

文章编号:1001-893X(2012)07-1174-04

远程无线控制系统的设计与实现^{*}

潘高峰,薛 军,谢 勇,梁 盛

(中国卫星海上测控部,江苏 江阴 214431)

摘 要:由于保密的要求以及铺设专网耗资巨大等问题,测量船对远程的标校设备无法进行有效的控制。通过选用无线网桥技术设计了一套无线控制系统,并开发了网络控制模块以及相应的软件,进而实现了测量船对远端设备的有效控制。测试表明,系统设计合理,控制便捷,具有可靠性、安全性和扩展性高等优点,完全适用于测量船远程控制。

关键词:测量船;标校设备;远程控制;无线网桥

中图分类号:TN914 **文献标志码:**A doi:10.3969/j.issn.1001-893x.2012.07.026

Design and Implementation of a Remote Control System Based on Wireless Bridge

PAN Gao-feng, XUE Jun, XIE Yong, LIANG Sheng

(China Satellite Maritime Tracking and Control Department, Jiangyin 214431, China)

Abstract: For some problems as security requirements and high cost to laid the special network, the TT&C ship can't control the remote calibration equipment effectively. In this paper, a control system using the wireless bridge is designed, and the network control module and the software are developed. The effective control of the equipment for TT&C ship is realized. The test results show that the system design is reasonable and the system is featured by convenient control, high reliability, safety and extensibility, so it is suitable for TT&C ship completely.

Key words: TT&C ship; calibration equipment; remote control; wireless bridge

1 引 言

随着我国航天事业的发展,测量船所承担的任务呈现高密度、高强度的趋势,造成码头期间的任务准备工作越来越繁重,面临着考核项目多、考核时间短和多船协调对标等现实情况,如何提高对标效率、确保安全可靠对标成为紧迫的课题。由于保密要求,原研制的远程标校控制系统无法接入现有网络,而铺设专网的耗资巨大,性价比低,也非首选方案。近些年来,无线通信已经成为信息通信领域中发展最快、应用最广的技术,广泛应用于家居、农业、工业、航天等领域,已成为信息时代社会生活不可或缺的一部分^[1],这种技术也为解决测量船远程控制标

校设备提供了支持。

本文通过对常用中远距离无线通信方式的比较,择优选择了无线网桥,采用了桥接中继的网络模式,通过开发远程设备端的网络控制模块,以及相应的控制软件,实现了测量船对远程设备的有效、安全控制。

2 无线通信方式比较

无线通信技术是利用电磁波信号在自由空间中进行信息传播的一种通信方式,按技术形式可分为两类:一是基于蜂窝的接入技术,如蜂窝数字分组数据、通用分组无线传输技术、EDGE 等;二是基于局域网的技术,如 WLAN、Bluetooth、IrDA、Home - RF、微

^{*} 收稿日期:2012-03-05;修回日期:2012-04-16

功率短距离无线通信技术等。在中远距离无线通信常用的有 ISM 频段的通信技术(比如 ZigBee 以及其他频段的数传模块等)和无线网络技术(比如 GSM、GPRS 以及无线网桥等)。

基于 ISM 频段的数传模块的通信频率为公共频段,产品开发没有限制,因此发展非常迅速,得到了广泛应用。特别是近年来新兴的 ZigBee 技术,因其低功耗、低复杂度、低成本,尤其是采用自组织方式组网,对网段内设备数量不加限制,可以灵活地完成网络链接,在智能家居、无线抄表等网络系统开发中得到应用^[2]。但是,对于本系统的开发而言,需要分别研制控制点和被控制点的硬件模块,并需通过软件配置网络环境,开发周期长,研制成本高,故非本系统开发的最优方案。

GSM、GPRS 这种无线移动通信技术已经成为人们日常生活工作必不可少的部分,在其他如无线定位、远程控制等领域的应用也屡见不鲜^[3],但是由于保密、通信费用、开发成本等因素,也无法适用于本系统的开发。

而无线网桥为本系统的低成本、高效率的研发提供了有利支持,是开发本系统的首选无线通信方式。无线网桥是无线网络的桥接,它可在两个或多个网络之间搭起通信的桥梁,也是无线接入点的一个分支。无线网桥工作在 2.4 GHz 或 5.8 GHz 的免申请无线执照的频段,因而比其他有线网络设备更方便部署,特别适用于城市中的近距离、远距离通信。

3 系统设计

该远程控制系统是以保障测量船对远端标校设备的有效控制为目标,包括标校设备的开关机、状态参数的采集等,主要由测量船控制微机、标校设备、网络控制模块、主控微机以及无线网桥等组成。工作流程为测量船控制微机或主控微机发送控制指令,通过无线网桥进行信息传播,网络控制模块接收、解析指令,按照 Modbus 协议规定的格式通过串口发给某一标校设备,该标校设备响应控制指令并执行;网络控制模块定时发送查询指令,并将采集的状态数据打包,通过无线发给远程控制微机,便于操作人员监视。

网络通信协议采用 UDP 方式,对于测量船控制微机、主控微机只需按照一定的数据格式发送或接收 UDP 包即可。网络控制模块是系统的核心部件,是本文研究、设计的重点。目前,常用的网络芯片主要有 ENC28J60、CP2200 等,这里选用了 ENC28J60,

设计、加工了基于 STC89C52RC 单片机的硬件电路。通过网络信息处理软件模块的开发,满足了网络信息交互的功能要求;通过 Modbus 串口协议软件模块的开发,满足了标校设备监控功能,从而实现了系统设计目标。

3.1 组网模式

无线网桥有 3 种工作方式,即点对点、点对多点、中继连接。根据系统的控制要求以及环境因素,本系统采用了中继连接的方式,其网络拓扑如图 1 所示。从图中可以清晰看出,这种中继连接方式在远程控制端布置两个无线网桥,分别与主控点和客户端进行通信,通过网络控制模块完成数据交互,从而完成组网。

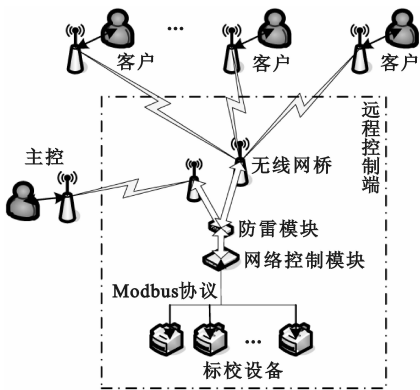


图 1 系统网络拓扑图
Fig. 1 System network topology diagram

3.2 安全防范

由于是开放性设计,无线网络安全是一个必须考虑的问题。本系统的特点是非定时或全天候开机,涉密数据仅为频点参数,而被控设备自身均有保护措施(协议保护)。因此,系统在设计时重点考虑接入点防范、防止攻击,采取的措施有登录密码设施、网络密钥设置、固定 IP、对数据结构体的涉密数据采取动态加密等方式,从而最大限度地防止了“被黑”。同时,采用了网络防雷器来防护雷电破坏。

3.3 网络控制模块设计

3.3.1 硬件设计

网络控制模块的功能是收命令信息、发状态信息,并通过串口与标校设备实现信息交互,其硬件电路主要由 MCU(微控制单元)、ENC28J60(网络芯片)、Max232(串口芯片)以及外围电路组成,其电原理图如图 2 所示。硬件设计的核心是 MCU、网络芯片的选型,本系统 MCU 选用的 STC89C52RC 单片机,是一种低功耗、高性能 CMOS 8 位微控制器,可直

接使用串口下载,为众多嵌入式控制应用系统提供高灵活、超有效的解决方案。ENC28J60 是由 Microchip 公司出的一款集成度的以太网控制芯片,其接口符合 IEEE802.3 协议,仅 28 个引脚就可提供相应的功能,大大简化了相关设计。ENC28J60 提供了 SPI 接口,与 MCU 的通信通过两个中断引脚和 SPI 实现,数据传输速率为 10 Mbit/s。ENC28J60 符合 IEEE 802.3 的全部规范,采用了一系列包过滤机制对传入的数据包进行限制,它提供了一个内部 DMA 模块,以实现快速数据吞吐和硬件支持的 IP 校验和计算^[4]。ENC28J60 对外网络接口采用 HR911102A,其内置有网络变压器、电阻网络,并有状态显示灯,具有信号隔离、阻抗匹配、抑制干扰等特点,可提高系统抗干扰能力和收发的稳定性。

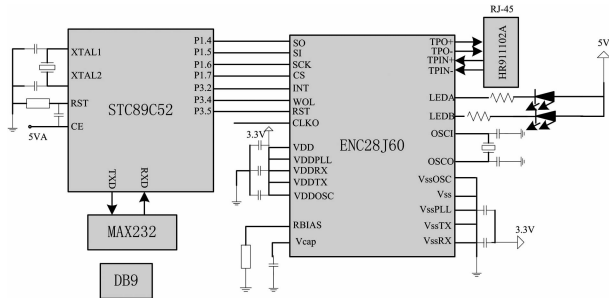


图2 网络控制模块硬件原理图

Fig.2 Network control module hardware principle diagram

3.3.2 软件设计

网络控制模块的软件设计主要包括两部分,一是基于 SPI 总线的 ENC28J60 的驱动程序编写,包括以太网数据帧结构定义、初始化和数据收发;二是 Modbus 协议编制,其软件流程如图 3 所示。

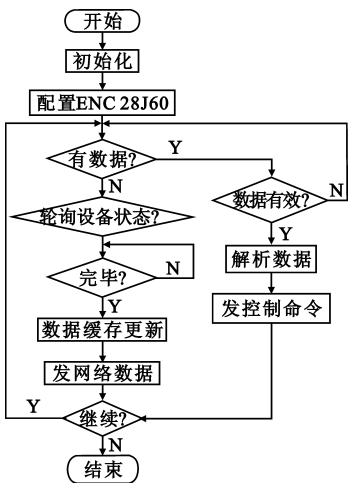


图3 软件流程图

Fig.3 Software flow chart

3.3.2.1 ENC28J60 的驱动程序编写

(1)以太网数据帧结构

符合 IEEE802.3 标准的以太网帧的长度是介于 64 ~ 1 516 byte 之间,主要由目标 MAC 地址、源 MAC 地址、类型/长度字段、数据有效负载、可选填充字段和循环冗余校验组成。另外,在通过以太网介质发送数据包时,一个 7 byte 的前导字段和 1 byte 的帧起始定界符被附加到以太网数据包的开头。以太网数据包的结构如图 4 所示。

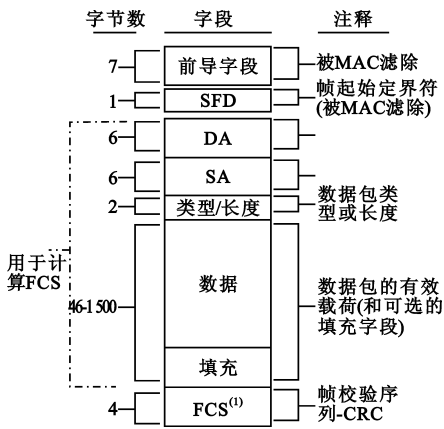


图4 以太网数据帧结构图

Fig.4 Ethernet data frame structure

(2)驱动程序编写

1)ENC28J60 的寄存器读写规则

由于 ENC28J60 芯片采用的是 SPI 串行接口模式,其对内部寄存器读写的规则是先发操作码 < 前 3 bit > + 寄存器地址 < 后 5 bit >,再发送欲操作数据。通过不同操作码来判别操作时读寄存器(缓存区)还是写寄存器(缓冲区)或是其他。

2)ENC28J60 芯片初始化程序

ENC28J60 发送和接收数据包前必须进行初始化设置,主要包括定义收发缓冲区的大小,设置 MAC 地址与 IP 地址以及子网掩码,初始化 LEDA、LEDB 显示状态通以及设置工作模式,常在复位后完成,设置后不需再更改。

3)ENC28J60 发送数据包

ENC28J60 内的 MAC 在发送数据包时会自动生成前导符合帧起始定界符。此外,也会根据用户配置以及数据具体情况自动生成数据填充和 CRC 字段。主控器必须把所有其他要发送的帧数据写入 ENC28J60 缓冲存储器中。另外,在待发送数据包前要添加一个包控制字节。包控制字节包括包超大帧

使能位 (PHUGEEN)、包填充使能位 (PPADEN)、包 CRC 使能位 (PCRCEN) 和包改写位 (POVERRIDE) 4 个内容。

4) ENC28J60 接收数据包

如果检测到 EIR.PKTIF 为 1, 并且 EPKTCNT 寄存器不为空, 则说明接收到数据, 进行相应处理。

3.3.2.2 ModBus 协议流程

本系统 ModBus 协议的数据通信采用 RTU 模式^[5], 网络控制模块作为主节点与从节点 (标校设备) 通过串口建立连接, 主节点定时向从节点发送查询命令, 对应从节点响应命令向主节点发送设备状态信息。当侦测到网络数据时, 从 ENC28J60 接收数据包中解析出命令, 将对应的功能代码以及数据, 按照 Modbus 数据帧结构进行组帧, 发送给从节点; 对应从节点响应控制命令, 进行设备参数设置。

4 系统调试与验证

试验调试环境按照图 1 进行布置, 主要包括 5 个无线网桥、1 个主控制点、2 个客户端、1 块网络控制模块板以及标校设备等, 主要测试有网络通信效果、网络控制能力以及简单的安全防护测试。测试结论: 网络连接可靠, 各控制点均能安全地对远端设备进行控制, 具备一定安全防护能力, 完全满足远程设备控制要求。

5 结束语

本文从实际需要出发, 通过对当下流行的无线通信技术的比较, 选用无线网桥实现远控系统组网; 通过开发网络控制模块, 以及相应的控制软件编制, 研制了一套用于测量船远程控制设备的系统。经几艘测量船的应用表明, 采用无线网桥进行组网完全满足系统设计要求, 具有高安全性、高可靠性、高扩展性等优点, 在日趋繁重的保障任务中发挥了重要的作用。本系统所采用的无线组网方法, 以及硬件电路的设计方案, 对其他相关控制领域均有一定的参考价值。

参考文献:

[1] 丁奇. 大话无线通信系统与技术 [M]. 北京: 人民邮电出版社, 2009.

DING Qi. Big Wireless Communication System and Technology [M]. Beijing: People's Posts and Telecommunications Press, 2009. (in Chinese)

[2] 郭渊博. ZigBee 技术与应用—CC2430 设计、开发与实践 [M]. 北京: 国防工业出版社, 2010.

GUO Yuan-bo. ZigBee Technology and Application - CC2430 Design, the Development, and the Practice [M]. Beijing: National Defense Industry Press, 2010. (in Chinese)

[3] 魏崇毓. 无线通信基础及应用 [M]. 西安: 西安电子科技大学出版社, 2009.

WEI Chong-yu. Wireless Communication Foundation and Application [M]. Xi'an: Xidian University Press, 2009. (in Chinese)

[4] 温子祺, 刘志峰, 沈安胜, 等. 51 单片机 C 语言创新教程 [M]. 北京: 北京航空航天大学出版社, 2011.

WEN Zi-qi, LIU Zhi-feng, SHEN An-sheng, et al. 51 SCM C language Innovation Tutorial [M]. Beijing: Beijing Aerospace University Press, 2011. (in Chinese)

[5] 潘高峰, 王珏. 基于 Modbus 协议的校飞集中监控系统 [J]. 遥测遥控, 2008, 29(6): 59-61.

PAN Gao-feng, WANG Yu. The Flighting Monitoring System Based on the Modbus [J]. Journal of Telemetry, Tracking and Command, 2008, 29(6): 59-61. (in Chinese)

作者简介:

潘高峰 (1972—), 男, 辽宁锦州人, 1995 年获学士学位, 现为高级工程师, 主要从事智能仪器、自动测试系统方面的研究;

PAN Gao-feng was born in Jinzhou, Liaoning Province, in 1972. He received the B.S. degree in 1995. He is now a senior engineer. His research concerns intelligent instrument and ATS.

Email: pgfzhy@163.com

谢勇 (1972—), 男, 江西余江人, 2004 年获硕士学位, 现为高级工程师, 主要从事航天测控总体技术方面的研究;

XIE Yong was born in Yujiang, Jiangxi Province, in 1972. He received the M.S. degree in 2004. He is now a senior engineer. His research concerns aerospace TT&C technology.

薛军 (1971—), 男, 内蒙古包头人, 2002 年获硕士学位, 现为高级工程师, 主要从事航天测控总体技术方面的研究;

XUE Jun was born in Baotou, Inner Mongolia Autonomous Region, in 1971. He received the M.S. degree in 2002. He is now a senior engineer. His research concerns aerospace TT&C technology.

梁盛 (1985—), 男, 江苏扬州人, 2011 年获硕士学位, 现为工程师, 主要从事软件无线电技术方面的研究。

LIANG Sheng was born in Yangzhou, Jiangsu Province, in 1985. He received the M.S. degree in 2000. He is now an engineer. His research concerns SDR technology.