DOI:10.16086/j.cnki.issn1000-0380.2005.06.002



# ZigBee 无线通信技术及其应用探讨

## ZigBee Wireless Communication Technology and Investigation on Its Application

周怡[illegible]　凌志浩　吴勤勤
（华东理工大学，上海　200237）

摘　要　在对现有无线通信技术进行比较的基础上，着重对ZigBee技术及其协议和特点等作了剖析，对目前市场上所能提供的器件和开发套件作了简单叙述，并对ZigBee在工控无线通信网络中的应用支持作了探讨。

关键词　无线通信　ZigBee　协议　套件

**Abstract**　Analyse the ZigBee technology based on the comparison of the present wireless communication technology, laying stress on its protocol and features. Introduce the ZigBee device and development kits available in market. And discuss the ZigBee application especially in industrial control wireless network.

**Keywords**　Wireless communcation　ZigBee　Protocol　kit

## 0　引言

工业领域在现代化的进程中通过引入各种先进技术，实现了劳动生产率的提高和生产成本的下降。在这些技术中，最典型的就是数字化技术和现代通信技术。在现代工业数字化的基础上，工业生产监控早已突破了单回路控制与监视的功能。随着计算机软硬件技术、网络技术和工业综合自动化系统整合水平的不断发展，对数据接口的开放性、数据传输的实时性、数据连接的安全性等方面提出了更高的要求。许多大型企业其生产地域分散，业务分工复杂，往往设有一个或者多个控制中心，以及大量的现场数据采集点。这些采集点因分散而需要通过一定的通信手段来实现与中心控制单元间的数据交互，进而实现生产过程的自动化。由于传统有线网络本身的局限性，许多特殊环境下的网络覆盖和网络支持仍然是个难题。比如在某些工业现场，一些工业环境禁止或限制使用电缆，而在其他一些工业环境要求完全把电缆屏蔽起来以高度防止来自大多数工业设施中的机器或其它无线电控制设备的干扰，更有一些高速旋转的设备根本无法通过电缆来传输数据信息。而无线广域网、无线局域网和无线个人网技术却能有效地提供对这些问题的解决方案。

在现有的无线网络技术发展条件下，无线标准增加了灵活性，并降低了集成专利无线通信的风险。在工控场合的应用条件下，短距离的无线传输尤其受到瞩目。在最近的几年中，人们不断探索，形成了当今令人眼花缭乱的无线通信协议和产品。最流行的短距离无线数据通信的标准有蓝牙（Bluetooth）、Wi-Fi（IEEE802.11）、IrDA以及极具发展潜力、已被众多业界认可的ZigBee（IEEE802.15.4）等。

## 1　几种无线传输技术及其比较

### 1.1　蓝牙（BlueTooth）

蓝牙（BlueTooth）最早是爱立信在1994年开始研究的一种能使手机与其附件（如耳机）之间互相通信的无线模块。1998年，爱立信、诺基亚、IBM等公司共同推出了蓝牙技术，主要用于通信和信息设备的无线连接。它的工作频率为2.4GHz，有效范围大约在10m半径内。Bluetooth列入了IEEE802.15.1，规定了包括PHY、MAC、网络和应用层等集成协议栈。为对语音和特定网络提供支持，需要协议栈提供250kB系统开销，从而增加了系统成本和集成复杂性。另外，Bluetooth对每个“Piconet”（微微网）有只能配置7个节点的限制，制约了其在大型传感器网络开发中的应用。

### 1.2　Wi-Fi（IEEE802.11）

Wi-Fi（Wireless Fidelity，无线高保真）也是一种无线通信协议。IEEE802.11的最初规范是在1997年提出的。主要目的是提供WLAN接入，也是目前WLAN的主要技术标准，其工作频率也是2.4GHz。目前，IEEE802.11标准还没有被工业界广泛接受。IEEE802.11流行的几个版本包括“a”（在5.8GHz波段带宽为54MBps）、“b”（波段2.4GHz带宽为11MBps）、“g”（波段2.4GHz带宽为22MBps）。这种复杂性为用户选择标准化无线平台增加了困难。Wi-Fi规定了协议的物理（PHY）层和媒体接入控制（MAC）层，并依赖TCP/IP作为网络层。由于其优异的带宽是以大的功耗为代价

的,因此大多数便携 Wi-Fi 装置都需要常规充电。这些特点限制了它在工业场合的推广和应用。

### 1.3　IrDA

红外线数据协会 IrDA(Infrared DataAssociation)成立于 1993 年。IrDA 是一种利用红外线进行点对点通信的技术。IrDA 标准的无线设备传输速率已从 115.2kbps 逐步发展到 4Mbps、16Mbps。目前,支持它的软硬件技术都很成熟,在小型移动设备(如 PDA、手机)上被广泛使用。它具有移动通信所需的体积小、功耗低、连接方便、简单易用成本低廉的特点。IrDA 用于工业网络上的最大问题在于只能在 2 台设备之间连接,并且存在有视距角度等问题。

### 1.4　ZigBee

ZigBee(IEEE802.15.4)技术是最近发展起来的一种短距离无线通信技术,功耗低,被业界认为是最有可能应用在工控场合的无线方式。它同样使用 2.4GHz 波段,采用跳频技术和扩频技术。

另外,它可与 254 个节点联网。节点可以包括仪器和家庭自动化应用设备。它本身的特点使得其在工业监控、传感器网络、家庭监控、安全系统等领域有很大的发展空间。

几种常用无线传输方式的主要性能比较见表 1。

表 1　无线传输方式的比较

| | BlueTooth (802.15.1) | Wi-Fi (802.11b) | IrDA | ZigBee (802.15.4) |
|---|---|---|---|---|
| 系统开销 | 较大 | 大 | 小 | 小 |
| 电池寿命 | 较短 | 短 | 长 | 最长 |
| 网络节点 | 7 | 30 | 2 | 255/65000+ |
| 物理范围(有效) | 10m | 100m | 定向 1m | 1—100+ |
| 传输率 | 1Mbps | 11Mbps | 16Mbps | 20/250kbps |
| 传输介质 | 2.4GHz 射频 | 2.4GHz 射频 | 980nm 红外 | 2.4GHz 射频 |

## 2　ZigBee 的技术内容及特点

ZigBee 是最新确定的商业名称,在以前曾被发起者以“HomeRF lite”、“Firefly”和“RF-EasyLink”等命名。为了满足类似于传感器的小型、低成本设备无线联网的要求,2000 年 12 月 IEEE 成立了 IEEE802.15.4 工作组,致力于定义一种供廉价的固定、便携或移动设备使用,且复杂度、成本和功耗均很低的低速率无线连接技术。ZigBee 联盟成立于 2001 年 8 月。

到目前为止,除了 Invensys、三菱电子、摩托罗拉、三星和飞利浦等国际知名的大公司外,该联盟大约已有百余家成员企业,并在迅速发展壮大。其中涵盖了半导体生产商、IP 服务提供商、消费类电子厂商及 OEM 商等,例如 Honeywell、Eaton 和 Invensys Metering Systems 等工业控制和家用自动化公司,甚至还有像 Mattel 之类的玩具公司。所有这些公司都参加了负责开发 ZigBee 物理和媒体控制层技术标准的 IEEE802.15.4 工作组。

在工业、农业、车载电子系统、家用网络、医疗传感器和伺服执行机构等领域,对于无线网络的要求与民用场合有很大区别。它通常对数据吞吐量的要求很低,功率消耗要低。此外,简单方便、可以随意使用的无线装置大量涌现,需要布置大量的无线接入点,而低廉的价格将起着关键作用。所以 ZigBee 标准要解决的问题是设计一个维持最小流量的通信链路和低复杂度的无线收发信机。要考虑的核心问题是低功耗和低价格的设计,这就要求该标准应提供低带宽、低数据传输率的应用。

### 2.1　ZigBee 的特点

① 低功耗:由于 ZigBee 的传输速率低,发射功率仅为 1mW,而且采用了休眠模式,功耗低,因此 ZigBee 设备非常省电。据估算,ZigBee 设备仅靠两节 5 号电池就可以维持长达 6 个月到 2 年左右的使用时间,这是其它无线设备望尘莫及的。

② 成本低:ZigBee 模块的初始成本在 6 美元左右,估计很快就能降到 1.5～2.5 美元,并且 ZigBee 协议是免专利费的。低成本对于 ZigBee 也是一个关键的因素。

③ 时延短:通信时延和从休眠状态激活的时延都非常短,典型的搜索设备时延为 30ms,休眠激活的时延是 15ms,活动设备信道接入的时延为 15ms。因此 ZigBee 技术适用于对时延要求苛刻的无线控制(如工业控制场合等)应用。

④ 网络容量大:一个星型结构的 ZigBee 网络最多可以容纳 254 个从设备和一个主设备,而且网络组成灵活。

⑤ 可靠:采取了碰撞避免策略,同时为需要固定带宽的通信业务预留了专用时隙,避开了发送数据的竞争和冲突。MAC 层采用了完全确认的数据传输模式,每个发送的数据包都必须等待接收方的确认信息。如果传输过程中出现问题可以进行重发。

⑥ 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。

### 2.2　ZigBee 与 IEEE802.15.4 的联系

人们常会把 ZigBee 和 IEEE802.15.4 等同起来，其实两者之间还是有所区别的：

① ZigBee 完整、充分地利用了 IEEE802.15.4 定义的功能强大的物理特性的优点；

② ZigBee 增加了逻辑网络和应用软件；

③ ZigBee 基于 IEEE802.15.4 射频标准，同时 ZigBee 联盟通过与 IEEE 紧密工作来确保一个集成的完整的市场解决方案；

④ 802.15.4 工作组主要负责制定物理层（PHY）和媒体访问控制（MAC）层标准，而 ZigBee 负责网络层和应用层的开发。

图 1 示意了 ZigBee 的结构和分工。

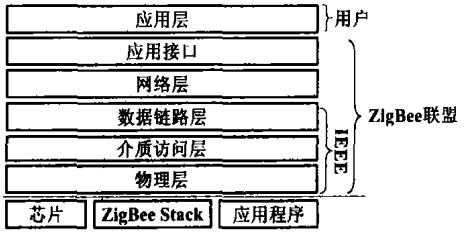


图 1　ZigBee 的结构和分工

### 2.3　802.15.4 协议架构及其技术特点

IEEE802.15.4 满足国际标准组织（ISO）开放系统互连（OSI）参考模式，定义了单一的 MAC 层和多样的物理层。ZigBee 联盟制定了 MAC 层以上协议，其协议套件由高层应用规范、应用汇聚层、网络层、数据链路层和物理层组成。

#### 2.3.1　物理层

IEEE802.15.4 提供了图 2 所示的两种物理层的选择（868/915MHz 和 2.4GHz），物理层与 MAC 层的协作扩大了网络应用的范畴。这两种物理层都采用直接序列扩频（DSSS）技术，降低了数字集成电路的成本，并且都使用相同的帧结构，以便低作业周期、低功耗地运作。

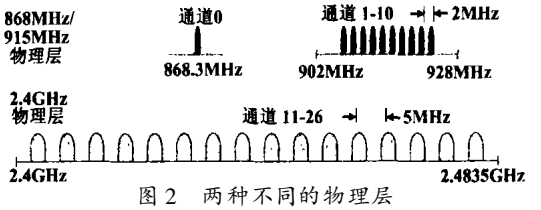


图 2　两种不同的物理层

2.4G 物理层的数据传输率为 250kbps，868/915MHz 物理层的数据传输率分别是 20kbps、40kbps。2.4GHz 物理层的较高速率主要归因于基于 DSSS 方法（16 个状态）的准正交调制技术。来自物理层收敛协议数据单元（PPDU）的二进制数据被依次（按字节从低到高）组成 4 位二进制数据符号，每种数据符号（对应 16 状态组中的一组）被映射成 32 位伪噪音码片，以便传输。然后采用最小移位键控方式 MSKI 对这个连续的伪噪音码片序列进行调制，即采用半正弦脉冲波形的偏移四相移相键控（O－QPSK）方式调制。868/915MHz 物理层使用简单 DSSS 方法，每个 PPDU 数据传输位被最大长为 15 的码片序列（m－序列）所扩展。不同的数据传输率适用于不同的场合，如 868/915MHz 物理层的低速率换取了较好的灵敏度（－85dbm/2.4G，－92dbm/868，915MHz）和较大的覆盖面积，从而减少了覆盖给定物理区域所需的节点数；而 2.4G 物理层的较高速率适用于较高的数据吞吐量、低延时或低作业周期的场合。

#### 2.3.2　介质访问层

ZigBeeMAC 层的设计需要考虑到降低成本、容易实现、可靠的数据传输、短距离操作及非常低的功耗等要求，为此采用了如下所示的简单且灵活的协议：

① 采用 IEEE 标准 64－bit 和 16－bit 短地址；

② 基本网络容量可以达到 254 节点；

③ 可以配置使用大于 65,000（$2^{16}$）节点的本地简单网络，而且开销不大；

④ 网络协调器、全功能设备（FFD）和简化功能设备（RFD）等 3 种指定设备；

⑤ 简化帧结构；

⑥ 可靠的数据传输；

⑦ 联合/分离；

⑧ AES－128 安全机制；

⑨ CSMA－CA 通道；

⑩ 可选的使用信标的超级帧结构。

IEEE802.15.4MAC 子层定义了广播帧、数据帧、确认帧和 MAC 命令帧等 4 种帧类型。只有广播帧和数据帧包含了高层控制命令或者数据，确认帧和 MAC 命令帧则用于 ZigBee 设备间 MAC 子层功能实体间控制信息的收发。广播帧和确认帧不需要接收方的确认，而数据帧和 MAC 命令帧的帧头包含帧控制域，指示收到的帧是否需要确认，如果需要确认，并且已经通过了 CRC 校验，接收方将立即发送确认帧。若发送方在一定时间内收不到确认帧，将自动重传该帧。这就是 MAC 子层可靠传输的基本过程。

MAC 层的通用帧格式如图 3 所示。

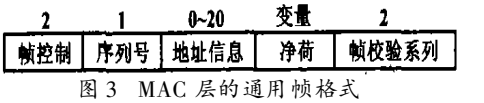


图 3　MAC 层的通用帧格式

#### 2.3.3　网络层

网络层包括逻辑链路控制子层。802.2 标准定义了 LLC，并且通用于诸如 802.3、802.11 及 802.15.1 等

802 系列标准中，而 MAC 子层与硬件联系较为紧密，并随不同物理层的实现而变化。网络层负责拓扑结构的建立和维护、命名和绑定服务，它们协同完成寻址、路由及安全这些不可或缺的任务。

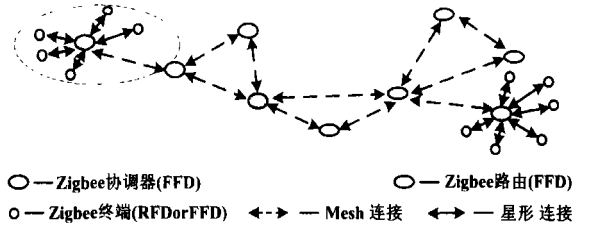


图 4　ZigBee 的网络结构

IEEE802.15.4 标准草案支持多种网络拓扑结构，包括图 4 所示的新型网状网络(Mesh)。计算机外围设备等要求低延迟等待接入的应用一般采用星型网络结构，而其它一些应用，如周边安全等可能要求大面积网状网络的覆盖。多址的形式包括 IEEE 标准 64 位和短地址 8 位。

## 3　ZigBee 目前的开发环境

由于 ZigBee 问世不久，加之协议也刚刚确定，所以市场上可供选择的产品不多。在几大 IC 厂商的鼎力支持和推动下，现在市面上已经有了一些供开发人员应用的器件或者套件，而且越来越多的 ZigBee 芯片和模块陆续问世，这将极大地方便人们进行产品开发。

下面就已面市的开发模块或套件作一简单叙述。

### 3.1　摩托罗拉——飞思卡尔

摩托罗拉的全资子公司飞思卡尔(Freesacle Semiconductor)是 IEEE802.15.4 标准机构的重要成员。摩托罗拉已经推出了针对 ZigBee 的开发套件。

① MC13191＋GT16/32 套件：支持简单的 MAC 层(SMAC)(＜2.5kB)；提供源代码以方便开发人员了解 ZigBee 的运作流程；支持点对点和星状网的网络拓扑结构。

② MC13192＋GT32/60 套件：提供 802.15.4MAC(目标码)；支持简单的 MAC；支持点对点、星状网和树状网的网络拓扑结构。

③ MC13192＋GT60 套件：支持网状(Mesh)网络，同时提供 Z－stack 等开发工具和源代码

飞思卡尔的 ZigBee 解决方案主要是通过一个 8 位 MCU 和一个 ZigBee 收发模块来实现基于 ZigBee 的应用开发。它提供参考手册、开发板和源代码，以帮助用户加快开发速度。图 5 示意了 Motorola 的解决方案。

### 3.2　Ember

作为 ZigBee 的 Promoter 之一，Ember 在开发 ZigBee 方面也做了很多工作。现已开发出 EM1020、EM2040 两款 RF 收发器。它提供一个高速的硬件串口与主机连接，并且提供 EmberNet 的开发环境以方便用户开发。EM2420 是一个真正兼容 IEEE802.15.4 的 2.4GHz 单芯片 RF 收发器，满足低功耗和低电压设计，包括 DSSS 基带 modem 和 250kbps 数据速率，但只适用于 Ember 授权的网络栈以供 8 位芯片使用。图 6 所示为使用 EM2420 的嵌入式无线网络。

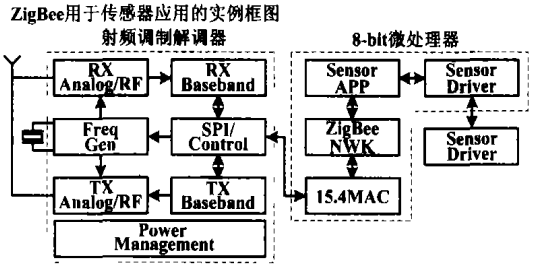


图 5　Freescale 的 ZigBee 解决方案

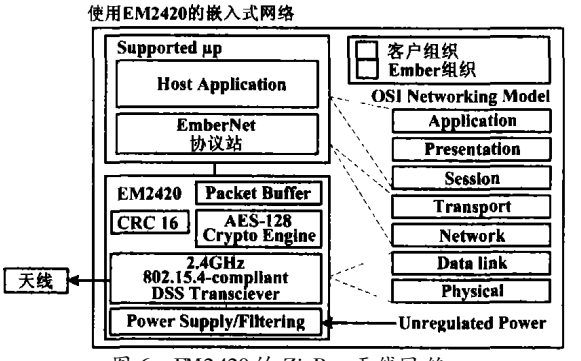


图 6　EM2420 的 ZigBee 无线网络

### 3.3　Chipcon

挪威半导体公司 Chipcon 推出的 CC2420 是全球首颗符合 ZigBee 联盟标准的 2.4GHz 射频芯片。CC2420 基于 Chipcon 公司的 SmartRF03 技术，采用 0.18μm 工艺。为了保持和 ZigBee 标准一致，CC2420 支持 250kbps 数据传输率。

该公司现在还提供开发工具套件。通过套件用户可以很快地进行 ZigBee 网络的评估和设计。这个套件包括一个基于 CC2420 的内嵌 Z－Stack™ ZigBee 协议栈的硬件模块。软件包括用于首次定制的 Z－Stack™ ZigBee 网络配置器、用于建立用户自己应用程序框架的 Z－Stack™ ZigBee Profile Builder 以及为方便网络调试而提供的 Z－Tool™ ZigBee Protocol Stack Trace 工具。Chipcon 公司可以提供 CC2420 样片。

此外 Atmel 也将提供 AT86RF210Z－Link™ 收发器，允许在 868/915MHz 的物理层实现 20kbps 到 40kbps 的数据收发速率；Crossbow 提供小型多频段智能的无线模块 MICAz(MPR2400)、MICA2(MPR400)和 MICA2DOT

(MPR500);赫立讯科技(Helicomm)提供 ZigBee 小型无线模块,包括射频收发器、10－bit A/D 转换和兼容 8051 的微控制器。另外 Jennic 和 Microchip 也都有各自 ZigBee 的单芯片或套件设备面市。

从以上的介绍中可以看出,使用上述公司提供的开发器件或套件就可以方便地开发出自己的 ZigBee 产品。随着 ZigBee 越来越被大家熟识和进入快速发展期,市场上提供的开发套件和芯片将会越来越多,这对简化设计、加快开发速度有利。

## 4　ZigBee 的应用支持及其设计方案

由上述介绍可以发现,利用现有的工具和套件已经可以进行应用产品的开发。下面以 Motorola 的 ZigBee/802.15.4 Evaluation Kit 为例,着重对开发方式加以说明。

ZigBee/802.15.4 Evaluation Kit 是一套 ZigBee 的评估开发套件,它能帮助开发人员较快地掌握 ZigBee 系统的开发方式。

### 4.1　硬件部分

该评估套件包括 13192－EVB 和 13192－SARD 两块印刷板。板上载有预先上传的显示程序,并允许用户通过工具上传用户应用程序。

两块电路板都包括了一块 Freescale 的 MC908HCS08 GT60 MCU 和一块 Freescale MC13192 射频芯片。MC908HCS08 GT60 是 HCS08 系列之一,是一款 8 位、低功耗、高性能的微处理器,内部包括 60KB 的嵌入式 Flash 和 4KB 的 RAM,其 Flash 的段大小为 512B。

MC13192 射频收发器是一个小型的无线电收发装置,使用 2.4GHz ISM 波段,可以通过 SPI 接口同微处理器进行通信,支持 IEEE802.15.4 标准的拓扑结构。如果需要 Mesh 结构可以选用 MC13193。

### 4.2　软件部分

包括简单应用的 SMAC 软件包和 CodeWarrior™ Development Studio。开发过程可以通过 CodeWarrior™ Development Studio 进行,简单方便。

开发前期可以通过提供的板载演示程序或简单应用程序来熟悉 ZigBee 的具体内容;开发中期可以针对某个简单任务开发自己的最小系统或简单系统;开发后期可以尝试开发一些有一定难度的应用方案,也可以针对某种仪表进行 ZigBee 无线解决方案的应用。

## 5　结束语

ZigBee 是一个针对传感器网络、建筑自动化等应用的短距离无线技术规范。ZigBee 是近距离、低复杂度、低功耗、低数据速率、低成本的双向无线通信技术,主要适用于自动控制和远程控制领域,是为满足小型、廉价设备的无线联网和控制而制定的。它按高度省电要求设计,因此低功耗和较低数据传输率意味着不会和 Wi－Fi 等其它无线技术竞争,而是作为传感路网络等应用的性价比较高的方案。业界对它在上述领域的应用进展充满信心。

2004 年 12 月 14 日,ZigBee 联盟宣布 ZigBee 规范已获批准。这一消息将极大激励 ZigBee 相关产品的发展,也将大大加快 ZigBee 进入市场的步伐。

参考文献


1　郦亮. IEEE802.15.4 标准及其应用. 电子设计应用, 2003
2　王权平, 王莉. ZigBee 技术及其应用. 现代电信科技, 2004
3　韩旭东, 张春业, 李鹏. 传感器无线互联标准及实现. 电子技术应用, 2004
4　陈晓琛, 申伟, 王隽. 低速无线个人区域网的实现. 电信快报, 2004
5　彭立, 徐红漫. 发展中的 IEEE802.15.4 现代电信科技, 2004
6　王永铭, 邵之江. 工业监控中的无线网络设计与应用. 工业仪表与自动化装置, 2003
7　彭天笑, 缪小红. 基于 ZigBee 的 WPAN 构建方案. 电信工程技术与标准化, 2003
8　戴迎瑁, 方会平. 无线个人区域网(WPAN)技术综述. 浙江万里学院学报, 2004
9　陈宏林. 无线新手短兵相接——Bluetooth 的同类新技术 ZigBee. 2004
10　蔡型, 张思全. 短距离无线通信技术综述. 现代电子技术, 2004
11　Jon Adams. Designing with 802.15.4 and ZigBee. www.zigbee.org 2004
12　Patrick Kinney. IEEE802.15.4 Status. www.zigbee.org 2004
13　Dick Caro. ZigBee short on power by design. www.eedesign.com, 2004
14　Patrick Kinney ZigBee Technology: Wireless Control that Simply Works. www.zigbee.org 2003
15　Microchip Technology Inc. Microchip 推出完整 ZigBee™ 演示和开发平台支持多种射频收发器并提供免费软件堆栈. www.eetchina.com, 2004
16　Microchip Technology Inc. PICDEMZ Demonstration Kit User's guide. www.microchip.com, 2004
17　Freescale Semiconductor, Inc. ZigBee Technology from Freescale. www.freescale.com, 2004
18　Freescale Semiconductor, Inc. Zigbee802.15.4 Evaluation Kit. www.freescale.com, 2004
19　Freescale Semiconductor, Inc. 802.15.4 MAC/PHY Software guide. www.freescale.com, 2004


修改稿收到日期:2005－01－24。

第一作者周怡[illegible],男,1979 年生,2002 年毕业于华东理工大学自动化系,现为华东理工大学检测专业在读硕士研究生;主要从事工控嵌入式系统的研究和开发。