

基于嵌入式 TCP/IP 的远程 GPRS 控制终端的设计与实现

刘 峰^{1,2}, 韩春燕³, 林 浒²

¹(中国科学院 研究生院, 北京 100039)

²(中国科学院 沈阳计算技术研究所, 辽宁 沈阳 110004)

³(东北大学 软件学院, 辽宁 沈阳 110004)

E-mail: liufeng@sict.ac.cn

摘 要: 介绍了基于 8 位单片机的嵌入式 TCP/IP 的远程无线控制终端的设计与实现。描述了基于 GPRS 网的数据传输过程, 嵌入式实时操作系统 RTX51 以及嵌入式 TCP/IP 协议栈简化的思路, 并着重阐述了控制终端的技术实现。

关键词: TCP/IP; GPRS; RTX51 单片机

中图分类号: TP393

文献标识码: A

文章编号: 1000-1220(2006)06-1069-03

Design and Implementation of Embedded TCP/IP-Based Long-Range GPRS Controls Terminal Station

LU Feng^{1,2}, LIN Hu², WANG Zhong²

¹(Graduate School of Chinese Academy of Science, Beijing 100039, China)

²(Shenyang Institute of Computing Technology, Liaoning, Shenyang 110004, China)

³(Software College of Northeast University, Shenyang 110004, China)

Abstract This paper introduces the design and implementation of the long-range wireless controls terminal station based on 8-bit single chip which embeds TCP/IP. It describes transmission course of data based on GPRS network, embedded real-time operating system RTX51 and embedded simple thinking of TCP/IP agreement. And illuminates the technology implementation of controls terminal station in detail.

Key words: TCP/IP; GPRS; RTX51; MCU

1 引言

随着数据无线传输需求的增加和中国移动 GPRS 业务全面投入运营, 利用移动运营商提供的无线网络实现工业设备远程控制, 可更好的适应地域跨度较大, 环境恶劣情况下的设备控制, 是工业控制系统现代化的一个重要发展方向。基于分组交换的 GPRS 网具有覆盖范围广、数据传输速度快、实时性好、通信质量高、持续在线和费用低等优点, 并可直接与 Internet 网互通, 可更好的满足工业设备控制的需要。

我们研究开发的控制终端采用单片机控制外部设备和 GPRS 模块来实现, 并在嵌入式系统中实现 TCP/IP 协议栈, 利用 GPRS 模块在网络中完成与控制中心的数据通讯。在设计中为了降低设备成本, 选用 8 位单片机, 因此如何在有限的硬件资源上较好的支持 TCP/IP 协议, 实现控制功能是本文讨论的主要内容。

2 GPRS 网络数据的收发^[1]

中国移动 GPRS 网络建立在原有 GSM 网络的基础上, 新引入了分组控制单元 (PCU)、服务支持节点 (SGSN) 和网关支持节点 (GGSN) 等新部件而构成的无线数据传输系统, 其用户能够在端到端分组方式下发送和接收数据。GPRS 网

提供网络功能将 IP 信息包从移动用户点传送至外部网络

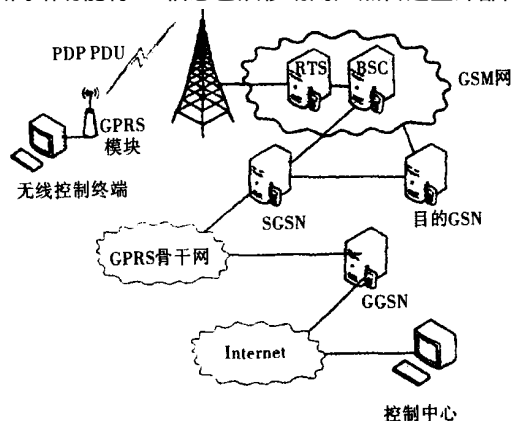


图 1 GPRS 数据收发图

GPRS 无线模块作为控制系统的无线收发模块, 用于实现与 GPRS 网络的连接。当该模块与 GPRS 连接成功之后, 通过发送 PDP 上下文激活, 由 GGSN 为其分配 IP 地址并参与外部网络建立连接。完成连接后, 即可进行数据传输, 其发送数据过程如图 1 所示。

· GPRS 模块通过串行接口从控制模块获得上传数据;

- 处理后以 GPRS 分组数据的形式发送到 GSM 基站 (BTS);
- 分组数据经 SGSN 封装后, 发送到 GPRS IP 骨干网;
- 若分组数据是发送到另一 GPRS 终端, 则先发送到目的 SGSN, 再经 BSS 发送到 GPRS 终端; 若分组数据是发送到外部网络 (如 Internet), 则将分组数据包经 GGSN 进行协议转换后, 发送到外部网络, 送达控制中心

3 RTX51

为了满足系统开发过程中控制任务的实时性和移植 TCP/IP 协议栈, 需要选定一个实时操作系统 RTX51 Tiny^[2] 是一种应用于 MCS51 系列单片机的小型多任务实时操作系统, 它完全集成在 Keil C51 编译器中, 具有运行速度快、对硬件要求不高、使用方便灵活等优点, 满足系统的要求。该系统最多可支持 16 个任务, 仅占用 800 字节左右的程序存储空间, 可以在没有外部数据存储器的 8051 系统中运行, 应用程序仍然可以访问外部存储器, 不需要扩展外部 RAM, 能满足大多数简单控制系统的需要。

该操作系统以系统函数调用的方式运行, 因此可以很容易地使用 KEIL C51 语言编写和编译一个多任务程序, 可以灵活的分配硬件系统资源 (CPU, 存储器等) 给各个任务, 从而大大的缩短了程序开发的时间并增强了软件工作的稳定性。

4 嵌入式 TCP/IP 协议栈的剖析^[3]

在设计中, 根据系统采用 GPRS 进行数据传输的特点, 这里我们只须实现 IP、ICMP、TCP 三个协议, 即可满足系统控制的需要。在其代码的实现中, 为了节省资源, 我们采用基于单一全局数组的收发数据缓冲区, 由应用负责处理收发的数

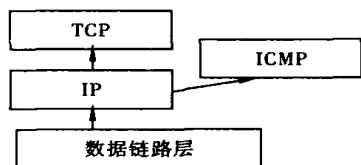


图 2 简化 TCP/IP 协议

据, 不支持内存动态分配。采用基于事件驱动的应用程序接口, 各并发连接采用轮循处理, 仅当 GPRS 网络事件发生时, 由 IP 内核唤起应用程序处理。应用程序主动参与部分协议栈功能的实现 (如 TCP 的重发机制, 数据包分段和流量控制), 由 IP 内核设置重发事件, 应用程序重新生成数据提交发送, 免去了大量内部缓存的占用。协议结构如图 2 所示。下面分别对这几个协议实现的主要细节进行阐述。

4.1 IP 协议

IP 协议是 TCP/IP 的基础, 嵌入式系统只把 IP 作为传输工具, 只需传送一些简单的数据和命令, 数据报的长度很小, 因此对于分段的功能可以裁减不要。IP 数据包头中, 服务类型是指一些服务质量的参数, 这些参数用在特定网络指示所需要的服务。而选项包括时间戳, 安全和特殊路由, 在数据包中可以没有。因此, 为简化嵌入 TCP/IP 的复杂程度, 这 2 个字段都可以忽略, 而不用作任何处理。由于不采用分段功能,

标识和段偏移量这些字段都无须考虑也不用作任何处理, 但标记字段第 2 位必须标记 1, 表示是不可分段的。因此根据控制系统实际需要, 只需实现 IP 协议中两个功能: 验证到来的 IP 报文报头的正确性, 并且对 TCP 和 ICMP 报文实行分流。

4.2 网间报文控制协议 ICMP

对于嵌入式系统, ICMP 协议只需实现它的回应机制, 而其他功能则可以忽略。只需要将接收到的回应请求消息中分组的源端 IP 和目的端 IP 交换一下, 然后将该分组的 ICMP 类型由 "ECHO" 改为 "REPLY", 最后按标准方法计算 ICMP 校验和即可。

4.3 传送控制协议 TCP

由于工业实时监控系统中数据传输量很小, 而可靠性要求较高, 所以传输层只采用 TCP 协议。标准 TCP 协议应用于嵌入式系统显得过于复杂, 因此, 需要结合 GPRS 网络传输的特点对其进行简化。

基于 GPRS 网络的 TCP 协议数据传输, 在采用公网的 Apn ("cmnet") 的条件下, GPRS 模块所获得的动态 IP 地址是移动的一个特殊的内部网段上的地址, 这个动态地址对于公网上的其他机器来说是不可访问的。对于控制终端而言, 它仅是一个客户端, 采用主动打开, 发送与控制中心的连接请求以建立连接, 然后实现对远程监控设备的遥测遥控。因此在 TCP 层的上层如只需实现客户端的应用, 可以将标准 TCP 状态机建立连接过程中服务器端建立连接的状态机部分简化掉。协议中断开连接中的主动断开部分比较复杂。在设计中我们采用, 当需要主动断开连接的时候, 发送一个 Fin 数据报; 接收到对 Fin 数据报的确认后, 再发送一个 Reset 数据报的方法, 即可顺利完成一次主动断开连接。

标准的 TCP 协议使用慢启动的滑动窗口机制。滑动窗口算法需要使用许多 32 位操作数, 并且需要较多的缓冲空间来缓冲多个要发送的数据段, 这对资源有限的 8 位微处理器来说无法较好的实现。因此, 在本系统中, TCP 并不使用滑动窗口来接收和发送数据, 而是在发送数据时, 采用在每次发送完一个数据包后等待确认信息, 当接收到确认后才能发送下一个数据段的方式。每个活动连接只能一次发送一个 TCP 数据包。这样, 网络中并发的 TCP 数据段就得到了控制。因为 TCP/IP 数据包是通过 GSM 网传输的, 所以考虑到端对端连接的带宽延迟的存在, 在控制中心我们采用同样的确认机制, 这样就可以很好的进行数据传输的流量控制。对于控制终端而言, 当有 TCP 报文到达时, 并不进行缓冲而是立刻交给应用程序处理。使用该方法后, 所有的处理只是对单个数据报的发送和确认, 简化了协议, 节约了系统的资源, 保证了协议的兼容性。

5 控制终端实现

5.1 终端的硬件实现

控制系统主要由四部分构成: 嵌入 TCP/IP 协议的 MCU、MC35 模块、电源部分和外部接口部分。该模块的硬件框图如图 3 所示。

系统选用 C8051F020MCU, 该单片机具有 25M IPS 高速

流水线式 支持标准的KeilC高级语言,有高速指令处理能力

C8051F020 内部除了具有标准 8051 机的数字外设部件外,片内还集成了数据采集与控制系统中常用的模拟部件和其它数字外设及功能部件,包括模拟多路选择器,可编程增益放大器,ADC、DAC、电压比较器、电压基准、温度传感器、可编程计数器/定时器阵列、定时器、I/O 端口、电源监视器、看门狗定时器和时钟振荡器等,通过配置内部交叉开关可灵活的实现各引脚的配置,以实现对外部设备输入量进行转换和监控,并通过系统控制模块完成被控设备状态的调整

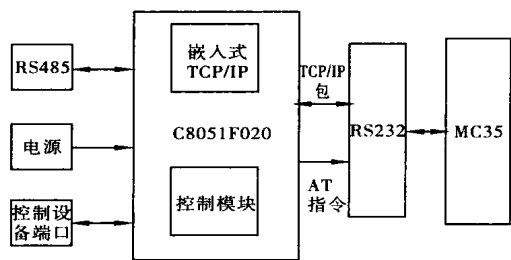


图3 硬件结构图

C8051F020 具有标准 8051 机的程序和数据地址配置,包括 256 字节的 RAM 和外部数据存储器地址空间的 4KB 的 RAM. 此外 C8051F020 的程序存储器包含 64KB 的 FLASH, 本系统最后实现的代码用 KEIL C 编译后,内核对 RAM 的占用小于 4KB, 整个系统程序的代码量小于 50KB.

C8051F020 内部具有 2 个全双工 UART, 完全用硬件实现, 都能向 CIP51 产生中断, 这些串行总线不共享定时器、中断或 I/O 端口, 所以允许用户全部同时使用. 在系统中应用 UART0 与 MC35 连接, 实现 TCP 数据报的收发. 而 UART1 用于实现 RS485, 用于与其他串行控制终端之间的通讯.

MC35 模块是西门子公司生产的 GSM 双频 GSM 900/GSM 1800 无线模块. 系统中主要应用它的分组交换操作模式 (GPRS). 在该模式下, GPRS 传输数据时不需要再拨号, 其操作通过 AT 指令来实现. 该模块通过 UART0 与 C8051F020 进行数据传输.

电源部分使用 R111M3 和 LM2576 来为单片机系统和 GPRS 模块提供 3v 和 5v 的电源.

5.2 终端软件实现

单片机上电复位后, 首先对 MAX3223, MAX3485 模块进行初始化, 完成与外接模块协商处理, 如波特率、是否有奇偶校验等. 接着, 通过串口发送 AT 指令初始化 GPRS 无线模块 MC35 (GPRS 模块采用 IP over PPP 实现数据终端的接入), 使之附着在 GPRS 网上, 检查诸如 SM 卡情况、GPRS 网络覆盖情况、信号情况等. 获得网络运营商动态分配给 GPRS 终端的 IP 地址, 并与控制中心或服务器之间建立连接.

主程序采用中断加轮循的方式, 用中断触发的方式接收被控制设备发出的数据, 并设置了一个接收队列暂存这些数据. 如数据不需上传则由本地控制处理模块直接处理并返回控制信号, 如果是上传控制中心的数据则对其进行 TCP/IP

封装处理发送, 在数据打包处理过程中, 如果检测到系统的信号不好, 网络连接不畅通, 或者不是 GPRS 网络覆盖区, 将进行数据发送缓存处理, 同时将数据放进发送队列等待发送.

程序始终轮循有无 GPRS 网络数据到达, 如有使用 AT 命令读入数据, 然后调用 IP 的相关处理函数进行 TCP/IP 数据解包处理. 首先判断是否为 IP 数据包, 如是则判断是 ICMP 报文还是 TCP 包, 并根据相应的协议对其解包, 获得相应的控制数据, 控制模块或根据远程控制指令采取控制操作.

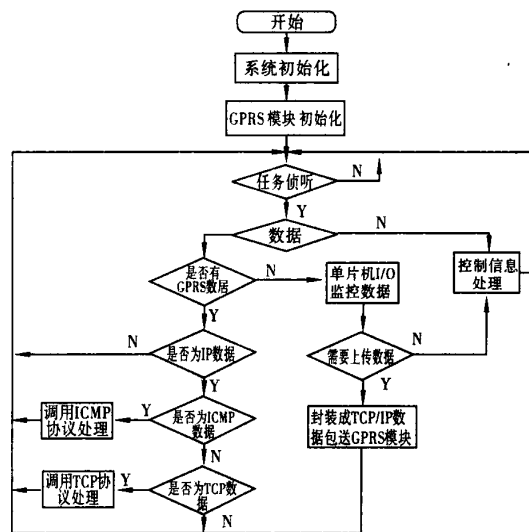


图4 系统软件工作流程图

系统如果没有数据到达, 则保持中断轮循状态. 工作流程如图4所示.

6 结束语

本文讨论的远程控制系统在 8 位单片机中实现了嵌入式 TCP/IP 协议, 并通过对 MC35 模块的控制, 实现 GPRS 业务的数据传输功能, 提高了数据传输的实时性、可靠性和数据传输的能力, 具有外围器件少、电路简单、系统成本低等优点. 本文设计的 GPRS 无线通信控制器, 已应用在广东联通的直放站控制系统, 具有较好的工作稳定、可靠性.

References

- [1] Lv Jie. GPRS Technology [M]. Beijing: University of Posts and Telecommunications Press, 1998
- [2] Pan Zuo-jin. C8051F020/1/2/3 mixed-signal ISP FLASH MCU Family Datasheet Rev 1.1 2002, 10
- [3] Douglas E. Comer. Internetworking with TCP/IP Vol 1: principles, protocols, and architectures fourth edition [M]. Publishing House of Electronics Industry, 1998
- [4] Embedded Network Microcontroller [Z]. Myson Century Semiconductor Inc, 2002