

第3章

ZigBee网络技术

3.1 ZigBee 概述

ZigBee 是 Zigzag 和 Bee 的合成词,这个合成词形象地表述了两个含义:其一是 ZigBee 就像蜜蜂一样,具有小巧而敏捷的无线感知功能;其二是 ZigBee 系统就像蜜蜂交换信息一样,能够通过蜿蜒曲折(Zigzag)的线路将数据传输到目的地,即 ZigBee 是一种采用多跳技术传输数据的通信方式。

虽然传感器和测控系统对数据传输速率的要求并不高,但是低成本和由于电池驱动所要求的低功耗是首要考虑的条件。在 ZigBee 规范出现之前,因为没有一个能够满足上述要求的技术标准,所以市场上出现的无线测控产品都是装配了厂商自己的协议,这种情况使产品的相互运用和新技术的引入遇到了许多障碍。

针对上述问题,全球性的无线传感器网络业界标准组织——ZigBee 联盟对无线传感器网络进行了标准化活动,制定了 ZigBee 规范。通常,ZigBee 就是指 ZigBee 无线传感器网络(ZigBee Wireless Sensor Networks,ZigBee WSN)。另外,因为 ZigBee 采用多跳方式传输数据,结点之间直接通信的距离(一跳距离)通常小于 100 米,即使是 Jennic 公司提供的高功率模块,在空旷区域内的实际的直接通信距离也小于 1000 米,所以 ZigBee 也是一种短距离通信规范。

ZigBee 规范是一个面向传感器及测控无线网络的国际标准化技术,这个规范能够满足如下四点要求。

(1) 低消耗功率:用无线方式取代感测信号线,并且不需要电源线。在低耗电待机模式下,两节 5 号干电池可支持一个结点工作 6~24 个月,甚至更长。这是 ZigBee 的突出优势。相比较,蓝牙能工作数周,Wi-Fi 可工作数小时。

(2) 低成本:不仅要求设备成本低,而且要求装配、维护等运营成本费也尽可能低。通过大幅简化协议(不到蓝牙的 1/10),降低了对通信控制器的要求,按预测分析,以 8051 的 8 位微控制器测算,全功能的主结点需要 32KB 代码,子功能结点少至 4KB 代码,而且 ZigBee 免协议专利费。每块芯片的价格大约为 2 美元。

(3) 网络容量大:ZigBee 可采用星状、片状和网状网络结构,由一个主结点管理若干子结点,最多一个主结点可管理 254 个子结点;同时主结点还可由上一层网络结点管理,最多可组成具有 65 000 个结点的大网。

(4) 相互接续性好：设想 ZigBee 产品可由多个厂商提供，可以采用多个厂商的设备构筑一个可以用简单的协议确保相互运用的网络。

在 ZigBee 联盟成员企业的努力下，2004 年 12 月发表了第一个 ZigBee 规范 (ZigBee v. 1.0 draft ratified)，此后，经过多次修改，于 2006 年 10 月发表了 ZigBee-2006 v. r13，一个月之后 (2006 年 11 月 9 日) 发表了 ZigBee-2007 v. r14。ZigBee-2007 v. r14 发表之后，又经过了多次勘误和改进，2006 年 12 月发表了 ZigBee-2007 v. r15，2007 年 5 月发表了 ZigBee-2007 v. r16，2007 年 10 月发表了 ZigBee-2007 v. r17。2009 年 3 月，ZigBee RF4CE 推出，具备更强的灵活性和远程控制能力。

在 ZigBee-2007 规范中包含 ZigBee 功能子集和 ZigBee PRO 功能子集两个子集的定义，这两个子集的主要功能如表 3-1 所示。由该表可见，两个子集的功能不尽相同。例如，ZigBee 功能子集支持 Mesh 网络及树状网络，ZigBee PRO 功能子集仅支持 Mesh 网络；ZigBee 功能子集中单个网络可以支持数百个结点，而 ZigBee PRO 功能子集中单个网络可以支持数千个结点。两个子集的设备在一定的条件下是可以相互运用的，具体表现如下：

(1) ZigBee 设备可以作为终端设备加入 PRO 网络，ZigBee PRO 设备也可以作为终端设备加入 ZigBee 网络。

(2) 在同一个网络的应用级，ZigBee 设备和 ZigBee PRO 设备完全可以相互运用。

(3) 在网络中使用标准的安全模式时，ZigBee 设备和 ZigBee PRO 设备完全可以相互运用。

表 3-1 ZigBee 功能子集和 ZigBee PRO 功能子集的主要特征及其差异

特 征	ZigBee 功能子集	ZigBee PRO 功能子集
单个网络支持的结点数	数百个	数千个
自组织网络的特征	支持 Mesh 网络和树状网络； 支持单播、广播及组播功能	仅支持 Mesh 网络； 支持网络层的多播功能； 强化了多对一通信功能及原路由功能
网络设备类型及管理	协调器、路由器、终端； 支持 PAN ID 冲突避免及频率敏捷选择的网络管理	
应用服务	设备及服务检测； 任选认知服务； 可选择的分割/重组服务； 支持应用消息标准定义类库； 在同一个网络内支持公共 Profile 和厂商独自の Profile 的混合适用	
安全性	网络及应用级的认证和加密； 使用 AES-128b 加密方式的对称密钥； 分层密钥：网络密钥和应用链路密钥	除具备 ZigBee 功能子集的标准安全性之外，还支持高级安全性
认证	平台合法性认证； 厂商产品认证； 公共 Profile 产品认证； 定期实施的相互运用性事件 (从 2003 年下半年开始，每两年实施一次)	

3.1.1 ZigBee 网络体系结构

ZigBee 的通信模型如图 3-1 所示,图中给出了 ZigBee 模型与国际标准化组织(International Organization for Standardization,ISO)提出的 OSI 参考模型(Open System Interconnection Basic Reference Model)的对应关系。根据网络功能,OSI 参考模型分为7层,其中 ZigBee 模型的第 1 和第 2 层对应于 OSI 参考模型的第 1 和第 2 层,在上面所述的各种 ZigBee 版本中都采用 IEEE 802.15.4-2003 通信标准(本书所讲到的 IEEE 802.15.4 专指 IEEE 802.15.4-2003);第 3 和第 4 层对应于 OSI 参考模型的第 3 层,第 4 层对应于 OSI 参考模型的第 4~第 7 层,采用 ZigBee 联盟制定的标准。与第 1 和第 2 层不同的是,对于不同的 ZigBee 版本其功能有所差异,即随着版本升级功能在不断优化,需要注意的是,虽然各个版本的基本功能差别不大,但是高版本不一定与低版本兼容,例如在 ZigBee v1.0 中支持键值对(Key Value Pair,KVP)和消息帧(Message,MSG)两种帧格式,而在 ZigBee-2006 之后的规范中只支持 MSG 帧结构。APL 层是由应用框架(Application Framework,AF)、ZigBee 设备对象(ZigBee Device Objects,ZDO)及应用支持子层(Application Support Sub-layer,APS 层)共同构成的。ZigBee 应用层与 OSI 参考模型中的应用层的定义不太一致,在 OSI 参考模型中,应用完全是由用户自己开发的,而 ZigBee 规范中给用户提供了许多应用接口。下面简要说明 ZigBee 通信模型中各层的功能。

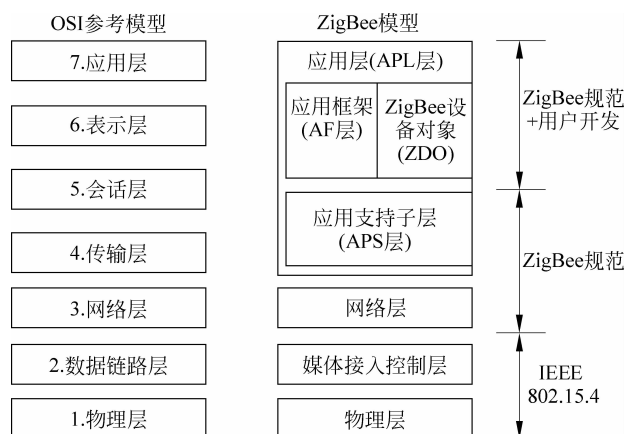


图 3-1 ZigBee 通信模型

1. 物理层

物理层(PHYsical layer,PHY)规定了无线通信中所需要采用的媒体,例如,采用的频率、信道、调制方式以及帧结构。

2. 媒体接入控制层

媒体接入控制层(Medium Access Control,MAC)规定了在电波直接到达范围内(一跳范围)的消息传输方法。例如,由于干扰电波等原因导致通信错误时,对错误进行检测、纠正、重发请求以及正确接收消息情况下的 ACK 应答等都属于 MAC 层的功能。

3. 网络层

网络层(Network,NWK)规定了网络管理、路由管理及网络内的消息传输方式。网络

管理是指通过建立网络、结点加入网络、网络地址分配等过程使网络结点相互认识的功能。路由管理是指在电波不能直接到达目标结点的情况下,需要由中继结点将消息进行转发,对能够可靠转发消息的路径进行选择和维护的功能。

4. 应用支持子层

应用支持子层 APS 虽然在网络层确定了结点之间的通信路径,但有时一个结点会承担多个应用。在这种情况下,就需要像 TCP port 那样,在多个应用之间建立逻辑通信路径。所以 APS 层的主要功能之一就是支持这种作为逻辑子信道的 Endpoint (3.5 节介绍 Endpoint 的详细定义)。另一个问题是,网络层能够传输的信息只是一定长度以下的二进制数据的有效载荷。因为用户的应用是多种多样的,所以要求传输的数据格式也各不相同。例如,如果应用只是监测环境温度,只需要传输温度数据;如果应用需要监测温度和湿度,就需要同时传输温度和湿度数据。因此,APS 层的第二个功能是将来自应用层的发送数据变换为网络层所要求的帧格式,或者将来自网络层的有效载荷数据变换为应用层能够理解的消息。并且,通信帧的收信确认和重发请求也是 APS 层的功能。

5. 应用层框架和 ZigBee 设备对象

如图 3-1 所示,ZigBee 应用层 (Application, APL) 是由应用框架 AF、ZigBee 设备对象 ZDO 以及 APS 层组合构成的。除了上面所述 APS 层的功能外,AF 为用户构建了应用骨架,用户可以根据需求在骨架内添加、改写或删除应用程序;ZDO 为用户提供了管理网络的接口,可以避免直接操作协议栈的底层带来的麻烦。换言之,ZigBee 应用层与 OSI 参考模型中的应用层不同,OSI 参考模型中的应用层完全由用户自己开发,而 ZigBee 应用层并非全部由用户自己开发,ZigBee 协议栈已经为用户提供了大量的应用接口。

3.1.2 ZigBee 设备类型

1. ZigBee 硬件与协议栈

一般来讲,嵌入式系统的装配方法有两种类型,其一是像半导体集成电路那样的硬件装配方法;其二是称为协议栈的微处理器程序软件的装配方法。半导体集成电路的开发成本高,但可以获得良好的性能。软件装配虽然难以获得像硬件那样的性能,但是灵活性强。因此,在能够保证性能要求的情况下,为了降低成本,用软件装配的方法是比较合理的。

IEEE 802.15.4 • ZigBee 的装配形态如图 3-2 所示。对于市场上出售的 IEEE 802.15.4 标准产品,其物理层的功能基本上都是由 CMOS 等硬件实现的,MAC 层的功能大都由半导体集成电路和协议栈共同分担。为了提高处理速度,MAC 层的前半部分装配集成电路,如 ACK 的自动发送、加密处理等。而网络层以上的各层,毫无例外地装配协议栈。因为微处理器中的程序被保存在闪存中,所以,程序所需容量也就是栈的大小对传感器网络产品的成本是极其重要的。除了用户应用程序之外,装配 IEEE 802.15.4 • ZigBee 的全部规范所需栈的大小总计约为 50KB 以上。其中,IEEE 802.15.4 的 MAC 层的库约占 20KB,剩余是 ZigBee 规范所需部分。为此,对于简单的 IEEE 802.15.4 • ZigBee 应用,可以采用内置 64KB 闪存的微处理器,当然,如果采用 128KB 闪存的微处理器,就具有较大的余量,能够实现复杂的应用。

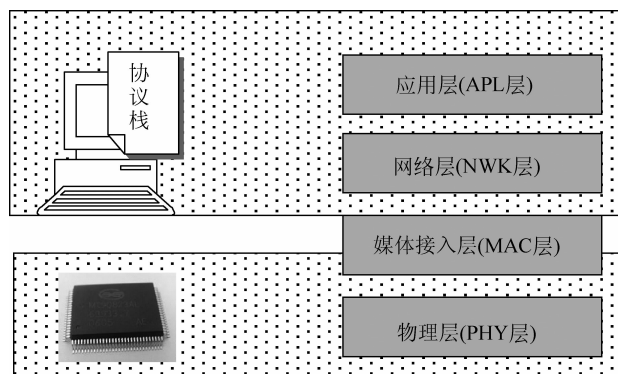


图 3-2 IEEE 802.15.4 • ZigBee 的装形态

上面从嵌入式系统的装配方法描述了硬件和协议栈的概念,然而,在 ZigBee 规范的文档中,将 PHY 层、MAC 层、NWK 层及 APL 层的集合称为协议栈,也就是说协议栈包含了硬件(PHY 和 MAC 层的前半部分)和软件两大部分。ZigBee 规范中定义的协议栈结构如图 3-3 所示。对于构成协议栈的每一层,不论其构建形态是硬件还是软件都是实现某些特定功能的实体,并且,每一层又可从功能上分为数据实体和管理实体。数据实体完成数据传

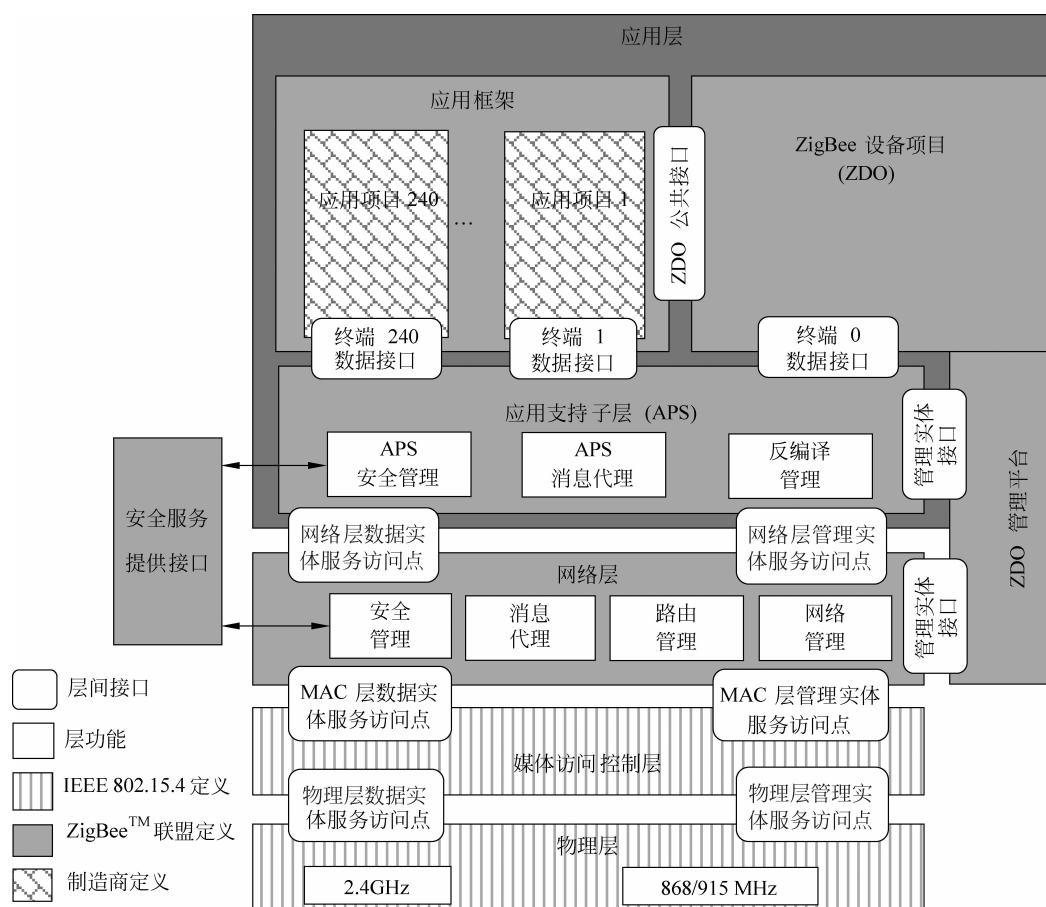


图 3-3 ZigBee 协议栈结构

输服务,管理实体完成空闲信道判定、电场能量测量、网络建立、结点入网等数据传输之外的其他服务。相邻层之间通过称为服务接入点(Service Access Point,SAP)的接口进行信息交换,进一步讲,每个 SAP 支持实现某种功能的若干原语(Primitive),相邻层之间使用原语交换信息。表 3-2 给出了协议栈中各种 SAP 的说明。

表 3-2 服务接入点的意义

服务接入点名称	意 义
PD-SAP: PHY Data Entity-Service Access Point	物理层数据实体服务接入点
PLME-SAP: Physical Layer Management Entity-Service Access Point	物理层管理实体服务接入点
MLDE-SAP: Medium Access Control Sub-Layer Data Entity-Service Access Point	媒体接入控制子层数据实体服务接入点
MLME-SAP: Medium Access Control Sub-Layer Management Entity-Service Access Point	媒体接入控制子层管理实体服务接入点
NLDE-SAP: NWK Layer Data Entity-Service Access Point	网络层数据实体服务接入点
NLME-SAP: NWK Layer Management Entity-Service Access Point	网络层管理实体服务接入点
APSD-SAP: APS Sub-Layer Data Entity-Service Access Point	应用支持子层数据实体服务接入点
APSME-SAP: APS Management Entity-Service Access Point	应用支持子层管理实体服务接入点

2. 逻辑设备类型和物理设备类型

1) 逻辑设备类型

在 IEEE 802.15.4 标准中,根据功能的不同,把逻辑设备分别定义为个域网(PAN)、协调器(Coordinator)及网络设备(Network Device)三种类型。而在 ZigBee 规范中,名称略有不同,分别称为 ZigBee 协调器(ZigBee Coordinator)、ZigBee 路由器(ZigBee Router)以及 ZigBee 终端设备(ZigBee End Device)三种类型(见表 3-3)。在本书中采用 ZigBee 规范中采用的名称。

表 3-3 逻辑设备分类

IEEE 802.15.4 的名称	PAN Coordinator	Coordinator	Network Device
ZigBee 名称	ZigBee Coordinator	ZigBee Router	ZigBee End Device
网络的启动功能	有	无	无
路由功能	有	有	无
信标发布	可能	可能	不可
管理范围	所有结点	自己的子结点	自己
可能的结点数	只有一个	可有多个	可有多个
功率消耗	大	大	小
要求的微处理器的资源	大	中	小

2) 物理设备类型

为了提供低成本的无线传感器网络设备,IEEE 802.15.4 定义了全功能设备(Full-

Function Device, FFD) 和功能限定设备 (Reduced-Function Device, RFD) 两种物理设备类型。FFD 和 RFD 的最大差别在于有无路由功能。具有路由功能的 FFD 能够作为星状网、网状网 (Mesh Network) 等拓扑结构中的设备, 可以用于所有的逻辑设备。而对于低成本的 RFD, 因为没有路由功能只能和父结点通信, 所以只能作为终端设备使用。FFD 和 RFD 的差别见表 3-4。表 3-4 中给出了 MAC 层栈的尺寸, 它是 ZigBee 公开的预想的所需大小。实际上, 由于程序代码的优劣、微处理器的类型及编译器的性能, 得到的协议栈的大小也不相同。

表 3-4 物理设备类型

项 目	FFD	RFD
路由功能	有	无
Coordinator	可以	不可
Router	可以	不可
End Device	可以	可以
成本	略高	低
MAC 层的大小	16~20KB	12~16KB

3.1.3 原语

如 3.1.1 节所述, ZigBee 通信模型是一种分层结构, 低层为相邻高层提供服务。例如, 物理层为 MAC 层提供服务, MAC 层为 NWK 层提供服务……为了表述网络中各层提供服务的接口, IEEE 802.2 LAN/MAN 标准委员会提出了原语 (Primitive) 的概念。对所有的服务, 在相当于客户机的服务请求端和相当于服务器的服务提供端之间通过原语传递信息。

根据不同的目的, 把原语分为请求 (Request) 原语、通知 (Indication) 原语、应答 (Response) 原语及确认 (Confirm) 原语, 这些原语的类型及说明如表 3-5 所示。但是, 并非所有的服务中都需要 4 种原语, 有时只使用部分原语。

表 3-5 原语的类型及说明

原 语	原语装配端	方 向	目 的
Request	服务请求端	上层→服务层	服务请求
Confirm	服务请求端	服务层→上层	服务结果确认
Indication	服务提供端	服务层→上层	服务要求通知
Response	服务提供端	上层→服务层	对服务要求的响应

图 3-4 给出了原语的概念, 原语按照如下的步骤实现服务。

(1) 由服务请求端的上层向服务层发布服务请求原语, 要求提供服务。服务层将该请求继续传输给下层。当服务层是最下层的物理层时, 用电波发送请求消息, 向服务提供端提出服务请求。

(2) 服务请求端明确了服务执行结果时, 作为确认服务结果的原语, 传输到上层。

(3) 服务提供端接收到来自下层的请求时, 将该请求作为通知原语, 向上层发送通

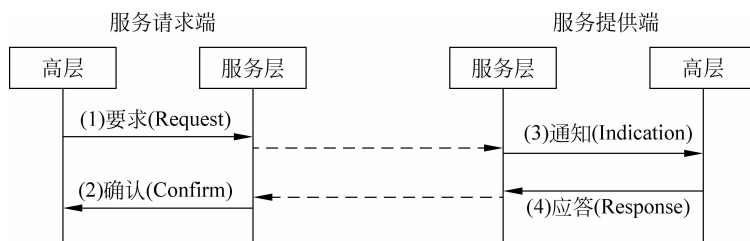


图 3-4 原语的概念

知。一般情况下,通知是以回调(Callback)的形式发生事件并向上层传输。

(4) 服务提供端的上层将被请求的服务的结果作为响应原语,返回给下层。当下层是物理层时,以电波发送结果给服务请求端。

在 IEEE 802.15.4 和 ZigBee 规范中,原语采用规定的格式表示。下面给出两个原语的例子,对于其他原语虽然功能不同,但表示格式是相同的。

例 1 物理层的数据通信请求原语。

```
PD - DATA.request (
psduLength,           //物理层数据有效载荷的长度
psdu                   //物理层数据有效载荷
)
```

例 2 结点加入网络的确认原语。

```
NLME - JOIN.confirm {
Status,                //结点入网请求的状态
NetworkAddress,        //网络地址
ExtendedPANID,         //IEEE PAN ID
ActiveChannel           //加入网络的信道
}
```

在上面给出的两个例子中,由大写字母组成的字符串表示原语的基本含义。如 PD-DATA 表示物理层数据通信, NLME-LEAVE 表示网络层的结点离网。由小写字母组成的字符串表示原语的类型。如 Request 表示请求原语, Confirm 表示确认原语。括号内的字符串表示原语使用的参数。由上面两个例子可以看出,在 IEEE 802.15.4 规范和 ZigBee 规范中,表示原语的格式略有不同,即 IEEE 802.15.4 使用圆括号,而 ZigBee 规范使用花括号。

原语描述了相邻层之间的接口关系,就像 API (Application Programming Interface)。但是,它并不是实际的软件接口,而仅仅是规定了必要的功能。在实际的协议栈或软件设计中,需要根据原语规定的功能编写实现相关功能的程序代码。

3.2 物理层

IEEE 802.15.4 物理层规定了无线电波的传输方式,提供了通信信道的电场强度检测、通信信道的频率设置、收发信功能的开始和结束、空闲信道判断、基本通信帧的收发信状态设置以及通信链路的质量测量等功能。

3.2.1 通信频带和信道

频率是不可再生的有限资源,移动通信、卫星通信、电视广播等通信系统占用的频带是由无线电管理部门统一分配的,并且必须付费。但是,世界各国都根据本国的具体情况预留了一些供工业、科学及医学应用的免费频段,即 ISM(Industrial Scientific Medical)频段。使用这些频段时,不需要付费也申请。在 IEEE 802.15.4 标准中采用表 3-6 所示的 3 个频段,共 27 个信道。我国使用 2.4GHz 免费频段的 16 个信道,其中心频率如表 3-7 所示。2.4GHz 频段的 IEEE 802.15.4 物理层的其他主要参数如表 3-8 所示。

表 3-6 IEEE 802.15.4 的频段和信道

频 段	信 道 数	调 制 方 式	数据速率/kb/s	可 用 区 域
868MHz	1	BPSK	20	欧洲
9.5MHz	10	BPSK	40	北美、南美
2.4GHz	16	O-QPSK	250	全球通用

表 3-7 2.4GHz 频段的 IEEE 802.15.4 的信道

信 道	中心频率/MHz	信 道	中心频率/MHz
11	2405	19	2445
12	2410	20	2450
13	2415	21	2455
14	2420	22	2460
15	2425	23	2465
16	2430	24	2470
17	2435	25	2475
18	2440	26	2480

表 3-8 2.4GHz 频段的 IEEE 802.15.4 物理层参数

参 数	规 定 值	说 明
数据速率	250kb/s	理论上的最高数据传输速率
符号速率	62.5ksymbol/s	扩散前的调制信号速率
码片速率	2Msymbol/s	扩散后的调制信号速率
PN 序列长度	32 码片	扩散因子
发送功率	大于-3dBm	
接收灵敏度	小于-85dBm	正确接收信号所需要的最小场强,是一个与通信距离及 RF 电路的性能密切相关的重要参数

注: Bluetooth(IEEE 802.15.1)的最小接收灵敏度为-70dBm; 无线 LAN(IEEE 802.11b)的最小接收灵敏度为-76dBm; 手机的接收灵敏度为-110dBm。

3.2.2 调制方式和频谱扩散

在 IEEE 802.15.4 物理层,数据调制采用 O-QPSK(Offset Quadrature Phase Shift Keying)调制方式; 频谱扩散采用直接序列扩频(Direct Sequence Spread Spectrum, DSSS)方式。扩频时采用的 16 个 PN 序列如表 3-9 所示,表中的 16 个 PN 序列几乎互不相关,序

列之间存在如下关系：

(1) PN 序列(0)~(7)或(8)~(15)中,后一序列是由前一序列循环右移 4 位生成的,如图 3-5(a)所示。

(2) 将序列(0)~(7)中的偶数码片反转(0→1,1→0)分别得到(8)~(15)中的码片序列,如图 3-5(b)所示,将 PN 序列(0)中的偶数码片 C1,C3,...,C31 反转后,得到 PN 序列(8)。

表 3-9 IEEE 802.15.4 可用的 16 种 PN 码

b(b0, b1, b2, b3)	符号(十进制)	符号序列(C0, C1, ..., C31)
0000	0	11011001110000110101001000101110
1000	1	11101101100111000011010100100010
0100	2	00101110110110011100001101010010
1100	3	00100010111011011001110000110101
0010	4	01010010001011101101100111000011
1010	5	00110101001000101110110110011100
0110	6	11000011010100100010111011011001
1110	7	10011100001101010010001011101101
0001	8	10001100100101100000011101111011
1001	9	10111000110010010110000001110111
0101	10	011110111100011001001011000000111
1101	11	01110111101110001100100101100000
0011	12	00000111011110111000110010010110
1011	13	01100000011101111011100011001001
0111	14	10010110000001110111101110001100
1111	15	11001001011000000111011110111000

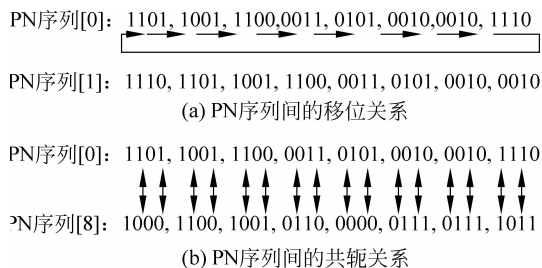


图 3-5 PN 序列的相互关系

3.2.3 物理层服务

如第 2 章所述,IEEE 802.15.4 和 ZigBee 规范中低层要为其相邻的高层提供数据服务和管理服务功能,本节简要介绍物理层提供的两种服务。

1. 物理层数据服务

在 IEEE 802.15.4 物理层的数据服务 PD-DATA(Physical layer Data-DATA)中,具有请求、确认及通知原语,没有应答原语,如表 3-10 所示。