数据加密在远程监控系统中的应用研究

张 京*

（成都电子机械高等专科学校计算机系 成都 610031）

【摘要】寻呼发射机是无线寻呼系统中的关键设备之一，针对其可靠工作和安全运行问题，提出了一种专用远程监控系统，介绍了智能寻呼发射机监控系统中的系统组成和系统功能，并论述了系统的硬件设计方案，从地址码和遥控命令集的设计等方面分析了系统中遥控遥测的实现原理，并重点讨论了系统为保障数据安全而采用的 IDEA 数据加密算法与 MD5 报文鉴别等关键实现技术。现场测试表明，该监控系统对提高寻呼发射机运行的安全性和可靠性具有重要作用。

关 键 词 遥控遥测； 监控系统； 数据加密； 报文鉴别

中图分类号 TP273

1 远程监控系统概述

无线寻呼发射机的作用是将传呼信息传递给用户的接受机或转发到其他发射机，只有保证其运行的稳定可靠才能实现寻呼系统的正常运转，因此对寻呼发射机进行日常监控和维护极其重要。由于寻呼发射机的安装地通常是山顶或建筑物顶部，所以难以用人工的方法对所有寻呼发射机进行持续检查和控制。本文研制了一种远程智能监控系统以实现寻呼发射台控制中心对寻呼发射机的实时遥控、遥测。

本监控系统支持 LCD 液晶显示、全中文菜单，操作上直观简便。功能上主要包括测量、控制、信息存储、遥控遥测命令接收和应答等四部分。测量功能实现对寻呼发射机的前向功率、反向功率、温度、交直流电压、电流等工作数据的测量和采集。控制功能实现对监控系统自身工作参数的设定，如工作频率、地址码等的设定和对寻呼发射机的各类保护值、报警值等，并可指根据条件对寻呼发射机的工作进行控制，如进行高驻波保护、功率切换、风机控制、后备机切换、声光报警等。信息存储功能指存储异常测量值、异常测量值开始时间、异常测量值持续时间、故障停机情况、市电停电等信息，以作为检查、维修寻呼发射机的参考和依据。遥控遥测命令接收和应答功能实现对发自寻呼发射台控制中心的 POCSAG 通信码格式遥控遥测命令的接收，经解码后执行相应的操作，并回送相应的应答信息。

2 硬件设计方案

远程监控系统硬件结构框图如图 1 所示。监控系统的控制核心采用 NEC 单片机 UPD78054，其内部有 32k 程序存储器、1kRAM 和 8 路 A/D 输入通道，并具有丰富的指令系统。存储系统采用 SRAM 芯片 43256、串行 EEPROM 芯片 24C04、EEPROM 芯片 SST 29EE020。SRAM 芯片 43256 用于存储运行状态信息和故障信息，即使系统掉电，也能通过启动备用电池保持内部信息的完整。EEPROM 芯片 SST 29EE020 用来存储汉字字库，用以支持全中文界面，显示系统采用液晶显示控制器 EMC-A0723。

解码芯片选用一种功耗极低的 POCSAG 码解码器 MA93C08，用于对遥控、遥测信息的接收和解码。利用 RS-232 串行接口与 POCSAG 编码卡连接，编码卡将监控系统欲发送的信息转换成 POCSAG 格式码流输出，用于向控制中心发送遥控、遥测应答信息。选用美国 DALLAS 公司的集

2001 年 4 月 16 日收稿

* 女 32 岁 大学 讲师

成温度传感器 DS1821 实现对电源和功率放大器的温度检测，此温度传感器变换速度快，具有独特的单线接口。系统利用单片机的 A/D 输入通道完成对功率、电压、电流等工作数据的检测，采用 DDS 芯片 AD9850 和 PLL 芯片 MB1504 实现高精度数字调制与频率合成[1,2]。

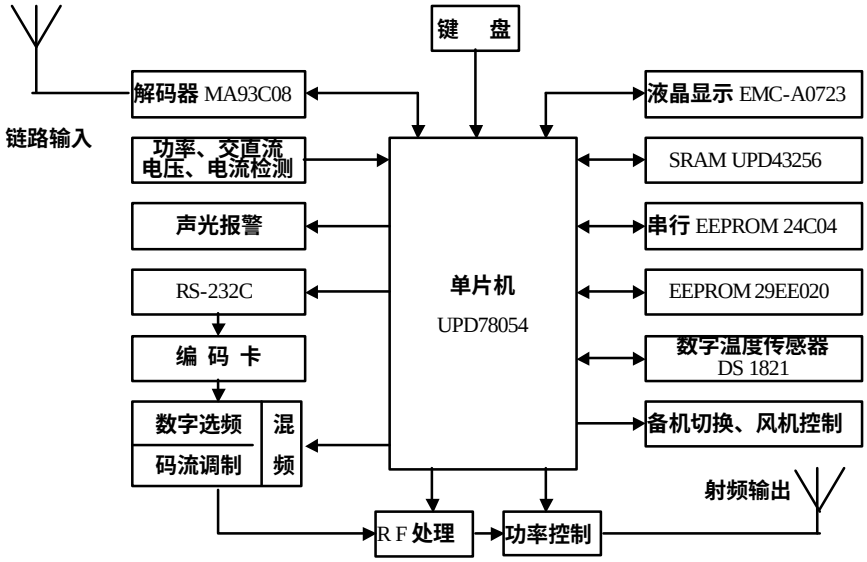

图 1　硬件结构框图

3　遥控遥测的实现原理

遥控遥测指实现寻呼发射台控制中心和本监控系统间的无线信息传送和接收，包括对控制信息及测量信息的无线传送和接收。为支持遥控、遥测的实现，控制中心和本监控系统分别分配独立的地址码。在整个监控过程中，寻呼发射台控制中心要向监控系统发送各种遥控命令和遥测命令，监控系统也要给予相应的遥控应答和遥测应答，本文设计了一个自定义遥控命令集，包含：

遥控格式：Cnnnnnnnt 控[参数类型=参数值] [参数类型=参数值]…

遥测格式：Cnnnnnnnt 测[参数类型] [参数类型]…

遥控应答格式：Cmmmmmmmt 控 Cnnnnnnnt[参数类型=成功|失败] [参数类型=成功|失败]…

遥测应答格式：Cmmmmmmmt 测 Cnnnnnnnt[被测参数=测量值] [被测参数=测量值]…

其中，nnnnnnn 为本监控系统地址码，mmmmmmm 为控制中心地址码。

在遥控遥测的实现中，为保障数据的安全，对通过公用信道传送的无线信息采用了国际数据加密算法(IDEA)进行加密。另外，还引入了报文摘要算法(MD5)对报文进行数字签名、鉴别和提供数据完整性检测，使系统信息的安全性和可靠性得到了进一步提高。

在监控系统中实现遥控遥测的原理是：寻呼发射台控制中心根据监控系统的地址码和遥控命令集经编码生成遥控、遥测报文，利用 IDEA 和 MD5 分别对除地址码外的报文进行加密和签名后得到密文，然后将此密文通过公用信发送出去。与报文地址码对应的监控系统接收到报文后，经 MD5 进行鉴别和完整性检测后，再经 IDEA 还原成遥控、遥测报文，完成解码后执行命令规定的操作，最后再向控制中心发送作相应加密和签名处理后的应答密文。监控系统发送报文、控制中心接收密文的处理过程与前述类似。

4　数据加密与报文鉴别

4.1　数据加密

由于信息是在公用信道传送，为了保证数据安全，必须采用加密算法对报文进行加密处理后再进行发送。数据加密作为一项基本技术是所有通信安全的基石。数据加密过程是由某种加密算法来

具体实施，它以很小的代价提供很大的安全保护。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。常规密码算法有 DES 、IDEA、FEAL-8 等,其优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，密钥管理成为系统安全的重要因素。在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导解密密钥。公钥密码算法有 RSA、背包密码、McEliece 密码等。其优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证，但其算法复杂，加密数据的速率较低[3]。

在监控系统中，寻呼发射台控制中心与各个发射机相对固定，密钥管理简单，可以采用常规密码算法对数据进行加密。

国际数据加密算法(IDEA)具有极高的安全性，且加(解)密速度较 DES 快得多，因此选用 IDEA 作为本系统的加密算法。IDEA 是一个迭代分组密码，分组长度为 64 bit，密钥长度为 128 bit。先将明文划分成一个个 64 bit 长的数据分组，然后经过 8 次迭代和一次变换，得出 64 bit 密文。每一次迭代包含三种运算：16 bit 的数相加、16 bit 的数相乘、16 bit 的数异或操作。通过调用编写的此三种运算的子程序即可完成复杂的迭代运算以完成加密操作[4]。

4.2 报文鉴别

无线信道干扰较强，报文经常产生误码。为了提高系统的抗干扰能力和可靠性，避免报文误码引起的误操作，必须对接收的报文进行身份鉴别和数据完整性检查。

MD5 是一种安全高效的报文鉴别算法，任何一个报文经 MD5 运算后，可得到一个报文鉴别码，利用其唯一性，可以实现数字签名、鉴别和数据完整性检测。MD5 算法中通信双方共享一小段秘密的他人无法获知的数据块，发送端先将此秘密数据块追加在报文 M 的前面，再输入到散列函数 H，计算出 MD0，然后将 MD0 加到报文 M 的后面，同时去除一开始加上的秘密数据块后发送。接收端则先将 MD0 去除，然后在报文 M 的前面追加上自己拥有的秘密数据块后，输入给散列函数 H，计算出 MD1，比较 MD1 和 MD0，若一致，则收到的报文 M 是真的，否则为假或报文在传送过程中出错[4]。其中具体的散列函数非常复杂，在此不作详细讨论，此算法可对任意长的报文进行运算，然后得出 128 bit 的 MD 代码。

5 结 束 语

本远程智能寻呼发射机监控系统通过严格测试后，已在多家寻呼台投入使用。用户在使用过程中普遍反映良好，系统的操作灵活方便、遥控遥测准确可靠、节省人力物力等优点得到了广泛认同。系统中使用的数据加密与报文鉴别等关键实现技术，很好地保证了系统信息的安全性和可靠性。

参 考 文 献

1 Yang Guoyu, Su Xianyi. A new method of DDS hybrid PLL technology in an S-band frequency synthesizer. Journal of University of Electronic Science and Technology of China, 1999, 28(4): 388~391 [杨国渝，粟显义．采用 DDS+PLL 技术实现 S 波段频率合成的一种方法．电子科技大学学报 1999, 28(4): 388~391]

2 Tang Yu,Yan Mei,Hong Fuming.A combined adaptive filter techniques for interference suppression in spread spectrum systems. Journal of University of Electronic Science and Technology of China, 1998, 28(2): 123~127 [唐 瑜，严 梅，洪福明．扩频通信中组合自适应抗干扰技术．电子科技大学学报，1998, 28(2): 123~127]

3 卢开澄．计算机密码学计算机网络中的数据保密与安全．北京．清华大学出版社，1998

4 谢希仁．计算机网络．北京．电子工业出版社．1999

Application and Research of a Date Encryption in Monitor System

Zhang Jing
(ComputerDepartment, Chengdu Electromechanical College　Chengdu　610031)

Abstract　The paging transmitter is an important equipment in wireless paging system. To ensure reliable work and the safety of the paging transmitter, this paper offers a intelligent monitor system of the special purpose. This paper describes the work principle and the structures of hardware for intelligent monitor system., also analyzes the realization principle used for remote control and measurement from how to design the address codes and the remote control commands. In this paper, the key techniques of intelligent monitor system to ensure the security of data and system reliability such as IDEA (International Data Encryption Algorithm) cryptographic and decipher method, MD5(Message Digest 5) message authentication are illustrated here. Practical test verifies the validity of this intelligent monitor system in improving the security and the reliability of the paging transmitter.

Key words　remote control and measurement ;　monitor system;　cryptographic;　decipher; message authentication

·科研成果介绍·

高速数据采集与实时信号处理

主研人员：管 庆　习友宝　陈 东等

高速数据采集与实时信号处理采用 SCXI、PCI **总线技术，实现体系结构的开放性、通用性、可扩展性及组态灵活性的特点，突破了高速数据采集的定时与控制，抑制突发噪声的数字预处理、各种采集与触发方式等关键技术。信号调理采用总线与模块化设计，使不同功能的调理模块具有互换、便于通道扩充的特点。小信号调理中采用了零漂、噪声与干扰的抑制技术，使系统达到较高的精度。软件设计采用虚拟仪器技术，为用户提供了实现系统各种功能的友好界面。**

400MHz/102 通道逻辑分析仪

主研人员：师奕兵　王厚军　田书林等

逻辑分析仪是一种重要的通用数据域测试仪器，采用多通道分相时基和分相存储技术和高精度多通道信号延时技术，实现了 400 MHz **高速定时的功能。采用高速触发存储器技术，实现了多功能高速触发跟踪功能。利用异步双沿检测技术实现了窄毛刺捕获功能。采用高密设贴片技术实现了** 102 **通道可程控探头，使探头集成化程度高、实用性强。**