

# 蓝牙传感器网络与 HSE 互连的研究\*

任 磊<sup>1</sup>, 刘明哲<sup>2</sup>, 王 宏<sup>2</sup>

(1. 上海师范大学 数理信息学院, 上海 200234; 2. 中国科学院 沈阳自动化研究所, 辽宁 沈阳 110016)

摘 要: 针对有线工业 HSE 现场总线网络中存在的问题, 提出了一种基于无线蓝牙技术的传感器网络解决方案。为了保证蓝牙传感器网络与 HSE 网络的互操作, 介绍了通过蓝牙网关实现两者互连的方法。

关键词: 现场总线; HSE; 蓝牙; 蓝牙传感器网络; 蓝牙网关

中图分类号: TP393. 13 文献标识码: A 文章编号: 1001-3695(2007)02-0310-03

## Research on Interconnection of Bluetooth Sensor Network and HSE

REN Lei<sup>1</sup>, LIU Ming-zhe<sup>2</sup>, WANG Hong<sup>2</sup>

(1. College of Mathematics & Science, Shanghai Normal University, Shanghai 200234, China; 2. Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang Liaoning 110016, China)

**Abstract:** The paper presents a sensor network solution based on wireless bluetooth technology according to the problems in wired industrial HSE Fieldbus. In order to enable the co-operation between bluetooth sensor network and HSE, the paper introduces the method of implementing their interconnection by bluetooth gateway.

**Key words:** Fieldbus; HSE; Bluetooth; Bluetooth Sensor Network; Bluetooth Gateway

随着工业企业生产规模的扩大和自动化程度的提高, 现场总线网络系统在大中型工业企业的自动生产控制中得到了广泛应用。大部分现场总线均使用有线传输技术作为其底层通信方式, 而在一些特殊工业现场环境中, 现场设备需要具有一定的移动性, 有线介质的使用限制了设备的移动。为了解决设备的移动问题可以选择使用红外线、802. 11x、蓝牙等线缆替代技术来替代有线介质作为底层通信介质。

使用无线技术连接的现场无线网络虽然提高了网络的灵活性, 但却造成遗留有线现场总线和无线现场网络形成网络“孤岛”。为了实现两种网络的信息共享, 需要在两者的边界使用互联网关设备实现两者的互操作。

本文通过对有线现场总线网络 HSE(High Speed Ethernet)的结构及其缺点的分析, 结合蓝牙技术的特点, 提出一种在 HSE 现场总线中使用蓝牙技术构成无线传感器网络的解决方案, 并实现了该方案的蓝牙网关。

### 1 HSE 现场总线的结构和问题

HSE 现场总线是一种基于传统以太网技术的 FF(Foundation Fieldbus) 现场总线系统, 它主要适用于过程控制领域。HSE 基金会现场总线技术因具有协议开放、全数字化通信、分布式控制和可互操作等优点, 在自动化领域得到了广泛支持并具有良好的发展前景。

HSE 现场总线协议采用 ISO/OSI 模型中的五层, 即物理层、数据链路层、网络层、传输层和应用层; 并且针对工业现场控制的特点, HSE 在应用层上定义了针对自动化业务逻辑的用户层。HSE 的体系结构及其与 OSI 各层的对照关系如图 1 所示。

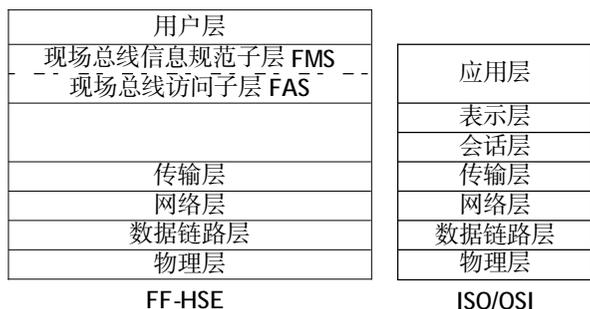


图 1 HSE 现场总线协议体系结构

其中, 物理层使用传统的双绞线、同轴电缆和光纤等有线介质, 但标准中规定可以使用其他无线介质, 传统现场总线的物理拓扑结构为总线型, 而 HSE 使用星型连接, 中心连接设备一般为交换机。根据实现功能的不同, HSE 网络可以连接通用主机设备、以太网现场设备、用于连接 H<sub>1</sub> 网络的 LD 连接设备、用于连接其他网络的网关设备。数据链路层采用传统以太网协议, 可以方便实现与其他 FF 现场总线 (H<sub>1</sub>/H<sub>2</sub>) 以及企业管理信息网络的互连, 为了保证系统的可靠性, HSE 网络允许在系统中存在通信设备和线路的冗余; 网络层和传输层使用标准 TCP/IP 协议; 应用层由现场总线访问子层 FAS 和现场总线信息规范子层 FMS 两个子层构成, 应用层使用数据链路层提供的服务, 描述了用户应用所需要的通信服务、信息格式和行为状态等。

用户层规定了标准功能块、对象字典、设备描述、网络管理和系统管理功能, 用户层实体中运行的功能块应用进程用于完成 FF 现场总线中的自动化系统功能, 多个现场设备的功能块应用进程集合构成了 HSE 的逻辑功能系统。

HSE 现场总线的物理层传输介质一般为有线介质, 有线介质具有良好的适应性, 可以适应大部分的工业现场环境。但是, 在特殊的工业现场中, 有线介质的布线是很困难的, 归纳起来, 以下情况不适宜使用有线介质作为传输通道: 现场环境

具有强腐蚀性, 或其他可能对有线介质产生破坏作用的现场环境; 现场环境比较复杂, 存在体积比较大的障碍物, 有线介质无法穿透这些障碍物或弯曲角度大大超过有线介质的弯曲限度; 现场设备的空间位置需要动态改变, 以及设备移动路径可能产生交叉; 现场设备需要做旋转动作, 使用有线介质可能出现缠绕; 现场设备数量需要动态变化。

## 2 蓝牙协议体系结构

蓝牙技术是由非营利性组织蓝牙 SIG 标准化的短距离无线射频通信技术。蓝牙无线技术是完全开放的, 不同厂家生产的蓝牙设备可以保证互操作和兼容性。它使用的射频信号工作在全球免费的 2.4GHz ISM 频段, 而且其信号功率可在 1mW ~ 100mW 之间动态变化, 不会对人体和其他设备产生影响。

蓝牙协议的体系结构采用分层结构, 蓝牙协议栈是按最大限度地重用已有通信协议的原则进行设计的, 保证了蓝牙协议与已有协议的兼容性, 简化了遗留系统的移植。蓝牙协议的体系结构分为四层, 如图 2 所示。

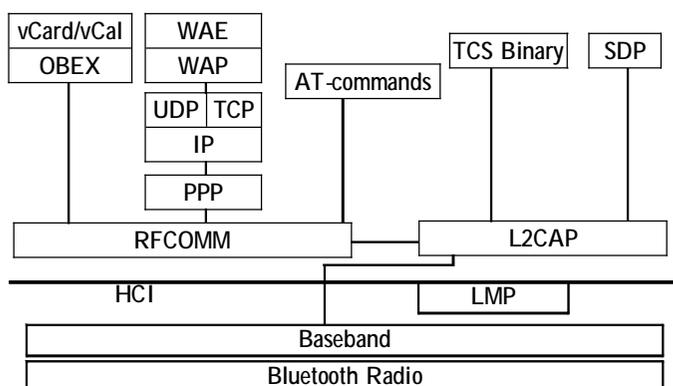


图 2 蓝牙协议体系结构

- (1) 核心协议: 基带 (Baseband)、链路管理协议 (LMP)、逻辑链路控制和适配协议 (L2CAP)、服务发现协议 (SDP);
- (2) 电缆替代协议: 串行电路仿真协议 (RFCOMM);
- (3) 电话控制协议: 二元电话控制规范 (TCS Binary) 和 AT-命令 (AT-command);
- (4) 选用协议: 点到点协议 (PPP)、UDP/TCP/IP、对象交换协议 (OBEX) 及无线应用协议 (WAP)。

蓝牙射频与蓝牙基带提供了无线传输介质和物理链路, L2CAP 层则为上层提供无链接的分组服务。为简化遗留系统的移植, 在 L2CAP 层上定义了串口仿真协议 RFCOMM。多个共享信道的蓝牙设备构成蓝牙微网。微网中发起通信的设备为主设备, 其他设备为从设备, 同一微网中只有一个主设备和最多七个从设备。蓝牙微网中主从设备之间采用 C/S 模式工作, 蓝牙客户机设备在使用蓝牙服务器设备提供的服务之前, 必须使用服务发现协议 SDP 从蓝牙服务器上获得服务信息。

## 3 蓝牙传感器网络解决方案

通过前述分析, HSE 现场总线的问题主要集中于: HSE 物理层传输介质为有线介质, 有线介质的使用要求现场总线的部署必须进行布线。而前述的一些特殊应用情况是不适宜进行布线的, 可以使用无线介质替代电缆解决布线所带来的问题。常用的无线介质主要有红外线、802.11x 和蓝牙等。其中红外线的传输距离过短, 最大传输距离为 10m, 而且通信双方要直线可视, 不能实现广播通信; 802.11x 无线以太网的最大传输距离可以达到 100m, 但功耗过大, 不适合小型移动便携设备,

而且其较强的电磁干扰可能对无屏蔽电子设备的工作造成影响; 蓝牙技术为射频技术, 不需要通信双方直线可视, 其最大传输距离可以达到 100m, 最大功率只有 100mW, 而且根据设备工作状态的变化, 其工作功率还可自动动态调整, 在功耗方面远低于 802.11x, 特别适合使用在对功耗要求严格的小型设备上, 其信号也不会对其他设备产生大的干扰。所以蓝牙技术是一种比较理想的中短距离电缆替代技术。

由此提出一种蓝牙传感器网络解决方案, 该方案可以分为三部分, 即现场蓝牙传感器网络、蓝牙网关和 HSE 网络。现场设备是配置了蓝牙模块的传感器, 称为蓝牙传感器。蓝牙传感器之间通过蓝牙射频通信, 构成蓝牙传感器网络。蓝牙传感器网络的覆盖范围和连接的设备数量有限, 而且为了保证已有 HSE 网络能够继续使用, 在蓝牙现场传感器网络与 HSE 现场总线的边界设置互连设备, 实现两者的透明连接。该互连设备称为蓝牙网关。HSE 现场总线通信覆盖范围相对较大, 可以充当整个现场总线的主干网络, 与蓝牙传感器网络构成分级网络。蓝牙传感器网络解决方案的系统结构如图 3 所示。

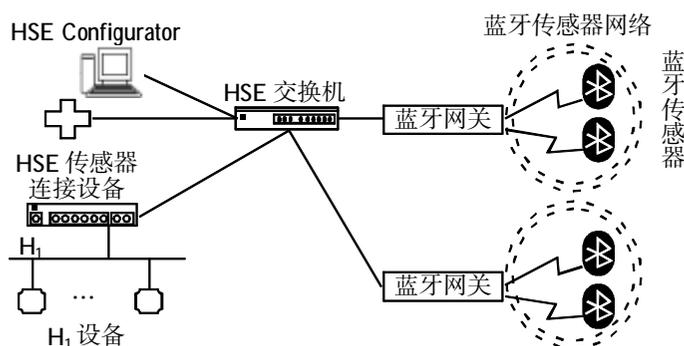


图 3 蓝牙传感器网络方案物理结构

蓝牙传感器网络方案的主要物理组成部分及其功能:

- (1) 蓝牙传感器作为现场设备, 它由通用传感器模块和蓝牙模块组成。通用传感器负责对工业现场设备的运行状态数据采集, 蓝牙模块通过蓝牙空中接口实现蓝牙传感器之间、蓝牙传感器与蓝牙网关之间的数据和控制信息交换。蓝牙传感器在蓝牙微网中充当 Slave 从设备, 蓝牙传感器可以在蓝牙网络中实现即插即用。
- (2) 蓝牙网关应用运行在配置有蓝牙模块的网关硬件上。蓝牙网关硬件可以是微型计算机或其他计算设备, 网关的底层蓝牙模块负责在空中接口中实现与蓝牙传感器的数据和控制信息交换, 保证 HSE 网络对蓝牙传感器的透明性; 蓝牙网关应用设备本地同时运行 HSE 协议栈和功能块应用, 蓝牙网关应用对从蓝牙模块接收到的数据进行处理, 然后将经过格式化、转换等处理的数据发送给 HSE 功能块, 由功能块和 HSE 协议栈将数据发送至 HSE 网络。网关应用还负责接收 HSE 网络的控制信息, 并且将控制信息转换为蓝牙传感器可以识别的信息格式, 保证蓝牙网络对 HSE 网络的透明性。蓝牙网关应用设备在蓝牙微网中充当 Master 主设备。

(3) HSE 组态软件 (HSE Configurator) 可以运行在任意接入 HSE 现场总线的计算机上。组态软件在系统启动之前对总线上的自控设备、网络节点 (包括蓝牙网关) 进行配置, 定义其在总线功能系统中的角色, 设置其运行参数, 使总线上的各设备协调工作完成过程控制任务。

## 4 蓝牙网关的实现

蓝牙网关是蓝牙传感器网络与 HSE 现场总线互连的关键部分。本部分介绍蓝牙网关的实现。在该实现中, 蓝牙网关硬

件与蓝牙传感器均使用 CSR 公司的 BlueCore 01 单芯片蓝牙模块作为底层蓝牙通信硬件, 蓝牙传感器的传感器模块为 I<sup>2</sup>C AD7416 温度传感器芯片, 蓝牙网关硬件平台为集成有蓝牙通信模块和以太网通信模块的通用 PC 机或专用工控机, HSE 现场总线的软硬件使用中国科学院沈阳自动化研究所开发的相关产品。蓝牙传感器软件使用 CSR CASIRA 集成工具开发, 蓝牙网关软件使用 Widcomm BTW DK 蓝牙协议软件工具开发。

蓝牙网关使用的蓝牙协议层次主要包括 LMP, L2CAP, RFCOMM 和 SDP。其软件工作层次如图 4 所示。

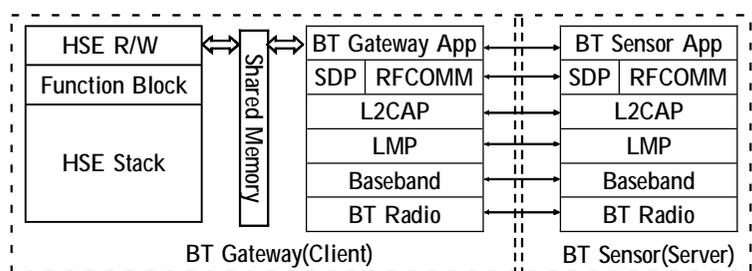


图 4 蓝牙网关应用协议软件结构1

在软件结构上, 蓝牙网关与蓝牙传感器之间采用 C/S 工作模式, 蓝牙传感器充当现场数据采集服务器, 蓝牙网关充当客户机, 采集数据的格式化和转换由蓝牙网关来实现; 在硬件结构上, 蓝牙网关与蓝牙传感器采用蓝牙微网的主从结构, 其中蓝牙传感器为从设备, 蓝牙网关为主设备, 则一个蓝牙网关同时可最多与七个现场蓝牙传感器进行数据交换和调度。

蓝牙规范中定义了不同的蓝牙设备分类, 不同的蓝牙设备通过设备标志类区分。其格式如图 5 所示。

11 位	5 位	6 位	2 位
Service of Class	Major Device Class	Minor Device Class	Format Type

图 5 蓝牙设备标志类

标准蓝牙设备分类中没有定义蓝牙传感器的分类, 则按照蓝牙规范自定义蓝牙传感器的设备标志类为

(1) 服务类: Class of Service = 00001000000 表示蓝牙采集服务;

(2) 主设备类: Major Device Class = 10111 表示自定义主设备类为传感器设备;

(3) 次设备类: Minor Device Class = 000001 表示自定义次设备类为温度传感器, 其他传感器分类为 000000 表示未分配, 000010 表示压力传感器, 依次类推;

(4) 格式类型: Format Type = 00 表示未分类。

为了实现与 HSE 现场总线的互连, 蓝牙网关软件与 HSE 协议栈及功能块应用工作在同一网关硬件设备上, 但两者工作在不同软件进程空间。为了实现两者的数据和控制信息交换, 蓝牙网关软件使用 Win32 平台上数据交换速度最快的共享内存方式实现。蓝牙网关与现场蓝牙传感器的协同工作过程主要包括以下七个过程:

(1) 程序启动。蓝牙网关应用软件启动、生成程序用户图形接口、进行程序初始化。

(2) 设备发现。对现场蓝牙微网中的蓝牙设备(蓝牙传感器和一般蓝牙设备)进行查询, 并且启动与 HSE 功能块的通信线程。

(3) 设备选择。用户对发现的现场蓝牙传感器进行选择, 网关应用向 HSE 功能块添加设备信息。

(4) 服务发现。蓝牙网关对每个监控的蓝牙传感器的数据采集服务进行服务发现, 获得服务参数。

(5) 设备匹配。蓝牙网关与被监控的蓝牙传感器进行设备匹配。

(6) 建立物理与逻辑连接。蓝牙网关与每个被监控的蓝牙传感器建立无线空中接口连接及独立的 RFCOMM 会话。

(7) 数据传送。蓝牙传感器根据网关对数据采集服务的参数设置进行数据采集, 并向网关应用发送数据, 蓝牙网关应用进程动态获得 HSE 功能块的数据请求消息, 并将采集的现场传感器数据发送给 HSE 功能块。

## 5 结束语

蓝牙传感器网络解决方案是蓝牙技术在工业现场应用的一次有益尝试, 具有一定的创新性。鉴于蓝牙技术的诸多优点, 该方案具有很大的可行性, 并且可以降低现场总线的整体建设成本, 扩大现场总线的适用范围。但是, 文中提及的蓝牙网关实现还有尚待完善的地方, 如不能很好地适应实时环境等。在后续的研究中将实现蓝牙网关系统向实时嵌入式平台的移植。

## 参考文献:

- [1] 刘高平, 殷伟凤, 李国胜. 蓝牙与以太网互连技术的实现[J]. 计算机工程, 2004, 30(17): 86-88.
- [2] 肖爱平, 孙汉旭, 谭月胜. 基于蓝牙技术的机器人模块化无线通信设计[J]. 北京邮电大学学报, 2004, 27(1): 75-78.
- [3] 张磊, 沈连丰. 蓝牙网关中高速异步串行通信的研究与实现[J]. 计算机应用研究, 2004, 21(9): 256-260.
- [4] 严紫建, 刘元安. 蓝牙技术[M]. 北京: 北京邮电大学出版社, 2001. 25-27.
- [5] 阳宪惠. 现场总线技术及其应用[M]. 北京: 清华大学出版社, 2000. 134-137.
- [6] Bluetooth SIG-2001, Bluetooth Specification (volume 1 core) version 1.1[S].
- [7] Bluetooth SIG-2001, Bluetooth Network Encapsulation Protocol (BNEP) Specification[S].
- [8] Bartolomeu P, et al. Distributed Monitoring Subsystems Based on a Bluetooth Implementation[C]. Proc. of IEEE Conference on Emerging Technologies and Factory Automation, 2003. 121-124.
- [9] Urban Bilstrup, Per-Arne Wiberg. Bluetooth in Industrial Environment[C]. Proc. of the 11th IEEE International Workshop on Factory Communication Systems, 2000. 239-246.
- [10] Daniele Miorandia, Stefano Vitturi. A Wireless Extension of Profibus DP Based on Bluetooth Radio System[J]. Ad hoc Networks, 2005, 3(4): 479-494.
- [11] Daniele Miorandia, Stefano Vitturi. Hybrid Wired/Wireless Implementations of Profibus DP: A Feasibility Study Based on Ethernet and Bluetooth[J]. Computer Communications, 2004, 27(10): 946-960.
- [12] Soo-Hwan Choi, Byung-Kug Kim, Jinwoo Park, et al. An Implementation of Wireless Sensor Network[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 236-244.
- [13] Xin Zhang, Riley G F. Bluetooth Simulations for Wireless Sensor Networks Using GTNetS[C]. Proc. of the IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004. 375-382.
- [14] Rouhana N, Horlait E. BWIG: Bluetooth Web Internet Gateway[C]. Proc. of the 7th International Symposium on Computers and Communications, 2002. 679-684.

## 作者简介:

任磊(1976-), 男, 讲师, 硕士, 主要研究方向为计算机网络、分布式系统; 刘明哲(1974-), 男, 工程师, 主要研究方向为现场总线、嵌入式系统; 王宏(1963-), 男, 研究员, 博导, 主要研究方向为计算机网络、工业通信、嵌入式系统。