

# 甚低功耗无线通信技术——ZigBee

## ZigBee—Very Low-Power Wireless Communication Technology

**摘要:** ZigBee技术作为无线传感器网络的主要支撑技术获得人们广泛的关注。完整的ZigBee协议套件由高层应用规范、应用会聚层、网络层、数据链路层和物理层组成。网络层以上协议由ZigBee联盟制订,物理层和媒体访问控制(MAC)层采用IEEE 802.15.4标准。IEEE802.15.4物理层简单采用比特到符号映射技术、符号到码片序列转换技术、偏移正交相移键控(OQPSK)调制技术,无须信道编码等复杂算法;MAC层采用载波监听多址-冲突避免技术,支持休眠模式。整个协议的设计使得ZigBee技术具有数据传输速率低、功耗低、成本低等特点,更加适合于工业监控系统、传感器网络、家庭监控系统、安全系统等应用。

**关键词:** 无线传感器网络; ZigBee技术; IEEE 802.15.4协议; 物理层; 多址接入控制

**Abstract:** ZigBee, an important technology supporting wireless sensor networks, has drawn broad attention. A complete ZigBee's protocol suite consists of high-layer application specifications, the application convergence layer, the network layer, the data link layer, and the physical layer. ZigBee Alliance focuses on defining the protocols above the network layer. The Physical (PHY) layer and the Media Access Control (MAC) layer are defined by the IEEE 802.15.4 standard. The IEEE 802.15.4 physical layer adopts technologies of mapping from bit to symbol, conversion from symbol to chip sequence and Offset Quadrature Phase-shift Keying (OQPSK) modulation, avoiding such complex algorithms as channel coding. The IEEE 802.15.4 MAC layer adopts Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) technology and supports the sleeping mode. ZigBee enables low data rates, low power consumption and cost-effectiveness, and is more applicable to industrial monitoring system, sensor networks, home monitoring system and security system.

**Key words:** wireless sensor network; ZigBee technology; IEEE 802.15.4; the physical layer; multiple access control

张平/ZHANG Ping  
康桂霞/KANG Gui-xia  
田辉/TIAN Hui

(北京邮电大学 无线新技术研究所, 北京 100876)  
(Wireless Technology Innovation Institute,  
Beijing Univ. of Posts and Telecommunications,  
Beijing 100876, China)

中图分类号:

TN915

文献标识码:

A

文章编号:

1009-6868 (2006) 04-0021-05

近十几年来, 无线与移动通信以前所未有的速度迅猛发展。随着各种便携式个人通信设备与家用电器设备的增加, 人们享受蜂窝移动通信系统带来的便利的同时, 对短距离的无线与移动通信又提出了新的需求, 使得短距离无线通信异军突

起, 包括无线局域网、蓝牙技术、移动Ad Hoc网、超宽带(UWB)以及ZigBee技术等各种热点技术相继出现, 均展现出各自巨大的应用潜力。其中, 低速率、低功耗、低成本的ZigBee技术作为无线传感器网络的主要支撑技术获得广泛的关注<sup>[1-4]</sup>。

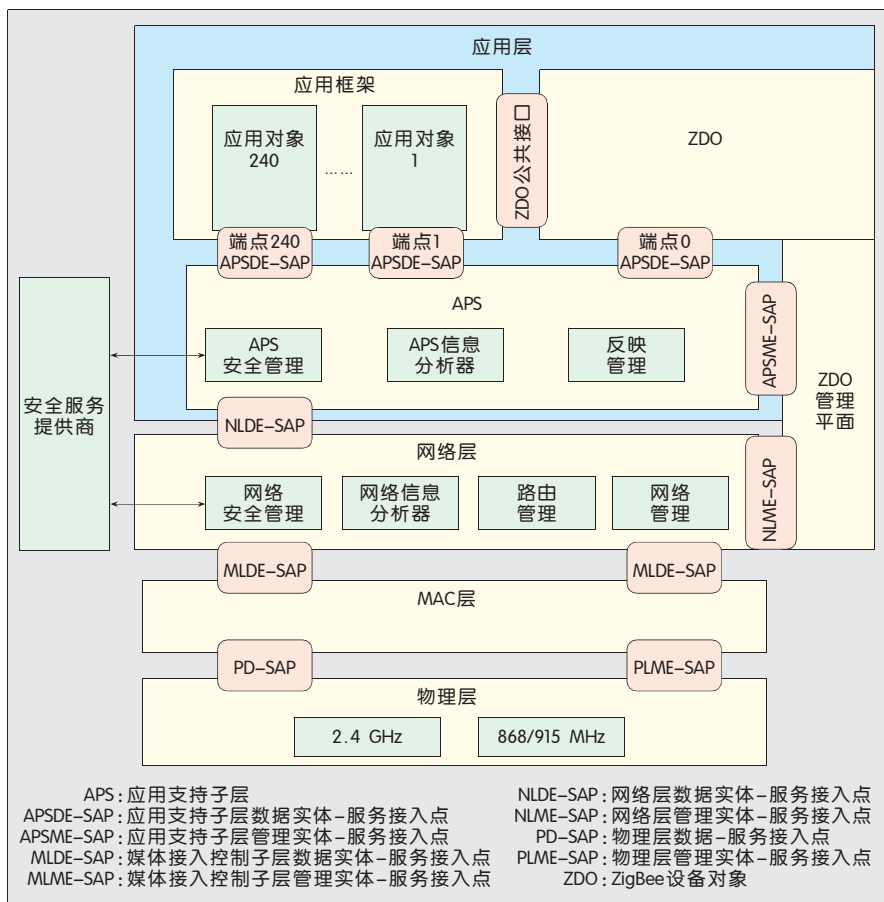
ZigBee是短距离通信的一种新兴技术。它使用2.4 GHz波段, 采用跳频

技术。与蓝牙相比, ZigBee更简单、功率及费用也更低, 能够比蓝牙更好地支持游戏、消费电子、仪器和家庭自动化应用。人们期望能在工业监控、传感器网络、家庭监控、安全系统和玩具等领域拓展ZigBee的应用<sup>[5]</sup>。

ZigBee的技术特点在于:

- 数据传输速率低, 只有10 ~ 250 kb/s。

**基金项目:** 北京市自然科学基金项目 (4062023)



▲图1 ZigBee协议框架

• 功耗低。在低功耗待机模式下,两节普通5号干电池可使用6个月到2年,免去了充电或者频繁更换电池的麻烦。

• 成本低。ZigBee数据传输速率低,协议简单,且免收专利费,所以大大降低了成本。

• 网络容量大。每个ZigBee网络最多可支持255个设备。

• 时延短。通常时延为15~30ms。

• 安全。ZigBee提供了数据完整性检查和鉴权功能,采用先进加密标准-128(AES-128)加密算法。

• 有效范围小。有效覆盖范围10~75m,具体依据实际发射功率的大小和各种不同的应用模式而定,基本上能够覆盖普通的家庭或办公室环境。

• 工作频段灵活。使用频段为2.4 GHz、868 MHz(欧洲)及915 MHz(美

国),均为免执照频段。

## 1 ZigBee协议

### 1.1 ZigBee协议框架

ZigBee协议栈由一组子层构成。每层为其上层提供一组特定的服务:一个数据实体提供数据传输服务,一个管理实体提供全部其他服务。每个服务实体通过一个服务接入点(SAP)为其上层提供服务接口,并且每个SAP提供了一系列的基本服务指令来完成相应的功能。

ZigBee协议栈的体系结构<sup>[6]</sup>如图1所示。它虽然是基于标准的七层开放式系统互联(OSI)模型,但仅对那些涉及ZigBee的层予以定义。IEEE 802.15.4-2003标准<sup>[7]</sup>定义了最下面的两层:物理层(PHY)和介质接入控制子层(MAC)。ZigBee联盟提供了网络层

和应用层(APL)框架的设计。其中应用层的框架包括了应用支持子层(APS)、ZigBee设备对象(ZDO)和由制造商制订的应用对象。

相比于常见的无线通信标准,ZigBee协议套件紧凑而简单,具体实现的要求很低。以下是ZigBee协议套件的需求估计:硬件需要8位处理器,如80c51;软件需要32 kB的ROM,最小软件需要4 kB的ROM;网络主节点需要更多的RAM以容纳网络内所有节点的设备信息、数据包转发表、设备关联表、与安全有关的密钥存储等。

### 1.2 IPv6与IEEE 802.15.4的结合

Zigbee联盟希望建立一种可连接每个电子设备的无线网。它预言Zig-Bee将很快成为全球高端的无线技术,到2007年ZigBee节点将达到30亿个。具有几十亿个节点的网络将很快耗尽已不足的IPv4的地址空间。因此IPv6与IEEE 802.15.4结合是传感器网络的发展趋势。IPv6采用128位地址长度,几乎可以不受限制地提供地址。按保守方法估算,IPv6实际可为整个地球的每平方米面积分配1 000多个地址。IPv6在设计过程中,除了一劳永逸地解决了地址短缺问题以外,还考虑了在IPv4中解决不好的其他问题,如端到端IP连接、服务质量(QoS)、安全性、多播、移动性、即插即用等。

### 1.3 工作频段和速率

IEEE 802.15.4工作在工业科学医疗(ISM)频段,定义了两个工作频段,即2.4 GHz频段和868/915 MHz频段。

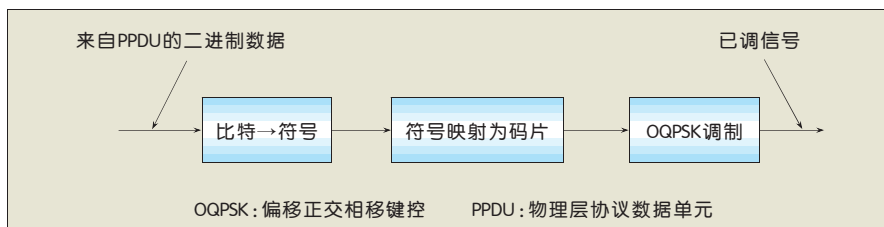
在IEEE 802.15.4中,总共分配了27个具有3种速率的信道:在2.4 GHz频段有16个速率为250 kb/s的信道,在915 MHz频段有10个40 kb/s的信道,在868 MHz频段有1个20 kb/s的信道。

这些信道的中心频率按如下定义( $k$ 为信道数):

$$F_c = 868.3 \text{ MHz}, k=0;$$

$$F_c = 906 \text{ MHz} + 2(k-1) \text{ MHz},$$

$$k=1, 2, \dots, 10;$$



▲图2 IEEE 802.15.4物理层传输格式

$F_c = 2\,405\text{ MHz} + 5(k-11)\text{ MHz}$ ,  
 $k=11, 12, \dots, 26$ 。

一个IEEE 802.15.4网可以根据可用性、拥挤状况和数据速率在27个信道中选择一个工作信道。从能量和成本效率来看,不同的数据速率能为不同的应用提供较好的选择。例如,对于有些计算机外围设备与互动式玩具,可能需要250 kb/s速率,而对于其他许多应用,如各种传感器、智能标记和家用电器等,20 kb/s这样的低速率就能满足要求。

## 2 IEEE 802.15.4物理层

来自IEEE 802.15.4物理层协议数据单元(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位伪噪声码片(CHIP),以便传输。然后这个连续的伪噪声CHIP序列被调制(采用最小键控方式)到载波上,即采用半正弦脉冲波形的偏移正交相移键控(OQPSK)调制方式。IEEE 802.15.4物理层传输格式如图2所示。

868/915 MHz频段物理层使用简单的直接序列扩频(DSSS)方法,每个PPDU数据传输位被最大长为15的

CHIP序列所扩展(即被多组+1、-1构成的 $m$ -序列编码),然后使用二进制相移键控技术调制这个扩展的位元序列。不同的数据传输率适用于不同的场合。例如:868/915 MHz频段物理层的低速率换取了较好的灵敏度和较大的覆盖面积,从而减少了覆盖给定物理区域所需的节点数。2.4 GHz频段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。

## 3 IEEE 802.15.4 MAC层

IEEE 802.15.4 MAC层提供两种服务:MAC层数据服务和MAC层管理服务。管理服务通过MAC层管理实体(MLME)服务接入点(SAP)访问高层。MAC层数据服务使MAC层协议数据单元(MPDU)的收发可以通过物理层数据服务。IEEE 802.15.4 MAC层的特征有信标管理、信道接入机制、保证时隙(GTS)管理、帧确认、确认帧传输、节点接入和分离。

### 3.1 超帧结构

低速率的无线个域网允许使用超帧结构。超帧的格式由传感器网络的协调器定义。超帧被分为16个大小

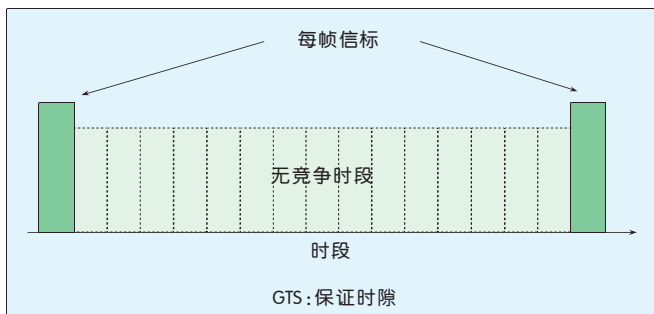
相等的时隙,由协调器发送,如图3所示。每个超帧之间由网络信标分隔。信标帧在超帧的第一个时隙被传输。如果协调器不想使用超帧结构,它将会停止信标的传输。信标可用于使接入的设备同步,区分个域网,描述超帧结构。任何想要在竞争接入时段(CAP)通信的设备都要使用有时隙的载波监听多址接入-冲突避免(CSMA-CA)。所有的传输要在下一个信标到来之前结束。

超帧结构有活跃和非活跃两部分。在非活跃部分,协调器将不和网络联系,进入低能模式。

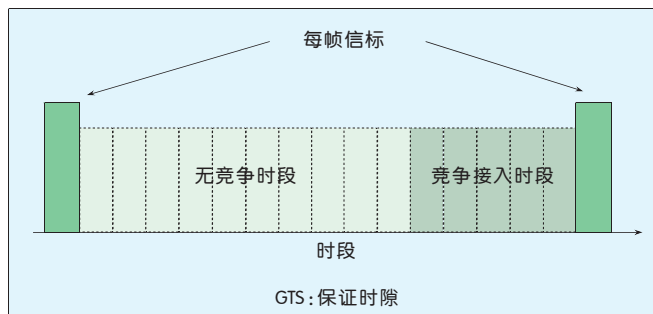
对于低延迟应用或需要特殊带宽的应用来说,网络协调器为它贡献出超帧的活跃部分。这部分叫做GTS。GTS由无竞争时段(CFP)组成,它总是紧跟着CAP,在活跃的超帧尾部,如图4所示。网络协调器可以分配7个GTS,每个GTS可以占用一个以上的时隙。而CAP有充足的时间留给基于竞争的接入的网络设备或想加入网络的设备。所有基于竞争的传输都要在CFP开始前结束,同样,GTS的传输也要确保在下一个GTS开始前结束。

### 3.2 CSMA-CA机制

低速率的无线个人区域网依据网络的结构不同,使用两种信道接入机制。无信标网络使用无时隙的CSMA-CA信道接入机制。每当设备想要传输数据帧或MAC命令时,它将等待随机的一段时间。在随机退避之后,如果信道被检测为空闲,设备将传输数据;如果信道被检测为忙,设备在

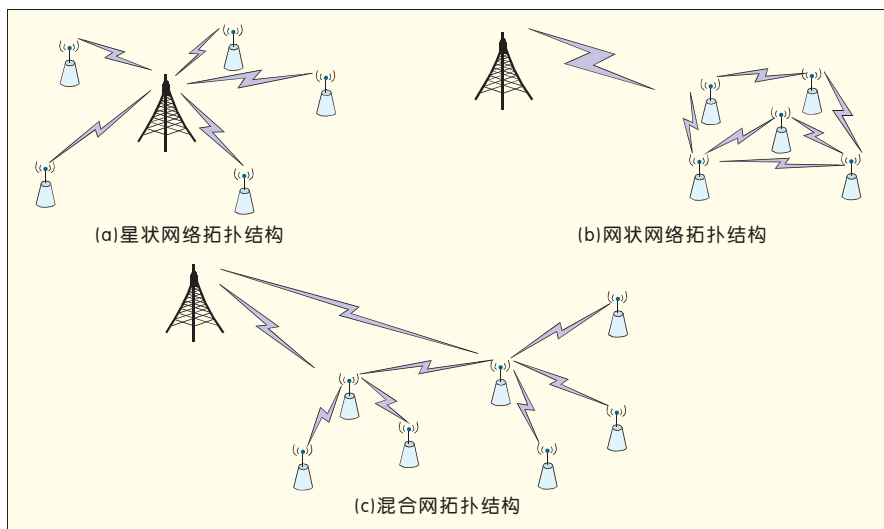


▲图3 无GTS的超帧结构



▲图4 带有GTS的超帧结构





▲图5 网络拓扑

再次尝试接入信道之前,要重新等待随机的一段时间,确认帧的发送不使用CSMA-CA机制。

有信标网络使用有时隙的CSMA-CA信道接入机制,退避时隙在信标传输的开始排列好。每当设备在竞争接入时段要传输数据时,它需要确定下一个退避时隙的界限,之后等待随机的几个退避时隙。在随机退避之后,如果信道被检测为忙,设备在再次尝试接入信道之前,要重新等待随机的几个退避时隙;如果信道被检测为空闲,设备将在下个退避时隙传输数据。确认帧和信标帧的发送将不需要CSMA-CA机制。

### 3.3 安全模式

在低速率无线个人区域网络中设备可根据自身需要选择不同的安全模式:无安全模式、访问控制列表(ACL)模式和安全模式。

无安全模式是MAC子层默认的安全模式。处于这种模式下的设备不对接收到的帧进行任何安全检查。当某个设备接收到一个帧时,只检查帧的目的地址。如果目的地址是本设备地址或广播地址,这个帧就会被转发给上层,否则丢弃。在设备被设置为混杂模式(Promiscuous)的情况下,它会向上层转发所有接收到的帧。

访问控制列表模式为通信提供了访问控制服务。高层可以通过设置MAC子层的ACL条目指示MAC子层根据源地址过滤接收到的帧。因此这种方式下MAC子层就没有提供加密保护,高层有必要采取其他机制来保证通信的安全。

安全模式对接收或发送的帧提供全部的4种安全服务:访问控制、数据加密、帧完整性检查和顺序更新。

## 4 ZigBee网络层

ZigBee网络层将主要考虑采用基于Ad Hoc技术的网络协议,应包含以下功能:

(1)通用的网络层功能:拓扑结构的搭建和维护,命名和关联业务,包含寻址、路由和安全。

(2)同IEEE 802.15.4标准一样,非常省电。

(3)有自组织、自维护功能,可以最大程度减少消费者的开支和维护成本。

ZigBee用于无线传感器网络,由于网络拓扑的多变和形式多样化,应选择适合应用场景的网络层协议。

无线网络拓扑结构一般分为星状网、网状网、混合网(星状+网状),如图5所示。而无线传感器网络拓扑结构具有网络节点数目众多,网络结

构动态变化纷繁复杂等特点,在此我们主要比较3种基本网络拓扑结构,并选出比较适合大型传感器网络使用的拓扑结构。

基本的星状网拓扑结构(图5(a))是一个单跳(Single-hop)系统,如传统无线网络。基站节点可以是一台PC、个人数字助理(PDA)、专用控制设备、嵌入式网络服务器,或其他与高数据率设备通信的网关,网络中各终端节点也可以不同。依据星状网的特点可以看出,当各个传感器节点距离基站节点比较远,传感器节点分布范围大时,这种拓扑结构是行不通的。因为传感器节点能量有限,如果每个节点都要保证数据正确接收的信噪比(SNR)值,则传感器节点必须以较大功率向基站节点发送数据,能量很快就会耗尽。

网状网拓扑结构是一种多跳的网络系统,网络中的所有无线传感器节点都相同,可以直接互相通信,每一次网络都会选择一条或者多条路由进行多跳传输,将所要传输的数据信息传给基站(图5(b))。网状网的每个传感器节点都有多条路径到达基站节点,因此它的容故障能力较强,而且这种多跳系统以多跳代替了单跳的传输距离,减小了源传感器所需要的发送功率。但是同时由于传感器网络节点数量大,中继节点数目众多,且分布随机分散,因此在网状网中查找多跳路由和进行路由维护和修复(自愈)是非常困难的,同时网络中传感器节点必须一直“监听”网络中某些路径上的信息和变化,以有效地传递数据,这些从另一方面增加了网络的能量损耗,减少了网络寿命。

混合网拓扑结构(图5(c))力求兼具星状网的简洁以及网状网的多跳传输和自愈性等优点。其中分层式的网络结构属于混合网中较为典型的一种,尤其适合节点数量众多的无线传感器网络应用。在分层网中,整个传感器网络形成分层结构。相邻传感器通过由基站节点指定或者自组织

等方法形成各个独立的簇,每个簇选出簇首节点,每簇中所包含的传感器节点通过簇首所安排的机制将所收集的数据信息传给簇首,然后由簇首将所接收到的信息进行融合,再转发给基站节点。这种分层式网络中,传感器节点之间不是平等的。这种方法,既通过簇首的数据融合减少了信息冗余度,通过多跳减小了源节点的发送功率,减少了网络的能量消耗,又可以通过簇首的控制减小网络中大部分节点的传输范围,增加带宽复用率,同时使网络节点不必一直保持“监听状态”,减少了网络中路由和数据处理的开销,延长了网络寿命。这种分层簇结构拓扑协议尽管在传统Ad Hoc网络中也有大量的研究,但是传统Ad Hoc网络拓扑结构中的分层网络协议并没有考虑传感器网络中节点数量众多和节点能量及计算能力有限的特点,其协议不能直接利用于无线传感器网络中。因此,研究者在传统Ad Hoc网络协议的基础上,研究出了旨在针对传感器网络中各种问题的网络拓扑协议,使得拓扑协议针对性和实用性更强,采用这种混合网分层拓扑结构的典型协议有低功耗自适应分簇算法(LEACH)、传感器信息系统中能量高效的数据收集(PEGAGIS)、域值敏感能量高效传感器网络协议(TEEN)<sup>[8-9]</sup>。

综上所述,不同网络拓扑结构的选择是根据网络中节点与基站的相对位置,以及网络中的无线参数的不同而定的。当网络中基站的位置比较靠近传感器节点,甚至处于传感器节点中间,同时整个网络的分布范围比较小的时候,星形网络有其相应的优势,而网状网与混合式分层网络结构比较适用于基站位置比较远,传感器节点比较分散的情况。可以看到,尽管网状网拓扑结构鲁棒性比较强,但是由于需要清楚地了解各个传感器节点的位置信息,同时路由开销比较大,使得节点构造和网络实现比较复杂,尤其是对于具有移动节点的传感

器网络,以上问题就更加突出。因此,为了节省功率,简便实现传感器组网,简化传感器节点,大多数传感器路由研究均基于分层式网络结构。

## 5 ZigBee应用演示实例

利用ZigBee无线传感器网络,北京邮电大学搭建了环境监测系统。

系统以北京邮电大学校园为环境监测对象,随机布置传感器数据采集节点,感知采集校园环境的温度和光强等环境参量的实时变化。

采集节点通过微处理器收集数据信息,通过天线发射模块传送数据至传感器网关汇聚节点。网关节点与计算机之间交互通信,通信软件可视化实时显示环境信息。硬件采用Crossbow公司生产的传感器数据采集节点与网关汇聚节点,符合ZigBee工业标准。软件平台采用TinyOS软件编译平台并结合硬件进行演示开发。

## 6 结束语

IEEE 802.15.4协议标准主要用于低速无线个人区域网及无线传感器网络应用,是ZigBee的物理层和MAC层的主要支撑技术。该标准由于采用了简单的物理层和MAC层协议而使得其具有低功耗、低成本等特征,从而使得ZigBee更适用于工业监控、传感器网络、家庭监控等应用。同时,采用分层式的网络结构能够在基站位置较远、传感器节点分散的无线传感器网络中进一步节省功率。

## 7 参考文献

- [1] IEEE Std 802.15.4-2003 IEEE standard for information technology: Telecommunications and information exchange between systems: Local and metropolitan area networks specific requirements: Part 15.4 Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)[S]. 2003.
- [2] 孙利民, 李建中, 等. 无线传感器网络[M]. 北京:清华大学出版社, 2005.
- [3] GHARAVI H, KUMAR S P. Special issues on sensor networks and applications[J]. Proceeding of the IEEE, 2003,91(8): 1151-1153.

- [4] AKYILDIZ L F, SU W L, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002,40(8):102-105.
- [5] EVANS-PUGHE C. Bzzzz zzz (Zigbee wireless standard)[J]. IEE Review, 2003,49(3):28-31.
- [6] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocols for wireless microsensor networks[C]//Proceedings of the 33rd International Conference on System Sciences(HICSS'00), Jan 4-7, 2000, Maui, HI, USA. Los Alamitos, CA, USA:IEEE Computer Society, 2000:223.
- [7] EGAN D. The emergence of Zigbee in building automation and industrial control[J]. Computing & Control Engineering Journal, 2005,16(2):14-19.
- [8] Lindsey S, Raghavendra C S. PEGASIS: Power-efficient gathering in sensor information systems[C]//Proceedings of the IEEE Aerospace Conference: Vol 3, Mar 9-16, 2002, Big Sky, MT, USA. Piscataway, NJ, USA:IEEE, 2002:1125-1130.
- [9] Manjeshwar A, Agrawal D. Teen: A routing protocol for enhanced efficiency in wireless sensor networks[C]//Proceedings of 16th Annual International Parallel & Distributed Processing Symposium(IPDPS2002), Apr 15-19, 2002, Lauderdale, FL, USA. Los Alamitos, CA, USA:IEEE Computer Society, 2002:192-202.

收稿日期:2006-05-23

### 作者简介



**张平**, 北京邮电大学教授、博士生导师。北京邮电大学无线新技术研究所(WTI)所长,《北京邮电大学学报》编委会副主任,北京邮电大学学术委员会委员,中国C3G总体组专家成员,国家“863”未来移动通信Future计划项目总体组成员,国际无线研究论坛(WWRF)副主席及其愿景委员会成员,中国信息产业部第三代移动通信技术实验专家组成员。



**康桂霞**, 北京邮电大学副教授、硕士生导师、博士。2007年IEEE ICC、IEEE WCNC国际会议技术委员会委员。从事3G及后3G移动通信系统物理层关键技术研究,同时从事短距离无线通信技术及其在无线电子健康领域的应用研究。已出版专著1部,发表论文20余篇。



**田辉**, 北京邮电大学副教授、硕士生导师、博士。IEEE会员,全国智能运输系统标准化技术委员会(ITS)联网电子收费工作组专家组成员。从事移动通信、无线网络技术的研究。已发表论文30余篇,出版教材、专著5部。