基于 GPRS 的嵌入式无线数据传输终端的设计①

Design of Embedded Wireless Data Transmission Unit Based on General Packet Radio Service

郭启军　张浩然　姜　彬　(浙江师范大学 数理与信息工程学院 浙江 金华 321004)

摘　要：本文介绍了一种基于 GPRS 的嵌入式 DTU 模块通过现有 GSM 网络连接互联网实现远程无线数据传输方案。系统以 Microchip 公司的 PIC24 系列单片机为基础,移植入 TCP/IP 协议,采用 UC/OS－Ⅱ操作系统进行进程管理,进而实现控制 Q2403 GPRS 模块的目的来设计出一种嵌入式的 DTU,利用该 DTU 则可同 Internet 上的主机进行数据的传输。在 3G 技术尚未成熟阶段,该模块的实现具有一定的现实应用意义,现已成功应用于金华市电力设备的环境监测中。

关键词：无线分组交换业务 微芯公司 TCP/IP 协议栈 UC/OS－Ⅱ 无线数据传输终端

1　引言

GPRS 为第二代移动通信技术 GSM 向第三代移动通信(3G)的过渡技术,具有接入迅速、永远在线、流量计费等特点,并且 GPRS 理论上提供高达 171.2Kbps 的传输率,这就使得移动通信无线数据传输成为可能。现在市面上各种基于 GPRS 的适用于无线数据传输的数据传输终端(DTU)层出不穷,这类 DTU 在传输协议的选择上,大多采用 UDP＋IP 的方案,其实现简单,协议移植工作少。在无线数据业务透明传输的要求下,数据传输的实时性是人们关注的重点。本文在 MCU 上通过移植入 UC/OS－Ⅱ操作系统来管理 GPRS DTU 各进程设计出了一种实时性强,可靠性好的 DTU。该 DTU 在远程突发性数据传输中有不可比拟的优势,特别适用于频发小量的实时传输,也适用于偶尔的大数据量传输[1]。

2　基于 GPRS 的嵌入式无线 DTU 的功能及硬件组成

基于 GPRS 的数据业务的优势,各种应用于无线数据传输的 DTU 在工业控制和监测中发挥着越来越重要的作用。

2.1 嵌入式无线 DTU 的功能

DTU 作为数据传输单元,其主要有如下核心功能:

(1)内部集成 TCP/IP 协议栈

GPRS DTU 内部封装了 PPP 拨号协议以及 TCP/IP 协议栈并且移植入了嵌入式操作系统。它可看作是嵌入式 PC 与无线 GPRS MODEM 的结合;它具备 GPRS 拨号上网以及 TCP/IP 数据通信的功能、采用心跳包保持永久在线,支持断线自动重连、自动重拨号等特点。

(2)提供串口数据双向转换功能

GPRS DTU 提供了串行通信接口,可以将串口上的原始数据转换成 TCP/IP 数据包进行传送,不需要改变原有的数据通信内容,可以和各种使用串口通信的用户设备进行连接。

2.2 硬件组成

基于 GPRS 的嵌入式无线 DTU 其硬件设计方案是采用:MCU 控制 GPRS 模块来实现因特网的接入,从而具有数据传输功能。其总体的硬件设计框架如下图 1 所示:

(1)GPRS DTU 采用 PIC24FJ128GA010 单片机为主控单元。它是微芯公司的 16 位单片机,具有大容量的 ROM 和 RAM,不需扩展 ROM,RAM 即可移植入 TCP/IP 协议栈和 UC/OS－Ⅱ。外部资源丰富,利于产品的更新;双串口:一个串口连接 GPRS 模块,实现了单片机控制

① 基金项目:浙江省新苗人才计划(KYZKJY08070)

GPRS 模块的通信连接;另一串口连接数据采集设备。

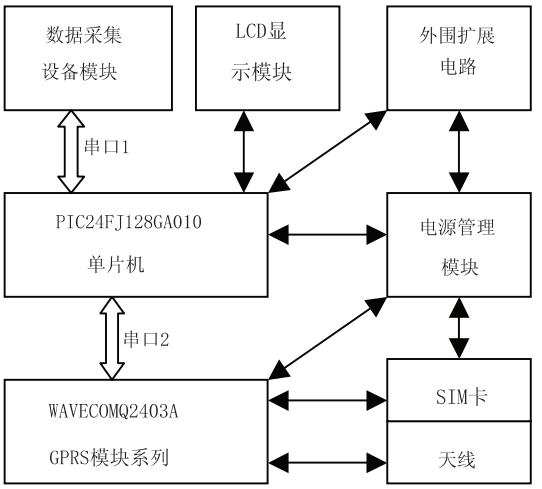

图 1　GPRS DTU 硬件框架图

(2) GPRS 模块采用的是 WAVECOM 公司的 Q2403A,该模块不带协议栈,给整个 DTU 的协议设计上更大的空间,有利于协议代码的自裁减。

(3) 电源管理模块,在电源设计上,MCU 工作电压为 2.0v ~3.6v,Q2403A 工作电压为 3.3v,外围扩展电路有工作电压为 12v 的继电器,工作电压为 5v 的其他设备。电源管理模块解决好各器件的点电平转换。

(4) 显示模块采用 HS12864 LCD,通过 PIC24 单片机的 I/O 口控制,实现通信交互显示。

3　基于 GPRS 的嵌入式无线 DTU 的软件设计

GPRS DTU 其传输数据的可靠性,实时性,很大一部分还是要通过软件设计来完成。软件设计的好坏关系着 DTU 的通信质量。在 GPRS DTU 的软件设计上,本文引进 UC/OS – Ⅱ 操作系统作为系统软件的核心。本系统软件基于两层设计,包括操作系统层,用户任务层。各任务层以操作系统层为基础,统一由操作系统对其进行管理[2]。

3.1 操作系统层

UC/OS – Ⅱ 操作系统可以管理多达 64 个任务,采取 OSTaskCreate( ) 或 OSTaskCreatExt( ) 来创建任务;OSTaskDel( ) 来使任务返回并将其处于休眠状态;OSTaskSuspen( ) 和 OSTaskResume( ) 来挂起和恢复进程;通过 OSTaskChangePrio( ) 来改变进程的优先级进而保证系统运行的实时性。在整个 GPRS DTU 中 UC/OS – Ⅱ 需要管理的进程如下图 2 所示:

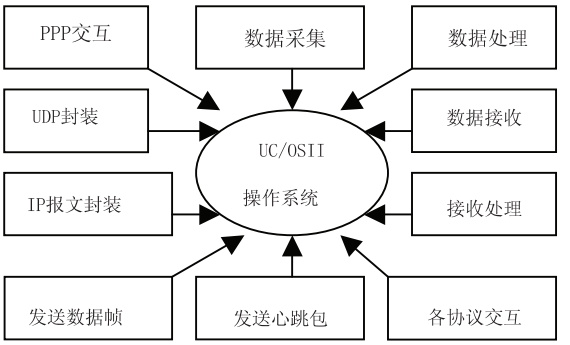

图 2　UC/OS – Ⅱ 管理用户进程

3.2 用户任务层

在用户任务层中,各个任务是通过抢占 CPU 的使用权来运行的,它们之间存在一定的逻辑关系,彼此互相联系又互相制约。信号量、邮箱、消息队列等功能为实现任务间的通信提供了有力工具。在实现 GPRS DTU 的通讯功能中,用户任务层主要分为如下几个部分:PPP 链路通信进程,TCP/IP 数据包封装进程,数据接收处理发送进程。各部分通信处理流程如下图 3 所示:

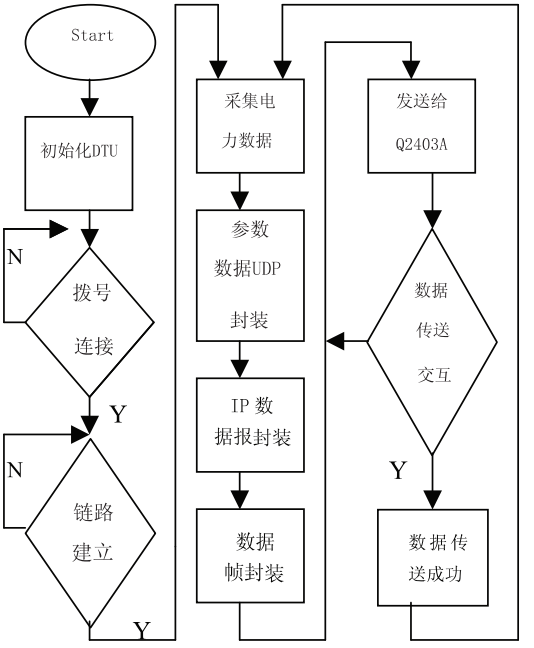

图 3　各进程通信流程

3.2.1 PPP 链路通信进程

在 GPRS 模块登录到 GSM 网络后,采用拨号的方

式,通过 PPP 协议进行链路建立,链路过程中,采用交互机制向 ISP 申请 IP 地址。在获得 IP 地址后,GPRS DTU 就可以和因特网上的主机进行数据传输了。PPP 链路通信主要分为如下几步:

(1)拨号连接:

拨号连接由单片机通过串口给 Q2403A GPRS 模块发送 AT 指令,GPRS 模块通过拨"*99***1#"登录到 GGSN。拨号过程中,设置了检测 GSM 网络信号强度,采取超时重联的机制,确保 GPRS DTU 能顺利的连接上网络。

(2)用 LCP 建立 PPP 连接阶段

LCP 协议用于建立、构造、测试链路连接。在拨号成功连接后,GGSN 首先会返回一个 PAP REQ 数据帧。DTU 通过发送一个 LCP REQ 帧,以强迫进行协议协商阶段。

在此我们在单片机中采用接收中断来获得 DTU 收到的 LCP 数据,并进行交互。其过程如下:

```
Void recdata_gprs(void)
{ recdata = SBUF;
If((*recdata = =0x7E)&&(*recdata+1 = =
0XFF)&&(*recdata+3 = =0XC0)&&(*recdata+4
= =0x21)&&(*recdata+5 = =0x01)) //查询 ISP
发送的包是否此类型。
{ PPP_EXCH_SEND1( ); } //接到了 LCP - RE-
QUEST 包,则发送应答包。
……
}
```

该函数用来查询 ISP 是否发送过来 LCP - REQUEST,LCP 协议包格式如下:

LCP PACKET: 7E FF 03 C0 21 01……7E。首尾的数据 7E 是协议的结束和开始标志;FF 03 为地址域,控制域; C0 21 为协议域,代表链路控制数据;01 为代码域,表示请求配置。

DTU 在接收到该配置请求时,通过发送一个 LCP REQ 帧,以强迫 DTU 和 ISP 进入协议协商阶段。采用 PPP_EXCH_SEND1()函数返回 LCP - ACK 应答接收配置 LCP 协议包。该函数如下:

```
Void PPP_EXCH_SEND1( )
{ WORD xdata i, len=22;
    PPP_Fcs(EXCH_DATA, len); //此函数计算
出改交互包的 CRC 校验码值。
    For(i=0;i<len;i++)
    { TI=0;
      SBUF=EXCH_DATA[i];
        //逐个发送 LCP 应答包。
        While(TI= =0); }
}
```

其中:EXCH_DATA[ ] 数组存放的 LCP - ACK 包。格式如下:7E FF 03 C0 21 01 01 00 0E 02 06 00 00 00 00 07 02 08 02 00 00 7E。

上面是一个完整的 LCP 链路交互过程。在 LCP 协议协商阶段,可能会多次进行这样的交互,但是各交互过程同上述程序的编制类似。LCP 协商成功后进入身份验证阶段。

(3)认证授权阶段

一旦 LCP 的配置参数选项协商完后,通信的双方就会根据 LCP 配置请求报文中所协商的认证配置参数选项来决定链路两端设备所采用的认证方式。GPRS DTU 向 ISP 发送请求认证配置,进入认证授权阶段。认证授权请求其协议包格式如下:7E FF 03 C0 23 01 ……7E。

在协议包中 C0 23 为协议域,代表 PAP 协议认证。01 表示请求认证。之后单片机接收串口数据来查询检测 ISP 发送过来的 PAP 认证应答协议包。检测到了,则认证成功。

(4)网络层协议阶段

一旦 PPP 完成上述阶段,便进入网络协议阶段。DTU 通过发送 NCP 帧,以选择和配置一个或多个网络层协议。NCP 协议主要使用 IPCP 协议了。IPCP 控制协议主要是负责完成 IP 网络层协议通信所需配置参数的选项协商的。依据两端设备的配置选项可将 IPCP 的协商过程分为"静态"和"动态"。本文采用动态协商的方式。即:动态获取 IP 地址。

IPCP 协议过程如下:

① DTU 向 ISP 发送 NCP 协议包,请求配置。协议包为:7E FF 03 80 21 01…… 00 00 00 00 CRC1 CRC2 7E。

协议包中:80 21 系协议域,为网络控制协议,01 为请求配置。00 00 00 00 是 Config - Request 报文的 IP 地址配置参数全填充为 0。

② DTU 检测 ISP 发送过来的 NCP - ACK 报文,检

测到了,则可获取改报文中的网关地址和 IP 地址。并将此保存。

上述过程即为一个完整的 PPP 链路建立[3]。

3.2.2 TCP/IP 数据传输进程

PPP 完成了链路建立后,DTU 就可以和网络上的主机进行通信了。在因特网上通信采用 TCP/IP 协议。对于庞大的 TCP/IP 协议族,Microchip 公司为其 MCU 开出发了裁剪的 TCP/IP Stack。该协议栈能很好的整合在 PIC 各类型的单片机中,在本 GPRS DTU 中移植入了精简的 Microchip TCP/IP Stack。

(1) UDP / IP 数据报的封装

DTU 获得了一个动态的网络 IP 地址,在互联网上通信,要进行数据传输,还需要通过上层协议来进行数据的封装。

在传输层,本系统采用了 UDP 协议实现数据的透明传输。GPRS DTU 处理完采集到的电力设备数据要在运输层封装成一个 UDP 数据报。UDP 数据报封装的格式是在数据前添加 8 个字节的固定首部,即:源端口号(2 字节) + 目的端口号(2 字节) + 总长度(2 字节) + 校验和(2 字节)。端口号可由自己来定义,在此我们定义了一个 8888 端口。

产生了用户数据报以后,需要组装成一份待发送的 IP 数据报。IP 数据报是在用户数据报的基础上添加 IP 报头。在 IP 报头中最重要的是定义了源 IP 地址(也即是嵌入式设备的地址),以及目的 IP 地址。在此通过改写 TCP/IP 协议栈的 API 函数来达到数据封装,最终形成一个可以在因特网上传输的数据帧[4]。

(2) 无线数据传输的实现

在完成了 PPP 链路建立后,GPRS DTU 就可以采用 TCP/IP 协议将数据采集设备采集到的数据信息传送到数据接收控制中心。数据接收控制中心是安装在网络上另一个主机上的软件,该软件可以采用 VB 或 DELPHI 来编制。数据接收控制中心软件部分截图如下所示(图 4):

图 4　GPRS DTU 数据接收控制中心软件

从当前状态中,我们截取了一个采集到电力设备 1 温度的完整 IP 包,其数据包如下:45 00 00 1E 00 F0 00 00 9F 17 7E 16 3D AF E4 0A 3D AF E4 AC 22 B8 22 B8 00 0A 7F 7A 02 32 。

该 IP 数据报的数据分析如下:45:4 表示 IP 版本号为 VER4;5 表示数据报首部的总长度(5 * 4 = 20),首部没有选项;00:服务类型;00 1E:整个数据报的总长度为 30(也即整个数据包的个数为 30);00 F0 为 16 位标识;00 00 为 3 位标志和 13 位分片偏移;9F 为生存时间;17 为 UDP 协议;7E 16 为首部校验和; 3D AF E4 0A 表示源 IP 地址为:61.175.228.10;3D AF E4 AC 表示目的 IP 地址:61.175.228.172;22 B8 22 B8 表示通信双方端口号都为 8888;00 0A 为 UDP 数据报总长度为 10(即:22 B8 22 B8 00 0A 7F 7A 02 32 数据串的长度);7F 7A 为 UDP 数据报的校验和;02 表示数据标识 2(机器温度),32:温度为 50。从该 IP 数据报,反映双方通信成功。GPRS DTU 无线数据传输功能实现。

4　小结

论文讨论了 GPRS DTU 的 INTERNET 接入技术,通过点对点协议建立通信链路,将集成有 GPRS 模块的 DTU 采集处理后的数据经 UDP/IP 封包,采用 TCP/IP 协议进行远程无线数据传输。系统实现了 GPRS 业务的数据传输功能,具有外围器件少、电路简单、系统成本低等优点。无线网络数据传输, 对远程抄表,医疗监控、家居安全监测,车载设备检测等具有重要的意义。GPRS DTU 的设计得到浙江省新苗人才计划的资助,该课题现正成应用于金华市电力设备的环境监测中,经实验,该 DTU 具有较好的稳定性和可靠性。

参考文献

1 侯婷,杨宏业,李俊芬,等. GPRS 无线数据传输终端的设计和实现. 微计算机信息,2006,(23):167,295 -297.

2 王琦,刘丽丽. 基于 μC/OS - Ⅱ的远程抄表系统终端设计. 计算机系统应用,2005,14(7):77 -80.

3 关宇东,陈学泉,朱伟明. 嵌入式单片机 PPP 协议的应用研究. 计算机应用,2003(2):15 -18.

4 谢希仁. TCP/IP 协议族. 北京:清华大学出版社,2006:150 -233.