第3章 无线传感器网络中的无线通信技术

3.1 IEEE 802.15.4 标准概述

IEEE 802.15.4 标准是针对低速无线个人区域网络(Low-Rate Wireless Personal Area Network,LR-WPAN)制定的。该标准把低能量消耗、低速率传输、低成本作为重点目标,旨在为个人或者家庭范围内不同设备之间的低速互连提供统一标准。IEEE 802.15.4 标准为 LR-WPAN 网络制定了物理(Physical,PHY)层和介质访问控制(Medium Access Control,MAC)子层协议。LR-WPAN 网络的特征与传感器网络有很多相似之处,很多研究机构把 IEEE 802.15.4 标准作为传感器的通信标准。LR-WPAN 网络是一种结构简单、成本低廉的无线通信网络,它使在低电能和低吞吐量的应用环境中使用无线连接成为可能。与无线局域网(Wireless Local Area Network,WLAN)相比,LR-WPAN 网络只需很少的基础设施,甚至不需要基础设施。

IEEE 802.15.4 网络协议栈基于开放系统互连(Open System Interconnection,OSI)模型,每一层都实现一部分通信功能,并向高层提供服务。IEEE 802.15.4 标准只定义了 PHY 层和数据链路层的 MAC 子层。PHY 层由射频收发器以及底层的控制模块构成。MAC 子层为高层访问物理信道提供点对点通信的服务接口。

IEEE 802.15.4 标准定义的 LR-WPAN 网络具有如下特点。

(1) 在不同的载波频率下实现了 20kb/s、40kb/s 和 250kb/s 三种不同的传输速率。

(2) 支持星形和点对点两种网络拓扑结构。

(3) 有 16 位和 64 位两种地址格式,其中 64 位地址是全球唯一的扩展地址。

(4) 支持冲突避免的载波多路侦听技术(Carrier Sense Multiple Access with Collision Avoidance,CSMA-CA)。

(5) 支持确认(ACK)机制,保证传输可靠性。

3.1.1 网络简介

IEEE 802.15.4 网络是指在一个个人操作空间(Personal Operating Space,POS)内使用相同的无线信道并通过 IEEE 802.15.4 标准相互通信的一组设备的集合,又名 LR-WPAN 网络。这个网络中的设备可以根据通信能力分为全功能设备(Full Function Device,FFD)和精简功能设备(Reduced Function Device,RFD)。FFD 之间以及 FFD 与 RFD 之间都可以通信。RFD 之间不能直接通信,只能与 FFD 通信或者通过一个 FFD 向外转发数据。这个与 RFD 相关联的 FFD 称为该 RFD 协调器。RFD 主要用于简单的控制应用,例如灯的

开关、被动式红外线传感器等，传输的数据量较少，对传输资源和通信资源占用不多，这样RFD可以采用非常廉价的实现方案。

在IEEE 802.15.4网络中，有一个被称为PAN协调器的FFD，是LR-WPAN网络中的主控制器。PAN协调器(以下简称网络协调器)除了直接参与应用以外，还要完成成员身份管理、链路状态信息管理和分组转发等任务。

无线通信信道的特征是动态变化的。结点位置或天线方向的微小改变、物体移动等周围环境的变化都有可能引起通信链路信号强度和质量的剧烈变化，因而无线通信的覆盖范围不是确定的，这就造成了LR-WPAN网络中设备的数量以及它们之间关系的动态变化。

3.1.2 拓扑结构

IEEE 802.15.4网络根据应用的需要可以组织成星形，也可以组织成点对点的网络。在星形结构中，所有设备都与中心设备PAN网络协调器通信。在这种网络中，网络协调器一般采用持续电力系统供电，而其他设备采用电池供电。星形结构的网络适合家庭自动化、个人计算机的外设以及个人健康护理等小范围的室内应用。

与星形结构不同，点对点网络只要彼此都在对方的无线辐射范围之内，则任何两个设备之间都可以直接通信。点对点网络中也需要网络协调器，网络协调器负责实现管理链路状态信息，认证设备身份等功能。点对点网络模式可以支持AD-Hoc网络，允许通过多跳路由的方式在网络中传输数据。不过，一般认为自组织问题由网络层来解决，不在IEEE 802.15.4标准的讨论范围之内。点对点网络可以构造更复杂的网络结构，适合设备分布范围广的应用，例如在工业检测与控制、货物库存跟踪和智能农业等方面都有非常好的应用前景。

3.1.3 网络拓扑的形成过程

虽然网络拓扑结构应由网络层实现，但IEEE 802.15.4为形成各种网络拓扑结构提供了充分支持。下面主要讨论IEEE 802.15.4对形成网络拓扑结构提供的支持，详细地描述了星形结构和点对点网络的形成过程。

1. 星形结构网络的形成

星形结构网络以网络协调器为中心，所有设备只能与网络协调器进行通信，因此在星形结构网络的形成过程中，第一步就是建立网络协调器。任何一个FFD都有成为网络协调器的可能，一个网络如何确定自己的网络协调器由上层协议决定。下面介绍一种简单的策略，一个FFD在第一次被激活后，首先广播查询网络协调器的请求，如果接收到回应说明网络中已经存在网络协调器，再通过一系列认证过程，FFD就成为这个网络中的普通设备。如果没有收到回应或者认证过程不成功，这个FFD就可以建立自己的网络并且成为这个网络的网络协调器。当然，这里还存在一些更深入的问题：一是网络协调器过期问题，例如原有的网络协调器损坏或者能量耗尽；二是偶然因素造成多个网络协调器竞争问题，例如物体阻挡导致一个FFD自己建立网络，当物体离开时，网络中将出现多个协调器。

网络协调器要为网络选择一个唯一的标识符，所有该星形结构网络中的设备都使用这个标识符来规定自己的属主关系。不同星形结构网络之间的设备通过设置专门的网关完成相互通信。选择一个标识符后，网络协调器就允许其他设备加入自己的网络，并为这些设备转发数据分组。

星形结构网络中的两个设备如果需要互相通信，都是先把各自的数据包发送给网络协调器，然后由网络协调器转发给对方。

2. 点对点网络的形成

在点对点网络中，任意两个设备只要能够彼此收到对方的无线信号，就可以进行直接通信，不需要其他设备的转发。点对点网络仍然需要一个网络协调器，不过该协调器的功能已不再是为其他设备转发数据，而是完成设备注册和访问控制等基本的网络管理功能。网络协调器的产生同样由上层协议规定，例如把某个信道上第一个开始通信的设备作为该信道上的网络协议器。簇树网络是点对点网络的一个例子，下面以簇树网络为例描述点对点网络的形成过程。

在簇树网络中，绝大多数设备是 FFD，而 RFD 总是作为簇树的叶设备连接到网络中。任意一个 FFD 都可以充当 RFD 协调器或者网络协调器，为其他设备提供同步信息。在这些协调器中，只有一个可以充当整个点对点网络的网络协调器。网络协调器可能和网络中其他设备一样，也可能拥有比其他设备更多的计算资源和能量资源。网络协调器首先将自己设为簇头，并将簇标识符设置为 0，同时为该簇选择一个未被使用的 PAN 标识符，形成网络中的第一个簇。接着，网络协调器开始广播信标帧，邻近设备收到信标帧后就可以申请加入该簇。设备可否成为簇成员由网络协调器决定，如果请求被允许，则该设备将作为簇的子设备加入网络协调器的邻居列表。新加入的设备会将簇头作为它的父设备加入自己的邻居列表中。

IEEE 802.15.4 是 ZigBee、WirelessHART、Mi-Wi 等规范的基础，描述了低速率无线个人局域网的物理层和媒体接入控制协议，属于 IEEE 802.15 工作组。在 868/915M、2.4GHz 的 ISM（Industrial Scientific Medical，工业科学医学）频段上，数据传输速率最高可达 250kb/s。由于 IEEE 802.15.4 具有低功耗、低成本的优点，因此在很多领域获得了广泛的应用。在打包提供的免费协议栈代码中，美国德州仪器公司的协议栈部分以库的形式提供，限制了其应用范围即只能应用于本公司所生产的单片机芯片上，不方便扩展、修改。而美国微芯科技公司尽管提供了源代码，但在编程风格、多任务操作系统上的运行考虑欠周。鉴于此，设计实现结构清晰、层次分明、移植方便、能运行在多任务环境符合的 IEEE 802.15.4 协议代码，可为架构上层协议及应用扩展建立良好的基础。

3.2 蓝牙技术

蓝牙是一种短程宽带无线电技术，是实现语音和数据无线传输的全球开放性标准。它使用跳频扩谱（Frequency-Hopping Spread Spectrum，FHSS）、时分多址（Time Division Multiple Access，TDMA）、码分多址（Code Division Multiple Access，CDMA）等先进技术，在小范围内建立多种通信与信息系统之间的信息传输。

3.2.1 蓝牙技术概述

1. 蓝牙技术的起源

蓝牙的名字来源于 10 世纪的丹麦国王 Harald Blatand（英文名称为 Harold

Bluetooth)。1994 年,瑞典爱立信公司研发了一种新型的短距无线通信技术,致力于为 POS 内相互通信的无线通信设备提供通信标准。POS 一般是指以用户为中心半径约为 10m 的空间范围,在这个范围内,用户位置可以是固定的,也可以是移动的。在筹备阶段,行业协会需要一个极具表现力的名字来命名这项高新技术。组织人员在经过一夜关于欧洲历史和未来无线技术发展的讨论后,认为用国王 Blatand 的名字命名再合适不过。这项即将面世的技术将被定义为允许不同工业领域(例如计算机、手机和汽车行业)之间的协调工作。

蓝牙技术由蓝牙技术联盟组织研发。该组织成立于 1998 年,成员包括爱立信、IBM、Intel、东芝和诺基亚等国际通信巨头。1998 年 3 月,美国的电气和电子工程师学会(Institute of Electrical and Electronics Engineers,IEEE)为蓝牙技术制定 IEEE 802.15.1 标准。蓝牙技术的物理层采用跳频与扩频相结合的调制技术,频段范围是 2.402～2.480GHz,通信速率一般能达到 1Mb/s。蓝牙通信中的设备有两种角色——主设备和从设备。同一个蓝牙设备可以在这两种角色之间转换。一个主设备最多可以同时和 7 个从设备通信。在任意时刻,主设备单元可以向任何一个从设备单元发送信息,也可以用广播方式同时向多个从设备发送信息。截至 2010 年 7 月,蓝牙技术联盟共推出 6 个技术版本,即 V1.1/1.2/2.0/2.1/3.0/4.0。按照通信距离的远近,蓝牙技术版本可分为 Class A(1)和 Class B(2)。在 4.0 版本中,蓝牙的通信距离提高到 100m 以上,通信速率达到 24Mb/s。

2. 蓝牙技术的发展

1994 年,蓝牙技术的出台立刻引起全世界的关注,美国《网络计算》杂志将其评为“十年来十大热门新技术”之一。事实上,蓝牙技术也的确广泛地应用于移动设备(手机、PDA)、个人计算机与无线外围设备(耳机、鼠标、键盘)、GPS 设备、医疗设备以及游戏平台(PS3、Wii)等各个领域。

尽管如此,蓝牙技术一开始并未如人们期望的那样成为个域网的绝对标准。随着 IEEE 802.11 技术的兴起,蓝牙技术自 21 世纪以来,仅在耳机、鼠标、车载语音系统等小范围市场内取得成功。究其原因,从市场角度来看,蓝牙技术主要存在芯片价格高、模块小型化、安装成本高、天线设计和组装困难等问题。从技术角度来看,蓝牙技术的建立连接时间长、功耗高、安全性低。正当蓝牙技术快要被人遗忘的时候,移动互联网和物联网的快速发展拯救了它。智能手机正在以前所未有的速度普及,基于安卓(Android)操作系统的智能手机零售价迅速降低至 600 元,这意味着全世界绝大多数人可以轻松拥有智能手机。目前,蓝牙技术已经是智能手机的标准配置。手机智能化是未来的发展趋势,智能手机在运动、健身、健康和医疗等领域具有极为广阔的应用前景,作为连接智能手机和外设的标准手段,蓝牙技术的市场前景不可限量。蓝牙技术联盟目前拥有 16 000 家成员,应用蓝牙技术的产品日出货量达到 50 000 台,蓝牙技术将重获新生。

目前,智能手机外设是一个新的研究热点,例如由 Nike 公司研发的 FuelBand 腕带,由美国麻省理工学院的 4 名学生发明的 Amiigo 智能腕带等。以 Amiigo 智能腕带为例,它可以记录和测量日常生活中的运动量(如跑步赶上公交车、从超市拎回大包小包等日常生活中随时随地获得的运动量),以激励人们更好地运动。Amiigo 测量的时间、能量、步数、体温等数据可以通过蓝牙技术传送到智能手机上。当用户打开 iPhone 或者 Android 智能手机的 Amiigo 应用时,便可以了解自己的身体状况、运动量等。

3. 蓝牙技术的特点

(1) 工作频段：2.4GHz 属于 ISM 频段，无须申请许可证。大多数国家使用 79 个频点，载频为(2402+k)MHz(k=0，1，2，…，78)，载频间隔 1MHz。采用 TDD 时分双工方式。

(2) 传输速率：1Mb/s。

(3) 调试方式：BT=0.5 的 GFSK 调制，调制指数为 0.28～0.35。

(4) 采用跳频技术：跳频速率为 1600 跳/秒，在建链时(包括寻呼和查询)提高为 3200 跳/秒。蓝牙通过快跳频和短分组技术减少同频干扰，保证传输的可靠性。

(5) 语音调制方式：连续可变斜率增量调制，抗衰落性强，即使误码率达到 4%，话音质量也可接受。

(6) 支持电路交换和分组交换业务：蓝牙技术支持实时的同步定向连接(SCO 链路)和非实时的异步不定向连接(ACL 链路)，前者主要传送语音等实时性强的信息，后者以传送数据包为主。语音和数据可以单独或同时传输。蓝牙技术支持一个异步数据通道、3 个并发的同步话音通道或同时传送异步数据和同步话音的通道。每个话音通道支持 64kb/s 的同步话音；异步通道支持 723.2/57.6kb/s 的非对称双工通信或 433.9kb/s 的对称全双工通信。

(7) 支持点对点及点对多点的通信：蓝牙设备按特定方式可组成微微网和分布式网络两种网络，其中微微网的建立由两台设备的连接开始，最多可由 8 台设备组成。在一个微微网中，只有一台为主设备，其他均为从设备，不同的主从设备对可以采用不同的连接方式，在一次通信中，连接方式也可以任意改变。几个相互独立的微微网以特定方式连接在一起便构成了分布式网络。所有的蓝牙设备都是对等的，所以在蓝牙技术中没有基站的概念。

(8) 工作距离：蓝牙设备分为 3 个功率等级，分别是 100mW(20dBm)、2.5mW(4dBm)和 1mW(0dBm)，相应的有效工作范围为 100m、10m 和 1m。

3.2.2 蓝牙协议体系

蓝牙协议体系结构可以分为底层协议、中间应用层协议、高端应用层协议 3 部分，如图 3-1 所示。

1. 底层协议

链路管理器(LM)、基带(BB)和射频(RF)构成了蓝牙的物理模块。射频通过 2.4GHz 的 ISM 频段实现数据流的传输，主要用于定义蓝牙收发器应满足的条件。基带负责跳频和蓝牙数据、信息帧的传输。基带就是蓝牙的物理层，负责管理物理层信道和链路中除了错误纠正、数据处理、调频选择和蓝牙安全之外的所有业务。基带在蓝牙协议中位于蓝牙无线电上，基本上起链路控制和链路管理的作用，例如承载链路连接和功率控制这类链路级路由等。基带还管理异步和同步链路、处理数据包、寻呼、查询接入和查询蓝牙设备等。基带收发器采用时分复用(TDD)方案(交替发送和接收)，因此除了不同的跳频之外(频分)，时间都被划分为时隙。在正常的连接模式下，主单元总是以偶数时隙启动，而从单元则总是从奇数时隙启动(尽管它们可以不考虑时隙的序数而持续传输)。

链路管理器负责链路的连接建立、拆除、安全和控制，为上层软件模块提供不同的访问入口，但是两个模块接口之间的消息和数据传输必须通过蓝牙主机控制器接口(HCI)的解

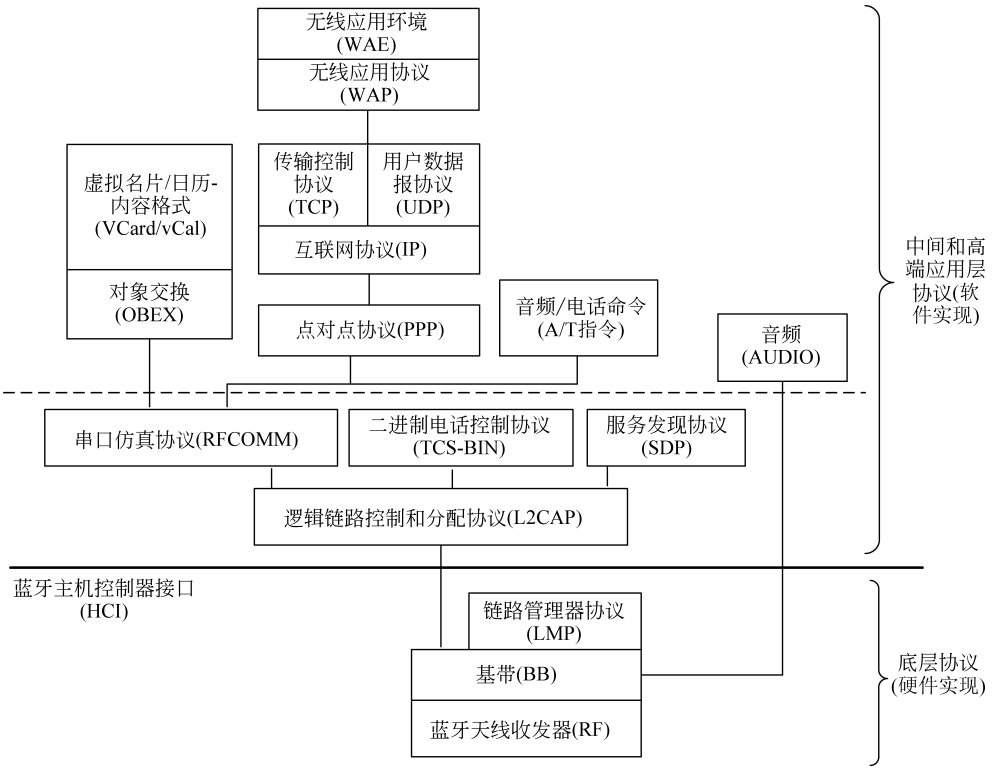

图 3-1　蓝牙协议体系结构

析。也就是说，HCI 就是蓝牙协议中软件和硬件接口的部分，它提供了一个调用下层的基带、链路管理器、状态和控制寄存器等硬件的统一命令接口，HCI 以上的协议软件实体运行在主机上，而 HCI 以下的功能由蓝牙设备完成，两者直接通过传输层进行交互。

2. 中间和高端应用层协议

设计协议和协议栈的主要原则是尽可能地利用现有的各种高层协议，保证现有协议与蓝牙技术的融合以及各种应用之间的互通；充分利用兼容蓝牙技术规范的软、硬件系统和蓝牙技术规范的开放性，便于开发新的应用。蓝牙标准包括 Core、Profiles 两部分。Core 部分是蓝牙的核心，主要定义蓝牙的技术细节；Profiles 部分定义蓝牙的各种应用中协议栈的组成以及相应协议栈的实现，这就为蓝牙的全球兼容性打下了基础。中间和高端应用层协议是蓝牙协议的关键部分，包括基带部分协议和其他低层链路功能的基带链路控制器协议；用于链路的建立、安全和控制的链路管理器协议；描述主机控制器接口（HCI）的协议；支持高层协议复用、帧的组装和拆分的逻辑链路控制和分配的协议；发现蓝牙设备提供服务的协议等。

1）链路管理器协议

链路管理器协议（LMP）负责建立各个蓝牙设备之间的连接，通过连接的发起、交换、核实进行身份验证和加密，通过协商确定基带数据分组的大小。LMP 还控制无线设备的电源模式、工作周期，以及微微网内设备单元的连接状态。

2）逻辑链路控制和分配协议

逻辑链路控制和分配协议（L2CAP）是基带的上层协议，可以认为它与 LMP 并行工作。

两者的区别在于，当业务数据不经过 LMP 时，L2CAP 为上层提供服务。L2CAP 向上层提供面向连接或无连接的数据服务，采用了多路技术、分割和重组技术、群提取技术。L2CAP 允许高层协议以 64KB 为单位收发数据分组。虽然基带协议提供了同步定向连接(SCO)和异步无连接(ACL)两种连接类型，但 L2CAP 只支持 ACL。

3) 服务发现协议

服务发现协议(SDP)的发现服务在蓝牙技术框架中起到至关重要的作用，它是所有用户模式的基础。使用 SDP，可以查询设备信息和服务类型，从而在蓝牙设备间建立相应的连接。

3. 应用层协议

1) 电缆替代协议

电缆替代协议(RFCOMM)是一种仿真协议，在蓝牙基带协议上仿真 RS-232 的控制和数据信号，为上层协议提供服务。

2) 电话控制协议

电话控制协议(TCS)是面向比特的协议，用于定义蓝牙设备间建立数据和话音呼叫的控制命令与处理蓝牙 TCS 设备群的移动管理进程；AT Command 控制命令集是定义在多用户模式下控制移动电话、调制解调器和用于仿真的命令集。

3) 与 Internet 相关的高层协议

与 Internet 相关的高层协议定义了与 Internet 相关的点对点协议(PPP)、用户数据报协议(UDP)、传输控制协议/互联网协议(TCP/IP)及无线应用协议(WAP)。两个蓝牙设备必须具有相同的协议才能进行通信。

4) 无线应用协议

无线应用协议(WAP)是由无线应用协议论坛制定的，它融合了各种广域无线网络技术，目的是将互联网内容传送到手机与其他无线终端上。使用 WAP 可以充分利用为无线应用环境(WAE)开发的高层应用软件。

5) 点对点协议

在蓝牙技术中，点对点协议(PPP)位于 RFCOMM 上层，用于完成点对点的连接。

6) 对象交换协议

对象交换协议(IrOBEX，简写为 OBEX)是由红外数据协会制定的会话层协议，它采用简单和自发的方式交换目标。OBEX 是一种类似于 HTTP 的协议，它假设传输层是可靠的，采用客户/服务器模式，独立于传输机制和传输应用程序接口。电子名片交换格式(vCard)、电子日历及日程交换格式(vCal)都是开放性规范，它们都没有定义传输机制，只是定义了数据传输模式。蓝牙特别兴趣小组(SIG)采用 vCard/vCal 规范，是为了进一步促进个人信息交换。

7) TCP/UDP/IP

TCP/UDP/IP 是由互联网工程任务组(The Internet Engineering Task Force，IETF)制定的广泛应用于互联网通信的协议，在蓝牙设备中使用这些协议是为了与互联网设备进行通信。

3.2.3 蓝牙数据包

1. 蓝牙链路

蓝牙基带可以处理两种类型的链路：SCO 链路和 ACL 链路。SCO 链路是微微网中单一主单元和单一从单元之间的一种点对点对称的链路。主单元采用按照规定间隔预留时隙(电路交换类型)的方式可以维护 SCO 链路，SCO 链路携带语音信息。主单元可以支持多达 3 条并发 SCO 链路，而从单元则可以支持 2 条或者 3 条 SCO 链路。SCO 数据包永不重传。SCO 数据包用于 64kb/s 语音传输。

ACL 链路是微微网内主单元和全部从单元之间的点对多点链路。在没有为 SCO 链路预留时隙的情况下，主单元可以对任意从单元在每时隙的基础上建立 ACL 链路，其中包括从单元已经使用某条 SCO 链路的情况(分组交换类型)。一个微微网只能存在一条 ACL 链路。大多数 ACL 数据包都可以应用数据包重传。

2. 蓝牙前导接入码

微微网信道内的数据都是通过数据包传输的。通常情况下，数据包的结构如图 3-2 所示。

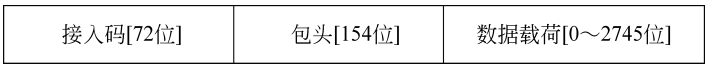

图 3-2　蓝牙数据包的结构

接入码用于时序同步、偏移补偿、寻呼和查询。接入码分为 3 类：信道接入码(Channel Access Code，CAC)、设备接入码(Device Access Code，DAC)和查询接入码(Inquiry Access Code，IAC)。CAC 标识微微网(对微微网唯一)，DAC 则用于寻呼及其响应，IAC 用于查询。数据包的包头包含了数据包确认、乱序数据包重排的数据包编号、流控、从单元地址和包头错误检查等信息。数据包的数据部分可以包含语音字段、数据字段或者两者皆有。数据包可以占据一个以上的时隙(称为多时隙数据包)，而且可以在下一个时隙中持续传输。数据部分还可以携带一个 16 位的 CRC 用于数据错误检测和错误纠正。SCO 数据包则不包括 CRC。

3. 蓝牙数据包

1) 蓝牙单时隙、多时隙结构

为了实现在同一信道中的主、从通信，蓝牙定义了时分双工(TDD)的工作模式。实际工作中，蓝牙跳频频率为 1600 跳/秒，这也说明了在每个跳频点上停留的时间为 625μs，这 625μs 就被定义为蓝牙的一个时隙。在实际工作中，时隙可以分为单时隙和多时隙。工作时隙的选择依据是当前的数据流量以及工作状态下的无线环境。

2) V1.2 标准蓝牙数据包的类型

V1.2 标准蓝牙有 5 种普通类型数据包、4 种 SCO 数据包和 7 种 ACL 数据包，如表 3-1 所示。

表 3-1　V1.2 标准蓝牙数据包的类型

类型	名称	说　明
普通类型数据包	ID	携带设备接入码(DAC)或者查询接入码(IAC)；占据 1 个时隙
	NULL	NULL 数据包没有数据，用于获得链路信息和流控；占据 1 个时隙，无确认
	POLL	无数据和确认；主设备用它检查从设备是否启动；占据 1 个时隙
	FHS	表明蓝牙设备地址和发送方时钟的特殊控制数据包，用于寻呼主设备响应
	DM1	支持任何链路中的控制消息，还可以携带规则用户数据；占据 1 个时隙
SCO 数据包	HV1	携带 10 信息字节，通常用做语音传输；1/3FEC 编码；占据 1 个时隙
	HV2	携带 20 信息字节，通常用做语音传输；2/3FEC 编码；占据 1 个时隙
	HV3	携带 30 信息字节，通常用做语音传输；无 FEC 编码；占据 1 个时隙
	DV	数据-语音组合数据包；语音字段没有 FEC 保护，数据字段采用 2/3FEC 编码；语音字段从不重传，数据字段可以重传
ACL 数据包	DM1	携带 18 信息字节；2/3FEC 编码；占据 1 个时隙
	DH1	携带 28 信息字节；无 FEC 编码；占据 1 个时隙
	DM3	携带 123 信息字节；2/3FEC 编码；占据 3 个时隙
	DH3	携带 185 信息字节；无 FEC 编码；占据 3 个时隙
	DM5	携带 226 信息字节；2/3FEC 编码；占据 5 个时隙
	DH5	携带 341 信息字节；无 FEC 编码；占据 5 个时隙
	AUX1	携带 30 信息字节；类似 DH1，但没有 CRC 代码；占据 1 个时隙

3) 蓝牙 EDR 数据包结构

蓝牙 EDR 是 SIG 开发的一种协议，能使蓝牙无线连接的带宽提高到 3Mb/s，V2.0＋EDR 蓝牙的主要改进在于它使数据传输速率较传统的蓝牙速率提高到原来的 3 倍。这就意味着无线单元运行的时间只有原来的三分之一，功耗也只有原来的三分之一。因此可以实现更快速的连接，并可同时支持多条蓝牙链路，以及实现新的更高带宽的应用，如音频流。

数据传输速率得以提高的部分原因在于数据包传输方式的根本改变。

蓝牙 EDR 数据包仍然采用高斯频移键控(GFSK)来调制接入码和数据包的包头，而对有效载荷采用下列两种调制方式之一：一种是强制性的，提供两倍的数据传输速率，并且可以容忍较大的噪声；另一种是选择性的，可以提供三倍的数据传输速率。

两倍数据传输速率采用 π/4 差分四相移相键控(π/4-DQPSK)。顾名思义，这种调制方法改变的是载波的相位而不是频率的相位。四相是指每个符号有 4 个可能的相位，从而允许每个符号有 2 位的数据进行编码。因为符号速率保持不变，所以数据传输速率增加了两倍。

三倍数据传输速率采用 8-DPSK。8-DPSK 类似于 π/4-DQPSK，但允许差分移动至 8 个可能相位中的任何一个。相邻相位之间较小的相差和 ±π 相位跳变的利用，意味着 8-DPSK 更易受到干扰，但它允许每个符号有 3 位的数据进行编码。

3.2.4 蓝牙地址

蓝牙地址由十六进制码构成。每台蓝牙设备都有唯一的一个地址，就像网络的 IP 地址一样。每一个蓝牙设备生产商都有不同的地址号段，通过读取蓝牙地址码可以查出该设备的生产商及批次。手机的蓝牙地址就像人的身份证号码，具有唯一性，可用来区分其他蓝牙设备、保存蓝牙配对配置信息。

蓝牙地址的表示格式为

××：××：××：××：××：××

其中×可以是数字，也可以是字母，与网络设备的 MAC 地址一样，是设备之间通信的唯一身份证。

蓝牙地址分为 3 部分：24 位地址低端部分(LAP)、8 位地址高端部分(UAP)和 16 位无意义地址部分(NAP)。其中，NAP 和 UAP 是生产厂商的唯一标识码，必须由蓝牙权威部门分配给不同的厂商，而 LAP 是由厂商内部自由分配。对于某一种型号的手机或者设备，所有个体的 NAP、UAP 是固定的，可变的是 LAP。LAP 共有 24 位，一般来说厂家在制造时会从 0 开始分配地址直到 224，以保证个体之间地址的区别。但是如果产品数量太多导致地址都用完了或者在写地址时出了问题，就会出现蓝牙地址重复使用的情况，但是出现的概率非常小。

3.2.5 蓝牙的状态

蓝牙控制器主要运行在待命和连接两个状态下。

1. 蓝牙待命状态

微微网内共有 7 种子状态可用于增加从设备或者实现连接，这些状态是寻呼(Page)、寻呼扫描(Page Scan)、查询(Inquiry)、查询扫描(Inquiry Scan)、主设备响应(Master Response)、从设备响应(Slave Response)和查询响应(Inquiry Response)，如表 3-2 所示。

表 3-2 蓝牙待命状态的子状态

子 状 态	描 述
寻呼	该子状态被主设备用于激活和连接从设备，主设备通过在不同的跳频信道内传送从设备的识别码来发出寻呼消息
寻呼扫描	在该子状态下，从设备在一个窗口扫描存活期内以单一跳频侦听自己的设备接入码
查询	该子状态被主设备用于收集蓝牙设备地址，发现相邻蓝牙设备的身份
查询扫描	在该子状态下，蓝牙设备侦听来自其他设备的查询。此时扫描设备可以侦听一般查询接入码或者专用查询接入码
主单元响应	主设备在该状态下发送 FHS 数据包给从设备。如果主设备收到从设备的响应后即进入该子状态。从设备收到主设备发送的 FHS 数据包后，将进入连接状态
从单元响应	从设备在该子状态下响应主设备的寻呼消息。如果处于寻呼扫描子状态下的从设备和主设备寻呼消息相关即进入该状态
查询响应	对查询而言，只有从设备才可以响应而主设备则不能。从设备用 FHS 数据包响应，该数据包包含了从设备的接入码、内部时钟和某些其他从设备信息

2. 蓝牙连接状态

连接状态开始于主设备发送 POLL 数据包。通过这个数据包，主设备即可检查从设备是否已经交换到了主设备的时序和跳频信道，从设备即可以任何类型的数据包响应。

连接状态的蓝牙设备可以处于以下 4 种模式：激活(Active)、保持(Hold)、休眠(Sniff)和监听(Park)模式。蓝牙技术中一个显著的技术难点就是如何实现这些模式之间的迁移，特别是从监听到激活(或者反之)的迁移难度更大。这些模式的简要说明如表 3-3 所示。

表 3-3　连接状态的蓝牙设备的模式

模式	描　　述
激活	在该模式下，主设备和从设备通过侦听、发送或者接收数据包的方式主动参与信道操作。主设备和从设备相互保持同步
保持	在该模式下，设备只有一个内部计数器在工作，不支持 ACL 数据包，可为寻呼、扫描等操作提供可用信道。保持模式一般用于连接几个微微网或能耗低的设备。进入该模式前，主结点和从结点应就从结点处于保持模式的持续时间达成一致。当时间耗尽时，从结点将被唤醒并与信道同步，等待主结点的指示
休眠	在该模式下，主设备只能有规律地在特定的时隙发送数据，从设备只在指定的时隙“嗅探”消息，可以在空时隙睡眠而节约功率。呼吸间隔可以根据应用需求做适当调整
监听	在该模式下，从设备无须使用微微网信道可以和信道保持同步，设备几乎没有任何活动，不支持数据传送，偶尔收听主设备的消息并恢复同步、检查广播消息。设备被赋予一个监听成员地址，并失去其活动成员地址

蓝牙设备的各种子状态可以相互转换，在待命状态下，如果设备有数据传输需求，可以采用两种方式进入连接状态：第一，如果主设备知道从设备的蓝牙地址，可以采用直接寻呼的方式进入连接状态；第二，如果主设备不知道从设备的蓝牙地址，可通过查询来获得从设备的蓝牙地址，再进行寻呼从而进入连接状态，也可以从连接状态进入各种低功耗模式。但是进行射频测试时，必须进入蓝牙的测试模式。

在微微网建立之前，所有设备都处于待命状态。在该状态下，未连接的设备每隔 1.28s 监听一次消息，设备一旦被唤醒，就在预先设定的 32 个跳频频率上监听信息。虽然跳频数目可因地区而异，但 32 个跳频频率为绝大多数国家所采用。

连接进程由主设备初始化。如果一个设备的地址已知，就采用页信息(Page Message)建立连接；如果地址未知，就采用紧随页信息的查询信息(Inquiry Message)建立连接。查询信息主要用来查询地址未知的设备(例如公用打印机、传真机等)，它与页信息类似，需要附加一个周期来收集所有的应答。在初始页状态(Page State)，主设备在 16 个跳频频率上发送一串相同的页信息给从设备，如果没有收到应答，主设备就在另外的 16 个跳频频率上发送页信息。主设备到从设备的最大延迟为两个唤醒周期(2.56s)，平均延迟为半个唤醒周期(0.64s)。

在微微网中，无数据传输的设备转入节能工作模式。主设备可将从设备设置为保持模式。此时，只有内部定时器工作；从设备也可以要求转入保持模式。设备由保持模式转出后，可以立即恢复数据传输。连接几个微微网或管理低功耗器件(如温度传感器)时，常使用保持模式。监听模式和休眠模式是另外两种低功耗工作模式。在监听模式下，从设备监听网络的时间间隔增大，其间隔大小视应用情况由编程确定；在休眠模式下，从设备放弃了

MAC 地址，仅偶尔监听网络同步信息和检查广播信息。各节能模式按照电源效率由高到低的顺序排列依次为休眠、保持和监听。

3.2.6 蓝牙的关键技术

1. 无线频段的选择和抗干扰

蓝牙技术采用 2.4～2.4835GHz 的 ISM 频段，这是由于以下 3 个原因：该频段内没有其他系统信号的干扰；该频段向公众开放，无须特许；频段在全球范围内有效。世界各个国和地区的相关法规不同，一般只规定信号的传输范围和最大传输功率。对于一个在全球范围内运营的系统，只有选用的频段必须同时满足所有规定，才能使任何用户都可接入，因此必须将所需要素最小化。在满足规则的情况下，可自由接入无线频段，此时，抗干扰问题变得非常重要。因为 2.4GHz 的 ISM 频段为开放频段，使用其中的任何频段都会遇到不可预测的干扰源（例如某些家用电器、无线电话和汽车开门器等）。此外，对外部和其他蓝牙用户的干扰源也应做充分估计。

抗干扰的方法分为避免干扰和抑制干扰两种。避免干扰可通过降低各通信单元的信号发射电平来达到，抑制干扰则是通过编码或直接序列扩频来实现。然而，在不同的无线环境下，专用系统的干扰和有用信号的动态范围变化极大。在超过 50dB 信噪比和不同环境功率差异的情况下，要达到 1Mb/s 以上速率，仅靠编码和处理增益是不够的。相反，由于信号可在频率（或时间）没有干扰时（或干扰低时）发送，因此避免干扰更容易一些。若采用时间避免干扰法，当遇到时域脉冲干扰时，发送的信号将会中止。大部分无线系统的带宽是有限的，而在 2.4GHz 频段上，系统带宽为 80MHz，可找到一段无明显干扰的频谱。同时，可利用频域滤波器对无线频带其余频谱进行抑制，以达到理想效果。因此，频域避免干扰法更为可行。

2. 多路访问接入体和调制方式

选择专用系统多路访问接入体系，是因为在 ISM 频段内尚无统一的规定。频分多路访问（Frequency Division Multiple Access，FDMA）的优势在于信道的正交性仅依赖发射端晶振的准确性，结合自适应或动态信道分配结构，可免除干扰，但单一的 FDMA 无法满足 ISM 频段内的扩频需求。时分多路访问 TDMA 的信道正交化需要严格的时钟同步。在多用户专用系统连接中，保持共同的定时参考十分困难。码分多路访问 CDMA 可实现扩频，应用于非对称系统，可使专用系统达到最佳性能。

直接序列（DS）CDMA 因远近效应，需要一致的功率控制或额外的增益。与 TDMA 相同，其信道正交化也需要共同的定时参考，随着使用数目的增加，会需要更高的芯片速度、更宽的带宽（抗干扰）和更多的电路消耗。跳频（FH）CDMA 结合了专用无线系统中的各种优点，信号可扩频至很宽的范围，因而使窄带干扰的影响变得很小。跳频载波为正交的，通过滤波，邻近跳频干扰可得到有效抑制，对窄带和用户间干扰造成的通信中断，可依赖高层协议来解决。在 ISM 频段，跳频系统的信号带宽限制在 1MHz 以内。为了提高系统的鲁棒性，选择二进制调制结构。由于受带宽限制，其数据传输速率低于 1Mb/s。为了支持突发数据传输，最佳的方式是采用非相干解调检测。蓝牙技术采用高斯频移键控调制，调制系数为 0.3。逻辑“1”发送正频偏，逻辑“0”发送负频偏。解调可通过带限 FM 鉴频器完成。

3. 媒体接入控制

蓝牙系统可实现同一区域内大量的非对称通信。与其他专用系统实行一定范围内的单元共享同一信道不同，蓝牙系统设计为允许大量独立信道存在，每一个信道仅为有限的用户服务。由调制方式可以看出，在 ISM 频段，一条跳频信道所支持的比特率为 1Mb/s。理论上，79 条载波频谱支持 79Mb/s。由于跳频序列非正交化，理论容量 79Mb/s 不可能达到，但可远远超过 1Mb/s。

一条跳频蓝牙信道与一个微微网相连。微微网信道由一个主设备标识（提供跳频序列）和系统时钟（提供跳相位）定义，其他为从设备。每一个蓝牙无线系统有一个本地时钟，没有通常的定时参考。当一个微微网建立后，从设备进行时钟补偿，使之与主设备同步，微微网释放后，补偿也取消，但可存储起来以便再用。不同信道有不同的主设备，因而存在不同的跳频序列和相位。一条普通信道的设备数量为 8（1 主 7 从），可保证设备之间有效寻址和大容量通信。蓝牙系统建立在对等通信的基础上，主从任务仅在微微网生存期内有效。当微微网取消后，主从任务随即取消。每个设备皆可为主设备或从设备，可定义建立微微网的设备为主设备。除定义微微网外，主设备还控制微微网的信息流量并管理接入。接入为非自由竞争，625μs 的驻留时间仅允许发送一个数据包。基于竞争的接入方式需要较多开销，效率较低。在蓝牙系统中，实行主设备集中控制，通信仅存在于主设备与一个或多个从设备之间。主从设备通信时，时隙交替使用。在进行主设备传输时，主设备确定一个欲通信的从设备的地址，为了防止信道中从设备发送冲突，采用轮流检测技术，即对每个从到主时隙，由主设备决定允许哪个从设备进行发送。这一判定是以前一个时隙发送的信息为基础实施的，有且仅有恰为前一个由主到从被选中的从地址可进行发送。若主设备向某个从设备发送了信息，则此从设备被检测，可发送信息。若主设备未发送信息，它将发送一个检测包来标明从设备的检测情况。主设备的信息流体系包含上行和下行链路，目前已出现考虑从设备特征的智能体系算法。主设备控制可有效阻止微微网中的设备冲突。当互相独立的微微网设备使用同一跳频时，可能会发生干扰。系统在利用 Aloha 技术后，当信息传送时不检测载波是否空载（无侦听），若信息接收不正确，将进行重发（仅有数据）。由于驻留期短，跳频系统不宜采用避免冲突的结构。对每一个跳频，会遇到不同的竞争设备，后退机制效率不高。

4. 基于包的通信

蓝牙系统采用基于包的传输：将信息流分片（组）打包，在每一时隙内只发送一个数据包。所有数据包格式均相同：开始为接入码，接下来是包头，最后是负载。

接入码具有伪随机性，在某些接入操作中，可使用直接序列编码。接入码包括微微网主设备标志，在该信道上，所有包交换都使用该主设备标志进行标识，只有接入码与接入微微网主设备的接入码相匹配，才能被接收，从而防止一个微微网的数据包被恰好加载到相同跳频载波的另一个微微网设备所接收。在接入端，接入码与一个滑动相关器内要求的编码匹配，相关器提供直接序列处理增益。包头包含：从地址连接控制信息 3 位，以区分微微网中的从设备；用于标明是否需要自动查询方式（Automatic Repeat-reQuest，ARQ）的响应/非响应 1 位；包编码类型 4 位，定义 16 种不同负载类型；头差错检测编码（Head Error Control，HEC）8 位，采用循环冗余检测编码（Cyclic Redundancy Check，CRC）检查头错误。为了限制开销，数据包头只用 18 位，包头采用 1/3 速率前向纠错编码（Forward Error

Correction,FEC)进一步保护。

蓝牙系统定义了4种控制包。

(1) ID控制包,仅包含接入码,用于信令。

(2) 空(NULL)包,仅有接入码和包头,必须在包头传送连接信息时使用。

(3) 检测(POLL)包,与空包相似,用于主单元迫使从单元返回响应。

(4) FHS包,即FH同步包,用于在设备间交换实时时钟和标志信息(包括两单元跳频同步所需的所有信息)。其余12种编码类型用于定义包的同步或异步业务。

在时隙信道中定义了异步和同步连接。目前,异步连接对有无2/3速率FEC编码方式的负载都支持,还可进行单时隙、3时隙、5时隙的数据包传输。异步连接最大用户速率为723.2kb/s,这时,反向连接速率可达到57.6kb/s。通过交换包和依赖于连接条件的FEC编码,自适应连接可用于异步传输,依赖有效的用户数据,负载长度可变。然而,最大长度受限于RX和TX之间的最少交换时间(为200ps)。对于同步传输,仅定义了单时隙数据包传输,负载长度固定,可以有1/3速率、2/3速率或无FEC同步连接支持全双工,用户速率双向均为64kb/s。

5. 采用物理连接类型建立连接

蓝牙技术支持同步业务(如话音、信息)和异步业务(如突发数据流),定义了两种物理连接类型:同步面向连接的连接SCO和异步无连接的连接ACL。SCO为主设备与从设备的点对点连接,通过在常规时间间隔内预留双工时隙建立起来。ACL是微微网中主设备到所有从设备的点对多点连接,可使用SCO连接未用的所有空余时隙,由主单元安排ACL连接的流量。微微网的时隙结构允许有效地混合利用异步连接和同步连接。

专用系统设计中的关键问题是如何在设备间找到对方并建立连接。在蓝牙系统中,建立连接分为扫描、呼叫和查询3步。在空闲模式下,一个设备保持休眠状态,以节省能量,但是为了允许建立连接,该设备必须经常侦听是否有其他设备欲建立连接。在实际的专用系统中,没有通用的控制信道(一个设备为侦听呼叫信息而锁定),这在常规蜂窝无线系统中是很普遍的。而在蓝牙系统中,一个设备为侦听其标志而周期性被唤醒,当一个蓝牙设备被唤醒时,便开始扫描,打开与从自身标志得到的接入码相匹配的滑动相关器。蓝牙的唤醒跳频序列的数量仅为32跳,循环使用,覆盖整个80MHz带宽中的64MHz。序列是伪随机的,在每一个蓝牙设备中都是唯一的。序列从设备标志中得到,序列的相位由设备中的自行时钟决定。在空载模式下,要注意功率消耗和响应时间的折中选择:增加休眠时间可降低功耗,但会延长接入时间,由于不知道空闲单元在哪一个频率上何时被唤醒,想要连接的设备必须解决时频不定问题。无线设备大部分时间处于空闲模式,这种不确定的任务应由呼叫设备来完成。假定呼叫设备知道欲连接设备的标志,也知道唤醒序列产生用于呼叫信息的接入码,在不同频率上,每1.25ms呼叫设备重复发送接入码,对于一次响应,需发送和监听两次接入码。

将连续接入码发送到不同唤醒序列所选择的跳频上。在10ms周期内,访问16个不同跳频载波,为唤醒序列的一半。在空闲设备的休眠期内,呼叫设备在16个频率上循环发送接入码,空闲设备被唤醒后,将收到接入码,并开始建立连接。然而,因为呼叫设备不知道空闲设备的相位,32个跳频唤醒序列中的其余16个频率也可能被唤醒。若呼叫设备在相应的休眠期内收不到空闲设备的响应,它将会在其余的一半跳频序列载波上重复发送接入码。

因此，最大的接入码延迟为休眠时间的两倍。当空闲设备收到呼叫信息后，会返回一个提示呼叫设备的信息，即从空闲设备标志中得到的接入码。然后，呼叫设备发送一个 FHS 数据包给空闲设备，包含呼叫设备的全部信息(标志和时钟)。呼叫设备和空闲设备用该信息建立微微网，此时呼叫设备用其标志和时钟定义 FH 信道为主设备，而空闲设备成为从设备。

上述呼叫过程建立在呼叫设备完全不知道空闲设备时钟信息的假设上。如果两设备之间建立过联系，呼叫设备会对空闲设备时钟有一个估计。当设备连接时，将交换时钟信息，存储各自自由运行本地时钟间的补偿时间。这种补偿仅在建立连接时准确，当连接释放后，由于时钟漂移，补偿信息变得不可靠。补偿的可靠性与最后一次连接后的时间长度成反比。

建立连接时，接收标志用于决定呼叫信息和唤醒序列。若不知道该信息，欲进行连接的设备可发布一条查询消息，让接收方返回其地址和时钟信息。在查询过程中，查询者可决定哪个设备在需要的范围内，特性如何。查询信息也为接入码，但从预留标志(查询地址)处得到。空闲设备根据 32 跳的查询序列侦听查询信息，收到查询信息的设备返回 FHS 数据包。对于返回的 FHS 数据包，采用随机阻止机制，以防止多个接收端同时发送。

在呼叫和查询过程中，使用了 32 跳载波。对于纯跳频系统，最少要使用 75 跳载波。然而，在呼叫和查询过程中，仅有一个接入码用于信令。接入码用作直接序列编码，得到由直接序列编码处理增益结合 32 跳频序列的处理增益，以满足混合 DS/FH 系统规定所要求的处理增益。因此，蓝牙系统在呼叫和查询过程中是混合 DS/FH 系统，而在连接时为纯 FH 系统。

6. 纠错

蓝牙系统的纠错机制分为 FEC 和包重发。FEC 支持 1/3 速率和 2/3 速率 FEC 码。1/3 速率仅用 3 位重复编码，大部分在接收端判决，既可用于数据包头，也可用于 SCO 连接的包负载。2/3 速率码使用一种缩短的汉明码，误码捕捉用于解码，它既可用于 SCO 连接的同步包负载，也可用于 ACL 连接的异步包负载。使用 FEC 码后，编码和解码过程会变得简单、迅速，这对 RX 和 TX 间的有限处理时间非常重要。

在 ACL 连接中，可用 ARQ 结构。在这种结构中，若接收方没有响应，则发送端将重发包。每一个负载包含一个 CRC，用来检测误码。ARQ 结构分为停止等待 ARQ、向后 N 个 ARQ、重复选择 ARQ 和混合结构。为了减少复杂性，使开销和无效重发为最小，蓝牙执行了一种改进的快速 ARQ 结构：发送端在 TX 时隙重发包，在 RX 时隙提示包接收情况。若加入 2/3 速率 FEC 码，将得到Ⅰ类混合 ARQ 结构的结果。ACK/NACK 信息加载在返回包的包头里，用于在 RX/TX 的结构交换时，判定接收包是否正确。在返回包的包头里生成 ACK/NACK 域时，接收包包头的 ACK/NACK 域可表明前面的负载是否被正确接收，由此可决定是否需要重发或发送下一个包。由于处理时间短，当包接收时，可在空闲时间进行解码，由于简化了 FEC 编码结构，所以加快了处理速度。快速 ARQ 结构与停止等待 ARQ 结构相似，但延迟最小，实际上没有由 ARQ 结构引起的附加延迟。该结构比向后 N 个 ARQ 更有效，并与重复选择 ARQ 效率相同。由于只有失效的包被重发，因此可减少开销。在快速 ARQ 结构中，仅有 1 位序列号就足够了(为了滤除在 ACK/NACK 域中的错误而正确接收两次数据包)。

7. 功率管理

在蓝牙系统的设计中，要特别注意减少耗电量。在空闲模式下，在唤醒周期的 1.28～

3.84s 区间内，设备仅扫描 10ms，有效循环低于 1%。在监听状态下，有效循环可减少更多。监听模式仅在微微网建立之后才能使用，从设备可停止工作，即以非常低的有效循环来侦听信道。从设备仅须侦听接入码和包头来重新使时钟同步来决定是否可重新进入休眠状态。因为在时间和频率上都已确定(不工作的从设备被锁定到主设备，与无线和蜂窝电话被锁定到基站类似)，所以可达到非常低的有效循环。在连接中，另一个非功耗模式是休眠模式，在这种模式下，从设备不是每次都遵循主/从时隙扫描，因此扫描之间有较大的间隔。

在连接状态下，数据仅在有效时发送，这使能量消耗最小且可防止干扰。若仅有连接控制信息要传送(ACK/NACK)，则将发送没有负载的空包。因为 NACK 为默认设置，NACK 的空包不一定要发送。在长静默期内，主设备每隔一定时间就会在信道上重发一个数据包，使所有从设备对其时钟重新同步，以达到对时间漂移进行补偿的目的。在连续的 TX/RX 操作中，一个设备开始扫描始于 RX 时隙的接入码，若未找到该接入码的某窗口，则该设备返回休眠状态，直到下一个 TX 时隙(对主设备)或 RX 时隙(对从设备)；若接入码被接收(即接收信号与要求的接入码匹配)，包头就会被解码。若有 3 位的从设备地址与接收到的不匹配，将停止进一步接收。包头用于表示包的类型和包的持续时间，由此，非接收方可决定休眠时间。

8. 微微网间通信

经过优化的蓝牙系统可以在同一区域中组成数十个微微网，而没有明显的性能下降(在同一区域的多个微微网称为分散网)。蓝牙时隙连接采用的是基于包的通信方式，可使不同的微微网互连。要连接的单元可加入不同的微微网，但因无线信号只能调制到单一跳频载波上，因此设备不能同时在两个微微网中进行通信。通过调整微微网的信道参数(即主设备标志和主设备时钟)，单元可从一个微微网跳到另一个微微网，并可改变任务。例如，某一个时刻在一个微微网中作为主设备，另一个时刻在另一个微微网中作为从设备。主设备参数标示了微微网的跳频信道，因此一个设备不可能在不同的微微网中都为主设备。跳频选择机制应设计成允许微微网间可以相互通信，通过改变标志、时钟输入或选择机制，新微微网可立即选择新的跳频。为了使不同微微网之间的跳频可行，数据流体系中设有保护时间，以防止不同微微网的时隙差异。蓝牙系统中引入了保持模式后，允许一个单元临时离开一个微微网去访问另一个微微网(保持模式也可在离开一个微微网后无新的微微网访问期间作为附加的低功率模式)。

3.3 ZigBee 技术

3.3.1 ZigBee 技术概述

1. ZigBee 的起源

ZigBee 这个名称来源于蜜蜂的八字舞。ZigBee 是基于 IEEE 802.15.4 标准的低功耗局域网协议，用于实现类似蜂群通信的低功耗、低复杂度、低速率、自组织的短距离无线通信网络，为个人或者家庭范围内不同设备之间的低速互连提供统一的标准。

长期以来，工业控制和自动化领域一直存在低价格、低传输率、短距离、低功耗无线通信组网的需求。蓝牙技术的出现曾让市场雀跃不已，但是蓝牙系统具有售价居高不下、建立连

接时间长、功耗大、组网规模太小的缺点，不能满足工业自动化生产的需要。此外，工业自动化生产需要的无线数据传输必须具有高可靠性，能够抵抗工业自动化生产现场的各种电磁干扰。

基于这种应用需求，IEEE 802.15.4 工作组于 2001 年成立了 TG4 工作组，制定了 IEEE 802.15.4 标准。同年，ZigBee 联盟正式成立。2004 年，ZigBee V1.0 协议正式发布，成为 ZigBee 的第一个规范。由于 ZigBee V1.0 协议的推出比较仓促，因此存在一些错误，于是该工作组于 2006 年又推出了 ZigBee 2006，它比上一个版本更为完善。于 2007 年 12 月推出的，ZigBee PRO 和 2009 年 3 月推出的 ZigBee RF4CE 具备了更强的灵活性和远程控制能力。从 2009 年开始，ZigBee 采用了 IETF 6LoWPAN（IPv6 over IEEE 802.15.4）标准。作为新一代智能能源标准，它致力于形成全球统一且易于与互联网集成的网络，实现端到端的网络通信。

2. ZigBee 技术的特点

ZigBee 技术是一种双向无线通信技术，具有低功耗、低成本、低速率、近距离、短延迟、高容量、高安全、免执照频段等特点，适用于自动控制和远程控制领域，可以嵌入各种设备。ZigBee 技术的目标是建立一个无所不在的传感器网络，同时支持地理定位等功能。

（1）低功耗。在低耗电待机模式下，两节 5 号干电池可支持 1 个结点工作 6～24 个月甚至更长。这是 ZigBee 技术的突出优势。相比之下，蓝牙系统仅能工作几周，WiFi 仅可工作几小时。由美国的德州仪器公司和德国的 Micropelt 公司共同推出新能源的 ZigBee 结点，采用了 Micropelt 公司的热电发电机给德州仪器公司的 ZigBee 系统提供电源。

（2）低成本。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，ZigBee 系统中全功能的主结点需要 32KB 代码，子功能结点仅需 4KB 的代码且免协议专利费。芯片价格大约为 2 美元。

（3）低速率。ZigBee 系统工作时的传输速率为 20～250kb/s，分别提供 250kb/s（2.4GHz）、40kb/s（915MHz）和 20kb/s（868MHz）的原始数据吞吐率，满足低速率传输数据的应用需求。

（4）近距离。传输范围一般为 10～100m，提高发射功率后，也可增加到1～3km（指相邻结点间的距离）。如果通过路由和结点间通信的接力，传输距离将可以更远。

（5）短延迟。ZigBee 系统的响应速度较快，一般从睡眠转入工作状态只需 15ms，结点连接进入网络只需 30ms，进一步节省了电能。而蓝牙需要 3～10s，WiFi 需要 3s。

（6）高容量。ZigBee 系统可采用星形、树状和网状结构，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 65 000 个结点的大网。

（7）高安全。ZigBee 技术提供了三级安全模式，包括无安全设定、使用访问控制清单防止非法获取数据，以及采用高级加密标准的对称密码，以灵活确定其安全属性。

（8）免执照频段。使用的 ISM 频段包括 915MHz（美国）、868MHz（欧洲）和 2.4GHz（全球）。这 3 个频段的物理层并不相同，各自信道带宽也不同，分别为0.6MHz、2MHz 和 5MHz，分别有 1 个、10 个和 16 个信道。这 3 个频段的扩频和调制方式也有区别。扩频都使用直接序列扩频（DSSS），但从二进制数据位到码片（chip）的变换差别较大。调制方式都用了调相技术，但 868MHz 和 915MHz 频段采用的是 BPSK，而 2.4GHz 频段采用的是

OQPSK。

在发射功率为 0dBm 的情况下，蓝牙系统的作用范围通常为 10m，而 ZigBee 系统的作用范围在室内通常能达到 30～50m，在室外空旷地带甚至可以达 400m（TI CC2530 不加功率放大），所以 ZigBee 技术可归为低速率的短距离无线通信技术。

如今，ZigBee 网络系统已经应用于智能家居、工业自动化、农业、医疗监控等领域。随着 ZigBee 技术的不断完善，其应用范围将更加广泛。

由于 ZigBee 系统的传输速率低，因此不适合用于视频传输。此外，由于 ZigBee 采用随机媒体接入控制层且不支持时分复用的信道接入方式，因此也不能很好地支持一些实时数据传输。

3.3.2 ZigBee 网络的组成

1. ZigBee 网络的设备类型

ZigBee 标准采用一整套技术来实现可扩展的、自组织的、自恢复的无线网络，并能够管理各种数据传输模式。为了降低系统成本，ZigBee 网络依据 IEEE 802.15.4 标准定义了全功能器件（FFD）和精简功能器件（RFD）这两种类型的物理设备。表 3-4 给出了这两种物理设备的功能描述。

表 3-4 ZigBee 物理设备的功能描述

设备类型	适用的拓扑结构	功 能 描 述
FFD	星形网络、网状网络、树状网络	FFD 是具有转发与路由能力的结点，拥有足够的存储空间来存放路由信息，其处理控制能力也相应得到增强。FFD 可作为协调器或其他设备，并与任何设备进行通信
RFD	星形网络	RFD 内存小、功耗低，在网络中作为源结点，只发送与接收信号，并不起转发器或路由器的作用。RFD 不能作为协调器，只能与全功能器件通信，消耗的资源和存储开销极少

在 ZigBee 网络中，每个结点都具备一个无线电收发器、一个很小的微控制器和一个能源。这些装置互相协调工作，以确保数据在网络内进行有效的传输。一个网络只需要一个网络协调器，其他终端设备可以是 RFD，也可以是 FFD。

依据 IEEE 802.15.4 标准，ZigBee 网络在逻辑上又将这两种物理设备定义为 ZigBee 协调器、ZigBee 路由器和 ZigBee 终端设备 3 种。

（1）ZigBee 协调器是 3 类设备中最为复杂的一种。它的存储容量最大，计算能力最强，因此必须是 FFD。一个 ZigBee 网络中只能存在一个协调器。ZigBee 协调器负责发送网络信标，建立和初始化 ZigBee 网络，确定网络工作的信道以及 16 位网络地址的分配等工作。

（2）ZigBee 路由器是一个 FFD，与 IEEE 802.15.4 定义的协调器类似。在接入网络后它就自动获得一个 16 位网络地址，不但允许在其通信范围内的其他结点加入或者退出网络，而且还具有路由和转发数据的功能。

（3）ZigBee 终端设备可以由 RFD 或者 RFD 构成。它只能与父结点进行通信，并从父结点处获得网络标识符和短地址等信息。

2. ZigBee 网络的拓扑结构

ZigBee 是介于无线标记技术和蓝牙之间的技术方案，在无线传感器网络等领域应用非常广泛，这得益于它强大的组网能力。ZigBee 可以根据实际需要形成星形、树状和网状这 3 种 ZigBee 网络结构。3 种 ZigBee 网络结构各有优势。ZigBee 网络中的设备可分为协调器结点、汇聚结点、传感器结点 3 种。

1）星形拓扑

星形拓扑是最简单的一种拓扑结构，如图 3-3 所示。它包含一个协调器结点和一系列传感器结点，每一个汇聚结点只能和协调器结点进行通信。如果需要在两个汇聚结点之间进行通信必须通过协调器结点进行信息的转发。

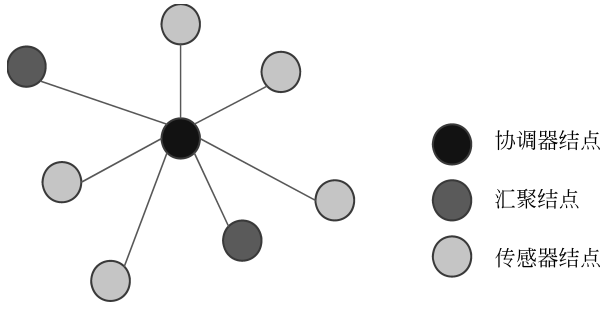

图 3-3　星形拓扑结构示意图

这种拓扑结构的缺点是结点之间的数据路由只有唯一的一条路径，协调器结点有可能成为整个网络的瓶颈。实现星形网络拓扑不需要使用 ZigBee 的网络层协议，这是因为 IEEE 802.15.4 协议的协议层就已经实现了星形拓扑形式，但是这需要开发者在应用层做更多的工作，包括自己处理信息的转发。

2）树状拓扑

树状拓扑包括一个协调器结点以及一系列的汇聚结点和传感器结点。协调器结点连接一系列的汇聚结点和传感器结点，它的子结点的汇聚结点也可以连接一系列的汇聚结点和传感器结点。以此类推，可以重复多个层级。树状拓扑的结构如图 3-4 所示。

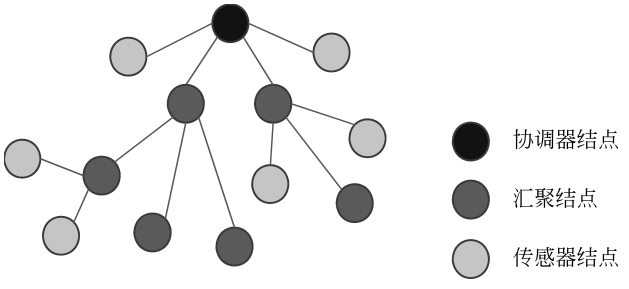

图 3-4　树状拓扑结构示意图

在树状拓扑结构中，需要注意以下 3 点。

（1）协调器结点和汇聚结点可以包含自己的子结点。

（2）有同一个父结点的结点称为兄弟结点。

(3) 有同一个祖父结点的结点称为堂兄弟结点。

树状拓扑结构的通信规则如下。

(1) 每一个结点都只能与它的父结点和子结点通信。

(2) 如果需要从一个结点向另一个结点发送数据,那么信息将沿着树的路径向上传递到最近的祖先结点,然后再向下传递到目标结点。

树状拓扑结构的缺点是信息只有唯一的路由通道。另外,信息的路由是由协议栈层处理的,整个路由过程对于应用层是完全透明的。

3) 网状拓扑

网状拓扑(Mesh 拓扑)包含一个协调器结点以及一系列的汇聚结点和传感器结点,与树状拓扑相同。但是,网状拓扑具有更加灵活的信息路由规则,在可能的情况下,路由结点之间可以直接通信。这种路由机制使信息的通信变得更有效率,而且意味着一旦一个路由路径出现了问题,信息可以自动沿着其他路由路径进行传输。网状拓扑的结构如图 3-5 所示。

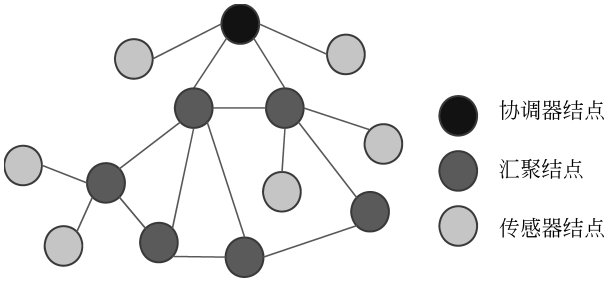

图 3-5　网状拓扑结构示意图

在网状拓扑结构的网络上,网络层通常会提供相应的路由探索功能,这一特性使网络层可以找到信息传输的最优路径。需要注意的是,以上所提到的特性都由网络层来实现,应用层不需要进行任何参与。

网状拓扑结构的网络具有强大的功能,可以组成极为复杂的网络,网络可以通过“多级跳”的方式来通信,还具备自组织、自愈功能。

3.3.3　ZigBee 协议栈的原理

作为物联网的一个典型的应用,无线传感器网络近几年受到了广泛关注。IEEE 802.15.4/ZigBee 通信协议由于其低功耗、低复杂度、自组织等特性,成为最早出现在无线传感器网络领域的无线通信协议,也是该领域最著名的无线通信协议之一。由于传感器网络和物联网具有一定的相似性,无线传感器网络也能为物联网的通信协议设计提供一些启发。

如图 3-6 所示,IEEE 802.15.4/ZigBee 采用开放系统互连(Open System Interconnect,OSI)五层模型,包括物理层、链路层、网络层、传输层和应用层。IEEE 802.15.4 标准规定了物理层和链路层的规范,物理层包括射频收发器和底层控制模块,链路层中的介质访问控制层为高层提供了访问物理信道的服务接口。ZigBee 提供了网络层、传输层和应用层规范。

1. *物理层协议规范*

ZigBee 体系结构的物理层不仅规定了信号的工作频率范围、调制方式和传输速率,还