第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)20—0260—03 文献标识码：A 中图分类号：TP391

IEEE802.11x在CAN总线系统中的无线扩展

夏继强，丁瑞全，满庆丰
(北京航空航天大学机械工程及自动化学院，北京 100083)

摘 要：针对工业控制网络中的无线接入、系统互连及扩展等问题，提出将IEEE802.11与现场总线系统融合的方案。设计了基于ARM和Linux平台的CAN/WLAN网关，其体积小、功耗低、成本低以及移动性强，无缝连接了CAN网络和WLAN。对无线扩展的关键环节无线网卡驱动进行了陈述，给出一种USB无线网卡的驱动模型。并针对现场总线的无线扩展，探讨其调度策略，保证数据传输的实时性和可靠性。

关键词：无线现场总线；IEEE802.11技术；USB无线网卡驱动；无线扩展

Wireless Extension of IEEE802.11x in CAN Field-bus System

XIA Ji-qiang, DING Rui-quan, MAN Qing-feng
(School of Mechanical Engineering and Automation, Beijing University of Aeronautics and Astronautics, Beijing 100083)

【Abstract】 In terms of wireless access, system interconnection and extension in industrial control networks, the combination of IEEE802.11x and field-bus system is proposed. Arm-Linux based CAN/WLAN gateway is designed to interconnect CAN networks and WLAN characterized by shorter dimensions, lower power consumption, lower cost and stronger mobility. Detailed information is given about key issues of wireless extension, namely the wireless card driver, and a USB wireless adapter model is presented. The schedule strategy of wireless field-bus extension is analyzed to meet the real-time and stability requirements.

【Key words】 wireless field-bus; IEEE802.11; USB wireless adapter driver; wireless extension

1 概述

在工业控制环境下，存在许多移动对象或旋转设备、手持的数据采集设备、距离远的单设备、临时安装的器件等，它们之间以及与固定现场总线网络的通信很难通过有线的物理介质连接来实现。另外由于现场总线缺乏对互联网的支持，组网能力有限，而在大型控制系统中有时需要网络之间互连。上述问题都需要无线技术和现场总线的结合方案来解决。

目前无线通信迅速进入工控领域的现场设备层，有关协会及自动化厂商纷纷组建联盟进行无线现场总线的研究，主要集中在无线通信在工业中的适应性评估、现场总线的无线扩展模型及链路延时等方面[1]。国外主要以PROFIBUS为研究重点，但由于无线链路的不稳定性，其令牌丢失的问题使得系统的稳定性和实时性大大降低[2]。国家“863”计划基金资助项目“机群智能化工程机械”对CAN总线的无线应用做了研究，但其无线网桥基于嵌入式工控机，体积大、功耗高、成本高以及移动性不足[3]。

无线数据通信技术主要有：Zigbee, GPRS, DECT, Bluetooth, HiperLan2, IEEE 802.11x等，综合考虑产品的成熟度、通信速率、覆盖范围等因素，802.11x标准为工业无线通信应用的最佳选择[4]。而随着其技术的成熟，安全性和稳定性也提高了很多，进军工业控制领域势在必行。其在无线数据采集传输、嵌入式手持移动终端及远程无线视频监控中都有具体应用[5]。

CAN总线基于改进型的总线共享机制，不存在令牌传递的问题，同时CAN总线在国内的应用范围最为广泛，因此，本文利用WLAN IEEE802.11x技术对CAN总线系统进行无线扩展，即可实现一种在工厂现场设备层的具有无线移动接入能力的高性能无线现场总线，有效地扩展现场总线的通信范围。

2 系统的总体设计

由于CAN总线采用多主工作方式、非破坏性的仲裁技术、报文滤波及短帧结构，因此结构简单、可靠性高、受干扰概率低、传输时间短实时性好，但是CAN总线没有路由器、网关等网络连接设备，网络规模有限，大型组网能力和网络处理能力差。为了实现移动终端及其他应用情况的无线接入及有效扩展CAN网络的通信范围，需将无线局域网技术融合到现场总线网络中，同时可以有效减少无线信道的不稳定性带来的影响，实现优势互补。系统总体结构如图1所示。

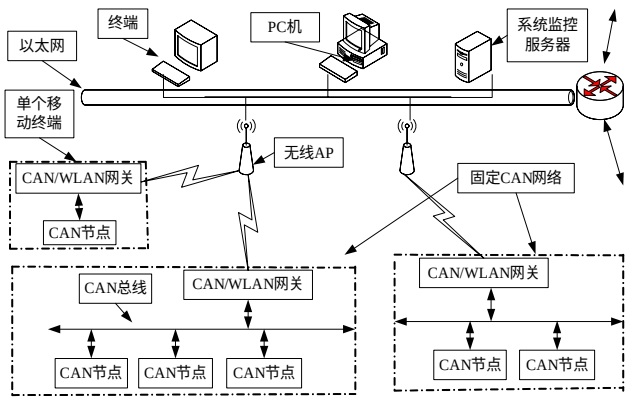

图1 系统总体结构

作者简介：夏继强(1970－)，男，副教授，主研方向：工业测控网络，现场总线；丁瑞全，硕士研究生；满庆丰，教授

收稿日期：2007-11-30 **E-mail：**sailing_0325@163.com

系统的关键部分是 CAN/WLAN 网关，其实现了协议之间的相互转换，无缝链接 CAN 现场总线系统与无线局域网，使得有线站点和无线站点可以在同一个 CAN 网络内运行，已经存在和使用的设备和投资不必替换。

嵌入式系统基本都有 USB 主机接口，其相比 PCMCIA 接口的无线网卡扩展更方便，因此，选用了基于 RT2573 芯片集的 ASUS WL-167G USB 接口的无线网卡；通过 SPI 接口可以方便地扩展 CAN 控制器，相比数据地址总线复用的 SJA1000 扩展更方便，因此，选用了 Microchip 公司的 MCP2510。基于以上要求，硬件平台选用了基于 ATMEL 公司的 AT91RM9200。该 CAN/WLAN 嵌入式网关体积小、功耗低、成本低以及移动性强，在以太网、无线和 CAN 总线接口基础之上即可通过无线链路将移动终端接入有线以太网或固定 CAN 网络，实现企业级的管理、控制一体化。

3 系统的软件设计

3.1 软件总体结构设计

无线局域网和现场总线协议之间的转换器可分为物理层的中继器、MAC 层的网桥及应用层的网关等几种形式，中继器方式需要更改底层硬件，网桥方式对应 MAC 层的协议转换复杂，而无线网关的形式则使得原有的无线网段和有线网段的协议不需做任何改变，实现起来最为简单。

本系统采用的网关总体结构如图 2 所示，主要实现了 USB 无线网卡的驱动程序和 CAN 总线驱动程序，同时在应用层实现了 IEEE802.11x 和 CAN 总线协议及数据帧的转换。

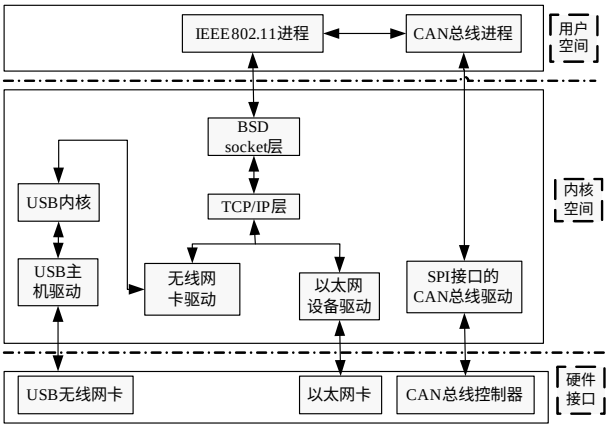

图 2 系统软件总体结构

USB 主机驱动提供对 USB 网卡的直接控制，通过 USB 内核与无线网卡驱动交互；网络应用进程通过 socket 套接字与无线网卡驱动联系，同时与 CAN 总线应用进程通信，完成 CAN 总线数据帧和无线数据帧的转换；CAN 总线进程通过 SPI 接口的 MCP2510 控制器进行数据收发，以达到无线链路的数据和 CAN 总线的交互。

3.2 无线网卡驱动

3.2.1 Linux 下无线网卡驱动的体系结构

Linux 对所有的网络设备进行了抽象并定义了一个统一的概念，称之为接口(interface)。对于每个网络接口，都用一个 net_device 数据结构来表示。

无线网卡驱动程序的体系结构及其在内核中的位置如图 3 所示，大致划分为 5 层，从上到下分别为用户无线应用与配置层、网络协议接口层、网络设备接口层、提供实际功能的设备驱动功能层以及网络设备和网络媒介层。本系统中的无线网卡驱动包括网络设备接口层和设备驱动功能层，大致分为接口和协议处理两部分，协议部分实现无线 802.11 MAC 的管理及数据帧的转换，接口部分实现与底层无线网卡的数据交互以及与上层交互的应用、配置、查询等接口。

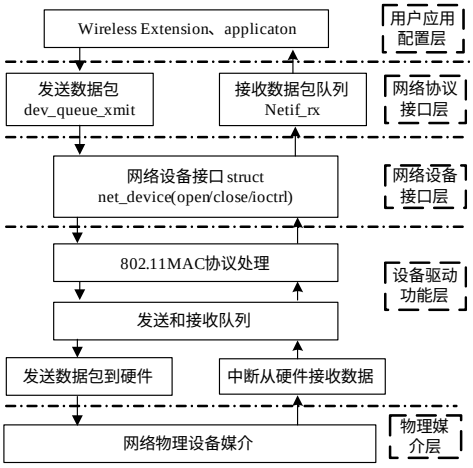

图 3 Linux 下无线网卡驱动的体系结构

3.2.2 USB 无线网卡驱动的实现

本系统开发的 USB 接口的网卡驱动结构如图 4 所示，其对硬件平台的依赖性非常小，只要 USB 主机接口可用即可，能方便地在各种嵌入式开发平台上移植。这里通过 ASUS WL-167G 驱动实例讨论 USB 网卡驱动的一般写法，有关硬件部分的相关代码由于硬件的不统一而予以省略。

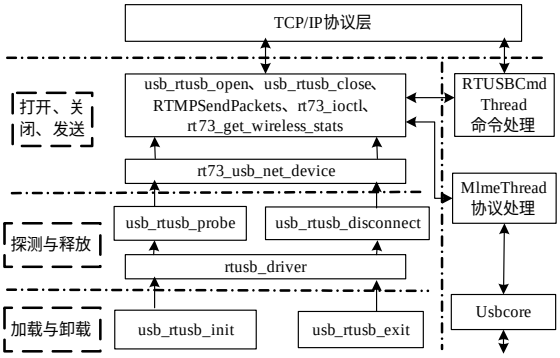

图 4 USB 无线网卡的驱动模型

(1)驱动模块的加载和卸载

```
module_init(usb_rtusb_init);
module_exit(usb_rtusb_exit);
```

这是整个驱动程序的入口点和出口点，通过 usb_register (&rtusb_driver)及 usb_deregister(&rtusb_driver)向内核注册及注销 rtusb_driver

```
struct usb_driver rtusb_driver = {
.name="wlan",
.probe=usb_rtusb_probe,
.disconnect=usb_rtusb_disconnect,
.id_table=rtusb_usb_id,
};
```

USB 内核根据 rtusb_usb_id 来探测它所支持的网卡系列，由此决定是否注册或注销 USB 网络设备。

(2)无线网卡的探测和注销

USB 内核通过 USB 主机接口来得到硬件设备插入或拔出的信息，调用 rtusb_driver 所注册的探测或注销回调函数 usb_rtusb_probe 及 usb_rtusb_disconnect。

设备侦测函数通过 rtusb_usb_id 检测 PID(产品标识)和 VID(厂家标识)等信息，若确认网络设备存在，则初始化网络

接口，注册网络设备，主要实现以下几个回调函数的设置：usb_rtusb_open, usb_rtusb_close, RTMPSendPackets, rt73_ioctl, RTUSBRxPacket 以及与无线网络密切相关的 rt73_get_wireless_stats, rt73_iw_handler_def。

设备拔出或模块卸载时将调用 usb_rtusb_disconnect，它的作用与侦测函数正好相反，主要完成网络设备注销，以及释放驱动程序申请的各种资源。

(3)无线网卡设备的打开与关闭

网卡设备的打开与关闭通过 usb_rtusb_open, usb_rtusb_close 方法实现。

Open 方法激活网络设备，open 函数一般包括以下几个方面内容：初始化网络参数、发送接收区缓冲队列；加载固件并初始化无线网卡；启动 RTUSBCmd Thread 命令处理进程及 MlmeThread 协议处理进程；同时通过 netif_start_queue 开启与网络协议层的服务。

Close 方法与 open 方法截然相反，主要是释放被设备占用的资源，改变设备的状态等。

(4)数据包的发送与接收

数据包的发送接收是所有网络设备都必须实现的功能，本系统通过函数 RTMPSendPackets 及 RTUSBRxPacket 实现。网络协议层传递过来的 sk_buff 数据包已经包含硬件帧头，所以在一般情况下，发送函数可以不必做填充直接交给硬件发送，但对于无线网卡，就要将以太网协议转换为 802.11 协议，然后才能交给硬件发送。

数据包的接收方法并不存在于 net_device 网络设备接口中，因为数据包的接收需要设备通知系统，一般的设备驱动程序都采用硬件中断请求机制。但本系统中的 USB 中断只能告诉 USB 内核，由 USB 内核读取数据，然后由 tasklet_struct 所定义的 RTUSBRxPacket 中断的函数来进行数据的处理，其申请用来存储新到数据包的 skb 缓冲区，从硬件中读取相应的数据，将帧格式转换为以太网帧格式，调用函数 netif_rx()，将数据包传给网络协议层。

4 WLAN/CAN 协议转换器的原理

在本系统中，设计了如图 5 所示的应用层协议转换器 WLAN/CAN。

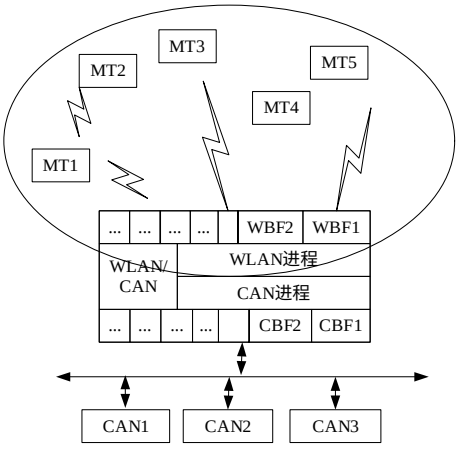

图 5 协议转换器 WLAN/CAN

该协议转换器在整个无线现场总线结构中起着重要的作用，不仅实现现场总线和无线局域网协议之间的转换，而且协调两段网络的时间和速度，保证无线现场总线中数据传输的实时性和可靠性，主要完成了下列任务：

(1)在无线或有线各自的逻辑环网内，保证站点一致性，即提供统一的访问策略；

(2)从有线网段向无线网段传送数据帧或反之，转化不同的帧协议。

WLAN/CAN 可以处理两种不同的协议，其在作为 CAN 协议站点的同时，也作为 IEEE 802.11x 无线局域网的虚拟主机。其开启了 2 个进程，每个协议使用一个进程，2 个进程同时工作分别处理各自网络内的数据传输，同时通过队列或邮箱进行通信。

协议转换器为每个 CAN 总线网络内的站点和 IEEE 802.11x 网络内的虚拟移动终端 MT 设置缓冲区。任何从 CAN 总线到 IEEE 802.11x 的数据传输都先被协议转换器接收并存储在 CBFx 中，随后 CAN 进程将其转给 WLAN 进程存储在 WBFx 中，反之亦然。

为了保证数据传输的实时性和可靠性，需要设计合适的调度策略。WLAN 的 DCF 方式具备不确定时延的特性，PCF 方式可以提供轮询机制，但由于超级帧中可能存在的媒体延迟接入导致下一个论询周期长度的变化，因此本系统采用了在应用层设置虚拟轮询列表 VPL 的方式，轮询周期固定，同时有效地减少 DCF 协议竞争特性给无线网络部分带来的不确定性延迟。

例如，CAN 网络节点 CAN1 和虚拟终端 MT4 之间进行数据交换，则执行下面的流程：CAN1 节点在其获取总线控制权时将数据发往 CBF1，然后传送至 WBF4，CAN/WLAN 按照虚拟访问列表中的顺序，将数据传递给 MT4，反之亦然。

5 结束语

本文将无线局域网 IEEE802.11 技术融合到现场总线系统中，通过无线链路实现了移动单元及危险环境下节点的无线接入，有效地扩展了现场总线的通信范围，真正实现了企业级的管控一体化。给出的一种 USB 无线网卡驱动模型对于嵌入式设备的无线应用具备借鉴意义，同时提出的 CAN 总线无线扩展架构也为其他现场总线的无线连接提供了参考。

参考文献

[1] Francesco D P. On the Use of Wireless Networks at Low Level of Factory Automation Systems[J]. IEEE Transactions on Industrial Infomatics, 2006, 2(2): 129-143.

[2] Willig A, Wolisz A. Ring Stability of the PROFIBUS Token Passing Protocol over Error-prone Links[J]. IEEE Trans. on Ind. Electron, 2005, 48(5): 1025-1033.

[3] 唐天勇. 车载 CAN、WLAN 及 GSM 无线网桥的研究与设计[D]. 南京: 东南大学, 2003.

[4] Willig A. An Architecture for Wireless Extension of PROFIBUS[C]//Proc. of the 29th Annu. Conf. of IEEE Industrial Electronics Society. [S. 1.]: Press, 2003: 2369-2375.

[5] Li Ming. Embedded Video Surveillance System for Vehicle over WLAN and CDMA1X[C]//Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing. [S. 1.]: IEEE Press, 2005: 1292-1295.