一系列脉冲串信号，通过红外发射管发射红外信号。接收端将接收到的光脉冲转换为电信号，再经过放大、滤波等处理后送给解调电路进行解调，还原为二进制数字信号后输出。常用的有通过脉冲宽度来实现信号调制的脉宽调制（Pulse Width Modulation，PWM）和通过脉冲串之间的时间间隔来实现信号调制的脉时调制（Pulse Position Modulation，PPM）两种方法。

6. 5G 技术

近年来，第五代移动通信技术（5th Generation Mobile Communication Technology，5G）快速发展。5G 具有高速率、低时延和大连接的特点，是新一代宽带移动通信技术。5G 通信设施是实现人机物互联的网络基础设施。

国际电信联盟（ITU）定义的 5G 的三大类应用场景如图 1-7 所示。

国际电信联盟（ITU）定义的 5G 的三大类应用场景包括增强移动宽带（enhanced Mobile Broadband，eMBB）、超高可靠低时延通信（ultra-Reliable Low-Latency Communication，uRLLC）和海量机器类通信（massive Machine Type Communication，mMTC）。其中，增强移动宽带主要面向移动互联网流量爆炸式增长的应用需求，为移动互联网用户提供更加极致的应用体验；超高可靠低时延通信主要面向工业控制、远程医疗、自动驾驶等对时延和可靠性具有极高要求的垂直行业应用需求；海量机器类通信主要面向智慧城市、智能家居、环境监测等以传感和数据采集为目标的应用需求。

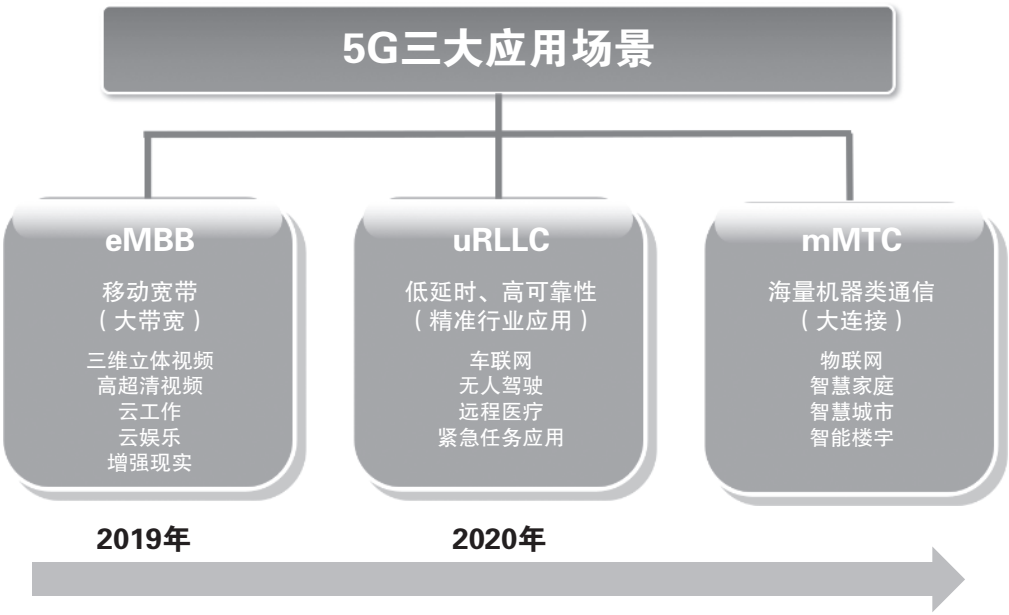

图 1-7　5G 的三大类应用场景

1.4.6　GPS 全球定位系统

全球定位系统（Global Positioning System，GPS），是具有海、陆、空全方位实时三维导航与定位能力的卫星导航与定位系统。

GPS 结构如图 1-8 所示。

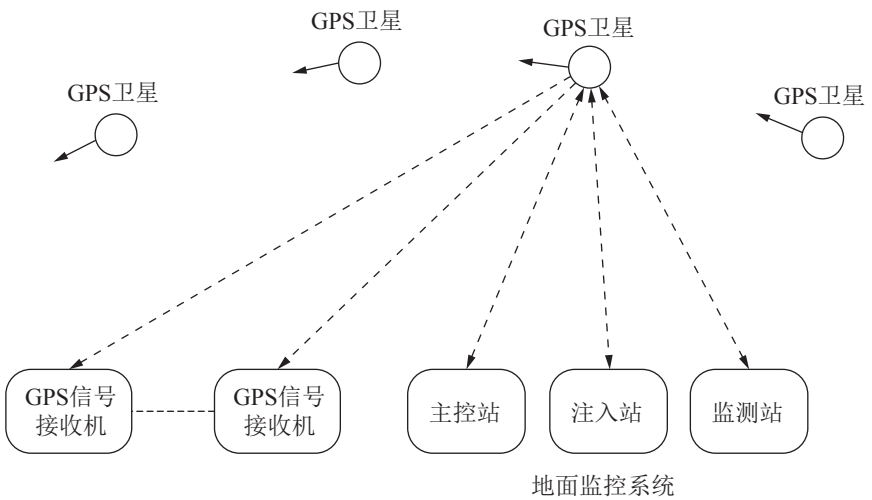

图 1-8　GPS 结构

全球定位系统由 GPS 卫星星座、地面监控系统和 GPS 信号接收机三部分构成。

1. GPS 卫星星座

GPS 卫星星座由 21 颗工作卫星和 3 颗在轨备用卫星组成，记作（21+3）GPS 星座。

24 颗卫星均匀分布在 6 个轨道平面内，轨道倾角为 55°，各个轨道平面之间相距 60°，即轨道的升交点赤经各相差 60°。每个轨道平面内各卫星之间的升交角距相差 90°，每一轨道平面上的卫星比西边相邻轨道平面上的相应卫星超前 30°。

对于在 20000km 高空的 GPS 卫星，当地球相对恒星自转一周时，它们绕地球运行二周；也就是说它们每 12 恒星时绕地球一周。这样对于地面观测者来说，每天将提前 4min 见到同一颗 GPS 卫星。位于地平线以上的卫星颗数随着时间和地点的不同而不同，最少可见到 4 颗，最多可见到 11 颗。在使用 GPS 信号导航定位时，为了计算观测站的三维坐标，必须观测到至少 4 颗 GPS 卫星，它们称为定位星座。这 4 颗卫星在观测过程中的几何位置分布对定位精度有一定的影响。此外，某地某时甚至不能精确测得观测点的位置坐标，这种时间段称作“间隙段”。但这种时间间隙段很短暂，并不影响全球绝大多部分地区全天候、高精度、连续实时的导航定位测量。GPS 工作卫星的编号和试验卫星基本相同。

2. 地面监控系统

GPS 工作卫星的地面监控系统包括一个主控站、三个注入站和五个监测站。

对于导航定位来说，GPS 卫星是一个动态已知点。卫星的位置是依据卫星发射的星历——描述卫星运动及其轨道的参数算得的。每颗 GPS 卫星所播发的星历由地面监控系统提供。卫星上的各种设备是否正常工作，以及卫星是否一直沿着预定轨道运行，都要由地面设备进行监测和控制。地面监控系统的另一重要作用是保持各颗卫星处于同一时间标准——GPS 时间系统。这就需要地面站监测各颗卫星的时间求出钟差，然后由地面注入站发给卫星，再由卫星将导航电文发给用户的 GPS 信号接收机。

3. GPS 信号接收机

GPS 信号接收机的作用是捕获按一定卫星高度截止角所选择的待测卫星的信号，并跟踪这些卫星的运行，对所接收到的 GPS 信号进行变换、放大和处理，以便测量出 GPS 信号从卫星到接收机天线的传播时间。它可以解译出 GPS 卫星所发送的导航电文，实时地计算出测站的三维位置，甚至三维速度和时间。

GPS 卫星发送的导航定位信号是一种可供广大用户共享的信息资源。对于陆地、海洋和空中的广大用户，只要拥有能够接收、跟踪、变换和测量 GPS 信号的接收设备，即 GPS 信号接收机，就可以在任何时候用 GPS 信号进行导航定位测量。

根据使用目的的不同，用户要求的 GPS 信号接收机也各有差异。目前世界上已有数十家工厂生产 GPS 接收机，产品有数百种。这些产品可以按照原理、用途、功能等来分类。

静态定位中，GPS 接收机在捕获和跟踪 GPS 卫星的过程中固定不变，接收机高精度地测量 GPS 信号的传播时间，利用 GPS 卫星在轨的已知位置计算接收机天线所在位置的三维坐标。而动态定位则是用 GPS 接收机测定一个运动物体的运行轨迹。GPS 信号接收机所位于的运动物体称作载体（如航行中的船只、空中的飞行器、行驶中的车辆等）。载体上的 GPS 接收机天线在跟踪 GPS 卫星的过程中相对地球而运动，接收机用 GPS 信号实时测得运动载体的状态参数（瞬间三维位置和三维速度）。

GPS 接收机硬件、机内软件、GPS 数据的后处理软件包构成了完整的 GPS 用户设备。

GPS 接收机分为天线单元和接收单元两部分。对于测地型接收机来说，两个单元一般分成两个独立的部件，观测时天线单元安置在测站上，接收单元则置于观测站附近的适当位置，用电缆线将两者连接成一个整机。也有的将天线单元和接收单元制作成一个整体，观测时将其安置在观测站点上。

GPS 接收机一般用蓄电池作电源，同时采用机内、机外两种直流电源。设置机内电池的目的是当更换机外电池时不会中断连续观测。在使用机外电池的过程中，机内电池自动充电。关机后，机内电池会自动为 RAM 存储器供电以防止丢失数据。

GPS 技术能够快速、高效、准确地提供点、线、面要素的精确三维坐标及其他相关信息，具有全天候、高精度、自动化、高效益等显著特点，广泛应用于军事、民用交通（船舶、飞机、汽车等）导航、大地测量、摄影测量、野外考察探险、土地利用调查、精确农业及日常生活等不同领域。

GPS 与现代通信技术相结合，使得测定地球表面三维坐标的方法从静态发展到动态，从数据后处理发展到实时的定位与导航，极大地扩展了它的应用广度和深度。载波相位差分法 GPS 技术可以极大提高相对定位精度，在小范围内可以达到厘米级精度。此外，由于 GPS 测量技术对观测点间的通视和几何图形等方面的要求比常规测量方法更加灵活、方便，已完全可以用来观测各种等级的物联网。

目前，全球卫星系统已经有美国的 GPS、欧盟的伽利略卫星定位系统、俄罗斯的格洛纳斯卫星定位系统和中国的北斗卫星定位系统。

如今，随着技术的进步，各种受中国的北斗卫星定位系统支持 5G 智能手机都已经具备了全球卫星导航功能，国内常用的卫星导航软件包括百度地图、高德地图和腾讯地图等。

1.4.7 云计算技术

1. 云计算的概念与特点

云计算（cloud computing）是一种基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展的虚拟化资源。云是网络、互联网的一种比喻。过去往往用云来表示电信网，后来也用它来表示互联网和底层基础设施的抽象。

云计算可以让使用者体验高达每秒 10 万亿次的运算能力，可以用于模拟核爆炸、预测气候变化和市场发展趋势。用户可以通过计算机、手机等方式接入数据中心，按自己的需求进行运算。云计算系统的结构如图 1-9 所示。

云计算让计算分布在大量的分布式计算机上，而非本地计算机或远程服务器上，企业数据中心的运行与互联网更相似。这使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

正如从早期的单台发电机模式转向后来的电厂集中发电的模式，云计算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，使用方便，费用低廉。二者最大的不同在于，它的数据是通过互联网进行传输的。

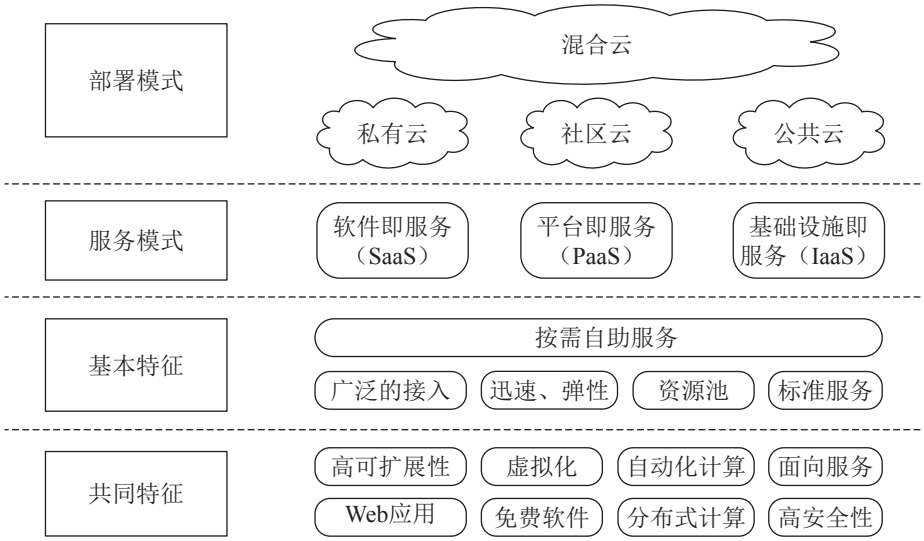

图 1-9　云计算系统的结构

云计算的主要特点如下。

（1）超大规模。“云”具有相当的规模，Google 云计算已经拥有 100 多万台服务器，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数百上千台服务器。“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”，而不是固定的有形的实体。应用在“云”中某处运行，但实际上用户无须了解，也不必担心应用运行的具体位置。只需要一台笔记本计算机或者一部手机，就可以通过网络服务实现需要的一切，包括超级计算这样的任务。

（3）高可靠性。“云”使用数据多副本容错、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更可靠。

（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，可以按需购买;“云”可以像水、电、煤气那样计费。

（7）极其廉价。由于“云”的特殊结构，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须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，还必然提供了存储服务。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。政府机构、商业机构（特别是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。对于信息社会来说，“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云计算用户是保密的，但是对于提供云计算的商业机构来说确实毫无秘密可言。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问题。

2. 云计算的服务

云计算可以提供以下三个层次的服务：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。

（1）基础设施即服务。基础设施即服务（Infrastructure as a Service，IaaS），指消费者通过 Internet 可以从完善的计算机基础设施获得服务。例如，硬件服务器租用。

（2）平台即服务。平台即服务（Platform as a Service，PaaS）实际上指将软件研发的平台作为一种服务，以 SaaS 的模式提交给用户。因此，PaaS 也是 SaaS 模式的一种应用。但是，PaaS 的出现可以加快 SaaS 的发展，尤其是加快 SaaS 应用的开发速度。例如，软件的个性化定制开发。

（3）软件即服务。软件即服务（Software as a Service，SaaS）是一种通过 Internet 提供软件的模式，用户无须购买软件，而是向提供商租用基于 Web 的软件来管理企业经营活动。例如，阳光云服务器就是一种 SaaS 应用。

1.4.8 中间件技术

国际数据中心对中间件的定义：“中间件（middleware）是一种独立的系统软件或服务程序，分布式应用软件借助中间件在不同的技术之间共享资源。中间件位于客户机、服务器的操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件”。对于相连接的系统，即使它们具有不同的接口，但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递。通过中间件，应用程序可以工作于多平台或多操作系统（Operating System，OS）环境。

中间件是一类连接软件组件和应用的计算机软件，它包括一组服务，以便于运行在一台或多台机器上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进，该架构通常用于支持并简化那些复杂的分布式应用程序。它包括 Web 服务器、事务监控器和消息队列软件。

中间件处于操作系统、网络和数据库之上，应用软件之下，为处于自己上层的应用软件提供运行与开发环境，帮助用户灵活、高效地开发和集成复杂的应用软件。

国际数据中心关于中间件的定义表明，中间件是一类软件，而非一种软件；中间件不仅仅实现互连，还实现应用之间的互操作；中间件是基于分布式处理的软件，最突出的特点是其网络通信功能。

具体地，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统一的开发环境，降低了程序设计的复杂性。程序开发人员可以将注意力集中在自己的业务上，不必再为程序在不同系统软件上的移植而重复工作，从而大大减少了技术上的负担。

中间件带给应用系统的，不只是开发的简便、开发周期的缩短，也减少了系统维护、运行和管理的工作量，还减少了计算机总体费用的投入。

由于标准接口对于可移植性和标准协议对于互操作性的重要性，中间件已成为许多标准化工作的主要部分。对于应用软件开发，中间件远比操作系统和网络服务更为重要，中间件提供的程序接口定义了一个相对稳定的高层应用环境，不管底层的计算机硬件和系统软件怎样更新换代，只要将中间件升级更新，并保持中间件对外的接口定义不变，应用软件几乎不需任何修改，从而保护了企业在应用软件开发和维护中的重大投资。

基于中间件的物联网终端体系结构如图 1-10 所示。

图 1-10　基于中间件的物联网终端体系结构

中间件大致可以分为六类：终端仿真 / 屏幕转换中间件、数据访问中间件、远程过程调用中间件、消息中间件、交易中间件、对象中间件。

物联网终端主要由传感器模组、主控模组和通信模组组成。中间件主要加载在主控模组上，这样可以加强终端管理功能。中间件对终端提供统一的接入规范，在通信层面屏蔽不同终端和外设传输协议的差异，从而实现标准化。

通过中间件可以实现物联网终端业务的灵活扩展，与业务需求完全独立实现，可以为物联网终端协议增加或删除协议栈。

1.5　物联网系统的安全特征

物联网系统安全，指物联网系统可以连续地、可靠地和正常地运行，服务不会中断，物联网系统中的软件、硬件和系统中的数据受到保护，不受人为的恶意攻击、破坏和更改。

感知信息的多样性、网络环境的复杂性和应用需求的多样性，使物联网安全面临新的严峻的考验。信息和网络安全的目标是保证被保护信息的机密性、完整性和可利用性。物联网以数据为中心且与应用密切相关，这一特征决定了物联网总体安全目标要达到机密性，避免攻击者读取机密信息；物联网系统应具有数据鉴别能力，避免节点被注入虚假信息；物联网系统应具有设备鉴别能力，避免非法设备接入物联网；物联网系统应保证数据完整性，校验数据是否被修改；物联网系统还应具有可用性，保证系统的网络服务无论在任何时间都可以提供给合法的用户。

1.5.1 传统网络面临的安全威胁

物联网是基于互联网技术将设备连接起来的一个综合性网络，因此，互联网技术是物联网的基础，互联网的安全直接关系到整个物联网的安全。互联网安全问题涉及网络设备基础安全、网络安全、Web 安全和基于 Web 应用的安全等各个方面，包括编码安全、数据帧安全和密钥管理与交换等。

1. 编码安全

由于任意一个标签的标识或识别码都能被远程主机任意地扫描，标签可能会自动地、不加区分地回复读写器的指令，并且将其所存储的信息传输给读写器，因此编码的安全性必须引起重视。

2. 数据帧安全

由于在互联网信息传输环境下，攻击者可能会窃听和截取数据帧的内容，获取相关的信息，并为进一步攻击做准备，因此必须重视数据帧的安全。

3. 密钥管理与交换

在互联网中实施的机密性和完整性措施，关键在于密钥的建立和管理过程，由于物联网中节点的计算能力和电源供给能力等有限，因此传统的密钥管理方式不适用于物联网。

1.5.2 物联网面临的安全威胁

根据物联网本身的特点，物联网除了面临传统网络的安全问题以外，还存在着一些有别于现有互联网安全的特殊安全问题。这是因为物联网是由大量的传感器等设备构成的，缺少人对设备的有效监控，并且物联网设备种类繁多、数量庞大。

1. 点到点消息认证

由于物联网可以代替人完成一些复杂、危险和机械的工作，物联网传感器和设备往往部署在无人监控的场景中，因此攻击者可以轻易接近这些设备，从而对它们进行破坏，甚至通过本地操作更换机器的软硬件，使得物联网中可能存在大量的恶意节点和已经损坏的节点。

2. 重放攻击

在物联网的标签体系中，无法证明信息已经传递给读写器，攻击者可以获得已认证的身份，从而获得相应的服务。

3. 拒绝服务攻击

一方面，物联网以域名服务（Domain Name Service，DNS）技术为基础，同样继承了 DNS 技术的安全隐患；另一方面，由于物联网中节点数量庞大且以集群方式布置，因此在传输数据时，大量机器的数据传输会引发网络拥塞，形成拒绝服务攻击。另外，攻击者广播 Hello 信息，或者利用通信机制中的优先级策略、虚假路由等协议安全漏洞，同样可

以发起拒绝服务攻击。

4. 篡改或泄露标签数据

攻击者一方面可以破坏标签数据，使得物品服务无法正常使用；另一方面可能会窃取标签数据，获得相关的服务，为进一步攻击做准备。

5. 权限提升攻击

攻击者可以通过协议漏洞或物联网的其他脆弱环节，获得高级别服务，甚至控制物联网其他节点的运行。

6. 业务安全

传统的认证是区分不同层次的，例如，网络层的认证负责网络层的身份鉴别，业务层的认证负责业务层的身份鉴别，二者独立存在。然而在物联网体系中，在多数情况下，设备都有专门的用途，其业务应用与网络通信紧密地捆绑在一起。由于网络层的认证是必不可少的，因此业务层的认证机制就不再是必需的，而是根据业务由谁来提供和业务的敏感程序来设计。

7. 隐私安全

在物联网系统中，每一个人包括其拥有的每一个物品都将随时随地连接到网络上，随时随地被感知，在这样的网络环境下，如何确保信息的安全性和隐私性，防止个人信息、业务信息和物品丢失或被他人盗用，将是物联网发展过程中需要解决的技术难题之一。

1.5.3　物联网系统的安全特征

物联网系统除了面临传统网络安全威胁以外，还具有一些特殊的安全问题。从物联网的信息处理过程来分析，感知信息经历了采集、汇聚、融合、传输、决策和控制等过程，整个信息处理的过程体现了物联网安全的特征和要求。因此，物联网安全与传统网络安全存在较大的差别。

物联网系统的安全特征如图 1-11 所示。

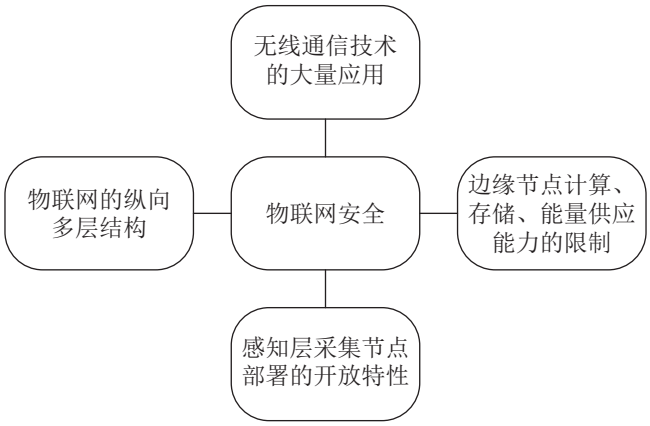

图 1-11　物联网系统的安全特征

1. 设备、节点无人看管，容易受到黑客操纵

物联网常用来替代人完成一些复杂、危险和机械的工作。在这种工作环境下，物联网中的设备、节点均无人看管。因此，攻击者很容易就能接触到这些设备，从而对设备或者嵌入其中的传感器节点进行破坏。攻击者甚至可以通过更换设备的软硬件，对物联网进行非法操控。例如，在远距离电力输送过程中，供电企业可以使用物联网来远程操控一些供电设备。由于缺乏看管，攻击者有可能使用非法装置来干扰这些设备上的传感器。假如供电设备的某些重要工作参数被篡改，其后果不堪设想。

2. 信息传输主要靠无线通信方式，信号容易被窃取和干扰

物联网的信息传输中一般采用无线传输方式，暴露在空中的无线电信号很容易成为攻击者窃取和干扰的对象，这会对物联网的信息安全产生严重的威胁。例如，目前的第二代身份证都嵌入了 RFID 标签，在使用过程中，攻击者可以通过窃取、感知节点发射的信号来获取所需要的信息，甚至是用户的隐私信息，并据此来伪造身份，其后果非常严重。又如，攻击者可以在物联网无线信号覆盖区域内，通过发射无线干扰信号，使无线通信网络无法正常工作，甚至瘫痪。再如，在物流运输过程中，嵌入物品中的标签或读写设备的信号受到恶意干扰时，很容易造成一些物品丢失。

3. 基于低成本的设计，传感器节点通常是资源受限的

在物联网的实际应用中，通常需要部署大量的传感器，以充分覆盖特定区域。对于已经部署的传感器，一般不会进行回收或维护。因为具有数量多和一次性的特点，传感器必须具有较低的成本，只有这样，大规模使用才可行。为了降低成本，传感器通常是资源受限的。传感器一般体积较小，而且能量、处理能力、存储空间、传输距离、无线信号频率和带宽等都是受限的。由于上述原因，传感器节点无法使用比较复杂的安全协议，因此传感器设备或节点无法拥有较强的安全保护能力。攻击者针对传感器的这一弱点，可以采用连续通信的方式来使节点的能量耗尽。

4. 物联网中的物品的信息能够被自动地获取和传送

物品的感知是物联网应用的前提。物品与互联网相连接后，通过射频识别（RFID）、传感器、二维识别码和全球卫星定位等技术能够随时随地且自动地获取物品的信息。因此，人们随时随地都可以获取物品的准确位置和周围环境等相关信息。在物联网的应用中，RFID 标签可以被嵌入到任何物品中。一旦 RFID 标签被嵌入到人们的生活用品中，如嵌入到帽子或衣服中，而使用者并没有察觉，那么物品的使用者将会被定位和跟踪，这无疑会对个人的隐私构成极大的威胁。

5. 物联网在原有的网络基础上进行了延伸和扩展

物联网是在互联网基础上的延伸和扩展。物联网覆盖的范围更加广泛，涵盖无处不在的数据感知、以无线信号为主的信息传输、智能化的信息处理和广泛的应用，用户端可以延伸和扩展到任何物品与物品之间。因此物联网安全的设计、部署和管理更为困难。

1.6　物联网安全体系结构

物联网安全的总体需求是物理安全、信息采集安全、信息传输安全和信息处理安全的综合，物联网安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性。

结合物联网的分布式连接和管理（Device Connect Manage，DCM）模式，可以得出物联网的安全体系结构，如图 1-12 所示。

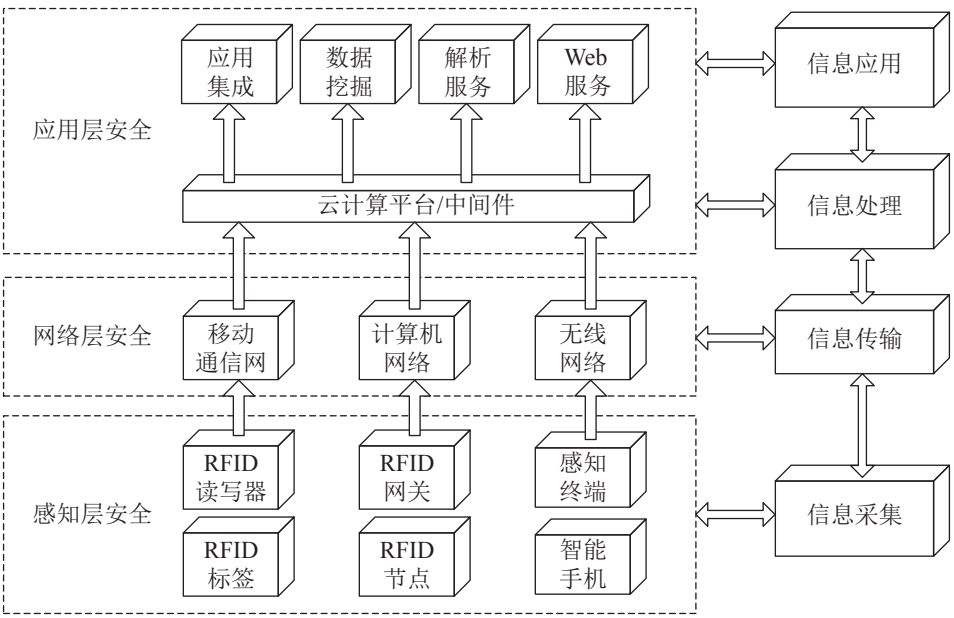

图 1-12　物联网安全的体系结构

正如前面所述，物联网的三个基本特征是全面感知、可靠传输和智能处理。

虽然人们对物联网的概念有多种不同的描述，但其内涵基本相同。因此，在分析物联网安全性时，也相应地将其分为三个层次，即感知层安全、网络层安全和应用层安全。在物联网的综合应用方面，应用层是对智能处理后的信息的利用。尽管在某些物联网安全框架中，将信息处理安全与信息应用安全分开进行分析，但是从物联网系统的整体信息安全角度考虑，将二者的安全问题统一到应用层，更容易建立物联网安全体系结构。

1.7　感知层安全分析

物联网感知层的任务是实现智能感知外界信息的功能。感知层也称为原始信息收集层，包括信息采集、信息、捕获和物体识别。该层的典型设备包括射频识别装置、各类传感器（如红外、声音、温度、湿度、速度等）、图像捕捉装置（摄像头）、卫星导航系统（GPS、北斗卫星导航系统等）、激光扫描仪、环境检测仪和地震监测仪等。这些设备所收集的信息一般都具有明确的目的，所以在传统观念中这些信息直接被处理并进行应用。例如，公路边摄像头捕捉的视频信息直接用于交通监控。然而，在物联网应用中，多种类型的感知信息可能会同时处理，综合应用，甚至不同感应信息的结果会反馈给控制方，产生控制和调节行为。例如，湿度传感器收集到的湿度信息，可能会导致温度或光照程度的调

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。又如，交通监控的录像信息可能同时被用于公安侦破、城市规划、环境监测等领域。因此，由什么部门来统一处理这些信息将直接影响应用的有效性。为了使这些信息能够被不同的应用领域共同分享并有效使用，应该有一个综合物联网信息处理平台，这就是物联网的智能应用层。物联网感知的所有信息，都需要传输到该信息处理平台中。

物联网的安全状况，主要体现在其体系结构的各个要素中。首先，是物联网的物理安全，主要是各类传感器的安全，包括对传感器的干扰、屏蔽、电磁泄漏攻击、信道攻击等；其次，是物联网的运行安全，主要是各个计算模块的安全，如嵌入式计算模块、服务器计算中心的安全等，包括密码算法的实现、密钥管理（软件或硬件所存储的密钥）、数据接口和通信接口管理等，涉及传感器节点、数据汇聚节点和数据处理中心；最后，是物联网的通信安全，即数据在传输过程中的安全保护，确保数据在传输过程中不会被非法窃取、篡改和伪造。

根据物联网感知层安全所涵盖的内容，可以把物联网的感知层分为两大类，即 RFID 系统和无线传感器网络。以下分别对这两类网络的安全技术进行分析。

1.7.1 RFID 系统安全分析

1. RFID 系统在安全防护方面的优势

RFID 系统是一种电子身份识别系统，性质相当于条形码或二维码，但是功能却比条形码和二维码更强大。RFID 不仅提供电子身份标识，而且具有少量的计算处理能力，因此在安全防护方面，RFID 系统有着条形码和二维码不可比拟的优势。

RFID 系统一般包括一个或多个 RFID 电子标签，一个或多个读写器和一个后台数据库。读写器通过与后台数据库的交互，判断标签所提供的数据是否真实，RFID 标签也可以通过一些安全机制识别试图读取数据的读写器是否合法。RFID 标签与读写器之间的通信距离很短。尤其是无源标签，通常与读写器之间的通信距离只有几十厘米。而有源标签与读写器之间的通信距离，通常也仅有几十米，而且在很短的时间内就可以完成数据通信。

2. RFID 系统面临的安全问题

RFID 系统与无线传感器网络有着本质的区别。无线传感器网络传输的是采集到的环境信息，包括传感器自己的身份信息，而 RFID 标签传输的仅是身份标识信息。从表面上看，似乎 RFID 系统的工作机制要简单得多，然而实际情况却并非如此。原因是 RFID 系统面临着以下安全问题。

（1）非法复制。对于条形码或者二维码，非法复制非常容易实现，而 RFID 系统同样也会面对非法复制问题，但是 RFID 系统应有能力对抗非法复制。

（2）非法跟踪。非法读写器可能试图对合法的 RFID 标签进行访问，以获取合法 RFID 标签的身份标识，从而判断该标签是否与在其他位置读取的 RFID 身份信息属于同一个标签。这种攻击的目的在于对某些标签实施跟踪。

（3）近距离攻击。攻击者同时使用一对非法的 RFID 标签和读写器来实施攻击。首先

使用非法的读写器接近一个合法的 RFID 标签，然后将该合法标签的数据传给远方的非法标签。该非法标签试图接近一个合法读写器，将非法读写器传来的信息发送给它，并将该合法读写器返回的任何信息传给远方的非法读写器返回给它所接近的合法标签。通过这种攻击方式，将远处的合法标签与合法读写器连接起来，看起来就像二者在真正地交互一样，从而试图通过认证。这种攻击行为是近年来提出的，其目的是通过 RFID 标签非法进入物联网系统。

RFID 标签的主要用途是识别某个账户或者某个物品，并且能够在数据库中记录该账户或该物品的相关信息。非法复制是攻击者希望实现的，通过一些密码技术和物理保护措施可以有效防止非法复制，至少可以使非法复制的成本大大提高；即使不能非法复制，追踪 RFID 标签也是一种重要的攻击手段。因此，隐私保护是 RFID 系统安全的重要部分。此外，近年来提出的近距离攻击也对 RFID 系统安全提出了新的挑战。

3. RFID 系统安全技术

针对以上所描述的 RFID 系统的安全问题，其安全技术可以归纳如下。

（1）信息加密技术。通过信息加密技术，将 RFID 标签的机密信息存储在一个抗破解的硬件区域，可以有效地防止标签复制。同时，RFID 标签与读写器之间的信息交互过程也需要精心设计，否则在信息交互过程中可能出现信息泄露。

（2）身份隐私保护技术。通过加密措施，使标签提供给读写器的标识数据每次都产生变化，掌握机密信息的数据库可以识别该标签，但是非法截获数据的攻击者则无法识别这些不同的身份标识之间是否存在关联，这样就避免标签被非法读写器识别，从而提供隐私保护机制。

（3）抗近距离攻击技术。近年来，研究者们针对近距离攻击技术提出了许多解决方案，但是这些方案需要经过较长时间的实践考验，才能确认是否可行，因此针对这种攻击行为的研究尚停留在实验室阶段。

1.7.2　无线传感器网络安全分析

当感知信息从传感器采集以后但尚未传输到网络层之前，可以把传感器网络本身（由各种传感器构成的网络）看作感知的部分。感知信息的传输要通过一个或多个与外部网络相连接的传感节点，这些节点称为网关（gateway）节点或汇聚（sink）节点。所有与传感网内部节点的通信，都需要经过网关节点与外部网络联系。因此，在物联网的感知层，仅需要分析无线传感器网络本身的安全性。

1. 无线传感器网络面临的安全威胁

典型的传感器网络是无线传感器网络，解决传感器网络安全的目标也应针对无线传感器网络，因为适合无线传感器网络的安全技术对有线传感器网络同样适用。下面分别对无线传感器网络所面临的常见安全威胁进行分析。

（1）遭受非法用户的入侵。

无线传感器网络最容易遭受的是非法用户的入侵，即使入侵失败，攻击者反复地尝试入侵的过程，也可以造成对传感器节点的拒绝服务攻击。原因是无线传感器终端节点的资

源有限，特别是采用电池供电的传感器节点，在不断对攻击者进行认证的过程中将会产生大量额外的功耗，从而造成电能耗尽。另外，在接收入侵请求的过程中，也可能造成自身计算超负荷而导致拒绝服务攻击。对于汇聚节点，通常在能耗上没有太多的限制，绝大多数汇聚节点都可以保证电能的供应，但是由于其设计目标是服务于少数传感器节点的，并且每一个传感器节点与汇聚节点之间的通信量一般都有限，因此汇聚节点应对拒绝服务攻击的能力很弱，在拒绝服务攻击下很容易导致计算资源耗尽。有时候，造成网络服务器受到攻击的原因不一定是拒绝服务攻击，可能是入侵尝试过程造成的拒绝服务攻击。当物联网被接入互联网，成为物联网系统的一部分时，受到拒绝服务攻击的概率将会大幅提高。因此，感知层能否抵抗拒绝服务攻击，应作为一个物联网系统是否健康的重要指标，这也是物联网安全所面临的重要挑战。

（2）被攻击者非法捕获。

由于无线传感器网络所处的环境一般都具有公开性，因此容易被攻击者非法捕获。最容易捕获的是传感节点发出的信号，不需要知道它们的预置密码和通信密码，只需要鉴别传感节点的种类即可。例如，检查传感节点是用于检测温度还是用于检测噪声等。有时候这种分析对攻击者也很有用。因此，安全的传感器网络应该具有保护其工作类型的安全机制。

（3）被攻击者剖析密钥。

攻击者不仅可以捕获无线传感器数据，而且可以捕获无线传感器网络的物理实体，然后进行离线分析。例如，将数据带回实验室进行深入剖析，这样就有可能得到传感器所用的密钥信息，从而恢复该传感器之前的所有通信数据，甚至非法复制传感器，添加到无线传感器网络上发送虚假数据。

（4）对汇聚节点的攻击。

攻击者对无线传感器网络更为严重的攻击是对汇聚节点的攻击。如果攻击者能够控制汇聚节点，则不仅能得到所有该汇聚节点所服务的传感节点所上传的数据，而且可以任意制造虚假数据，甚至蒙骗数据处理中心和感知终端。攻击者对汇聚节点的安全性分析，不一定需要到实验室进行硬件剖析，更多的是根据传感器网络所使用的认证安全技术，通过协议漏洞和其他方面可能的漏洞分析，找到成功入侵的机会。一旦入侵成功，就可以对汇聚节点实施所有可能的攻击，如解密数据、捏造虚假数据等，并有可能导致服务器端的混乱。

2. 无线传感器网络的安全技术

针对以上所描述的安全威胁，无线传感器网络的安全技术可以归纳如下。

（1）节点认证。这主要包括普通传感器节点之间、普通传感器节点与汇聚节点之间的单向和双向认证，从而确保信息的来源和去向正确，防止假冒攻击。

（2）消息机密性。消息机密性主要指保护数据不被非法截获者获知。在实施过程中，需要考虑密钥管理问题。在无线传感器网络中使用公钥系统是不现实的，因为公钥系统所消耗的计算资源过多，而且公钥基础设施在传感器网络中无法运转。假如使用对称密钥，无论是给每一个传感节点赋一个单独的密钥，还是让一个传感器网络内的所有节点共享一个预置密钥，都是现实中需要考虑的问题。

（3）数据完整性。数据完整性指保护传输的数据不被非法修改，同时可以有效地拒绝攻击者制造的假信息。

（4）数据新鲜性。在互联网中数据的新鲜性保障不是很强，在无线传感器网络中则需要保障数据的新鲜性。一方面，传感器上传的数据具有很高的时效性甚至实时性；另一方面，从数据中心传给传感节点的消息通常都是重要的控制指令，如果仅仅保证机密性和完整性，并不能完全满足要求。因为简单的重放攻击可以通过消息机密性和数据完整性验证，可能造成很大的问题，例如，控制开关的开启或者关闭指令的重放，就有可能导致非常严重的后果。

（5）安全路由。安全路由在一些无线传感器网络中非常重要，但并不是所有的无线传感器网络都需要安全路由。许多物联网无线传感器网络根本就不需要路由，感知节点可以直接将感知数据传送给汇聚节点。

（6）密钥管理。尽管无线传感器网络大多使用对称密钥技术，但是在资源有限的环境下，对密钥的有效和安全管理同样具有技术挑战性。在汇聚节点和感知终端节点使用同一个密钥，虽然有利于物联网系统的搭建，但是只要攻击者控制传感器网络中任意一个感知节点，则整个无线传感器网络将不再具有安全性；如果在每个感知节点使用不同的密钥，则会增加汇聚节点的计算工作量，因为汇聚节点需要管理所有节点对应的密钥。此外，汇聚节点处于相对公开的环境，容易遭受入侵甚至物理攻击，因此这些与感知节点共享的密钥，无论是长期保存还是临时存放，都是对物联网安全技术的挑战。

（7）抗拒绝服务攻击。拒绝服务攻击并不是互联网独有的，在无线传感器网络中实施拒绝服务攻击更加容易。每当出现某个访问请求时，接收节点就对该请求进行一系列的认证，许多同类请求导致许多次重复认证，对一个处理能力不强的汇聚节点来说，很容易造成计算超出负荷，从而导致拒绝服务；对于计算能力更弱的一个普通传感节点来说，则更容易导致瘫痪，甚至电能耗尽。对于传感节点来说，对抗拒绝服务攻击的有效手段是采取适当的睡眠机制。但是对于汇聚节点来说，睡眠机制是否有效还有待进一步的研究。

1.7.3　感知层安全机制

在物联网感知层，需要提供消息机密性、数据完整性和认证等安全机制，然而物联网感知层的感知节点受资源所限，常常只能执行少量的计算和通信任务。特别地，对于一些资源非常受限的感知节点（包括 RFID 标签），如何提供所需要的安全机制面临着诸多技术挑战。为此，针对物联网感知层的安全，需要轻量级加密算法和轻量级安全认证协议。

1. 轻量级加密算法

随着移动电子设备的普及和 RFID、无线传感器网络等技术的发展，越来越多的应用需要解决相应的安全问题。但是，相对于传统的台式和高性能计算机，移动设备的资源环境通常有限，存在计算能力较弱、计算时可以使用的内存空间较少、能耗有限的问题。传统的加密算法并不能很好地应用于这种环境，这样就使得资源受限环境下加密算法的研究成为当前的一个热点。适用于资源受限环境下的加密算法称为轻量级加密算法。

轻量级加密算法与传统加密算法互相促进，互相影响。一方面，传统加密算法为轻量

级加密算法的设计与安全性分析提供了理论依据和技术支持；另一方面，轻量级加密算法的“轻量级”特点，使传感器网络的安全性分析能够更加深入、全面地展开。在这个过程中，可能会出现新的问题，从而促进加密算法和安全技术的发展。

物联网的感知层安全需要轻量级加密算法，以适应资源受限的感知节点的环境需求。然而，到底什么是轻量级并没有严格的定义，也很难给出严格的定义。根据国际 RFID 标准委员会的规定，RFID 标签需要留出 2000 个门电路和相当的硬件资源用于加密算法的实现。因此，研究者通常把轻量级加密算法定义为那些在 2000 个门电路硬件资源之内可以实现的加密算法。准确地说，2000 个门电路硬件资源仅仅是一个供参考的性能技术指标，实际上，轻量级加密算法允许有不同的性能技术指标，某些传感节点对硬件资源的限制可能更为苛刻，而另一些传感节点则允许使用更多的硬件资源。

基于物联网技术的发展，近年来轻量级加密算法引起了业界的广泛关注。轻量级加密算法逐步从实验室迈向实用阶段。轻量级加密算法设计的关键问题是处理安全性、实现代价和性能之间的平衡。有些研究者针对已有的标准分组密码算法，如 AES 算法和 IDEA 算法等，进行高度优化并面向硬件资源尝试简化实现，希望将硬件资源需求降低到 RFID 系统所允许的范围之内，然而效果并不理想；有些研究者对传统加密算法稍做修改，使其适用于轻量级环境，例如，在 DES 算法的基础上对 S 盒加以改进产生了 DESL 算法；还有些研究者提出一些专门为低资源环境设计的分组加密算法，如 PRESENT 算法和 CLEFIA 算法等。

虽然目前已经提出了许多种轻量级加密算法，但是其安全性和可靠性还有待时间考验。KATAN 密码在发表之后不到两年的时间就已经被破译，还有一些轻量级加密算法的整体结构和算法设计有待进一步优化。因此，轻量级加密算法的商业化应用可能还需要一些时间，尤其是对轻量级加密算法的标准化需要谨慎对待，因为标准化后的轻量级加密算法可能无法适应众多感知环境的需求。

2. 轻量级认证技术

认证技术通过基础服务设施的形式将用户身份管理与设备身份管理关联起来，以实现物联网中所有人员和接入设备的数字身份管理、授权、追踪，以及传输消息的完整性保护，这是整个物联网的安全核心和命脉。

轻量级认证技术可以分为两类，一类是对消息本身的认证，通常使用消息认证码，目的是提供消息完整性认证，使得接收方能够验证消息是否在传输过程中被修改；另一类是认证协议，用于对通信双方身份的确认，通常使用挑战 – 应答协议。身份认证协议通常伴随着会话密钥的建立，在移动通信中的认证协议称为 AKA（Authentication and Key Agreement）协议。

1.8 网络层安全分析

1.8.1 网络层面临的安全挑战

物联网的网络层主要用于把感知层收集到的信息安全可靠地传输到应用层，然后根据不同的应用需求进行信息处理，即网络层主要提供信息传输所用的网络基础设施，包

括互联网、移动通信网和一些专用网络。在信息传输过程中，可能需要在一个或多个不同架构的网络中进行信息交换。例如，手机与固定电话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。在传统的信息传输过程中，跨越不同类型网络的信息传输很常见，在物联网环境下，这种传输方式变得更为典型，并且很可能在传输过程中产生信息安全隐患。

物联网网络层涉及移动通信网、国际互联网和无线网络等多种网络环境。

移动通信网的发展早已超越了提供语音服务的原始用途。以智能手机为代表的移动设备的普及，也给移动通信网不断地提出新的需求。目前移动通信网所提供的服务主要包括移动互联网、多媒体服务、互动游戏、网络聊天等。因此，对移动通信网的攻击也远远超越了窃听语音的范围。

在物联网中，当前的 IPv4 网络和下一代的 IPv6 网络都是物联网信息传输的核心载体，绝大多数信息要经过互联网传输。传统的互联网受到的拒绝服务攻击（DoS 攻击）和分布式拒绝服务攻击（DDoS 攻击）依然存在，因此需要有更好的防范措施和灾难恢复机制。由于物联网所连接的终端设备的性能和对网络的需求存在着巨大差异，抵抗网络攻击的能力也存在很大差别，因此很难设计通用的安全方案，需要针对不同的网络安全需求采取不同的解决方案。

物联网中感知层所获取的感知信息通常由无线传感器网络传输到系统，与互联网相比，恶意程序在无线网络环境和传感器网络环境下有很多入口。对这些暴露在公共场所之中的信息，如果不进行合适的保护，就很容易被入侵。例如，类似蠕虫病毒的恶意代码一旦入侵成功，其隐蔽性、传播性和破坏性等就更加难以防范，将直接影响物联网系统的安全性。物联网建立在互联网基础之上，对互联网高度依赖，在互联网中存在的各种危害信息安全的因素，在一定程度上同样也会对物联网造成危害。随着物联网的发展，病毒攻击、黑客入侵、非法授权访问等都会对物联网用户造成损害。

总之，传统的互联网网络环境遭遇到前所未有的安全挑战，而物联网网络层所处的网络环境也同样存在安全隐患。与此同时，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方面面临着更大的挑战。

1.8.2　网络层安全分析

在网络层，异构网络的信息交换将成为安全性的脆弱点，尤其是在网络认证方面，难免出现中间人攻击和其他类型的攻击。针对这些攻击，需要有更高层的安全防护措施。如果仅仅考虑互联网、移动网络及其他专用网络，物联网网络层对安全的需求可以概括如下。

（1）数据机密性。数据机密性，指网络层需要保证数据在传输过程中不泄露其内容。

（2）数据完整性。数据完整性，指网络层需要保证数据在传输过程中不被非法篡改，或者非法篡改的数据很容易被检测出来。

（3）数据流机密性。数据流机密性，指在网络层，需要对数据流进行保密。

（4）分布式拒绝服务攻击的检测与预防。物联网网络层需要解决如何对脆弱节点的分布式拒绝服务攻击进行防护。

（5）跨区域、跨网络认证机制。该机制包括不同无线网络所使用的跨区域认证、跨网络认证机制。

1.8.3 网络层的安全机制

物联网网络层的安全机制，可以分为端到端的机密性和节点到节点的机密性两种类型。

端到端的机密性，需要建立以下安全机制：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择机制等。在这些安全机制中，可以按需增加数据完整性服务。

节点到节点的机密性，需要用到节点间的认证和密钥协商协议，这一类协议要重点考虑效率因素。机密性算法的选择和数据完整性服务，可以根据需求选取或省略。由于存在跨网络架构的安全需求，因此需要建立不同网络环境的认证衔接机制。此外，根据应用层的不同需求，网络传输模式又可分为单播通信、组播通信和广播通信。针对不同类型的通信模式，也应具备相应的认证机制和机密性保护机制。

1.9 应用层安全分析

1.9.1 云计算平台

1. 云计算平台概述

物联网应用层的任务就是对感知数据进行处理与应用。从物联网的行业应用方面分析，应用层必须是具有一定规模的信息处理中心和应用平台，否则无法支撑物联网的各种行业应用。为了支持物联网产业的发展，目前许多国家和地区都建立了自己的云计算平台，因此物联网应用层的安全机制主要是针对云计算平台来说的。

作为物联网应用层基础设施的云计算平台，应当具有处理海量数据的能力。云计算平台除了需要具有强大的信息处理能力以外，还必须具有备份和抗击灾害等能力；云计算平台应能够应对大量不同用户的访问，而这种访问不同于普通的网站访问，需要为用户提供私有数据空间和私有计算处理能力，因此虚拟化成为云计算的典型特征；云计算平台将难免遭受各类网络攻击和系统安全的威胁，因此云计算平台还必须具有抗攻击和抗病毒的能力。

2. 云计算面临的安全挑战

云计算的重要特征是智能，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快捷，而非智能的处理手段可能无法应对海量数据。但是在自动处理过程中，对恶意数据特别是恶意代码的判断能力有限，而智能也仅限于按照一定规则进行过滤和判断，因此攻击者很容易避开这些规则。例如，对于垃圾电子邮件的过滤就是一个多年无法彻底解决的棘手问题。制定防御规则时需要考虑尽可能多的攻击手段，而攻击者只需要应对已知的规则。云计算面临的安全挑战主要包括以下几方面。

（1）来自超大量终端的海量数据的识别和及时处理。

（2）智能是否会被敌方利用。

（3）自动是否会变为失控。

（4）灾难控制和恢复能力。

（5）如何杜绝非法攻击。

由于在物联网时代需要处理的信息是海量的，云计算平台也是分布式的，因此当不同性质的数据通过一个云计算平台处理时，这个云计算平台需要多个功能各异的处理平台协同处理。但是首先应该知道将哪些数据分配到哪个处理平台，因此数据的分类是必需的。同时，基于安全性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。

3. 云计算平台的安全机制

云计算技术的智能处理过程与人类的智能相比仍存在本质的区别，但是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。因此，基于物联网环境的云计算技术，在智能处理的水平上有望不断提高。换言之，只要智能处理过程存在，就有可能让攻击者躲过智能处理的识别和过滤，从而达到攻击的目的。因此，物联网云计算平台需要具备高智能的处理机制。

如果智能水平很高，那么就可以有效识别并自动处理恶意数据和指令。但是再好的智能也会存在失误的可能，特别是在物联网环境下，即使失误概率非常小，但由于自动处理过程的数据量非常庞大，失误的情况还是难以避免。在处理发生失误而使攻击者成功入侵后，如何将攻击所造成的损失降到最低，并尽快使系统从灾难中恢复到正常工作状态，是物联网智能应用层需要解决的另一个重要问题。

云计算虽然使用智能的自动处理手段，但是同样允许人工干预，而且人工干预在某些时候是必需的。人工干预可能发生在智能处理过程中无法做出正确判断的时候，也可能发生在智能处理过程中出现关键性中间结果或最终结果的时候，还可能发生在出于任何其他原因而需要人工干预的时候。人工干预的目的是使应用层更好地工作。此外，由于来自于人的恶意破坏行为具有很大的不可预测性，因此针对人类的恶意破坏行为，除了采用技术手段以外，还需要依靠严格和科学的管理手段。

为了实现物联网云计算的安全需求，需要提供以下安全机制。

（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。

（4）密文查询、秘密数据挖掘、安全云计算技术。

（5）可靠和高智能的处理能力。

（6）抗网络攻击，具有入侵检测和病毒检测能力。

（7）恶意指令分析与预防、访问控制及灾难恢复机制。

（8）保密日志跟踪和行为分析、恶意行为模型的建立机制。

（9）具有数据安全备份、数据安全销毁及流程全方位审计能力。

（10）移动设备的识别、定位和追踪机制。

1.9.2 应用层行业应用安全分析

物联网应用层行业应用针对的是某个具体行业的综合性或者个性化的应用业务。行业应用所涉及的安全问题，仅仅通过感知层、网络层、应用层这三层的安全解决方案，仍然有可能无法解决。在这些安全问题中，隐私保护就是一个典型的应用需求。无论是感知层、网络层还是应用层，都没有涉及隐私保护问题，但是它却是物联网特殊应用环境下的实际需求，即应用层的特殊安全需求。其次，物联网的数据共享分多种情况，涉及不同权限的数据访问。最后，物联网应用层还涉及知识产权保护、计算机数据取证、计算机数据销毁等安全需求及相关技术。

1. 应用层行业应用面临的安全挑战

物联网应用层的安全需求和安全挑战主要来自以下几方面。

（1）根据不同访问权限对同一数据库的内容进行筛选。

（2）提供用户隐私信息保护，同时又能正确认证。

（3）解决信息泄露和追踪问题。

（4）进行计算机数据取证。

（5）销毁计算机数据。

（6）保护电子产品和软件的知识产权。

物联网需要根据不同的应用需求给共享数据分配不同的访问权限，并且不同权限访问同一数据时可能得到不同的结果。例如，当道路交通监控视频数据用于城市规划时仅需要很低的分辨率，因为城市规划仅需要了解交通拥塞的大致情况；而监控视频用于交通管制时分辨率需要清晰一些，因为交通管制需要准确地了解交通实际情况，及时发现究竟哪里发生了交通事故，以及交通事故的基本情况等；当监控视频用于公安侦查时可能需要更高的分辨率，以便看清楚嫌疑人的身材和外貌，或者识别汽车牌照等信息。因此，如何以安全方式处理信息是物联网应用中的一项挑战。

在很多情况下，用户信息是认证过程中的必需信息，如何为这些信息提供隐私保护，是一个必须解决的安全问题。

随着商业信息和个人信息的网络化，越来越多的信息被认为是用户隐私信息。需要隐私保护的场景至少应包括以下几种。

（1）移动用户既需要知道自己的位置信息，又不希望非法用户获取该信息。

（2）物联网用户既需要证明自己合法使用某种业务，又不希望别人知道自己在使用这种业务，如金融交易、在线游戏等。

（3）许多物联网业务需要匿名操作，如网络投票。

（4）在医疗管理系统中，需要保存病人的相关信息，以便医生诊病时可以获取正确的病例数据，但又要避免这些病例数据跟病人的身份信息相关联。在应用过程中，主治医生允许知道病人的病历数据。在这种情况下，对隐私信息的保护具有一定的困难，可以通过加密技术对病人病历的隐私信息加以保护。

在互联网环境的商业活动中，无论采用何种技术，都难以避免恶意行为的发生。假如能够根据恶意行为所造成的后果的严重程度给予相应的惩罚，则可以减少恶意行为的发

生。在技术上，这需要收集相关的犯罪证据。因此，计算机取证就显得尤为重要。然而计算机取证技术难度较大，原因在于计算机平台种类繁多，包括多种计算机操作系统和智能设备操作系统等。

与计算机取证相对应的是计算机数据销毁。数据销毁的目的是销毁那些在密码算法和密码协议实施过程中所产生的临时中间变量。一旦加密算法和密码协议实施完成，这些中间变量将不再有用，但是这些中间变量如果落入攻击者手中，就有可能为攻击者提供重要的信息，进而提高成功攻击的可能性。因此，这些临时中间变量需要及时从计算机内存和硬盘存储空间中删除。计算机数据销毁技术有可能为计算机犯罪者提供证据销毁工具，从而增大计算机取证的难度。如何在计算机取证与计算机数据销毁之间权衡，也是物联网应用中需要解决的安全问题之一。

2. 应用层行业应用的安全机制

物联网的典型应用是商业应用，在商业应用中存在大量需要保护的知识产权产品，包括专利、商标、软件和电子产品等。在物联网应用中，对电子产品知识产权的保护将会提高到一个新的高度，对相应的安全技术要求也是一项新的挑战。

基于物联网应用层的安全需求和安全挑战，需要实现以下的安全机制。

（1）有效的数据库访问控制和内容筛选机制。

（2）不同应用场景中的隐私信息保护技术。

（3）叛逆追踪和其他信息泄露追踪机制。

（4）有效的数据取证技术。

（5）安全的数据销毁技术。

（6）安全的电子产品和软件的知识产权保护技术。

针对物联网应用层的安全机制，需要提供相应的加密技术，包括访问控制、匿名签名、匿名认证、密文验证、门限密码、叛逆追踪、数字水印和数字指纹技术等。

1.10　本章小结

物联网是通过射频识别器、红外感应器、全球定位系统、激光扫描器等信息传感设备，按照约定的协议，把任何物品与互联网连接起来，从而进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

物联网具备四个特征：全面感知、可靠传输、智能处理和综合应用。

物联网体系结构分为三个层次：感知层、网络层和应用层。

感知层由传感器节点和接入网关等组成，传感器感知外部世界的温度、湿度、声音和图像等信息，并传送给上层网关，由网关将收集到的信息通过网络层提交给后台处理。当后台将数据处理完毕后，发送执行命令到相应的执行机构，完成对被控对象或被测对象的控制参数调整，或者发出某种信号以实现远程监控。

网络层是物联网的“神经中枢”和“大脑”，用于实现信息传递和处理。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等。

应用层主要根据行业特点，借助物联网的技术手段，开发各类行业的应用解决方案，

将物联网的优势与本行业的生产经营、信息化管理、组织调度有效结合起来，从而形成各类物联网解决方案，构建智能化的行业应用。

物联网的关键技术很多，主要包括 RFID 技术、身份认证技术、无线传感器网络技术、M2M 技术、全球定位技术、云计算技术、中间件技术、IPv6 技术等。

RFID 是一种无线通信技术，可以通过无线电信号识别特定目标并读写相关数据，而无须在识别系统与特定目标之间建立机械或者光学接触。

身份认证技术用于识别物联网用户的身份，可以分为基于 PKI 的身份认证技术和各种生物识别技术，如指纹识别、掌形识别、虹膜识别、视网膜识别、面部识别、签名识别、声音识别等。

无线传感器网络（WSN）是由大量静止的或移动的传感器以自组织和多跳的方式构成的无线网络。它以协作方式感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给网络的所有者。

M2M 是机器对机器通信（Machine to Machine）的简称，主要指通过“通信网络”传递信息从而实现机器之间的数据交换，也就是通过通信网络实现机器之间的互连互通。

全球定位系统由空间星座、地面控制和用户设备等三部分构成。全球定位技术能够快速、高效、准确地提供点、线、面要素的精确三维坐标及其他相关信息，具有全天候、高精度、自动化、高效益等显著特点，广泛应用于军事导航、民用交通（如船舶、飞机、汽车等）导航、大地测量、摄影测量、野外考察探险、土地利用调查、精确农业及日常生活（如人员跟踪、休闲娱乐）等不同领域。

云计算是基于互联网相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态、易扩展且经常是虚拟化的资源。云是对网络、互联网的一种比喻。过去人们往往用云来表示电信网，后来也用来表示对互联网和底层基础设施的抽象。

中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源。中间件位于客户机、服务器操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口，但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递。通过中间件，应用程序可以工作于多平台或多操作系统（Operating System，OS）环境。

IPv6 是英文 Internet Protocol version 6 的缩写，其中 Internet Protocol 译为“互联网协议”。IPv6 是 IETF 设计的用于替代现行版本 IP 协议（IPv4）的下一代 IP 协议。IPv6 不但解决了网络地址资源数量的问题，而且为除计算机以外的海量传感器接入物联网在数量限制上扫清了障碍。

物联网系统安全指物联网系统可以连续地、可靠地和正常地运行，服务不会中断，物联网系统中的软件、硬件和系统中的数据受到保护，不受人为的恶意攻击、破坏和更改。

互联网技术是物联网的基础，互联网的安全直接关系到整个物联网的安全。互联网安全问题涉及网络设备基础安全、网络安全、Web 安全和基于 Web 应用的安全等各个方面，包括安全编码、数据帧安全、密钥管理与交换等。

物联网的感知层由大量的传感器等设备构成，缺少人对设备的有效监控，并且物联网设备种类繁多、数量庞大，所以物联网还面临其特有的安全威胁，包括点到点消息认证、重放攻击、拒绝服务攻击、篡改或泄露标签数据、权限提升攻击、业务安全和隐私安

全等。

物联网感知层安全的特点包括设备、节点无人看管，容易受到物理操纵；信息传输主要依靠无线电信号，信号容易被窃取和干扰；基于低成本的设计，传感器节点通常是资源受限的；物联网中的物品信息能够被自动地获取和传送；物联网在原有的网络基础上进行了延伸和扩展。

物联网安全体系结构包括信息采集安全、信息传输安全、信息处理安全和信息应用安全。

根据物联网感知层安全所涵盖的内容，可以把物联网的感知层分为两大类，即传感器网络和 RFID 系统。针对物联网感知层的安全，需要轻量级加密算法和轻量级安全认证协议。

物联网网络层涉及移动通信网、国际互联网和无线网络等多种网络环境。物联网网络层的安全机制，可以分为端到端的机密性和节点到节点的机密性。

代表物联网应用层的云计算平台，除了需要有能力处理海量数据，还必须具有备份和防灾等能力，能为用户提供私有数据空间和私有计算处理能力，并且具有抗攻击和抗病毒的能力。

物联网的典型应用是商业应用，在商业应用中存在着大量需要保护的知识产权产品，包括专利、商标、软件和电子产品等。针对物联网应用层的安全机制，需要提供相应的加密技术，包括访问控制、匿名签名、匿名认证、密文验证、门限密码、叛逆追踪、数字水印和数字指纹技术等。

复习思考题

一、单选题

1. 早在（　　）年，美国麻省理工学院（MIT）的凯文·阿什顿教授（Kevin Ashton），就已经提出了物联网的概念。

A. 1990　　B. 1991　　C. 1992　　D. 1993

2. 2009 年 8 月，温家宝总理在（　　）视察时提出“感知中国”。

A. 无锡　　B. 杭州　　C. 苏州　　D. 广州

3. 做到“运筹帷幄之中，决胜千里之外”的是（　　）。

A. 物联网　　B. 广域网　　C. 城域网　　D. 局域网

4. 在广义物联网中，不仅包括机器到机器（M2M），也包括（　　）之间广泛的通信和信息的交流。

A. 机器到人（M2P）　　B. 人到人（P2P）

C. 人到机器（P2M）　　D. 以上都是

5. 物联网具备以下的特征：全面感知、（　　）、智能处理、综合应用。

A. 可靠传输　　B. 单向传输　　C. 双向传输　　D. 加密传输

6. 业界广泛认可的物联网体系结构分为（　　）个层次。

A. 3　　B. 4　　C. 5　　D. 7

7. 射频识别技术的英文简写为（　　）。

A. AFID　　B. BFID　　C. RFID　　D. VFID

8. 网络层是物联网的（　　）。

A. 神经中枢和大脑　B. 心脏　C. 四肢　D. 以上都不是

9. 无线传感器网络系统通常包括传感节点、汇聚节点和（　　）。

A. 任务管理节点　B. 任务处理节点　C. 中央管理节点　D. 中央处理节点

10. M2M 平台包括（　　）个模块。

A. 3　B. 4　C. 5　D. 6

11. 无线通信网络不包括（　　）技术。

A. 蓝牙　B. xDSL　C. Wi-Fi　D. 4G/5G

12. 云计算可以提供的三个层次的服务中，IaaS 指（　　）。

A. 基础设施即服务　B. 平台即服务　C. 软件即服务　D. 以上都不是

13. 云计算的主要特点包括（　　）。

A. 超大规模　B. 虚拟化　C. 极其廉价　D. 以上都是

14. 中间件位于（　　）之间。

A. 传感器与操作系统　B. 操作系统与应用软件

C. 传感器与应用软件　D. 终端与无线网络

15. 信息和网络安全的目标是保证被保护信息的（　　）。

A. 机密性　B. 完整性　C. 可利用性　D. 以上都是

16. 传统的互联网安全问题涉及网络设备基础安全、网络安全、Web 安全和基于 Web 应用的安全等各个方面，包括（　　）。

A. 安全编码　B. 数据帧安全　C. 密钥管理与交换　D. 以上都是

17. 物联网面临的安全威胁分为（　　）种。

A. 4　B. 5　C. 6　D. 7

18. 物联网的安全特征可以分为（　　）方面。

A. 3　B. 4　C. 5　D. 6

19. RFID 系统面临的安全问题包括（　　）。

A. 非法复制　B. 非法跟踪　C. 近距离攻击　D. 以上都是

20. 无线传感器网络的安全技术可以归纳为（　　）点。

A. 4　B. 5　C. 6　D. 7

21. 针对物联网感知层的安全，需要（　　）的加密算法。

A. 轻量级　B. 中量级　C. 重量级　D. 以上都可以

22. 云计算面临的安全挑战主要包括（　　）方面。

A. 3　B. 4　C. 5　D. 6

23. 物联网应用层的安全需求和安全挑战主要来自（　　）方面。

A. 3　B. 4　C. 5　D. 6

24. 基于物联网应用层的安全需求和安全挑战，需要实现（　　）种安全机制。

A. 3　B. 4　C. 5　D. 6

25. 针对物联网应用层的安全机制，需要提供相应的加密技术，包括访问控制、匿名签名、匿名认证、密文验证、门限密码和（　　）等。

A. 叛逆追踪　B. 数字水印　C. 数字指纹技术　D. 以上都是

二、简答题

1. 请简述物联网的起源和发展历程。
2. 请简述物联网的定义。
3. 请指出物联网的四个特征。
4. 请画图表示物联网的体系结构，并分别说明每一层实现的功能。
5. 什么是 RFID 技术？
6. 什么是身份认证技术？
7. 生物识别技术主要包括哪些技术？
8. 什么是无线传感器网络技术？
9. 什么是 M2M 技术？
10. 什么是 Wi-Fi 技术？
11. 什么是 WiMAX 技术？
12. 什么是 ZigBee 技术？
13. 什么是蓝牙技术？
14. 什么是全球定位系统？
15. 什么是云计算技术？云计算的主要特点是什么？
16. 什么是中间件技术？
17. 什么是 IPv6 技术？
18. 物联网安全的含义是什么？
19. 传统网络面临哪些安全威胁？
20. 物联网面临哪些特有的安全威胁？
21. 请分析物联网的安全特征。
22. 请画图描述物联网安全的体系结构。
23. 请简要分析无线传感网的安全威胁。
24. 请简要分析 RFID 系统的安全威胁。
25. 请简要说明物联网感知层的安全机制。
26. 请简要说明物联网网络层的安全机制。
27. 请简要说明物联网云计算平台的安全机制。
28. 请简要说明物联网行业应用的安全机制。