第 3 章　物联网网络技术

3.1　近距无线通信技术

全面的互联互通是物联网的特点之一。通常情况下，网络中既有智能设备又有非智能设备，非智能设备通常速率较低、通信覆盖范围较小、计算能力较差、自身能量也非常有限。低速无线网络是为适应物联网中这些智能程度较低的设备而提出的短距离、低功耗无线通信方式。

3.1.1　红外

红外是一种点对点的近距离无线通信方式。任何具有红外端口的设备间都可进行信息交互，且设备通常体积小、成本低、功耗低、不需要频率申请。由于需要将端口对接才可进行点对点数据传输，因此保密性较强。但其设备必须在可见范围内，传输距离较短，对障碍物的衍射能力较差。

红外的标准是红外数据组织 IrDA（the Infrared Data Association，红外线数据协会，简称红外数据协会）提出的 IrDA 数据协议。IrDA 数据协议由物理层、链路接入层和链路管理层三个基本协议层组成，并且 IrDA 协议栈支持 IrLAP、IrLMP、IrIAS、IrIAP、IrLPT、IrCOMM、IrOBEX 和 IrLAN 等。

红外端口是目前在世界范围内被广泛使用的一种无线连接端口，被众多的硬件和软件平台所支持，尤其在小型移动设备中应用更为普遍。如配备有红外端口的手机只需要设置好红外连接协议便可轻松实现无线上网，不需要有线媒介和智能卡支持。但由于红外技术功能单一，扩展性差，且传输过程不可控，现已逐渐退出市场，被其余的无线通信技术所取代[39]。红外模块及正在利用红外端口传送数据的手机如图 3-1 所示。

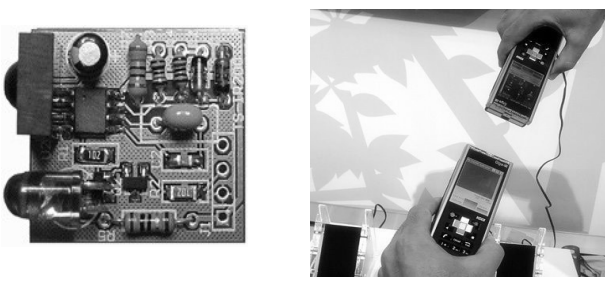

图 3-1　红外模块及正在利用红外端口传送数据的手机

3.1.2　蓝牙

1. 蓝牙技术概述

随着通信技术不断深入到人类的日常生活，人们提出了在自身附近几米范围内通信的要求，这样就出现了个人区域网络（Personal Area Network，PAN）和无线个人区域网络（Wireless Personal Area Network，WPAN）的概念。WPAN 为近距离范围内的设备建立无线连接，把几米到几十米范围内的多个设备通过无线方式连接在一起，使它们可以相互通信甚至接入 Internet 和移动通信网。蓝牙及 ZigBee 都是为满足人们在几米到几十米的活动范围内的通信要求，可用于无线个人区域网络中的技术，其中蓝牙是一种支持设备短距离、高数据速率通信的无线电技术，工作在 2.4 GHz ISM（即工业、科学、医学）频段，可在移动电话、PDA、无线耳机和笔记本电脑等众多设备之间以无线传输的方式实现信息交互。为保证在复杂的无线环境中能够安全可靠地工作，蓝牙采用跳频和快速确认技术以确保链路稳定[40]。理论上，蓝牙所采用的跳频技术可达到每秒 1600 次，有 79 个可用的信道。蓝牙标志及蓝牙耳机如图 3-2 所示。

图 3-2　蓝牙标志及蓝牙耳机

蓝牙标准将输出功率范围提高为−20～+20 dBm，为蓝牙信号在更大范围内有效传输提供了保障。但是，无线信号在传输过程中受到的影响因素较多，发射功率与覆盖范围之间的关系难以准确计算。另外，材料、墙壁和其他 2.4 GHz 源的干扰都可能改变信号所达的范围。除了增加发射功率，在工程实践中还可通过提高接收灵敏度来加大传输距离。理论上，蓝牙发射和接收设备的有效工作距离可达 300 m。

蓝牙可支持最大为 2 Mbps 的数据流量。然而由于需要考虑跳频、纠错开销、协议开销、加密和其他环境因素，用于有效净荷传输的流量无法达到最大值。其他工作于 2.4 GHz 的设备，如 IEEE 802.11b 的 WAN 也将对蓝牙设备的信号造成干扰。

蓝牙是一个开放性、低功耗、低成本、短距离的无线通信技术，其采用 FM 调制方式以抑制干扰、防止衰落并降低设备的复杂性；同时，蓝牙以时分双工（TDD）方式进行全双工通信，其基带协议是电路交换和分组交换的组合。单个跳频频率发送一个同步分组，每个分组可以占用 1～5 时隙。此外，蓝牙技术支持异步数据信

道，或三个并发的同步语音信道，同时，还支持单个信道同时传送异步数据和同步语音。每个语音信道支持 64 kbps 同步语音；异步信道可以支持非对称连接，两个节点的速率分别为 721 kbps 和 57.6 kbps，也可以支持 432.6 kbps 的对称连接。采用前向纠错（FEC）编码技术，包括 1/3 FEC、2/3 FEC 和自动重传请求（ARQ），以降低重发次数，减少远距离传输时的随机噪声影响。不过由于增加了冗余信息，造成了不必要的开销，使数据的吞吐量减小[41]。

2. 蓝牙标准分析

作为一种无线通信标准，蓝牙标准由相关特别兴趣小组（SIG）制定。SIG 于 1998 年 5 月，由 Ericsson、Intel、IBM、Nokia 和 Toshiba 等公司发起，目前，在全球范围内有超过 20 000 家成员，包括消费类电子产品制造商、芯片制造厂家与电信运营商等。

蓝牙标准体系中的协议按特别兴趣小组（SIG）的关注程度分为四层：核心协议，包括基带（Base-Band，BB）协议、链路管理协议（Link Manager Protocol，LMP）、逻辑链路控制适配协议（Logic Link Control and Adaptation Protocol，L2CAP）、服务发现协议（Service Discovery Protocol，SDP）；串口仿真协议（RFCOMM）；电话控制协议规范（Telephone Control Protocol Specification，TCS）；选用协议，包括点对点协议（Point to Point Protocol，PPP）、网际协议、传输控制协议、用户数据报协议（User Datagram Protocol，UDP）、对象交换协议（OBEX）和无线应用协议（WAP）等。此外，还定义了主机控制器接口（Host Controller Interface，HCI），为基带控制器、连接管理器、硬件状态和控制寄存器提供命令接口。蓝牙核心协议由 SIG 制定的蓝牙专用协议组成。绝大部分蓝牙设备都需要核心协议，而其他协议则根据用户需求选择性地使用。电缆代替协议和电话控制协议规范与被采用的协议在核心协议基础上构成了面向应用的协议。

3. 蓝牙网络拓扑结构

从 2011 年的蓝牙 4.2 到 2016 年的蓝牙 5，蓝牙主标准针对的都是点对点连接和点对多点连接，对应两种网络拓扑结构：微微网（Piconet）和散射网（Scatternet），如图 3-3 所示。微微网中只有一个主单元（Master），最多支持 7 个从单元（Slave）与主单元通信。主单元以不同的跳频序列来识别从单元，并与之通信。若干个微微网形成一个散射网，蓝牙设备既可以作为一个微微网中的主单元，也可以在另一个微微网中作为从单元。

多个微微网可以连接在一起组成更大规模的网络，靠跳频顺序识别每一个微微网，同一个微微网中的所有用户都与跳频顺序同步，其拓扑结构可以被描述为多微微网结构。在一个多微微网结构中，在带有 10 个全负载的独立微微网的情况下，全双工数据速率超过 6 Mbps。

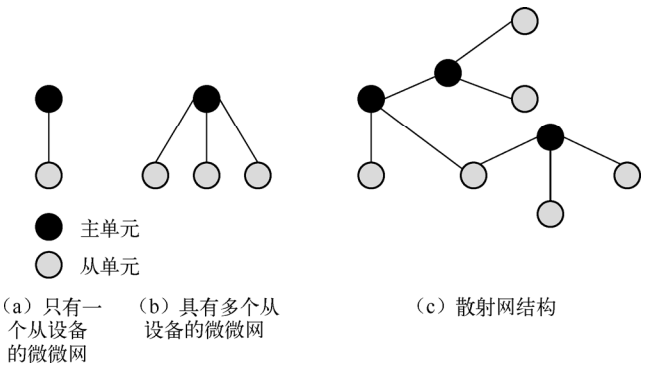

图 3-3　微微网与散射网

2017 年 7 月，蓝牙技术开始全面支持 Mesh（网状）网络，形成多点对多点的连接。图 3-4 给出了蓝牙 Mesh 网络拓扑，节点可配置多个属性，包括代理节点（Proxy）、边缘节点（Edge）、中继节点（Relay）、朋友节点（Friend）和低功耗节点（Low Power）。与上述的星状网络不同，蓝牙 Mesh 网络中不存在主节点，每个节点可以跨越一定数量的中间节点以多跳的方式到达网络中的其他节点。在蓝牙 Mesh 网络中，没有静态或动态路由，而是采用可管理的洪泛机制进行消息传输，每个节点都采用广播方式转发收到的数据。多点对多点的 Mesh 技术让蓝牙在组网能力上有了巨大的提升，且具有较高的稳健性、安全性和兼容性。

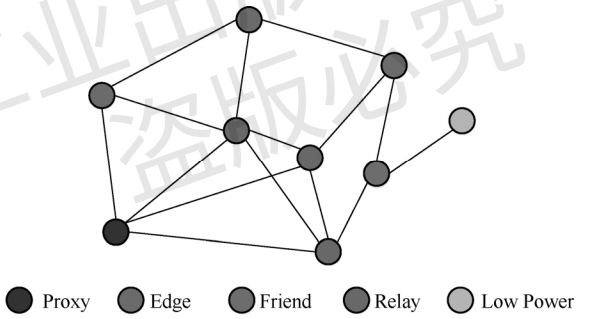

图 3-4　蓝牙 Mesh 网络拓扑

4. 蓝牙技术特点及应用

蓝牙技术设计之初是为取代现有的掌上电脑、移动电话等各种数字设备上的有线电缆连接，为用户提供低成本、近距离的无线通信，使得近距离内各种设备能够实现无缝资源共享。因此，蓝牙技术拥有如下几个特点。

- 全球范围适用；
- 可同时传输语音和数据信息；
- 可建立临时性的对等连接；
- 具较好的抗干扰能力；
- 体积小，便于集成；
- 功耗低；

- 开放的接口标准；
- 成本低。

2016 年 12 月初 SIG 推出了新的蓝牙核心规范版本——蓝牙 5，为物联网设备的低功耗连接提供了一个可行、高效的解决方案。蓝牙 5 除了具有蓝牙技术的特性，如无线频段选择、媒体介入控制和纠错等特性，还加入了以下全新的特性：4 倍的传输距离、2 倍的传输速度和 8 倍的广播数据传输量的提升，更好的兼容性和更高的室内定位精度[42]。蓝牙 5 新特性使数据传输多样化，优化用户获取信息的体验。更长的传输距离可以满足更广的覆盖范围；更快的传输速度可以提高设备的响应能力和性能；广播数据量的提升极大地提升了设备的数据发送量，满足更多的应用要求。蓝牙 5 的这些新特性使其可以在日新月异的智能家居、楼宇、医疗、信标、定位和其他物联网场景中的应用更为广泛。

2019 年 1 月，SIG 公布了蓝牙 5.1 标准。蓝牙 5.1 在蓝牙 5.0 的基础上引入了寻向功能，让蓝牙成为继 GPS 和 WiFi 之外另外一种使用定位服务的方式。寻向功能主要采用了两种定位技术，一种是到达角（Angle of Arrival，AoA）测量技术；另一种是出发角（Angle of Departure，AoD）测量技术。该测向功能不但可以在蓝牙 5.1 上检测到特定对象的距离，还能找到设备信号发射的方向，从而实现追踪物品和引导的功能，其精度达到了厘米级，能够应用于室内导航、物品追踪、房屋门禁等场景。此外，规范还增加了一些其他功能，例如，对通用属性配置文件（Generic ATTribufe ProFile，GATT）缓存的改进，可以在服务器和客户端之间实现更快、更节能的连接。

2020 年年初发布的蓝牙 5.2 标准主要增加了 LE 同步信道、增强 ATT 和 LE 功率控制三个功能。LE 同步信道是支撑下一代蓝牙音频的核心技术，LE 同步信道为实现下一代蓝牙音频的多声道音频流和基于广播音频流的共享音频应用打下了基础。蓝牙 5.2 版本还对 ATT 协议进行了完善，用于快速读取属性值，这一新增功能将提高基于 ATT 协议的信息交互效率，实现快速服务发现等功能。同时，蓝牙 5.2 版本定义了低功耗蓝牙的双向功率控制协议，有助于在保持连接的情况下进一步降低功耗并提高设备连接的稳定性和可靠性，可用于实现多种应用场景。

3.1.3　ZigBee

1. ZigBee 技术概述

与蓝牙标准类似，ZigBee 技术也是针对 WPAN 网络而产生的一种面向自动控制的低速率、低功耗、低成本短距离无线通信技术。该技术标准由 IEEE 802.15.4 小组与 ZigBee 联盟专为低速率传感器和网络控制设计。ZigBee 联盟是一个全球性的企业联盟，由 Honeywell、Mitsubishi、Motorola、Philips 和 Invensys 共同成立，旨在合作实现基于全球开放标准的、可靠、低成本、低功耗的无线联网产品。

ZigBee 的名称来源于蜜蜂的八字舞，蜜蜂之间通过跳 Zigzag 形状的舞蹈互相

交流，与同伴传递花粉所在方位和距离等信息。同其他无线协议相比，ZigBee 提供了低复杂性、低功耗的通信方式。ZigBee 技术能融入各类电子产品，应用范围横跨全球民用、商用、公用及工业等领域。随着 ZigBee 技术的不断完善，它将成为当今世界最前沿的数字无线技术，它的广泛应用必将为人们的日常生活带来极大的方便与快捷。ZigBee 模块与 ZigBee 网络如图 3-5 所示。

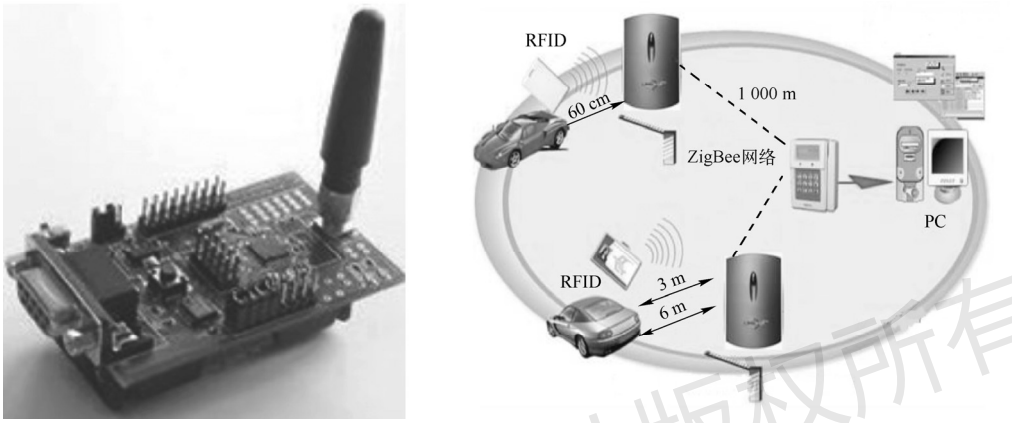

图 3-5　ZigBee 模块与 ZigBee 网络

2. ZigBee 协议栈

ZigBee 协议栈是在 OSI 七层模型的基础上根据市场和实际需要定义的，自下而上包括物理层、媒体访问控制（MAC）层、网络层（NWK）和应用层（APL）。其中，物理层和 MAC 层由 IEEE 802.15.4 制定，网络层和应用层由 ZigBee 联盟制定[43]。ZigBee 协议栈如图 3-6 所示。

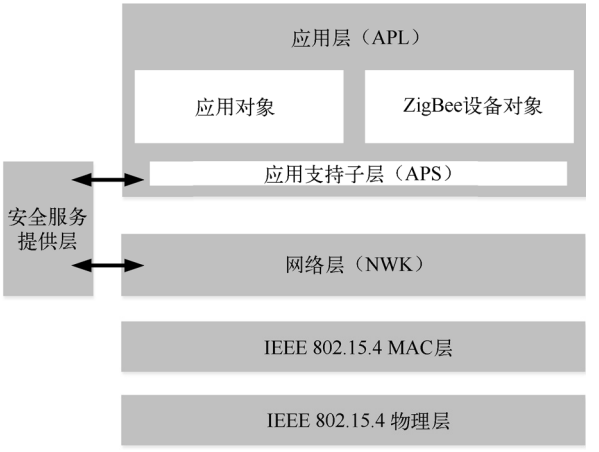

图 3-6　ZigBee 协议栈

（1）物理层

IEEE 802.15.4 物理层负责无线发射机的激活或非激活状态管理，节点采用

CSMA/CA 方式进行空闲信道评估、信道频率选择、数据的发送和接收，同时，节点还可以在当前信道内进行能量检测，衡量当前节点之间的链路质量。IEEE 802.15.4 定义了两个物理层标准，分别是 2.4 GHz 物理层和 868/915 MHz 物理层。两者均基于直接序列扩频（Direct Sequence Spread Spectrum，DSSS）技术。868 MHz 支持一个信道，传输速率为 20 kbps；915 MHz 支持 10 个信道，传输速率为 40 kbps，两个频段均采用 BPSK 调制。2.4 GHz 支持 16 个信道，能够提供 250 kbps 的传输速率，采用 O-QPSK 调制。

信道能量检测为网络层提供信道选择依据，它主要测量目标信道中接收信号的功率强度，由于检测过程本身不进行解码操作，所以得到的结果是有效信号功率和噪声信号功率之和。

当网络层或应用层接收数据帧时，链路质量参数能够为节点提供无线信号的强度和质量相关信息，与信道能量检测不同，链路质量评估过程需要对信号进行解码，生成信噪比相关指标数值，进而，与物理层数据单元一起提交给上层进行进一步处理。

空闲信道评估：IEEE 802.15.4 定义了三种空闲信道评估模式。第一种模式，简单判断信道的信号能量，当信号能量低于某一个门限值时就认为信道空闲；第二种模式，通过无线信号的特征判断信道空闲，该特征主要包括两个方面，即扩频信号特征和载波频率；第三种模式是前两种模式的综合，同时检测信号强度和信号特征，给出信道空闲判断。

（2）MAC 层

IEEE 802.15.4 标准中所定义的 MAC 层主要对无线物理信道的接入过程进行管理，并产生和识别节点网络地址以及帧校验序列。具体功能包括：网络协调器（Coordinator）产生网络信标、网络中设备与网络信标同步、完成 PAN 的入网和脱离网络的过程、网络安全控制、利用 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）机制进行信道接入控制、处理和维持保护时隙（Guaranteed Time Slot，GTS）机制、在两个对等的 MAC 实体间提供可靠的链路连接。

IEEE 802.15.4 LR-WPAN 标准允许使用超帧结构，每个超帧都以网络协调器在规定的时间间隔内发出信标帧为开始，在该信标帧中包含了超帧将持续的时间以及对这段时间的分配等信息。网络中的普通设备接收到超帧开始时的信标帧后，就可以根据其中的内容安排自己的任务，例如，进入休眠状态直到这个超帧结束。

超帧将通信时间划分为活动期和睡眠期（不活跃时段）。在睡眠期，协调器不会同网络中的其他节点发生信息交换，进入低功耗模式以节省能量。超帧的活动期又划分为三个时段：信标发送时段、竞争访问时段（Contention Access Period，CAP）和非竞争访问时段（Contention Free Period，CFP）。超帧活动期被划分为 16 个等长的时隙，每时隙的长度、竞争访问时段包含的时隙数等参数都由协调器设定，并通过超帧开始时发出的信标帧广播到整个网络。图 3-7 所示为超帧结构。

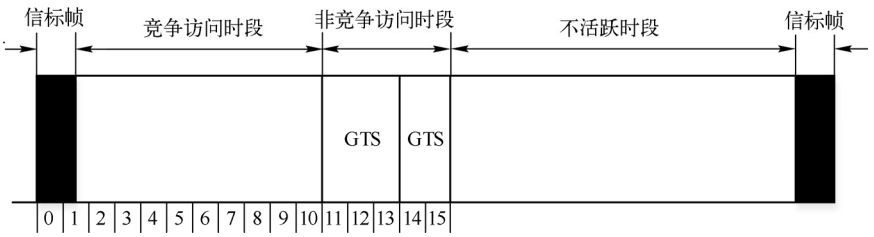

图 3-7　超帧结构

在超帧的竞争访问时段，IEEE 802.15.4 网络设备使用 CSMA/CA 访问机制，并且任何通信都必须在竞争访问时段结束前完成。竞争访问时段结束后是非竞争访问时段，它由保护时隙构成，一般情况下，保护时隙的数量最多为 7 个。在超帧结构中，必须保证有足够长的非竞争访问时段，以向网络中的设备提供竞争接入的机会。任何设备的信息传输必须在下一个保护时隙开始前或者非竞争访问时段结束前完成。

媒体访问控制（MAC）层的帧被称为 MAC 层协议数据单元（MPDU），由 MAC 头（MAC Header，MHR）、MAC 净荷（MSDU）和 MAC 尾（MAC Footer，MFR）三部分组成。MAC 帧结构如图 3-8 所示。

<table>
<tr><td>字节：2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>可变</td><td>2</td></tr>
<tr><td rowspan="2">帧控制域</td><td rowspan="2">帧序列号域</td><td>目的 PANID</td><td>目的地址</td><td>源 PANID</td><td>源地址</td><td rowspan="2">帧净荷</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">地址域</td></tr>
<tr><td colspan="6">MHR</td><td>MSDU</td><td>MFR</td></tr>
</table>

图 3-8　MAC 帧结构

其中，MAC 头由帧控制域、帧序列号域和地址域组成；MAC 净荷（MSDU）为 MAC 帧携带的数据净荷；MAC 尾（MFR）包含相应 MAC 帧的 FCS 校验信息，保证数据的可靠传输。

MAC 帧有四种不同的帧形式，即信标帧、数据帧、确认帧和 MAC 命令帧。

① 信标帧。

信标帧的 MSDU 由四个部分组成：超帧描述字段、GTS 分配字段、待转发数据目标地址字段和信标净荷数据。其中，超帧描述字段规定了该超帧的持续时间、活跃时段持续时间以及竞争访问时段持续时间等信息。GTS 分配字段将非竞争时段分为若干个 GTS，并把每个 GTS 具体分配给某个设备。待转发数据目的地址字段列出了与协调器保存的数据相对应的设备地址。信标帧净荷数据为上层协议提供数据传输接口。

② 数据帧。

在 ZigBee 设备之间进行数据传输时，要传输的数据由应用层生成，经过逐层处理后发送给 MAC 层，形成了 MAC 层服务数据单元（MSDU），再加上 MHR 信

息和 MFR 信息后，就构成了 MAC 帧。

③ 确认帧。

为保证设备之间通信的可靠性，发送设备通常要求接收设备在接收到正确的帧信息后返回一个确认帧，向发送设备表示已经正确地接收了相应的信息。帧确认机制是一种可选机制，发送设备可以要求发送确认信息，也可以不要求发送确认信息。设备只对数据帧和 MAC 命令帧使用帧确认机制，在任何情况下都不会给信标帧或确认帧回应确认信息。设备设有超时重传机制，在一定时间内没有收到确认帧，会择机重新发送该帧。对于不要求确认的数据帧，发送以后就认为该数据帧发送成功，并从本地缓冲队列中删除该数据帧。

④ MAC 命令帧。

MAC 命令帧主要用于完成三个功能：关联设备到 PAN 网络、与协调器交换数据和分配 GTS。命令帧在帧格式上与其他类型的帧没有太多的区别，只是帧控制字段的帧类型位有所不同。命令帧的具体功能由帧的负载数据表示。负载数据是一个变长结构，所有命令帧负载的第一字节是命令类型字节，后面的数据针对不同的命令类型有不同的含义。

（3）网络层

ZigBee 的网络层负责完成网络层级的通信，包括网络拓扑结构管理、节点间的路由选择以及消息安全性控制。ZigBee 网络是一种动态网络，因而网络层需要不断维护网络中的节点信息。在实际应用中，网络层协议的配置需指定网络的性能及参数。例如，网络拓扑类型、节点数量以及数据安全性等。具体来说，ZigBee 网络层的主要功能就是通过相关的功能实体确保 ZigBee 的 MAC 层（IEEE 802.15.4）正常工作，并且为应用层提供合适的服务接口。为了向应用层提供接口，网络层提供了两个必需的功能服务实体，它们分别为数据实体和管理实体[44]。网络层数据实体（NLDE）通过网络层数据实体服务接入点（NLDE-SAP）提供数据传输服务，网络层管理实体（NLME）通过网络层管理实体服务接入点（NLME-SAP）提供网络管理服务，并且，网络层管理实体还需要完成对网络信息库（NIB）的维护和管理[45]。MAC 层实体通过 MAC 公共部分服务接入点（MCPS-SAP）提供数据服务，通过 MAC 层管理实体服务接入点（MLME-SAP）提供管理服务。网络层参考模型如图 3-9 所示。

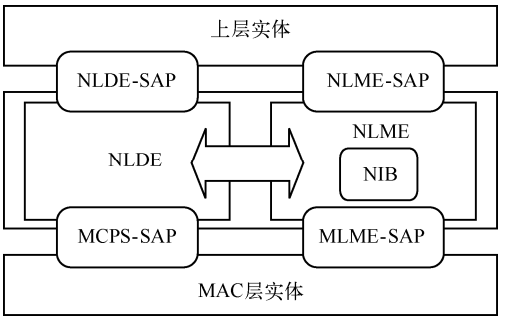

图 3-9　网络层参考模型

每个网络层帧由网络层（NWK）帧头和网络层（NWK）净载荷组成；其中，NWK 帧头由帧控制域、地址域（包括目的地址、源地址和广播半径）和序列号组成；NWK 净载荷长度可变，其中包含了指定帧类型的信息。

NWK 帧格式如图 3-10 所示。

图 3-10　NWK 帧格式

1）帧控制域

NWK 帧控制域长度为 16 bit，其格式如图 3-11 所示，各子域说明如下。

图 3-11　NWK 帧控制域格式

① 帧类型子域如表 3-1 所示，其长度为 2 bit，且设置为非保留值。

表 3-1　帧类型子域

帧类型值	帧类型名称
00	数据帧
01	NWK 命令帧
10～11	保留

② 协议版本子域的长度为 4 bit，反映了当前使用的 ZigBee 网络层协议版本号，该版本号为网络层参数 nwkcProtocolVersion，如果使用 ZigBeeSpecification Version 1.0，则该值为 0x01。

③ 发现路由子域如表 3-2 所示，其长度为 2 bit，该子域用于控制路由发现。

表 3-2　发现路由子域

发现路由子域的值	域的含义
0x00	禁止路由发现
0x01	使能路由发现
0x10	强制路由发现
0x11	保留

④ 广播标记子域的长度为 1 bit，为 0 表示单播或者广播，为 1 表示组播。

⑤ 安全子域的长度为 1 bit，只在该子域的值为 1 时，实现网络层安全操作。如果该帧的安全在另一层执行，或不使能，该子域值为 0。

2）地址域

① 目的地址域的长度为 2 字节，并且持有 16 bit 网络地址或者广播地址（OxFFFF），设备的网络地址应该与它的 IEEE 802.15.4—2003 MAC 短地址相同。

② 源地址域的长度为 2 字节，是这帧的源设备的网络地址。

③ 广播半径的长度为 1 字节，它规定了一个传输范围（又称半径）。网络层帧中的半径只有在目的地址为广播地址时才存在，该半径限定了广播范围。

3）序列号

序列号的长度为 1 字节，每传输一个新的帧，该值加 l，源地址和序列号唯一确定一帧数据。

NWK 层包含两种帧类型：一种是数据帧；另一种是命令帧，包括路由请求命令、路由响应命令、路由错误命令和离开命令四种。数据帧的 NWK 净载荷部分是数据载荷，命令帧的净载荷部分包括 NWK 命令标识符和命令净载荷。NWK 命令帧格式如图 3-12 所示。

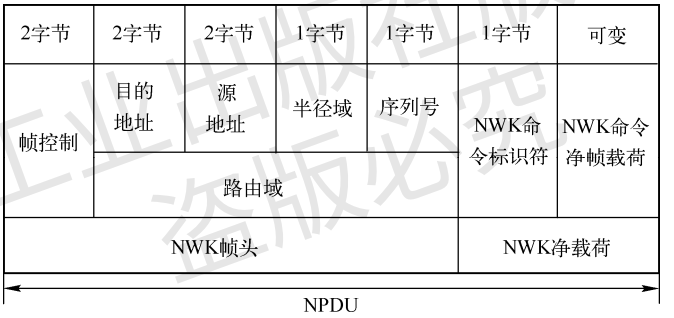

图 3-12　NWK 命令帧格式

（4）应用层

ZigBee 的应用层主要根据应用由用户自主开发，维持器件的功能属性，根据服务和需求使多个节点间能够进行通信。应用层由应用支持子层（APS）、设备对象（ZDO）及应用框架三部分组成。APS 的作用包括维护绑定列表（绑定列表的作用是将基于两个设备的服务和需要绑定在一起），并在绑定的设备间传输信息，同时，定义、删除并过滤组地址信息，完成 64 位 IEEE 地址到 16 位 NWK 地址的地址映射。ZDO 的作用是在网络中定义一个设备（如协调器、路由器、终端设备），发现网络中的设备并确定它们能提供何种应用的服务：起始或回应绑定需求，在网络设备中建立一个安全连接。ZigBee 应用层除了提供一些必要的函数以及为网络层提供合适的服务接口，一个重要的功能就是应用者可以通过 APS 灵活地定义自己的应用对象，APS 帧格式如图 3-13 所示。

<table>
<tr><td>1字节</td><td>0/1字节</td><td>0/2字节</td><td>0/2字节</td><td>0/2字节</td><td>0/1字节</td><td>1字节</td><td>可变</td></tr>
<tr><td rowspan="2">帧控制</td><td>目的端点</td><td>组ID</td><td>群集ID</td><td>配置ID</td><td>源端点</td><td rowspan="2">APS
帧计数器</td><td rowspan="2">帧负载</td></tr>
<tr><td colspan="5">地址信息</td></tr>
<tr><td colspan="6">APS帧头</td><td colspan="2">APS负载</td></tr>
</table>

图 3-13　APS 帧格式

3. ZigBee 路由协议

ZigBee 路由协议的设计是组网的关键，为满足 ZigBee 组网要求，其路由协议应满足如下条件：

- 对拓扑的变化具有快速反应能力，并且避免路由环路的产生；
- 高效利用带宽资源，尽可能压缩开销；
- 尽可能缩减传递的数据量，节约能源。

为达到上述目标，ZigBee 网络采用 Cluster-Tree 与 AODV（Ad Hoc On-Demand Distance Vector Routing，Ad Hoc 按需距离矢量路由）相结合的路由协议，其中 Cluster-Tree 协议包括地址的分配与寻址路由两部分，包括子节点的 16 位网络短地址的分配，以及根据分组目的节点的网络地址来计算分组的下一跳的协议。AODV 是一种按需路由协议，利用扩展环搜索的方法来限制搜索发现过程的范围，该协议支持组播，同时，可以在 ZigBee 节点间实现动态、主动路由，使节点以较快的速度获得到达目的节点的路由[46]。但 ZigBee 中所使用的 AODV 协议与自组织网络（Ad Hoc）中的 AODV 协议并不完全相同，准确地说，ZigBee 网络针对自身特点使用了一种简化版的 AODV，即 AODVjr（AODV Junior）。在 ZigBee 网络中，节点可以按照父子关系（当网络中的节点允许一个新节点通过它加入网络时，它们之间就形成了父子关系）使用 Cluster-Tree 算法选择路径，即当一个节点接收到分组后发现该分组不是给自己的，则只能转发给它的父节点或子节点。显然这并不一定是最优的路径，为了提高路由效率，ZigBee 网络中也让具有路由功能的节点使用 AODVjr 协议发现路由，即具有路由功能的节点可以不按照父子关系而直接发送信息到其通信范围内的其他具有路由功能的节点，而不具有路由功能的节点仍然使用 Cluster-Tree 路由发送数据分组和控制分组。

（1）Cluster-Tree 协议

Cluster-Tree 是一种由网络协调器展开生成树状网络的拓扑结构，适合于节点静止或者移动较少的场合，属于静态路由，不需要存储路由表。树簇中的大部分设备为全功能设备（Full Function Device，FFD），精简功能设备（Reduced Function Device，RFD）只能作为树枝末尾的叶节点，其主要原因在于 RFD 一次只能连接一个 FFD。在建立一个 PAN 时，首先 PAN 主协调器将自身设置成簇标识符（CID）为 0 的簇头（CLH），然后选择没有使用的 PAN 标识符，向邻近的其他设备以广播方式发送信标帧，从而形成第一簇网络。接收到信标帧的候选设备可以向簇头申请加入该网络，主协调器根据

请求信息做出是否允许其加入网络的判断。若允许，将该设备作为子节点加入自己的邻居列表，同时子设备也将其父节点加入邻居列表。当网络达到规模上限时，PAN 主协调器将会指定一个子设备为另一簇新网络的簇头，成为 PAN 主协调器，随后其他设备逐个加入形成一个多簇网络。簇树网络结构如图 3-14 所示。

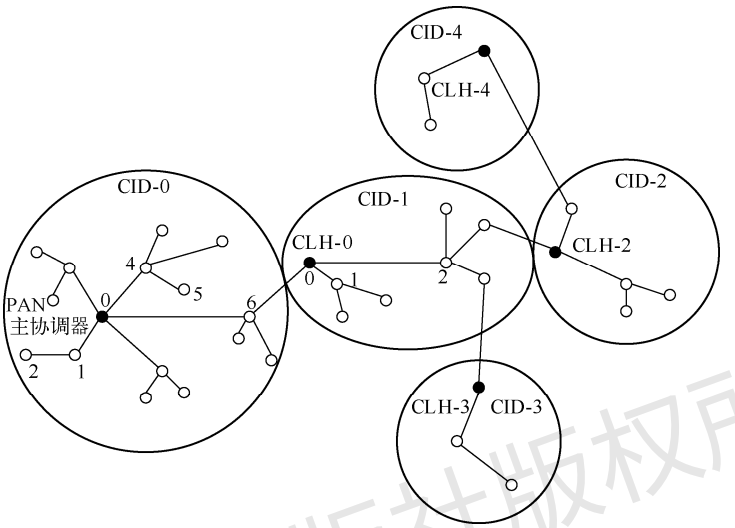

图 3-14　簇树网络结构

分簇协议是动态加表簇树算法的一种变形，用于构成多簇网络，典型的分簇路由协议有 LEACH 协议（Low Energy Adaptive Clustering Hierarchy，低能耗自适应聚类层次协议，又称低功耗自适应集簇分层型协议）、TEEN 协议（Threshold sensitive Energy Efficient sensor Network protocol，阈值敏感节能传感器网络协议，又称门限敏感的高效能传感器网络协议）、PEGASIS 协议（Power Efficient GAthering in Sensor Information System，传感器信息系统中的节能采集协议）、EEUC 协议（Energy-Efficient Uneven Clustering，节能型非均匀分簇协议，又称节能不均匀聚类协议）[47]。

其中 LEACH 协议强调数据融合的功能，采用簇式的集群型结构，具有本地数据处理和压缩、动态分配簇首等功能，可用于对于数据具有高度相关性的应用场景。由于采用了数据融合技术，节点能够消除大部分冗余数据，因此在能耗方面性能较好。但其没有考虑网络中节点的剩余能量，且簇首分布不均匀，易产生簇首数量不稳定等问题。

在 LEACH 协议的基础上，TEEN 协议进行了改进。该协议定义了两个门限：硬门限与软门限。硬门限是根据用户对感兴趣的数据范围设定的，达到极大地降低冗余数据传输的目的。如果获知的数据波动情况较小，则节点就不需要向簇首报告。感应数据所耗能量比传输数据所耗能量要少得多，虽然节点一直处于感应状态，但是由于减少了很多不必要的数据传输，因此较为节能。

PEGASIS 协议是在 LEACH 协议基础上发展而来的基于“链”的路由协议。该协议的核心思想是利用贪婪算法在无线传感器网络中形成一个包含所有节点的“链”，节点从邻居节点接收数据，融合后发送给相应的邻居节点，直至到达“簇头”节点，进而将数据发给目的节点。该协议比 LEACH 协议更节能，但维护节点

位置信息（相当于传统网络中的拓扑信息）需要额外的资源。

EEUC 协议是一种基于非均匀分簇的无线传感器网络多跳路由协议，候选簇首通过使用非均匀的竞争范围来构造大小不等的簇。EEUC 协议通过减小靠近基站的簇规模来达到减少簇内成员节点数量的目的，使簇首能够节省在簇内相关处理中消耗的能量，用于簇首间的数据转发，从而解决网络“热区”问题。

（2）AODVjr 协议

AODVjr 协议是对 AODV 协议的改进，具有 AODV 协议的主要功能，考虑到节能、应用方便性等因素，简化了 AODV 协议的一些特点。

① AODVjr 协议中并没有使用目的节点序列号，以减少控制开销和简化路由发现的过程。AODV 协议中使用目的节点序列号确保所有路径在任何时间无环路，而在 AODVjr 协议中为了保证路由无环路，规定只有分组的目的节点能够回复 RREP（路由应答消息），即使中间节点有通往目的节点的路由也不能回复 RREP。

② AODVjr 协议不存在 AODV 协议中的先驱列表（Precursor List），从而简化了路由表结构。在 AODV 协议中，如果节点探测到下一跳链路中断，则通过上游节点转发 RERR，通知所有受到影响的源节点。在 AODVjr 协议中，RERR 仅转发给传输失败的数据分组的源节点，因而不需要先驱列表。

③ AODVjr 协议采用本地修复解决在数据传输中的链路中断问题，由于没有使用目的节点序列号，在路由修复的过程中仅允许目的节点回复 RREP。若本地修复失败，则发送 RERR 至数据分组源节点，通知它由于链路中断而引起目的节点不可达。RERR 的格式也被简化至仅包含一个不可达的目的节点，而 AODV 协议的 RERR 中包含多个不可达的目的节点。

④ 在 AODV 协议中节点周期性地发送 Hello 分组（又称 Hello 数据包），为其他节点提供连通性信息；而 AODVjr 协议中节点不发送 Hello 分组，仅根据收到的分组或者 MAC 层提供的信息更新邻居节点列表。

（3）ZigBee 路由

在 ZigBee 路由中，可以将节点分为两类：RN+和 RN−。其中 RN+是指具有足够的存储空间和能力执行 AODVjr 协议的节点，RN−是指由于存储空间受限，不具有执行 AODVjr 协议能力的节点，RN−收到一个分组后只能用 Cluster-Tree 协议处理。

在 Cluster-Tree 协议中，节点收到分组后可以立即将分组传输给下一跳节点，不存在路由发现过程，这样节点就不需要维护路由表，从而减少了路由协议的控制开销和节点能量消耗，并且降低了对节点存储能力的要求；但由于采用 Cluster-Tree 协议建立的路由不一定是最优的路由，会造成分组传输时延较大，而且较小深度的节点（即靠近 ZigBee 协调点的节点）往往业务量较大，较大深度的节点业务量又比较小，容易造成网络中通信流量分配不均衡。因而，ZigBee 中允许 RN+节点使用 AODVjr 协议去发现一条优化路径，RN+节点收到分组后，执行 AODvjr 协议中的路由发现过程，找到一条通往目的节点的最优路径。ZigBee 中的路由度量指标需要考虑 IEEE 802.15.4 物理层提供的 LQI（Link Quality Indicator，链路质量指示）值，

LQI 值越大表示链路质量越好。在选择路由时考虑 LQI 指标的方法有很多，综合考虑路由的各项性能指标，我们可以按照以下规则选择路径：选择一条通往目的节点的最短路径，当存在两条相同跳数的最短路径时，节点选择 LQI 值较大的那条路径。路由建立过程结束后，节点沿着刚刚建立的路由发送分组。如果某条链路发生中断，RN+节点将发起本地修复过程修复路由。由于 AODVjr 协议的使用，降低了分组传输时延，提高了分组投递率[48]。

4. ZigBee 组网方式

（1）两种功能类型设备

ZigBee 定义了两种功能类型设备：全功能设备（FFD）和精简功能设备（RFD）。FFD 实现完整的协议功能，支持任何拓扑结构，可充当协调器（Coordinator）、路由器（Router）和普通节点（Device）。RFD 是为实现最简单的协议功能而设计的，只能作为普通节点存在于网络中。FFD 可以与 RFD 或其他的 FFD 通信，而 RFD 只能与 FFD 通信，RFD 之间不能直接通信。

（2）三种类型节点

ZigBee 网络包含三种类型的节点，即协调器（Coordinator）、路由器（Route）和终端设备（End Device），其中协调器和路由器均为全功能设备（FFD），而终端设备为精简功能设备（RFD）。一个 Zigbee 网络由一台协调器、若干台路由器和一些终端设备组成。

① 协调器：该设备负责启动网络，配置网络成员地址，维护网络，维护节点的绑定关系表等。一旦启动和配置网络的任务完成，协调器就以路由器节点的角色运行。

② 路由器：主要实现网络扩展及路由消息功能。网络扩展是指路由器作为网络中的潜在父节点，允许更多的设备加入网络。路由器只有在树状网络和网状网络中存在。路由器必须不断准备转发数据，通常采用干线供电，而非电池供电。

③ 终端设备：不具备成为父节点或路由器的能力，没有维持网络的基础结构的特定责任，一般作为网络的边缘设备，负责与实际的监控对象相连。这种设备只与自己的父节点主动通信，具体的信息路由任务则全部交由其父节点及网络中具有路由功能的协调器和路由器完成。

（3）三种网络拓扑

ZigBee 网络支持三种网络拓扑结构：星状拓扑、树状拓扑和网状拓扑[49]。如图 3-15 所示。

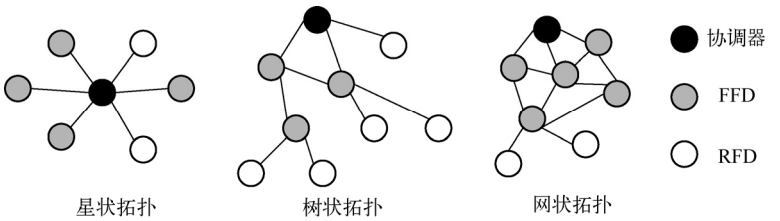

图 3-15　ZigBee 网络拓扑结构

星状拓扑由一台协调器和一系列的 FFD/RFD 构成，其他节点分布在协调器的通信范围内，节点之间的数据传输都要通过协调器转发。通常情况下，星状网的控制和同步都比较简单，适合应用于节点数量较少的场合。

树状拓扑由一台协调器和一个或多个星状拓扑组合而成。节点可以与自己的父节点或子节点进行点对点的直接通信，也可采用 Cluster-Tree 路由进行数据和控制消息的传输，即当一个节点向另一个节点发送数据时，信息将沿着树的路径向上传递到最近的协调器然后再向下传递到目标节点。树状网的优点是可以加大网络覆盖范围，但随之产生的消息传输时延也会增加。

网状拓扑由若干台 FFD 连接在一起组成骨干网，节点之间可完全对等通信。网状网中除了允许父节点和子节点之间通信，也允许通信范围之内具有路由能力的非父子关系的邻居节点之间进行通信。网状网是在树状网基础上实现的，其路由可自动建立和维护。网状拓扑为传输的数据提供了多条路径，一旦一条路径出现故障，可快速切换至另一条路径，并且网络还可以通过多跳的方式进行通信，因此，网状网是一种高可靠性、高冗余的网络。网状拓扑结构减少了消息的传输时延，增强了可靠性，但其缺点是存储空间的开销较大[50]。

3.1.4　6LowPAN

1. 6LowPAN 概述

随着网络的迅速发展和用户规模的不断扩大，现有 IPv4 的网络协议由于其地址空间缺乏等因素，不能满足实际的网络需求，于是新的网络协议 IPv6 应运而生[51]。IPv6 拥有几乎取之不尽的地址空间和突出的通信性能，这为物联网的发展创造了良好的网络通信条件和可拓展性。IPv6 还具有很多适合物联网大规模应用的特性，例如，IPv6 简洁的报头和良好的可扩展性、突出的安全性、自动地址配置和移动性等特性，这些都促使 IPv6 成为物联网应用的基础网络技术。

尽管新的 IPv6 通信协议能解决 IPv4 在地址资源数量上的限制，但在窄带宽、低功耗的嵌入式网络中直接采用完整的协议栈也会带来一系列的问题。为了扫除 IPv6 技术在物联网中的障碍，互联网工程任务组（IETF）提出了针对嵌入式网络设计的 6LoWPAN（IPv6 over Low Power Wireless Personal Area Network）协议，它融合了互联网协议 IPv6 与无线个域网标准 IEEE 802.15.4，从而使得物联网和 IP 网络得以衔接。IETF 对 6LoWPAN 有如下定义：“6LoWPAN 是一种通过适配层技术使得基于 IEEE 802.15.4 标准的低功耗有损网络节点能够采用 IPv6 技术进行通信和交互的技术。”IETF 已经完成了 6LowPAN 的核心标准规范，包括 IPv6 数据报文和帧头压缩规范，面向低功耗、低速率、链路动态变化的无线网络路由协议[52]。

2. 6LowPAN 协议栈

6LowPAN 与 ZigBee 和蓝牙等无线技术类似，在数据通信上也符合标准的 OSI 模型。图 3-16 给出了典型的 6LowPAN 协议栈，同 ZigBee 技术一样，6LowPAN 技术采用 IEEE 802.15.4 规定的物理层和 MAC 层，用于支持低功耗、低速率、窄带宽消耗通信。不同之处在于 6LowPAN 技术在网络层只支持 IFTF 规定的 IPv6。为了提供对 IPv6 的必要支持，需要在网络层和 MAC 层之间加入一个适配层（LowPAN），对上层信息进行有效处理，再发送到下层。在传输层，6LowPAN 最常用的传输协议为用户数据报协议（UDP），并用互联网控制消息协议版本 6（ICMPv6）进行消息控制[53]。因为 TCP 的效率较低，复杂度较高，在 6LowPAN 中的性能较差，所以它不常被 6LowPAN 使用。

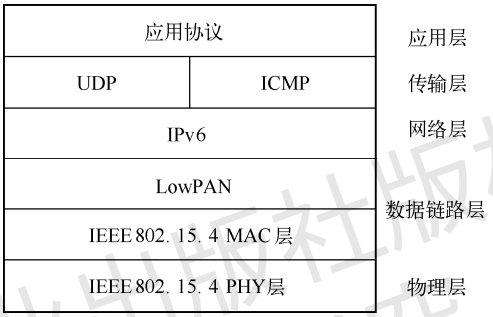

图 3-16　典型的 6LowPAN 协议栈

3. 6LowPAN 适配层技术

在 6LowPAN 中，网络层采用的 IPv6 和 MAC 层的 IEEE 802.15.4 MAC 协议由于设计特性上的不同，导致了 IPv6 无法像以太网那样直接构架到 MAC 层上。6LowPAN 在网络层和 MAC 层之间增加适配层以屏蔽各自的差异性，从而实现了二者的互通。

适配层在 6LowPAN 的协议栈中起承上启下作用，它主要提供数据的压缩、分段和重组功能[54]。

（1）头部压缩

6LowPAN 的底层协议的最大传输单元为 127 字节，除去自身所需要的控制部分和安全头部，还需要承载上层头部，其中，仅 IPv6 就占用了 40 字节，如果 IPv6 的负载里还有上层协议数据，如 UDP，其报头也会占用一定的空间，这使得剩余数据负载非常有限。虽然通过分段和重组可通过下层协议传输较大的数据报，但这会降低传输效率并增加电池的耗电量，因此需要对数据报进行压缩。IEEE 802.15.4 和 IPv6 的数据格式如图 3-17 所示，该图给出了两种协议规范的数据格式对比。

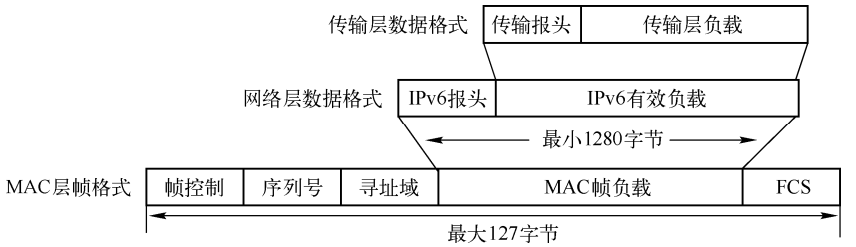

图 3-17　IEEE 802.15.4 和 IPv6 的数据格式

6LowPAN 适配层主要是通过压缩编码对 IPv6、ICMPv6 和 UDP 的头部字段进行压缩的。核心思想是通过下层信息导出上层字段，以消除消息的冗余。借鉴传统 IP 压缩技术，可以总结 6LowPAN 报头压缩技术的基本原则如下：

- 在链路连接过程中报头中保持不变的域可以压缩；
- 报头中可以提前预知的信息域可以压缩；
- 可从链路层推断得出的域可以压缩；
- 报头中的可选域视情况压缩。

目前，6LoWPAN 工作组已经提出了 LoWPAN_HC1 和 LoWPAN_HC2（在 RFC 4944 中提出）、LoWPAN_IPHC 和 LoWPAN_NHC（在 RFC 6282 中提出）、LoWPAN_GHC 在（RFC 7400 中提出）等相对成熟的报头以及下一个报头的压缩方案[55]。6LoWPAN 在 MAC 报头之后定义了一个分配报头，用于表示决定压缩报头的具体格式和算法。

当分配报头为“01000010”时，表示采用 HC1 算法对 IPv6 数据报的头部信息进行压缩。HC1 压缩技术采用无状态的报头压缩方案，其主要思想是对本地链路地址进行高度压缩优化，HC1 的压缩字段如图 3-18 所示。使用 HCl 压缩可以对 IPv6 头部进行相当大的裁剪，对端口地址、流标签和类型等共同信息进行压缩，只留下一些需要被顺序携带的信息，如 6LowPAN 字节、HC1 字节和跳数限制字段，在理想情况下，可将 40 字节的 IPv6 报头压缩至 3 字节。HC1 报头压缩方案对于链路本地单播通信是十分有效的[56]。但是，由于链路本地地址通常适用于局部协议交互，一般不用于应用层数据流，因此 HC1 的实际应用价值非常有限。

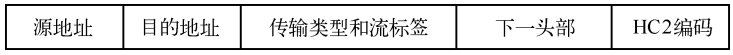

图 3-18　HC1 的压缩字段

HC2 压缩方案是用来压缩 UDP 头部的一种方法。一般情况下，HC2 在 HC1 字节后面提供 UDP 头部压缩方案的信息，允许把 UDP 头压缩到不同的程度[57]。使用 HC1 的同时也可以选择使用 HC2。UDP 的报文格式较为简单，包含源端口、目的端口、长度和校验和四个字段。其中，端口号可通过偏移量代替进行压缩；长度字段包含报头和数据负载，固定的报头长度也是可压缩的；校验和用于判断报文在网络内传输过程中是否被更改或遭到破坏，其校验值是变化的，不能被压缩。在 6LowPAN 中，HC2 压缩方案按照上述方式对 UDP 报头进行压缩，HC2_UDP 压缩

字段如图 3-19 所示。最理想的情况下，UDP 报头可以被压缩成 4 字节，包括 1 字节的 HC2 编码域，1 字节的端口号，以及未被压缩的 2 字节的校验和字段。

图 3-19　HC2_UDP 压缩字段

上述两种压缩方式皆为针对无状态地址机制的报头压缩技术，在本地链路通信中十分有效，但无法适应大规模物联网中多播通信的场景。IEIF 在说明文档里提出了基于上下文的头部压缩算法，用于弥补无状态压缩算法的缺陷。基于上下文的报头压缩方案主要采用两种新的压缩技术：LOWPAN_IPHC 和 LOWPAN_NHC，简称 IPHC 和 NHC。

IPHC 可以解决 HC1 算法无法高效压缩全局可路由地址和广播地址的问题。为了能够有效地进行压缩，IPHC 使用整个 6LoWPAN 相关的信息，根据上下文的共享信息可有效地压缩 IPv6 本地单播地址、全局单播地址和组播地址，其中，单播地址可能被压缩到 64 bit、16 bit 或者完全省略。多播地址可以被压缩为 8 bit、32 bit、48 bit。对于跳数限制的几个常用值，IPHC 也进行了压缩。负载长度字段在一般情况下往往被省略，可从 IEEE 802.15.4 的长度字段或者从 6LoWPAN 分片头中计算出来。

NHC 技术实现了对 UDP 报头的压缩。当 UDP 头部被采用 NHC 算法压缩之后，被顺序携带的部分与它们在原来报头格式中的出现顺序完全相同。UDP 数据分组的长度字段可通过在接收节点使用 6LoWPAN 分片报头的 MAC 层帧头计算得出，因此可以省略。需要注意的是，NHC 的端口号压缩也是针对固定端口的，不能将该范围端口作为动态端口分配使用。因为 NHC 只能对这 16 个连续的端口号进行有效压缩，所以这 16 个连续的端口号不能包含太多的应用信息。

尽管上述压缩方法的压缩效果非常明显，但对于每次要压缩的 IP 头，都要有一种新的规范与之对应。这将导致 6LowPAN_HC 在每次收到新头部时都需要重新处理，而 GHC 算法可用于解决该问题。GHC 算法通过在数据中添加一些简单明了的标记字节来完成压缩。同时，为了实现反向查询，在 GHC 算法中定义一个 48 字节的预定义字典。预定义字典包括源地址、目的地址和 16 字节的静态字典。在 GHC 算法中为各种类型的报头添加了一种效率不高却极其通用的压缩方案。

（2）数据报的分片和重组

为了缩短报文长度，适配层帧头部分为两种格式，一种为分片格式，另一种为不分片格式。分别用于负载大于 MAC 层最大传输单元（MTU）以及负载小于 MAC 层 MTU 的报文。当 IPv6 报文要在 IEEE 802.15.4 链路上传输时，IPv6 报文必须封装在这两种格式的报文中[58]。

适配层不分片报文格式如图 3-20 所示。

- LF：链路分片（Link Fragment），此处应该为 0。

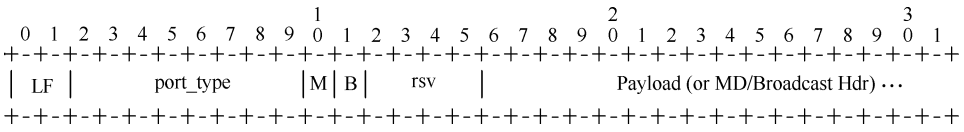

图 3-20　适配层不分片报文格式

- port_type：指出紧随在头部后的报文类型。当其为 1 时表示 IPv6，当其为 2 时表示头部压缩编码字段。
- M：指出头部后是否存在 Mesh Delivery 字段。
- B：指出头部后是否存在 Broadcast 字段。
- rsv：保留，应该全部设置为 0。

分片报文格式如图 3-21 所示。

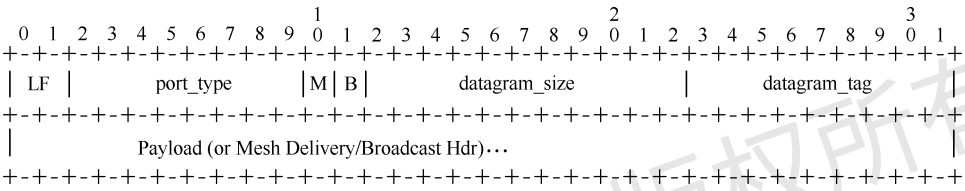

图 3-21　适配层分片报文格式

- LF：链路分片状态，其中 00 表示不分片；01 表示第一片；10 表示最后一片；11 表示中间分片。
- port_type：报文类型，只在第一个链路分片中出现。
- M：如果需要在多跳拓扑中路由，每个分片中都应该包含该字段。
- B：广播帧中每个分片都要包含此字段。
- datagram_size：表示分片前整个 IP 包的长度，值的大小在所有分片中都相等，比 IPv6 中的负载字段的值多 40 字节，最大值为 1280 字节。并不是所有的分片中都必须携带此字段的信息，可以只在第一个分片中携带该字段信息，在其他分组中省略，但这会增加后续分组先于第一个分组到达时所带来的重组风险。
- fragment_offset：报文分片偏移，只出现在第二个以及后继分片中，该字段以 8 字节为单位，因此分片报文 Payload 必须以 8 字节边界对齐。
- datagram_tag：分片标识，同一负载报文的所有分片的 datagram_tag 应该相同。每个节点需要维护一个变量来记录该值，一开始是一个随机的初始值，每发送一个完整的帧该值加 1，达到 511 后翻转为 0。

当 6LowPAN 适配层启动分片过程时，首先要判断网络层协议数据单元长度加上 6LowPAN 适配层字段的长度之和是否大于 MAC 层的最大载荷长度[59]。

确认需要分片后，则开始组装第一个分片。需要建立一个新的 IEEE 802.15.4 数据帧，并将第一个分片前 5 位置为“11000”；接下来将 datagram_tag 填入计数器当前值，将 datagram_size 填入分片前网络层报文总长度；最后将网络层数据报文复制到第一个分片中以完成第一个分片的组装。

接下来判断剩余报文是否需要继续分片，是则组装后续分片，否则进行最后一

个分片的组装。后续分片与第一个分片类似，但需要在 datagram_size 字段中填入当前分片在原数据分组中的偏移量，以 8 字节为一个偏移单位。datagram_tag 和 datagram_size 字段的值与第一片中的相同。适配层数据分片过程如图 3-22 所示。

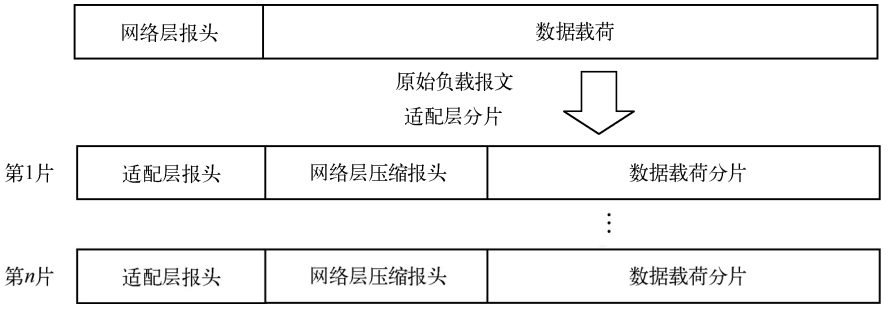

图 3-22　适配层数据分片过程

数据的重组是分片的逆过程。当接收端的适配层收到某分片时，需要根据片头判断是否为分片数据帧，是则进行重组。首先启动重组定时器，要求在规定时间内接收到该数据分组的所有分片，否则需要进行重传。然后判断该分片属于哪个数据分组，如果是第一次收到某负载报文的分片，适配层会将该分片的源 MAC 地址和 datagram_tag 字段进行缓存，以便接收其他分片；如果已经收到该数据分组的其他分片，则根据当前分片的 fragment_offset 字段进行重组。当成功接收某数据分组的所有分片时，将所有分片按 offset（偏移量）进行重组，并将重组好的原始数据分组传递给上层，同时删除缓存区内容[60]。

4. 6LowPAN 移动性和路由

6LoWPAN 的路由根据负责路由决策程序所属层的不同，可分为 Mesh-under 路由和 Route-over 路由两种。

Mesh-under 路由：路由决策在 6LoWPAN 适配层完成，采用链路层地址，根据 Mesh 头部实现二层转发，为点对点路由。

Route-over 路由：在 IPv6 网络层实现路由，采用 IP 地址，根据网络层头部实现路由转发，为逐跳路由。

6LowPAN 路由决策如图 3-23 所示，该图给出了二者的对比。

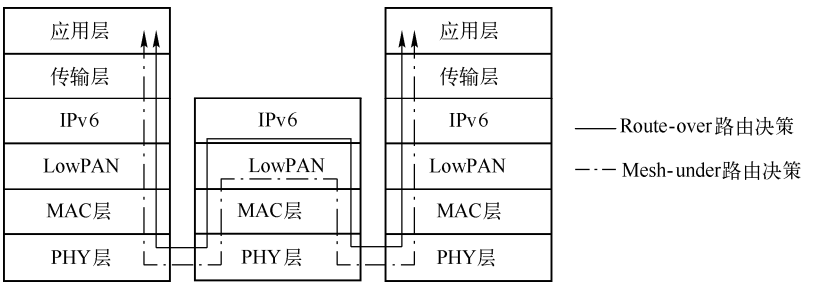

图 3-23　6LowPAN 路由决策

在 Mesh-under 路由机制下，6LowPAN 网络的路由决策在适配层完成，适配层要执行路由发现和路由选择过程，主要路由协议有 AODV 协议、LOAD 协议和 Hilow 协议等。

（1）AODV 协议

AODV 协议是一种非常适合移动网络的按需路由协议。该协议的关键在于对序列号的使用，序列号在路由发现、路由响应与链路修复中有重要作用。对处理能力强、内存大、网络带宽宽的节点而言，序列号的使用最大限度地避免了路由环路的产生，但是使用序列号带来了操作复杂、逻辑多、时间长、占用内存大的缺点，对低功耗网络来说是一个致命的缺陷。同时，AODV 协议对于 6LoWPAN 网络而言，还存在以下几个问题。

① AODV 协议是传输层协议，要将其移植到适配层，使其能够更好地匹配 6LoWPAN 是一个难点。

② AODV 协议在设计之初就未将能耗纳入考虑，这对于 6LowPAN 而言难以承受，另外，AODV 协议的路由代价是链路跳数，也无法满足当前的行业需求。

③ AODV 协议通过周期性发送 Hello 分组（又称 Hello 数据包）检测断链，这种机制虽然增加了算法发现链路断链的机会，但是也增加了无效数据在网络中的传播，增加了路由的开销，对于 6LoWPAN 也不可取。

（2）LOAD 协议

LOAD（6LoWPAN Ad Hoc On-demand Distance Vector Routing）协议是对 AODV 协议的修正。LOAD 路由基本操作，如路由发现、路由响应、路由维护都与 AODV 协议相似，但为了匹配 LowPAN 网络低速、低功耗等特点，LOAD 路由删除了 AODV 协议中的先驱列表和控制包的目的序列号，减少了路由表条目，减小了控制分组大小，从而简化了路由发现过程[61]。为了避免环路，LOAD 协议只有目的节点发起对路由请求消息的回复。LOAD 协议除了使用跳数和弱链路，还使用源节点到目的节点的累计链路开销作为路由度量指标，即 IEEE 802.15.4 PHY 层的 LQI 指标。LOAD 路由协议为 LQI 设置了一个门限阈值，在阈值限制下，选择跳数和弱链路条数均最少的路径作为最优路由路径。此外，LOAD 协议还采用 MAC 层的确认机制来保证传输的可靠性。

（3）Hilow 协议

Hilow 协议采用与 AODV 协议和 LOAD 协议完全不同的路由机制，是一种层次式路由机制。HiLow 协议使用 16 位唯一短地址作为接口标识符来增强路由的可扩展性和节省内存占用。在 HiLow 协议中，当设备加入 LoWPAN 网络时，首先通过扫描进程发现存在的网络，如果没有发现 6LoWPAN 网络，节点将成为一个初始节点，并且指定它的短地址为 0。否则，节点将会在已存在的网络中寻找邻居节点，并且通过与其通信来获取自己的短地址。在 HiLow 路由操作中，假定所有节点都知

道自己的深度[62]。当一个节点收到一个 IPv6 数据分组时，将判断自身是目的节点的上升节点还是下降节点，从而推算出数据分组的下一跳节点地址。Hilow 协议的路由结构简单，可扩展性很强，能耗低。然而，如果在路由过程中出现链路故障，HiLow 协议不再支持类似于 AODV 协议和 LOAD 协议中的链路修复机制。

目前，Route-over 路由的研究尚属初级阶段，许多问题仍需要解决。路由在网络层进行，所以必须要使用 IPv6 地址进行寻路，而 IPv6 地址占用了大量的存储空间，因此给资源受限的传感器节点带来很大的负担。同时，IP 网络现有的三层路由协议，如 RIP、OSPF 等无法直接应用到无线传感器网络当中。可用于 Route-over 路由的协议并不多，主要有 IETF RoLL 工作组研究制定的 RPL（IPv6 Routing Protocol for LLN）。

RPL 是一个基于 IPv6 的距离矢量路由协议，它通过一个目标函数和一些路由代价、路由约束建立一个面向目的地的有向无环图（Destination Oriented Directed Acyclic Graph，DODAG）。RPL 支持点对点、多点对点和点对多点三种数据流动方式，并同时支持存储模式和非存储模式[63]。在点对点数据流动方式中，非存储模式会将数据移交给源节点和目的节点的共同父节点进行转发，存储模式则由根节点进行转发；在多点对点的数据流动方式中，非存储模式和存储模式都会将父节点作为默认的下一跳节点，由父节点转发到根节点，根节点再转发数据到目的节点；在点对多点的模式下，非存储模式只有根节点有到下跳节点的路由表，而在存储模式下，所有的节点都有路由表。

RPL 的路径构建过程包括两部分：向上路由建立和向下路由建立。构建过程由三种路由消息控制，包括 DIO（DODAG Information Object，DODAG 信息对象）消息、DIS（DODAG Information Solicitation，DODAG 信息征集）消息和 DAO（Destination Advertisement Object，目标公告对象）消息。可通过 DIS 消息和 DIO 消息建立向上路由，通过 DAO 消息来完成向下路由的建立。在向下路由过程中，每个节点将其子孙节点的地址信息与自身地址信息单播给其父节点，建立由根节点到网络各个节点的路径。在向上路由过程中，从根节点开始，每个节点广播自身的 DIO 消息，邻居节点根据收到的消息选择最佳父节点加入，建立由节点到根节点的路径。

5. 6LowPAN 安全性

在物联网中最值得关注的是安全性，随着自动驾驶、智能家居等行业的兴起，网络的安全性显得越发重要。将 IPv6 引入 LowPAN 网络是一把双刃剑，它不仅带来了 IP 网络的优点，同时也带来了在当前 IP 网络中存在的一些安全问题[64]。为了满足 6LowPAN 网络的安全，需要满足以下几个方面的需求。

① 数据机密性：数据机密性对网络安全十分重要。数据机密性是指数据在传输和存储的过程中保证数据的机密性，未被授权者不能获取数据的内容。例如，一个 6LowPAN 节点不应该将采集的数据泄露给邻居网络。

② 数据完整性：数据的机密性可以保证攻击者无法获取数据的真实内容，而对数据完整性的鉴别可以确保数据在传输过程中没有被恶意篡改。然而，数字签名

鉴别对于内存资源有限的 6LoWPAN 网络，代价太大并不适合。在 6LoWPAN 网络中，一般采用消息认证码的方式来对数据完整性进行校验。

③ 数据真实性：数据真实性指数据来源于合法节点而非伪造。在 6LoWPAN 网络中，向网络注入恶意消息很容易，这就非常有必要进行节点身份认证，接收者需要对数据源认证以确定数据的可靠性。

④ 可用性：可用性指合法用户能够正常使用 6LoWPAN 网络所提供的各种服务，并能抵御非法用户的恶意攻击。对于资源受限的 6LoWPAN 网络应该选用一种简单、高效的安全机制，以减少能耗并延长网络寿命。

⑤ 安全路由：在 6LoWPAN 网络中路由和数据转发是极其关键的功能。攻击者可以针对路由协议发起 DOS 等攻击，从而阻止正常通信。由于 6LowPAN 的路由协议较为简单且尚未成熟，健壮性较差，需要设计强壮的安全路由来抵抗各种攻击。

6LowPAN 网络中节点受到以下条件的约束：节点的各种资源有限，如能量有限，缓存资源和计算资源有限。同时，6LowPAN 网络具有节点间通信不可靠、物理安全无法保证、节点的部署密度大且随机布置、网络拓扑灵活多变，以及安全需求与应用相关等特点，因此，6LowPAN 的安全机制主要面临以下挑战：

① 最大限度地减少资源消耗和提高安全性能。

② 链路层的攻击从被动监听扩展到积极干预。

③ 必须有中间节点参与网络内端到端的信息传输。

④ 传统的安全机制不再适合 6LoWPAN 网络通信。

3.2 低功耗广域网通信技术

随着物联网的发展，物联网技术在各行业中的应用越来越广泛，不同的应用对无线传输技术的需求也各不相同。现如今广泛使用的无线传输技术具有传输距离短、速度快等特征，并不适用于物联网数据传输所要求的窄带宽、低功耗、长距离通信。因此，有了一项新兴技术：低功耗广域网（Low-Power Wide-Area Network，LPWAN）[65]。LPWAN 是一种革命性的物联网无线接入新技术，与蓝牙和 ZigBee 等现有成熟商用的无线技术相比，具有远距离、低功耗、低成本、覆盖容量大等优点，适合长距离发送小数据量且使用电池供电方式的物联网终端设备。LPWAN 与传统的互联网技术在工作模式上有很大的区别，为了减少终端功耗，LPWAN 仅在有数据传输的条件下才会建立连接。因此，LPWAN 使用少量的数据集中节点、传输设备就可以支撑大规模的终端通信。

LPWAN 采用了 NB-IoT、LoRa 和 Sigfox 等几种比较典型的技术，根据工作模式可将其分为两类：授权频段和非授权频段。截至目前，低功耗广域网络大部分部署在非授权频段上，即 ISM 频段，如 LoRa 和 Sigfox。而 NB-IoT 则基于现有的移动网络。总的来说，在技术方面，多种 LPWAN 技术的特点各异，采用不同的方式，实现物联网专用网络低成本、低功耗、远距离、大量连接的特性。

3.2.1　NB-IoT

1. NB-IoT 概述

NB-IoT 是一种全新的基于移动网络的窄带物联网技术，由 3GPP 定义，作为 3GPP R13 的一部分，在 2016 年 6 月实现标准化。NB-IoT 的特点是可以直接使用运营商的当前授权频段，可直接部署在 LTE 网络环境中，是一种可以在全球范围内广泛应用的新型物联网通信技术。

NB-IoT 技术优势主要体现在如下几个方面[66]。

- 网络覆盖广：相对 LTE，NB-IoT 技术的最大链路预算提升了 20 dB，几乎提升了 100 倍，即便处于恶劣的通信环境中，NB-IoT 仍然能保持较强的信号穿透力。

① 功耗管理灵活：NB-IoT 通过减少不必要的信令、采用更长的寻呼周期、使终端进入省电状态等机制来达到节能的目的，相比于其他低功耗广域网技术，NB-IoT 在电池寿命上依然具有优势。

② 成本低：NB-IoT 终端成本低，可以广泛应用于物联网环境。另外，基于移动网络的 NB-IoT 大大减少了部署成本和运营成本。

③ 大连接：NB-IoT 通过提高功率密度和重复传输的方式提高了网络覆盖的广度和深度。同时，NB-IoT 终端数据发送速率低，对时延不敏感，能够满足大量设备的连接请求。

④ 部署方式灵活：NB-IoT 可直接部署在 LTE 网络中，也可以利用 2G 和 3G 的频谱来部署，在数据安全和建网成本，以及产业链和网络覆盖方面相对于非授权频段都具有较大的优越性。

⑤ 安全性：继承了 4G 网络安全的能力，支持双向鉴权和空口严格的加密机制，确保 UE 在发送接收数据时的空口安全性。

2. NB-IoT 物理层

物理层位于 NB-IoT 协议栈的底层，提供物理介质中数据传输的所有功能，为高层提供信息传输服务，物理层用于解决如何通过无线接口传输数据，与传输内容相互独立。

（1）上下行传输方案

NB-IoT 的上下行传输广泛地复用 LTE 的设计方案。NB-IoT 上下行传输方案如图 3-24 所示。

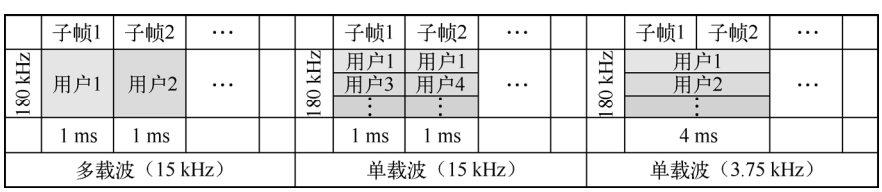

图 3-24　NB-IoT 上下行传输方案

NB-IoT 上行采用 SC-FDMA 多址方式，支持多载波和单载波两种传输方式。多载波方式与 LTE 具有相同的 15 kHz 子载波间隔，时隙长度为 0.5 ms、子帧长度为 1 ms，每时隙包含 7 个 SC-FDMA 符号；单载波方式配置 15 kHz 和 3.75 kHz 两种子载波间隔，由于每时隙符号数需要保持不变，3.75 kHz 的子载波每时隙长度为 2 ms，子帧长度为 4 ms。

NB-IoT 下行采用 OFDMA 多址方式，在频域中仅使用 1 个 LTE PRB，即 12 个 15 kHz 子载波，共计 180 kHz。子载波间隔为 15 kHz，时隙长度为 0.5 ms，子帧长度为 1 ms，每时隙包含 7 个符号。此外，当进行带内部署时，NB-IoT 与其他 LTE PRB 之间的物理信道保持正交。

（2）频率部署方案

NB-IoT 定义了 3 种部署场景，按其分配频段与 LTE 频段的关系分为独立（Stand-alone）部署、保护带（Guard-band）部署和带内（In-band）部署。NB-IoT 频带部署方案如图 3-25 所示[67]。

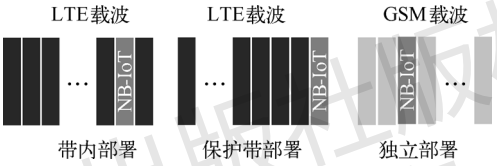

图 3-25　NB-IoT 频带部署方案

带内部署是将 NB-IoT 部署在 LTE 的有用带宽内，占用 LTE 载波的任意一个物理资源块。该模式可通过增加 NB-IoT 载波进行载波扩展，较为灵活，但会占用 LTE 的频谱资源。同时，为了减少对 LTE 的干扰，该模式下的 NB-IoT 需要控制下行发射功率，覆盖能力较弱。

保护带部署将 NB-IoT 部署在 LTE 的边缘保护频带内，不占用 LTE 的物理资源块，但需要预留和 LTE 之间的 100 kHz 以上的保护带，而且和带内部署一样，需要考虑下行发射功率对 LTE 的干扰。

独立部署是在 LTE 载波外选择任意空闲的超过 180 kHz 的频段部署 NB-IoT。相比于以上两种方式，独立部署对 LTE 系统的影响较小，可以有效增强 NB-IoT 的下行能力。但是，独立部署方案需额外占用频谱资源，并需要留出一定的频率保护间隔。实际上真正可用于部署的频率资源并不丰富，适用于部署在重耕的 GSM 频段。

（3）物理信道

① 下行链路。

针对 180 kHz 下行传输带宽的特点，同时满足覆盖增强的需求，NB-IoT 系统对下行物理信道类型进行了简化，重新设计了部分下行物理信道、同步信号和参考信号，具体包括窄带物理广播信道（NB-PBCH）、窄带物理下行共享信道（NB-PDSCH）、窄带物理下行控制信道（NB-PDCCH）、窄带主同步信号（NB-PSS）、窄带辅同步信号（NB-SSS）和窄带参考信号（NB-RS），并在下行物理信道上引入了重复传输

机制，通过重复传输的分集增益和合并增益来提高解调门限，更好地支持下行覆盖增强[68]。NB-IoT 物理层的下行信道结构如表 3-3 所示。

表 3-3　NB-IoT 物理层的下行信道结构

#0（0 号子帧）	#1	#2	#3	#4	#5	#6	#7	#8	#9
NB-PBCH	NB-PBCH 或 NB-PDSCH	NB-PBCH 或 NB-PDSCH	NB-PBCH 或 NB-PDSCH	NB-PBCH 或 NB-PDSCH	NB-PSS	NB-PBCH 或 NB-PDSCH	NB-PBCH 或 NB-PDSCH	NB-PBCH 或 NB-PDSCH	偶数帧：NB-SSS 奇数帧：NB-PDCCH 或 NB-PDSCH

② 上行链路。

NB-IoT 系统也缩减了上行物理信道类型，重新设计了部分上行物理信道，具体包括窄带物理随机接入信道（NPRACH）、窄带物理上行共享信道（NPUSCH）；不支持物理上行控制信道（PUCCH）。为了更好地支持上行覆盖增强，NB-IoT 系统在上行物理信道上也引入了重复传输机制，通过该机制提高信道在条件恶劣时的传输可靠性，上行最多可重复传输 128 次。

3. NB-IOT 关键流程

（1）随机接入过程

在 NB-IoT 系统中，随机接入过程是一个至关重要的过程，只有通过随机接入过程实现上行同步后，用户方可进行上行数据传输。相对 LTE 系统而言，由于 NB-IoT 系统不支持切换功能，因此，随机接入场景被简化为以下 5 种。

① 无线资源控制（Radio Resource Control，RRC）空闲状态下的初始接入。

② RRC 连接重建过程。

③ RRC 连接态下，上行失步情况下的接收下行数据过程。

④ RRC 连接态下，上行失步或触发调度请求情况下的发送上行数据过程。

⑤ RRC 连接态定位功能。

根据覆盖增强的对象，NB-IoT 系统选择包含了覆盖水平的随机接入。UE 依照测量所得的信号强弱对目前的覆盖级别进行分析，同时按照覆盖级别选取合适的资源完成随机接入过程。覆盖等级由 UE 测量的参考信号接收功率 RSRP 确定。UE 通过小区广播的系统消息获取 RSRP 阈值列表，其中至多包含两个 RSRP 阈值，UE 通过将接收信号与 RSRP 阈值进行对比得到当前所处等级。表 3-4 所示为 UE 覆盖等级判断[69]。

表 3-4　UE 覆盖等级判断

RSRP 测量值 R	覆盖等级	信道条件
$R<\mathrm{RSRP}_2$	CE Lever 2	差
$\mathrm{RSRP}_2 \leqslant R<\mathrm{RSRP}_1$	CE Lever 1	中等
$\mathrm{RSRP}_1 \leqslant R$	CE Lever 0	好

（2）寻呼过程

NB-IoT 寻呼是指在系统信息变更或有下行数据到达时对空闲态的终端进行通知。当核心网需要向终端发送数据时，将通过 MME 经 S1 接口向基站发送寻呼消息，基站收到该寻呼消息后，在收到的 TA 列表中的小区内进行寻呼。NB-IoT 寻呼过程如图 3-26 所示。

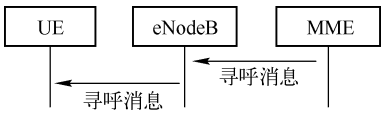

图 3-26　NB-IoT 寻呼过程

NB-loT 终端在空闲态下的被叫寻呼分为不连续接收（DRX）寻呼和扩展间断接收（eDRX）寻呼，处于空闲态的终端只要定义好固定的周期，就可以对 PDCCH 进行不连续的监听，这样可以节省终端发射功率。由于 NB-loT 对低功耗方面要求更高，新增的 eDRX 功能可进一步延长终端在空闲模式下的睡眠周期，减少接收单元不必要的启动。eDRX 适用于低速率、低频次的业务模型[70]。

4. NB-IoT 数据传输

NB-IoT 技术主要面向小数据传输、非频繁传输和低移动性、时延不敏感的业务场景。在 NB-IoT 标准制定过程中，为了降低基带芯片复杂度、降低成本，延长电池寿命，在协议层引入了两种数据传输模式，分别是 CP 模式和 UP 模式。其中，CP 模式是必选项，UP 模式是可选项。如果 UE 同时支持两种模式，则用户具体采用的模式由用户通过 NAS 信令与核心网设备进行协商确定。

CP 优化方案基于控制面的数据传输方式。由于采用控制平面来转发数据，用户数据被直接封装在 NAS 信令消息中，并采用部分加密方式进行加密。与传统 LTE 用户面的数据传输方式相比，CP 优化方案简化了 RRC/S1 信令流程，用户数据仅通过原控制面的 NAS PDU 打包进行传递，无须建立 S1-U，无须通过 RRC 重配置过程和 AS 安全过程，也不建立 DRB，用户直接在 SRB1bis 上进行数据传输，简化了流程，减小了信令开销，更适合短数据业务[71]。但 CP 优化方案需要在 MME 中增加用户面功能，以支持用户面流量的重定位和数据缓冲，增加了 MME 的处理负载。

UP 优化方案采用原有 LTE 用户面进行数据传输。与 LTE 用户面相比，UP 优化方案虽然也会通过 RRC 连接重配置过程和 AS 安全过程，建立 SRB 和 DRB，但引入了新的挂起 / 恢复机制，可快速恢复空口 / S1-U 承载，减少了空口和核心网的信令流程。UP 优化方案对 eNodeB 的处理能力要求更高，需要一直存储 UE 空口和 S1 承载上下文。UP 优化方案是 3GPP 标准的可选方案，但在 eMTC 接入时，UP 方案优化为必选。

数据业务可采用两种数据分组方式：IP 或者 non-IP，non-IP 是为应对物联网发送的数据分组频率低、字节少而产生的，对于物联网的数据分组来说，UDP/IP 传输层协议栈占用字节中数据报头比例很高，尤其是在有效负荷小的情况下，报头甚

至超过了数据。在这种情况下，终端传输 non-IP 数据可以大幅提高无线网络的数据传输效率[72]。

5. NB-IoT 组网方式

考虑到 NB-IoT 独立建网成本高，可共软硬件支持 NB-IoT 和 LTE，所以现网多采用联合规划，即 NB-IoT 基于 LTE 目标网络进行规划建设。在 LTE 规划站址上分布部署 NB-IoT，实现不同覆盖能力，一般有 LTE 1∶1 组网和 1∶*N* 组网两种方案，1∶1 组网深度覆盖效果较好，邻频干扰较小，但投资成本相对较高。

基于 LTE 的 NB-IoT 组网形式如图 3-27 所示，主要分为如下所述的 5 个部分[73]。

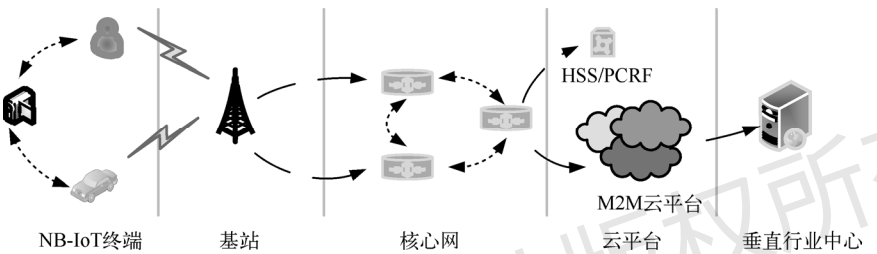

图 3-27　基于 LTE 的 NB-IoT 组网形式

① NB-IoT 终端：NB-IoT 终端指实际联网的物联网物理设备，包括专用业务芯片实体模块、传感器和无线传输模块等基础硬件，只需要安装相应的 SIM 卡就可以接入 NB-IoT。

② NB-IoT 基站：NB-IoT 基站是移动通信中组成小区的基本单元，主要指运营商已架设的 LTE 基站，可以实现移动通信网和窄带物联网终端之间的通信和管理功能，是连接移动通信网和窄带物联网终端的桥梁。

③ 核心网：核心网可以将基站与云平台连接起来。核心网网元包括负责物联网接入业务的移动管理实体、服务网关和物联网专网网关，需要根据标准进行开发，可通过现网升级改造的方式支持 NB-IoT 相关核心网特性，也可以新建独立的 NB-IoT 核心网。

④ 云平台：NB-IoT 云平台负责对各种业务数据进行处理和调度，比如应用层协议栈的适配以及大数据的分析等，并将处理结果转发给垂直行业中心的服务器或相应的 NB-IoT 终端。

⑤ 垂直行业中心：不同行业的应用服务器，可以获取 NB-IoT 终端数据，并控制各行业终端的业务周期。

3.2.2　LoRa

1. LoRa 概述

LoRa 全称是 Long Rang，是一种基于扩频技术的低功耗长距离无线通信技术，主要面向物联网，应用于电池供电的无线局域网和广域网设备[74]。LoRa 在 2013 年

首先由 Semtech 公司推出，而后在 2015 年 3 月的世界通信大会上，由物联网界的领导者发起成立 LoRa 联盟。作为一个开放性的、非营利性组织，LoRa 联盟志在将 LoRa 技术在全球推广并实现商用。与其他 LPWAN 无线技术相比，LoRa 产业链更成熟，商业化应用较早，目前已成为新物联网和智慧城市发展的重要基础支撑技术。

LoRa 技术具有完善的网络架构、协议以及成熟的通信模块[75]。LoRa 的网络架构和协议栈如图 3-28 所示，网络架构中包括终端、网关、网络服务器和业务服务器等。其中终端节点包括物理层、MAC 层和应用层，处于整个网络的底层，主要功能是采集应用所需的传感信息，或执行上层发送的命令；终端通过星状拓扑连接到网关，由网关完成空口物理层的处理。网关收集 LoRa 终端上报的信息，将解调设备上发的射频信息，调制服务器下发的命令信息发送给终端；而网络服务器负责进行 MAC 层处理，包括自适应速率选择、网关管理和选择、MAC 层模式加载等。应用服务器从网络服务器获取应用数据，完成应用状态展示和即时告警等。

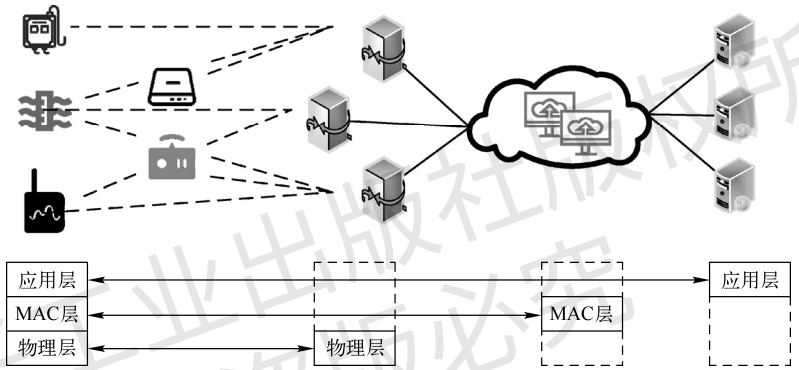

图 3-28　LoRa 网络架构和协议栈

LoRa 采用的通信模块在调制解调部分配置了标准的 FSK 调制解调器和远距离扩频调制解调器，用户可根据实际通信环境，选择适当的模式，如 OOK、FSK 调制以及 LoRa 扩频技术。LoRa 扩频技术可以实现长距离的通信并对干扰信号有较强的抵抗能力，可适应于低信噪比环境下的无线通信。

2. LoRa 物理层

LoRa 物理层主要完成不同地区的频段划分和 LoRa 技术的调制解调机制，以及对数据的发送与接收。数据在物理层以物理帧的形式传输。

LoRa 物理层信息有两种，分别为上行链路消息和下行链路消息。

① 上行链路消息：终端采集数据经过一个或多个网关透传到网络服务器。一台 LoRa 终端设备可以同时接入多个网关，并可与多个网关进行上行通信。

② 下行链路消息：服务器下发数据通过网关发给终端设备，每一个下发的数据对应的终端地址是唯一确定的，而且只通过一个网关转发。

（1）物理层帧格式

LoRa 数据帧在物理层增加了前导码和报头以及 CRC（循环冗余校验），以提高

数据传输的可靠性。LoRa 物理层数据帧结构如图 3-29 所示。

图 3-29　LoRa 物理层数据帧结构

其中，前导码用于保持接收机与输入的数据同步，其长度可根据具体应用而变化。例如，在接收密集型应用中，可以缩短前导码长度，以减少传输数据与接收机的同步时间。可选报头分为显式报头和隐式报头。显示报头包括有效载荷的相关信息，如载荷长度、编码率、是否采用 CRC 等信息。报头含有自己的 CRC 用于接收机检验，接收机可以通过报头中的信息来判断是否继续接收该数据或直接将其丢弃。当有效载荷的相关信息固定且已知时，可采用隐式报头以缩短发送时间[76]。

（2）频段划分

LoRa 物理层对网络中的信道频率进行了规范，不同的国家和地区使用不同的工作频段，主要为各国的 ISM 频段，中国采用的频段为 470～510 MHz。物理层还定义了物理无线信道与 MAC 层之间的接口，每个区域可使用的频段至少可以划分出 16 个信道。各个地区对频段的规定除频率范围不同外，其他参数基本一致。

3. LoRa MAC 层

MAC 层是整个通信系统的关键层，是完善整个 LoRa 系统的关键。2015 年 6 月，LoRa 联盟发布了第一个开放性标准 LoRaWAN R1.0。LoRaWAN 提供了一种物理接入控制机制，使得众多使用 LoRa 调制的终端可以和基站进行通信。

（1）消息格式

MAC 层消息格式如图 3-30 所示[77]。其中，MHDR 为 MAC 头；MACPayload 为 MAC 负载；MIC 为消息一致性校验码。

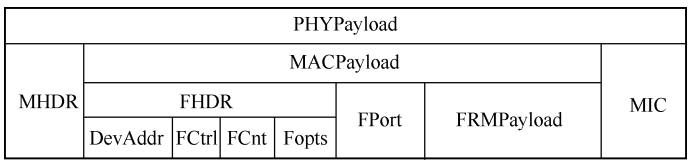

图 3-30　MAC 层消息格式

在 MHDR 中定义了消息类型（MType）和当前消息结构所遵循的 LoRaWAN 协议的主版本号。LoRaWAN 自定义了 6 种不同的 MAC 消息类型：请求入网、同意入网、无须确认的上行消息、无须确认的下行消息、需要确认的上行消息和需要确认的下行消息。

MACPayload 为 MAC 负载，即所谓的数据帧，包含帧头（FHDR）、端口（Fport）和帧荷载（FRMPayload）。

帧头中包含了设备地址（DevAddr）、帧控制字节（FCtrl）、帧计数器（FCnt）

和配置字段（Fopts），其中 Fopts 用来配置传输 MAC 命令，最多 15 字节；帧控制字节（FCtrl）定义了上行和下行消息的信息。LoRa 帧控制字节如图 3-31 所示。

第几位(bit)		7	6	5	4	[3～0]
FCtrl	下行	ADR	RFU	ACK	Fpending	FOptLen
	上行	ADR	ADRACKReq	ACK	RFU	FOptLen

图 3-31　LoRa 帧控制字节

FCtrl 中的 ADR 和 ADRACKReq 用于数据速率自适应控制（Adaptive Date Rate，ADR），ADR 决定是否启用速率自适应功能，当 ADR 为 1 时则启用，当 ADR 为 0 时则不启用。在重发次数达到上限后，如果终端依然没有收到来自服务器的数据，终端将降低数据速率，以获得更远的射频传输距离，并重复上述过程直到终端达到最低数据速率。ACK 为消息确认位，当收到 Confirmed 类型的消息时用其进行应答。Fpending 为帧挂起位，只在下行交互中使用，表示网关还有数据挂起等待下发，此时要求终端尽快发送上行消息来再次打开接收窗口。FOptLen 被修改为帧配置长度，表示 FOpts 的实际长度。RFU 为保留字段，保留供将来使用。

（2）终端设备类型

在 LoRaWAN MAC 协议中将节点（终端设备）划分为三类，分别为 Class A、Class B 和 Class C。三类节点的主要区别在于数据传输时延和节点功耗[78]。

① Class A。

Class A 终端设备在上行传输结束后会打开两个下行的接收窗口 RX1 和 RX2，打开接收窗口的时延通过 ALOHA 协议进行微调，上行传输时间基于自身的数据传输需求[79]。Class A 终端设备的接收窗口开启时间较短，在没有数据发送任务时处于休眠状态，是功耗最低的终端模式，它只要求基站在终端设备发送一次上行数据后发送一次下行数据，发送数据和接收数据是交替进行的，这导致 Class A 终端设备的下行传输灵活性非常差，下行数据的时延也最长。简言之，Class A 终端设备的通信过程是由终端设备发起的，若基站想发送下行数据，必须等待终端设备先发送完上行数据。图 3-32 给出了典型的 Class A 传输模型。

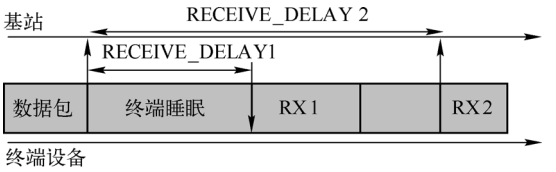

图 3-32　典型的 Class A 传输模式

② Class B。

Class B 终端设备的模式在 Class A 模式的基础上增加了同步接收窗口和预设接收窗口，分别用于接收时间同步信标（Beacon）和服务器指定时间的下行数据。由

终端设备应用层根据需求来决定是否将终端设备切换到 Class B 模式。首先，网关会广播一个 Beacon 来为终端设备提供一个时间参考。据此，终端设备定期打开额外的接收窗口供基站发起下行数据，其个数根据服务器的下行数据量、下行时延要求及终端设备对能耗的要求确定。当终端设备的网络位置或者身份发生变化时，需要发送上行帧以更新下行路由表，否则终端设备会失去与网络的同步，此刻终端设备将切换回 Class A 模式。图 3-33 给出了典型的 Class B 传输模型。

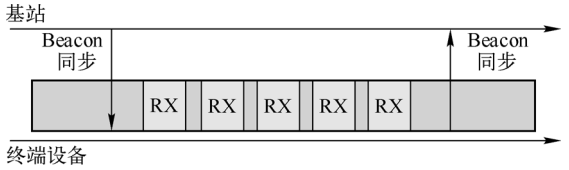

图 3-33　典型的 Class B 传输模式

③ Class C。

Class C 终端设备几乎持续为接收窗口开放，只要不是正在发送信息或正在 RX1 接收信息，Class C 终端设备就会在 RX2 侦听下行传输。为此，终端设备会根据 RX2 的参数设置，在上行传输和 RX1 之间打开一个短的接收窗口（图 3-34 中第一个 RX2），打开接收窗口的时间间隔很短，在 RX1 关闭后，终端设备会立刻切换到 RX2，直到有上行数据传输才关闭。Class C 终端设备和服务器交互的时延小，但比 Class A 终端设备和 Class B 终端设备更耗能，适用于供能充足的场景。图 3-34 给出了典型的 Class C 传输模型。

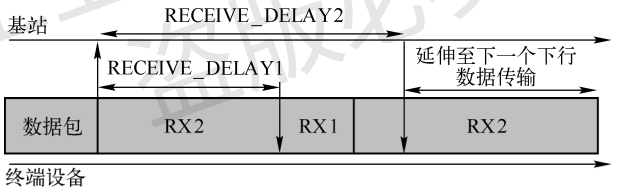

图 3-34　典型的 Class C 传输模型

LoRaWAN 协议规定，接入 LoRa 网络的 LoRa 节点需要至少实现 Class A 模式，不同类别的节点 MAC 协议定义也不同。Class A 终端设备节能效果最好，最适合用于移动供电的场景中，因此目前针对 LoRaWAN 的研究大多基于 Class A 节点协议进行。

（3）节点入网模式

LoRa 节点终端设备有两种入网模式，分别为 OTAA（Over-The-Air Activation，无线激活）和 ABP（Activation By Personalization，个性激活）[80]。ABP 是一种个性化激活模式，直接把终端设备和特定的网络连接到一起，这意味着节点在开启前就已经将所需信息全部烧写至节点内部，终端设备上电后就自动入网，无须注册即可进行正常的双向数据通信。而 OTAA 模式下的终端设备需要经历一个接入流程。终端设备在刚上电时并不处于入网状态，需要向服务器发送入网请求，由服务器响

应并建立长地址和短地址之间的映射关系，生成通信密钥并下发给终端设备，终端设备根据响应内容生成注册信息，而后方可收发数据。

4. LoRa 关键技术

LoRa 技术本质上是扩频调制技术，同时结合了数字信号处理和前向纠错编码技术。LoRa 扩频调制技术是由 Semtech 公司针对超高信噪比环境推出的一种基于线性扩频调制技术的超远距离无线传输技术，采用在时间上线性变化的频率啁啾（Chirp）对信息进行编码。与传统扩频技术相比，它具有良好的对抗多径衰落和多普勒效应的能力，传输距离远，消耗能量低，同时放松了对晶体基准振荡器的频率容限要求，从而在降低成本的基础上保证了性能。

在 LoRa 调制模式下，最重要的参数为带宽、扩频因子以及编码速率。这些参数共同决定了 LoRa 收发器的能量消耗、信号传输范围、传输速率及抗噪声能力[81]。其中，扩频因子是指在使用扩频技术进行数据传输时，扩频后的码片速率与数据速率的比值。扩频因子的使用可以产生正交码，这样就可以在同一个频段内同时传输多路数据，合理选择扩频因子可以在保证数据传输可靠性的同时提高数据传输速率，扩频因子取值为 6～12。编码率表示数据流中有用部分的比例，LoRa 采用循环纠错编码对传输的数据信息进行编码，这会带来一定的开销，但能提高传输信号在强干扰环境下的信噪比，针对不同的应用环境可以设置相应的编码率。信号带宽指允许通过的最高频率信号与最低频率信号的频率之差。LoRa 调制解调器中描述的带宽指双边带带宽，取值为 7.8～500 kHz，较为常用的是 125 kHz 和 250 kHz。在 LoRa 调制模式下，带宽数值等于 Chirp 速率，带宽越大，比特速率越高，但同时接收灵敏度却在降低。

3.2.3　Sigfox

Sigfox 是一种商用化速度较快的 LPWAN 技术，由法国 Sigfox 公司提出，旨在构建低成本、低功耗的物联网专用网络。它使用工作于 1 GHz 以下的 ISM 频段。该技术使用极窄频带，通过 BPSK 调制，以 100 bps 的超低速率进行数据发送。由于超窄带技术将噪声能量密度扩展到整个频谱，所以其信号在任何窄的频谱内都大于噪声。通过低速率抗干扰的调制方式，Sigfox 可以换取极强的覆盖能力，最大允许路径损耗可达 160 dB，远超传统的移动通信技术，适用于深入地底下或被掩埋的传感器节点数据传输。然而，Sigfox 的数据发送能力较弱，每条信息最多为 12 字节，且每天的数据发送量不超过 140 条信息。因此，需要传输大量数据或保持长时间在线连接的物联网设备并不适用于 Sigfox 技术。Sigfox 更多应用于物联网应用中的短信息类业务，通过限制数据包传输大小，限定了单个节点占用的资源，以一种高效的方式满足类似温 / 湿度、位置等简单信息的传输需求[82]。Sigfox 没有上行信息确认能力，需要通过时频分集和重复传输技术来保证上行传输的可靠性。每个终

端设备随机选择不同的频率通道发送三次信息，基站可以在所有信道上同时接收信息，降低了终端设备的复杂度和成本。

3.3　移动通信技术

全面的信息采集是物联网的基础，传感节点采集到的物体特征信息需要由网关节点通过承载网络传递到处理单元，这就要求承载网络“无所不在”，能够随时随地传输被采集的信息。不同的物联网应用对承载网络的要求存在较大的差异，因此能够全面接入并承载所有物联网应用的承载网络必须具备无缝的广域覆盖，灵活的接入手段。物联网中人与物、物与物之间的互联，大量信息的采集和交换设备的使用，使得信息安全和隐私保护成为亟待解决的问题。有线接入方式虽然可以为数据的传输提供安全、稳定、高速的通道，但物联网感知节点的广泛性与移动性决定了有线方式的应用场景有很大的局限性。移动通信网络以其相对有线网络无可比拟的可移动性与灵活性成为节点与远端控制中心进行远距数据传输的首选。将移动通信技术应用于物联网中的信息接入和传输，实现移动通信网络和物联网的有机融合，将能极大地促进物联网的普及与应用。

移动通信由若干个无线小区组成，每个小区都设置有一个小功率基站，随着用户数的增加，可以通过小区分裂、频率再用、小区扇形化等技术提高系统容量。近几十年来，移动通信技术一直在稳步发展，从第一代移动通信系统到第五代移动通信系统，移动通信一直致力于为用户提供更优质、更快捷、更有价值的服务。然而传统的移动通信主要满足人与人之间的通信需求，设备的成本较高且功耗巨大，而没有考虑物联网场景低成本、广覆盖、大容量和低功耗的需求，无法直接应用于物联网。在 4G/4.5G 中，增加了面向物联网的标准，如 LTE-eMTC，支持更低功耗，更低成本的设备。5G 更是将物与物之间的通信作为一个主要场景，有效支持物联网设备的海量连接。随着物联网场景日趋复杂化，6G 的智能化将为物联网提供强有力的支撑。

3.3.1　第四代移动通信技术

1. 4G 概述

第四代移动通信技术，即 4G，现阶段主要包括 TD-LTE 和 FDD-LTE 两种制式。其中 TD-LTE 主要由中国主导制定，TD-LTE 的下行速率最高为 100 Mbps，上行速率最高为 50 Mbps; FDD-LTE 的下行速率最高为 150 Mbps，上行速率最高为 50 Mbps。4G 网络主要核心技术包括正交频分复用技术、基于 IP 的核心网技术、多用户检测技术、多输入多输出技术和智能天线技术等。4G 网络是 3G 网络的延伸，与 3G 网络相比，4G 网络采用了新的调制方式、更好的编码方案和分集接收等新技术，4G 网络采用多载波正交频分复用调制技术，提高了频谱的利用率。

4G 网络具有高速率、良好的兼容性和灵活性、多类型用户并存、多种业务相融等特性。与 3G 网络相比，4G 网络速率更高，并且能够兼容 2G 网络和 3G 网络，具有全球漫游和开放接口的功能。4G 网络采用智能技术，不仅能根据用户业务的变化自动分配相应业务所需要的资源，而且可以根据网络动态和信道变化自动处理，使各种用户设备能够共存与互通，满足多类型用户的各种需求。由于 4G 具有的高速率特性，因此 4G 网络不仅可以实现语音通话功能，还可以支持视频会议、移动采访等功能。

LTE 是当前 4G 采用的技术标准，要实现 4G 和物联网的有机融合，需要对 LTE 的技术核心有清晰的认识，并充分发挥其技术优势。

2. LTE 网络架构

LTE 系统由核心网络（EPC）、地面无线接入网（E-UTRAN）和用户设备（UE）3 部分组成。其中 EPC 是 LTE 系统的核心部分；由 eNodeB（简称 eNB）组成的 E-UTRAN（LTE）是 LTE 系统的接入网部分；UE 为用户终端设备。eNB 与 EPC 通过 S1 接口连接；eNB 之间通过 X2 接口连接。E-UTRAN 结构如图 3-35 所示。

eNB 提供无线资源管理、IP 头压缩和用户数据流加密、从 MME 发起的寻呼消息的调度和发送、从 MME 或操作和维护系统发起的广播消息的调度和发送、移动性及调度测量与测量上报配置等功能。

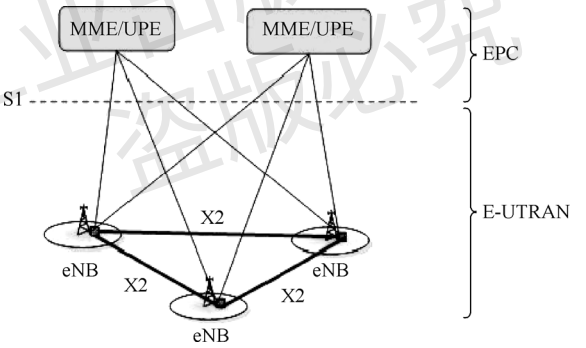

图 3-35　E-UTRAN 结构

eNB 是向 UE 提供的控制平面和用户平面协议的终点。eNB 之间通过 X2 接口互连。eNB 通过 Sl 接口同演进的分组交换核心网相连。eNB 提供无线资源管理功能，包括无线承载控制、无线接入控制、连接移动性控制和动态资源分配功能。

移动性管理实体（MME）负责将寻呼信息分发至 eNB。用户平面实体（UPE）负责对用户数据流的 IP 首部进行压缩和加密，终止用于寻呼的用户平面数据包，为支持 UE 移动性进行用户平面的切换。

Sl 接口是区分 E-UTRAN 和 EPC 的接口。S1 接口包括两部分，分别是控制平面接口（S1-C）和用户平面接口（S1-U）。S1-C 是 eNB 与 EPC 中 MME 之间的接口，而 Sl-U 是 eNB 与 EPC 中 UPE 之间的接口。S1-C 无线网络层协议支持的功能有：移动性功能（支持系统内和系统间的 UE 移动性）、连接管理功能（处理 LTE_IDLE

到 LTE_ACTIVE 的转变，漫游区域限制等功能）、SAE 承载管理（SAE 承载的建立、修改和释放）、总的 Sl 管理和错误处理功能（释放请求、所有承载的释放和 S1 复位功能）、在 eNB 中寻呼 UE、在 EPC 和 UE 间传输 NAS 信息，以及 MBMS 支持功能。

S1-U 无线网络层协议支持 eNB 和 UPE 之间用户数据包的隧道传输。隧道协议支持的功能有：对数据包所属的目标基站节点的 SAE 接入承载的标识、减少由于移动性而导致的数据包丢失、错误处理机制、MBMS 支持功能和包丢失检测机制。

X2 接口是 eNB 之间的接口，X2 接口包括两部分，分别是控制平面接口（X2-C）和用户平面接口（X2-U）。X2-C 是 eNB 之间控制平面的接口，而 X2-U 是 eNB 之间用户平面的接口。X2-C 无线网络层协议支持移动性功能（支持 eNB 之间的 UE 移动性，包括信令切换和用户平面隧道控制）、多小区 RRM 功能（支持多小区的无限资源管理及总的 X2 管理和错误处理功能）。X2-U 无线网络层协议支持 eNB 之间用户数据包的隧道传输。隧道协议支持的功能有：对数据包所属的目标基站节点的 SAE 接入承载的标识和减少由于移动性而导致的数据包丢失。

随着信息技术的快速发展，物联网信息的种类和数量等都在不断增加，需要分析的数量呈爆发式增长，物联网面临着如何有效处理各种异构网络以及系统之间的数据融合的挑战。

LTE 与已有的其他移动通信网络相比，其根本的优点就是采用了全 IP 的网络体系架构，可以实现不同网络间的无缝互联。LTE 的核心网采用 IP 后，所使用的无线接入方式和协议与核心网络（CN）协议、链路层是相互独立的。IP 与多种无线接入协议相兼容，因此在设计核心网络时具有很大的灵活性，不需要考虑无线接入究竟采用何种方式和协议。

3. LTE 协议架构

3G 网络由基站（NB）、无线网络控制器（RNC）、服务通用分组无线业务支持节点（SGSN）和网关通用分组业务支持节点（GGSN）组成。RNC 的主要功能是负责网络相关功能、无线资源管理、无线资源控制（RRC）的维护和运行，提供网管系统的接口等。RNC 的主要缺点是负责与空中接口相关的许多功能都在 RNC 中，导致资源分配和业务不能适配信道，协议结构过于复杂，不利于系统优化。2006 年 3 月，3GPP 决定 LTE 网络由 E-UTRAN 基站（eNB）和接入网关（AGW）组成，网络结构呈现扁平化。

E-UTRAN 的总体协议架构如图 3-36 所示，其中，AGW 是否被分为用户平面和控制平面还需要进一步研究；图中还给出了 E-UTRAN 的两个主要实体：eNB 和 AGW；图中也给出了各个实体在用户平面的主要功能。由于 MBMS（Multimedia Broadcast Multicast Service，多媒体广播组播业务）的特殊之处，关于 MBMS 与 E-UTRAN 的相关描述将在后面给出。

eNB 主要包含空中接口的 PHY、MAC、RLC、RRC 各层实体单元，可以实现资源调度及动态资源分配。eNB 主要功能有：① 无线资源管理功能，包括无线承载控制、无线接入控制、链路管理控制、UE 的上下行动态资源分配等；② IP 头压

缩及用户数据流加密；③ 移动性管理实体的选择；④ 寻呼消息的组织和发送；⑤ 路由用户面数据；⑥ 广播消息的组织和发送；⑦ 以移动性或调度为目的的测量及测量报告配置。

AGW 的主要功能有：产生寻呼信息、用户平面的数据加密、PDCP 执行与维护、LTE-IDLE 状态下的移动性管理和系统架构演进（SAE）承载控制等。

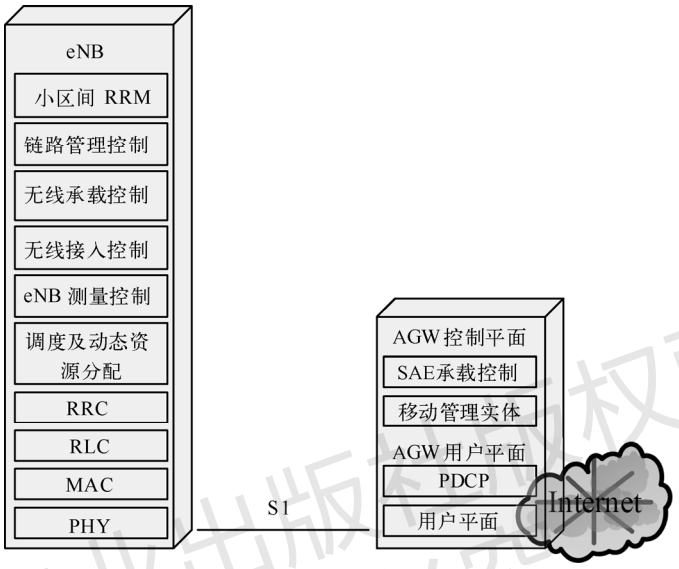

图 3-36　E-UTRAN 的总体协议架构

E-UTRAN 的协议栈结构从整体上主要进行了如下简化：

- 使用共享信道用于承载用户的控制信令和业务，取代了 R6 中的专用信道，减少传输信道个数，使多个用户共享空中接口的资源；
- 减少 MAC 层实体个数；
- 使用 MBMS 代替 BMC（Broadcast/Multicast Control，广播 / 组播控制）和 CTCH（Common Traffic Channel，公共业务信道）。
- 删除下行宏分集；
- 使用时隙统筹方案代替 UTRAN 的压缩模式；
- 简化无线资源控制（RRC）状态，删除了 CELL_FACH 状态，将 UTMS 中的 RRC 状态和 PMM 状态合并为一个状态集。

（1）用户平面协议栈结构

用户平面用于执行无线接入承载业务，主要负责处理用户发送和接收的所有信息。用户平面协议栈结构如图 3-37 所示，该图展示了 E-UTRAN 的用户平面协议栈结构，可以看出，其中包括了传统 UTRAN 中的各个子层，如分组数据汇聚协议（Packet Data Convergence Protocol，PDCP）子层、无线链路控制（RLC）子层、媒体访问控制（MAC）子层和物理层，只是位置稍有变化。在 E-UTRAN 中不采用传统的 RNC，采用 AGW 和 eNB 直连的方式实现用户面的快速接入。在这种接入方式下，各功能

体的功能也有了变化，RNC 功能在 E-UTRAN 中被分别分配到了 eNB 和 AGW 实体，其中 RLC 和 MAC 功能在 eNB 实现，而 PDCP 功能在 AGW 实体执行。

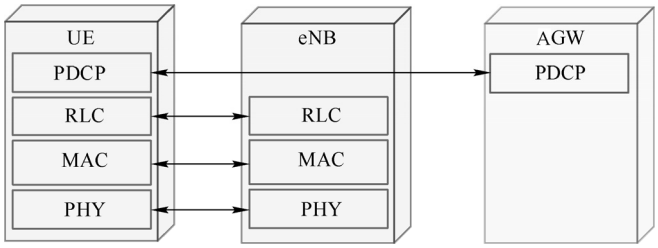

图 3-37　用户平面协议栈结构

LTE 中 MAC 层的主要功能有：逻辑信道和传输信道的映射、复用和解复用；数据量测量；HARQ 功能；UE 内的优先级调度和 UE 间的优先级调度；TF（传输格式）选择；RLC PDU（协议数据单元）的按序提交。

RLC 层支持的主要功能有：AM（确认模式）、UM（非确认模式）、TM（透明模式）数据传输；ARQ；数据切分（重切分）和重组（级联）；SDU（业务数据单元）的按序发送；数据的重复检测；协议错误检测和恢复；AGW 和 eNB 间的流量控制；SDU 丢弃。

PDCP（分组数据的报头压缩）层位于 UPE（User Plane Entity，用户面实体），主要任务是：报头压缩，只支持 ROHC 算法；用户面数据加密；下层 RLC 按序投递 SDU 时，PDCP 的重排缓冲（主要用于跨 eNB 切换）。

（2）控制平面协议栈结构

控制平面负责用户无线资源的管理、无线连接的建立、业务的 QoS 保证和资源释放，主要由 RRC 层和 NAS 层实现。这种结构简化了控制平面从睡眠状态到激活状态的过程，使得迁移时间相应减少。控制平面协议栈结构如图 3-38 所示，该图展示了 E-UTRAN 的控制平面协议栈结构，其中 RLC 和 MAC 层完成与用户平面内同样的功能。

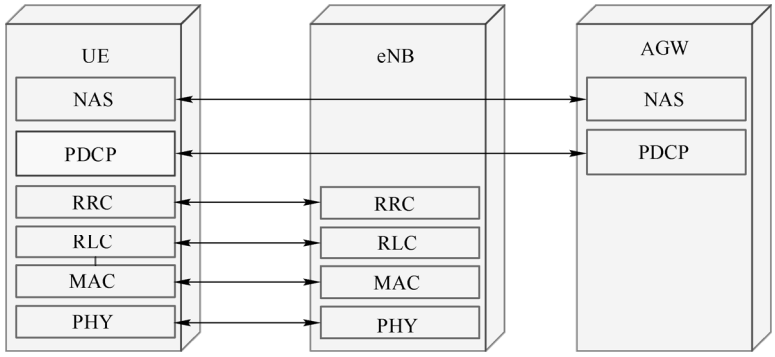

图 3-38　控制平面协议栈结构

在 E-UTRAN 的控制平面协议栈中，NAS 功能有：SAE 承载管理；鉴权；AGW