

# ZigBee（紫峰）技术简介

工业互联网领域常见短距离物联网技术，除了 Wi-Fi、蓝牙之外，还有一个很有前景的技术——ZigBee。

ZigBee 在过去的几年，一直是重要的无线通信协议之一，在物联网领域被广泛应用。



## 一、技术起源

### 1、ZigBee 由来

在使用蓝牙技术的过程中，人们发现，尽管它有许多优点，但对工业、家庭自动化控制和工业遥测遥控领域而言，它太复杂，功耗大，距离近，精度低、组网规模太小等弱点。

并且，对于工业现场，要求高可靠性的无线数据传输，能抵抗工业现场的各种电磁干扰，蓝牙技术并不能满足要求。

因此，ZigBee 协议在 2003 年正式问世了。

### 2、ZigBee 释义

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和远近信息的，依靠着这样的方式构成了群体中的通信网络。因此，ZigBee 的发明者们形象地利用蜜蜂的这种行为来给它命名。

### 3、ZigBee 协议

ZigBee 的 Mac 层、PHY 层是基于 IEEE802.15.4 协议的。

根据这个协议规定的技术，是一种近距离、低复杂度、低功耗、低数据速率、低成本的双向无线通信技术。主要适合于自动控制和远程控制领域，可以嵌入各种设备中，同时支持地理定位功能。

### 4、ZigBee 特点

**ZigBee 的特点**主要有以下几个方面：

(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。相比之下蓝牙可以工作数周、WiFi 可以工作数小时；

(2)低成本：通过大幅简化协议，使得 Zigbee 成本很低(不足蓝牙的 1/10)。另外，Zigbee 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 的协议专利免费；

(3)低速率：ZigBee 工作在 250kbps 的通讯速率，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 ~ 100m 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。相比较，蓝牙需要 3-10s、WiFi 需要 3s；

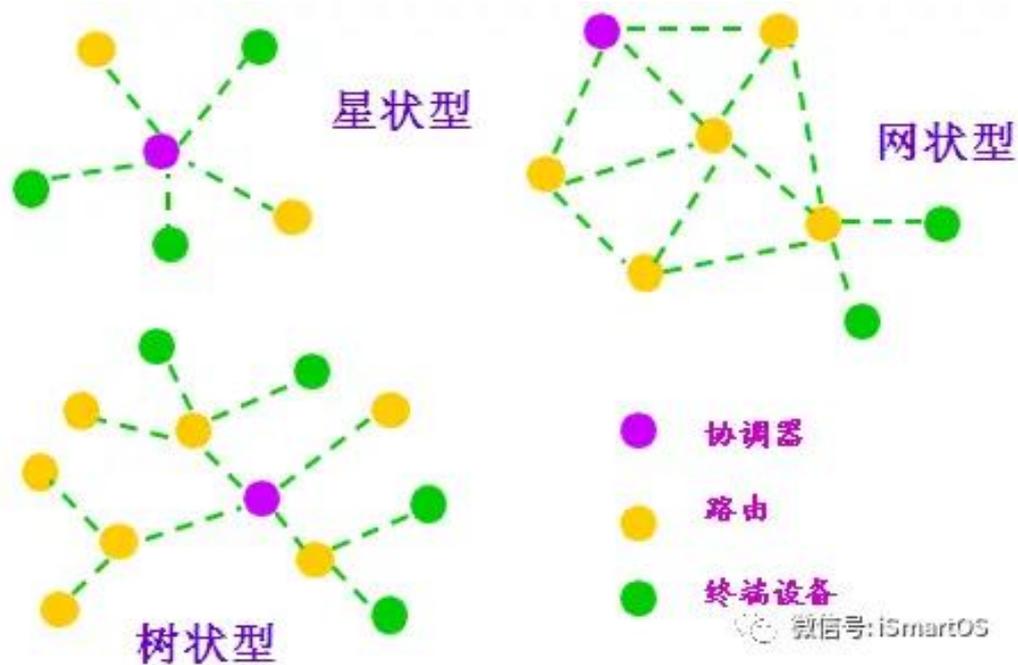
(6)大容量：ZigBee 可采用星状、片状和网状网络结构，由一个主节点管理若干子节点，最多一个主节点可管理 254 个子节点；同时主节点还可由上一层网络节点管理，最多可组成 65000 个节点的大网；

(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(AES128)的对称密码，以灵活确定其安全属性；

(8)免费频段：使用工业科学医疗(ISM)频段，915MHz(美国)，868MHz(欧洲)，2.4GHz(全球)，无需支付频段使用费用。

## **5、组网特点**

ZigBee 技术使用**网状网拓扑结构**，支持自动路由、动态组网、直序扩频的方式。这些特点，使之能够满足工业自动化控制现场的需要（低数据量，低成本，低功耗，高可靠性）。



## 二、通信技术篇

### 1、免费 2.4G 频段

在世界上大多数国家，使用无线电设备都是要支付频率使用费的，包括手机通信。只不过移动运营商或服务提供商已经向国家支付了这笔费用，并通过各种方式向用户收取了这笔费用。

而免费频段，是指各个国家根据各自的实际情况，并考虑尽可能与世界其他国家规定的一致性，而划分出来的一个频段，专门用于工业，医疗以及科学研究使用(ISM 频段)，不需申请而可以免费使用。

我们国家的 2.4G 频段，就是这样一个频段。

然而，为了保证大家都可以合理使用，国家对该频段内的无线收发设备，在不同环境下的使用功率做了相应的限制。例如在城市环境下，发射功率不能超过 100mW。

### 2、近距离通信

ZigBee 局域网络不仅可以通过提高每个节点模块的发射功率和接收灵敏度以及增加节点数量来扩展网络，而且可以通过传统的互联网去监控路途遥远的 ZigBee 控制网络。

但是，需要注意的是：

(1)随着发射功率的增加，耗电量自然要增大，便会失去 ZigBee 本身电能消耗很低的优势；

(2)尽管 2.4Ghz 是免费频段，但是不能超过电波法中对于最大功率的限制。

所以，通常还是将 Zigbee 用于**近距离通信场景**。

### 3、直序扩频通信

同样的频段，采用不同的通信方式则结果也许会有很大的差别。例如 ASK、FSK、FHSS、DSSS 等的抗干扰能力，通信安全保密性，可靠性都各不相同。

ZigBee 系统和 CDMA 系统一样，都采用的是直序扩频技术(DSSS)，它是一种抗干扰能力极强，保密性和可靠性都很高的通信方式。

扩频技术在正常通信时所要求的信噪比可以很低。也就是说，在干扰很强的环境下，它仍然能够正常工作。根据计算和实验，这相当于接收灵敏度提高了 7dBm。同时不容易干扰别人。

换句话说，它可以使用较低的功率传输更远的距离（在发射功率为 0dBm 的情况下，蓝牙通常能有 10 米的作用范围。而 ZigBee 在室内通常能达到 30-50 米的作用距离，在室外空旷地带甚至可以达到 400 米）

### 4、抗干扰性能

ZigBee 抗干扰特性主要是**抗同频干扰**，即来自共用相同频段的其他技术的干扰。

主要特性如下：

#### 1、空闲信道评估（Clear Channel Assessment, CCA）：

判断信道是否空闲。IEEE 802.15.4 物理层在碰撞避免机制中提供 CCA 的能力，即如果信道被其他设备占用，则允许传输退出而不必考虑采用该信道的通信协议。

#### 2、动态信道选择：

ZigBee 个人局域网（PAN）中的协调器（网络的中心节点，负责网络的组织和维护）。首先要扫描所有的信道，然后确认并加入一个合适的 PAN（不需要创建一个新的 PAN），减少同频段 PAN 的数量，降低潜在的干扰。如果干扰

源出现在重叠的信道上，协调器上层的软件要应用信道算法选择一个新的信道。

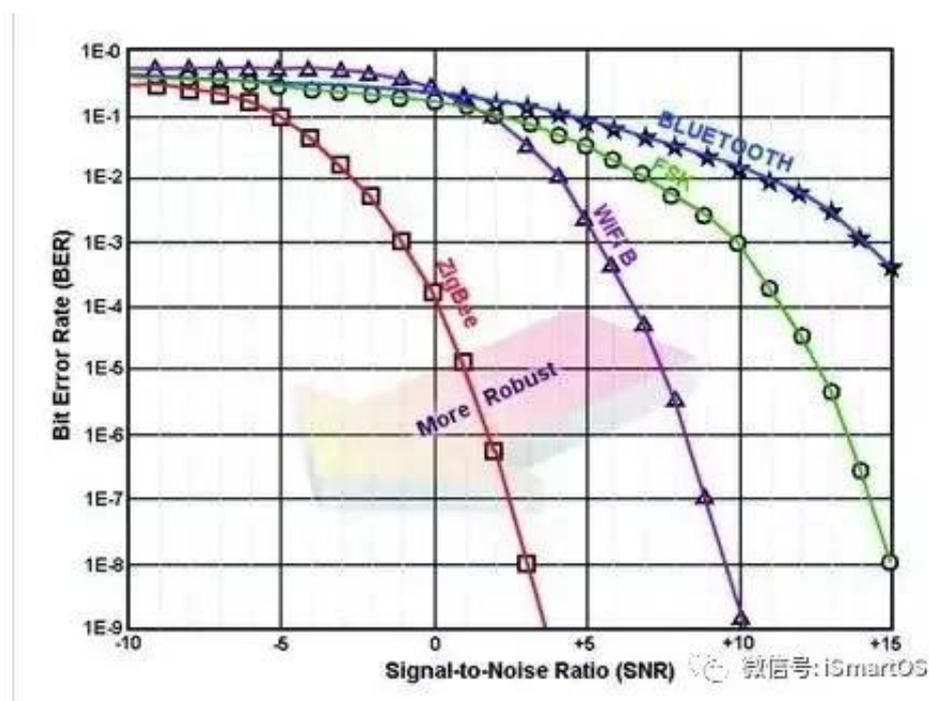
### 3、信道算法：

在网络初始化或者响应中断时，ZigBee 设备都会先扫描一系列被列入信道表参数中的信道，以便进行动态信道选择，按照上述空闲信道来设置信道表参数，以便加强网络的共存性能。

在严重干扰期间，ZigBee 不改变信道，而是依靠其低占空比、免冲突算法（每个设备在发送数据之前侦听信道）来减小由于传输冲突所造成的数据丢失。

### 4、直序扩频技术（DSSS）和频率快变 FA：

直接序列扩频技术具有一定的抗干扰效果（如下图所示），在其他条件相同情况下传输距离要大于跳频技术。所谓频率快变是改变频率、以避开一个已知干扰源或信号源的影响。



由上图可见，ZigBee 的误码率在信噪比为 4dB 的情况下可达  $10^{-9}$ ，要达到同样误码率，Wi-Fi 要达 10dB，蓝牙要达 16dB，Zigbee 的抗干扰性能明显高于 Wi-Fi 和蓝牙技术。

### 5、应答重传和帧缓存：

ZigBee 的 MAC 层和应用层(APS 部分)具有自动请求重传 ARQ 和帧缓存功能。当传送数据帧给设备时，如果接收设备处于忙或者休眠状态而不能接收该帧，那么网络的主协调设备就暂时缓存该帧，直到接收端接收该帧。

虽然调制方式很简单，但 ZigBee 在 2.4GHz ISM 频段表现出了很好的抗干扰性能，非常适合于低功耗、低数据传输的应用场合。

### **三、网络技术篇**

#### **1、无线数据传输**

ZigBee 是一个多个无线数传模块（多达 65000 个）组成的一个无线数传网络平台，十分类似现有的移动通信网络。每一个 ZigBee 网络数传模块类似移动网络的一个基站，在整个网络范围内，它们之间可以进行相互通信；每个网络节点间的距离可以从标准的 75 米，到扩展后的几百米，甚至几公里。

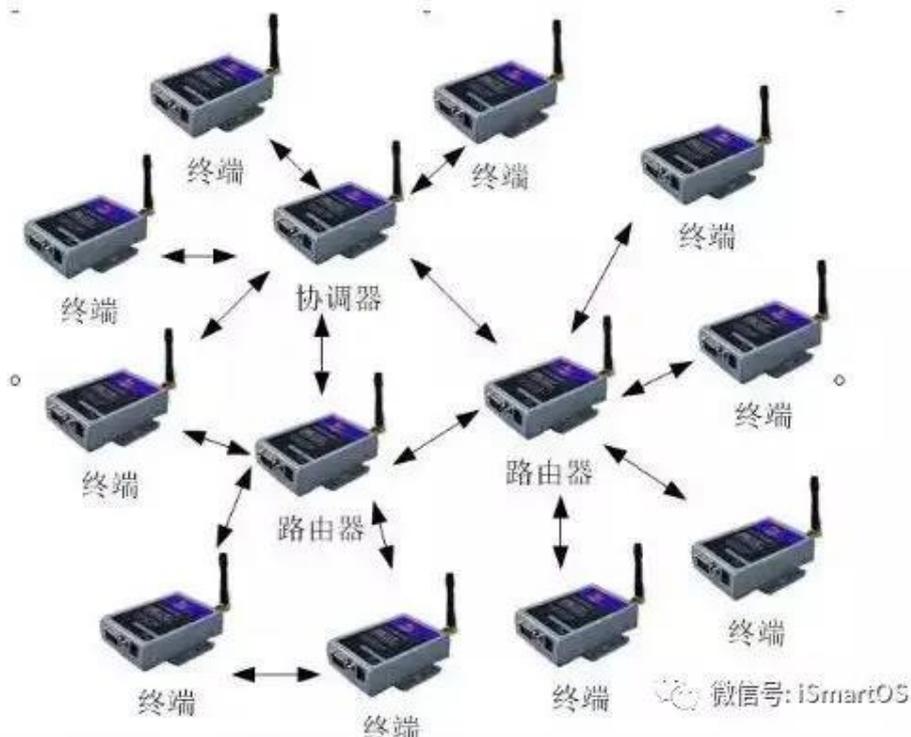
与移动通信网络不同的是，移动通信网每个基站价值一般都非常昂贵，而每个 ZigBee“基站”却非常便宜。

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，和多个不承担网络信息中转任务的孤立的子节点(RFD)无线连接。

#### **2、自组织网**

举一个简单的例子就可以说明这个问题，当一队伞兵空降后，每人持有一个 ZigBee 网络模块终端，降落到地面后，只要他们彼此间在网络模块的通信范围内，通过彼此自动寻找，很快就可以形成一个互联互通的 ZigBee 网络。模块还可以通过重新寻找通信对象，确定彼此间的联络，对原有网络进行刷新。这就是自组织网。



### 3、自组织网通信

网状网通信实际上就是多通道通信，在实际工业现场，由于各种原因，往往并不能保证每一个无线通道都能够始终畅通，就像城市的街道一样，可能因为车祸，道路维修等，使得某条道路的交通出现暂时中断。

此时由于我们有多个通道，车辆(相当于我们的控制数据)仍然可以通过其他道路到达目的地，而这一点对工业现场控制而言则非常重要。

### 4、自组织网动态路由

所谓动态路由是指网络中数据传输的路径并不是预先设定的，而是传输数据前，通过对网络当时可利用的所有路径进行搜索，分析它们的位置关系以及远近，然后选择其中的一条路径进行数据传输。

在我们的网络管理软件中，路径的选择使用的是“梯度法”，即先选择路径最近的一条通道进行传输，如传不通，再使用另外一条稍远一点的通路进行传输，以此类推，直到数据送达目的地为止。

在实际工业现场，预先确定的传输路径随时都可能发生变化，或者因各种原因路径被中断了，或者过于繁忙不能进行及时传送。动态路由结合网状网拓扑结构，就可以很好解决这个问题，从而保证数据的可靠传输。

## 四、市场应用

## 1、应用领域

ZigBee 因其低功耗、低时延、高可靠性和短距离的无线通信协议特点，主要适用于无线自动控制领域，可嵌入到各种小型设备之中，目前广泛应用于短距离通讯、智能家居、工业自动化、智慧城市以及智慧农业等行业。



## 2、拓展应用

ZigBee 应用范围非常广泛，可以针对工业自动化、家庭自动化、遥测遥控、汽车自动化、农业自动化和医疗护理、油田、电力、矿山和物流管理等应用领域。

实际应用举例如下：区域定位、照明控制、环境控制、自动读表系统、各类窗帘控制、烟雾传感器、医疗监控系统、大型空调系统、内置家居控制的机顶盒及万能遥控器、暖气控制、家庭安防、工业和楼宇自动化。

另外它还可以对局部区域内移动目标例如城市中的车辆进行定位。

## 3、应用条件

通常，符合如下条件之一的短距离通信就可以考虑应用 ZigBee：

- (1)需要数据采集或监控的网点多;
- (2)要求传输的数据量不大，而要求设备成本低;
- (3)要求数据传输可靠性高，安全性高;
- (4)要求设备体积很小，不便放置较大的充电电池或者电源模块;
- (5)可以用电池供电;
- (6)地形复杂，监测点多，需要较大的网络覆盖;
- (7)对于那些现有的移动网络的盲区进行覆盖;
- (8)已经使用了现存移动网络进行低数据量传输的遥测遥控系统。

## 4、应用情况

尽管国内不少人已经开始关注 ZigBee 这项新技术，而且也有不少企业开始涉足 ZigBee 技术的开发，然而，考虑到 ZigBee 本身是一种新的系统集成技术，应用软件的开发必须用网络传输，射频技术和底层软硬件控制技术结合在一起，所以对于初期开发的企业来说具有一定的技术难度。由于各方面的制约，ZigBee 技术的大规模商业应用还有待时日。

但是目前已经展示出了非凡的应用价值，相信随着相关技术的发展和推进，一定会得到更大的应用。

## **五、总结**

ZigBee 信道带宽是一种用于无线网络的高性能信道带宽技术，它可以提供高效的信号传输，并且可以在低功耗和高速率的情况下使用。ZigBee 信道带宽技术可以被用于无线传感器网络，物联网，自动化系统，家庭自动化，网络安全，移动设备和其他应用。它的传输距离可以达到 30 米，可以支持多个节点的连接，每个节点可以支持多个设备，使用 ZigBee 信道带宽可以实现高效的信号传输。