第1部分

NB-IoT 基础理论篇

第 1 章

本章配套资源

物联网概述

NB-IoT 是应物联网（Internet of Things，IoT）发展需求而诞生的一种低功耗广域（Low Power Wide Area，LPWA）网络技术，是 5G 物联网技术的重要组成部分。为了更好地理解和学习 NB-IoT 技术，首先有必要对物联网的基本概念和相关技术有所认识。本章主要介绍物联网的定义、物联网的产生和发展现状、物联网的网络结构组成和协议分层、物联网各层涉及哪些关键技术，以及物联网的安全问题，同时将 NB-IoT 技术和 LoRa、eMTC（LTE-M）和 Sigfox 等同类技术进行对比，从而能够直观地了解 NB-IoT 技术的特性。

1.1 物联网的诞生

最广为人知的物联网起源，恐怕要追溯到 1991 年的“特洛伊咖啡壶服务器”事件。当时，剑桥大学特洛伊计算机实验室的科学家们，经常要下楼去看咖啡煮好了没有，但又怕影响工作，为了解决麻烦，他们编写了一套程序，在咖啡壶旁边安装了一个便携式摄像头，利用终端计算机的图像捕捉技术，以 3 帧/s 的速率传输到实验室的计算机上，以方便工作人员随时查看咖啡是否煮好。

关于物联网的起源，还有另外一种说法：1990 年，在卡内基梅隆大学的校园里，有一群程序设计师，他们每次敲完代码后都习惯到楼下的可乐贩卖机购买一罐冰可乐。可是很多时候他们都会因可乐已售完或者没有冰可乐败兴而回，这令他们十分苦恼。于是他们就把楼下的贩卖机连上网络，并写了一段代码去监视可乐机。

由上可见，无论是远程监控咖啡壶还是监视可乐机，都是一群“懒人”为了方便自己“偷懒”而设计出来的“物”和“物”，以及“人”和“物”之间的互联系统，这就是物联网最早的雏形，也是物联网概念的由来。

国际电信联盟（ITU）在 2005 年的互联网报告中提出：物联网是任何时间、任何地点、人和物之间的互联；它是泛在的网络世界和泛在的计算；RFID 技术、无线传感器技术、智能技术和纳米技术都是物联网的关键促成因素。

欧洲物联网研究项目组（CERP-IoT）在 2009 年研究报告中指出：物联网是未来因特网的一个组成部分，可以被定义为基于标准的和可互操作的通信协议，且具有自配置能力的动态的全球网络和服务基础架构。物联网中的“物”都具有标识、物理属性和自身的独

特性，能使用通用的接口实现与因特网无缝且安全的整合。

我国 2010 年政府工作报告中的物联网定义：通过信息传感设备，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，以实现智能化识别、定位、跟踪、监控和管理的一种网络。它是在互联网基础上延伸和扩展的网络。

事实上，在近 20 年的研究和探索中，不同的组织和学者对物联网给出了不同的定义。相信随着科技的进步，物联网的内涵和外延还会不断地演进和发展。

1.2　物联网发展概况

随着移动通信技术和传感器技术的进步，物联网产业得到迅猛发展。尤其是近些年来，随着电信运营商的大力投入，物联网产业链已呈现全球化趋势，发展势头更加强劲。物联网产业链的从业者众多，既包括离客户较远的电信运营商、通信设备商、芯片制造商、通信模组商、配套服务商等，也包括离客户较近的各种各样的物联网垂直应用服务商。物联网的应用场景也非常广泛，已经涉及远程抄表、智慧城市、资产管理、智慧物流、电梯物联网、智能交通、消防物联网、环保物联网、地下空间、智慧家庭、工业物联网、农业物联网、可穿戴设备等领域。

1.2.1　全球物联网发展概况

近年来，世界各国都高度重视物联网的发展，纷纷从战略高度制定出物联网发展策略以抢占先机。各种物联网联盟纷纷成立，各种物联网创新项目纷纷出台，各种物联网新技术不断诞生。

早期的物联网主要采用蓝牙、Wi-Fi、ZigBee 等中距离无线通信技术，真正承载到移动网络（传统的 2G、3G、4G 等移动通信网）上的物与物连接只占到连接总数的 10%。为了充分发挥移动网络的覆盖优势和成本优势，为了扩展物联网的应用领域，在移动运营商的大力支持下，一些专门针对物联网业务的低功耗广域（LPWA）移动通信技术应运而生，最主流的就是 NB-IoT 和 eMTC。

NB-IoT 是 3GPP 制定的专门针对窄带物联网应用的低功耗广域蜂窝移动通信技术标准。现在，NB-IoT 已经被广泛部署于现有各种网络中，并得到大量应用，这就使它成为世界上极具影响力的一种物联网。NB-IoT 标准的演进历程如图 1-1-1 所示。

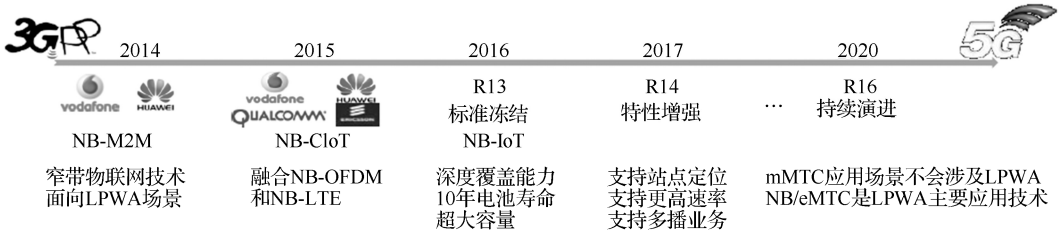

图 1-1-1　NB-IoT 标准的演进历程

最早时 3GPP 提出了一个窄带物联网的设计目标，由此产生了一个新空口的需求。2014 年 5 月，GERAN 技术规范组确立“新空口”项目；同时，华为提出了新空口技术 NB-M2M。2014 年 7 月，高通公司提交了 NB-OFDM 技术方案。2015 年 5 月，NB-M2M 和 NB-OFDM 融合形成了 NB-CIoT。2015 年 7 月，爱立信联合中兴、诺基亚等公司提出了 NB-LTE 技术方案。2015 年 9 月，NB-LTE 和 NB-CIoT 进一步融合，窄带物联网技术最终定名为 NB-IoT。2016 年，3GPP 的 R13 版本冻结。R13 是 NB-IoT 的基础版本，在满足 4 个需求（覆盖、时延、功耗、连接数）的同时，可以支持 IP 和非 IP 连接，也可以支持短信功能。2017 年的 R14 版本在 R13 版本的基础上增加了一些特性：定位精度提高、峰值速率提升、引入更低的设备功耗等级、多播、覆盖增强授权等。相比 R14 版本，R15 版本在 NB-IoT 的降低功耗、减小时延和 QoS 提升等基本性能上做了进一步增强。R15 版本还增加了对 TDD 的支持。2020 年 7 月发布的 R16 版本主要是增强下行控制，提高下行消息可达性，增强互操作性，实现小区互重选等。

2020 年 7 月 9 日，国际电信联盟无线电通信部（ITU-R）举行会议宣称 NB-IoT 满足各种目标需求，被正式接受成为 5G IMT-2020 技术标准。换句话说，在 3GPP 组织的推动下，ITU 已经公开接受 NB-IoT 成为 5G IMT-2020 技术标准的一个组成部分。将来，物联网设备不仅能够通过 NB-IoT 的核心网接入互联网，还能够连接到 5G 核心网中，共享 5G 的边缘计算、网络切片和其他业务。

根据全球移动通信系统协会（GSMA）统计，截止到 2018 年 8 月，全球已有超过 30 家主流运营商推出 60 张蜂窝物联网。其中，NB-IoT 为 47 张，eMTC 为 13 张，有 8 家运营商在同一地区同时使用 NB-IoT 和 eMTC。根据 GSMA 预测，到 2025 年，全球蜂窝物联网连接数将达到 3100 百万（其中传统的 2G/3G/4G 网络占 1300 百万，NB-IoT/eMTC 占 1800 百万），如图 1-1-2 所示。

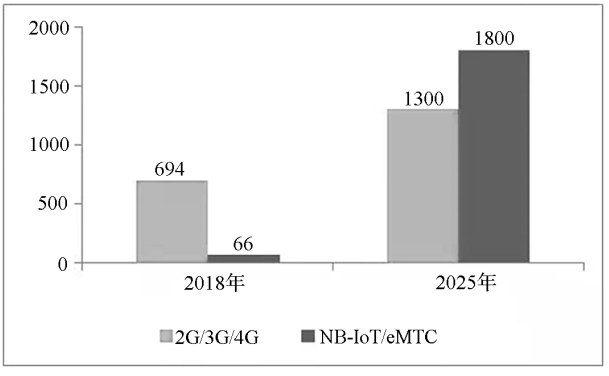

图 1-1-2　全球蜂窝物联网连接数（单位：百万）

除了基于移动通信设计的 NB-IoT 和 eMTC 这两个采用授权频谱的系统，基于 IT 通信设计并采用非授权频谱的两个 LPWA 网络（LoRa 和 Sigfox）也将保持持续发展势头，并且抢占了部分物联网市场。LoRa 是这里的领跑者。虽然许多 LoRa 网络是专用网，但它有强大的行业组织 LoRa 联盟（目前有 500 多家成员公司）和 5 万多家开发者生态圈的支持。目前有 10 个国家已经推出了 14 张全国性的公共 LoRa 网络，而且全球 120 家服务提供商

正在支持这项技术。

由上可见，窄带物联网巨大的“蓝海”市场已经开启，并将在未来出现爆炸式增长。据著名国际研究咨询公司 Omdia 的观点：新型冠状病毒感染对全球经济发展都有一定影响，也不可避免地影响到了物联网某些领域的投资，但物联网在帮助应对新型冠状病毒感染挑战方面发挥了重要作用。同时，新的物联网应用连同 5G、宽带消费等应用的增长，预计在 2025 年电信收入的增长率将超过 2%，其中以移动收入为首。

1.2.2　国内物联网发展概况

中国政府高度重视物联网产业的发展，早在 2010 年出台的《国务院关于加快培育和发展战略性新兴产业的决定》中，物联网已经作为新一代信息技术产业中的重要项目位列其中，成为国家首批加快培育的七个战略性新兴产业之一。随后，国家又出台了一系列的规划政策，保证了我国物联网产业健康有序的发展。

由于中国政府的大力支持和华为、中兴等具有国际影响力的通信公司的技术引领，中国在物联网领域始终处于世界领先地位。全球物联网领域的前三大通信业务提供商（CSP）分别是中国移动、中国联通和中国电信。截止到 2019 年，这三家公司总共拥有 9.7 亿个物联网连接（占全球总连接数的 77%），它们在 2018 年总共增加了 4.2 亿个物联网连接。中国第 4 家 5G 运营商——中国广电网络已于 2019 年年中获得牌照，它的加入将进一步推动中国物联网市场的壮大。

不只是在通信技术领域，中国物联网终端和芯片组的生产制造也已实现本土化。中国作为制造业大国的优势使其成为全球物联网市场上的中坚力量。

以物联网典型应用场景智慧城市为例，在世界前 10 大城市中，中国占了 2 个。根据中国政府十三五规划（截至 2020 年），中国政府计划对智慧城市投资高达 5000 亿元人民币（合 740 亿美元）。

据麦肯锡公司预测：到 2030 年，发达国家将占物联网经济价值的 55%左右，但细分地理位置后发现，真正增长的是中国，中国已成为全球物联网的重要力量。

NB-IoT 在中国市场更是取得了重大成功。截至 2019 年年底，中国占全球授权频谱 LPWAN 连接总量的 72%以上，其中绝大多数使用的是 NB-IoT。

2014—2020 年中国 NB-IoT 基站规模如图 1-1-3 所示，到 2017 年年末，国内的 NB-IoT 网络已实现覆盖直辖市、省会城市等主要城市，基站规模达到 40 万个。到 2020 年 2 月，网络已基本实现全国普遍覆盖，并开始面向室内、交通路网、地下管网等应用场景实现深度覆盖，基站数量超过 90 万个。预测到 2025 年，国内 NB-IoT 基站数量有望突破 300 万个。

截至 2020 年 2 月，NB-IoT 在全国范围内完成了超过 300 个城市的覆盖，终端连接数突破 1 亿，且每年以千万级的数量在递增，覆盖了智慧城市、环保、农业、医疗、物流等各个行业。

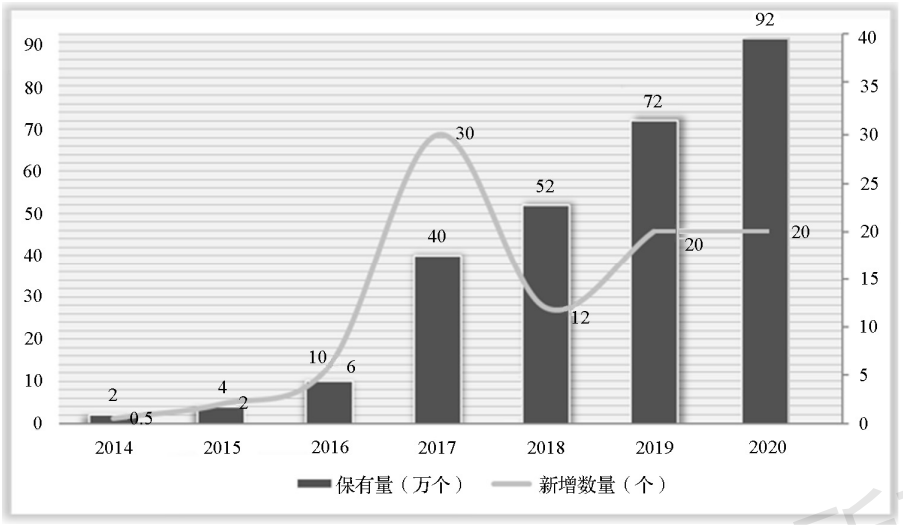

图 1-1-3　2014—2020 年中国 NB-IoT 基站规模

1.3　物联网分层架构

物联网是为了打破地域限制，实现物与物之间按需进行的信息获取、传递、存储、融合、使用等服务的网络。为此，物联网应具有三个能力：全面感知、可靠传输和智能处理。因此，业界普遍认为物联网应至少具有三个层次：感知层、网络层和应用层。但是，在物联网实际部署和商用过程中，应用平台功能逐渐从应用层中分离出来，形成了一个单独的层次——平台层。物联网分层架构如图 1-1-4 所示。

图 1-1-4　物联网分层架构

1. 感知层

感知层又称为感知识别层，负责信息收集和信号处理（包括边缘计算）。它通过感知识

别技术，让物品“开口说话、发布信息”。感知层能够采集的信息包括用户位置、环境温湿度、个体喜好、身体状况、用户业务感受、网络状态等。感知层就像物联网的皮肤和五官，它也是物联网区别于其他网络的最独特部分。

感知层的感知识别需要依靠终端设备来实现，因此感知层也称为终端层，简称“端”。这些终端设备既包括采用信息自动生成方式的 RFID 卡、传感器、二维码、摄像头、定位系统等，也包括采用人工信息生成方式的各种智能设备，如智能手机、PDA、多媒体播放器等。第 1 部分 NB-IoT 基础理论篇 1.5.3 节将对有关感知层的相关技术进行介绍。

感知层将传统网络的用户终端向下延伸和扩展，扩大了通信对象的范围，即通信不仅仅局限于人和人之间，还扩展到了人和现实世界的各种物之间，甚至是物和物之间。它解决的是人类世界和物理世界的数据获取问题，是物理世界与数字世界的高度融合。

感知层位于物联网四层结构中的最底端，是所有上层结构的基础。

2. 网络层

网络层又称为网络构建层，它直接通过现有的互联网、移动通信网、卫星通信网等网络基础设施，对来自感知层的信息进行无障碍、高可靠性、高安全性、远距离地传输。它的作用就像感知层与平台层及应用层之间的传输管道，因此，简称“管”。

网络层是 NB-IoT、eMTC、LoRa、Sigfox 等物联网的关键技术所在。第 1 部分 NB-IoT 基础理论篇 1.5.2 节将对有关网络层的相关技术进行介绍。

在物联网四层结构中，网络层接驳感知层和平台层，具有强大的纽带和传递作用，如同物联网的神经网络。

3. 平台层

在物联网实际部署和商用过程中，遇到了三大挑战。

（1）挑战 1：新业务上线周期长（应用碎片化、开发周期长、产品上市慢）。

（2）挑战 2：终端/传感器厂家众多、标准不一，集成困难。

（3）挑战 3：网络连接复杂（网络类型多：2G/3G/4G/NB-IoT/ZigBee 等，如何满足安全性要求、实时性要求、QoS 要求等）。

为此，需要有一个统一的控制点。因此，平台层应运而生。采用物联网平台具有以下益处。

（1）能够聚合更多的应用，并实现快速集成。

（2）能够减少各种基础研发的成本。

（3）方便实现各种网络标准和通信协议与应用层的对接。

（4）将各种物联网应用的孤岛数据汇聚起来，充分挖掘数据价值。

（5）降低物联网技术方案升级、部署、扩展和维护的成本。

（6）提升物联网数据的安全性和网络的可靠性。

此外，对于电信运营商来讲，网络层是其传统优势，但 ARPU（每用户平均收入）较低。平台层是运营商物联网价值链的锚点，是其介入物联网垂直产业的核心竞争力。

平台层又称为平台管理层，它对感知和传输来的信息进行分析和处理，做出正确的控制和决策，实现智能化的管理。这一层解决的是海量数据信息如何处理的问题，自然地与云计算技术融合在一起，因此各种物联网平台都称为“云平台”，平台层简称为“云”。

在高性能网络计算机的环境下，平台层能够将网络内海量的信息资源通过计算机整合

成一个可互联互通的大型智能网络，进而解决数据如何存储（数据库与海量存储技术）、如何检索（搜索引擎）、如何使用（数据挖掘与机器学习）、如何不被滥用（数据安全与隐私保护）等问题。第 1 部分 NB-IoT 基础理论篇 1.5.1 节将对有关平台层的相关技术进行介绍。

平台层是物联网产业链的枢纽，向下接入分散的物联网感知层，汇集传感数据，向上面向应用服务提供商提供应用开发的基础性平台和面向底层网络的统一数据接口，支持具体的基于传感数据的物联网应用。它是物联网智慧的源泉，就像物联网的大脑一样。人们通常把各种物联网应用冠以“智能”的名称，如智能电网、智能交通、智能物流等，而其中的智慧就来自于这一层。

4. 应用层

应用层又称为综合应用层，是物联网系统的用户接口，解决的是人机界面的问题。它通过分析处理后的感知数据，为用户提供丰富的特定服务。

应用层是物联网的“社会分工”，与行业需求结合，与行业专业技术深度融合。物联网服务的各个行业将各自感知终端采集的数据，通过网络和平台传输到对应行业的物联网服务器中，各个行业根据其提供的高价值的数据，进行产业升级、提效及智能化改造。

1.4 物联网协议架构

互联网时代，TCP/IP 协议已经一统江湖，现在物联网的通信协议架构也是构建在传统互联网基础架构之上的。物联网协议分层架构如图 1-1-5 所示。按照功能作用不同，物联网协议可以分为两大类：传输协议（也叫接入协议）和通信协议。传输协议负责子网内部设备间的组网及通信，主要对应 OSI 七层模型的数据链路层/物理层的协议，如 NB-IoT、LTE、ZigBee、LoRa 等。通信协议是运行在传统互联网 TCP/IP 协议之上的设备通信协议，主要负责设备通过互联网进行数据交换及通信，对应 OSI 七层模型应用层的协议，如 MQTT、CoAP、HTTP 等。

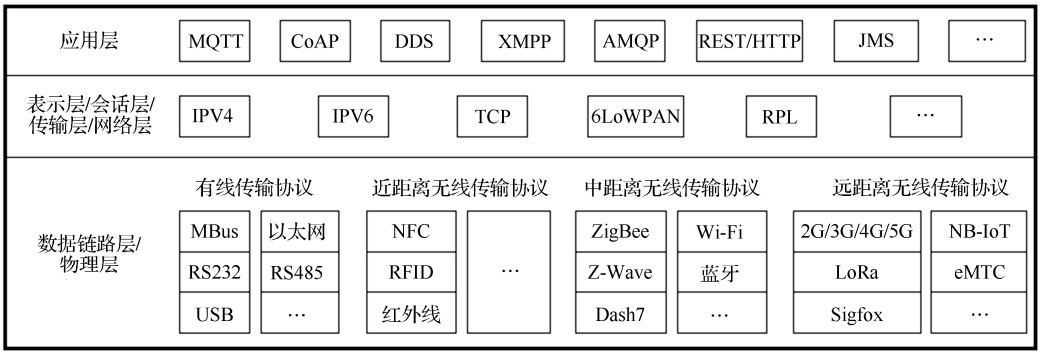

图 1-1-5　物联网协议分层架构

1.4.1 通信协议

物联网中存在如图 1-1-5 所示的七大通信应用协议：MQTT、CoAP、DDS、XMPP、

AMQP、REST/HTTP 和 JMS。这些协议都已被广泛应用，且每种协议都有至少十种以上的代码实现，都支持实时的发布/订阅。同时，每种通信协议都有各自的特点和一定的适用范围，如 AMQP、JMS、REST/HTTP 都工作在以太网，CoAP 是专门为资源受限设备开发的协议，而 DDS 和 MQTT 的兼容性则相对强很多。所以在具体物联网系统架构设计时，需要考虑实际场景的通信需求，选择合适的协议。

以智能家居为例：智能灯光控制可以使用 XMPP 协议控制灯的开关；电力供给、发电厂的发电机组的监控可以使用 DDS 协议；当电力输送到千家万户时，电力线的巡查和维护可以使用 MQTT 协议；家中所有电器的电量消耗，可以使用 AMQP 协议传输到云端或家庭网关中进行分析；如果用户想把自家的能耗查询服务公布到互联网上，那么可以使用 REST/HTTP 协议来发布 API（应用编程接口）服务。

七种通信协议的区别如表 1-1-1 所示。

表 1-1-1　七种通信协议的区别

特性	通信协议						
	DDS	MQTT	AMQP	XMPP	JMS	REST/HTTP	CoAP
交互模式	发布/订阅	发布/订阅	发布/订阅	NA	发布/订阅	请求/响应	请求/响应
架构风格	全局数据空间	代理	P2P 或代理	NA	代理	P2P	P2P
QoS	22 种	3 种	3 种	NA	3 种	通过 TCP 保证	确认或非确认消息
互操作性	是	部分	是	NA	否	是	是
性能	100000msg/s/sub	1000 msg/s/sub	1000 msg/s/sub	NA	1000 msg/s/sub	100 请求/s	100 请求/s
硬实时	是	否	否	否	否	否	否
传输层	默认为 UDP，也支持 TCP	TCP	TCP	TCP	不指定，一般为 TCP	TCP	UDP
订阅控制	消息过滤的主题订阅	层级匹配的主题订阅	队列和消息过滤	NA	消息过滤的主题和队列订阅	NA	支持多播地址
编码	二进制	二进制	二进制	XML	二进制	普通文本	二进制
动态发现	是	否	否	NA	否	否	是
安全性	提供方支持，一般基于 SSL 和 TLS	简单用户名/密码认证，SSL 数据加密	SASL 认证，TLS 数据加密	TLS 数据加密	提供方支持，一般基于 SSL 和 TLS，JAAS API 支持	一般基于 SSL 和 TLS	DTLS

由于篇幅受限，关于七种通信协议的具体内容请参考其他资料。本书将在第 2 部分 NB-IoT 应用开发篇项目 5 详细介绍专门为物联网应用设计的 CoAP 协议。

1.4.2　传输协议

如图 1-1-5 所示，传输协议分为有线传输协议和无线传输协议。无线传输协议又可分为近距离无线传输协议、中距离无线传输协议和远距离无线传输协议。

有线传输协议包括 MBus、以太网（Ethernet）、RS232、RS485、USB 等。有线传输可靠性高、稳定性好，缺点是通信依赖于传输介质，终端移动性受限，只能在物联网的特定场景中发挥作用。

近距离无线传输协议包括 NFC、RFID、红外线等，由于传输距离过短（几厘米～十米），适用于物联网终端的感知和识别，所以一般被归类为物联网感知层的识别技术，将在第 1 部分 NB-IoT 基础理论篇 1.5.3 节中加以详细介绍。

中距离无线传输协议包括 ZigBee、Wi-Fi、Z-Wave、蓝牙、Dash 7 等，传输距离介于近距离无线传输和远距离无线传输之间（几十米～几千米）。中距离无线传输归属于物联网感知层还是网络层是个没有定论的问题，由于物联网的纷繁复杂性，作者认为在研究不同的问题时可以因需而定。第 1 部分 NB-IoT 基础理论篇 1.5.2 节暂把中距离无线传输协议作为网络层技术加以详细介绍。

远距离无线传输协议（传输距离在千米以上）既包括传统的 2G、3G、4G 和 5G 移动通信网络，也包括专门设计的物联网类型，目前主要指 NB-IoT、eMTC、LoRa 和 Sigfox。远距离无线传输协议是构成物联网网络层的骨干技术，将在第 1 部分 NB-IoT 基础理论篇 1.5.2 节中加以详细介绍。

1.5 物联网关键技术

物联网涉及感知、控制、网络通信、微电子、软件、嵌入式系统、微机电等技术领域，因此物联网涵盖的关键技术也非常多。根据中国信息通信研究院 2010 年的研究成果，将物联网技术体系划分为感知关键技术、网络通信关键技术、应用关键技术、共性技术和支撑技术，如图 1-1-6 所示。这一成果对现今的物联网研究仍有重大指导意义。

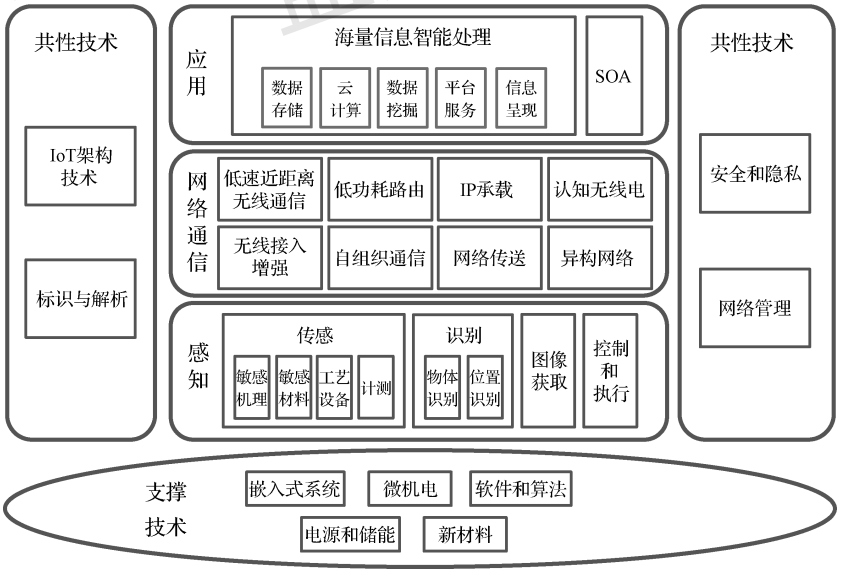

图 1-1-6　物联网技术体系

物联网支撑技术包括嵌入式系统、微机电、软件和算法、电源和储能、新材料等。共性技术中的标识，如感知层的 RFID 标识、条码标识、国际移动设备识别码（IMEI）等，

网络层的 IPv4、IPv6、国际移动用户识别码（IMSI）、MAC 地址等，以及应用层的统一资源定位器（URL）、内容标识（Content-ID）等。由于篇幅受限，这些技术请参考其他相关书籍。本节主要讲述物联网平台层技术、网络层技术和感知层技术，以及共性技术中的物联网安全问题。

1.5.1　平台层技术

物联网平台层的主要功能：连接管理、设备管理、应用使能和业务分析，因此整个物联网平台层可以进一步划分为相应的逻辑功能模块——设备管理平台、连接管理平台、应用使能平台和业务分析平台，如图 1-1-7 所示。不同的平台开发商可能对自己的平台有不同的命名方法，但都要至少包含这四大功能模块，其他所有的功能模块都是基于此四大功能模块的延展。

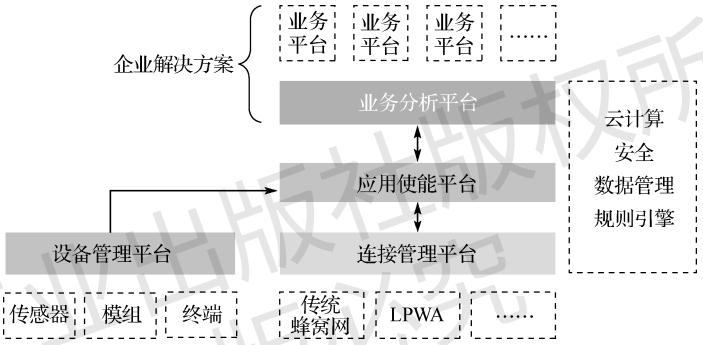

图 1-1-7　物联网平台按服务层次的分类

设备管理平台主要用于物联网设备的接入、数据收集和设备状态的监控与维护。设备管理平台提供的功能，如对物联网终端设备进行远程监控、设置调整、软件升级、系统升级、故障排查、生命周期管理等。

连接管理平台也称为用户管理平台、SIM 卡管理平台，一般应用于电信运营商网络之上，能够实现对物联网连接配置和故障管理，保证终端联网通道稳定，实现网络资源用量管理、连接资费管理、账单管理、号码/IP 地址/MAC 资源管理、套餐变更、更好地进行物联网 SIM 的管理。同时，作为面向用户的运营支撑平台，连接管理平台能够为用户提供用户卡信息查询、通信管理、数据统计分析等服务。

设备管理平台和连接管理平台都处于物联网平台层中的较低层次。更高层次的应用使能平台主要架构在连接管理平台之上。应用使能平台又称为服务能力开放平台，它是直接面向物联网应用开发者开放网络能力的 PaaS 平台。应用使能平台提供了成套应用开发工具（大部分能提供图形化操作界面，不需要开发者编写代码）、中间件、数据存储功能、业务逻辑引擎、对接第三方系统的 API 等，物联网应用开发者可以快速开发、部署和管理物联网应用，而不需要考虑下层基础设施管理、数据管理和归集、通信协议、通信安全等问题，从而大大降低了开发成本、缩短了开发时间。应用使能平台解决了随上层应用灵活扩展的问题——即使上层应用大规模扩张，也不需要担心底层资源跟不上连接设备的扩张速度。

业务分析平台是物联网平台分层中最高的，它与企业的各种具体业务平台共同构成了

企业物联网解决方案。业务分析平台主要包含大数据服务和机器学习两个功能：大数据服务在汇集云平台的各类相关数据后，对其进行分类处理、分析，并提供视觉化数据分析结果（图表、仪表盘、数据报告）；机器学习将沉淀在平台上的结构化和非结构化的数据进行训练，形成具有预测性的、认知的、复杂的业务分析逻辑。未来，机器学习必将向人工智能过渡。

综上所述，物联网平台层涉及云计算、大数据、数据挖掘、机器学习、人工智能等技术，这些技术可能分属不同的研究领域，但又存在着紧密的联系。下面加以简要介绍。

1. 云计算

迄今为止，对云计算最权威的解释是由美国国家标准与技术研究院（NIST）在 2010 年 7 月发布的。NIST 认为：云计算是一种模型，用来实现对可灵活配置的计算资源（如网络、服务器、存储、应用程序、服务等）便捷地、按需地访问，这些计算资源可以快速地被获取和释放，同时用户的管理成本极低，几乎不需要与供应商进行沟通。云计算应用示意图如图 1-1-8 所示。

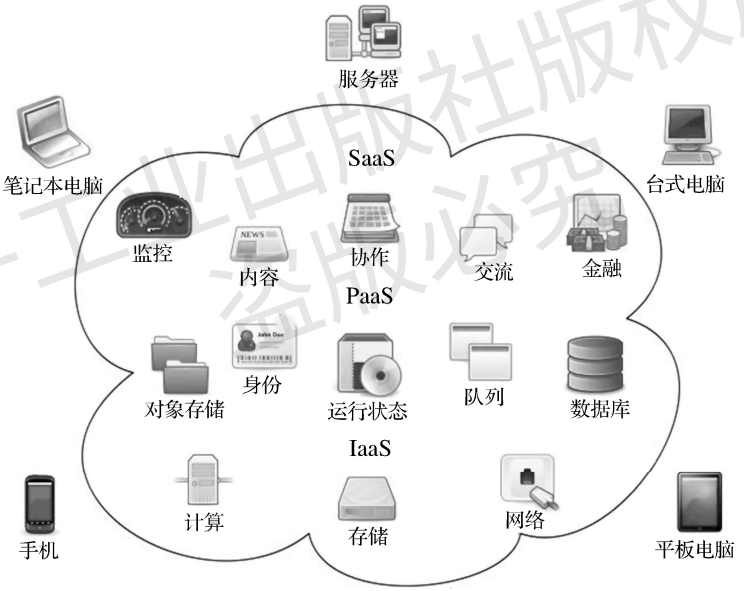

图 1-1-8　云计算应用示意图

NIST 同时明确了云计算的五个特性、三种服务模型和四种部署模式。其中，五个特性如下。

（1）按需提供服务：用户可以根据自己的需求，单方面完成对计算资源的获取（如服务器租用时间、网络存储大小），而不需要与供应商进行交流。

（2）宽泛的网络访问：遵循相应的标准就能通过网络访问到云计算的资源，这就保证了各种各样的客户端（手机、平板电脑、笔记本电脑等）都能实现对资源的访问。

（3）资源整合：供应商将计算资源整合成资源池，采用多租户模式可以同时向很多用户提供服务。资源池中的计算资源（物理的或虚拟的）可以根据用户需求动态地进行分配和再分配。

（4）快速可伸缩性：给用户分配的计算资源可以根据业务变化的需求快速地增多或减少。对于用户来讲，供应商的资源可以看成是无限多的，而且可以随时无限量地购买使用。

（5）计量付费服务：云计算系统能够按照合适的度量指标（如存储、处理、带宽和活跃用户数）、针对不同的服务类型进行计量，能够自动控制和优化资源的使用。资源的使用可以被监控和报告，以提升供应商和用户之间的透明度。

由上到下的三种服务模型如下。

（1）软件即服务（SaaS）：供应商通过部署在云基础设施上的应用程序为用户提供服务。用户不用去管控这些应用程序所依赖的基础设施（包括网络、服务器、操作系统或存储设备，甚至是单个应用程序的功能），除非需要对应用程序进行个性化设置。

（2）平台即服务（PaaS）：用户通过使用供应商所支持的编程语言和工具来把自己编写的或者购买的应用软件部署到云基础设施上，从而获得服务。用户不用去管控基础设施（包括网络、服务器、操作系统或存储设备），但是可以管理这些应用软件和一些环境配置。

（3）基础设施即服务（IaaS）：用户通过将软件（包括操作系统和应用软件）部署和运行到供应商所提供的基本计算资源（处理、存储、网络等）上来获得服务。用户不用去管控基础设施，但是可以管理操作系统、应用软件、存储方式，甚至网络组件（如主机防火墙）。

四种部署模式如下。

（1）私有云：云基础设施为某个组织所独占。这些基础设施可以由这个组织或者第三方来管理，存放位置可以在组织内部或外部。

（2）社区云：云基础设施为有共同关注点的某个社区中的多个组织所共有。这些基础设施可以由这些组织或者第三方管理，存放位置可以在组织内部或外部。

（3）公有云：云基础设施可以被公众或一个大的行业群体使用，但是归属权为云服务供应商所有。

（4）混合云：云基础设施是由两种或者两种以上的云（私有云、社区云或公有云）组成的，这些云在保持独立存在的同时通过标准化的或者专有的技术捆绑在一起，从而实现数据和应用的可移植性（如为了实现云间负载均衡的云爆发模式）。

以上云计算的三种服务模型和四种部署模式在实际物联网系统中都有所应用。NIST 对云计算的定义和解释为业界所认同，对于学习和研究云计算具有重大指导意义。

2. 大数据和数据挖掘

大数据（Big Data）是指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，需要采用划算的、创新的信息处理模式才能具有更强的洞察力、决策力和过程自动化能力。大数据一般都具有如下“3V”特性。

（1）海量（High Volume）：数据量级从太字节（TB）到泽字节（ZB）。

（2）高增长率（High Velocity）：近两年全球大数据相关产品和服务业务年均复合增长率超过 20%。

（3）多样化（High Variety）：数据来源不同；数据类型各式各样（结构化、半结构化和非结构化）。

数据挖掘是在大量的数据集合中寻找隐藏的、合理的和潜在有用的数据模式的过程。数据挖掘的目的是发现数据间未知的或以前未发现的关系。因此，数据挖掘也称为知识发

现、知识提取、模式分析、信息收获等。数据挖掘是一门交叉学科，涉及机器学习、统计学、人工智能和数据库等技术。

随着物联网的广泛应用，加上使用先进的自动数据采集和生成工具，物联网中的数据量急剧增大。如果使用传统的数据分析工具，那么很难对这样的数据进行足够广度和深层次的处理。大数据分析和数据挖掘技术克服了传统分析方法的不足，在物联网应用中，既能帮助人们准确地感知现在，也能有效地预测未来。

3. 机器学习和人工智能

人工智能（AI）是研究使各种机器模拟人的某些思维过程和智能行为（如学习、推理、思考、规划等），使人类的智能得以物化与延伸的一门学科。人工智能是一门边缘学科，属于自然科学和社会科学的交叉。除了计算机科学，人工智能还涉及信息论、控制论、自动化、仿生学、生物学、心理学、数理逻辑、语言学、医学和哲学等学科。人工智能学科研究的主要内容包括：知识表示、自动推理和搜索方法、机器学习和知识获取、知识处理系统、自然语言理解、计算机视觉、智能机器人、自动程序设计等方面。

机器学习（ML）是人工智能的一个子集，指的是不需要给机器系统一直编程，它就具有自我学习和优化的能力。简言之，机器学习是机器使用数据、统计学和反复试验来学习特定的任务，而不必为此任务专门编写代码。

在物联网中，将机器学习和人工智能与大数据分析和数据挖掘技术相结合，能够实现对物联网中产生的大量数据进行自动分析，进而实现计算机自动处理和可靠预测，从而提高物联网的运营效率和加强风险管理。

1.5.2 网络层技术

物联网无线通信技术除了第 1 部分 NB-IoT 基础理论篇 1.4.2 节的分类，还可以按照使用的频谱性质分为采用授权频谱（2G/3G/4G/5G、NB-IoT、eMTC 等）和采用非授权频谱（LoRa、Sigfox、Wi-Fi、蓝牙等）两类。

按照是否需要使用接入网关设备才能接入电信运营商，分为需要网关（LoRa、Wi-Fi、ZigBee 等）和不需要网关（2G/3G/4G/5G、NB-IoT、eMTC 等）两类。

按照数据传输速率不同，可以分为以下三类（见图 1-1-9）。

（1）低速率：＜100kbit/s，可用于农林牧渔、传感、抄表等数据采集类场景，典型技术如 NB-IoT、LoRa、Sigfox、各种中距离通信技术等。

（2）中速率：＜1Mbit/s，可用于智能家居、智能建筑、智慧电梯等交互协同类场景，典型技术如 2G/3G、eMTC 等。

（3）高速率：＞1Mbit/s，可用于视频监控、车联网、智慧医疗等监控控制类场景，典型技术如 3G/4G/5G、C-V2X、Wi-Fi 等。

可见，通信技术种类繁多，不同的技术具有不同的特点，适用不同的物联网应用场景，没有哪一种通信技术可以同时满足系统的所有需求。在物联网系统设计时，技术实现、功耗、成本、速率、安全性等都是需要考虑的重要因素。

本节将对物联网网络层中所采用的几种主流的中距离无线通信技术和远距离无线通信技术分别加以介绍，首先介绍几种主流的中距离无线通信技术。

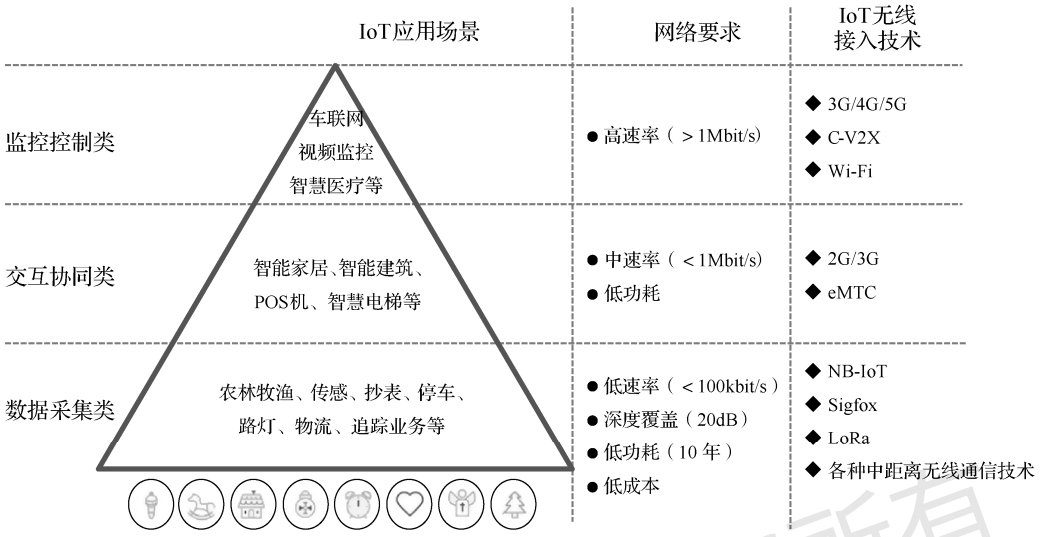

图 1-1-9　不同速率的无线通信技术

1. Wi-Fi

Wi-Fi 是 Wireless-Fidelity 的简称，基于 IEEE 802.11 标准，是一种无线保真的局域网通信技术。Wi-Fi 使用以太网通信协议，其组网只需要一个无线接入点（AP）或无线路由器即可。

早期的 Wi-Fi 技术采用 2.4GHz 或 5GHz 的高频频段，因此在传输距离、数据速率、功耗等方面都不能满足物联网的需求。2016 年，Wi-Fi 联盟发布的 IEEE 802.11ah 标准——Wi-Fi HaLow 是专门针对物联网设计的。HaLow 采用 900MHz 频段，覆盖范围最高 1000m，设备连接数可达数千个，可采用 BPSK、QPSK 或 QAM 的调制方式，支持 OFDM 和 MIMO，具有低功耗、干扰小等特点。

针对物联网应用的另外一种新的 Wi-Fi 技术是 IEEE 802.11af 标准，也称为超级 Wi-Fi。它旨在使用从几十兆赫兹到几百兆赫兹范围内的电视频率的白色空间（为电视频道保留的缓冲频段，随着电视的数字化而逐渐失去存在的意义），为人烟稀少地区提供无线高速物联网业务。这些白色空间频段具有良好的衍射能力，可以大大提高 Wi-Fi 的覆盖范围。IEEE 802.11af 采用 BPSK、QPSK 或 QAM 的 OFDM 调制技术，单空间流的最大数据速率可达 35.6Mbit/s，覆盖范围在室内可达数百米、室外可达上千米。

由于 Wi-Fi 并非国际标准，在实际应用时可能受到国家政策和使用频段等方面的限制。

2. 蓝牙

蓝牙（Bluetooth）是一种基于数据包传输，采用高速跳频（FH）技术，可支持点对点的语音和数据业务的中距离无线通信技术，常用于固定设备、移动设备和楼宇个域网（PAN）之间的通信连接。

蓝牙采用 GFSK 调制，占用 2.4GHz～2.485GHz 的 ISM 频段的特高频（UHF）无线电波，通信距离可达 100m 左右，最大数据传输速率为 2Mbit/s。

蓝牙曾被列为 IEEE 802.15.1 标准，后由蓝牙技术联盟（SIG）管理。4.0 版本后性能得到很大提升，最新的 5.2 版本中的功率控制技术可将蓝牙电池使用寿命延长至五年以上。

蓝牙在物联网中的应用主要存在以下两种场景。

一种场景是通过蓝牙网关部署网络。这种场景下，由于蓝牙点对点的通信方式，所以需要考虑如下问题。

（1）蓝牙网关的容量问题：一个蓝牙网关能够接入多少蓝牙设备。

（2）蓝牙设备的配对问题：蓝牙设备如果不能实现自动配对，大规模部署将是一个很麻烦的事情。

另一种场景是蓝牙设备不需要一直在线，而只在某些特殊情况下需要连接服务器。这种场景下，可以通过控制终端开启/关闭蓝牙功能来实现。

3. ZigBee

ZigBee 是 IEEE 802.15.4 标准的代称，是一种采用局域网协议，支持固定、便携或移动设备使用的无线通信技术。ZigBee 名称的由来有着仿生学的意味：蜜蜂（Bee）通过“嗡嗡”(Zig)地抖动翅膀飞翔的方法来向同伴传递消息，这样就形成了蜂群的通信网络。ZigBee 技术具有如下特点。

（1）大连接：受网关的硬件配置限制，一般可以支持数百个终端。

（2）短距离：单点传输距离在 10～100m 的范围内。

（3）工作频段灵活：典型频段包括 2.4GHz 的 ISM 非授权频段、欧洲的 868MHz 频段和美国的 915MHz 频段。

（4）低速率：对应上述三个频段，最高速率依次为 250kbit/s、20kbit/s 和 40kbit/s。

（5）低功耗：电池工作时间可以长达 2 年左右，在休眠模式下可达 10 年。

（6）自组织：节点间自动通信进行组网，采用动态路由的网状结构。

（7）安全性高：采用跳频技术，支持数据完整性检查和加密，支持鉴权和认证。

ZigBee 是专门针对低功耗无线传感器网络设计的，适用于对一些数据传输速率要求不高的中距离通信物联网场景。

这里给出了几种中距离无线通信技术的对比，如表 1-1-2 所示。有关 Z-Wave、Dash7、UWB 等中距离无线通信技术请参考其他资料进行学习。

表 1-1-2　几种中距离无线通信技术对比

性能	技术					
	Wi-Fi	蓝牙 5.0	ZigBee3.0	Z-Wave	Dash 7	UWB
标准	IEEE 802.11ah	IEEE 802.15.1	IEEE 802.15.4	Z-Wave 联盟	ISO18000-7	IEEE 802.15.3a
频段	＜1GHz	2.4GHz	868MHz，915MHz，2.4GHz	＜1GHz	433MHz，868 MHz，915 MHz	3.1GHz～10.6GHz
最大距离	数千米	300m	100m	30m	1000m	10m
最大速率	24Mbit/s	2Mbit/s	250kbit/s	9.6kbit/s，40kbit/s，100kbit/s	9kbit/s，55.55kbit/s，166.667kbit/s	480Mbit/s
功耗	中	低	低	低	低	低
成本	低	低	中	中	低	低
连接数	几千个	几个	几百个	几百个	几百个	几百个
带宽	1MHz，2MHz，4MHz，8MHz，16MHz	1MHz，2MHz	2MHz，5MHz	300kHz，400kHz	25kHz，200kHz	＞500MHz

要把数据传输得更远往往意味着需要更高的能耗和更大的成本，因此，中距离通信和远距离通信在技术实现、功耗、成本等方面均不相同。

传统的移动通信系统（2G、3G、4G 等）主要是为人和人之间通信而设计的，相对于物联网应用来说，协议过于复杂，终端功耗过高，数据传输速率对某些物联网场景纯属浪费，因此并不直接适用于物联网应用。

目前，主流的四大物联网系统（NB-IoT、LoRa、eMTC 和 Sigfox）都属于 LPWA 网络。LPWA 网络具有四大基本特性：广覆盖、大容量、低功耗和低成本。除此之外，一般还具有低速率和高时延等特点。

如前所述，四大物联网系统中 LoRa 和 Sigfox 使用非授权频谱（也称为免许可频谱），不需要支付频谱费用，但仍有政府对频谱的使用进行规范，以确保不同技术可以相互兼容。同时，非授权频谱系统存在干扰大、安全性低等问题。NB-IoT 和 eMTC 都使用授权频谱，也都属于 C-IoT（蜂窝物联网）技术，即使用政府授权的特定专用无线频段，需要支付频谱费用，以传统电信运营商为主体运营者，技术规范基于蜂窝网络技术，并由 3GPP 来定义和发布。由于 C-IoT 都是对传统蜂窝网络进行裁剪和优化以适应物联网应用的，因此，相比于 LoRa 和 Sigfox，其系统复杂度、成本和功耗都相对要高一些。

下面就对四种主流物联网技术分别加以详细介绍。

1. LoRa

LoRa 是由美国 Semtech 公司收购、由 LoRa 联盟制定的远距离无线通信技术标准。LoRa 这个名字源于远距离（Long Range）这个词组，其名字直接体现了该技术的特点——覆盖范围广（链路预算达到 168dB）。

LoRa 采用线性 Chirp 扩频调制，射频脉冲信号的载波频率进行线性变化，这种方式具有功耗低、抗干扰能力强、接收灵敏度高和传输距离远的特点，已经在军事和航天通信方面应用多年。而且，LoRa 允许用户自行设定扩频调制的带宽（7.8～500kHz）、扩频因子（6～12）和编码效率（1/2、4/7、4/6 和 4/5），从而可以在带宽占用、数据速率、链路预算改善和抗干扰性能之间达到更好的平衡。

LoRa 采用速率自适应（ADR）技术，具有很大的数据速率范围（0.3～50 kbit/s），网络服务器根据链路质量，独立地管理每个终端设备的数据速率和发射功率，这就实现了网络容量和速率的平衡，使终端可以获得更低的功耗，最大化电池使用寿命（长达十年以上），通过增加网关可以轻松实现扩容。

LoRa 采用异步空口结构，将空口的 MAC 层协议处理功能上移，站点网关只进行数据转发，用户调度都在机房的网络服务器上完成，这就大大简化了空口操作。

LoRa 采用基于 TDOA（精度为 500m）、RSS（精度为 1000m）和 DRSS（精度为 500m）免 GPS 定位技术，只需要每个网关通过 GPS 进行同步，以获得共同的时间基准，再通过更多的信道（获得 50%的频率分集增益）、更多的网关（获得 25%的网关分集增益）、更多的天线和使用统计技术，来提高定位精度。LoRa 还开放了其 API 接口，以允许系统集成商使用可用的第三方算法以提高位置精度。

LoRa 的典型覆盖范围是 2000～5000m（城市环境）和 15km（郊区环境），在极端情况

下，可以覆盖整个城市或者几十千米。LoRa 支持低功率、大频率范围的收发，频率范围为137～1020MHz，接收灵敏度为−148dBm，接收电流为 10.3mA，包长最大为 256 个字节。

LoRaWAN 是为 LoRa 网络设计的一套通信协议和系统架构，其空中接口协议分层架构图如图 1-1-10 所示。LoRaWAN 在协议和网络架构的设计上，充分考虑了节点功耗、网络容量、QoS、安全性和网络应用多样性等因素。而且在协议中定义了 Class A/B/C 三类终端设备，这三类终端设备基本覆盖了物联网所有的应用场景。

图 1-1-10　LoRaWAN 空中接口协议分层架构图

LoRaWAN 的网络架构如图 1-1-11 所示，其中包含了终端、网关、网络服务器和应用服务器四个部分。网关和终端之间采用星形网络拓扑，由于 LoRa 的长距离特性，它们之间得以使用单跳传输。空口采用基于 Aloha 协议的异步通信，上行可以多点接收。

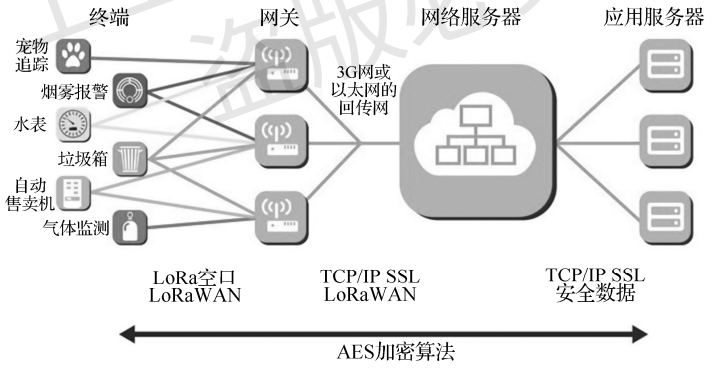

图 1-1-11　LoRaWAN 的网络架构

2. Sigfox

Sigfox 技术由同名的法国 Sigfox 公司设计研发，是专为微小上行链路数据容量的传感器网络而设计的，是技术成熟度最高的远距离物联网通信技术。

Sigfox 的最大特点是采用非授权频谱的超窄带（UNB）技术。超窄带技术利用极窄的物理带宽（采用 FDMA 技术，子信道仅为几百赫兹）进行通信。由于信号本身带宽小，带内的随机噪声功率很低，因而灵敏度非常高，相比于其他系统能够传输更远的距离，具有更强的穿透能力。

Sigfox 技术优势如下。

（1）终端成本低：在现有遥控器或者中距离传输的芯片硬件的基础上更新软件即可，

其芯片价格可低至 1 美元。

（2）功耗低：对于低频率使用的业务，终端电池的使用寿命可达十年以上。

（3）覆盖性能优：在链路预算为 162dB 的前提下，在城市环境中可传输 3～10km；在农村环境中可传输 30～50km。

（4）抗干扰能力强：采用 UNB 技术使其在单位频带上有更高的功率谱密度，再加上跳频、帧重复和多基站连接功能，使其具有强大的抗干扰能力。

（5）网络容量大：可支持三百万左右的终端连接数。

另外，Sigfox 技术也存在局限性。

（1）终端通信能力有限：使用非授权频谱会受到某些限制，如在 Sigfox 技术应用最广的欧洲地区，其管理法规要求 868MHz 频段每个终端的发射占空比必须小于 1%。

（2）数据传输速率低：Sigfox 技术可支持的数据传输速率为 10～1000bit/s，但是对于有极高功耗要求的物联网来说，100bit/s 的速率更合适。

（3）空口安全性差：采用非授权频谱本身就易受到干扰，Sigfox 技术空口设计过于简单，无法采用有效的加密和认证，存在数据被伪基站窃听并破解的风险。

（4）下行传输能力有限且无法支持软件升级更新：Sigfox 技术支持上/下行双向通信，但通信必须由终端发起。

Sigfox 网络称为 LTN（低吞吐率网络）。Sigfox 技术的 LTN 网络架构如图 1-1-12 所示，LEP（LTN End-Point）是终端设备，负责采集传感器数据。LAP（LTN Access Point）是网关，负责接收和转发无线数据。LEP 和 LAP 之间的无线接口（也称为空口）采用 A 接口协议。LAP 与 WAN 云通过 B 接口协议连接。WAN 云主要由各种类型的服务器组成（通过 C、C′、D、F 等接口实现连接）：LTN 服务器负责存储和转发应用层数据和管理网络；CRA（Center of Registration and Authentication）是注册鉴权中心，负责管理 LEP 和 LAP 的身份标识；OSS/BSS（Operation Support System/Business Support System）是操作支持系统或业务支持系统，负责网络管理；网络中还存在各种应用程序提供商服务器。

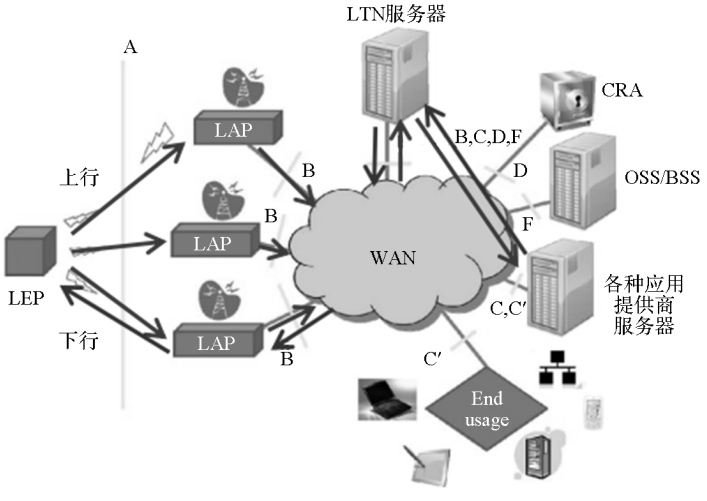

图 1-1-12　Sigfox 技术的 LTN 网络架构

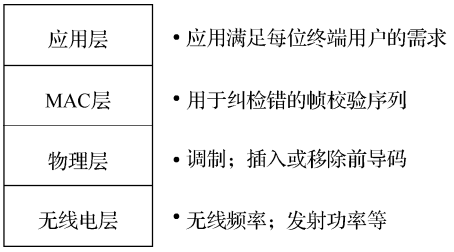

图 1-1-13　Sigfox 空中接口协议分层架构图

图 1-1-13 所示为 Sigfox 空中接口协议分层架构图，它由无线电层、物理层、MAC 层和应用层组成。各层功能如下。

（1）无线电层：负责终端设备和基站/网关的频率分配和收发功率要求。

（2）物理层：负责前导码插入（发送端）和移除（接收端）。Sigfox 在上行链路中使用 BPSK 调制，下行链路中使用 GFSK 调制。

（3）MAC 层：负责 MAC 消息的管理。按照定义的格式要求为上/下行链路准备数据帧，主要用于纠检错的帧校验序列（Frame Check Sequence，FCS）。

（4）应用层：支持 SNMP、HTTP、MQTT、IPv6 等各种接口协议，以支持不同的应用。

3. eMTC

eMTC 是增强型机器类通信（enhanced Machine Type Communication）的简称，是 3GPP 在 MTC 技术的基础上，在 R13 版本正式引入的。eMTC 是在 LTE 协议基础上，专门为满足中速率（上/下行峰值速率可达 1Mbit/s）物联网业务而进行裁剪和优化的蜂窝物联网技术，所以也称为 LTE-M（LTE-Machine-to-machine）。

相比于原有的 LTE 系统，窄带的 eMTC 具有以下几个特性。

（1）系统复杂度大幅度降低，成本得到了极大的优化（eMTC 芯片目标成本在 1～2 美元）。

（2）功耗极度降低，电池续航时间大幅度增强。

（3）网络的覆盖能力大大加强。

（4）网络覆盖的密度增强。

eMTC 的关键技术如下。

（1）15dB 增益的深度覆盖技术。

eMTC 的深度覆盖主要源于两个方面：一是在连续的子帧的相同资源块中调度相同数据的时域重传技术（将在第 1 部分 NB-IoT 基础理论篇 4.1 节介绍 NB-IoT 的这项技术），这样在接收端通过 HARQ（混合自动重传请求，将在第 1 部分 NB-IoT 基础理论篇 3.5 节介绍 NB-IoT 的这项技术）合并这些数据就可以获得 12dB 左右的合并增益；二是通过跳频技术，可以获得 2～3dB 的频域分集增益。

（2）节电技术。

eMTC 通过 PSM（省电模式）和 eDRX（扩展非连续接收）来延长终端电池的使用寿命。其中，99% 的待机时间处于 PSM，所消耗的电量小于 1%。电池使用寿命可以长达十年。本书将在第 1 部分 NB-IoT 基础理论篇 4.3 节介绍 NB-IoT 的节电技术。

（3）定位技术。

eMTC 采用 UTDOA（上行到达时间差）技术，不需要 GPS 也可以实现定位。UTDOA 通过三个基站构成的不同圆的交点估算终端位置，测试基站越多定位精度越高。而且，UTDOA 的实现不需要终端新增定位芯片。

（4）无缝切换技术。

eMTC 支持无缝切换以保证用户体验的平滑连续。具体来讲，eMTC 支持连接态的移动性管理，给用户提供连续的业务体验。无缝切换技术是 eMTC 与 NB-IoT 的最大区别之一。eMTC 还支持灵活的组网策略，满足运营商业务分层、负载平衡等需求。eMTC 通过自动频率控制来校正终端的频率偏差，以降低多普勒频移对解调的影响，从而能够支持终端在高速移动场景下的业务性能。

eMTC 端到端网络架构和 LTE 保持一致，不需要网络改造，只需要升级软件即可支持。从网络设备数量最多的基站角度来看，eMTC 可以重用 LTE 频谱资源，重用 LTE 射频、天馈等硬件资源，只需要软件升级即可。eMTC 的用户设备通过支持 1.4MHz 的射频和基带带宽，可以直接接入现有的 LTE 网络。

4. NB-IoT

NB-IoT 是窄带物联网（Narrow Band Internet of Things）的简称，是 3GPP 在 LTE 协议基础上针对低速率（100kbit/s～1Mbit/s）物联网业务而制定的蜂窝物联网技术标准。

NB-IoT 只占用 180kHz 的带宽，可直接部署于 GSM 网络、UMTS 网络或 LTE 网络，以降低部署成本、实现平滑升级。NB-IoT 支持以下三种部署方式（见图 1-1-14）。

（1）独立（Standalone）部署：通常是对 GSM/UMTS/LTE 频谱进行重耕或者使用空闲零散的频谱资源部署 NB-IoT。

（2）保护带（Guard band）部署：在 LTE 的保护带中部署 NB-IoT，这就要求 LTE 系统带宽在 10MHz 或以上。

（3）带内（In-band）部署：在 LTE 的资源块（RB）资源上直接部署 NB-IoT，这种方式相对应 LTE 可用的 RB 资源会减少。

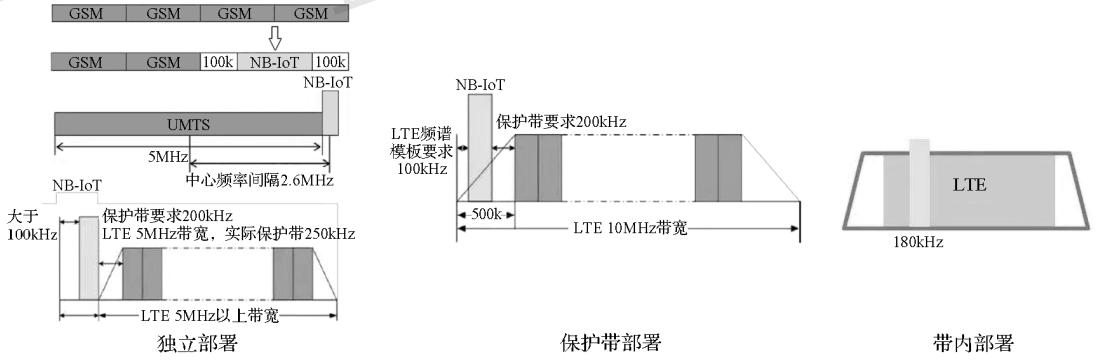

图 1-1-14　NB-IoT 的三种部署方式

NB-IoT、eMTC 同属 3GPP 标准内的 LPWA 技术，两者在标准化进程、产业发展、网络商用等方面几乎是齐头并进的，两者就像 3GPP 标准下的一对双胞胎，有很多相似之处，但也有一些区别，如表 1-1-3 所示。

表 1-1-3　NB-IoT 与 eMTC 的区别

性能	技术	
	NB-IoT	eMTC
频段	FDD	FDD，TDD
双工方式	半双工	半双工/全双工
部署方式	独立/保护带/带内	LTE 带内
上行覆盖	增益：20+dB	增益：15+dB
下行覆盖	164dB	156dB
信道带宽	180kHz	1.4MHz
峰值速率	UL：250kbit/s（多频）/200kbit/s（单频） DL：250kbit/s	UL：1Mbit/s（全双工）/375kbit/s（半双工） DL：1Mbit/s（全双工）/300kbit/s（半双工）
移动性	低速，小区重选	低/中/高速，小区切换
时延	秒级	100ms
业务	数据	数据，语音
芯片成本	目标：＜1 美元	目标：1～2 美元
子载波带宽	UL：15/3.75kHz（单频），15kHz（多频） DL：15kHz	UL：15kHz DL：15kHz
TTI	1ms	1ms/8ms
调制方式	BPSK，QPSK	QPSK，16QAM

由表 1-1-3 可见，在频段、移动性、峰值速率等有较高要求时，eMTC 技术占明显优势；反之，如果对这些方面要求不高，而对芯片成本、上/下行覆盖等有更高要求时，则可选择 NB-IoT。两者在不同领域有不同的优势，既竞争又互补。

为了方便对比 LoRa、Sigfox、eMTC 和 NB-IoT 四种 LPWA 技术，现给出表 1-1-4。具体选择哪种 LPWA 技术，与物联网性能需求、国家政策、频谱规划、运营商的实力等都有很大关系。

表 1-1-4　四种 LPWA 技术对比

技术	性能								
	频谱	信道带宽	吞吐量	容量	覆盖（MCL）	时延	模组成本	电池寿命	建网
LoRa	非授权频谱	7.8~500kHz	50kbit/s	NA	168dB	NA	5 美元	10 年	新建网络
Sigfox	非授权频谱	几百赫兹	100bit/s	NA	162dB	NA	5 美元	10 年	新建网络
eMTC	授权频谱	1.4MHz	1Mbit/s	每小区>50k	156dB	100ms	5~10 美元	10 年	LTE 网络软件升级
NB-IoT	授权频谱	180kHz	250kbit/s	每小区>50k	164dB	秒级	5 美元	10 年	LTE 网络软件升级

1.5.3　感知层技术

物联网终端的结构组成框图和物联网终端的实物组成分别如图 1-1-15 和图 1-1-16 所示。从硬件上来看，物联网终端最核心的部分是芯片，芯片主要负责通过无线接口和物联网网络层进行通信。芯片加上射频前端电路就构成了模组或模块（Module），模组主要完成无线信号

的收发处理。MCU 是物联网终端的核心控制部件，负责终端各个组成部分的管理和协调工作。传感器负责采集数据，定位单元负责提供终端位置信息。电池供电电路可以采用 LDO 低压差线性稳压器，以最大限度延长电池寿命，同时降低系统复杂度和成本。如果是电信运营商的网络，终端还需要插入 SIM/USIM 卡，以完成终端在网络中的身份识别和认证。

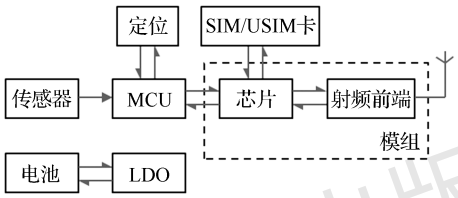

图 1-1-15　物联网终端的结构组成框图

图 1-1-16　物联网终端的实物组成

从分层协议角度来看，现在的物联网芯片/模组完成的是应用层以下各层的功能，如图 1-1-17 所示，应用层功能还要靠设备（主要是 MCU）来实现。未来，相信随着物联网的大规模普及和电子工艺技术的进一步提升，只靠物联网芯片/模组即可实现所有协议层功能。

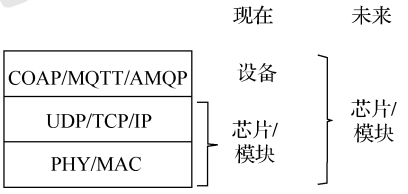

图 1-1-17　物联网终端的软件组成

物联网终端涉及的关键技术有操作系统、中间件、传感器、识别技术等，这里仅进行简单介绍，详情请参考其他相关教材。

1. 操作系统

终端智能化是物联网发展的基础和必然趋势。为了使物联网终端更智能，MCU 中可以采用带有操作系统的 X86/ARM/DSP/MIPS/FPGA 等芯片。这里的操作系统不能是普通嵌入式操作系统，而应该是符合 3GPP 规范的轻量级操作系统，即具有可伸缩的内核、μA 级功耗和 μs 级响应。采用轻量级操作系统，可使物联网终端在以下方面获得智能化。

（1）管理智能。

可以实现不同类型、不同接口传感器的接入（即插即用）和算法开发的统一管理；可以提高端/管/云协同的安全管理能力，降低终端被攻击的风险。

（2）连接智能。

可以实现近距离、远距离各种不同类型的通信协议的互联互通。

（3）组网智能。

可以帮助终端自组织网络（SON）快速组网、稳定组网，接入更多的组网设备。

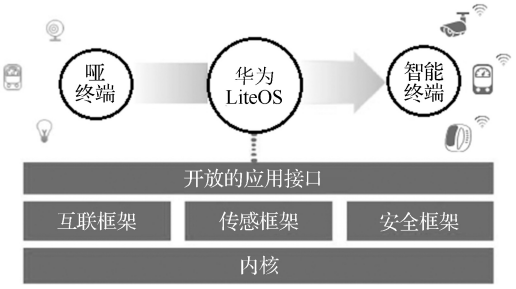

图 1-1-18　LiteOS 框架结构

这里以华为 LiteOS 操作系统为例，其框架结构如图 1-1-18 所示。有了 LiteOS 操作系统，物联网终端从哑终端变成了智能终端。

2. 中间件

对于不带操作系统的物联网终端，也可以利用中间件来实现一些功能。中间件是一种计算机软件，它有两种模式：一种是介于操作系统与应用软件之间的；另一种是介于硬件和应用软件之间的，发挥支撑和信息传递的作用。这里的中间件主要是指介于硬件和应用软件之间的。

由于物联网终端形态各异、传感器种类繁多、系统软硬件环境千差万别，物联网的应用开发难度很大，所以利用终端上的中间件来屏蔽底层软硬件差异，可以大大降低物联网应用开发的复杂度。同时，中间件也可以提供基础通信功能（因此也被称为基础通信套件或通信套件），对数据包进行封装，并调用底层接口实现网络连接。当物联网终端（芯片/模组）集成了这样的中间件后，对于这些芯片/模组的应用开发只需要通过中间件提供的接口进行简单操作（如 AT 指令）即可。

中间件实现 NB-IoT 网络连接如图 1-1-19 所示，为了说明中间件在 NB-IoT 系统中的位置和作用，可以将 NB-IoT 系统简单地分为终端侧和网络服务侧两个部分。而终端上的中间件就起到终端侧与网络服务侧连接和通信的作用。中间件提供了一套标准的 SDK（Software Development Kit，软件开发工具包），规范了终端设备管理接口的定义，并统一了终端侧的应用连接与通信协议，从而实现与网络服务侧的简易对接。

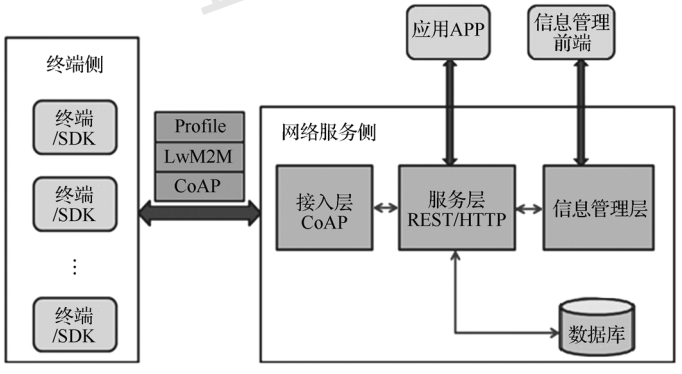

图 1-1-19　中间件实现 NB-IoT 网络连接

图 1-1-19 中的中间件采用物联网协议 CoAP 作为应用通信协议，以 LwM2M（Lightweight Machine-To-Machine，轻量级机器对机器）协议作为设备管理接口框架和资源管理模型基础（LwM2M 协议基于 CoAP 协议，而 CoAP 协议基于 UDP 协议）。网络服务侧采用相对成熟的互联网 Web 服务相关技术。接入层负责应用协议转换和 Web 服务协议之间的转换。之所以推荐 CoAP 作为通信协议，是因为它可以使接入层很方便地实现 CoAP 和 HTTP 之间的转换。服务层采用 REST/HTTP 架构。网络服务侧的后面需要提供信息管理数据库并进行信息管

理维护（信息管理层），以保证对终端设备中相关对象的识别，并与终端设备的认证信息一致。

3. 传感器

传感器是物联网终端进行感知和检测的重要部件，它可以检测周边环境的物理变化（温度、湿度、加速度、光学、图像、电磁场等），并将检测到的物理量以电子信号形式输出。在不同的物联网场景下，可能需要不同类型的传感器。传感器的常见分类如下。

（1）按元件特性分类。

传感器按元件特性分类，可分为电阻式传感器、电感式传感器、电容式传感器、压电式传感器、磁电式传感器、热电式传感器、光电式传感器、数字式传感器、光纤式传感器、超声波传感器、热敏传感器、模拟传感器等。

（2）按用途分类。

传感器按用途分类，可分为压力敏和力敏传感器、位置传感器、液位传感器、能耗传感器、速度传感器、加速度传感器、射线辐射传感器、热敏传感器。

（3）按原理分类。

传感器按原理分类，可分为振动传感器、湿敏传感器、磁敏传感器、气敏传感器、真空度传感器、生物传感器等。

（4）按输出信号分类。

传感器按输出信号分类，可分为模拟传感器、数字传感器、膺数字传感器、开关传感器。

4. 识别技术

物联网终端常用的识别技术有条形码、RFID、NFC、IrDA 等。

（1）条形码。

根据编码方法和信息存储容量不同，条形码包括一维码、二维码和三维码，如图 1-1-20 所示。但条形码的名称源于最早的一维码。一维码只在水平方向一个维度上由一组按一定规则排列的黑、白条组成，可以用来表示字符和数字。二维码包括堆叠式（也叫行排式）和矩阵式两种，堆叠式在形态上是由多行短截的一维条码堆叠而成的；矩阵式以矩阵的形式组成，在矩阵相应元素位置上用“点”表示二进制“1”，用“空”表示二进制“0”，由“点”和“空”的排列组成代码。二维码能够记录汉字和图片信息，同时信息的安全性得到提高。三维码在二维码基础上增加了视觉属性（24 层颜色），其编码方式是先将文本编译成一串二进制数字，然后通过特定的算法并结合图片整体的色彩内容，将该二进制数字串与图像信息编码为一组可以通过特定规则解读的阵列。三维码能够记录计算机中的所有信息。目前物联网中主要应用的是一维码和二维码。

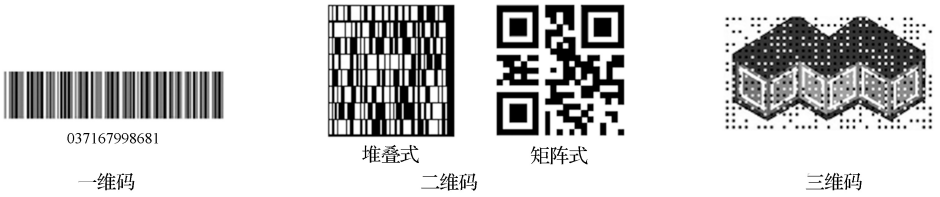

图 1-1-20　各种条形码

条形码技术涉及条码的编码技术、条码标识符号的设计、快速识别技术和计算机管理

技术等，它是物联网感知层重要的物品信息识别手段。

条形码识别系统如图 1-1-21 所示。首先通过某种图像采集器采集条形码的图像信息，然后经过放大整形电路，最后通过译码器译码转变成二进制数据存储到计算机中或者通过网络传输到物联网中。

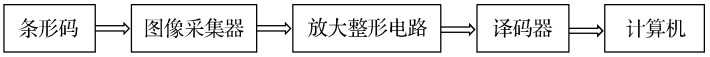

图 1-1-21　条形码识别系统

（2）RFID。

RFID（Radio Frequency Identification，无线射频识别）是 20 世纪 90 年代开始兴起的一种自动识别技术。它利用射频信号通过空间电磁耦合实现无接触信息传递，并通过所传递的信息实现物体识别。

典型的 RFID 系统主要由电子标签和读写器组成，如图 1-1-22 所示。电子标签中存储着规范且具有互用性的信息。电子标签和读写器中都集成了天线。当电子标签进入由读写器发出射频信号而产生的磁场后，凭借感应电流所获得的能量发送出存储在产品中的信息（无源标签或者叫被动标签），或者主动发送某一频率的信号信息（有源标签或者叫主动标签）；读写器读取信息并解码后，送至数据管理系统/计算机中进行有关数据处理。

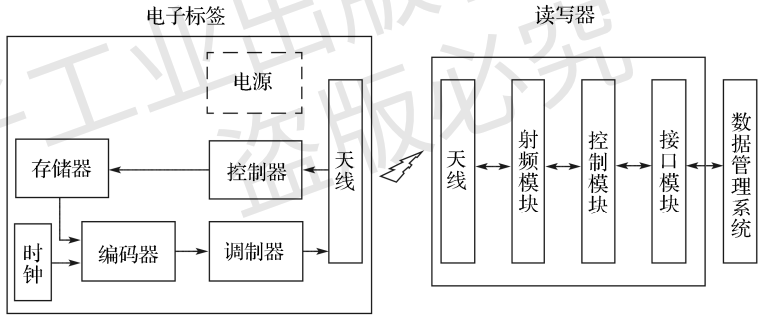

图 1-1-22　RFID 系统组成

RFID 的工作频段比较丰富，而且频段不同其读写距离也不同，因而应用场景也相同，如表 1-1-5 所示。

表 1-1-5　RFID 的工作频段、读写距离及应用场景

工作频段	读写距离	应用场景
低频 135kHz	1m 以下	动物识别与监控 货物、防盗管理
高频 13.5MHz	3m 以下	门禁系统 废弃物管理 智能卡系统
超高频 860～960MHz	10m 以下	全球供应链管理 集装箱追踪
微波 2.45GHz 或 5.8GHz	大于 10m	车辆识别 区域定位

RFID 作为条形码的无线版本，具有条形码所不具备的防水、防磁、耐高温、使用寿命长、读取距离大、标签上数据可加密、存储数据容量大、存储信息更改自如等优点，是物联网感知层终端设备识别的重要手段。

（3）NFC。

NFC（Near-Field Communication，近场通信）是一种近距离高频无线通信技术。它的工作频率为 13.56MHz（ISM 频段），理论上最大传输距离为 20cm（一般产品都采用功率抑制技术将其设置为 10cm，以获得更高的安全性）。NFC 信号带宽只有 14kHz，因此传输速率也很低，可以支持 106kbit/s、212kbit/s 或者 424kbit/s 三种传输速率。

NFC 与 RFID 同属于 ISO/IEC 标准序列，是在 RFID 的基础上发展而来的，可以向下兼容 RFID，同时，具有自己的特点和优势。

① NFC 工作距离短，具有更高的安全性。

② NFC 成本低，功耗更低。

③ NFC 在单一芯片上集成了感应式读卡器、感应式卡片和点对点通信的功能，而 RFID 不支持点对点通信，读卡器和卡是分离的实体。

④ NFC 连接速度非常快，可以帮助蓝牙设备或 Wi-Fi 设备实现快速连接。

⑤ NFC 有三种工作模式：读卡器（主动读取带有 NFC 芯片的对象中的信息）、仿真卡（就像一张卡，通过内置的射频器被动地读取卡内信息）和点对点通信（两个 NFC 设备都处于双向主动模式）。

在物联网中，NFC 和 RFID 侧重于不同的应用场景。RFID 更多地应用在生产、物流、跟踪和资产管理上，而 NFC 则在门禁、公交、手机支付等领域发挥着巨大的作用。

（4）IrDA。

IrDA 是由与其同名的红外数据通信协会（Infrared Data Association）制定的，是一种串行、半双工、点对点红外线通信技术。红外线频率主要集中在 300～400GHz，它的传输距离在 1m 以内，数据传输速率一般为 4Mbit/s，最高可以达到 16Mbit/s，传输角度为 15°～30°。

IrDA 数据传输的基本模型如图 1-1-23 所示。来自 MCU 或网络的二进制数据经过编码、调制等处理，再通过红外线发射器转变成红外线脉冲光信号发送出去；另外，红外线接收器将接收到的红外线信号转变成数字电信号，再经过解调、解码等处理恢复成二进制数据。这里的发射器和接收器通常使用红外收发对管。

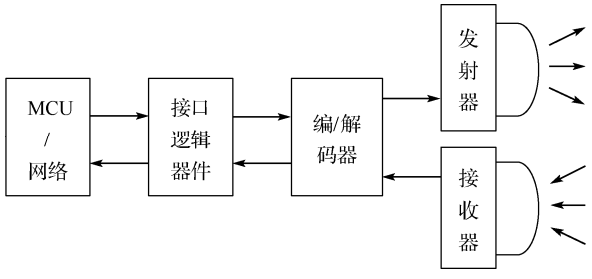

图 1-1-23　IrDA 数据传输的基本模型

IrDA 通信具有成本低廉、简单易用、功耗低等优点。此外，其发射角度小的特点在一

定程度上提高了通信的安全性。但 IrDA 是一种视距通信，传输空间不能被其他物体阻隔。而且，IrDA 通信只能用于两台设备之间，不能灵活组网。

IrDA 大都应用在家庭和办公环境下的个域网（PAN）场景中。目前，很多家电遥控器和小型移动设备都支持 IrDA 通信。IrDA 技术如何在物联网中得到广泛应用还有待研究。

1.5.4 物联网安全

安全问题是物联网运作的最大挑战，而且物联网的不同层次有不同的安全需求，因此需要建立不同的安全机制，下面分别加以说明。

1. 感知层

为了便于分析，这里将传感器网络也纳入感知层。物联网的感知层可能遇到的安全挑战如下。

（1）节点被非法控制。

① 网关节点被非法控制（节点密钥被窃取）。

② 普通节点被非法捕获（由于没有获得节点密钥而没被控制）。

（2）节点受来自网络的 DoS（Denial of Service，拒绝服务）攻击。

（3）接入物联网的超大量节点的识别、认证和控制问题。

针对上述挑战，感知层的安全需求包括以下几点。

（1）机密性：多数网络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器网络。

（2）密钥协商：内部节点进行数据传输前要先协商会话密钥。

（3）节点认证：数据共享的网络需要节点认证，以限制非法节点的接入。

（4）信誉评估：一些重要网络需要对可能被非法控制的节点行为进行评估，以降低入侵危害（某种程度上相当于入侵检测）。

（5）安全路由：几乎所有网络内部都需要不同的安全路由技术。

针对上述安全需求，感知层应建立以下安全架构。

（1）在网络内部，需要有效的密钥管理机制，用于保障传感器网络内部通信的安全。

（2）网络类型的多样性导致安全服务需求不能统一，但网络内部的安全路由、连通性解决方案等都可以相对独立地使用，同时机密性和认证性都是必要的。

2. 网络层

物联网网络层将主要遇到以下安全挑战。

（1）DoS 攻击、DDoS（分布式拒绝服务）攻击。

（2）假冒攻击、中间人攻击等。

（3）跨网络架构的安全认证等。

网络层的安全需求可以概括为以下几点。

（1）数据机密性：保证数据在传输过程中不被泄露。

（2）数据完整性：保证数据在传输过程中不被非法篡改或被非法篡改的数据容易被检测出来。

（3）数据流量机密性：某些特殊场景需要对数据流量信息进行保密，因此需要数据流量机密性。

（4）DDoS 攻击检测与预防：既包括对整个网络 DDoS 攻击的检测与防护，还包括对脆弱节点的 DDoS 攻击的防护。

（5）移动网中认证与密钥协商（AKA）机制的一致性或兼容性、跨域认证和跨网络认证（基于 IMSI）。

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。

端到端的机密性需要建立以下安全机制。

（1）端到端的认证机制。

（2）端到端的密钥协商机制。

（3）密钥管理机制。

（4）机密性算法选取机制。

在这些安全机制中，根据需要可以增加数据的完整性保护服务。

节点到节点的机密性，需要节点间的 AKA 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，针对单播通信、组播通信和广播通信等不同的网络传输模式也应该有相应的认证机制和机密性保护机制。

3. 平台层

平台层的安全挑战如下。

（1）来自超大量终端的海量数据的识别和处理。

（2）智能可能变为低能。

（3）自动控制变为失控。

（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。

相应地，平台层应包含以下安全机制。

（1）可靠的认证机制和密钥管理方案。

（2）高度的数据机密性和完整性服务。

（3）可靠的密钥管理机制，包括 PKI（公钥基础设施）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、定位和跟踪机制。

4. 应用层

应用层的安全挑战和安全需求主要来自以下几个问题。

（1）如何根据不同访问权限对同一个数据库内容进行筛选？
（2）如何在提供用户隐私信息保护的同时又能正确认证？
（3）如何解决信息泄露追踪问题？
（4）如何进行计算机取证？
（5）如何销毁计算机数据？
（6）如何保护电子产品和软件的知识产权？

针对以上问题，应用层应该设置如下安全机制。
（1）有效的数据库访问控制和内容筛选机制。
（2）不同场景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）有效的计算机取证技术。
（5）安全的计算机数据销毁技术。
（6）安全的电子产品和软件知识产权保护技术。

物联网的安全问题不仅仅是技术问题，还会涉及教育培训、信息安全管理、口令管理等非技术因素。

综上分析，物联网在不同层次应该采取不同的安全技术。物联网安全技术分类如图 1-1-24 所示，请参考其他相关教材进行学习。

应用环境安全技术 可信终端、身份认证、访问控制、安全审计等
网络环境安全技术 无线网安全、虚拟专用网、传输安全、安全路由、防火墙、安全域策略、安全审计等
信息安全防御关键技术 攻击监测、内容分析、病毒防治、访问控制、应急反应、战略预警等
信息安全基础核心技术 密码技术、高速密码芯片、PKI公钥基础设施、信息系统平台安全等

图 1-1-24　物联网安全技术分类

习题 1

1.1　试用自己的话概括出物联网的定义。
1.2　试到 3GPP 官网上任意下载一个 R16 版本的技术文档。
1.3　试说明 NB-IoT 与 5G 移动通信技术标准的关系。
1.4　试对本地区 NB-IoT 网络发展现状进行简单的调研。
1.5　绘制简单的物联网分层架构图，说明各层的功能并列举各层所涉及的关键技术。
1.6　试将物联网的四个分层同一张人体结构图建立起对应关系。
1.7　试从电信运营商的角度解释物联网平台层存在的必要性。
1.8　通过查询资料，进一步学习物联网七大通信应用协议，尤其是 CoAP 和 REST/HTTP 协议。

1.9　了解移动通信网中 IMEI 和 IMSI 的含义和作用。

1.10　通过查询资料，进一步学习云计算、大数据、数据挖掘、机器学习、人工智能等技术。

1.11　LPWA 网络有哪些特点？说出四种典型的 LPWA 物联网的技术名称，并说明哪几个采用的是授权频谱，哪几个采用的是非授权频谱。

1.12　与同学讨论自己熟知的各种高、中、低速物联网场景和技术。

1.13　与同学讨论在不同的应用场景下应该采用哪种近距离或中距离无线通信技术。

1.14　通过查询资料，进一步了解 NB-IoT 网络和 LoRa 网络在世界各地的商用情况。

1.15　详述 NB-IoT 网络的三种部署方式。

1.16　说明物联网终端有哪些组成部分和各部分的关系。

1.17　与同学讨论自己熟知的各种物联网终端识别技术的应用场景。

1.18　通过查询资料，了解密钥管理、安全路由、认证与访问控制、数据隐私保护、入侵检测与容错容侵、安全的决策与控制等物联网安全技术。