第3章 无线传感器网络技术

无线传感器网络(Wireless Sensor Network,WSN)是由部署在监测区域内大量的廉价微型传感器节点,通过无线通信方式形成的一个多跳的自组织的网络,其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息,并发送给观察者。

3.1 ZigBee 技术

传感器、感知对象和观察者构成了无线传感器网络的三个要素。无线传感网络内的各个要素通过一个统一的协议进行信息的传输,这个协议就是 ZigBee。可以说 ZigBee 是 IEEE 802.15.4 协议的代名词。根据这个协议规定的技术是一种短距离、低功耗的无线通信技术。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成了群体中的通信网络,其特点是近距离、低复杂度、低功耗、低数据速率、低成本。ZigBee 主要适合用于自动控制和远程控制领域,可以嵌入各种设备。

ZigBee 联盟是一个高速增长的非牟利业界组织,成员包括国际著名半导体生产商、技术提供者、代工生产商以及最终使用者,他们正制定一个基于 IEEE 802.15.4、可靠、高性价比、低功耗的网络应用规格。

目前超过 150 多家成员公司正积极进行 ZigBee 规格的制定工作,其中包括 7 位推广委员,包括半导体生产商、无线技术供应商及代工生产商。7 位推广委员分别为 Honeywell、Invensys、Mitsubishi、Freescale、Philips、Samsung、Chipcom 和 Ember。ZigBee 联盟主要成员如图 3-1 所示。

图 3-1 ZigBee 联盟主要成员

ZigBee 联盟的主要目标是通过加入无线网络功能，为消费者提供更富弹性、更易用的电子产品。ZigBee 技术能融入各类电子产品，应用范围横跨全球民用、商用、公用及工业用等市场。生产商终于可以利用 ZigBee 这个标准化无线网络平台，设计简单、可靠、便宜又省电的各种产品。ZigBee 联盟的焦点在于：制定网络、安全和应用软件层，提供不同产品的协调性及互通性测试规格，在世界各地推广 ZigBee 品牌并争取市场的关注，管理技术的发展。

3.2　ZigBee 无线数据传输网络描述

简单地说，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 无线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、几公里，并且支持无限扩展。ZigBee 是一个由可多达 65 000 个无线数据传输模块组成的无线数据传输网络平台，在整个网络范围内，每一个 ZigBee 无线数据传输模块之间可以相互通信。ZigBee 无线数据传输模块如图 3-2 所示。

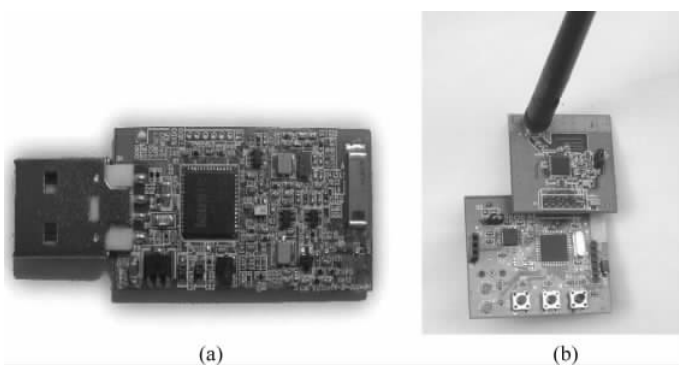

图 3-2　ZigBee 无线数据传输模块

简单的点对点、点对多点通信（目前很多这样的无线数据传输模块）方式，包装结构比较简单，主要由同步序言、数据、CRC 校验几部分组成。ZigBee 采用数据帧的概念，每个无线帧包括了大量无线包装，包含了大量时间、地址、命令、同步等信息，真正的数据信息只占很少的部分，而这正是 ZigBee 可以实现网络组织管理、实现高可靠传输的关键。同时，ZigBee 采用了 MAC 技术和 DSSS（直扩序列调制）技术，能够实现高可靠、大规模的网络传输。

ZigBee 定义了两种物理设备类型：全功能设备 FFD（Full Function Device）和精简功能设备 RFD（Reduced Function Device）。一般来说，FFD 支持任何拓扑结构，可以充当网络协调器（Network Coordinator），能和任何设备通信；RFD 通常只用于星形网络拓扑结构中，不能实现网络协调器功能，且只能与 FFD 通信，两个 RFD 之间不能通信；但它们的内部电路比 FFD 少，只有很少或没有消耗能量的内存，因此实现相对简单，也更利于节能。

在交换数据的网络中，有三种典型的设备类型：协调器、路由器、终端设备。

一个 ZigBee 由一个协调器节点、若干个路由器和一些终端设备节点构成。设备类型并不会限制运行在特定设备上的应用类型。

协调器用于初始化一个 ZigBee 网络，它是网络中的第一个设备。协调器节点选择一个

信道和一个网络标识符(也叫 PAN ID),然后启动一个网络。协调器节点也可以用来在网络中设定安全措施和应用层绑定。协调器的角色主要是启动并设置一个网络。一旦这一工作完成,协调器将以一个路由器节点的角色运行(甚至去做其他事情)。由于 ZigBee 网络的分布式特点,网络的后续运行不需要依赖于协调器的存在。

路由器的功能有:

(1) 允许其他设备加入到网络中。

(2) 多跳路由。

(3) 协助用电池供电的终端子设备的通信。

通常,路由器一直要处于工作状态,因此需要使用干线电源供电。路由器需要存储那些去往子设备的信息,直到其子节点"醒来"并请求数据。当一个子设备要发送信息,子设备需要将数据发送给它的父路由节点。这时,路由器就要负责发送数据,执行任何相关的重发,如果有必要还要等待确认。这样,自由节点就可以继续回到睡眠状态。有必要认识到的是,路由器允许成为网络流量的发送方或者接收方。由于这种要求,路由器必须不断准备转发数据,它们通常要用干线供电,而不是使用电池。如有某一工程不需要电池来给设备供电,那么可以将所有的终端设备作为路由器使用。

一个终端设备并没有对维持网络的基础结构有特定责任,所以它可以自己选择是休眠还是激活。终端设备仅在从它们的父节点接收或者发送数据时才会激活。因此,终端设备可以用电池供电来运行很长一段时间。

图 3-3 是一个 ZigBee 网络示意图,它具有 ZigBee 协调器(黑色)、路由器(灰色)和终端节点(白色)。

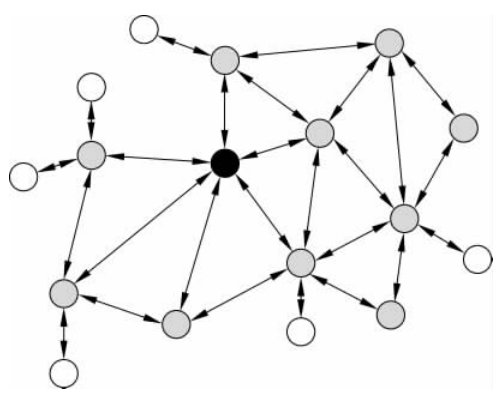

图 3-3 ZigBee 网络示意图

与移动通信的 CDMA 网或 GSM 网不同的是,ZigBee 网络主要是为工业现场自动化控制数据传输而建立,因而,它必须具有简单、使用方便、工作可靠、价格低的特点。而移动通信网主要是为语音通信而建立的,每个基站价值一般都在百万元人民币以上,而每个 ZigBee"基站"却不到 1000 元人民币。每个 ZigBee 网络节点不仅本身可以作为监控对象,例如其所连接的传感器可直接进行数据采集和监控,还可以自动中转别的网络节点传过来的数据资料。除此之外,每一个 ZigBee 网络节点(FFD)还可在自己信号覆盖的范围内,和多个不成单网络的孤立子节点(RFD)进行无线连接。

3.3 ZigBee 的技术优势

ZigBee 有如下技术优势。

(1) 低功耗。在低耗电待机模式下,2 节 5 号干电池可支持 1 个节点工作 6～24 个月,甚至更长。这是 ZigBee 的突出优势。与之相比较,蓝牙能工作数周、WiFi 可工作数小时。

(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,全功能的主节点需要 32KB 代码,子功能节点少至 4KB 代码,而且 ZigBee 免协议专利费。每块芯片的价格大约为 2 美元。

(3) 低速率。ZigBee 工作在 20～250kbps 的较低速率,分别提供 250kbps(2.4GHz)、40kbps(915MHz)和 20kbps(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。传输范围一般介于 10～100 m 之间,在增加 RF 发射功率后,亦可增加到 1～3km。这指的是相邻节点间的距离。如果通过路由和节点间通信的接力,传输距离将可以更远。

(5) 短时延。ZigBee 的响应速度较快,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。与之相比较,蓝牙需要 3～10s、WiFi 需要 3s。

(6) 高容量。ZigBee 可采用星状、片状和网状网络结构,由一个主节点管理若干子节点,最多一个主节点可管理 254 个子节点,同时主节点还可由上一层网络节点管理,最多可组成 65 000 个节点的大网。

(7) 高安全。ZigBee 提供了三级安全模式,包括无安全设定、使用接入控制清单(ACL)防止非法获取数据以及采用高级加密标准(AES 128)的对称密码,以灵活确定其安全属性。

(8) 免执照频段。采用直接序列扩频在工业科学医疗(ISM)频段,如 2.4 GHz(全球)、915MHz(美国)和 868MHz(欧洲)。

第4章 物联网组网技术

目前，物联网组网技术主要有现场总线技术、WiFi 技术、蓝牙技术、全球定位系统技术、电力线通信技术以及微机电系统技术等。

4.1 现场总线技术

现场总线控制系统技术是 20 世纪 80 年代中期在国际上发展起来的一种崭新的工业控制技术。

4.1.1 现场总线

现场总线控制系统(FCS)的出现引起了传统的、可编程逻辑控制器(PLC)和分布式控制系统(DCS)基本结构的革命性变化。现场总线系统技术极大地简化了传统控制系统烦琐且技术含量较低的布线工作量，使其系统检测和控制单元的分布更趋合理。更重要的是从原来的面向设备选择控制和通信设备转变成为基于网络选择设备。尤其是 20 世纪 90 年代现场总线控制系统技术逐渐进入中国以来，结合 Internet 和 Intranet 的迅猛发展，现场总线控制系统技术越来越显示出其传统控制系统无可替代的优越性。现场总线控制系统技术已成为工业控制领域中的一个热点。

现场总线是用于现场电器、现场仪表及现场设备与控制室主机系统之间的一种开放、全数字化、双向、多站的通信系统。而现场总线标准规定某个控制系统中一定数量的现场设备之间如何交换数据。数据的传输介质可以是电线电缆、光缆、电话线、无线电等。

通俗地讲，现场总线是用在现场的总线技术。传统控制系统的接线方式是一种并联接线方式，从 PLC 控制各个电器元件，对应每一个元件有一个 I/O 口，两者之间需用两根线进行连接作为控制和/或电源。当 PLC 所控制的电器元件数量达到数十个甚至数百个时，整个系统的接线就显得十分复杂、容易搞错，施工和维护都十分不便。为此，人们考虑怎样把那么多的导线合并到一起，用一根导线来连接所有设备，所有的数据和信号都在这根线上流通，同时设备之间的控制和通信可任意设置。因而这根线自然而然地称为了总线，就如计算机内部的总线概念一样。由于控制对象都在作业现场，不同于计算机通常用于室内，所以这种总线被称为现场的总线，简称现场总线。

4.1.2　现场总线的特点

现场总线技术实际上是采用串行数据传输和连接方式代替传统的并联信号传输和连接方式的方法，它依次实现了控制层和现场总线设备层之间的数据传输，同时在保证传输实时性的情况下实现信息的可靠性和开放性。一般的现场总线具有以下几个特点。

1．布线简单

这是大多数现场总线共有的特性，现场总线的最大革命是布线方式的革命，最小化的布线方式和最大化的网络拓扑使得系统的接线成本和维护成本大大降低。由于采用串行方式，所以大多数现场总线采用双绞线，还有直接在两根信号线上加载电源的总线形式。这样，采用现场总线类型的设备和系统给人明显的感觉就是简单直观。

2．开放性

一个总线必须具有开放性，这指两个方面：一方面能与不同的控制系统相连接，也就是应用的开放性；另一方面就是通信规约的开放，也就是开发的开放性。只有具备了开放性，才能使现场总线既具备传统总线的低成本，又能适合先进控制的网络化和系统化要求。

3．实时性

总线的实时性要求是为了适应现场控制和现场采集的特点。一般的现场总线都要求在保证数据可靠性和完整性的条件下具备较高的传输速率和传输效率。总线的传输速率要求越快越好，速度越快，表示系统的响应时间就越短，但是实时性不能仅靠提高传输速率来解决，传输的效率也很重要。传输效率主要是由有效用户数据在传输帧中所占的比率以及成功传输帧在所有传输帧中所占的比率决定的。

4．可靠性

一般总线都具备一定的抗干扰能力，同时，当系统发生故障时具备一定的诊断能力，以最大限度保护网络，同时较快地查找和更换故障节点。总线故障诊断能力的大小是由总线所采用的传输的物理媒介和软件协议决定的，所以不同的总线具有不同的诊断能力和处理能力。

4.2　WiFi 技术

WiFi 全称 Wireless Fidelity，又称 IEEE 802.11b 标准，它的最大优点就是传输速度较高，可以达到 11Mbps，另外它的有效距离也很长，同时也与已有的各种 802.11 DSSS 设备兼容。迅驰技术就是基于该标准的，无线上网已经成为现实。

IEEE 802.11b 无线网络规范是 IEEE 802.11a 网络规范的变种，最高带宽为 11Mbps，在信号较弱或有干扰的情况下，带宽可调整为 5.5Mbps、2Mbps 和 1Mbps，带宽的自动调整，有效地保障了网络的稳定性和可靠性。其主要特性为：速度快，可靠性高，在开放性区

域，通信距离可达 305m；在封闭性区域，通信距离为 76～122m，方便与现有的有线以太网络整合，组网的成本更低。

4.2.1 WiFi 无线网络结构

WiFi 无线网络的拓扑结构主要有两种，即 Ad-Hoc 和 Infrastructure。

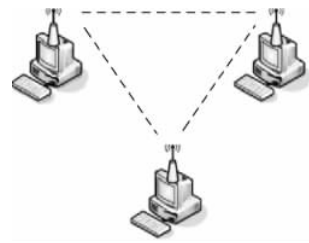

图 4-1 Ad-Hoc 拓扑结构

Ad-Hoc 是一种对等的网络结构，各计算机只需接上相应的无线网卡，或者具有 WiFi 模块的手机等便携终端即可实现相互连接、资源共享，无须中间作用的 Access Point（AP，接入点），这种网络的拓扑结构如图 4-1 所示。

Infrastructure 则是一种整合有线与无线局域网络架构的应用模式，通过这种网络结构，同样可实现网络资源的共享，此应用需通过 Access Point。这种网络结构是应用最广的一种，它类似于以太网中的星形结构，起中间网桥作用的无线接入点（AP）就相当于有线网络中的 HUB（集线器）或者 Switch（交换机），这种网络的拓扑结构如图 4-2 所示。

图 4-2 Infrastructure 拓扑结构

4.2.2 WiFi 的优点

WiFi 技术与蓝牙技术一样，同属于在办公室和家庭中使用的短距离无线技术。该技术使用的是 2.4GHz 附近的频段，该频段目前尚属没用许可的无线频段。其目前可使用的标准有两个，分别是 IEEE 802.11a 和 IEEE 802.11b。该技术由于有着自身的优点，因此受到政府企业的青睐。

WiFi 技术突出的优势在于：

（1）无线电波的覆盖范围广，基于蓝牙技术的电波覆盖范围非常小，半径大约只有 50 英尺左右（约合 15m），而 WiFi 的半径则可达 300 英尺左右（约合 100m），办公室自不用说，就是在整栋大楼中也可使用。最近，由 Vivato 公司推出的一款新型交换机能够把目前 WiFi 无线网络 300 英尺的通信距离扩大到 4 英里（约 6.5km）。

(2) 虽然由 WiFi 技术传输的无线通信质量不是很好,数据安全性能比蓝牙差一些,传输质量也有待改进,但传输速度非常快,可以达到 11Mps,符合个人和社会信息化的需求。

(3) 进入该领域的门槛比较低。只要在机场、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即可。这样,由于“热点”所发射出的电波可以达到距接入点半径数 10m 至 100m 的地方,用户只要将支持无线的笔记本电脑或 PDA 拿到该区域内,即可高速接入因特网。因此不用耗费资金来进行网络布线接入,从而节省了大量的成本。

4.2.3　WiFi 的技术发展

WiFi 技术的商用目前碰到了许多困难。一方面是受制于 WiFi 技术自身的限制,例如其漫游性、安全性和如何计费等都还没有得到妥善的解决;另一方面,由于 WiFi 的赢利模式不明确,如果将 WiFi 作为单一网络来经营,商业用户的不足会使网络建设的投资收益比较低,因此也影响了电信运营商的积极性。

虽然 WiFi 技术的商用遇到一些问题,但这种先进的技术也不可能包办所有功能的通信系统。可以说只有各种接入手段相互补充使用才能带来经济性、可靠性和有效性。因而,它可以在特定的区域和范围内发挥对 3G 的重要补充作用,WiFi 技术与 3G 技术相结合将具有广阔的发展前景。

4.3　蓝牙技术

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、笔记本电脑、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 Internet 之间的通信,从而数据传输变得更加迅速高效,为无线通信拓宽道路。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,其数据速率为 1Mbps,采用时分双工传输方案实现全双工传输。蓝牙模块如图 4-3 所示。

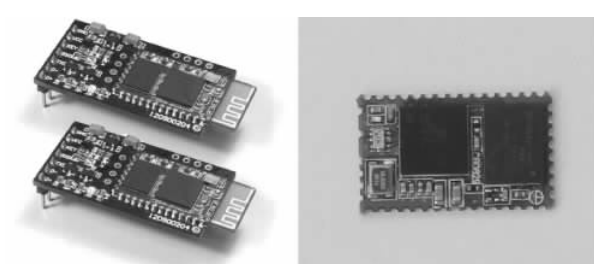

图 4-3　蓝牙模块

蓝牙技术是一个开放性、短距离无线通信的标准,它可以用来在较短距离内取代目前多种电缆连接方案,通过统一的短距离无线链路在各种数字设备之间实现方便快捷、灵活安全、低成本、小功耗的语音和数据通信。常见的蓝牙标志与蓝牙耳机如图 4-4 所示。

(a) 蓝牙标志　　(b) 蓝牙耳机

图 4-4　蓝牙标志与蓝牙耳机

4.3.1　蓝牙技术指标

蓝牙技术产品采用低能耗无线电通信技术来实现语音、数据和视频传输，其传输速率最高为 1Mbps，以时分方式进行全双工通信，通信距离为 10m 左右，配置功率放大器可以使通信距离进一步增加。

蓝牙产品采用跳频技术，能够抗信号衰落；采用快跳频和短分组技术，能够有效地减少同频干扰，提高通信的安全性；采用前向纠错编码技术，以便在远距离通信时减少随机噪声的干扰；采用 2.4GHz 的 ISM（即工业、科学、医学）频段，以省去申请专用许可证的麻烦；采用 FM 调制方式，使设备变得更为简单可靠；蓝牙技术产品一个跳频频率发送一个同步分组，每组一个分组占用一个时隙，也可以增至 5 个时隙；蓝牙技术支持一个异步数据通道，或者 3 个并发的同步语音通道，或者一个同时传送异步数据和同步语音的通道。蓝牙的每一个话音通道支持 64kbps 的同步话音，异步通道支持的最大速率为 721kbps、反向应答速率为 57.6kbps 的非对称连接，或者 432.6kbps 的对称连接。

蓝牙技术产品与 Internet 之间的通信，使得家庭和办公室的设备不需要电缆也能够实现互通互联，大大提高了办公和通信效率。蓝牙的系统参数与技术指标如表 4-1 所示。

表 4-1　蓝牙的系统参数与技术指标

系统参数与技术指标	说　　明
工作频段	ISM 频段，2.402～2.408GHz
双工方式	全双工，TDD 时分双工
业务类型	支持电路交换和分组交换业务
数据速率	1MBps
非同步信道速率	非对称连接 21 kb/s 或 57.6 kb/s，对称连接 432.6 kb/s
同步信道速率	64kb/s
功率	美国 1mW（FCC 要求＜0dbm），其他国家可扩展为 100mW
跳频频率数	79 个频点/1MHz
跳频速率	1600Hz
工作模式	PAPK/HOLD/SNIFF/ACTIVE
数据连接方式	SCO、ACL
纠错方式	1/3FEC、2/3FEC、ARQ
认证	竞争—应答方式
信道加密	0 位、40 位、60 位密钥
语音编码方式	CSVD
发射距离	10～100m

4.3.2　蓝牙技术特点

蓝牙技术提供低成本、近距离的无线通信，构成固定与移动设备通信环境中的个人网络，使得近距离内各种设备能够实现无缝资源共享。显然，这种通信技术与传统的通信模式有明显的区别，它的初衷是希望以相同成本和安全性实现一般电缆的功能，从而使移动用户摆脱电缆束缚。这决定了蓝牙技术具备以下技术特性。

(1) 能传送语音和数据。

(2) 使用频段、连接性、抗干扰性和稳定性。

(3) 低成本、低功耗和低辐射。

(4) 安全性。

(5) 网络特性。

4.4　全球定位系统技术

全球定位系统(Global Positioning System，GPS)是 20 世纪 70 年代由美国陆海空三军联合研制的新一代空间卫星导航定位系统。其主要目的是为陆、海、空三大领域提供实时、全天候和全球性的导航服务，并用于情报收集、核爆监测和应急通信等一些军事目的，是美国独霸全球战略的重要组成。经过 20 余年的研究实验，耗资 300 亿美元，到 1994 年 3 月，全球覆盖率高达 98%的 24 颗 GPS 卫星已布设完成。

4.4.1　GPS 组成

全球定位系统由空间卫星部分、地面监控部分和用户设备部分(GPS 接收机)三大部分组成，如图 4-5 所示。三者有各自独立的功能和作用，但又是有机地组合在一起而成为缺一不可的整体部分。

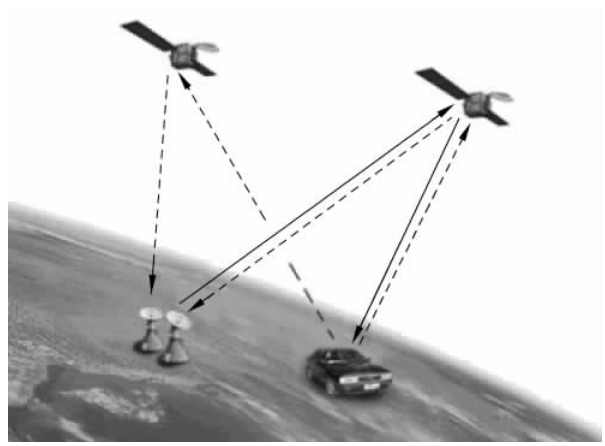

图 4-5　全球定位系统示意图