

第3章

网络通信技术

网络通信技术(Network Communication Technology,NCT)是指通过计算机网络系统和数据通信系统实现对数据、图形和文字等形式的资料进行采集、存储、处理和传输,使信息资源达到充分共享的技术。

在信息通信领域中,发展最快、应用最广的就是无线通信技术。无线通信(Wireless Communication)是利用电磁波信号可以在自由空间中传播的特性进行信息交换的一种通信方式。

无线电波的频率从几十 kHz 到几万 MHz。为了便于应用,习惯上将无线电频率范围划分为若干区域,叫作频段或波段。

不同频段的无线电波,其传播方式、主要用途和特点也不相同。

表 3-1 列出了按波长划分的波段名称、相应波长范围和它们的主要用途。

表 3-1 无线电频段划分

波段名称	波长范围	频率范围	频段名称	传播媒质	用 途
长波	$10^3 \sim 10^4$ m	30~300kHz	LF 低频	地面波	电报、导航、长距离通信
中波	$2 \times 10^2 \sim 10^3$ m	300~1500kHz	MF 中频	天波、地面波	无线电波广播、导航、海上移动通信、地对空通信
中短波	$50 \sim 2 \times 10^2$ m	1.6~6MHz	IF	天波为主	广播中长距离通信
短波	10~50m	6~30MHz	HF 高频	电离层反射波	无线电广播通信、中长距离通信
超短波	1~10m	30~300MHz	VHF 甚高频	天波	雷达、电视、短距离通信
分米波	1~10dm	300~3000MHz	UHF 超高频	天波、空间波	短距离通信、电视通信
厘米波	1~10cm	3~30GHz	SHF 特高频	天波、外球层传播	中继通信、无线电通信
毫米波	1~10mm	30~300GHz	EHF 极高频		雷达通信
亚毫米波	1mm 以下	300GHz 以上	超极高频	光纤	光通信

信息传播过程可以简单地描述为:信源-信道-信宿。其中,信源是信息的发布者,即上传者;信宿是信息的接收者,即最终用户。信道是传送信息的物理性通道,是指由有线或无线线路提供的信号通路。习惯上,人们根据信道的不同将通信分为有线通信和无线通信两大类。

有线信道是指传输媒介为明线、对称电缆、同轴电缆、光缆及波导等一类能够看得见的媒介。有线信道是现代通信网中最常用的信道之一。如对称电缆(又称电话电缆)广泛应用于(市内)近程传输。无线信道的传输媒质比较多,它包括短波电离层、对流层散射等。可以

这样认为,凡不属于有线信道的媒质均为无线信道的媒质。无线信道的传输特性没有有线信道的传输特性稳定和可靠,但无线信道具有方便、灵活、通信者可移动等优点。

无线通信系统也称为无线电通信系统,是由发送设备、接收设备、无线信道三大部分组成的,是利用无线电波实现信息和数据传输的系统,如图 3-1 所示。

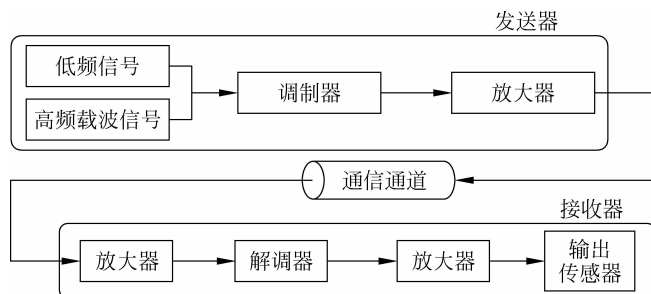


图 3-1 无线通信系统组成

一般的无线收发装置如图 3-2 所示,其中包括收发模块、接收天线和时钟晶振等模块。

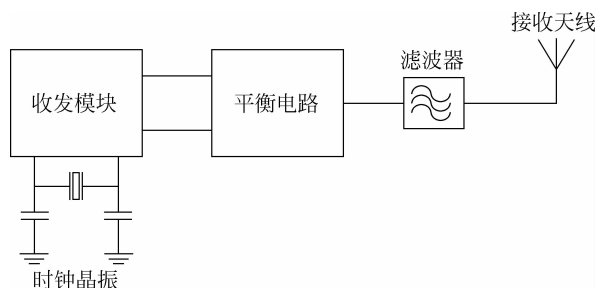


图 3-2 无线收发装置结构

无线收发装置的内部结构如图 3-3 所示。

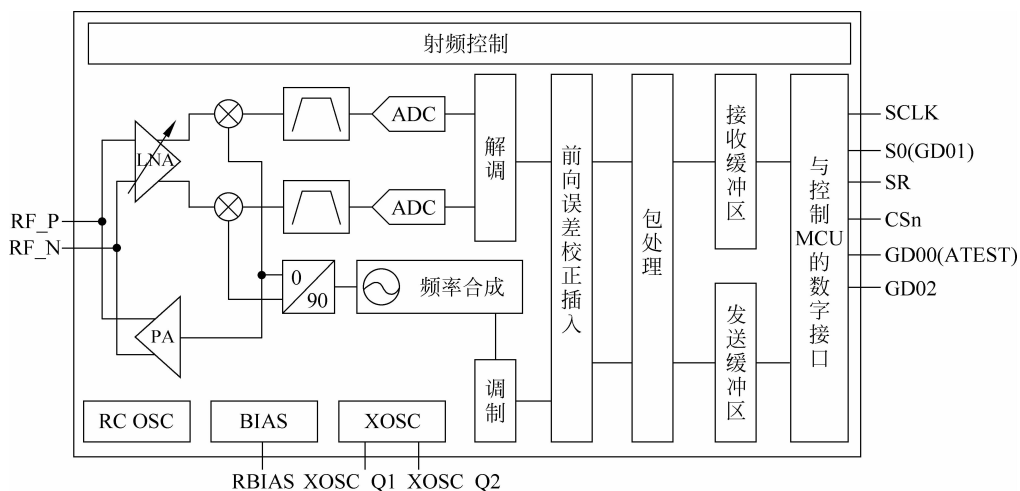


图 3-3 无线收发装置内部结构

3.1 短距离无线通信技术

短距离无线通信是指在较小的区域内(数百米)提供无线通信,它是以无线个域(Wireless Personal Area, WPA)应用为核心特征的。随着 RFID 技术、ZigBee 技术、蓝牙技术、WiFi 技术及超宽带(UWB)技术等低、高速无线应用技术的发展,短距离无线通信正深入到通信应用的各个领域,表现出广阔的应用前景。

短距离无线通信涵盖了无线个域网(Wireless Personal Area Networks, WPAN)和无线局域网(Wireless Local Area Networks, WLAN)的通信范围。短距离无线通信技术一般指作用距离在毫米级到千米级的,局部范围内的无线通信应用。其中,WPAN 的通信距离可达 10m 左右,而 WLAN 的通信距离可达 100m 左右。除此之外,通信距离在毫米至厘米量级的近距离无线通信(Near Field Communication, NFC)技术和可覆盖几百米范围的无线传感器网络(Wireless Sensor Networks, WSN)技术的出现,进一步扩展了短距离无线通信的涵盖领域和应用范围。

从通信速率看,短距离无线通信应用中既有几个千比特的低速率的 RFID 技术,也有支持高速率的可达几个吉比特的 60 GHz 毫米波个域通信(Millimeter-wave WPAN)技术;从通信模式看,有点到点(Point-to-Point)、点到多点(Point-to-multipoint)链接的蓝牙(Bluetooth)技术,也有具备网状网拓扑(Mesh Networking topology)结构的 ZigBee 技术;而红外线通信(Infrared Data Association, IrDA)和可见光通信(VisibleLight Communications, VLC)更进一步拓展了短距离无线应用的通信方式。各种短距离无线通信技术的应用范围既有相互交叉重叠,也彼此补充。

短距离无线通信中,各项技术及性能指标有所不同,但也有一些共同特点:

(1) 低功耗(Low Power)。由于短距离无线应用的便携性和移动特性,低功耗是基本要求。另一方面,多种短距离无线应用可能处于同一环境之下,如 WLAN 和微波 RFID,在满足服务质量的要求下,要求有更低的输出功率,避免造成相互干扰。

(2) 低成本(Low Cost)。短距离无线应用与消费电子产品联系密切,低成本是短距离无线应用能否推广普及的重要决定因素。此外,如 RFID 和 WSN 应用,需要大量使用或大规模铺设,成本成为技术实施的关键。

(3) 多在室内环境(Indoor Environments)下应用。与其他无线通信不同,由于作用距离限制,大部分短距离应用的主要工作环境是在室内,特别是 WPAN 应用。

(4) 使用 ISM 频段。考虑到产品和协议的通用性及民用特性,短距离无线技术基本上使用免许可证 ISM(Industrial, Scientific and Medical)频段。

(5) 电池供电(Battery Driven)的收发装置。短距离无线应用设备一般都有小型化、移动性要求。在采用电池供电后,需要进一步加强低功耗设计和电源管理技术的研究。

3.1.1 WiFi

WiFi 技术,就是把笔记本中的无线网卡虚拟成两个无线空间,充当两种角色:当与其他 AP(无线信号发射点)相连时,相当于一个普通的终端设备,这是传统应用模式;当与其

他无线网络终端设备(如计算机、手机、打印机等)连接时,可作为一个基础 AP,此时只要作为 AP 的笔记本能通过无线、有线、3G 等方式接入网,那么与之连接的其他无线网络终端设备就可以同时上网了。从使用上来看,英特尔的“My WiFi”技术和最近几年兴起的“闪联”标准类似。

1. 基本概念

WiFi 全称 Wireless Fidelity,又称 802.11b 标准,是 IEEE 定义的一个无线网络通信的工业标准(IEEE 802.11)。802.11b 定义了使用直接序列扩频(Direct Sequence Spread Spectrum, DSSS)调制技术在 2.4GHz 频带实现 11Mb/s 速率的无线传输,在信号较弱或有干扰的情况下,宽带可调整为 5.5Mb/s、2Mb/s 和 1Mb/s。

WiFi 是由 AP(Access Point,无线访问节点)和无线网卡组成的无线网络,AP 是当作传统的有线局域网络与无线局域网络之间的桥梁,其工作原理相当于一个内置无线发射器的 HUB 或者是路由;无线网卡则是负责接收由 AP 所发射信号的客户端设备。因此,任何一台装有无线路网卡的 PC 均可透过 AP 分享有线局域网络甚至广域网络的资源。

最早的 802.11 无线局域网标准是 802.11b 标准。802.11b 工作在 2.4GHz 的频段,采用 DSSS 技术和 CCK 编码方式,使数据传输速率达到 11Mb/s。

几乎和 802.11b 同时制定的是 802.11a 标准,802.11a 工作在 5GHz 开放 ISM 频段,采用 OFDM 技术,数据传输速率高达 54Mb/s。

802.11b 由于工作在低频段,成本低而获得了广泛的应用,但其数据传输速率低,为此在 802.11b 和 802.11a 的基础上又诞生了 802.11g 标准。802.11g 工作在 2.4GHz,采用 OFDM 技术,数据传输速率达到了 54Mb/s,并兼容 802.11b 标准。

然后,在 2004 年 1 月,IEEE 成立了一个新的工作组制定速度更高的标准,这就是 802.11n,802.11n 可以工作在 2.4GHz 或 5GHz,采用 OFDM 技术,同时又引入 MIMO 技术,使得数据传输速率达到了 270Mb/s 甚至高达 540Mb/s。

除了 WiFi 这种无线网络之外,还有其他通信范围和速率的不同的无线技术,如图 3-4 所示。

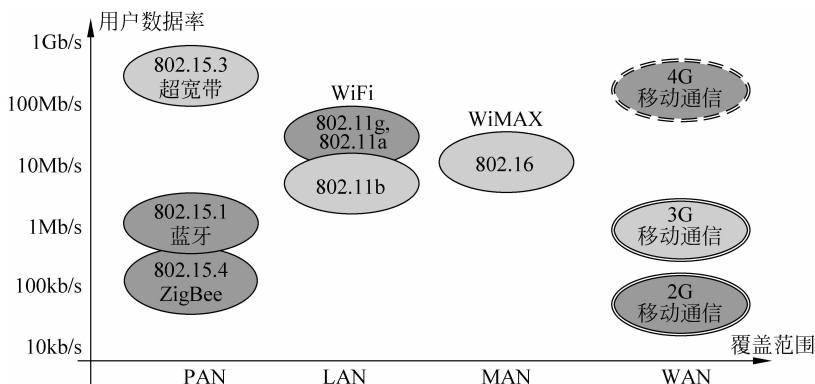


图 3-4 几种无线网络的比较

2. WiFi 的两种工作模式

WiFi 有两种工作模式：一种是有基站的模式，一种是无基站的模式，如图 3-5 所示。

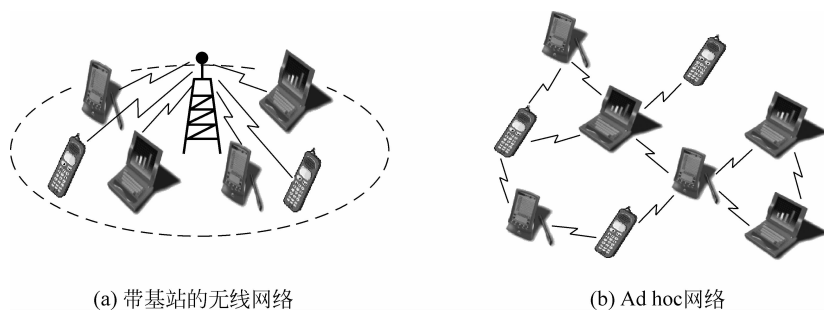


图 3-5 WiFi 的网络模式

在第一种情况下，所有的通信都经过基站，按照 802.11 的术语，基站称为访问点 (Access Point)。在第二种情况下，计算机互相之间直接发送数据，这种模式有时候也称为 Ad hoc 网络 (Ad hoc networking)。

3. WiFi 网络结构和原理

IEEE 802.11 标准定义了介质访问接入控制层 (MAC 层) 和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上，总数据传输速率设计为 2Mb/s(802.11b)~54Mb/s(802.11g)。如图 3-6 所示为 802.11 的标准和分层。

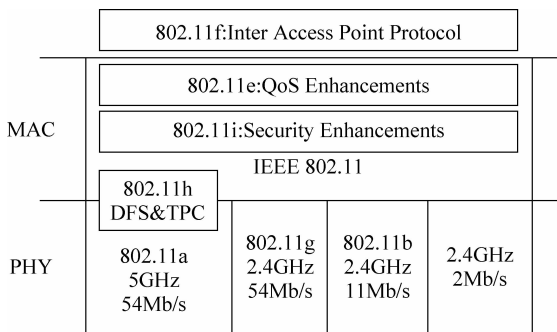


图 3-6 802.11 标准和分层

在 802.11 的物理层，IEEE 802.11 规范是在 1997 年 8 月提出的，规定工作在 ISM 2.4~2.4835GHz 频段的无线电波，采用了两种扩频技术 DSSS 和 FHSS。

一种是工作在 2.4GHz 的跳频模式，使用 70 个工作频道，FSK 调制，0.5MBPS 通信速率。工作原理如图 3-7 所示。

与 IEEE 802.11 不同，IEEE 802.11b 发布于 1999 年 9 月，它只采用 2.4GHz 的 ISM 频段的无线电波，且采用加强版的 DSSS，可以根据环境的变化在 11Mb/s、5Mb/s、2Mb/s 和 1Mb/s 之间动态切换。目前 802.11b 协议是当前最为广泛的 WLAN 标准。

一个 WiFi 连接点、网络成员和结构站点 (Station) 是网络最基本的组成部分。

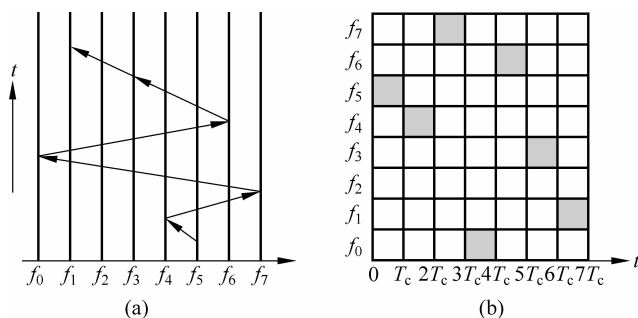


图 3-7 使用跳频工作原理

(1) 基本服务单元(Basic Service Set, BSS)。网络最基本的服务单元。最简单的服务单元可以只由两个站点组成。两个设备之间的通信可以自由直接(Ad hoc)的方式进行,也可以在基站(Base Station, BS)或者访问点(Access Point, AP)的协调下进行,也称为Infrastructure 模式。站点可以动态地连接(associate)到基本服务单元中。

(2) 分配系统(Distribution System, DS)。分配系统用于连接不同的基本服务单元。分配系统使用的媒介(Medium)逻辑上和基本服务单元使用的媒介是截然分开的,尽管它们物理上可能会是同一个媒介,例如同一个无线频段。

(3) 接入点(Access Point, AP)。接入点既有普通站点身份,又有接入到分配系统功能。

(4) 扩展服务单元(Extended Service Set, ESS)。由分配系统和基本服务单元组合而成。这种组合是逻辑上的,并非物理上的,不同的基本服务单元有可能在地理位置上相去甚远。分配系统也可以使用各种各样的技术。

(5) 关口(Portal)。也是一个逻辑成分。用于将无线局域网和有线局域网或其他网络联系起来。

这里的媒介有三种,站点使用的无线的媒介、分配系统使用的媒介以及和无线局域网集成在一起的其他局域网使用的媒介。物理上它们可能互相重叠。IEEE 802.11 只负责在站点使用的无线媒介上的寻址,分配系统和其他局域网的寻址不属于无线局域网的范围。

WiFi 网络的结构如图 3-8 所示。

802.11 网络底层和以太网 802.3 结构相同,相关数据包装,也使用 IP 通信标准和服务,完成互联网连接,具体 IP 数据结构和 IP 通信软件结构如图 3-9 所示。

4. WiFi 技术的特点

WiFi 技术的优点:

1) 较广的无线电波的覆盖范围

WiFi 的覆盖半径可达 100m,适合办公室及单位楼层内部使用。而蓝牙技术只能覆盖 15m 左右。

2) 传输速度快,可靠性高

802.11b 无线网络规范是 IEEE 802.11 网络规范的变种,最高带宽为 11Mb/s,在信号较弱或有干扰的情况下,带宽可调整为 5.5Mb/s、2Mb/s 和 1Mb/s,带宽的自动调整,有效

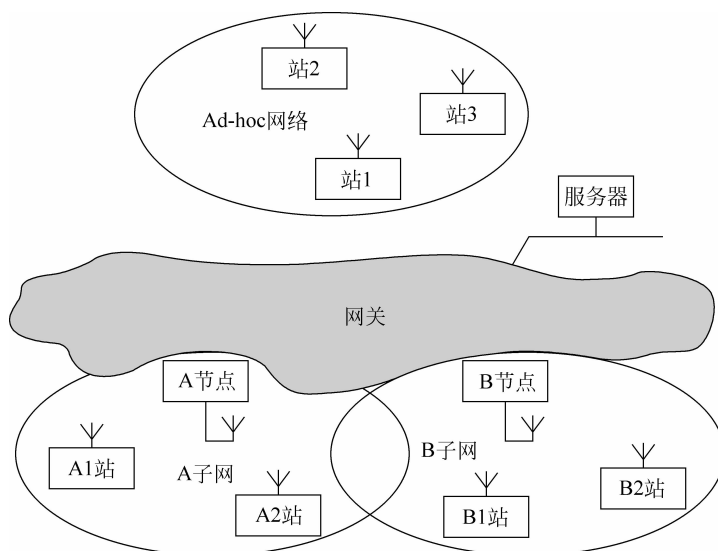


图 3-8 802.11 两种主要网络通信结构

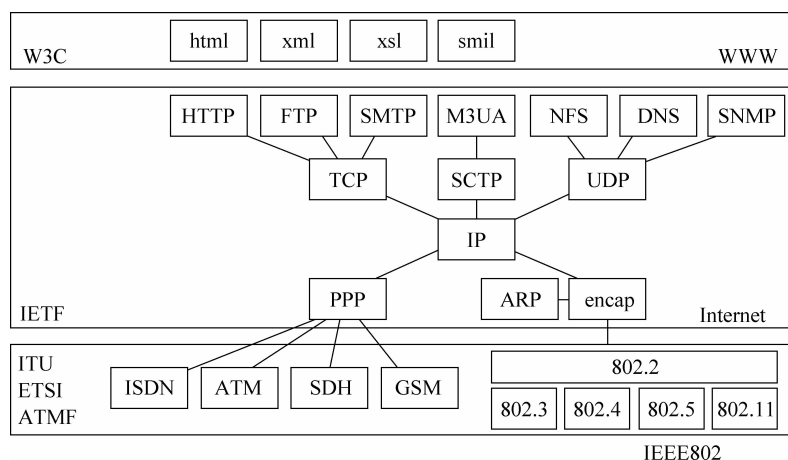


图 3-9 802.11 的 IP 网络结构

地保障了网络的稳定性和可靠性。

3) 无须布线

WiFi 最主要的优势在于不需要布线,可以不受布线条件的限制,因此非常适合移动办公用户的需要,具有广阔市场前景。在机场、车站、咖啡店、图书馆等人员较密集的地方设置“热点”,并通过高速线路将因特网接入上述场所,用户只要将支持 WiFi 的笔记本或 PDA 拿到该区域内,即可高速接入因特网。目前它已经从传统的医疗保健、库存控制和管理服务等特殊行业向更多行业拓展开去,甚至开始进入家庭及教育机构等领域。

4) 健康安全

IEEE 802.11 规定的发射功率不可超过 100mW,实际发射功率约 60~70mW,手机的发射功率约 200mW~1W,手持式对讲机高达 5W,而且无线网络使用方式并非像手机直接

接触人体, WiFi 产品的辐射更小, 是绝对安全的。

WiFi 技术也有它的缺点。

首先是它的覆盖面有限, 一般的 WiFi 网络覆盖面只有 100m 左右。其次它的移动性不佳, 只有在静止或者步行的情况下使用才能保证其通信质量。为了改善 WiFi 网络覆盖面积有限和低移动性的缺点, 最近又提出了 802.11n 协议草案。802.11n 相比前面的标准技术优势明显, 在传输速率方面, 802.11n 可以将 WLAN 的传输速率由目前 802.11b/g 提供的 54Mb/s 提高到 300Mb/s 甚至 600Mb/s。在覆盖范围方面, 802.11n 采用智能天线技术, 可以动态调整波束, 保证让 WLAN 用户接收到稳定的信号, 并可以减少其他信号的干扰, 因此它的覆盖范围可扩大到几平方千米。这使得原来需要多台 802.11b/g 设备的地方, 只需要一台 802.11n 产品就可以了。不仅方便了使用, 还减少了原来多台 802.11b/g 产品互相关联时可能出现的盲点, 使得终端移动性得到了一定的提高。

5. WiFi 技术的应用

由于 WiFi 的频段在世界范围内是无须任何电信运营执照的免费频段, 因此 WLAN 无线设备提供了一个世界范围内可以使用的, 费用极其低廉且数据带宽极高的无线空中接口。用户可以在 WiFi 覆盖区域内快速浏览网页, 随时随地接听拨打电话, 而其他一些基于 WLAN 的宽带数据应用, 如流媒体、网络游戏等功能更是值得用户期待。有了 WiFi 功能人们打长途电话(包括国际长途)、浏览网页、收发电子邮件、音乐下载、数码照片传递等, 再无须担心速度慢和花费高的问题。

WiFi 在掌上设备上的应用越来越广泛, 而智能手机就是其中一分子。与之前应用于手机上的蓝牙技术不同, WiFi 具有更大的覆盖范围和更高的传输速率, 因此 WiFi 手机成为目前移动通信业界的时尚潮流。

现在 WiFi 的覆盖范围在国内越来越广泛了, 高级宾馆、豪华住宅区、飞机场以及咖啡厅之类的区域都有 WiFi 接口。当人们去旅游、办公时, 就可以在这些场所使用掌上设备尽情网上冲浪了。

随着 3G 时代的来临, 越来越多的电信运营商也将目光投向了 WiFi 技术, WiFi 覆盖小带宽高, 3G 覆盖大带宽低, 两种技术有着相互对立的优缺点, 取长补短相得益彰。WiFi 技术低成本、无线、高速的特征非常符合 3G 时代的应用要求。在手机的 3G 业务方面, 目前支持 WiFi 的智能手机可以轻松地通过 AP 实现对互联网的浏览。随着 VOIP 软件的发展, 以 Skype 为代表的 VOIP 软件已经可以支持多种操作系统。在装有 WiFi 模块的智能手机上装上相应的 VOIP 软件后就可以通过 WiFi 网络来实现语音通话。所以 3G 与 WiFi 是不矛盾的, 而 WiFi 可以作为 3G 的高效有利的补充。

在网络高速发展的时代, 人们已经尝到了 WiFi 带来的便利。我们坚信 WiFi 与 3G 的融合必定会开启一个全新的通信时代。

3.1.2 ZigBee

ZigBee 这一名称来源于蜜蜂的八字舞。由于蜜蜂(bee)是靠飞翔和“嗡嗡”(zig)地抖动翅膀的“舞蹈”来与同伴传递花粉所在方位信息的, 也就是说, 蜜蜂依靠这样的方式构建了群体中的通信网络。

ZigBee 是规定了一系列短距离无线网络的数据传输速率通信协议的标准,主要用于近距离无线连接。基于这一标准的设备工作在 868MHz、915MHz、2.4GHz 频带上。最大数据传输率为 250kb/s。ZigBee 具有低功耗、低速率、低时延等特性。在很多 ZigBee 应用中,无线设备的活动时间有限,大多数时间均工作在省电模式(睡眠模式)下。因此,ZigBee 设备可以在不更换电池的情况下连续工作几年。

1. ZigBee 技术的概述

ZigBee 技术有别于 GSM、GPRS 等广域无线通信技术和 IEEE 802.11a、IEEE 802.11b 等无线局域网技术,其有效通信距离在几米到几十米之间,属于个人区域网络(Personal Area Network, PAN)的范畴。IEEE 802 委员会制定了三种无线 PAN 技术:适合多媒体应用的高速标准 IEEE 802.15.3;基于蓝牙技术,适合语音和中等速率数据通信的 IEEE 802.15.1;适合无线控制和自动化应用的较低速率的 IEEE 802.15.4,也就是 ZigBee 技术。得益于较低的通信速率及成熟的无线芯片技术,ZigBee 设备的复杂度、功耗和成本等均较低,适于嵌入到各种电子设备中,服务于无线控制和低速率数据传输等业务。

1) ZigBee 信道

IEEE 802.15.4 定义了两个物理层标准,分别是 2.4GHz 物理层和 868/915MHz 物理层。两者均基于直接序列扩频(Direct Sequence Spread Spectrum, DSSS)技术。

ZigBee 使用了三个频段,定义了 27 个物理信道,其中 868MHz 频段定义了一个信道;915MHz 频段附近定义了 10 个信道,信道间隔为 2MHz;2.4GHz 频段定义了 16 个信道,信道间隔为 5MHz。

具体信道分配如表 3-2 所示。

表 3-2 信道分配表

信道编号	中心频率/MHz	信道间隔/MHz	频率上限/MHz	频率下限/MHz
$k=0$	868.3		868.6	868.0
$k=1,2,3\cdots 10$	$906+2(k-1)$	2	928.0	902.0
$k=11,12,13\cdots 26$	$2401+5(k-11)$	5	2483.5	2400.0

其中,在 2.4GHz 的物理层,数据传输速率为 250kb/s;在 915MHz 的物理层,数据传输速率为 40kb/s;在 868MHz 的物理层,数据传输速率为 20kb/s。

2) ZigBee 的 PANID

PANID 其全称是 Personal Area Network ID,网络的 ID(即网络标识符),是针对一个或多个应用的网络,用于区分不同的 ZigBee 网络,所有节点的 PANID 唯一,一个网络只有一个 PANID,它是由协调器生成的,PANID 是可选配置项,用来控制 ZigBee 路由器和终端节点要加入哪个网络。

PANID 是一个 32 位标识,范围为 0x0000~0xFFFF。

3) ZigBee 物理地址

ZigBee 设备有两种类型的地址:物理地址和网络地址。

物理地址是一个 64 位 IEEE 地址,即 MAC 地址,通常也称为长地址。64 位地址是全球唯一的地址,设备将在它的生命周期中一直拥有它。它通常由制造商或者被安装时设置。

这些地址由 IEEE 来维护和分配。

16 位网络地址是当设备加入网络后分配的,通常也称为短地址。它在网络中是唯一的,用来在网络中鉴别设备和发送数据,当然不同的网络 16 位短地址可能是相同的。

2. ZigBee 技术的特点

ZigBee 传感器网络的节点、路由器、网关,都是由一个单片机+ZigBee 兼容无线收发器构成的硬件为基础或者一个 ZigBee 兼容的无线单片机(例如 CC2530),其内部都运行同一套软件来实现,这套软件由 C 语言代码写成,大约有数十万行。

ZigBee 的设计目标是在保证低耗电性的前提下,开发一种易部署、低复杂度、低成本、短距离、低速率、自组织的无线网络,在工业控制、家庭智能化、无线传感器网络等领域有广泛的应用前景。简而言之,ZigBee 就是一种便宜的、低功耗的近距离无线组网技术。

ZigBee 技术的特点主要有:

(1) 低功耗。低功耗意味着较高的可靠性和可维护性,更适合体积小的大量日常应用。工作模式下,ZigBee 技术传输速率低,传输数据量很小,因此信号的收发时间很短。其次,在非工作模式时,ZigBee 节点处于休眠模式。设备搜索时延一般为 30ms,休眠激活时延为 15ms,活动设备信道接入时延为 15ms。由于工作时间较短、收发信息功耗较低且采用了休眠模式,使得 ZigBee 节点非常省电。ZigBee 节点的电池工作时间可以长达 6 个月到两年左右,对于某些占空比 $[\text{工作时间}/(\text{工作时间}+\text{休眠时间})]$ 小于 1%的应用,电池的寿命甚至可以超过 10 年。相比较,蓝牙仅能工作数周,WiFi 仅可工作数小时。

(2) 低成本。对用户来说,低成本意味着较低的设备费用、安装费用和维护费用,ZigBee 设备可以在标准电池供电的条件下(低成本)工作,而不需要任何重换电池或充电操作(低成本、易安装);通过大幅简化协议,降低了对节点存储和计算能力的要求。根据研究,以 8051 的 8 位微控制器测算,全功能设备需要 32KB 代码,精简功能设备仅需要 4KB 代码,而且 ZigBee 协议免专利费。

(3) 低速率。ZigBee 工作在 20~250kb/s 的较低速率,分别提供 250kb/s(2.4GHz)、40kb/s(915MHz)和 20kb/s(868MHz)的原始数据吞吐率,能够满足低速率传输数据的应用需求。

(4) 近距离。ZigBee 设备点对点传输范围一般介于 10~100m 之间。在增加射频发射功率后,传输范围可增加到 1~3km。如果通过路由和节点间的转发,传输距离可以更远。

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

(6) 网络容量大。ZigBee 通过使用 IEEE 802.15.4 标准的 PHY 和 MAC 层,支持几乎任意数目的设备。ZigBee 低速率、低功耗和短距离传输的特点使它非常适宜支持简单器件。ZigBee 定义了两种器件:全功能器件(FFD)和简化功能器件(RFD)。对于全功能器件,要求它支持所有的 49 个基本参数。而对于简化功能器件,在最小配置时只要求它支持 38 个基本参数。一个全功能器件可以与简化功能器件和其他全功能器件通话,可以按三种方式工作,分别为个域网协调器、协调器或器件。而简化功能器件只能与全功能器件通话,仅用于非常简单的应用。一个 ZigBee 的网络最多包括 255 个 ZigBee 网络节点,其中一个为主控设备,其余则是从属设备。若是通过网络协调器,整个网络最多可以支持超过 64 000

个 ZigBee 网络节点,再加上各个网络协调器可互相连接,整个 ZigBee 网络节点的数目将十分可观。

(7) 高安全。ZigBee 提供了基于循环冗余校验(CRC)的数据包完整性检查功能,支持鉴权和认证,采用了 AES-128 的加密算法,各个应用可以灵活确定其安全属性。ZigBee 提供了数据完整性检查和鉴权功能,在数据传输中提供了第三级安全性。第三级安全级别在数据传输中采用 AES 的对称密码。AES 可以用来保护数据净荷和防止攻击者冒充合法用户。

(8) 数据传输可靠。ZigBee 的媒质接入控制层(MAC 层)采用 talk-when-ready 的碰撞避免机制。在这种完全确认的数据传输机制下,当有数据传送需求时则立刻传送,发送的每个数据分组都必须等待接收方的确认信息,并进行确认信息回复。若没有得到确认信息的回复就表示发生了冲突,将重传一次。采用这种方法可以提高系统信息传输的可靠性。ZigBee 为需要固定带宽的通信业务预留了专用时隙,避免了发送数据时的竞争和冲突。同时,ZigBee 针对时延敏感的应用做了优化,通信时延和休眠状态激活的时延都非常短。

(9) 免执照频段。ZigBee 设备物理层采用工业、科学、医疗(ISM)频段。

表 3-3 为 ZigBee 技术的主要特征。

表 3-3 ZigBee 技术的主要特征

特 性	取 值	特 性	取 值
数据速率	868MHz; 20kb/s; 915MHz; 40kb/s; 2.4GHz; 250kb/s	频段	868/915MHz; 2.4GHz
通信范围	10~20m	寻址方式	64b; IEEE 地址,8b 网络地址
通信时延	≥15ms	信道接入	非时隙 CSMA-CA; 有时隙 CSMA-CA
信道数	868/915MHz; 11; 2.4GHz; 16	温度	-40~85℃

3. ZigBee 网络拓扑

ZigBee 采用 IEEE 802.15.4 标准作为物理层(PHY)和媒体访问控制子层(MAC)标准,ZigBee 联盟在此基础上建立了网络层(NWK)和应用层构架。应用层构架由应用支持子层(APS)、ZigBee 设备对象(ZDO)和制造商定义的应用对象组成。ZigBee 用于组建低速率、低功耗的无线个域网(LR WPAN)。网络的基本组成单元是设备,在同一个物理信道范围内,两个或者两个以上的设备可以构成一个无线个域网。

IEEE 802.15.4 协议中规定的 PAN 协调器、协调器、一般在 ZigBee 网络中被称为 ZigBee 协调器、路由器和终端设备。一个 ZigBee 网络由一个协调器节点、多个路由器和多个终端设备节点组成。协调器的主要功能是建立网络,并对网络进行相关配置,它是网络上的第一个设备。协调器首先选择一个信道和网络标识(PAN ID),然后开始这个网络。协调器也可以辅助建立安全和应用等级绑定在网络中。一旦网络建立完成,协调器的作用就像路由器节点(或者甚至可以离开),网络的后续操作不依赖这个协调器的存在。路由器的主要功能是寻找、建立和修复网络报文的路由信息,并转发网络报文。路由器允许其他设备加入网络,多跳路由和协助它自己的由电池供电的子终端设备的通信。通常,路由器全时间处

在活动状态,因此对能源消耗较大。网络终端的功能相对简单,它可以加入、退出网络,可以发送、接收网络报文。终端设备不能转发报文。终端设备不负责网络维护,为减少能量消耗,可以进入休眠状态。

ZigBee 无线数据传输网络设备按照其功能的不同可分为全功能设备(Full-Function Device,FDD)和精简功能设备(Reduced-Function Device,RFD)两种。全功能设备可以作为无线个域网的协调器、路由器和终端设备;可以实现全部 IEEE 802.15.4 协议功能,一般在网络结构中拥有网络控制和管理的功能;一个全功能设备可以同时与多个精简功能设备和全功能设备通信。精简功能设备结构简单,造价低,一次只能与一个全功能设备通信。仅能实现部分 IEEE 802.15.4 协议功能,可以用于实现简单的控制功能,传输的数据量较少,对传输资源和通信资源占用不多,在网络结构中一般作为通信终端。由于网络中的大部分设备都是精简功能设备,因此可以组建低功耗和低成本的无线网络。

ZigBee 网络中的所有设备均有一个 64b 的 IEEE 地址,这是一个全球唯一的地址。在子网内部,协调器可以为设备分配一个 16b 的地址,作为网内通信地址,以减小数据报的大小。

地址模式有以下两种:①星状拓扑,即网络号+设备标识;②点对点拓扑,即直接使用源/目的地址。这种地址分配模式决定了每个 ZigBee 网络协调器可以支持多于 64 000 个设备,而多个协调器可以互联从而构成更大规模的网络。

ZigBee 网络有三种不同的拓扑结构,分别为:星状网,树状网和网状网。

1) 星状网络

星状拓扑结构的网络是一种发散式网络,这种网络属于集中控制型网络,在星状拓扑中,网络由一个 PAN 协调器作为中央控制器和多个从设备构成,整个网络由中心节点执行集中式通行控制管理,协调器负责发起和维护网络中的设备,以及所有其他设备,终端设备可以直接与 ZigBee 协调器通信。终端设备之间要进行通信都要先将数据发送到网络协调器,再由网络协调器将数据送到目的地节点。协调器必须是全功能设备。从设备既可以是全功能设备,也可以是精简功能设备,从设备之间的通信通过协调器转发,如图 3-10 所示。

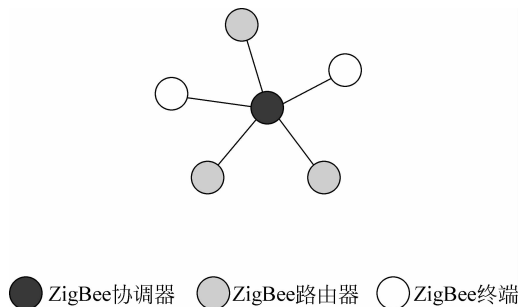


图 3-10 星状结构

这种结构中,路由器不具有路由功能。星状网络适合小范围的室内应用:比如家庭自动化、个人计算机外设以及个人健康护理等。

星状结构的网络优点:

- (1) 构造简单。
- (2) 易于管理。
- (3) 网络成本低。

星状结构的网络缺点：

- (1) 中心节点负担过重。
- (2) 节点之间灵活性差。
- (3) 网络过于简单,覆盖范围有限,只能适用于小型网络。

2) 树状网络

树状网络拓扑是由 ZigBee 协调器、若干个路由器及终端设备组成的,如图 3-11 所示。整个网络是以 ZigBee 协调器为根组成一个树状网络,树状网络中的协调器的功能不再是转发数据,而是进行网络的控制和管理功能,还可以完成节点注册。网络末端的“叶”节点为终端设备。一般而言,协调器是 FFD,终端设备是 RFD。ZigBee 协调器负责启动网络,选择某些关键的网路参数,但是网络可以通过使用 ZigBee 路由器进行扩展。

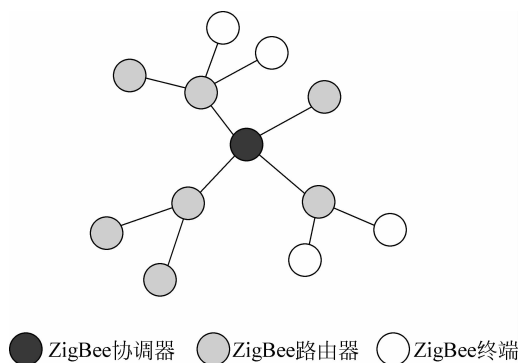


图 3-11 树状网络

树状网络的组网过程：

同星状网络一样,创建网络也需要 ZigBee 协调器完成。

如果网络中不存在其他协调器：

- (1) FFD 作为 ZigBee 协调器选择网络标识符。
- (2) ZigBee 协调器向邻近的设备发送信标,接受其他设备的连接,形成树的第一级,此时 ZigBee 协调器与这些设备之间形成父子关系。
- (3) 被协调器连接的路由器所连接的目的协调器为它分配一个地址块,路由器根据接收到的协调器信标的信息,配置自己的信标并发送到网络中,允许其他设备与自己建立连接,成为其子设备。

如果网络中存在其他协调器,ZigBee FFD 以路由器的身份与网络连接,进行上述第(3)步骤的过程。终端设备与网络连接时,则 ZigBee 协调器分配给它一个唯一的 16 位网络地址;路由器在转发消息时需要计算与目标设备的关系,并据此来决定向自己的父节点转发还是子节点转发。

树状拓扑支持“多跳”信息服务网络,可以实现网络范围扩展。树状拓扑利用路由器对星状网络进行了扩充,保持了星状拓扑的简单性。然而,树状结构路径往往不是最优的,不

能很好地适应外部的动态环境。由于信息源与目的之间只有一条通信链路,任何一个节点发生故障或者中断时,将使部分节点脱离网络。一般来说,ZigBee 是一种高可靠的无线数据传输网络,类似于 CDMA 和 GSM 网络。ZigBee 数据传输模块类似于移动网络基站。通信距离从标准的 75m 到几百米、几千米,并且支持扩展。

树状网络的优点:

- (1) 由于树状网络是对星状网络的扩充,所以其成本也较低,所需资源较少。
- (2) 网络结构简单。
- (3) 网络覆盖范围较大。

树状网络的缺点是网络稳定性较差,如果其中某节点断开,会导致与其相关联的节点脱离网络,所以这种结构的网络不适合动态变化的环境。

3) 网状网络

网状网络是 ZigBee 网络中最复杂的结构,如图 3-12 所示。在网状网络中,只要两个 FFD 设备位于彼此的无线通信范围内,它们都可以直接进行通信。也就是说,网络中的路由器可以和通信范围内的所有节点进行通信。在这种特殊的网络结构中,可以进行路由的自动建立和维护。每个 FFD 都可以完成对网络报文的路由和转发。

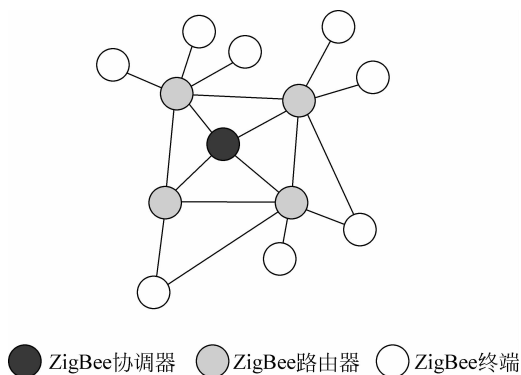


图 3-12 网状网络

网状网络采用多跳式路由通信。网络中各节点的地位是平等的,没有父子节点之分。对于没有直接相连的节点可以通过多跳转发的方式进行通信,适合距离较远比较分散的结构。

网状网络的优点:

- (1) 网络灵活性很强。节点可以通过多条路径传输数据。网络还具备自组织、自愈功能。
- (2) 网络的可靠性高。如果网络中出现节点失效,与其相关联的节点可以通过寻找其他路径与目的节点进行通信,不会影响到网络的正常运行。
- (3) 覆盖面积大。

网状网络的缺点:

- (1) 网络结构复杂。
- (2) 对节点存储能力和数据处理能力要求较高;由于网络需要进行灵活的路由选择,节点的处理数据能力和存储能力显然要求比前两种网络要更高。

一般来讲,由于和星状网络、树状网络相比,网状网络更加复杂,所以在组建网络拓扑结

构时,常常采用星状网络和树状网络。

4. ZigBee 的协议栈

ZigBee 协议栈架构是建立在 IEEE 802.15.4 标准基础上的。由于 ZigBee 技术是 ZigBee 联盟在 IEEE 802.15.4 定义的物理(PHY)层和媒体访问控制(MAC)层基础之上制定的一种低速无线个域网(LR-WPAN)技术规范,所以 ZigBee 的协议栈的物理(PHY)层和媒体访问控制(MAC)层是按照 IEEE 802.15.4 标准规定来工作的。ZigBee 联盟在其基础上定义了 ZigBee 协议的网络(NWK)层、应用层(APL)和安全服务规范,如图 3-13 所示。



图 3-13 ZigBee 协议栈结构

ZigBee 协议栈由高层应用规范、应用层、网络层、数据链路层和物理层组成,其中网络层以上的协议由 ZigBee 联盟负责,IEEE 制定物理层和链路层标准。应用层把不同的应用映射到 ZigBee 网络上,为 ZigBee 技术的实际应用提供一些应用框架模型,主要包括安全属性设置、多个业务数据流的汇聚等功能;网络层采用基于 Ad hoc

技术的路由协议,除了包含通用的网络层功能外,还应该同底层的 IEEE 802.15.4 标准同样省电;主要用于 ZigBee 网络的组网连接、数据管理和网络安全等;媒体访问控制层的功能包括信标管理、信道接入、时隙管理、发送与接收帧结构数据、提供合适的安全机制等;物理层主要完成无线收发器的启动和关闭,检测信道能量和数据传输链路质量,选择信道,空闲信道评估(CCA),以及发送和接收数据包等。

ZigBee 协议栈中,每层都为其上一层提供两种服务:数据传输服务和其他服务。其中数据传输服务由数据实体提供,其他服务由管理实体提供。

相对于常见的无线通信标准,ZigBee 协议栈紧凑而简单,其具体实现的要求很低。8 位处理器(如 80C51),再配上 4K ROM 和 64K RAM 等就可以满足其最低需要,从而大大降低了芯片的成本。ZigBee 模块如图 3-14 所示。

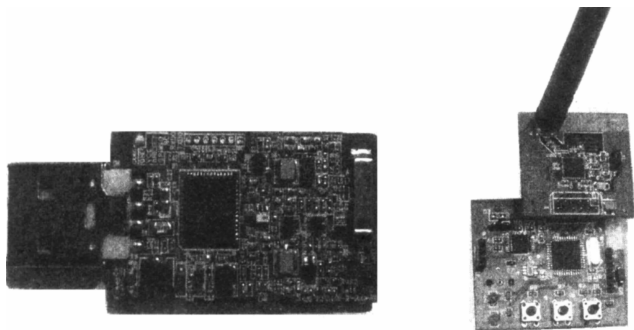


图 3-14 ZigBee 模块

5. ZigBee 应用领域

ZigBee 由于其低功耗的特性,有着广阔的应用前景,主要应用在数据传输速率不高的短距离设备之间,非常适合物联网中的传感器网络设备之间的信息传输,利用传感器和

ZigBee 网络,更方便收集数据,分析和处理也变得更简单。ZigBee 网络的冗余、自组织和自愈能力适合于许多类型的应用,主要包括数字家庭、工业控制和智慧交通等领域,如图 3-15 所示。

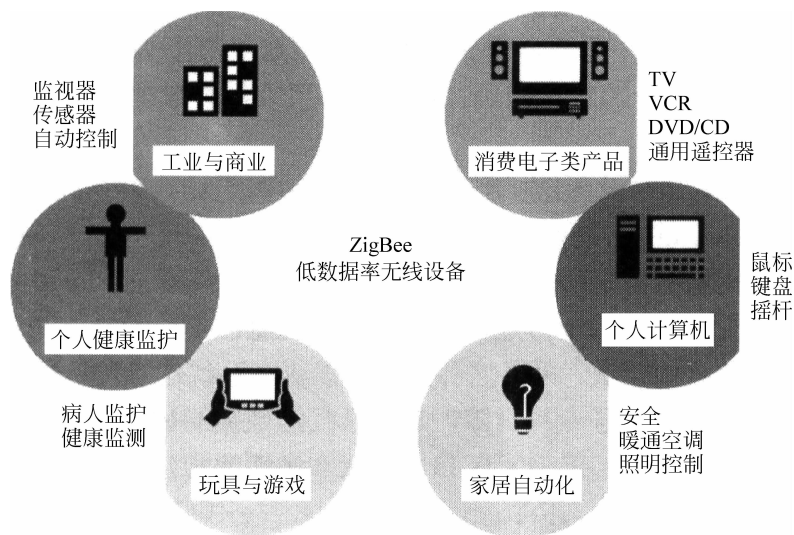


图 3-15 ZigBee 应用范围

1) 数字家庭领域

ZigBee 技术可以应用于家庭照明的自动控制、窗帘的自动控制、空调系统的温度控制、煤气计量控制、家用电器的远程控制以及安全控制等。ZigBee 模块可安装在电视、灯泡、遥控器、儿童玩具、游戏机、门禁系统、空调系统和其他家电产品等,例如,在灯泡中装置 ZigBee 模块,人们要开灯时就不需要走到墙壁开关处,直接通过遥控便可开灯。当你打开电视机时,灯光会自动减弱;当电话铃响起或你拿起话机准备打电话时,电视机会自动静音。通过 ZigBee 终端设备可以收集家庭的各种信息,传送到中央控制设备,或是通过遥控达到远程控制的目的,提供家居生活自动化、网络化与智能化。韩国第三大移动手持设备制造商 Curitel Communications 公司已经开始研制世界上第一款 ZigBee 手机。该手机将可通过无线的方式将家中或是办公室内的个人计算机、家用设备和电动开关连接起来。这种手机融入了 ZigBee 技术,能够使手机用户在短距离内操纵电动开关和控制其他电子设备。

2) 工业领域

通过 ZigBee 网络自动收集各种信息,并将信息回馈到系统进行数据处理与分析,以利工厂整体信息的掌握,例如火警的感测和通知、照明系统感测、生产机台流程控制等,都可由 ZigBee 网络提供相关信息,以达到工业与环境控制的目的。在矿井生产中,安装具有 ZigBee 功能的传感器节点可以告诉控制中心矿工的准确位置。韩国的 NURI Telecom 在基于 Atmel 和 Ember 的平台上成功研发出基于 ZigBee 技术的自动抄表系统。该系统无须手动读取电表、大天然气表及水表,从而为公用事业企业节省数百万美元,此项技术正在进行前期测试,很快将在美国市场上推出。

3) 智能交通

如果沿着街道、高速公路及其他地方分布式地部署大量 ZigBee 终端设备,人们就不会担心迷路。安装在汽车里的器件将告诉你当前所处位置,正向何处去。全球定位系统(GPS)也能提供类似服务,但是这种新的分布式系统能够提供更精确、更具体的信息。即使在 GPS 覆盖不到的楼内或隧道内,仍能继续使用此系统。从 ZigBee 无线网络系统能够得到比 GPS 多得多的信息,如限速、街道是单行线还是双行线、前面每条街道的交通情况或事故信息等。

使用这种系统,也可以跟踪公共交通情况,你可以适时地赶上下一班车,而不至于在寒风中或烈日下在车站等上数十分钟。基于 ZigBee 技术的系统还可以开发出许多其他功能,例如,在不同街道根据交通流量动态调节红绿灯,追踪超速的汽车或被盗的汽车等。

4) 精细农业

与传统农业相比,采用传感器和 ZigBee 网络以后,传感器收集包括土壤的温度、湿度、酸碱度等信息。这些信息经由 ZigBee 网络传输到中央控制设备,通过对信息的分析从而有助于指导农业种植。

5) 医疗卫生

借助于医学传感器和 ZigBee 网络,能够准确、实时地监测每个病人的血氧、血压、体温及心率等信息,从而减轻医生查房的工作负担。例如,老人与行动不便者的紧急呼叫器和医疗传感器等。

ZigBee 技术在其他领域也有着广阔的应用前景。在运动休闲领域、酒店服务行业、食品零售业中都有 ZigBee 技术的应用。在不久的将来,会有越来越多的具有 ZigBee 功能的设备进入人们的视野,这将极大地改善人民的生活。

3.1.3 蓝牙 Bluetooth

蓝牙(Bluetooth)是一个开放性的、短距离无线通信技术标准,也是目前国际上通用的一种公开的无线通信技术规范。它可以在较小的范围内,通过无线连接的方式安全、低成本、低功耗地进行网络互联,使得近距离内各种通信设备能够实现无缝资源共享,也可以实现在各种数字设备之间的语音和数据通信。目前超过 90% 的手机都具备了蓝牙功能,因此采用蓝牙技术作为物品接入互联网的方式具有广泛基础。在长时间通信中,低功耗特性非常关键,这是具有低功耗特性的蓝牙技术被广泛应用于物联网的内在动因之一。

蓝牙技术以低成本的近距离无线连接为基础,采用高速跳频(Frequency Hopping)和时分多址(Time Division Multi-access, TDMA)等先进技术,为固定与移动设备通信环境建立一个特别连接。蓝牙技术使得一些便于携带的移动通信设备和计算机设备不必借助电缆就能联网,并且能够实现无线连接因特网。例如,利用蓝牙技术,可以把任何一种原来需要通过信号传输线连接的数字设备,改为无线方式连接,并形成围绕个人的网络。无论在何处,无论是哪种数字设备在手,利用蓝牙技术都可以使其与周围的数字设备建立联系,共享这些设备中的数据库、电子邮件等。其实际应用范围还可以拓展到各种家电产品、消费电子产品和汽车等。打印机、PDA、桌上型计算机、传真机、键盘、游戏操纵杆以及所有其他的数字设备都可以成为蓝牙系统的一部分。

目前蓝牙的标准是 IEEE 802.15,工作在 2.4 GHz 频带,通道带宽为 1Mb/s,异步非对

称连接最高数据速率为 723.2kb/s。蓝牙速率也拟进一步增强,新的蓝牙标准 2.0 版支持高达 10Mb/s 以上速率(4Mb/s、8Mb/s 及 12~20Mb/s),这是适应未来愈来愈多宽带多媒体业务需求的必然演进趋势。

1. 基本原理

蓝牙是一种支持设备短距离通信(一般 10m 内)的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本、相关外设等众多设备之间进行无线信息交换。利用蓝牙技术,能够有效地简化移动通信终端设备之间的通信,也能够成功地简化设备与互联网之间的通信,从而使数据传输变得更加迅速高效,为无线通信拓宽道路。

蓝牙的基本原理是蓝牙设备依靠专用的蓝牙芯片使设备在短距离范围内发送无线电信号来寻找另一个蓝牙设备,一旦找到,相互之间便开始通信、交换信息。蓝牙的无线通信技术采用每秒 1600 次的快跳频和短分分组技术,减少干扰和信号衰弱,保证传输的可靠性;以时分方式进行全双工通信,传输速率设计为 1MHz;采用前向纠错(FEC)编码技术,减少远距离传输时的随机噪声影响。其工作频段为非授权的工业、医学、科学频段,以保证能在全球范围内使用这种无线通用接口和通信技术,语音采用抗衰弱能力很强的连续可变斜率调制(CVSD)编码方式以提高话音质量,采用频率调制方式,降低设备的复杂性。

蓝牙核心系统包括射频收发器、基带及协议堆栈。该系统可以提供设备连接服务,并支持在这些设备之间变换各种类别的数据。蓝牙采用分散式网络结构以及快跳频和短包技术,支持点对点及点对多点通信,工作在全球通用的 2.4GHz ISM(即工业、科学、医学)频段。其数据传输速率为 1Mb/s。采用时分双工传输方案实现全双工传输。它的一般连接范围是 10m,通过扩展可以达到 100m;不限制在直线的范围内,甚至设备不在同一间房内也能互相连接。蓝牙系统的网络结构为拓扑结构,有两种组网方式:微微网(Piconet)和散射网(Scatternet)。微微网(Piconet)是通过蓝牙技术连接起来的一种微型网络,如图 3-16 所示。一个微微网可以只是两台相连的设备,比如一台便携式计算机和一部移动电话,也可以是 8 台连在一起的设备。在一个微微网中,所有设备的级别是相同的,具有相同的权限。在微微网初建时,定义其中一个蓝牙设备为主设备,其余设备则为从属设备。分布式网络是由多个独立的非同步的微微网组成的,它靠调频顺序识别每个微微网。同一微微网所有用户都与这个调频顺序同步。一个分布网络中,在带有 10 个全负载的独立的微微网的情况下,全双工数据速率超过 6Mb/s。

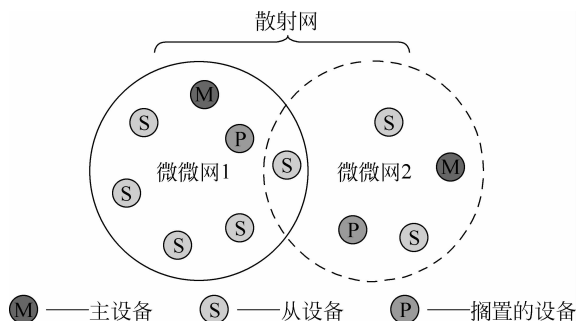


图 3-16 蓝牙系统中的微微网和散射网

2. 蓝牙网络基本结构

Bluetooth 功能一般是通过模块来实现的,但实现的方式不同。有些设备把 Bluetooth 模块内嵌到设备平台中,有些则是采用外加式。蓝牙系统由天线单元、链路控制单元、链路管理单元、软件功能 4 个单元组成,各单元间的连接关系如图 3-17 所示。

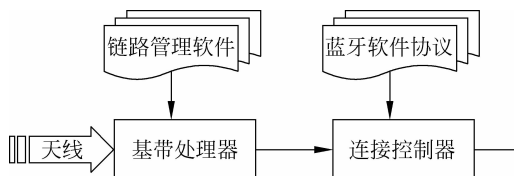


图 3-17 蓝牙系统各单元的连接关系

1) 天线单元

实现蓝牙技术的集成电路芯片要求其天线部分的体积要小、重量要轻,因此,蓝牙天线属于微带天线。蓝牙技术的空中接口是建立在天线电平为 0 dBm 的基础上的。空中接口遵循 FCC 有关电平为 0 dBm 的 ISM 频段的标准。

蓝牙系统的无线发射功率符合 FCC 关于 ISM 波段的要求,由于采用扩频技术,发射功率可增加到 100mW。系统的最大跳频为 1600 跳/秒,在 2.402~2.480GHz 之间。采用 79 个 1MHz 带宽的频点。系统的设计通信距离为 0.1~10m。如果增加发射功率,距离可以达到 100m。

2) 链路控制单元

链路控制单元由基带部分来实现,它描述了基带链路控制器的数字信号处理规范。基带链路控制器负责处理基带协议和其他一些低层常规协议。蓝牙基带协议是电路交换与分组交换的结合。在被保留的时隙中可以传输同步数据包,每个数据包以不同的频率发送。一个数据包名义上占用一个时隙,但实际上可以被扩展到占用 5 个时隙。蓝牙可以进行异步数据通信,还可以支持三个同步语音信道同时进行工作,还可用一个信道同时传送异步数据和同步语音。每个语音信道支持 64kb/s 同步语音链路。异步信道可以支持一端最大速率为 721kb/s,而另一端速率为 57.6kb/s 的不对称连接,也可以支持 43.2kb/s 的对称连接。蓝牙基带部分在物理层为用户提供保护和信息保密机制。鉴权基于“请求-响应”运算法则。鉴权是蓝牙系统中的关键部分,它允许用户为个人的蓝牙设备建立一个信任域,比如只允许主人自己的笔记本电脑通过主人自己的移动电话进行通信。连接中的个人信息由加密来保护,密钥由程序的高层来管理。网络传送协议和应用程序可以为用户提供一个较强的安全机制。

蓝牙产品的链路控制硬件单元包括三个集成器件:链路控制器、基带处理器及射频传输/接收器。此外还使用了 3~5 个单独调协元件,基带链路控制器负责处理基带协议和其他一些低层常规协议,蓝牙基带协议是电路交换与分组交换的结合。采用时分双工实现全双工传输。

3) 链路管理单元

链路管理(LM)软件模块携带了链路的数据设置、鉴权、链路硬件配置和其他一些协

议,LM 能够发现其他远端 LM,并通过 LMP(链路管理协议)与之通信。

4) 软件功能单元

蓝牙设备支持一些基本互操作的要求。对于某些设备,从无线电兼容模块、空中协议以及应用协议和对象交换格式,都要实现互操作性;另外一些设备(如头戴式设备)的要求则宽松得多。蓝牙设备必须能彼此识别并装载与之相应的软件以支持设备更高层次的性能。蓝牙对不同级别的设备(如 PC、手持机、移动电话、耳机等)有不同的要求,例如,蓝牙耳机不能提供地址簿;但配备蓝牙装置的移动电话、手持机、笔记本计算机则具有故障诊断、与外设通信、商用卡交易、号簿网络协议等功能。

蓝牙技术系统中的软件功能是一个独立的操作系统,不与任何操作系统捆绑,可确保任何带有蓝牙标记的设备都能进行互操作,它符合已制定好的蓝牙规范。

3. 蓝牙的协议栈

提出蓝牙技术协议标准的目的是,允许遵循标准的各种应用能够进行相互间的操作。为了实现互操作,在与之通信的仪器设备上的对应应用程序必须以同一协议运行。蓝牙协议栈包括蓝牙指定协议(LMP 和 L2CAP)和非蓝牙指定协议(如对象交换协议 OBEX 和用户数据报协议 UDP)。设计协议和协议栈的主要原则是尽可能利用现有的各种高层协议,以保证现有协议与蓝牙技术的融合及各种应用之间的互通性,充分利用兼容蓝牙技术标准的软硬件系统。

一个蓝牙系统在整体上可以分为底层硬件系统、中层软件系统和上层应用模型。如图 3-18 所示。蓝牙软件协议栈是整个蓝牙结构体系中的重要核心部分,是实现蓝牙各种功能的关键因素。在蓝牙主设备和从设备之间建立起一个无线连接,然后进行数据的发送与接收。蓝牙技术的整个协议体系结构分为底层硬件模块、中间协议层和高层应用框架三大部分。

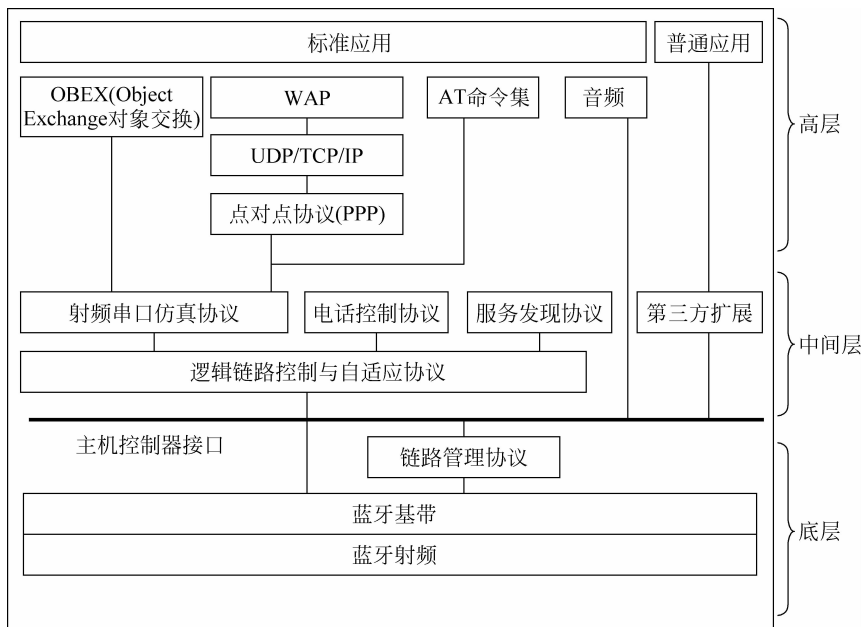


图 3-18 蓝牙技术协议结构

1) 底层硬件模块

底层硬件模块包括无线射频(RF)、基带(BB)和链路管理(LM)三层。RF层通过2.4GHz无须授权的ISM频段的微波,实现数据位流的过滤和传输,本层协议主要定义了蓝牙收发器在此频段正常工作所需满足的条件。BB层负责完成跳频和蓝牙数据及信息帧的传输。LM层负责建立和拆除链路连接,同时保证链路的安全。

2) 中间协议层

中间协议层包括逻辑链路控制与自适应协议(L2CAP)、服务搜索协议(SDP)、射频串口仿真协议(RF-COMM)和电话控制协议(TCS)4项。L2CAP主要完成数据拆装、协议复用等功能,是其他上层协议实现的基础。SDP为上层应用程序提供了一种机制来发现网络中可用的服务及其特性。RF-COMM基于ETSI标准TS07.10,在L2CAP上仿真9针RS-232串口的功能。TCS提供蓝牙设备间语音和数据呼叫控制信令。

3) 高层应用框架

高层应用框架位于蓝牙协议栈的最上部。其中较典型的应用模式有拨号网络、耳机、局域网访问、文件传输等。各种应用程序可以通过各自对应的框架实现无线通信。拨号网络应用模式可以通过RF-COMM仿真的串口访问微微网。在微微网初建时,其中一个单元被定义为主单元,其时钟和跳频顺序被用来同步其他单元的设备,其他单元被定义为从单元。数据设备也可由此接入传统的局域网。用户通过协议栈中的音频层在手机和耳塞中实现音频流的无线传输。多台PC或笔记本电脑之间不用任何连线,即可快速灵活地传输文件和共享信息,多台设备也可由此实现操作的同步。随着手机功能的不断增强,手机无线遥控也将成为蓝牙技术的主要应用方向之一。

除上述协议层外,在BB和LM上与L2CAP之间还有一个主机控制接口层(HCI)。HCI是蓝牙协议中软硬件之间的接口,它提供了一个调用下层BB、LM、状态和控制寄存器等硬件的统一命令接口。HCI位于L2CAP的下层,也可以位于L2CAP的上层。

4. 蓝牙的主要技术

蓝牙的主要技术包括无线通信与网络技术、软件工程、软件可靠性理论、协议的正确性验证技术、软硬件接口技术(如RS-232、USB等)以及高集成、低功耗芯片技术。

(1) 跳频技术。跳频是蓝牙使用的关键技术之一,数据包短,抗信号衰减能力强,并具有足够强的抗干扰能力。

(2) 射频技术。蓝牙的载频选用全球通用免费的2.4GHz ISM(Industrial Scientific Medicine)频段,无须申请许可证。

(3) 基带协议。当两个蓝牙设备成功建立链路后,Piconet便形成了,两者之间的通信通过无线电波在79个信道中随机跳转而完成。蓝牙给每个Piconet提供特定的跳转模式,因此它允许大量的Piconet同时存在。

(4) 网络特性。蓝牙支持点对点和对多点的连接,可采用无线方式将若干蓝牙设备连成一个微微网,多个微微网又可互联成特殊分散网,形成灵活的多重微微网的拓扑结构,从而实现各类设备之间的快速通信。蓝牙可以即连即用,组网灵活,具有很强的移植性,并且适用于多种场合。蓝牙的优势在于它的对等连接能力以及多重设定能力。

(5) 协议分层。蓝牙的通信协议也采用分层结构。层次结构使其设备具有最大可能的

通用性和灵活性。

(6) 安全性。采用快速跳频和前向纠错方案以保证链路稳定,减少同频干扰和远距离传输时的随机噪声影响。蓝牙系统的移动性和开放性使得安全问题极其重要,蓝牙系统所采用的跳频技术已经提供了一定的安全保障,并且在链路层中,蓝牙系统提供了认证、加密和密钥管理等功能,每个用户都有一个个人标识码(PIN),它会被译成 128b 的链路密钥来进行双向认证。

(7) 可同时支持数据、音频、视频信号传输。

(8) 全球性地址。任一蓝牙设备,都可根据 IEEE 802 标准得到唯一 48b 的 BD-ADDR。它是一个公开的地址码,可以通过人工或自动进行查询。

(9) 采用时分复用多路访问技术。基带传输速率为 1Mb/s,采用数据包的形式按时隙(Time Slot)传送数据,每时隙 0.625ms(不排除将来可能采用更高的传输速率)。每个蓝牙设备在自己的时隙中发送数据,这在一定程度上可有效避免无线通信中的“碰撞”和“隐藏终端”等问题。

5. 蓝牙的特点

蓝牙技术是一种短距离无线通信的技术规范。它最初的目标是取代现有的掌上计算机、移动电话等各种数字设备上的有线电视连接。蓝牙技术的特点如下:

1) TDMA 结构

蓝牙技术的传输速率设计为 1Mb/s,以时分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,一个跳频频率发送一个同步分组,每个分组占用一个时隙,也可以扩展到 5 个时隙。蓝牙技术支持一个异步数据通道,或三个并发的同步话音通道,或一个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,异步通道支持最大速率 721kb/s、反响应答速率为 57.6kb/s 的非对称连接,或者是 432.6kb/s 的对称连接。

2) 使用跳频技术

蓝牙技术采用跳频(FH)扩展频谱的技术来解决干扰的问题。跳频技术是把频带分成若干个跳频信道,在一次连接中,无线电收发器按一定的码序列不断地从一个信道跳到另一个信道,只有收发双方是按这个规律进行通信的,其他的干扰不可能按同样的规律进行干扰;跳频的瞬时带宽是很窄的,但通过扩展频谱技术使这个窄带宽成百倍地扩展成宽带宽,使干扰可能的影响变得很小。因此这种无线电收发器是窄带和低功率的且成本低廉,但具有很高的抗干扰性。

3) 全球范围适用

蓝牙设备工作的工作频段选在全球通用的 2.4GHz 的 ISM(即工业、科学、医学)频段。这样用户不必经过申请就可在 2400~2500Hz 范围内选用适当的蓝牙无线电收发器频段。其组件主要是芯片与无线电收发器两部分,芯片底部附有 USB 转接板,用来连接计算机电话或其他电子产品。当芯片收到电子信号后,就将其转化成无线电信号,送到无线电收发器发送出去。它能够穿过固体和非金属物质传送,其一般连接范围是从 1~10m,但通过增加传送能量的方法,其范围可扩大到 100m。

4) 组网灵活性强

设备和设备之间是平等的。无严格意义上的主设备,这使得测试设备与被测设备之间、被测设备与被测设备之间及测试设备与测试设备之间数据交换更加便利灵活。甚至被测设备也能发出测试请求,从而为测试系统的智能化提供了更可靠的保障依据,特别对于多传感数据融合测试系统具有更广泛的实用意义。

5) 成本低

为了能够替代一般电缆,蓝牙必须具备和一般电缆差不多的价格,才能被广大普通消费者所接受,也才能使这项技术普及开来,随着市场的不断扩大。各个供应商纷纷推出自己的蓝牙芯片和模块,蓝牙产品价格正飞速下降。

6. 蓝牙技术的应用

蓝牙技术把各种便携式与蜂窝移动电话用无线电链路连接起来,使计算机与通信密切结合,使人们能够随时随地进行数据信息交换与传输。蓝牙不仅可以应用于家庭网络,小范围办公,而且对个人数据通信也是非常重要的。

数据通信原本是计算机与通信相结合的产物。近年来移动通信迅速发展,便携式计算机如膝上型计算机、笔记本计算机、手持式计算机以及个人数字助理(PDA)等迅速普及,还有因特网的快速增长,使人们对电话通信以外的各种数据信息传递的需求日益增长。近来广泛使用的全球通(GSM)数字移动电话已经增加了数据通信的需求,不仅能够区分语音呼叫和数据呼叫,还能区分不同种类的数据呼叫。第三代移动通信更是把数据通信作为重要业务来考虑。无线数据通信是未来通信的主要方式。

跳频、TDD 和 TDMA 等技术的使用,使实现蓝牙技术的射频电路较为简单,通信协议的大部分内容可由专用集成电路和软件实现,保证了采用蓝牙技术的仪器设备的高性能和低成本。就目前的发展来看,蓝牙技术已经或将较快地与如下设备或系统融为一体。

1) 在手机上的应用

嵌入蓝牙芯片的移动电话已经出现,它可实现一机三用:在办公室可作为内部无线电话;回家后可当作无绳电话;在室外或乘车途中可作为移动电话与掌上计算机或个人数字助理(PDA)结合起来,并通过嵌入蓝牙技术的局域网接入点访问因特网。同时,借助嵌入蓝牙芯片的头戴式话筒和耳机及语音拨号技术,不用动手就可以接听或拨打移动电话。

2) 在掌上计算机中的应用

掌上 PC 已越来越普及,嵌入蓝牙芯片的掌上 PC 可提供各种便利。通过嵌有蓝牙芯片的掌上 PC,不仅可编写电子邮件,而且还可立即通过周围的蓝牙仪器设备发送出去。

3) 在其他数字设备上的应用

数字照相机、数字摄像机等设备装上蓝牙芯片,既可免去使用电线的不便,又可不受存储器容量有限的束缚,将所摄图片或影像通过嵌有蓝牙芯片的手机或其他设备传送到指定的计算机中。

蓝牙芯片的微型化和低成本将为它在家庭和办公室自动化、家庭娱乐、电子商务、工业控制、智能化建筑物等领域开辟广阔的应用前景。

4) 蓝牙技术在测控领域的应用

随着测控技术的不断发展,对数据传输、处理和管理提出了越来越高的自动化和智能化

要求。蓝牙技术可以在短距离内用无线接口来代替有线电缆连接,因而可以取代现场仪器之间的复杂连线,这对于需要采集大量数据的测控场合非常有用。例如,数据采集设备可以集成单独的蓝牙技术芯片,或者采用具有蓝牙芯片的单片机提供蓝牙数据接口。在采集数据时,这种设备就可以迅速地将所采集到的数据传送到附近的数据处理装置(例如 PC、笔记本、PDA)中,不仅避免了在现场铺设大量复杂连线和对这些接线是否正确的检查与核对,而且不会发生因接线可能存在的错误而造成测控的失误。与传统的以电缆和红外方式传输测控数据相比,在测控领域应用蓝牙技术的优点主要有:

(1) 抗干扰能力强。采集测控现场数据经常遇到大量的电磁干扰,而蓝牙系统因采用了跳频扩频技术,故可以有效地提高数据传输的安全性和抗干扰能力。

(2) 无须铺设缆线,降低了环境改造成本,方便了数据采集人员的工作。

(3) 没有方向上的限制,可以从各个角度进行测控数据的传输。

(4) 可以实现多个测控仪器设备间的联网,便于进行集中测量与控制。

蓝牙技术还可用于自动抄表领域。计量水、电、气、热量等的仪器仪表可通过嵌入的蓝牙芯片,将数据自动集中到附近的某个数据采集节点,再由该节点通过电力线以载波方式或电话线等传输到数据采集器以及供用水、电、气、热量等管理部门的数据处理中心。这种方式可有效地解决部分计量测试节点难以准确采集测控数据的问题。

3.1.4 超宽带技术

超宽带(Ultra-wideband, UWB)技术是一种与其他技术有很大区别的无线通信技术,与常见的通信方式使用连续的载波不同,UWB 采用极短的脉冲信号来传送信息,通常每个脉冲的持续时间只有几十皮秒到几纳秒,这些脉冲所占用的带宽甚至高达数吉赫兹(GHz),这样最大数据传输速率可以达到数百兆位每秒(Mb/s)。在高速通信的同时,UWB 设备发射的功率却很小,只有现有设备的几分之一。超宽带技术解决了困扰传统无线技术多年的有关传播方面的重大难题,具有对信道衰落不敏感、发射信号功率谱密度低、低截获能力、系统复杂度低、能提供数厘米的定位精度等优点。尤其适用于室内等密集多径场所的高速无线接入,非常适用于建立一个高效的无线局域网。

UWB 技术不仅可以缓解传统的无线技术在工业环境的通信质量下降问题,而且增加了带宽,解决了传统无线技术传输速率低,不能适应工业网络化控制系统向多媒体信息传输及监测、控制、故障诊断等多功能一体化方向发展的要求。因此建立基于 UWB 的网络化控制系统的体系结构,使控制网络系统实现定位、信息识别、控制、监测及诊断等一体化,形成真正意义的物联网具有重大的实际应用价值和意义。

1. UWB 技术的概念

UWB 技术凭借其超宽的信号带宽、较低的发射功耗以及高数据传输速率等特点,被认为是最有发展前景的无线电技术之一。近年来随着“泛在无线通信”概念的提出,无线局域网、无线个域网和无线体域网等短距离无线应用逐渐渗透到人们的生活当中。UWB 技术正是定位于短距离无线通信这一广阔的应用领域,特别是最近物联网应用的兴起,UWB 技术可以作为物联网的基础通信技术之一,实现不同设备之间的互联互通。同时 UWB 技术还可以应用于精确定位、雷达跟踪等领域,成为目前学术研究和业界关注的重点技术。

UWB 又称为超宽带冲击无线电 (Impulse Radio), 其信号带宽大于 500MHz 或信号带宽与中心频率之比大于 25%。实际上 UWB 信号是一种持续时间极短、带宽很宽的短时脉冲。它的主要形式是超短基带脉冲, 宽度一般在 0.1~20ns。脉冲间隔为 2~5000ns, 精度可控, 频谱为 50MHz~10GHz。频带大于 100% 中心频率, 典型点空比为 0.1%。传统的 UWB 系统使用一种被称为“单周期(monocycle)脉形”的脉冲。

超宽带无线通信应用大体上可以分为两类, 一类是短距离高速应用, 数据传输速率可以高达数百 Mb/s, 主要是构建短距离高速 WPAN、家庭无限多媒体网络以及替代高速短程有线连接, 如无线 USB 和 DVD 等, 典型的通信距离是 10m; 另一类中长距离(几十米以上)低速率应用, 通常数据传输速率为 1Mb/s 量级, 主要应用于无线传感器网络和低速率连接。超宽带无线通信的网络形式主要是自组织(Ad hoc)网络。就对应标准而言, 高速率应用对于 IEEE 802.15.3, 低速率应用对应于 IEEE 802.15.4。

UWB 实质上是以占空比很低的冲击脉冲作为信息载体的无载波扩谱技术, 它是通过对具有很陡上升和下降时间的冲击脉冲进行直接调制。典型的 UWB 直接发射冲击脉冲串, 不再具有传统的中频和射频的概念, 此时发射的信号既可看成基带信号(依常规无线电而言), 也可看成射频信号(从发射信号的频谱分量考虑)。

UWB 开发了一个具有吉赫兹容量和最高空间容量的新无线信道。冲击脉冲通常采用单周期高斯脉冲, 一个信息比特可映射为数百个这样的脉冲。单周期脉冲的宽度在纳秒级, 具有很宽的频谱。基于 CDMA 的 UWB 脉冲无线收发信机在发送端时钟发生器产生一定重复周期的脉冲序列, 用户要传输的信息和表示该用户地址的伪随机码分别或合成后对上述周期脉冲序列进行一定方式的调制, 调制后的脉冲序列驱动脉冲产生电路, 形成一定脉冲形状规律的脉冲序列, 然后放大到所需功率, 再耦合到 UWB 天线发射出去。在接收端, UWB 天线接收的信号经低噪声放大器放大后, 送到相关器的一个输入端, 相关器的另一个输入端加入一个本地产生的与发送端同步的经用户伪随机码调制的脉冲序列, 接收端信号与本地同步的伪随机码调制的脉冲序列一起经过相关器中的相乘、积分和取样保持运算, 产生一个对用户地址信息经过分离的信号。其中仅含用户传输信息以及其他干扰, 然后对该信号进行解调运算。

2. UWB 系统的关键技术

UWB 系统的基本模型主要由发射部分、无线信道和接收部分构成, 与传统的无线发射、接收机结构相比, UWB 的发射、接收机结构相对简单, 易于实现, 因为脉冲产生器只需产生大约 100mV 的电压就能满足发射要求, 因而发射端不需要功率放大器, 只需产生满足带宽要求的极窄脉冲即可, 在接收端, 天线收集的信号先通过低噪声放大器, 再通过一个匹配滤波器和相关接收机恢复出期望信号。UWB 无线传输的基本模型如图 3-19 所示。

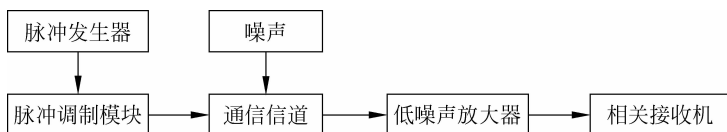


图 3-19 UWB 传输系统的基本模型

UWB 无线系统的关键技术主要包括：产生脉冲信号串(发送源)的方法、脉冲串的调制方法、适用于 UWB 有效的天线设计方法及接收机的设计方法等。

1) UWB 脉冲信号的产生

UWB 技术的前提条件是应具有产生脉冲宽度为纳秒级的信号源,单个无载波窄脉冲信号有两个突出的特点,即激励信号的波形为具有陡峭前沿的单个短脉冲和激励信号从直流(DC)到微波波段,包括很宽的频谱。

目前产生脉冲源的方法有两种：一是利用光导开关导通瞬间的陡峭上升沿获得脉冲信号的光电方法。这是最有发展前景的一种方法；二是对半导体 PN 结反向加电,使其达到雪崩状态,并在导通的瞬间取陡峭的上升沿作为脉冲信号的产生方法。这种方案目前应用最广泛,但由于采用电脉冲信号作为触发,其前沿较宽,触发精度受到限制,特别是在要求精确控制脉冲发生时间的场合,达不到控制的精度。

冲击脉冲通常采用高斯单周期脉冲,宽度在纳秒级,具有很宽的频谱。实际通信中使用的是一长串的脉冲,由于时域中的信号有重复周期性,将会造成频谱离散化,对传统无线电设备和信号产生干扰,需要通过适当的信号调整来降低这种干扰的影响。

2) 信息的调制

脉冲的幅度、位置和极性变化都可以用于传递信息。适用于 UWB 的主要单脉冲调制技术包括：脉冲幅度调制(PAM)、脉冲位置调制(PPM)、通断键控(OOK)、二相调制(BPM)和跳时、直扩二进制相移键控调制 TH/DS-BPSK 等。其中,脉冲位置调制(PPM)和脉冲幅度调制(PAM)是超宽带无线电的两种主要调制方式。

PPM 又称时间调制(TM),是用每个脉冲出现的位置超前或落后于某一标准或特定的时刻来表示某个特定信息的,因此对调制信号需要在接收端用匹配滤波的技术来正确接收,即对调制信息用交叉相关器在达到零相差的时候进行检测,否则,达不到正确接收的目的。

PAM 是用信息符号控制脉冲幅度的一种调制方式,它既可以改变脉冲幅度的极性,也可以仅改变脉冲幅度的绝对值大小。通常所讲 PAM 只改变脉冲幅度的绝对值。

BPM 和 OOK 是 PAM 的两种简化形式。BPM 通过改变脉冲的正负极性来调制二元信息,所有脉冲幅度的绝对值相同。OOK 通过脉冲的有无来传递信息。

在 PAM、BPM 和 OOK 调制中,发射脉冲的时间间隔是固定不变的。

在 UWB 系统中,采用跳时脉冲位置调制(TMPAM)对长脉冲序列进行调制时,每个用户的下一条信息将在时间上随机分布,可在频域内得到更为平坦的 RF 信号功率分布,这使得 UWB 信号在频域中类似于背景噪声。

UWB 系统中有一种典型的由伪随机序列控制的跳时信号。发射机在由伪随机序列确定的时间帧上发送一个单周期脉冲,通常单周期脉冲信号的 100 倍为随机出现的脉冲持续时间,其位置由 PN 码来确定。伪随机序列控制的跳时扩频与一般的扩频波形(直接序列扩频或跳频扩频)不同,UWB 波形的扩频带宽是直接产生的,即单个比特未经扩频序列由 PN 码调制,本质上是时域的概念。

3) 多址方式

在 UWB 系统中,多址接入方式与调制方式有密切联系。当系统采用 PPM 调制方式时,多址接入方式多采用跳时多址;若系统采用 BPSK 方式,多址接入方式通常有两种,即

直序方式和跳时方式。基于上述两种基本的多址方式,许多其他多址方式陆续提出,主要包括以下几种。

(1) 伪混沌跳时多址方式(PCTH)。PCTH 根据调制的数据产生非周期的混沌编码,用它替代 TH-PPM 中的伪随机序列和调制的数据,控制短脉冲的发送时刻,使信号的频谱发生变化。PCTH 调制不仅能减少对现有的无线通信系统的影响,而且更不易被检测到。

(2) DS-BPSK/TH 混合多址方式。此方式在跳时(TH)的基础上,通过直接序列扩频码进一步减少多址干扰,其多址性能优于 TH-PPM,与 DS-BPSK 相当。在实现同步和抗远近效应方面具有一定的优势。

(3) DS-BPSK/FixedTH 混合多址方式。此方式的特点是打破了 TH-PPM 多址方式中采用随机跳时码的常规思路,利用具有特殊结构的固定跳时码,减少不同用户脉冲信号的碰撞概率。即使有碰撞发生时,利用直接序列扩频的伪随机码的特性,也可以进一步削弱多址干扰。

此外,由于 UWB 脉冲信号具有极低的占空比,其频谱能够达到吉赫兹数量级,因而 UWB 在时域中具有其他调制方式所不具有的特性。当多个用户的 UWB 信号被设计成不同的正交波形时,根据多个 UWB 用户时域发送波形的正交性以区分用户,实现多址,这被称为波分多址技术。

4) 天线的设计

UWB 系统采用极短的脉冲信号来传送信息,信息被调制在这些脉冲的幅度、位置、极性 or 相位等参数上,对应所占用的带宽甚至高达几吉赫兹。能够有效辐射时域短脉冲的天线是 UWB 研究的一个重要方面。

UWB 天线应该是输入阻抗具有 UWB 特性和相位中心具有超宽频带不变特性的,就是要求天线的输入阻抗和相位中心在脉冲能量分布的主要频带上保持一致,以保证信号的有效发射和接收。

时域短脉冲辐射技术早期采用双锥天线、V-锥天线、扇形偶极子天线,这几种天线存在馈电难、辐射效率低、收发耦合强、无法测量时域目标的特性,只能用作单收发。现在出现了利用光刻技术制成的毫米、亚毫米波段的集成天线,还有利用微波集成电路制成的 UWB 平面槽天线,其特点是能产生对称波束、可平衡 UWB 馈电、具有 UWB 特性。

5) 收发信机的设计

在得到相同性能的前提下,UWB 收发信机的结构比传统的无线收发信机要简单。传统的无线收发信机大多采用超外差式结构,UWB 收发信机采用零差结构,实现起来也十分简单,无须本振、功放、压控振荡器(VCO)、锁相环(PLL)、混频器等环节。

在接收端,天线收集的信号经放大后通过匹配滤波或相关接收机处理,再经高增益门限电路恢复原来的信息。距离增加时,可以由发送端用几个脉冲发送同一信息比特的方式增加接收机的信噪比,同时可以通过软件的控制,动态地调整数据速率、功耗与距离的关系,使 UWB 具有极大的灵活性,这种灵活性正是功率受限未来移动计算所必需的。

现代数字无线技术常采用数字信号处理芯片(DSP)的软件无线电来产生不同的调制方式,这些系统可逐步降低信息速率以在更大的范围内连接用户。UWB 的一大优点是,即使最简单的收发信机也可采用这一数字技术。

3. UWB 技术的特点

超宽带带来了全新的通信方式及频谱管理模式。超宽带系统的主要性能特点及技术优势表现在以下几个方面:

1) 带宽极宽

传统的无线通信技术大都是基于正弦载波的,而消耗大量发射功率的载波本身并不传送信息,真正用来传送信息的是调制信号,即用某种调制方式对载频进行调制。而超宽带系统可以采用无载波方式,即不使用正弦载波信号,直接调制超短窄脉冲,从而产生一个数吉赫兹(GHz)量级的大带宽。UWB 使用的带宽在 1GHz 以上,高达几个吉赫兹,超宽带系统容量大,并且可以和目前的窄带通信系统同时工作而互不干扰;同时,作为一种与其他现存传统无线技术共享频带的无线通信技术,对于目前日益紧张的、有限的频谱资源,超宽带技术有其独特的优势,全球频谱规划组织也对其表示高度关注和支持。所以,超宽带不只是一项革命性的技术,它更是一段免许可证的频谱资源。目前 FCC 开放的频段是 3.1~10.6GHz, UWB 可共用 7.5GHz 的频带。

2) 抗多径能力强

UWB 发射的是持续时间极短的单周期脉冲,且占空比极低,多径信号在时间上是可分离的,因此具有很强的抗多径能力。多径衰落一直是传统无线通信难以解决的问题,而 UWB 信号由于带宽达数吉赫兹(GHz),具有高分辨率,能分辨出时延达纳秒级的多径信号,而恰好室内等多径场合的多径时延一般也是纳秒级的。这样,UWB 系统在接收端可以实现多径信号的分集接收。UWB 信号的抗多径衰落的固有鲁棒性特别适合于室内等多径、密集场合的无线通信应用。但 UWB 信号极高的多径分辨率也导致信号能量产生严重的时间弥散(频率选择性衰落),接收机必须通过牺牲复杂度(增加分集阶数)以便捕获足够的信号能量。这将对接收机设计提出严峻挑战。在实际的 UWB 系统设计中,必须折中考虑信号带宽和接收机复杂度,得到理想的性价比。

3) 定位精确

冲激脉冲具有很高的定位精度和穿透能力,采用超宽带无线电通信,很容易将定位与通信合一,在室内和地下进行精确定位。信号的距离分辨力与信号的带宽成正比。由于信号的超宽带特性,UWB 系统的距离分辨精度是其他系统的成百上千倍。UWB 信号脉冲宽度在纳秒级,其对应的距离分辨能力可高达厘米级,这是其他窄带系统所无法比拟的。这使得超宽带系统在完成通信的同时还能实现准确定位跟踪,定位与通信功能的融合极大地扩展了系统的应用范围。

4) 抗干扰性能强,保密性好

UWB 信号一般把信号能量弥散在极宽的频带范围内,功率谱密度低于自然的电子噪声,采用编码对脉冲参数进行伪随机化后,脉冲的检测将更加困难,接收机只有已知发送端扩频码时才能解出发射数据。由于 UWB 信号本身巨大的带宽及 FCC 对 UWB 系统的功率限制,使 UWB 系统相对于传统窄带系统的功率谱密度非常低。低功率谱密度使信号不易被截获,用传统的接收机无法接收,具有一定保密性,同时使对其他窄带系统的干扰可以很小。

5) 超高速、超大容量,抗截获性好

超宽带的低功耗特点对于用便携式电池供电的系统长时间工作是非常重要的。UWB

以非常宽的频率带宽来换取高速的数据传输,在 10m 的传输范围内,信号传输速率可达 500Mb/s。

6) 系统结构简单,成本低,易数字化

UWB 通过发送纳秒级脉冲来传输数据信号,其发射机直接用脉冲小型激励天线,不需要功放与混频器;同时在接收端,也不需要中频处理。UWB 系统发射和接收的是超短窄脉冲,无须采用正弦载波而直接进行调制,接收机利用相关器能直接完成信号检测。这样,收发信机不需要复杂的载频调制解调电路和滤波器等,系统结构简化,成本大大降低,同时更容易集成到 CMOS 电路中。因此,这可以大大降低系统复杂度,减小收发信机的体积和功耗,易于数字化和采用软件无线电技术。

7) 发送功率小,消耗电能少

通常情况下,无线通信系统在通信时需要连续发射载波,因此要消耗一定电能,而 UWB 不使用载波,只是发出瞬间脉冲电波,也就是直接按 0 和 1 发送出去,并且在需要时才发送脉冲电波,所以消耗电能少。

UWB 系统发射功率非常小,通信设备可以用小于 1mW 的发射功率就能实现通信,低发射功率大大延长了系统电源工作时间。

4. UWB 技术的应用

UWB 技术具有系统结构简单、发射信号功率低、抗多径衰落能力强、安全性高、穿透性强等优点,应用领域十分广泛,UWB 可应用于移动通信、计算机及其外设、消费电子、信息安全等诸多方面,如家用高清电视图像传送、数字家庭宽带无线连接、消费电子中高速数据传输、高清图片及视频显示、汽车视频与媒体中心等。概括起来分为以下三个方面:

1) 高速无线通信系统

在高速无线通信应用中,UWB 可以作为一种短距离高速传输的无线接入手段,非常适合支持无线个域网的应用。高速 WPAN 的主要目标是解决个人空间内各种办公设备及消费类电子产品之间的无线连接,以实现信息的高速交换、处理、存储等,其应用场合包括办公室、家庭等。个人空间内的设备类型按其功能大体可分为消费电子产品、个人计算机及其外围设备。这些设备之间互连都采用 USB 2.0 或 IEEE 1394 标准,但同时也被这些有线传输的线缆所束缚。超宽带技术具有让消费电子产品、个人计算机和外部设备无线化的潜力,并在将来统一这些个人计算机与消费电子产品甚至实现整个移动通信工业产品之间的互联。下面给出几个应用实例。

(1) 消费电子产品应用。随着技术的不断进步,消费电子产品逐步向数字化、智能化、网络化的方向发展。利用 UWB 技术具有 110Mb/s 的数据传输速率以及 10m 的传输距离,为消费电子产品提供高速无线连接,无须使用电缆等传输线建立家庭多媒体网络系统。例如,实现在住宅的几乎所有空间内从机顶盒向电视显示器无线传输高分辨率视频流的功能。使消费者无须为每台电视都添置新的机顶盒,即可让家中的多台电视都接收到高清节目的数据来源。

(2) 计算机外围设备应用。借助超宽带技术,计算机用户无须通过错综复杂的线路来连接计算机主机、显示器、键盘、鼠标、扬声器、打印机、扫描仪、电视等设备。甚至没有必要将这些设备都放置在同一个桌面或房间内,每种设备可以被自由地移动位置。这类应用一

般只需要支持 2~4m 的传输距离,但速率要求可以从几万比特每秒至几百兆比特每秒。

2) 在低速 WPAN 中的应用

低速 WPAN 与电信网络相结合的应用主要在信息服务、移动支付、远程监控以及某些 P2P 应用等,这些应用归纳到无线传感器网络的范畴。无线传感器网络是由部署在监测区域内几十到上百个廉价微型传感器节点组成的、采用无线通信方式、动态组网的多跳的移动性对等网络,通过动态路由和移动管理技术传输具有服务质量要求的多媒体信息流。其网络拓扑具有随机变化的特点,节点信息往往需要通过中间节点进行多次转发才能到达目的节点。若将各节点的地理位置信息作为路由计算的辅助信息,将很大程度上简化路由算法,降低能量消耗。因此,在无线传感器网络中采用超宽带技术作为无线连接手段,可以提供高精度测距和定位业务(精度 1m 以内),以及实现更长的作用距离和超低耗电量,可用于车载防撞雷达、远程传感器网络、家庭智能控制系统等很多领域。车载 UWB 雷达主要应用在 24GHz 频段。

3) 雷达成像系统

在雷达成像(包括穿地雷达、墙中成像雷达、穿墙成像雷达、医学成像系统、监视系统等)应用中,主要以 UWB 穿墙成像雷达为主。目前国外已有用于军事、抢险、反恐、资源探测方面的 UWB 穿墙成像雷达产品,这类产品主要依据的是 FCC 制定的频谱限值要求,最大平均等效全向发射功率(EIRP)不超过 -41.3dBm/MHz ,工作频段在 2GHz 以上。UWB 穿墙成像技术产品往往都是利用持续时间极为短暂的 UWB 信号脉冲穿过一定厚度的墙壁,通过设置在成像设备上的信息屏幕,获取墙壁另一侧的物体(运动)信息。此外,大地探测雷达也可以应用 UWB 技术,其工作原理与穿墙雷达是相仿的。

5. UWB 的发展趋势

UWB 具有带宽高、抗干扰能力强的特点,是物联网重要的通信手段。UWB 除了前面介绍的关键技术之外,还有一些新的方向,如 UWB 与认知无线电(Cognitive Radio,CR)结合的认知超宽带和基于协作模式的 UWB 定位研究。

1) 认知超宽带系统

CR 是一种智能的无线电技术,它具有学习能力,能与周围环境交互信息,以感知和利用在该空间的可用频谱,并限制和降低冲突的发生。CR 与 UWB 都是提高频谱利用率的技术手段,所以 CR 与 UWB 结合,具有广阔的应用场景。认知超宽带是一种基于频谱感知的具有自适应发射功率谱密度和灵活波形的新型超宽带系统。该系统的基本原理主要是利用 CR 能够感知周围频谱环境和 UWB 系统易于数字化软件化的特性,依据感知得到的频谱信息和动态频谱分配策略来自适应地构建 UWB 系统的频谱结构,并生成相应的频谱灵活的自适应脉冲波形,根据信道的状态信息进行自适应的发射与接收。

2) 基于协作模式的 UWB 定位技术

目前在反恐、应急、救援等应用中,室内定位是一个关注的热点。室内无法利用 GPS、北斗等卫星定位系统,需要采用新的技术实现室内定位。UWB 凭借其准确的定位优势,采用协作模式与 GPS 等室外定位系统结合,实现全方位立体化的定位。为此 3GPP 提出了基于 IMS 的 SR-VCC 方案,此方案支持将分组域的语音业务切换到电路域,但需要运营部署 IMS 系统。由于 IMSSR-VCC 方案需要额外投资,从而增加运营成本,且 IMS 技术复杂,

相关标准及产业化工作尚在进一步推进中,因此预计此方案在近几年中尚难以被运营商大规模采用。

3.1.5 NFC 技术

NFC 技术是在无线射频识别技术(RFID)和互联技术二者整合的基础上发展而来的,只要任意两个设备靠近而不需要线缆连接,就可以实现相互间的通信,可以广泛用于设备互联、服务发现以及移动商务等领域。

NFC 技术是一种近距离无线通信技术(NFCIP-1),NFC 设备可以用作非接触式智能卡、智能卡的读写器终端以及设备对设备的数据传输链路,其应用主要可分为以下 4 个基本类型。

(1) 用于交换、传输数据。

将两台支持 NFC 的设备连接,即可进行点对点网络数据传输,例如下载音乐、交换图像或同步处理通信录等。现在的大多数手机都配备了蓝牙等相关功能,所以 NFC 可以充当启动设备,使电话之间的数据交换传输更加便捷。NFC 还支持多台手机间的多人游戏,允许用户与环境进行交互式通信,而无需浏览复杂的菜单或执行复杂的设置程序。

(2) 用于付款和购票。

① NFC 手机可作为乘车票,通过接触进行支付。NFC 手机可以将车票内容保存在芯片中,从而实现瞬间购票。

② NFC 手机可当作电子钱包,通过接触和密码确认进行支付。

(3) 用于电子票证。

作为电子入场券和钥匙的 NFC 手机,可通过接触完成认证。使用者只要通过手机上网下载电子票券,带着手机就可以入场。NFC 手机当作公寓钥匙时,只要将手机贴近门,就可以开锁,还可在大楼内设置一台多媒体终端,方便用户直接利用手机交付房租及水电费。

(4) 用于智能媒体。

智能媒体将成为手机下载的上端。例如,使用内嵌 NFC 卡的手机,只需要在智能媒体表面晃动即可下载票务信息、广告信息、铃声和壁纸等。用户在智能海报旁闪动一下手机,就能从海报的智能芯片中下载关于该活动的信息。

1. NFC 技术优势

NFC 是一种近距离无线通信技术,具有如下技术要点:

(1) 以 ISO/IEC 18092 NFCIP-1 为基准进行标准化。

(2) 以 13.56MHz RFID 技术为基础,NFC 是非接触式 RFID 技术的演进,支持设备间的互联。

(3) 通信距离为 20cm(NFC 设备之间的极短距离接触,主动通信模式为 20cm,被动通信模式为 10cm,让信息能够在 NFC 设备之间点对点快速传递)。

(4) 与现有的非接触式智能卡国际标准相兼容。

(5) 支持的数据传输速率为 106kb/s、212kb/s 或 424kb/s。

NFC 的目标不是取代蓝牙、WiFi 等现有的无线技术,而是起着相互补充的作用。因为 NFC 的数据传输速率较低,最高只可达 424kb/s,比不上现有的一些技术。由于 NFC 单芯片

解决方案是一个开放式的平台,它既可以进行快速的无线网络自组,同时又可用作移动通信、蓝牙或无线 802.11 等现有设备的虚拟连接。除上述技术特点外,NFC 技术还具有下述优点。

- (1) 短距离通信:可以保证通信的安全性,防止被监听,保证通信的确定性。
- (2) 与现有的 RFID 标准兼容:例如省电模式下的 NFC 设备,相当于一张 RFID 标签。
- (3) 简化其他通信较繁杂的连接步骤:例如蓝牙或以太网的通信协定都需要在众多的设备当中选择正确的设备。

NFC 通信通常在发起设备和目标设备之间发生,任何的 NFC 装置都可以为发起设备或目标设备。两者之间以交流磁场方式相互耦合,并以 ASK 方式或 FSK 方式进行载波调制,传输数字信号。发起设备产生无线射频磁场来初始化 NFCIP-1 的通信(调制方案、编码、传输速率与 RF 接口的帧格式)。目标设备则响应发起设备所发出的命令,并选择由发起设备所发出的或是自行产生的无线射频磁场进行通信。

在主动模式下,每台设备要向另一台设备发送数据时,都必须产生自己的射频场。发起设备和目标设备都要产生自己的射频场,以便进行通信。这是点对点通信的标准模式,可以获得非常快速的连接设置。

在被动模式下,NFC 发起设备(也叫主设备,启动 NFC 通信的设备)在整个通信过程中提供射频场。它可以选择 106kb/s、212kb/s 或 424kb/s 其中一种传输速率,将数据发送到另一台设备。另一台设备称为 NFC 目标设备(从设备),不必产生射频场,利用感应的电动势提供工作所需的电源,使用负载调制技术进行数据收发。移动设备主要以被动模式操作,可以大幅降低功耗,并延长电池寿命。在一个应用会话过程中,NFC 设备可以在发起设备和目标设备之间转换自己的角色。利用这项功能,电池电量较低的设备可以要求以被动模式充当目标设备,而不是发起设备。

可以看出,NFC 与 RFID 一样,信息也是通过频谱中无线频率部分的电磁感应耦合方式传递的,尽管都采用了射频识别技术,NFC 与 RFID 却有着显著的不同点,特别是在安全功能和工作距离方面。首先,NFC 是一种提供轻松、安全、迅速的通信的无线连接技术,相对于 RFID 来说,NFC 具有距离近、带宽高、能耗低等特点。其次,NFC 与现有非接触智能卡技术兼容,目前已经成为得到越来越多主要厂商支持的正式标准。再者,NFC 还是一种近距离连接协议,提供各种设备间轻松、安全、迅速而自动的通信。与无线领域中的其他连接方式相比,NFC 是一种近距离的私密通信方式。由于 NFC 的部分应用(例如支付、门禁、防伪等)与安全密切相关,因此能否提供安全的解决方案至关重要。RFID 更多地被应用在生产、物流、跟踪、资产管理上,而 NFC 则在门禁、公交、手机支付等领域内发挥着巨大的作用。NFC 与 RFID 技术所针对的行业不同,NFC 针对的是消费类电子产品,而 RFID 针对的是所有行业,包括物流、交通等诸多行业。从某种意义上讲,NFC 也是 RFID 的一种应用,是 RFID 技术的一种延续产品。

2. NFC 工作原理

NFC 工作于 13.56MHz 频段,支持主动和被动两种工作模式及多种传输数据速率。在主动模式下,主呼和被呼各自发出射频场来激活通信,在被动工作模式下,如果主呼发出射频场,被呼将响应并且装载一种调制模式激活通信。

载波频率为 13.56MHz 的 RFID 的技术标准 ISO 14443 中,主要的调制编码技术为两

种类型：A类和B类。NFC技术同时采用了两种类型的技术，并对其中的某些技术细节进行了改进，在速率为106kb/s时完全采用了ISO 14443的A类标准；速率为212kb/s、424kb/s时采用了ISO 14443的B类的改进标准。

在主动通信模式下，通信双方均采用改进型米勒编码进行通信。

由于解调时复杂度最低的是OOK包络检波，也最容易硬件实现，这是采用ASK调制方式的原因。

依据EMCA-340定义的射频信号接口标准，对于速率为106kb/s，天线接收到的是100%ASK调制的改进米勒编码信号，采用此信号的优点是100%ASK调制能以100%的能量进行数据传输，保证了信号的较高抗干扰性，在一定程度上提高了通信的可靠性。理论分析表明，它在调制间隙处的信号电压不足1V，不能保证卡上数字部分的正常工作，即在数据传输期间，数字处理部分不能正常工作，所以在数字处理部分工作时停止数据传输。因此，尽管100%ASK调制以100%的能量进行数据传输，但它是数据传输与数据处理分开单独工作，即以通信时间的延长为代价的。同时，它也不适用于常规的数字信号处理器，除非在外加时钟的情况下可以采用常规的DSP。

对于212kb/s、424kb/s的通信速率，由于它采用8%~30%的ASK调制，仅用部分能量传输数据，同时NFC设备上的数字信号处理器并未用到所供给的全部能量，当受到噪声干扰时，对信号的可靠性会有一些影响，缩短其有效读写距离，但它能保证能量的无中断供给，可以实现数据传输与数据处理的同步进行，保障芯片在工作时永远不会失去电压供应以及运转时钟，使内部逻辑与软件可以连续正常工作，而不会在数据接收过程中因为电源消失而必须暂停工作，应用软件在工作时不必担心和处理电源消失或数据中断等问题。这对于高安全性芯片来说是一个显著优点，因为其安全算法需要不间断地运行。调制系数为8%~30%的ASK调制的另一优点是在完成NFC设备的选择之后，两个NFC设备之间可以有更高的通信速率。

以上所述的能量传输问题主要是针对的被动通信模式。在NFC技术中，除了兼容ISO 14443标准，还采用了ISO 14443没有的主动通信模式，在此种通信模式下并无能量中断的问题，其通信过程中，数据交换双方始终处于有源状态，射频信号交替关闭发射。

目前在被动通信模式下，NFC设备之间的通信在三种不同的速率下都采用了负载调制方式。106kb/s速率的通信方式使用847.5kHz副载波曼彻斯特编码。而212kb/s、424kb/s速率的通信方式的负载调制也使用847.5kHz的副载波，两台NFC设备之间的数据传输是连续进行的。副载波采用振幅键控的调制方式(ASK)。106kb/s采用改进米勒编码和曼彻斯特编码，因而速度很快，必须采用专门的硬件解码。

NFC传输协议包括三个过程：激活协议、数据交换、协议关闭。协议的激活包含属性的申请和参数的选择，激活的流程分为主动模式和被动模式两种；数据交换协议的帧结构中，包头包括2B的数据交换请求与响应指令、1B的传输控制信息、1B的设备识别码、1B的数据交换节点地址；协议关闭包含信道的拆线和设备的释放。在数据交换完成后，主呼可以利用数据交换协议进行拆线。一旦拆线成功，主呼和被呼都回到了初始化状态。主呼可以再次激活，但是被呼不再响应主呼的属性请求指令，而是通过释放请求指令切换到刚开机的原始状态。NFC设备之间的通用协议流程遵循下面的连续操作：

(1) 任何NFC设备均默认为目标方。

- (2) 作为目标方时,它不产生自身射频能量,应静候来自初始方的指令。
- (3) 如果应用需要,NFC 设备可以转换为初始方。
- (4) 由具体的应用来决定主动/被动通信模式及发送速率。
- (5) 初始方将监测是否存在外部射频磁场,如果检测出外部射频磁场,则不能激活其自身的射频磁场。
- (6) 如果初始方没有检测到外部射频磁场,将开启其自身的射频磁场。
- (7) 目标方通过初始方的射频磁场激活。
- (8) 不管是在主动通信模式还是被动通信模式下,初始方均以一个选定的传输速率发送指令。
- (9) 不管是在主动还是被动通信模式下,目标方以与初始方相同的通信模式、传输速率对初始方进行响应。

图 3-20 阐明了在主动和被动通信模式下,不同传输速率时的通用初始化和单设备检测流程。

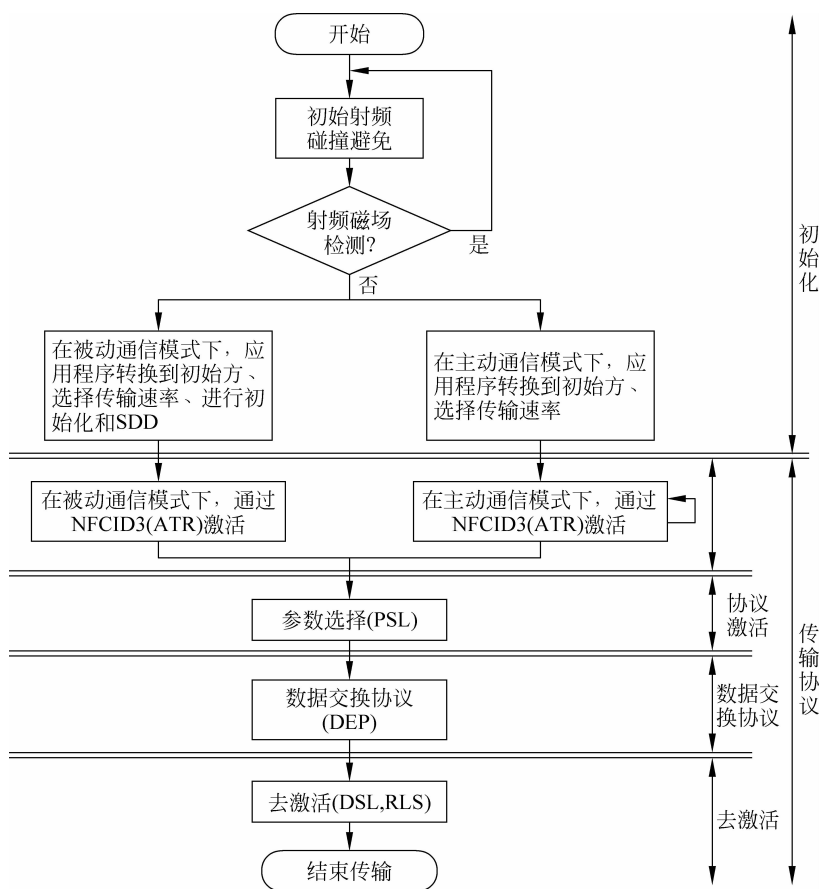


图 3-20 通用初始化流程和单设备检测流程

使用上,因为 NFC 的使用通常会遇到使用尖峰时期,为了避免不同的主动通信方或目标通信方同时通信造成数据链路错误,所以 NFC 采用了一种 Listen before talk 的机制。此

机制会在主动通信方要发出询问信号前,先侦测外界磁场强度来判断是否有其他的设备正在通信中,这种机制的实现称为 RF Collision Avoidance(RFCA),其动作行为是在每次主动发出询问信号时侦测外界磁场,当磁场强度超过门限强度时则会停止询问,直至外界磁场强度低于门限值。

在开启自身的射频信号后,对进入射频信号覆盖范围内的目标通信方进行多目标识别,选出唯一的目标进行点对点通信。被动通信模式下主要采用的多目标识别算法有二进制搜索树和时隙算法。前者主要针对通信速率为 106kb/s,后者主要应用于通信速率为 212kb/s、424kb/s。主动通信模式与被动通信模式采用不同的识别算法。数据的传输在多目标识别之后进行,其传输协议结构与 TCP/IP 类似,但相比 TCP/IP 要简单得多,只包含数据链路层和传输控制层的协议标准。

3. NFC 的应用

NFC 设备表现为一个非接触式智能卡,作为智能卡的读写终端,也作为设备到设备之间的数据传输链接。具备 NFC 技术的移动终端被设计工作在很短的距离,典型为小于 4cm,并为用户提供一种快速、简单和安全的方式来体验一系列全新的非接触式服务的业务应用。

在众多的“非接触式技术”中,NFC 技术支持多种应用,包括移动支付与交易、对等式通信及移动中信息访问等。NFC 设备可以用作非接触式智能卡、智能卡的读写器终端以及设备对设备的数据传输链路,其应用主要可分为以下 4 个基本类型:用于付款和购票、用于电子票证、用于智能媒体以及用于交换、传输数据。

NFC 技术集成于个人移动通信终端,充分体现了信息传输、安全支付与移动电话一体化的设计理念,满足了大多数消费者喜欢移动电话交易的便利、易用和“时尚”性需求。配备 NFC 功能的手机通过让消费者体验直观的连接方式,进而可以改变传统的信息和服务的分配、付费和访问方式。NFC 手机能够进行安全的移动支付和交易,还可以在移动过程中方便地进行点对点通信以及轻松获取信息。

NFC 装置大致上可分成两大类的应用:标签与读写器。把 NFC 装置当成标签使用时,通常有以下几种典型应用:非接触式付款、门禁卡、智能广告发布及 ID 识别等。当 NFC 装置被当成读写器使用时,通常有以下几种典型应用:多媒体信息传输(如电子名片交换、图铃交换和 MP3 音乐共享)以及下载智能广告取得产品或活动的相关资讯。

NFC 手机的应用场合有以下几个方面:

- (1) NFC 手机集成 IC 卡钱包,可实现随时随地的现场支付功能。
- (2) 可通过手机随时随地对 IC 卡钱包进行查询管理及钱包充值。
- (3) 可通过手机随时随地查询电子商品(如电影票等票物信息、手机铃声及游戏等信息)并直接支付购买,远程传送到 NFC 手机。
- (4) 与配套的 NFC 服务网站结合,可开展如音乐、铃声、游戏下载等多种增值服务应用。
- (5) 可提供各种身份识别及信用认证等应用。
- (6) 可通过手机实现公交一卡通功能。
- (7) 可通过手机短信或连接 NFC 服务网站获得各类促销信息。

(8) 可通过手机随时随地管理(删除/下载)各类优惠信息及优惠券。

(9) 可以为基于手机各类支付及增值应用提供安全保证。

(10) 可通过 NFC 网站推广各种广告业务。

NFC 手机的各种应用如图 3-21 所示。

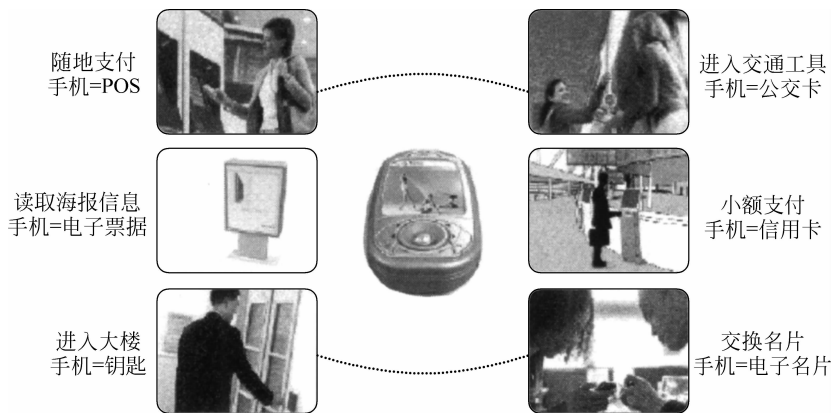


图 3-21 NFC 手机的各种应用

4. VLC-NFC 技术

VLC(可见光通信)是一种使用可见光的新型通信技术,可见光通信技术是利用荧光灯或发光二极管等发出的肉眼看不到的高速明暗闪烁信号来传输信息的,将高速因特网的电线装置连接在照明装置上,接通电源即可使用。利用这种技术作成的系统能够覆盖室内灯光达到的范围,计算机不需要电线连接,因而具有广泛的开发前景。与目前使用的无线局域网(无线 LAN)相比,可见光通信系统可利用室内照明设备代替无线 LAN 基站发射信号,其通信速率可达每秒数十兆至数百兆,未来传输速率还可能超过光纤通信。利用专用的、能够收发信号功能的计算机以及移动信息终端,只要在室内灯光照到的地方,就可以长时间下载和上传高清晰画面和动画等数据。该系统还具有安全性高的特点。用窗帘遮住光线,信息就不会外泄至室外,同时使用多台计算机也不会影响通信速率。由于不使用无线电波通信,对电磁信号敏感的医院等部门可以自由使用该系统。

VLC(可见光通信)的波长范围为 400nm (750THz) $\sim$ 700nm (428THz)。一般特性如下:

- (1) 可视。
- (2) 安全,所见即所发送。
- (3) 不规范,光频率无规范。
- (4) 卫生,对人体无害。
- (5) 与其他设备互不干扰。

目前室内无线通信能满足要求的最好选择就是白光 LED。白光 LED 在提供室内照明的同时,被用作通信光源有望实现室内无线高速数据接入。目前,商品化的大功率白光 LED 功率已经达到 5W ,发光效率也已经达到 90lm/W ,其发光效率(流明效率)已经超过白炽灯,接近荧光灯。白光 LED 的光效超过 100lm/W 并达到 200lm/W (可以完全取代现有

的照明设备)在不久的将来即可实现。因而,LED 照明光通信技术具有极大的发展前景,已引起人们的广泛关注和研究。

LED 作为 VLC 的光源,具有以下优点:

- (1) 体型小,寿命较长。
- (2) 效率高,能耗低。
- (3) 快速响应时间。
- (4) 抗外力打击。
- (5) 耐潮湿。
- (6) 低热量。

基于可视光通信的 NFC 技术的应用如图 3-22 所示。

	应用	功能
手机到手机	 手持设备、便携式设备	• 内容共享 • 数据传输
手机到固定台	 CE、售货亭、打印机	• 文件传输 • 视频流 • 移动电子商务
设施/物品到手机	 CE、招牌、交通信号、照明灯	• 室内导航 • 信息广播

图 3-22 基于可视光通信的 NFC 技术的应用

可见光通信与 RF 通信特征对比见表 3-4。

表 3-4 可见光通信与 RF 通信特征对比

特 征	可见光通信	RF 通信
带宽	无限制,400~700nm	严格规范,带宽受限
EMI	无	有
可视	是	否
标准	刚刚开始	成熟
功耗	低	中等
可见安全性	是	否
结构	LED 器件	接入点
移动性	受限	是
覆盖范围,距离	窄,短	宽,中等

基于可视光通信的 NFC 技术对一些新的应用具有独特的优势,如图 3-23 所示。

- (1) 在干扰敏感的环境下,可实现高速、安全的通信服务。

(2) 加密、安全性高,不受现有的无线电规则的限制。

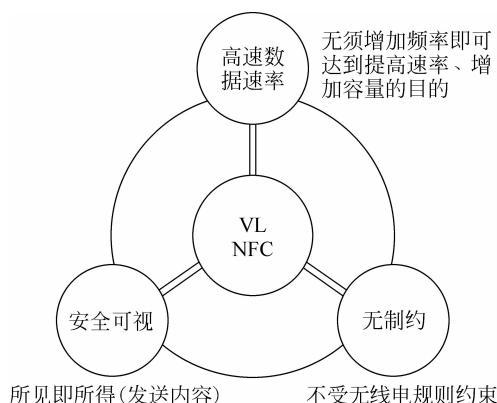


图 3-23 基于可视光通信的 NFC 技术的优势

3.2 无线传感器网络技术

自从人类进入信息时代,自然界的信息通过传感器源源而来。而随着技术的发展,人们已不满足于原有单一的、独立的传感器系统。很多时候,我们需要将来自不同区域的信息联合汇总,从而实现对现场状况的综合判断。这就是以感知为目的的物联网——传感网。传感网是物联网在感知领域的另一个术语,它将各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息,通过嵌入式系统对信息进行处理,并通过自组织无线网络通信,实现对物理世界的动态协同感知。无线传感器网络技术(WSN)是传感网中最核心的技术之一。无线传感器网络是在信息采集方面非常高效的网络。

无线传感器网络(WSN)是一种由独立分布的节点以及网关构成的传感器网络,是由部署在监测区域内大量的廉价微型传感器节点组成,通过无线通信方式形成的一个多跳的自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中告知对象的信息,并发送给观察者。安放在不同地点的传感器节点不断采集外界的物理信息,相互独立的节点之间通过无线网络进行通信。无线传感器网络的每个节点都能够实现采集和数据的简单处理,还能接收来自其他节点的数据,并最终将数据发送到网关。工程师可以从网关获取数据,查看历史数据记录或进行分析。

传感器网络中,除了少数节点需要移动以外,大部分节点都是静止的,它们可以运行在人无法接近的恶劣甚至危险的远程环境中,因此在物联网中有很广泛的应用前景。

无线传感器网络(WSN)是一个涉及多学科高度交叉、知识高度集成的前沿热点研究领域。传感器技术、微机电系统、现代网络和无线通信等技术的进步,推动了现代无线传感器网络的产生和发展。无线传感器网络扩展了人们的信息获取能力,将客观世界的物理信息同传输网络连接在一起,在下一代网络中将为人们提供最直接、最有效、最真实的信息。无线传感器网络能够获取客观物理信息,具有十分广阔的应用前景,能应用于军事国防、工农业控制、城市管理、生物医疗、环境检测、抢险救灾、危险区域远程控制等领域,已经引起了许多国家学术界和工业界的高度重视,被认为是对 21 世纪产生巨大影响力的技术之一。

3.2.1 无线传感器网络的组成

无线传感器网络包括传感器节点(Sensor Node)、汇聚节点(Sink Node)和任务管理单元,如图 3-24 所示。大量的传感器节点被随机分布在所需要监测的区域内,通过自组织的方式形成网络。传感器节点所监测到的数据通过附近的传感器节点依照一定的数据融合协议逐条地传送到汇聚节点,然后通过互联网等手段将数据传输到任务管理单元,用户可以通过任务管理单元对传感器节点进行配置管理,发布所需要监测的数据类型等任务并收集处理监测到的数据。

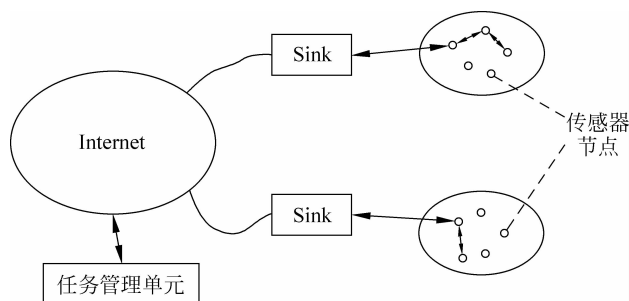


图 3-24 无线传感器网络结构

传感器节点的组成如图 3-25 所示。它一般由传感器模块、处理模块、无线收发模块和能量供应模块这 4 部分组成。

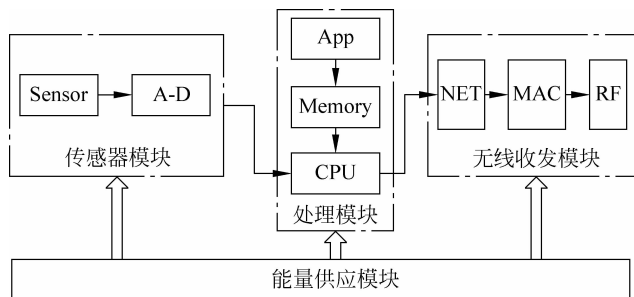


图 3-25 传感器网络节点的组成

传感器模块(由传感器和模/数转换器组成)负责监测区域内信息的采集和数据转换;处理模块(由嵌入式系统构成,包括 CPU、存储器、嵌入式操作系统等)负责控制整个传感器节点的操作、存储和处理本身采集的数据以及其他节点发来的数据;无线收发模块(由无线通信器件组成)负责与其他传感器节点进行无线通信,交换控制消息和收发采集数据;能量供应模块为传感器节点提供运行所需的能量,通常采用微型电池。

在无线传感器网络中,节点任意散落在被监测区域内,这一过程是通过飞行器撒播、人工埋置和火箭弹射等方式完成的,节点以自组织形式构成网络,通过多跳中继方式将监测数据传到汇聚节点,最终借助长距离或临时建立的 Sink 链路将整个区域内的数据传送到远程中心进行集中处理。卫星链路可用作 Sink 链路,借助游弋在监测区上空的无人飞机收集汇

聚节点上的数据也是一种方式。如果网络规模太大,可以采用聚类分层的管理模式,图 3-26 给出了无线传感器网络体系结构一般形式的描述。

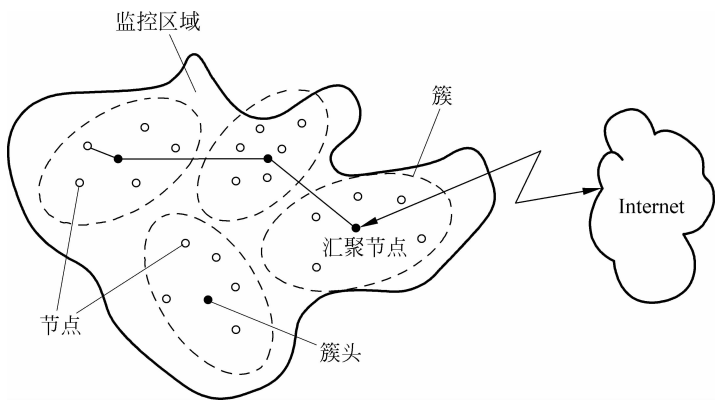


图 3-26 无线传感器网络的体系结构

3.2.2 无线传感器网络的通信协议

无线传感器网络汇聚节点和传感器节点的协议栈如图 3-27 所示,与互联网协议栈的 5 层协议相对应。协议栈还包括能量管理、移动管理和任务管理。这些管理平台使得传感器节点能够以高效的方式协同工作,在节点移动的无线传感器网络中转发数据,并支持多任务和资源共享。物理层负责提供简单但健壮的调制和无线收发技术,接收和发送数据;数据链路层负责无线信道的使用控制,减少邻居节点广播引起的冲突;网络层实现数据的融合、负责路由生成与路由选择;传输层负责数据流的传输控制,是保证通信服务质量的重要部分;应用层包括一系列基于监测任务的应用层软件。

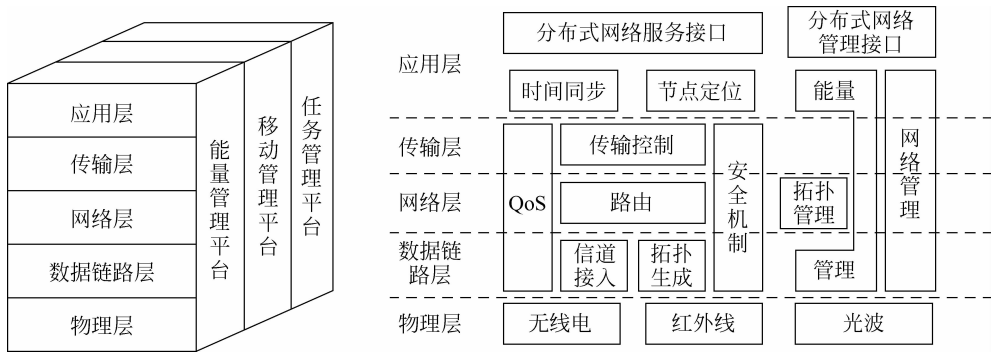


图 3-27 无线传感器网络协议栈

能量管理负责控制节点对能量的使用,为延长网络存活时间有效地利用能源;拓扑管理负责保持网络的连通和数据有效传输;网络管理负责网络维护、诊断,并向用户提供网络管理服务接口,通常包括数据收集、数据处理、数据分析和故障处理等功能;QoS 是为应用程序提供足够的资源使它们以用户可以接受的性能指标指示工作;时间同步为传感器节点提供全局同步的时钟支持;节点定位确定每个传感器节点的相对位置或绝对的地理坐标。

3.2.3 无线传感器网络的特点

1. 网络的自组织性强

在无线传感器网络应用中,传感器节点的位置不能预先精确设定,节点之间的相互邻居关系预先也不知道,如通过飞机播撒大量传感器节点到面积广阔的原始森林中,或随意放置到人类不可到达或危险的区域。这样就要求传感器节点具有自组织的能力,能够自动进行配置和管理,通过拓扑控制机制和网络协议自动形成转发监测数据的多跳无线网络系统。

在无线传感器网络使用过程中,部分传感器节点由于能量耗尽或环境因素造成失效,也有一些节点为了弥补失效节点、增加监测准确度而补充到网络中,这样在无线传感器网络中的节点个数就会动态地增加或减少,从而使网络的拓扑结构随之变化。无线传感器网络的自组织性要能够适应这种动态的网络拓扑结构。

2. 网络的规模大

为了获取精确信息,在监测区域通常部署大量传感器节点,传感器节点数量可能达到成千上万,甚至更多。无线传感器网络的大规模性有两种情况:第一是很大的地理区域,如在原始大森林采用无线传感器网络进行森林防火和环境监测,需要部署大量的传感器节点;第二是节点密集地部署在一个面积不是很大的空间内。

无线传感器网络的大规模性具有如下优势:通过不同空间视角获得的信息具有更大的信噪比;通过分布式处理大量的采集信息能够提高监测的准确度,降低对单个节点传感器的准确度要求;大量冗余节点的存在,使得系统具有很强的容错性能;大量节点能够增大覆盖的监测区域,减少盲区。

3. 网络的动态性好

无线传感器网络的拓扑结构可能因为下列因素而改变:环境因素或电能耗尽造成的传感器节点出现故障或失效;环境条件变化可能造成无线通信链路带宽变化,甚至时断时通;无线传感器网络的传感器、感知对象和观察者这三要素都可能具有移动性;新节点的加入。这就要求无线传感器网络系统要能够适应这种变化,具有动态的系统可重构性。

4. 网络的应用相关性好

无线传感器网络用来感知客观物理世界,获取物理世界的信息量。客观世界的物理量多种多样,不可穷尽,不同的无线传感器网络应用关心不同的物理量,因此对传感器的应用系统也有多种多样的要求。

不同的应用背景对无线传感器网络的要求不同,其硬件平台、软件系统和网络协议必然会有很大差别。所以无线传感器网络不能像互联网一样,有统一的通信协议平台。

只有让系统更贴近应用,才能做出最高效的目标系统。针对每一个具体应用来研究无线传感器网络技术,这是无线传感器网络设计不同于传统无线网络的显著特征。

5. 网络以数据为中心

在互联网中,网络设备用网络中唯一的IP地址标识,资源定位和信息传输取决于终端、

路由器、服务器等网络设备的 IP 地址。如果想访问互联网中的资源,首先要知道存放资源的服务器 IP 地址。可以说目前的互联网是一个以地址为中心的网络。

无线传感器网络是任务型的网络,是以数据为中心的。脱离无线传感器网络谈论传感器节点没有任何意义。无线传感器网络中的节点采用节点编号标识,节点编号是否需要全网仅取决于网络通信协议的设计。由于传感器节点随机部署,构成的无线传感器网络与节点编号之间的关系是完全动态的,表现为节点编号与节点位置没有必然联系。

3.2.4 无线传感器网络的关键技术

1. 时钟同步技术

时钟同步是网络协同工作、系统协同休眠、节省能耗以及目标定位技术的基础。目前已有多种针对无线传感器网络的时钟同步算法,主要集中在两个方面:第一,因为 WSN 中时钟同步的重要性,所以研究安全的时钟同步算法就显得尤为重要;第二,从能耗的角度,研究节能、高效的时钟同步算法。因此如何获得安全高效的时钟同步算法,是目前研究的一个热点。

2. 定位技术

地理位置信息是传感器节点采集数据中不可缺少的信息。确定事件发生的位置或采集数据的节点位置是无线传感器网络最基本的功能之一。由于传感器节点存在资源有限、随机部署、通信易受环境干扰甚至节点失效等特点,定位机制必须满足自组织性、健壮性、能量高效、分布式计算等要求。

在无线传感器网络定位过程中,通常会使用三边测量法、三角测量法或极大似然估计法确定节点位置。根据定位过程中是否实际测量节点间的距离或角度,把无线传感器网络中的定位分类为基于距离的定位和距离无关的定位。

3. 网络拓扑控制

无线传感器网络拓扑控制目前主要的研究问题是在满足网络覆盖度和连通度的前提下,通过功率控制和骨干网节点选择,剔除节点之间不必要的无线通信链路,生成一个高效的数据转发的网络拓扑结构。

通过拓扑控制自动生成的良好拓扑结构能够提高路由协议和 MAC 协议的效率,为数据融合、时钟同步和目标定位等很多方面奠定基础。

目前的无线传感器网络拓扑控制机制包括传统的功率控制和层次型拓扑控制以及启发式的唤醒/休眠机制。

4. 网络安全

无线传感器网络作为任务型的网络,不仅要进行数据的传输,而且要进行数据采集和融合、任务的协同控制等。如何保证任务执行的机密性、数据产生的可靠性、数据融合的高效性以及数据传输的安全性,就成为无线传感器网络安全问题需要全面考虑的内容。无线传感器网络需要实现一些最基本的安全机制:机密性、点到点的消息认证、完整性鉴别、新鲜性、认证广播和安全管理。

5. 其他关键技术

MAC 协议、路由协议、数据融合、数据管理、无线通信技术、嵌入式系统以及应用层技术等是目前无线传感器网络领域中的研究热点问题。

3.2.5 无线传感器网络的应用

1. 商业应用

自组织、微型化和对外部世界的感知能力是无线传感器网络的三大特点,这些特点决定了无线传感器网络在社会商业领域占有一席之地。智能化电器设计就是无线传感器网络的典型商业应用。很多智能家电带有嵌入式处理器,与执行机构组成的无线网络与互联网连接在一起,利用远程监控系统,可完成对家电的远程遥控,例如可以在回家之前半小时打开空调,这样到家的时候就可以直接享受适合的室温,也可以遥控电饭锅、微波炉、电冰箱、电话机、电视机、录像机、计算机等家电,按照自己的意愿完成相应的各种工作,也可以通过图像传感设备随时监控家庭安全情况。

2. 环境观测

环境检测中对无线传感器网络的应用主要有两个部分:

一是利用无线传感器网络的节点分布的广泛性,可以大范围地采集数据,例如,通过布置传感器节点,可以跟踪候鸟昆虫的迁移,研究它们的生活习性。另外,可以通过播撒微型传感器于海洋,监测海洋状况。无线传感器网络还可以监测土壤状态,利用多种传感器来监测降雨量、河水水位和土壤水分,并依此预测爆发山洪的可能性。类似地,无线传感器网络在森林火灾防控中准确预报、及时报警,天气预报,农作物中的害虫监测,土壤的酸碱度和施肥状况监测,农田管理等方面都有很大的应用前景。

另一方面,利用无线传感器网络的自组织的特点,可以借助于航天器布撒的传感器节点实现对星球表面长时间的监测。除了空间工作站,目前空间探索特殊的环境需要极高的自动化。因此,无线传感器网络技术在空间探索方面有着巨大的应用。NASA 的 JPL(Jet Propulsion Laboratory)研制的 Sensor Web 就是为将来的火星探测进行技术准备的,已在佛罗里达宇航中心周围的环境监测项目中进行测试和完善。

3. 医疗护理

传感器节点小的特点使其在医学上有特殊的用途。如果在住院病人身上安装特殊用途的传感器节点,如心率和血压监测设备,医生利用无线传感器网络就可以随时了解被监护病人的病情,及时有效抢救。将传感器节点按药品种类分别放置,计算机系统即可帮助辨认所开的药品,从而减少病人用错药的可能性。还可以利用无线传感器网络长时间地收集人体的生理数据,这些数据对了解人体活动机理和研制新药品都是非常有用的。

4. 军事应用

军事应用是无线传感器网络技术的主要应用领域,由于其特有的无须架设网络设施、可快速展开、抗毁性强等特点,是数字战场无线数据通信的首选技术,是军队在敌对区域中获

取情报的重要技术手段。

无线传感器网络是由密集型、低成本、随机分布的节点组成的,自组织性和容错能力使其不会因为某些节点在恶意攻击中的损坏而导致整个系统的崩溃,这一点是传统的传感器技术所无法比拟的,这就使传感器网络非常适合应用于恶劣的战场环境中,包括监控我军兵力、装备和物资,监视冲突区,侦察敌方地形和布防,定位攻击目标,评估损失,侦察和探测核、生物和化学攻击。美国 DARPA (Defense Advanced Research Projects Agency) 的 sensIT (Sensor Information Technology) 计划就是无线传感器网络应用于军事的典型案例。

5. 其他方面的应用

除上述作用之外,无线传感器网络还应用于生活的各个方面,例如,对建筑物状态监控是利用无线传感器网络来监控建筑物的安全状态。采用无线传感网络对复杂机械进行维护能够降低人工开销。尤其是目前数据处理硬件技术的飞速发展和无线收发硬件的发展,新的技术已经成熟,可以使用无线技术避免昂贵的线缆连接,采用专家系统自动实现数据的采集和分析。

3.2.6 无线传感器网络面临的挑战

1. 电源能量有限

传感器节点体积微小,通常携带能量十分有限的电池。由于传感器节点个数多、成本要求低廉、分布区域广,而且部署区域环境复杂,有些区域甚至人员不能到达,所以传感器节点通过更换电池的方式来补充能量是不现实的。如何高效使用能量来最大化网络生命周期是无线传感器网络面临的首要挑战。

2. 通信能力有限

随着节点之间通信距离的增加,通信消耗的能量也将急剧增加。因此,在满足通信连通度的前提下应尽量减少单跳通信距离。由于传感器节点的能量限制和网络覆盖区域大,无线传感器网络采用多跳路由的传输机制。传感器节点的无线通信带宽有限,通常仅有几百千比每秒的速率。在这样的通信环境和节点有限通信能力的情况下,就需要考虑特定的网络通信机制来满足无线传感器网络的通信需求。

3. 安全性的问题

无线信道、有限的能量,分布式控制都使得无线传感器网络更容易受到攻击。被动窃听、主动入侵、拒绝服务则是这些攻击的常见方式。此外,还包括数据包的完整性鉴定、新鲜性确认等问题。因此,安全性在网络的设计中至关重要。

3.3 现场总线技术

随着计算机技术的不断进步,其价格急剧降低,计算机与计算机网络系统得到了迅速发展。但处于企业生产过程底层的测控自动化系统,要与外界交换信息,要实现整个生产过程

的信息集成,要实施综合自动化,就必须设计一种能在工业现场环境运行的、性能可靠、造价低廉的通信系统,以实现自动化智能设备之间的多点通信,形成工厂底层网络系统,实现底层现场设备之间以及生产现场与外界的信息交换。现场总线就是在这种背景下产生的。

现场总线控制系统(FCS)既是一个开放的数据通信系统、网络系统,又是一个可以由现场设备实现完整控制功能的全分布控制系统。它作为现场设备之间信息沟通交换的联系纽带,把挂接在总线上、作为网络节点的设备连接为实现各种测量控制功能的自动化系统,实现 PID 控制、补偿计算、参数修改、报警、显示、监控、优化及控管一体化等自动化功能。

现场总线控制系统与传统控制系统相比,在结构方面具有优势。在传统模拟控制系统中采用一对一的设备连线,按控制回路分别进行连接,位于现场的测量变送器与位于控制室的控制器之间,以及控制器与位于现场的执行器、开关、马达之间均为一对一的物理连接;在现场总线控制系统中,由于通信能力的提高,可以将设备简单地串行连接在一起,原来单个分散的测量控制设备变成了网络节点,彼此间可以互相沟通,并可共同完成系统的各项任务。虽然现场总线的定义因为角度和出发点不同而各异,但都包含如下概念:

- (1) 现场总线是低带宽的计算机局域网。
- (2) 现场总线是一种数字通信协议。
- (3) 现场总线是开放式、数字化、多点通信底层控制网络。

现场总线控制系统(FCS)作为新一代控制系统,是以数字通信、计算机网络、自动控制为主要内容的综合技术,开放性、分散性与数字通信是现场总线系统最显著的特征。

3.3.1 主流的现场总线

1. CAN 总线

CAN(Controller Area Network)总线是一个控制器局域网络,也是一种高性能、高可靠性、易于开发和低成本的现场总线,它在全球范围内已得到广泛应用。CAN 总线最早由德国 BOSCH 公司推出,它广泛用于离散控制、机器人和楼宇自动控制等领域。其总线规范已被 ISO 制定为国际标准,得到了 Intel、Motorola、NEC 等公司的支持。CAN 协议分为两层:物理层和数据链路层。CAN 的信号传输采用短帧结构,传输时间短,具有自动关闭功能和较强的抗干扰能力。目前基于 CAN 的两层协议又开发出了新的总线协议,如 DeviceNet、SDS、CANOPEN 和 J1939 等。CAN 支持多主工作方式,并采用了非破坏性总线仲裁技术,通过设置优先级来避免冲突。MAC 子层是 CAN 协议的核心,它的功能主要是组帧控制,向下传送从 LLC 子层得到的报文,并把接收的报文传送给 LLC 子层,它负责执行仲裁、检测出错标志和规章界定。

2. DeviceNet 总线

CAN 定义了数据帧、远程帧、出错帧和超载帧。DeviceNet 使用标准格式的数据帧,不使用远程帧,出错帧和超载帧由 CAN 控制器芯片控制,DeviceNet 规范不作定义。由于采用了生产者/消费者通信模式,总线上的报文具有标示符,DeviceNet 可充分利用 CAN 的报文过滤技术,有效节省了节点资源。DeviceNet 是一种低成本的通信连接,也是一种简单的网络解决方案,有着开放的网络标准。DeviceNet 具有的直接互连性不仅改善了设备间的通

信而且提供了相当重要的设备级阵地功能。DeviceNet 基于 CAN 技术,传输速率为 125~500kb/s,每个网络的最大节点数为 64 个,通信模式为生产者/消费者(Producer/Consumer),采用多信道广播信息发送方式。位于 DeviceNet 上的设备可以自由连接或断开,不影响网上的其他设备,而且其设备的安装布线成本也较低。DeviceNet 总线的组织机构是开放式设备网络供应商协会(Open DeviceNet Vendor Association, ODVA)。

3. WorldFIP 总线

WorldFIP 是 World Factory Instrument Protocol(世界工厂仪表协议)的缩写。WorldFIP 作为通用现场总线标准广泛用于能源、化工、交通运输等工业领域,它直接提供现场设备和控制器以及控制器之间的数字连接。WorldFIP 适合各种应用结构:集中、分散和主从,WorldFIP 支持分布数据库,其中的控制器和协调设备室可以根据需求灵活设置,便于系统从 DCS 向 FCS 过渡。WorldFIP 采用三层结构,即物联网层、数据链路层和应用层。

WorldFIP 的北美部分与 ISP 合并为 FF 以后,WorldFIP 的欧洲部分仍保持独立,总部设在法国。其在欧洲市场占有重要地位,特别是在法国的占有率大约为 60%。WorldFIP 的特点是具有单一的总线结构,可以适应不同应用领域的需求,而且没有任何网关或网桥,是用软件的办法来解决高速和低速的衔接。

4. PROFIBUS 总线

PROFIBUS 针对不同的应用需要推出了三种类型:PROFIBUS-DP(Decentralized Periphery)、PROFIBUS-PA(Process Automation)和 PROFIBUS-FMS(Fieldbus Message Specification)。这三种类型均使用统一的总线访问协议,其中 PROFIBUS-DP 采用经过优化的高速、廉价的通信连接,是专为自动化控制系统和设备级的分散 I/O 之间的通信而设计的,能满足设备级分布式控制系统的实时性、稳定性和可靠性的要求;PROFIBUS-PA 是专为过程自动化而设计的,数据传输采用 IEC158-2 标准,支持本质安全要求和总线供电。PROFIBUS-DP 的数据传输服务包括循环的数据传输和非循环的数据传输。循环的数据传输是指主站按照预先定义的顺序循环地探寻各站。其服务形式只有一种:有回答要求的发送/请求数据,如主站的令牌管理、与 DP 从站交换用户数据等。非循环的数据传输的服务形式有两种:有/无应答要求的发送数据、有回答要求的发送/请求数据,如从站初始化阶段的参数配置、诊断等。

5. LonWorks 总线

LonWorks 是又一种具有强劲实力的现场总线技术,它由美国 Echelon 公司推出,并由 Motorola、Toshiba 公司共同倡导。它采用 ISO/OSI 模型的全部 7 层通信协议,采用面向对象的设计方法,通过网络变量把网络通信设计简化为参数设置。LonWorks 技术支持双绞线、同轴电缆、光缆和红外线等多种通信介质。目前已被广泛应用于楼宇自动化、家庭自动化、保安系统、办公设备、交通运输、工业过程控制等多个领域。

6. CC-Link 总线

CC-Link 是 Control & Communication Link(控制与通信链路系统)的缩写,在 1996 年

11 月由三菱电机为主导的多家公司推出。CC-Link 是一个复合的、开放的、适应性强的网络系统,能够适应从较高的管理层网络到较低的传感器层网络的不同范围的需求。它具有数据容量大、通信速度快、使用简单和成本低等优点,同时还具有优异的抗噪性能和兼容性。

7. INTERBUS 总线

INTERBUS 是德国 Phoenix 公司推出的较早的现场总线,2000 年 2 月成为国际标准 IEC61158。INTERBUS 现场总线是一种开放的串行总线,可以构成各种拓扑形式,并允许 16 级嵌套连接。该总线最多可挂接 512 个现场设备,设备之间的最大距离为 400m,无须中继器网络的最大距离为 12.8km。INTERBUS 总线包括远程总线和本地总线,远程总线用于远距离传送数据,采用 RS-485 传输。INTERBUS 采用 OSI 的简化模型(1,2,7 层),即物理层、数据链路层、应用层。它具有强大的可靠性、可诊断性和易维护性,同时实时性、抗干扰性也非常出色。目前,INTERBUS 广泛地应用于汽车、烟草、仓储、造纸、包装、食品等多个工业领域。

3.3.2 现场总线的技术特点

现场总线控制系统(FCS)既是一个开放的网络通信系统,又是一个全分布的自动控制系统。它是以智能传感器、控制、计算机、数字通信、网络为主的一门综合技术。现场总线控制系统与传统的集散控制系统(DCS)相比,具有以下特点:

(1) 总线式结构。一对传输线挂接多台设备,双向传输多个数字信号。如图 3-28 所示为集中控制、集散控制、现场总线控制结构示意图。

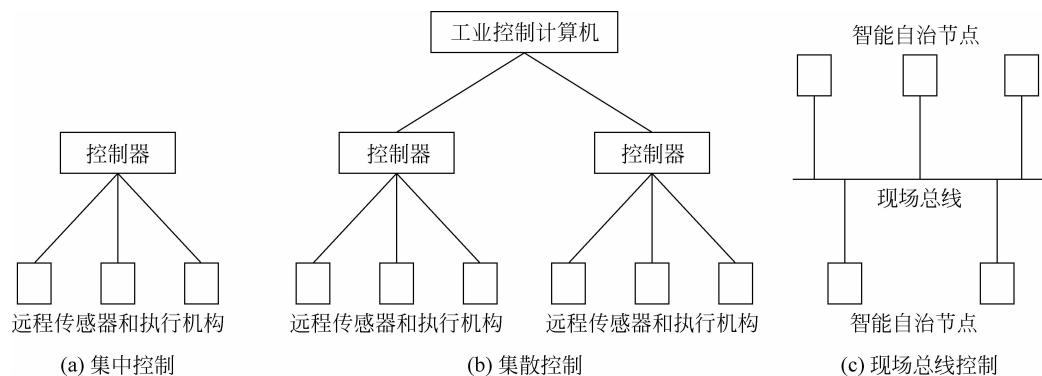


图 3-28 集中控制、集散控制、现场总线控制结构示意图

(2) 开放性、互操作性与互换性。现场总线采用统一的协议标准,用户可以购置不同制造商的现场总线产品,把它们集成在一个控制系统中。它是开放式的互联网,对用户是透明的。

(3) 环境适应性。现场总线能很好地适应现场的操作环境。由于采用数字通信方式,因此可使用多种传输介质进行通信。此外,根据控制系统中节点的空间分布情况,可应用多种网络拓扑结构。

(4) 分散控制和组态灵活。现场总线将控制功能下放到作为网络节点的现场仪表和设

备中,做到彻底的分散。同时引入了功能块的概念,通过统一组态方法,使系统组态简单灵活,不同现场设备中的功能块可以构成完整的控制回路。

3.3.3 CAN 总线技术介绍

CAN(Controller Area Network)总线技术由于其高性能、高可靠性以及独特的设计,越来越受到人们的重视。CAN 最初是由 BOSCH 公司为汽车监测、控制系统而设计的。由于 CAN 总线本身的特点,其应用范围已不再局限于汽车工业,而向过程工业、机械工业、纺织机械、农用机械、机械人、数控机床、医疗器械等领域发展。

1. CAN 总线的性能特点

CAN 总线的数据通信具有突出的可靠性、实时性和灵活性。其主要特点如下:

(1) CAN 为多主方式工作,网络上的任一节点均可在任意时刻主动地向网络上的其他节点发送信息而不分主从,通信方式灵活,且无须站地址等节点信息。

(2) CAN 网络上的节点信息分成不同的优先级,可满足不同的实时要求。

(3) CAN 采用非破坏总线仲裁技术,当多个节点同时向总线发送信息时,优先级较低的节点会主动地退出发送,而最高优先级的节点可不受影响地继续传输数据,从而大大节省了总线冲突仲裁时间。

(4) CAN 只需通过报文滤波即可实现点对点、一点对多点及全局广播等几种方式传送接收数据,无须专门的“调度”。

(5) CAN 上的节点数主要取决于总线驱动电路,目前可达 110 个;报文标识符可达 2032 种(CAN2.0A)。

(6) 采用短帧结构,传输时间短,受干扰概率低,具有极好的检错效果。

(7) CAN 的每帧信息都有 CRC 校验及其他检错措施,保证了数据出错率极低。

2. CAN 的技术规范

CAN 技术规范(Version 2.0)包括 A 和 B 两部分。其中,2.0A 给出了 CAN 报文标准格式,而 2.0B 给出了标准的和扩展的两种格式。

为了使设计透明和执行灵活,CAN 只采用了 ISO/OSI 模型中的物理层和数据链路层。物理层包括物理信令(PLS)、物理媒体附件(PMA)与媒体接口(MDI)三部分;数据链路层包括逻辑链路控制子层(LLC)和媒体访问控制子层(MAC)两部分。CAN 协议的分层结构如图 3-29 所示。

1) CAN 的物理层

CAN 技术规范的物理层定义信号如何进行发送,涉及电气连接、驱动器/接收器特性、位编码/解码、位定时及同步等内容。但对总线媒体装置,诸如驱动器/接收器特性未作规定,以便在具体应用中进行优化设计。CAN 物理层选择灵活,没有特殊的要求,可以采用共地的单线制、双线制、同轴电缆、双绞线、光缆等。网上节点数在理论上不受限制,取决于物理层的承受能力,实际可达 110 个。当总线长为 40m 时,最大通信速率为 1Mb/s;而当通信速率为 5kb/s 时,直接通信距离最大可达 10km。



图 3-29 CAN 协议的分层结构

总线具有两种逻辑状态：隐性或者显性。在隐性状态下， V_{CANH} 和 V_{CAN} 被固定于平均电压电平， V_{diff} 近似为零。显性状态以大于最小阈值的差分电压表示。在显位期间，显性状态改变隐性状态并发送。总线上的电平表示如图 3-30 所示。

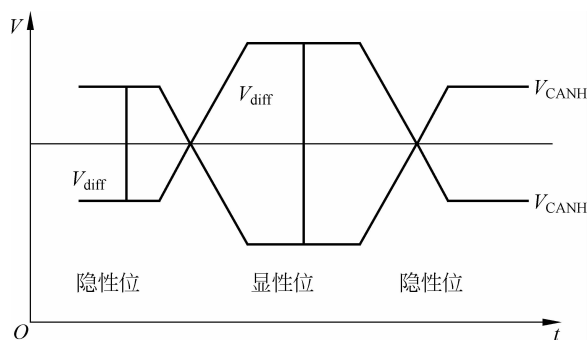


图 3-30 总线上的电平表示

在 1993 年形成的国际标准 ISO 11898 中对基于双绞线的 CAN 总线媒体装置特性给出了建议，这里，将总线上的每个节点称为电子控制装置(ECU)。总线每个末端均接有以 RL 表示的抑制反射的终端负载电阻，而位于 ECU 内部的 RL 应予取消。总线驱动可采用单线上拉、单线下拉或双线驱动，接收采用差分比较器。

2) CAN 的数据链路层

在 CAN 2.0A 的版本中，数据链路层的逻辑链路控制子层(LLC)和媒体访问控制子层(MAC)的服务和功能分别被描述为“目标层”和“传送层”。

LLC 子层的主要功能是：为数据传送和远程数据请求提供服务，确认要发送的信息，确

认接收到的信息,并为恢复管理和通知超载提供信息,为应用层提供接口。在定义目标处理时,存在许多灵活性。

MAC 子层的功能主要是传送规则,即控制帧结构、执行总线仲裁、错误检测、出错标定和故障界定。MAC 子层也要确定为开始一次新的发送,总线是否开放或者是否马上接收。MAC 子层是 CAN 协议的核心,该子层特性不存在修改的灵活性。

CAN 数据链路层由一个 CAN 控制器实现,采用了 CSMA/CD 方式,但不同于普通的 Ethernet,它采用非破坏性总线仲裁技术,网络上节点(信息)有高低优先级之分以满足不同的实时需要。当总线上有两个节点同时向网上输送信息时,优先级高的节点继续传输数据,而优先级低的节点主动停止发送,有效地避免了总线冲突及负载过重导致网络瘫痪的情况。

CAN 可以实现点对点、一点对多点(成组)以及全局广播等几种方式传送和接收数据。

CAN 采用短帧结构,每帧的有效字节数为 0~8 个,因此,传输时间短,受干扰概率低,重新发送时间短。数据帧的 CRC 校验域以及其他检查措施保证了极低的数据出错率。CAN 节点在严重错误的情况下具有自动关闭总线的功能,可以切断它与总线的联系而不影响其他操作。

3. CAN 总线的节点组成

一般说来,系统中的每个 CAN 模块都能够按照控制节点被分成不同的功能块,每个节点由微处理器、CAN 控制器和 CAN 收发器组成。对于每个控制节点(或称控制单元),首先是通过微处理器(或 CPU)读取外围设备、传感器和处理人机接口的检测与控制信号,并对该信号进行局部控制调节,执行具体的计算及信息处理等应用功能。同时,通过 CAN 总线控制器与其他控制节点或功能模块进行通信。CAN 总线节点模块如图 3-31 所示。

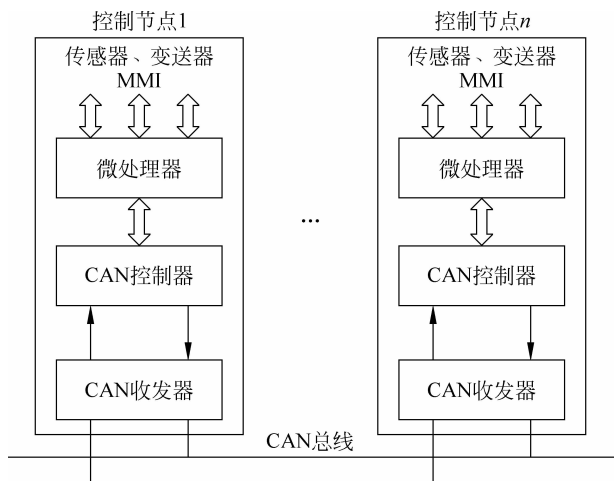


图 3-31 CAN 总线节点模块

CAN 总线的连接一般由 CAN 收发器建立,CAN 收发器增强了总线的驱动能力,它控制逻辑电平使信号从 CAN 控制器到达总线上的物理层,反之亦然。在 CAN 收发器上面一层是一个 CAN 控制器,它主要用于系统通信,执行在 CAN 规约里定义的 CAN 协议。CAN 控制器通常用于信息缓冲和验收滤波。因此,独立的 CAN 控制器总是位于微处理器

和收发器之间,一般情况下这个控制器是一个集成电路。

CAN 总线的突出优点使其在各个领域的应用得到迅速发展,这使得许多器件厂商竞相推出各种 CAN 总线器件产品,已逐步形成系列。而丰富廉价的 CAN 总线器件又进一步促进了 CAN 总线应用的迅速推广。目前,CAN 已不仅是应用于某些领域的标准现场总线,它正在成为微控制器的系统扩展及多机通信接口。

3.3.4 DeviceNet 总线技术介绍

DeviceNet 是一种低成本的通信总线。它将各种测试设备连接到网上,这种直接互连改善了设备间的通信,此外它还提供了重要的设备级诊断功能。DeviceNet 现场总线技术在美国半导体设备中应用较多,它是一个开放的网络标准,规范和协议都是开放的,供应商将设备连接到系统时,无须为硬件、软件或授权付费。

DeviceNet 是基于 CAN 总线技术的符合全球工业标准的开放性通信网络。作为一种串行通信技术,CAN 已经成为开放的国际标准通信协议(ISO 11898),在众多领域中得到广泛的应用。由于 CAN 本身并非一个完整的协议,它并未指定流量控制、数据分割、节点地址分配、通信控制等具体内容。这些内容被包括在更高层协议中,允许各厂商自行开发,CAN 突出的经济性和技术特点,极大地促进了基于 CAN 的控制网络产品的开发与推广。DeviceNet 协议正是这样一种基于 CAN 的高层协议。

DeviceNet 虽然属于工业控制网内的低端网络,通信速率不高,传输的数据量不大,却采用了先进的通信理念,具有低成本、高效率、高性能与高可靠性等优点。它适用于连接传感器、测量仪表、变频器、马达启动器等底层设备。网络采用五线电缆连接,其中包括两条信号线、两条电源线(DC 24V)和一条屏蔽线,设备既可以网络供电也可以独立供电。

1. DeviceNet 的网络结构

DeviceNet 遵从 ISO/OSI 参考模型,它的网络结构分为三层,即物理层、数据链路层和应用层,物理层下面还定义了传输介质。数据链路层又划分为逻辑链路控制(LLC)和媒体访问控制(MAC)。DeviceNet 的 ISO/OSI 参考模型如图 3-32 所示。

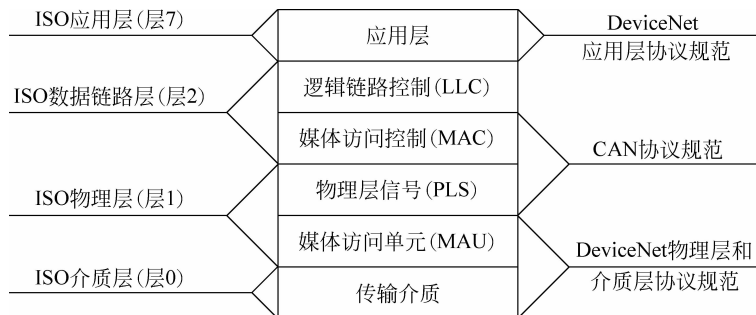


图 3-32 DeviceNet 的 ISO/OSI 参考模型

DeviceNet 建立在 CAN 协议的基础之上,但 CAN 仅规定了 ISO/OSI 参考模型中物理层和数据链路层的一部分,DeviceNet 沿用了 CAN 协议标准所规定的总线网络的物理层和数据链路层,并补充定义了不同的报文格式、总线访问仲裁规则及故障检测和隔离的方法。

DeviceNet 的物理层中的媒体访问单元是自定义的,同时,DeviceNet 增加了有关传输介质的协议规范。

2. 总线仲裁机制

DeviceNet 采用优先仲裁机制,即“带非破坏性逐位仲裁的载波侦听多址访问(CSMA/CD)”仲裁机制。总线空闲时,每个节点都可以尝试发送,但多于两个节点同时发送,发送权的竞争需要通过 11 位标识符的逐位仲裁来解决。网络上每个节点拥有一个唯一的标识符,这个标识符的值决定了总线冲突仲裁时节点优先级的高低。标识符值越小,优先级越高。

在任意时刻,DeviceNet 上的所有节点都在侦听总线状态,当总线上有节点正在发送时,任何节点都必须等待这一帧发送结束,经过约定的帧间隔,任何节点都可以申请下一帧的发送。当多个节点同时向总线发送报文时,要经过 11 位标识符的仲裁。在该标识符发送期间,每个发送节点都在监视总线上当前的电平,并与其自身发送的位电平进行比较,如果值相等,这个节点继续发送下一位,如果发送一个隐性位,而在总线上监测到一个显性位,则说明另一个具有更高优先级的节点发送了一个显性位,此节点失去仲裁权,立即停止下一位的发送。失去仲裁权的节点可以在当前帧结束时再次尝试发送。

3. DeviceNet 节点

DeviceNet 节点采用抽象的对象模型进行描述,每个 DeviceNet 节点都可以看作是对对象的集合。为了完整地体现一个特定模块具有的特性、功能和运行方式,DeviceNet 协议分别采用属性、服务和行为对一个对象加以描述。这些对象主要包括 Identity(标识对象)、DeviceNetObject(DeviceNet 对象)、Message Router(信息路由对象)、Connection Object(连接对象)。

对象支持的连接可以用如图 3-33 所示的连接路径形象地表示。其中,带箭头的连线表示其他对象与连接对象的数据交换,不带箭头的连线表示其他的数据交换。连接对象中又分为两种连接: I/O 连接和显式信息连接。组合对象支持的连接为 I/O 连接,应用对象可

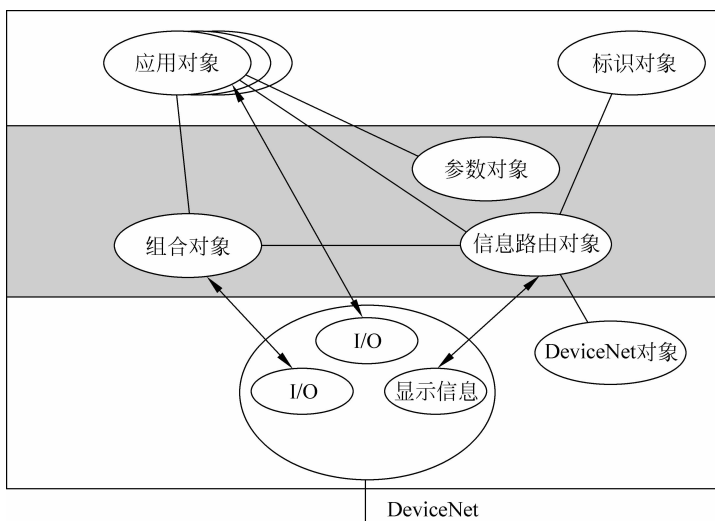


图 3-33 DeviceNet 对象连接路径

以支持 I/O 连接,也可以通过组合对象支持 I/O 连接,信息路由器支持的连接为显式信息连接。任何对象都可以通过信息路由器与连接类对象交换数据。

1) 连接对象(Connection Object)

DeviceNet 产品中一般至少包括两个连接对象。每个连接对象代表 DeviceNet 网络上两节点间虚拟连接中的一个端点。两种连接类型分别是显示报文连接和 I/O 报文连接。显示报文中包括属性地址、属性值和用以表述所请求行为的服务代码。I/O 报文中只包含数据,所有关于如何处理该数据的信息都包含在与该 I/O 报文相关的连接对象中。

2) DeviceNet 对象

DeviceNet 产品中一般都有一个 DeviceNet 对象实例,该实例具有的属性包括节点地址或其 MAC ID、波特率、总线离线动作、总线离线计数器、单元选择和主机的 MAC ID。

3) 标识对象(Identity Object)

DeviceNet 产品中一般都有一个标识对象实例,此实例包含各种属性,例如,供货商 ID、设备类型、产品代码、版本、状态、序列号、产品声明等。

4) 报文路由对象(Message Router)

DeviceNet 产品中一般都有一个报文路由对象实例,可将显式报文传送给其他相应的对象。一般在 DeviceNet 网络中它不具有外部可视性。

5) 组合对象(Assembly Object)

DeviceNet 产品中一般都有一个或多个组合对象。这些对象的任务就是将来自不同应用对象的不同属性(数据)组合成一个能够随单个报文传送的属性。

6) 参数对象(Parameter Object)

在带有可配置参数的设备中都用到了可选的参数对象。每个可配置参数的设备都应引入一个实例。参数对象为配置工具访问所有的参数提供标准的方法。

7) 应用对象(Application Object)

根据设备的具体要求定义应用对象,DeviceNet 协议中有一个标准设备库,提供了大量的标准对象。

4. DeviceNet 设备描述

DeviceNet 规范通过定义标准的设备模型促进不同制造商设备之间的互操作性,它对直接连接到网络的每一类设备都定义了设备描述。设备描述是从网络的角度对设备内部结构进行说明,它使用模型的方法说明设备内部包含的功能、各功能模块之间的关系和接口。设备描述说明了使用哪些 DeviceNet 对象库中的对象和哪些制造商定义的对象,以及关于设备特性的说明。

设备描述包括下列内容:

(1) 设备对象模型定义。定义设备中存在的对象类、各类中的实例数、各个对象如何影响行为以及每个对象的接口。

(2) 设备 I/O 数据格式定义。它包含组合对象的定义和组合对象中包含所需要的数据元件地址(类、实例和属性)。

(3) 设备可配置参数的定义和访问这些参数的公共接口。配置参数数据、参数对设备行为影响、所有参数组以及访问设备配置的公共接口。

DeviceNet 协议规范还允许厂商提供电子数据表(EDS),以文件的形式记录设备的一些具体操作参数等信息,便于在配置设备时使用。

5. DeviceNet 中的连接

DeviceNet 是基于连接的工业底层网络,网络上的任意两个节点在开始通信之前必须先建立连接,这种连接是逻辑上的关系,并不是物理上存在的。在 DeviceNet 中通过一系列参数和属性对连接进行描述,例如,这个连接所使用的标识符、这个连接传送报文的类型、数据长度、路径信息的产生方式、报文传送频率和连接的状态。

DeviceNet 现场总线中的连接提供在多种应用之间交换信息的路径,当建立一个连接时,与连接相关的信息的传送就会分配一个标识符,称为连接标识符(CID)。每一个连接由一个 11 位连接标识符来标识,该 11 位的连接标识符包括媒体访问标识符(MAC ID)和报文标识符(Message ID)。

DeviceNet 通信协议是基于连接概念的协议。要想同设备交换信息,就必须先与它建立连接。要想建立一个连接,每个 DeviceNet 产品都必须具有一个未连接信息管理器(UCMM)。当用 UCMM 或未连接端口建立一个显式报文连接时,这个连接可用于从一个节点向其他节点传送信息,或建立附加的 I/O 连接。一旦建立了连接,就可以在网络设备之间传送 I/O 数据。此时,DeviceNet I/O 报文的所有协议都包含在 11 位的 CAN 标识符中,其他部分都是数据。

6. DeviceNet 系统

下面介绍一个实际的 DeviceNet 系统,该系统主要包括操作站和现场数据采集控制系统两大部分,系统的硬件总体结构如图 3-34 所示。操作站由一台 PC 实现,操作站与总线之间由 DN-PCI-5110 DeviceNet 主站适配卡连接。操作站的主要功能是处理需要复杂计算的信息,将经过处理的信息再送回 DeviceNet 总线,并对整个网络进行管理。现场数据采集控制系统有采集模拟信号和采集数字信号两种节点: CADAM-3800 模拟量采集模块和 CADAM-1800 开关量采集模块。其主要功能是采集各个现场设备的实时信息,并根据所得到的信息发送控制命令去控制现场设备。

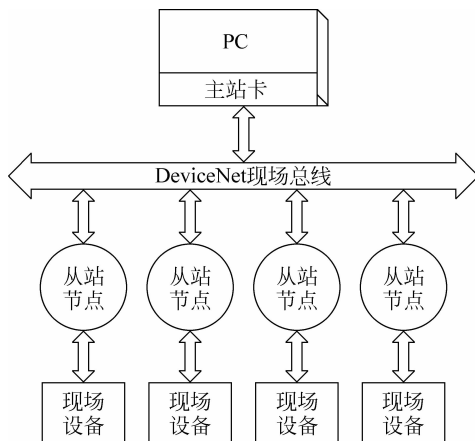


图 3-34 系统的硬件总体结构

整个系统的工作原理为,从控制现场传感器传送过来的信息可能是模拟量或开关量,根据信号的类型选择相应的信号采集模块,采集模块采集现场信息并将信号转化为 DeviceNet 协议规范信号,然后将信号发送到 DeviceNet 总线上。总线上的其他节点单元和操作站根据自己的需要和事先设计好的验收码及验收屏蔽码来判断是否接收该信息。处理后的信息再送回 DeviceNet 总线,经由从站节点控制现场设备。

3.4 IPv6

当前在用的各种有线无线通信网络,能够满足高带宽、远距离传输的要求。将现有通信网来承载物联网感知信息,必然会涉及寻址问题。为了满足 IP 地址需求量的空前提升,物联网协议必须尽快过渡到 IPv6。

现行 TCP/IP 体系结构中的网际协议是 IPv4(即网际协议版本 4),作为 Internet 的关键协议在全球获得了巨大的成功,但是随着 Internet 用户的快速增长和传输速率的不断发展,IPv4 协议面临着诸如地址不够用、难以很好地支持新业务等不容忽视的危机。为了解决 IPv4 所存在的不足,IETF 提出了一种新的 IP 协议,它就是 IPv6(Internet Protocol Version 6)。IPv6 拥有巨大的地址空间。

3.4.1 IPv6 的地址技术

1. 地址的类型

IPv6 支持单点通信地址、多点通信地址和任意点通信地址三种不同类型的网络地址。所有类型的 IPv6 地址都是属于接口而不是节点。一个 IPv6 单点通信地址被赋给某一个接口,而一个接口又只能属于某一个特定的节点,因此一个节点的任意一个接口的单点通信地址都可以用来标识该节点。

在 IPv6 中有多种单点通信地址形式,包括基于全局提供者的单点通信地址、基于地理位置的单点通信地址、NSAP 地址、IPX 地址、节点本地地址、链路本地地址和兼容 IPv4 的主机地址等。IPv6 中的单点通信地址是连续的,适用于点到点通信时使用,一个标识符仅标识一个接口的情况。

IPv6 多点通信地址用于表示一组节点。多点通信地址是一个地址标识符对应多个接口的情况(通常属于不同节点)。该组节点可能会属于几个多点通信地址。这个功能被多媒体应用程序所广泛使用,它们需要一个节点到多个节点的传输。当分组的目的地址是多点地址时,网络尽力将分组发到该组的所有接口上。

任意点通信地址也属于一个标识符对应多个接口的情况。如果一个报文要求被传送到一个任意点通信地址,则它将被传送到由该地址标识的一组接口中的最近一个(根据路由选择协议距离度量方式决定)。任意点通信地址是从单点通信地址空间中划分出来的,因此它可以使用表示单点通信地址的任何形式。从语法上来看,它与单点通信地址间是没有差别的。当一个单点通信地址被指向多于一个接口时,该地址就成为任意点通信地址,并且被指明。当用户发送一个数据包到这个任意点通信地址时,离用户最近的一个服务器将响应用户。这对于一个经常移动和变更的网络用户大有益处。

2. 地址表示方法

IPv6 的地址长度扩展到 128 位,为表示和理解方便,用冒号将其分割成 8 个字段,一个字段由 16 位二进制数组成。每个字段的最大值为 16 384,在书写时用 4 位的十六进制数字表示,字段与字段之间用“:”隔开,而不是原来的“.”。如

1324: 0000: 0000: 0000: 0009: 0900: 100B: 516A

字段中最高位为 0 的数值可以省略,如果整个字段为 0,那么也可以省略。于是上例可以缩写成

1324: 0: 0: 0: 9: 900: 100B: 516A

128 位地址空间包含的准确地址数是 340,282,366,920,938,463,463,374,607,431,768,211,456。

IPv6 地址前缀的表示方法类似于 CIDR 中 IPv4 的地址前缀表示法,可以表示为:

IPv6 地址=前缀+接口标识(类似 IPv4 网络号)+主机号

IPv6 的地址如图 3-35 所示。“FP”是地址前缀(也称为“格式前缀”),用于区别其他地址类型。随后是 13 位的顶级聚集 ID 号(TLA ID)、8 位的 Res(保留位,以备将来 TLA 或 NLA 扩充之用)、24 位的次级聚集 ID 号(NLA ID)、16 位的节点 ID 号(SLA ID)和 64 位的主机接口 ID 号(Interface ID)。TLA、NLA、SLA 三者构成了自顶向下排列的三个网络层次,并且依次向上一级申请 ID 号。分层结构的最底层是网络主机。

3	13	8	24	16	64 (b)
FP	TLA ID	Res	NLA ID	SLA ID	Interface ID

图 3-35 IPv6 的地址

IPv6 地址的基本表达方式是 x: x: x: x: x: x: x: x,其中 x 是一个 4 位十六进制整数(16 位)。每一个数字包含 4 位,每个整数包含 4 个数字,每个地址包括 8 个整数,共计 128 位($4 \times 4 \times 8 = 128$)。例如:

1020.23AB.C2631.10DC.5680.6731.E129.ACB1

7952.9630.85CB.35C0.61BA.9103.EDA6.6565

这些整数都是十六进制数,它们都是合法的 IPv6 地址。地址中的每个整数都要表示出来,但起始的 0 可以不必表示。这是一种比较标准的 IPv6 地址表达方式,此外还有另外两种更加清楚和易于使用的方式。某些 IPv6 地址中可能包含一长串的 0,当出现这种情况时,标准中允许用“空隙”来表示这一长串的 0。如地址 3000: 0: 0: 0: 0: 0: 0: 1 可以被表示为 3000: : 1,这两个冒号表示该地址可以扩展到一个完整的 128 位地址。在这种方法中,只有当 16 位组全部为 0 时才会被两个冒号取代,且两个冒号在地址中只能出现一次。

在 IPv4 和 IPv6 的混合环境中第三种表示方法。IPv6 地址中的最低 32 位可以用于表示 IPv4 地址,该地址可以按照一种混合方式表达,即 x: x: x: x: x: x: d. d. d. d,其中 x 表示一个十六进制整数,而 d 表示一个十进制整数。

例如,地址 0: 0: 0: 0: 0: 0: 10.0.0.1 就是一个合法的 IPv6 地址。把两种可能的表达方式组合在一起,该地址也可以表示为: : 10.0.0.1。

3. 地址的配置

支持无状态和有状态两种地址自动配置方式是 IPv6 的一个基本特性。无状态地址自动配置方式是获得地址的关键。自动将 IP 地址分配给用户是 IPv6 的标准功能,只要机器一连接上网络便可自动设定地址。IPv6 有两种自动设定功能,一种是和 IPv4 自动设定功能一样的名为“全状态自动设定”功能,另一种是“无状态自动设定”功能。

在 IPv4 中,动态主机配置协议(DHCP)实现了主机 IP 地址及其相关配置的自动设置。一个 DHCP 服务器拥有一个 IP 地址,主机从 DHCP 服务器租借 IP 地址并获得有关的配置信息(如默认网关、DNS 服务器等),由此达到自动设置主机 IP 地址的目的。IPv6 继承了 IPv4 的这种自动配置服务,并称其为全状态自动配置。

在无状态自动配置过程中,主机首先将它的网卡 MAC 地址附加在连接本地地址前缀 1111111010 之后,产生一个链路本地单点通信地址。然后向该地址发出一个称为“邻居探索”的请求,以探索是否有同名的地址。如果请求没有得到响应,则表明主机自我设置的链路本地单点传送地址是唯一的。否则,主机将使用一个随机产生的接口 ID 组成一个新的链路本地单点传送地址。然后,以该地址为源地址,主机向本地链路中所有路由器多点传送“路由器请求”的配置信息。路由器以一个包含一个可聚集全球单点传送地址前缀和其他相关配置信息的路由器公告响应该请求。主机用它从路由器得到的全球地址前缀加上自己的接口 ID,自动配置全球地址,然后就可以与 Internet 中的其他主机通信了。

使用无状态自动配置,无须手动干预就能够改变网络中所有主机的 IP 地址。例如,当企业更换了连入 Internet 的 ISP 时,将从新 ISP 处得到一个新的可聚集全球地址前缀。ISP 把这个地址前缀从它的路由器上传送到企业路由器上。由于企业路由器将周期性地向本地链路中的所有主机多点传送路由器公告,因此企业网络中的所有主机都将通过路由器公告收到新的地址前缀,此后,它们就会自动产生新的 IP 地址并覆盖旧的 IP 地址。使用 DHCPv6 进行地址自动设定,连接于网络的机器需要查询自动设定用的 DHCP 服务器才能获得地址及其相关配置。但有两种情况应当以使用无状态自动设定方法为宜:一是家庭网络,因为家庭网络中通常没有 DHCP 服务器;二是移动环境,因为在移动环境中往往是临时建立的网络。

IPv6 又被称为下一代因特网协议,凭借其丰富的地址资源以及支持动态路由机制等优势,能够满足物联网对通信网络在地址、网络自组织以及扩展性等诸多方面的要求。然而,在物联网中 IPv6 并不能简单地“拿来就用”,而是需要进行一次适配。IPv6 在应用于传感器设备之前,需要对 IPv6 协议栈和路由机制进行相应的精简,以满足对网络低功耗、低存储容量和低传输速率的要求。IETF(互联网工程任务组)成立的 6LoWPAN 就是研究并推动对 IPv6 进行精简的标准化组织。另外,目前基于 IEEE 802.15.4 的网络射频芯片也有待进一步开发以支持 IPv6 协议栈进行精简。

6LoWPAN 是物联网无线接入中的一项重要技术。6LoWPAN 是使用 IPv6 的低功率无线个人局域网,该技术结合了 IEEE 802.15.4 无线通信协议和 IPv6 技术的优点,解决了窄带宽无线网络中的低功耗、有限处理能力的嵌入式设备使用 IPv6 的困难,实现了短距离通信到 IPv6 的接入。

3.4.2 6LoWPAN 技术

无线嵌入式网络使得很多应用变得可能,6LoWPAN 是实现无线嵌入式网络的重点。IPv6 是 20 世纪 90 年代 IETF(互联网工程任务组)设计的用于替代 IPv4 的下一代互联网 IP。用来解决迅速增长的互联网需求。6LoWPAN 技术结合了 IEEE 802.15.4 无线通信协议和 IPv6 技术的优点。它采用的是 IEEE 802.15.4 规定的物理层和 MAC 层,不同之处在于 6LoWPAN 技术在网络层上使用 IETF 规定的 IPv6。

在物联网中,信息采集最基本和最重要的方式之一就是传感器,每个传感器都具有数据采集、简单的数据处理、短距离无线通信和自动组网的能力。大量传感器节点组成传感器网络。随着传感器与无线网络技术的迅速发展,需要进行处理和传输的数据量也急剧增加。为了实现对物体智能控制的目标,人们将大量的传感器节点接入互联网。而传统的 IP 地址协议空间不足以满足传感器网络的巨大需求。IPv6 协议可以很好地解决这一问题。在这种背景下,2004 年 11 月 IETF 正式成立了 6LoWPAN 协议工作组,即基于 IPv6 协议的低功耗无线个人局域网工作组,该工作组致力于研究如何解决 IPv6 数据包在 IEEE 802.15.4 上传输问题。规定 6LoWPAN 技术在物理层采取 IEEE 802.15.4,MAC 层以上采取 IPv6 协议栈。

IPv6 设计的特点有一个简单的头结构,并具有分级寻址模型,因而适用于在无线嵌入式网络中使用 6LoWPAN。此外,通过为这些网络创建一个专门的标准组,6LoWPAN 中一个很小的 IPv6 堆就可以兼顾最小的设备。最后,通过进行特别针对 6LoWPAN 的邻居发现协议版本的设计,可以将低功率无限网格网络的特性纳入考虑之中。结果是将 6LoWPAN 有效扩展到无线嵌入式领域,从而使端到端 IP 网络和特点得到广泛应用。

IPv6 技术在 6LoWPAN 上的应用具有广阔的发展空间,从而使得大规模 6LoWPAN 的实现成为可能。然而这些应用程序大量使用的专有技术使其难以融入更大的网络和并且很难更好地提供基于互联网的服务。这一问题可以通过使用 IP 解决,IP 整合各种不同应用使用它们互相融合,如图 3-36 所示。IP 的技术优势包括:

(1) 普及性。IP 技术被众多的人接受。作为下一代互联网核心技术的 IPv6,在 LoWPAN 网络中使用也更易于被大众接受。

(2) 适用性。基于 IP 的设备不需要翻译网关或授权书就可以很容易连接到其他的 IP 网络。

(3) 兼容性。IP 网络对现有的网络基础设施兼容。

(4) 开放性。IP 是开放性协议,随着标准化进程和文件对公众的开放,IP 技术在一个开放和自由的环境中越来越具体,从而产生了大量相关的创新。

(5) 更广阔的地址空间。单从数字上来说,IPv6 所拥有的地址容量是 IPv4 的约 8×10^{28} 倍,达到 $2^{128} - 1$ 个。这不但解决了网络地址资源数量的问题,同时也为除计算机外的设备连入互联网在数量限制上扫清了障碍。满足了部署大规模、高密度 LowPAN 网络设备的需求。

(6) IPv6 支持无状态自动地址配置。IPv6 采用了无状态

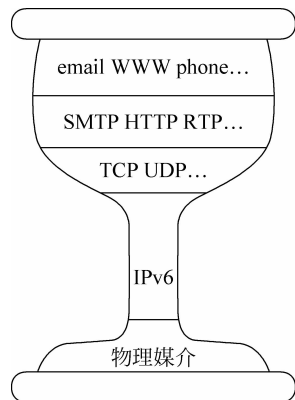


图 3-36 原 IP 架构

地址分配的方案来解决高效率海量地址分配的问题。其基本思想是网络侧不管理 IPv6 地址的状态。节点设备连接到网络中后,将自动选择接口地址(通过算法生成 IPv6 地址的后 64 位),并加上前缀地址,作为节点的本地链路地址。

由此可见,IPv6 技术在 6LoWPAN 上的应用具有广阔的发展空间,从而使得大规模 6LoWPAN 的实现成为可能。与传统的 IP 网络直接通信需要很多互联网协议,通常需要一个操作系统来处理这些协议的复杂性和可维护性。

3.4.3 6LoWPAN 架构

LoWPAN 有简单型、扩展型和自组织型三种不同的类型,如图 3-37 所示。一个 LoWPAN 是 6LoWPAN 节点的集合,这些节点具有相同的 IPv6 地址前缀(IPv6 地址中前 64 位),这意味着在 LoWPAN 中无论哪个节点的 IPv6 地址都保持一样。自组织型 LoWPAN 不需要连接到互联网,可以在没有互联网基础设施的情况下运行。简单型的 LoWPAN 通过一个 LoWPAN 边缘路由器连接到另一个 IP 网络。图中展示了一个回程连接(例如点对点 GPRS),但这也可能是中枢网络连接(共享的)。扩展型 LoWPAN 包含 LoWPAN 中心(例如以太网)连接的多边缘路由器。

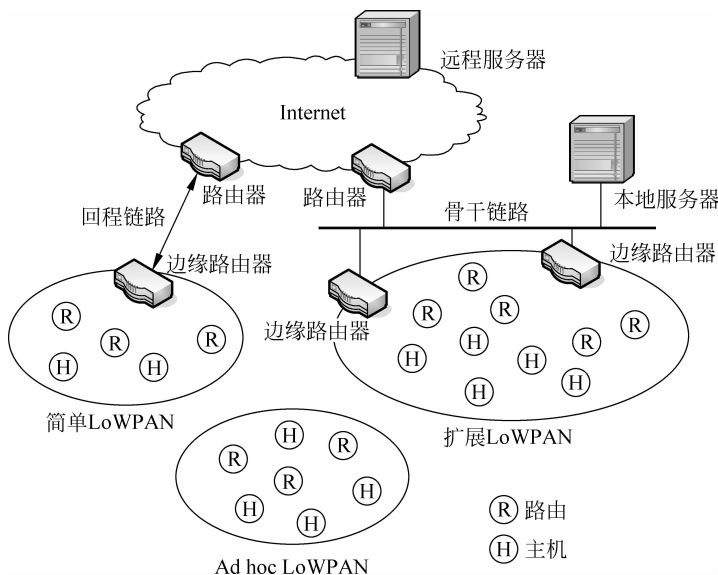


图 3-37 6LoWPAN 架构

LoWPAN 通过边缘路由器与其他的 IP 网络连接。边缘路由器起着非常重要的作用,因为在进行 6LoWPAN 压缩和邻居发现时,它可以连接内外网络。如果 LoWPAN 连接到一个 IPv4 网络,边缘路由器也能够处理与 IPv4 网络的互联。边缘路由器有典型的相关 IT 管理解决方案的管理特性。如果多个边缘路由器共享一个共同的骨干链接,它们能被相同的 LoWPAN 支持。

LoWPAN 由主节点或路由节点与一个或者更多的边缘路由器组成。一个 LoWPAN 节点接口具相同的 IPv6 前缀,IPv6 前缀被分配给边缘路由器和主机。为了方便有效的网络操作,节点在边缘路由器进行注册。这些操作是邻居发现的一部分,这是 IPv6 的一个重

要基本原理。

邻居发现定义了在不同链接中主机和路由器的相互作用。在同一时间内 LoWPAN 节点可以参与多个 LoWPAN(称为 multi-homing),并且边缘路由器之间可以达到容错性。LoWPAN 中的节点可以在边缘路由器之间甚至不同 LoWPAN 之间自由移动。由于没有物理变化的无线通信信道也可以改变网络拓扑结构。

如同正常 IP 节点间通信一样,LoWPAN 节点和其他 IP 网络节点之间的通信是以一种端到端的方式进行的。每一个 LoWPAN 节点都由一个 IPv6 地址唯一确定,并且可以发送和接收 IPv6 数据包,简单 LoWPAN 和扩展 LoWPAN 节点可以借助边缘路由器的服务器互相通信。由于 LoWPAN 节点的有效负荷和处理能力严格受限,应用协议经常在 UDP 负载中设计一个简单的二进制格式。

简单 LoWPAN 和扩展 LoWPAN 的主要不同在于 LoWPAN 中的多边缘路由器的存在,它们拥有共同的 IPv6 前缀和主干链接。多重 LoWPAN 可以与其他部分交叠(即使是在同样的信道中)。当节点从一个 LoWPAN 移动到另一个 LoWPAN 时,节点的 IPv6 地址会发生变化。简单 LoWPAN 通过回程链路连接到互联网。

网络调度时,根据网络管理需求,一般优先考虑多重简单 LoWPAN 而不是回程链接中的扩展 LoWPAN。

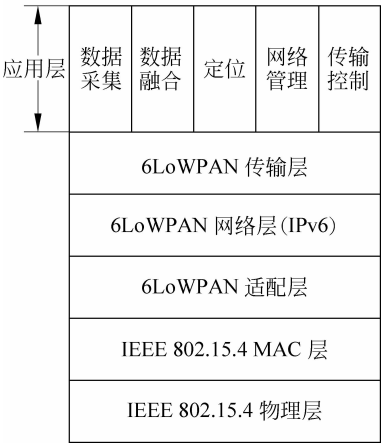
在扩展 LoWPAN 结构中,多个边缘路由器共享一个共同的骨干链接和通过拥有同样的 IPv6 的前缀合作,卸载的大多数邻居发现消息来自骨干链接。这大大简化了 LoWPAN 节点操作,因为 IPv6 地址在扩展 LoWPAN 和运动的边缘路由器之间是稳定的。

边缘路由器代表 IPv6 节点对外进行转发。对 LoWPAN 外面的 IP 节点而言,不管它们的接入点在哪里,LoWPAN 节点总是可以接入的。这使得大企业也可以建立 6LoWPAN 基础设施。运行起来和 WLAN(WiFi)接入点的基础设施相似,只是接入点第 3 层代替第 2 层。

6LoWPAN 不需要基础架构操作,但也可以作为 Ad hoc LoWPAN 进行操作。在这种拓扑结构中,一个路由器必须配置为一个简化的边缘路由器,实现两个基本功能:生成一个独特的本地单播地址(ULA),以及实现 6LoWPAN 邻居发现注册功能。

3.4.4 6LoWPAN 协议栈

为了实现无线传感器与 IP 网络的无缝互联,6LoWPAN 协议栈的架构如图 3-38 所示。该体系结构分别包括 IEEE 802.15.4 物理层、IEEE 802.15.4 媒体访问控制层(Medium Access Control, MAC)层、6LoWPAN 适配层,IPv6,6LoWPAN 传输层(UDP, ICMP)以及应用层。图 3-39 把 IPv6 协议栈与 6LoWPAN 协议栈进行了比较,给出了一个典型的 IP 协议栈相应的 5 层网络模型。由于互联网协议将大量不同的链路层技术与多个传输应用协议联系起来,互联网模型有时被称为“柳腰”模型。



6LoWPAN 中的 IPv6 协议栈与普通 IP 协议栈的 图 3-38 6LoWPAN 协议的体系结构

区别如图 3-39 所示。

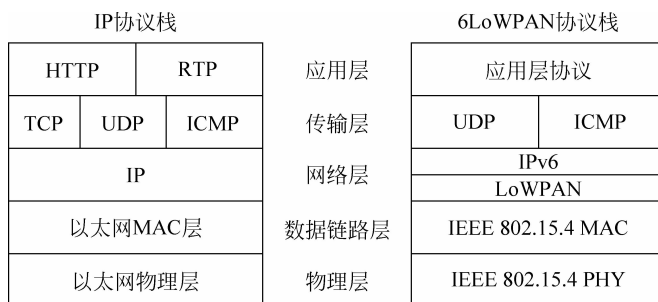


图 3-39 IP 和 6LoWPAN 协议栈区别

一个简单的 6LoWPAN 中的 IPv6 协议栈(也称为 6LoWPAN 协议栈)与普通 IP 协议栈基本相同,在以下几个方面有不同之处。

首先,6LoWPAN 仅支持 IPv6,在 IEEE 802.15.4 和(RFC4944)里面类似的链路层中,LoWPAN 适配层是定义在 IPv6 之上的优化。实际上,嵌入式设备实现 6LoWPAN 协议栈经常同 IPv6 一起对 LoWPAN 进行配置,因此它们作为网络层的一部分一起展示。

其次,在传输协议方面。最常见的 6LoWPAN 传输协议是用户数据协议(User Datagram Protocol,UDP),它也可以按照 LoWPAN 格式进行压缩。因为性能、效率和复杂性的问题,6LoWPAN 的传输控制协议(TCP)不常用。互联网控制消息协议(ICMPv6)用来进行信息控制。

LoWPAN 格式和全 IPv6 之间的转换由边缘路由器完成。这转换对双向都是透明、高效的。在边缘路由器中的 LoWPAN 转换是作为进行 6LoWPAN 网络接口驱动的一部分,并且对 IPv6 协议栈本身通常是透明的。

3.4.5 全 IP 融合与 IPv6 以及 IPv9

IP 规定了计算机在因特网上进行通信时应当遵守的规则,计算机系统只要遵守 IP 就可以与因特网互联互通,正因为有了 IP,因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。网络大融合已成为当今世界电信发展的一大主题,无论是固定网还是移动网,核心网还是接入网都在朝这个大方向发展,而 IP 技术是其中采用的首选技术。全 IP 网络是一种非常有前景的物联网接入方案,通过全 IP 无缝集成物联网和其他各种接入方式,诸如宽带、移动因特网和现有的无线系统,将其都集成到 IP 层中,从而通过一种网络基础设施提供所有通信服务,这样将带来诸多好处,如节省网络成本,增强网络的可扩展性和灵活性,提高网络运作效率,创造新的收入机会等。

目前,全 IP 过渡问题的研究正在进行之中,通信设备制造商、运营商都卷入到了这股热潮之中,它已成为下一阶段通信技术发展的主要研究方向之一。全 IP 网络架构的物联网集智能传感网、智能控制网、智能安全网的特性于一体,真正做到将识别、定位、跟踪、监控、管理等智能化融合,从而也更易于将所有需实现远程互操作的人和物直接连到现有网络诸如国际互联网上,从而从中找到商业模式,引发新的经济增长点。

随着全球经济和信息化浪潮的持续发展,下一步,世界上所有的人,以及万物都可能融

入到这个网络化世界中,形成更为广阔的数字化海洋。可以预见的是,未来网络化的技术如果仍然是 IP,那么下一代网络所容纳的巨大节点数量,将远远超越现有 IPv4 地址空间容量,因此,这个网络化世界的引擎将要升级到下一代互联网技术——以 IPv6 地址为基础标识的 IP 网络技术。在 IPv6 巨大容量的包容下,世界上人人都可拥有全球唯一的地址,实现更为公平的普遍通信服务,使得家庭、城市以及地球上的万物将可以逐步数字化和 IP 化,融入到这个新的网络中来,城市以及人类生活将变得高度智能化。

与之相应,物联网作为“物物相连的互联网”,真要把物和物连接起来,除了需要这样那样的传感器,首先要给它们每个都贴上一个标签,也就是每个物品都有个自己的 IP 地址,这样用户才可以通过网络访问物体。但是目前的 IPv4 受制于资源空间耗竭,已经无法提供更多的 IP 地址,而 IPv6 可以让人们拥有几乎无限大的地址空间,这使得全世界的人使用的手机、家电、汽车甚至鞋子等上网都成为可能,这样就能构筑一个人人有 IP、物物都联网的物联网世界。因此,IPv6 技术是物联网底层技术条件的基础,没有 IPv6 物联网就无从谈起。

对于物联网而言,无论是远程通信,还是近距离通信,为了满足 IP 地址需求量的空前提升,都必须尽快过渡到 IPv6。物联网的远程通信需求,将推动现有移动或者固定网络向 IPv6 的商用化演进。物联网应用,主要以公众无线网络为载体,大多使用 2G、3G 网络来实现远程通信,同时也有部分应用采用了固定光纤接入方式,根据不同的应用场景选择不同的接入方式。而现有的 2G、3G 网络,分组域核心网设备 GGSN/PDSN 均需要尽快升级支持给终端分配 IPv6 地址,同时分组域核心网设备与骨干承载网络之间需要尽快实现 IPv6 组网和路由。对于固定接入方式而言,接入路由器和骨干及城域承载网络也需要尽快完成向 IPv6 的升级,以满足快速业务接入的要求。

在近距离通信领域,主流技术也开始支持 IPv6。常用的近距离无线通信技术有 IEEE 802.11b、IEEE 802.15.4 (ZigBee)、Bluetooth、UWB、RFID、IrDA 等。其中,ZigBee 作为一种近距离、低复杂度、低功耗、低数据传输速率、低成本的双向无线通信技术,完整的协议栈只有 32KB,可以嵌入各种设备中,同时支持地理定位功能,因而成为构建近距离无线传感网的主流技术。当前,ZigBee 已在其智能电网的最新标准规范中加入了对 IPv6 协议的支持。

精简 IPv6 适配于物联网是当前面临的主要问题,作为下一代网络协议,IPv6 凭借着丰富的地址资源以及支持动态路由机制等优势,能够满足物联网对通信网络在地址、网络自组织以及扩展性等诸多方面的要求。然而,在物联网中应用 IPv6,并不能简单地“拿来就用”,而是需要进行一次适配。

IPv6 不能够直接应用到传感器设备中,而是需要对 IPv6 协议栈和路由机制进行相应的精简,以满足对网络低功耗、低存储容量和低传送速率的要求。由于 IPv6 协议栈过于庞大复杂,并不匹配物联网中互联对象,尤其是智能小物体的特点,因此虽然 IPv6 可为每一个传感器分配一个独立的 IP 地址,但传感器网需要和外网之间进行一次转换,起到 IP 地址压缩和简化翻译的功能。

目前,相关标准化组织已开始积极推动精简 IPv6 协议栈的工作。例如,IETF 已成立了 6LoWPAN 和 RoLL 两个工作组进行相关技术标准的研究工作。相比较传统方式,能支持更大的节点组网,但对传感器节点功耗、存储、处理器能力要求更高,因而成本要更高。另外,目前基于 IEEE 802.15.4 的网络射频芯片还有待进一步的开发来支持精简 IPv6 协

议栈。

总体上,物联网应用 IPv6 可按照“三步走”策略来实施。首先,承载网支持 IPv6;其次,智能终端、网关逐步应用 IPv6;最后,智能小物体(传感器节点)逐步应用 IPv6。目前,一些网络设备商的产品,包括骨干和接入路由器、移动网络分组域设备等,已经可以完全满足第一和第二阶段商用部署的要求,同时他们在积极跟踪第三阶段智能小物体应用 IPv6 的要求,包括技术标准和商用产品两大领域。有理由相信,在 IPv6 的积极适配与广泛应用下,物联网产业有望实现真正的大繁荣。

IPv6 协议的引入使得大量、多样化的终端更容易接入 IP 网,并在安全性和终端移动性方面都有了很大的增强。基于 IPv6 的物联网,可以在 IP 层上对数据包进行高强度的安全处理,使用 AH 报头、ESP 报头来保护 IP 通信安全,其安全机制更加完善;同时,终端移动性也更有利于监测物品的实时位置。从而,IPv6 将促进物联网向着更便捷、更安全的方向发展,IPv6 技术使大量、多样化的终端更容易接入 IP 网,并在安全性和终端移动性方面都有了很大的增强,其应用必将促进物联网向着更便捷、更安全的方向发展。

IPv6 虽然号称“能给世界上的每粒沙子分配地址”,但地址资源掌握在他国手中,我国实际能分得的地址数量尚未可知。事实上,IPv4 虽然可以为网络分配约 42 亿个 IP 地址,但美国占据了地址总量的 74%,而我国分到使用权的地址数不到美国公开地址的 10%。

目前尚有另一种 IP 演进策略即 IPv9,IPv9 协议是指 0~9 阿拉伯数字网络作虚拟 IP 地址,并将十进制作为文本的表示方法,即一种便于找到网上用户的使用方法;为提高效率和方便终端用户,其中有一部分地址可直接作域名使用;同时,由于采用了将原有计算机网、有线广播电视网和电信网的业务进行分类编码,因此,又称“新一代安全可靠信息综合网协议”。IPv4 和 IPv6 都采用十六进制技术,而 IPv9 采用十进制技术,能分配的地址量是 IPv6 的 8 倍。IPv9 协议的主要特点:

- (1) 采用了定长不定位的方法,可以减少网络开销,就像电话一样可以不定长使用。
- (2) 采用特定的加密机制。加密算法控制权掌握在我国手中,因此网络特别安全。
- (3) 采用了绝对码类和长流码的 TCP/ID/IP,解决声音和图像在分组交换电路传输的矛盾。
- (4) 可以直接将 IP 地址当成域名使用,特别适合 E164,用于手机和家庭上网。
- (5) 有紧急类别可以解决在战争和国家紧急情况下的线路畅通。
- (6) 由于实现点对点线路,因此对用户的隐私权加强了。
- (7) 特别适合无线网络传输。

虽然 IPv9 设计了一种具有全新报头结构的互联网通信协议,但当前问题在于这种全新协议不能与现有网络兼容,IPv9 迟迟不能大量部署,耗资巨大,很大一部分原因也在于此。

小结

本章重点介绍了物联网的网络通信技术。

以无线个域(WPA)应用为核心特征的短距离无线通信是指在较小的区域内(数百米)提供无线通信。

随着 RFID 技术、ZigBee 技术、蓝牙技术、WiFi 技术及超宽带(UWB)技术等低、高速无

线应用技术的发展,短距离无线通信正深入到通信应用的各个领域,表现出广阔的应用前景。

短距离无线通信技术一般指作用距离在毫米级到千米级的,局部范围内的无线通信应用。短距离无线通信涵盖了无线个域网(WPAN)和无线局域网(WLAN)的通信范围。其中 WPAN 的通信距离可达 10m 左右,而 WLAN 的通信距离可达 100m 左右。

短距离无线通信中,各项技术及性能指标有所不同,但也有一些共同特点,如:①低功耗;②低成本;③多在室内环境下应用;④使用 ISM 频段;⑤使用带电池供电的收发装置。

无线传感器网络(WSN)是一种由独立分布的节点以及网关构成的传感器网络。由部署在监测区域内大量的廉价微型传感器节点组成,通过无线通信方式形成的一个多跳的自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中告知对象的信息,并发送给观察者。

现场总线控制系统(FCS)既是一个开放的数据通信系统、网络系统,又是一个可以由现场设备实现完整控制功能的全分布控制系统。它作为现场设备之间信息沟通交换的联系纽带,把挂接在总线上、作为网络节点的设备连接为实现各种测量控制功能的自动化系统,实现 PID 控制、补偿计算、参数修改、报警、显示、监控、优化及控管一体化等自动化功能。

为了解决 IPv4 所存在的不足,IETF 提出了 IPv6 协议。IPv6 拥有巨大的地址空间。IPv6 支持单点通信地址、多点通信地址和任意点通信地址三种不同类型的网络地址。所有类型的 IPv6 地址都是属于接口而不是节点。一个 IPv6 单点通信地址被赋给某一个接口,而一个接口又只能属于某一个特定的节点,因此一个节点的任意一个接口的单点通信地址都可以用来标识该节点。

思考与练习

1. 什么是短距离无线通信?
2. 什么是 WiFi? 其特点是什么?
3. 一个 WiFi 连接点包括哪些组成部分? 各部分功能是什么? WiFi 的应用领域有哪些?
4. 简述 ZigBee 协议与 IEEE 802.15.4 标准的联系与区别。
5. ZigBee 协议有哪些优点? ZigBee 网络的拓扑结构有哪些?
6. 简述蓝牙技术的基本原理,包括蓝牙网络的基本结构单元。
7. 蓝牙技术的特点是什么? 根据其特点可以将蓝牙技术应用在哪些领域?
8. 超宽带技术的特点有哪些? 说明具体的应用领域。
9. NFC 技术有哪些优势? NFC 手机有哪些方面的用途?
10. 什么是无线传感器网络?
11. 无线传感器网络具有何显著特点?
12. 举例说明无线传感器网络广泛的应用。
13. CAN 总线有哪些性能特点?
14. 简述 DeviceNet 总线的适用范围。
15. 简述 IPv6 技术在 6LoWPAN 上的应用。