第 3 章 CHAPTER 3 ZigBee无线传感器网络通信标准

3.1 ZigBee 标准概述

ZigBee 技术在 IEEE 802.15.4 的推动下，不仅在工业、农业、军事、环境、医疗等传统领域取得了成功的应用，在未来其应用可能涉及人类日常生活和社会生产活动的所有领域，真正实现无处不在的网络。ZigBee 技术是一组基于 IEEE 802.15.4 无线标准研制开发的，有关组网、安全和应用软件方面的技术标准，无线个人局域网工作组 IEEE 802.15.4 技术标准是 ZigBee 技术的基础，ZigBee 技术建立在 IEEE 802.15.4 标准之上，IEEE 802.15.4 只处理低级 MAC 层和物理层协议，ZigBee 联盟对其网络层协议和 API 进行了标准化。

ZigBee 技术是一种近距离、低复杂度、低功耗、低速率、低成本的双向无线通信技术，主要用于距离短、功耗低且传输速率不高的各种电子设备之间进行数据传输以及典型的有周期性数据、间歇性数据和低反应时间数据传输的应用，因此非常适用于家电和小型电子设备的无线控制指令传输。其典型的传输数据类型有周期性数据（如传感器）、间歇性数据（如照明控制）和重复低反应时间数据（如鼠标）。其目标功能是自动化控制。它采用跳频技术，使用的频段分别为 2.4GHz（ISM），868MHz（欧洲）及 915MHz（美国），而且均为免执照频段，有效覆盖范围为 10～275m。当网络速率降低到 28kb/s 时，传输范围可以扩大到 334m，具有更高的可靠性。

ZigBee 标准是一种新兴的短距离无线网络通信技术，它是基于 IEEE 802.15.4 协议栈，主要是针对低速率的通信网络设计的。它功耗低，是最具有可能应用在工控场合的无线方式。它和 2.4GHz 频带提供的数据传输速率为 250kb/s，915MHz 频带提供的数据传输速率为 40kb/s，而 868MHz 频带提供的数据传输速率为 20kb/s。另外，它可与 254 个包括仪器和家庭自动化应用设备的节点联网。它本身的特点使得其在工业监控、传感器网络、家庭监控、安全系统等领域有很大的发展空间。ZigBee 体系结构如图 3.1 所示。

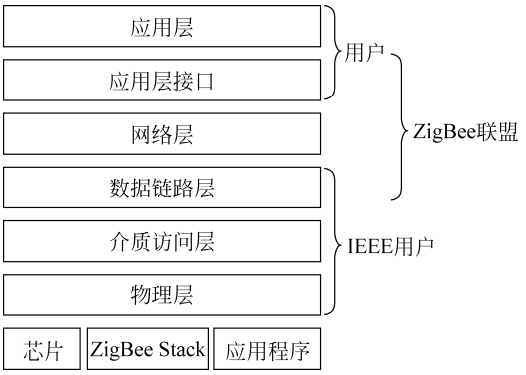

图 3.1　ZigBee 体系结构图

3.2　ZigBee 技术特点

ZigBee 是一种无线连接，可工作在 2.4GHz（全球流行）、868MHz（欧洲流行）和 915MHz（美国流行）三个频段上，分别具有最高 250kb/s、20kb/s 和 40kb/s 的传输速率，它的传输距离在 10～75m 的范围内，但可以继续增加。作为一种无线通信技术，ZigBee 自身的技术优势主要表现在以下几个方面。

1．功耗低

ZigBee 网络节点设备工作周期较短、收发数据信息功耗低，且使用了休眠模式（当不需接收数据时处于休眠状态，当需要接收数据时由“协调器”唤醒它们），因此，ZigBee 技术特别省电，据估算，ZigBee 设备仅靠两节 5 号电池就可以维持长达 6 个月到两年左右的使用时间，这是其他无线设备望尘莫及的，避免了频繁更换电池或充电，从而减轻了网络维护的负担。

2．成本低

由于 ZigBee 协议栈设计非常简单，所以其研发和生产成本较低。普通网络节点硬件只需 8 位微处理器，4～32KB 的 ROM，且软件实现也很简单。随着产品产业化，ZigBee 通信模块价格预计能降到 10 元人民币，并且 ZigBee 协议是免专利费的。低成本对于 ZigBee 也是一个关键的因素。

3．可靠性高

由于采用了碰撞避免机制并且为需要固定带宽的通信业务预留了专用时隙，避免了收发数据时的竞争和冲突，且 MAC 层采用完全确认的数据传输机制，每个发送的数据包都必须等待接收方的确认信息，所以从根本上保证了数据传输的可靠性。如果传输过程中出现问题可以进行重发。

4．容量大

一个 ZigBee 网络最多可以容纳 254 个从设备和 1 个主设备，一个区域内最多可以同时存在 100 个 ZigBee 网络，而且网络组成灵活。

5．时延小

ZigBee 技术与蓝牙技术的时延相比，其各项指标值都非常小。通信时延和从休眠状态激活的时延都非常短，典型的搜索设备时延 30ms，而蓝牙为 3～10s。休眠激活的时延是15ms，活动设备信道接入的时延为 15ms。因此 ZigBee 技术适用于对时延要求苛刻的无线控制（如工业控制场合等）应用。

6．安全性好

ZigBee 技术提高了数据完整性检查和鉴权功能，加密算法使用 AES-128，且各应用可以灵活地确定安全属性，从而使网络安全能够得到有效的保障。

7．有效范围小

有效覆盖范围在 10～75m 之间，具体依据实际发射功率的大小和各种不同的应用模式而定，基本上能够覆盖普通的家庭或办公室环境。

8．兼容性

ZigBee 技术与现有的控制网络标准无缝集成。通过网络协调器自动建立网络，采用载波侦听 / 冲突检测（CSMACA）方式进行信道接入。为了可靠传递，还提供全握手协议。

ZigBee 具有广阔的应用前景。ZigBee 联盟预言在未来的 4 到 5 年，每个家庭将拥有 50 个 ZigBee 器件，最后将达到每个家庭 150 个。据估计，ZigBee 市场价值将超过数亿美元/年。其应用领域如图 3.2 所示。

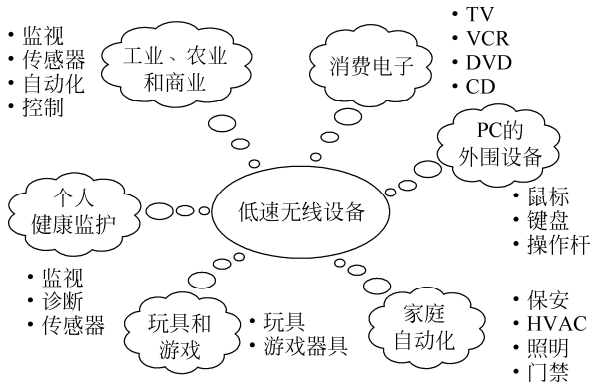

图 3.2　ZigBee 的应用场合

（1）家庭和楼宇网络。通过ZigBee网络，可以远程控制家里的电器、门窗等；可以方便地实现水、电、气三表的远程自动抄表；通过一个ZigBee遥控器，控制所有的家电节点。未来的家庭将会有50～100个支持ZigBee的芯片安装在电灯开关、烟火检测器、抄表系统、无线报警、安保系统、HVAC、厨房机械中，为实现远程控制服务。

（2）工业控制。在工业自动化领域，利用传感器和 ZigBee 网络，使得数据的自动采集、分析和处理变得更加容易，可以作为决策辅助系统的重要组成部分。例如，危险化学成分的检测、火警的早期检测和预报、高速旋转机器的检测和维护等。

（3）公共场所。例如，烟雾探测器等。

（4）农业控制。传统农业主要使用孤立的、没有通信能力的机械设备，主要依靠人力

监测作物的生长状况。采用了传感器和 ZigBee 网络后，农业将可以逐渐地向以信息和软件为中心的生产模式转化，使用更多的自动化、网络化、智能化和远程控制的设备来耕种。传感器可以收集包括土壤湿度、氮浓度、pH 值、降水量、温湿度和气压等信息。这些信息和采集信息的地理位置经由 ZigBee 网络传递到中央控制设备供农民决策和参考，这样就能够及早而准确地发现问题，从而有助于保持并提高农作物的产量。

（5）医疗。借助于各种传感器和 ZigBee 网络，准确且实时地监测病人的血压、体温和心跳速度等信息，从而减少医生查房的工作负担，有助于医生作出快速的反应，特别是对重病和病危患者的监护治疗。老人与行动不便者的紧急呼叫器和医疗传感器等。

（6）商业。例如智慧型标签等。

3.3　ZigBee 协议框架

ZigBee 堆栈是在 IEEE 802.15.4 标准基础上建立的，定义了协议的 MAC 和 PHY 层。ZigBee 设备应该包括 IEEE 802.15.4（该标准定义了 RF 射频以及与相邻设备之间的通信）的 PHY 和 MAC 层，以及 ZigBee 堆栈层：网络层（NWK）、应用层和安全服务提供层。

完整的 ZigBee 协议栈由物理层、介质访问控制层、网络层、安全层和高层应用规范组成，如图 3.3 所示。

图 3.3　ZigBee 协议栈

ZigBee 协议栈的网络层、安全层和应用程序接口等由 ZigBee 联盟制定。物理层和 MAC 层由 IEEE 802.15.4 标准定义。在 MAC 子层上面提供与上层的接口，可以直接与网络层连接，或者通过中间子层 SSCS 和 LLC 实现连接。ZigBee 联盟在 802.15.4 基础上定义了网络层和应用层。其中，安全层主要实现密钥管理、存取等功能。应用程序接口负责向用户提供简单的应用软件接口（API），包括应用子层支持（Application Sub-layer Support，APS）、ZigBee 设备对象（ZigBee Device Object，ZDO）等，实现应用层对设备的管理。

3.4　ZigBee 网络层规范

1．网络层参考模型及实现

网络层主要实现节点加入、离开、路由查找和传送数据等功能。目前 ZigBee 网络层主

要支持两种路由算法，即树路由（Cluster-Tree）和网状网路由。支持星状（Star）、树状（Cluster-Tree）、网格（Mesh）等多种拓扑结构，如图 3.4 所示。

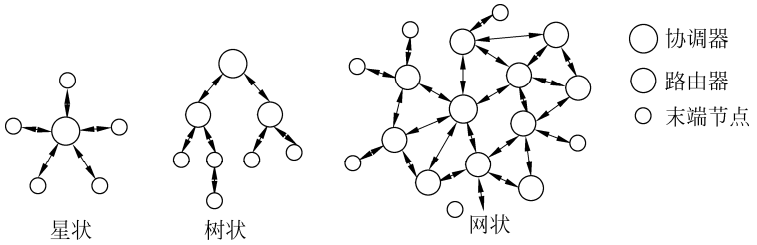

图 3.4　ZigBee 组网拓扑结构

在这些拓扑结构中一般包括三种设备：协调器、路由器和末端节点。

协调器也称为全功能设备（Full-Function Device，FFD），相当于蜂群结构中的蜂后，是唯一的，是 ZigBee 网络启动或建立网络的设备。一旦网络建立，该协调器就如同一个路由器，在网络中提供数据交换，建立安全机制，建立网络中绑定等路由功能。网络中的其他操作并不依赖该协调器，因为 ZigBee 网络是分布式网络。路由器相当于雄蜂，数目不多，需要一直处于工作状态，需要主干线供电。但在树状拓扑网络模式中，允许路由器周期地运行操作，所以可以采用电池供电。路由器的功能主要包括作为普通设备加入网络，实现多跳路由，辅助其他的子节点完成通信。末端节点则相当于数量最多的工蜂，也称为精简功能设备（Reduced-Function Device，RFD），只能传送数据给 FFD 或从 FFD 接收数据，该设备需要的内存较少（特别是内部 RAM）。为了维持网络最基本的运行，末端节点没有指定的责任，没有必不可缺少性，可以根据自己的功能需要休眠或唤醒，一般可由电池供电。树路由把整个网络看作是以协调器为根的一棵树，树状路由不需要路由表，节省存储资源，缺点是不灵活，浪费了大量的地址空间，路由效率低。网状网的路由算法是无线自组网按需平面距离矢量路由算法（Ad Hoc On-Demand Distance Vector Routing，AODV）的一个简化版本。在 AODV 中，一个网络节点要建立连接时才广播一个连接建立的请求，其他的 AODV 节点转发这个请求消息，并记录源节点和回到源节点的临时路由。当接收连接请求的节点知道到达目的节点的路由时，就把这个路由信息按照先前记录的回到源节点的临时路由发回源节点。源节点和目的节点之间使用这个经由其他节点并且有最短跳数的路由进行数据传输。当链路断掉，路由错误回送源节点，源节点就重新发起路由查找的过程。它可以用于较大规模的网络，需要节点维护一个路由表，耗费一定的存储资源，但往往能达到最优的路由效率，而且使用灵活。

除了这几种路由方法，ZigBee 还可以进行邻居表路由，其实邻居表可以看作是特殊的路由表，只不过只需要一跳就可以发送到目的节点。

2．网络层规范概述

ZigBee 协议栈的核心部分在网络层。网络层负责拓扑结构的建立和维护、命名和绑定服务，它们协同完成寻址、路由、传送数据及安全这些不可或缺的任务，支持星状（Star）、树状（Cluster-Tree）、网格（Mesh）等多种拓扑结构。为了满足应用层的要求，ZigBee 协议的网络层划分为网络层数据实体（NLDE）和网络层管理实体（NLME），NLDE 提供相

关的 SAP 的数据传输服务，而 NLME 则提供经由相关的 SAP 的管理服务。

网络层必须从功能上为 MAC 子层提供支持，并为应用层提供合适的服务接口。为了实现与应用层的接口，网络层从逻辑上分为两个具有不同功能的服务实体，即数据实体（NLDE）和管理实体（NLME）。数据实体通过和它相连的 NLDE-SAP 服务存取点提供数据管理服务；而网络层管理实体（NLME）则通过和它相连的 NLME-SAP 服务存取点提供管理服务。NLME 使用 NLDE 完成一些管理任务，并维护一个被称作网络信息中心（NIB）的数据库对象。

NLDE 提供如下服务：

（1）产生网络层协议数据单元（NPDU）。

（2）提供基于拓扑结构的路由策略。

NLME 提供如下服务：

（1）配置新设备。

（2）建立网络。

（3）加入和离开网络。

（4）寻址。

（5）邻居发现。

（6）路由发现。

（7）接收控制。

3．网络层服务规范

网络层提供了两种服务，可以通过两个服务存取点（SAP）分别进行访问。这两个服务是网络层数据服务和网络层管理服务。前者可以通过网络层数据实体服务存取点（NLDE-SAP）进行访问，后者则可以通过网络层管理服务实体服务存取点（NLME-SAP）进行访问。这两个服务与 MCPS-SAP 和 MLME-SAP 一起组成了应用层和 MAC 子层间的接口。除了这些外部接口，在网络层内部，NLME 和 NLDE 之间也存在一个接口，NLME 可以通过它访问网络层的数据服务。

4．网络层帧结构

网络层的帧是由网络层帧头和网络负载组成的。帧头部分域的顺序是固定的，但是根据具体情况，其他所有域不一定必须包含，如图 3.5 所示。

<table>
<tr><td>8B</td><td>2</td><td>2</td><td>1</td><td>1</td><td>变长</td></tr>
<tr><td rowspan="2">帧控制域</td><td>目标地址</td><td>源地址</td><td>半径</td><td>序列号</td><td>帧负载</td></tr>
<tr><td colspan="4">路由域</td><td></td></tr>
<tr><td colspan="5">帧头</td><td>网络负载</td></tr>
</table>

图 3.5　ZigBee 网络层帧结构

网络层定义了数据帧和命令帧，它的帧结构由网络层头信息和数据负载构成。网络层通用帧结构如图 3.5 所示。网络层帧头信息格式是固定的，帧控制 2B，目的地址 2B，源地址 2B，网络传输的半径 1B，但是地址域和序列号域并非在所有的帧结构中都出现。网络

层数据域 *n*B。其中目的地址、源地址、半径和序列统称为路由域。网络层数据帧和命令帧的区别在于命令的数据域有 1B 的 NWK 命令标识符。

5．网络层功能

网络层负责拓扑结构的建立和维护网络连接，主要功能包括设备连接和断开网络时所采用的机制，以及在帧信息传输过程中所采用的安全性机制。此外，还包括设备的路由发现和路由维护及转交。并且，网络层完成对一跳（one-hop）邻居设备的发现和相关节点信息的存储。一个 ZigBee 协议器创建一个新网络，为新加入的设备分配短地址等。并且，网络层还提供一些必要的函数，确保 ZigBee 的 MAC 层正常工作，并且为应用层提供合适的服务接口。

网络层的主要功能包括以下 8 个方面：

（1）通过添加恰当的协议头能够从应用层生成网络层的 PDU，即 NPDU。

（2）确定网络的拓扑结构。

（3）配置一个新的设备，可以是网络协调器，也可以向存在的网络中加入设备。

（4）建立并启动无线网络。

（5）加入或离开网络。

（6）ZigBee 的协调器和路由能为加入网络的设备分配地址。

（7）发现并记录邻居表、路由表。

（8）信息的接收控制，同步 MAC 子层或直接接收信息。

3.5 ZigBee 应用层规范

ZigBee 协议栈的层结构包括 IEEE 802.15.4 媒体接入控制层（MAC）和物理层（PHY），以及 ZigBee 网络层。每一层通过提供特定的服务完成相应的功能。其中，ZigBee 应用层包括 APS 子层、ZDO（包括 ZDO 管理层）以及用户自定义的应用对象。APS 子层的任务包括维护绑定表和绑定设备间的消息传输。所谓的绑定指的是根据两个设备所提供的服务和它们的需求而将两个设备关联起来。ZDO 的任务包括界定设备在网络中的作用，发现网络中的设备并检查它们能够提供哪些应用服务，产生或者回应绑定请求，并在网络设备间建立安全的通信。

ZigBee 应用层有三个组成部分，包括应用支持子层（Application Support Sub-Layer，APS）、应用框架（Application Framework，AF）、ZigBee 设备对象（ZigBee Device Object，ZDO）。它们共同为各应用开发者提供统一的接口，规定了与应用相关的功能，如端点（Endpoint）的规定，绑定（Binding）、服务发现和设备发现等。

1．应用支持子层

APS 主要作用包括：协议数据单元 APDU 的处理，APSDE 提供在同一个网络中的应用实体之间的数据传输机制，APSME 提供多种服务给应用对象，并维护管理对象的数据库。

APS 是网络层（NWK）和应用层（APL）之间的接口。该接口包括一系列可以被 ZDO 和用户自定义应用对象调用的服务。这些服务由两个实体提供：APS 数据实体（APSDE）

通过 APSDE 服务接入点（APSDE-SAP），APS 管理实体（APSME）通过 APSME 服务接入点（APSME-SAP）。APSDE 在同一个网络中的两个和多个设备提供传输应用 PDU 的数据传输服务。APSME 提供设备发现和设备绑定服务，并维护一个管理对象的数据库，也就是 APS 信息库（AIB）。

2．应用框架

在 ZigBee 应用中，应用框架提供了两种标准服务类型。一种是键值对（Key Value Pair，KVP）服务类型，另一种是报文（message，MSG）服务类型。KVP 服务用于传输规范所定义的特殊数据。它定义了属性（attribute）、属性值（value）以及用于 KVP 操作的命令：Set、Get、Event。其中，Set 用于设置一个属性值；Get 用于获取一个属性值；Event 用于通知一个属性已经发生改变。KVP 消息主要用于传输一些较为简单的变量格式。由于 ZigBee 的很多应用领域中的消息较为复杂，并不适用于 KVP 格式，因此 ZigBee 协议规范定义了 MSG 服务类型。MSG 服务对数据格式不作要求，适合任何格式的数据传输。因此可以用于传送数据量大的消息。

应用框架AF为每个应用对象提供了键值对（KVP）服务和报文（MSG）服务。KVP命令帧的格式如图3.6所示。MSG命令帧格式如图3.7所示。

位：4	4	16	0/8	可变
命令类型标识符	属性数据类型	属性标识符	错误代码	属性数据

图 3.6 KVP 命令帧的格式

位：8	可变
事务长度	事务数据

图 3.7 MSG命令帧格式

3．ZigBee设备对象

ZDO 实际上是介于应用层端点和应用支持子层中间的端点，其主要功能集中在网络管理和维护上。应用层的端点可以通过 ZDO 提供的功能来获取网络或者是其他节点的信息，包括网络的拓扑结构、其他节点的网络地址和状态以及其他节点的类型和提供的服务等信息。

端点是应用对象存在的地方，ZigBee 允许多个应用同时位于一个节点上，ZigBee 定义了几种描述符，对设备以及提供的服务进行描述，可以通过这些描述符来寻找合适的服务或者设备。

此外，ZigBee 协议栈还提供了安全组件，如采用了 AES128 的算法对网络层和应用层的数据进行加密保护；设立信任中心的角色，用于管理密钥和管理设备，可以执行设置的安全策略。

从以上分析可知，ZigBee 协议套件简单紧凑，因而与之兼容的硬件要求也比较简单，8 位微处理器 80C51 就可以满足要求，全功能协议软件需要 32KB 的 ROM，最小功能协议软件需求大约 4KB 的 ROM。目前，飞思卡尔、得州仪器 TI 等国际巨头已推出了比较成熟的 ZigBee 开发平台，如 TI 推出基于 CC2420 收发器和 TI MSP430 超低功耗单片机的平台，

CC2430 的 SOC 平台 C51RF-3-PK 等。

ZigBee 设备配置层提供标准的 ZigBee 配置服务，它定义和处理描述符请求。在 ZigBee 设备配置层中定义了称为 ZigBee 设备对象的特殊软件对象，在其他服务中提供绑定服务。远程设备可以通过 ZDO 接口请求任何标准的描述符信息。当接收到这些请求时，ZDO 会调用配置对象以获取相应的描述符值。在目前的 ZigBee 协议版本中，还没有完全实现设备配置层。ZDO 是特殊的应用对象，它在端点（end-point）0 上实现。

3.6 ZigBee 安全服务规范

ZigBee 设备之间的通信使用 IEEE 802.15.4 无线标准，该标准指定物理层（PHY）和媒介存取控制层（MAC）两层规范。而 ZigBee 规范了网络层（NWK）和应用层（APL）标准，各层规范功能分别如下。

PHY：提供基本的物理无线通信能力。

MAC：提供设备间的可靠性授权和一跳通信连接服务。

NWK：提供用于构建不同网络拓扑结构的路由和多跳功能。

APL：包括一个应用支持子层、ZigBee 设备对象和应用。

在安全服务规范方面，协议栈分别在 MAC、NWK 和 APS 三层具有安全机制，保证各层数据帧的安全传输。同时，APS 提供建立和保持安全关系的服务。ZDO 管理安全性策略和设备的安全性结构。