

# 基于 MC37I 的数传终端设计

李明明,何通能

(浙江工业大学 信息工程学院,浙江 杭州 310023)

**摘要:**为解决污染现场的数据上传(至服务中心)问题,将通用分组无线业务(GPRS)技术应用到环境污染监测领域,数据采集模块通过串口与 GPRS 模块连接,将数据以无线方式上传。介绍了一种基于 MC37I 和 STC12C5A56S2 无线数据传输终端的设计。研究了系统的硬件结构设计,介绍了 PPP 协议的数据包结构,重点分析了 PPP 协议数据包。采用了嵌入式 uIP 协议栈,通过在单片机(MCU)中移植嵌入式 TCP/IP 协议,实现了数传终端与服务中心的数据无线传输。实验结果表明,所设计的数据传输速率能够满足污染现场数据上传的速率要求。

**关键词:**微控制器;MC37I;PPP 协议;uIP;通用分组无线业务

中图分类号:TP393

文献标志码:A

文章编号:1001-4551(2011)04-0482-04

## Design of data transmission terminal based on MC37I

LI Ming-ming, HE Tong-neng

(School of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China)

**Abstract:** In order to solve the problem of transporting data from contaminated sites to service center, general packet radio service(GPRS) was applied in environmental pollution monitor domain, data acquisition module and GPRS module were connected by serial port, so data could transport by wireless. Based on MC37I and STC12C5A56S2, a design of wireless data transmission terminal was introduced. Its scheme and hardware were discussed, The structure of data packet of PPP protocol was analyzed in detail. uIP was used in the project, through transplanting of TCP/IP protocol on microcontroller unit(MCU), data communication between data transmission terminal and monitoring center was realized. The experimental results show that the speed of data transmission could meet the requirements.

**Key words:** microcontroller unit(MCU); MC37I; PPP protocol; uIP; general packet radio service(GPRS)

## 0 引言

在单片机系统中应用 GPRS 模块实现无线网络的接入技术已经被广泛地用于各种领域。例如,将 GPRS 应用于电源质量监测平台以实现远程电源质量的监测<sup>[1]</sup>;将单片机与 GPRS 模块设计成具有无线远程报警功能的汽车防盗器<sup>[2]</sup>;利用 GPRS 模块 MC39I 和 MSP430FG4619 单片机实现 GPRS 远程电能管理终端系统<sup>[3]</sup>;将基于 GPRS 的车载数据传输终端应用在智能运输系统中<sup>[4]</sup>;采用 AT89C52 单片机与西门子 MC39I 模块,设计了船舶智能火灾报警系统<sup>[5]</sup>;使用 MC39I 模块和 AVR 单片机设计了一种油井远程监控系统,该系统主要负责实时采集油井运行的各种生产

数据,并将这些信息经无线网络发送给监控中心服务器<sup>[6]</sup>。本研究介绍一种基于 GPRS 技术在单片机上实现的电力设备远程监控系统,该系统可以对电力设备运行情况进行监测,发生故障时可以及时地报警<sup>[7]</sup>。

本研究主要应用于环境污染领域,针对污染现场的数据上传问题,通过此数传终端实现数据采集设备与远程监控中心之间的数据通信。数传终端以 GPRS 方式实现对 Internet 的无线接入。GPRS 具有实时性好、可靠性高、成本低等优点。

## 1 设计方案

数传终端主要由单片机 STC12C5A56S2 和 GPRS 模块(MC37I)组成,其系统框图如图 1 所示。GPRS 模

块 MC371 通过串口与 MCU 进行通信。单片机通过发送 AT 命令对 MC371 进行初始化,在单片机上移植 TCP/IP 协议栈实现数据的 TCP/IP 封装,通过 MC371 模块发送至远程控制中心。

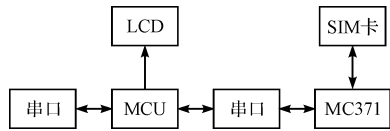


图1 数传终端结构框图

本研究所选择的 STC12C5A56S2 是新一代的 8051 系列单片机,主要性能如下:1 个时钟/机器周期,增强型 8051 内核,速度比普通 8051 快 8 ~ 12 倍;具有空闲模式,掉电模式低功耗设计;56 KB 片内 Flash 程序存储器,可擦写 10 万次以上,1 280 Bytes 片内 RAM 数据存储器。

本研究选用的 GPRS 模块为西门子 MC371,它是替代现已停产的 MC391 的 GPRS 模块。在温度特性上,MC371 比 MC391 更好,能在  $-45\text{ }^{\circ}\text{C} \sim +80\text{ }^{\circ}\text{C}$  使用;在性能上,MC371 比 MC391 多了一个串口,可以实现一个串口进行 GPRS 通讯,另一个串口进行 AT 指令控制;在接口方面,MC371 不再像 MC391 那样使用柔性排线进行连接,而是直接使用板到板的连接器进行连接,增加了可靠性和稳定性;而在功能上完全和 MC391 一样,AT 指令也是 100% 的兼容。

系统硬件主要由 STC12C5A56S2 微控制器、MC371 模块、SIM 卡座、串口接口、LCD 显示模块组成。

MC371 模块的接口为 50 针的 Hirose 连接器。这 50 个引脚可以划分为 5 类:电源接口、串口通信接口、SIM 卡接口、音频接口和控制信号接口。

当 MC371 加电后必须给 IGT 引脚一个大于 100 ms 的低电平信号,模块才能启动。MC371 提供了比较齐全的串口控制引脚,考虑到其与单片机的 UART 进行连接,因而采用两线连接:RXD0 和 TXD0,对 MC371 通信的控制可以通过软件的方法实现。SYNC 引脚用来驱动 LED,以此来表示 MC371 的工作状态:报警状态、空闲模式、无网络服务、数据传输中等状态。EMERGOFF 为控制信号输入引脚,当给此引脚一个大于 10 ms 的低电平信号时,MC371 将立即关闭,停止工作。

此外,MC371 提供了 6 个引脚用于连接 SIM 卡,该系统采用标准的 SIM 卡卡槽。

## 2 通信协议及实现

若要通过 MC371 模块实现对 Internet 的接入,需要使用一些必需的通信协议,如 TCP/IP 协议。鉴于

单片机资源有限,必须使用裁剪的 TCP/IP 协议。由于本设计选用的 MC371 为通用 GPRS 模块,模块本身并没有 TCP/IP 协议,需要编程实现这些协议。而 uIP 是专为 8 位和 16 位的嵌入式微控制器设计的微型 TCP/IP 协议栈。uIP 提供了网络通信所必需的协议,本身代码和占用的内存数都非常少,uIP 的源代码只有几 KB, RAM 占用仅几百字节。而且 uIP 是一个完全由 C 语言编写的开源软件。

### 2.1 协议选择

(1) 数据链路层选择 PPP 协议。PPP 协议在数据传输过程中有差错检测功能,通信双方可以协商数据包大小、认证方式、链路质量等,完成用户认证后,可以选择高层协议类型,使终端获得动态的 IP 地址。

(2) 网络层选择 IP (Internet Protocol) 协议和 ICMP (Internet Control Message Protocol) 协议。IP 协议是 TCP/IP 协议的核心部分,所有的上层数据报文,包括 TCP、UDP、ICMP 和 IGMP 报文都是以 IP 报封装传输的。ICMP 协议主要用来传送差错信息和控制信息。

(3) 传输层可以根据实际应用选择 TCP (Transmission Control Protocol) 协议或 UDP (User Datagram Protocol) 协议。TCP 是一种面向连接(连接导向)的、可靠的、基于字节流的传输层通信协议。UDP 是 OSI 参考模型中一种无连接的传输层协议,提供面向事务的简单不可靠信息传送服务。在本研究中,由于数据传输终端需要不断地将数据发送至远程控制中心,发送的数据量比较大,且对通信要求比较高的可靠性,故选用 TCP 协议。

### 2.2 PPP 协议

PPP 协议来自 ISO 标准通信协议中的 HDLC (高层数据链路协议),主要为串行链路提供一个简单高效的数据链路,并能承载高层的网络协议。PPP 提供了 3 个主要功能<sup>[8]</sup>:

(1) 组成帧的方法,明确规定一帧的结构以及下一帧的起始。帧格式也用于处理差错检测。

(2) 链路控制协议 (LCP, Link Control Protocol), 包括建立线路、测试线路、协商选择项和拆除线路。

(3) 网络控制协议 (NCP, Network Control Protocol), 以独立于所使用的网络层协议的方式提供协商网络层选项的方法。所选择的方法对每一种所支持的网络层有不同的 NCP。

为了在点到点连接中建立通信,PPP 连接的每一端都必须发送 LCP 数据包来配置和测试数据连接。在连接建立后,对等实体还有可能需要认证。然后,

PPP 必须发送 NCP 数据包来选择一种或多种网络层协议来配置。一旦被选中的网络层协议被配置好后,该网络层的数据包就可以在链路层上传送了<sup>[9]</sup>。PPP 帧格式如图 2 所示。

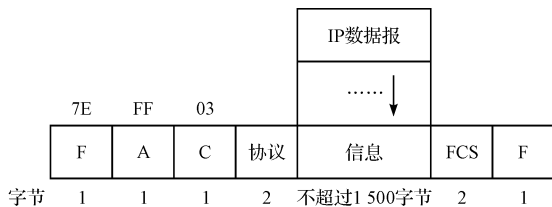


图 2 PPP 帧格式

图 2 中,F 为标志字段,用来标志 PPP 帧的边界;A 为地址字段,因为 PPP 协议是用于点对点连接,它使用绝大多数局域网中的广播地址 11111111,这样可避免在协议中使用数据链路层地址;C 为控制字段,其值为 00000011,表示在帧中不使用序号;协议字段对应不同的信息字段类型,如 0x0021 对应的信息字段是 IP 数据报,0xC021 对应的信息字段是链路控制数据 LCP,0xc023 对应的信息字段为安全性认证 PAP 等;FCS 为帧检验序列字段,用来进行差错检测。

在 GPRS 模块拨号成功后,就要进行 LCP 协商配置。LCP 协商配置的主要任务是建立、构造、测试链路连接。在本研究中,LCP 协商配置主要有协商 ACCM 项和验证方式。LCP 数据包封装在 PPP 帧的信息字段中,其协议字段为 0xC021。LCP 数据包格式如表 1 所示。

表 1 LCP 数据包格式

| 代码     | 标识     | 长度     | 数据     |
|--------|--------|--------|--------|
| 1 byte | 1 byte | 1 byte | 1 byte |

其中,代码字段表示 LCP 数据包类型;标识字段是数据包的标识,用于匹配请求与响应;长度字段是数据包的长度;数据字段其内容则根据数据包类型不同而不同。LCP 数据包类型代码如表 2 所示。

表 2 LCP 数据包类型代码

| 代码 | 描述   | 代码 | 描述   |
|----|------|----|------|
| 1  | 配置请求 | 7  | 代码拒绝 |
| 2  | 配置确认 | 8  | 协议拒绝 |
| 3  | 配置否定 | 9  | 回显请求 |
| 4  | 配置拒绝 | 10 | 回显应答 |
| 5  | 终止请求 | 11 | 放弃请求 |
| 6  | 终止确认 |    |      |

针对本研究,对于 MC371 与 MCU 连接的情况下,一般只考虑代码段位 1,2,3,4(配置请求,配置确认,配置否定,配置拒绝)4 种 LCP 资料包,这是实现应答所必需的最低限度。

### 2.3 PPP 协议包分析

捕获的 LCP 协商阶段的数据包如图 3 所示。数据包以 0x7E 开始和结束,因此若数据包内部若出现 7E 或控制字符的 ASCII 码,则用 7D,以及此特殊字符与 0x20 异或的结果代替。下面将给出部分数据包的解释、分析。

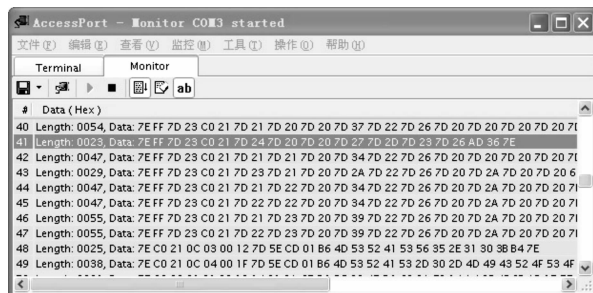


图 3 LCP 协商过程数据包

第 40 行:7E FF 03 C0 21 01 00 00 17 02 06 00 00 00 00 05 06 7E CD 01 B6 07 02 08 02 0D 03 06 C0 14 7E,其中,协议类型 C021 表示 LCP 协议,01 表示此数据包为配置请求包,00 为 ID,0017 为长度段,紧接着后面为配置选项:1 字节的配置选项类型,1 字节的长度,若干字节配置选项参数,如 02 为配置选项类型 (ACCM),06 表示配置选项长度,00 00 00 00 表示配置选项参数,05 为 Magic-Number 配置选项,06 为配置选项长度,配置参数为 7E CD 01 B6,07 为 Address-and-Control-Field-Compression (ACFC) 选项等;

第 41 行:7E FF 03 C0 21 04 00 00 07 0D 03 06 AD 36 7E,代码为 04 表示为配置拒绝包,说明数传终端在上一配置请求选项中含有部分不可识别或不被接受的选项,即 0D (Callback) 配置选项不被识别或不被接受;

第 42 行:7E FF 03 C0 21 01 01 00 14 02 06 00 00 00 00 05 06 7E CD 01 B6 07 02 08 02 38 A7 7E,经分析可知此数传终端已经将 ISP 不可识别或不被接受的 0D 配置选项删除了,再次封装成配置请求包发送给 ISP;

第 43 行:7E FF 03 C0 21 03 01 00 0A 02 06 00 0A 00 00 6C 50 7E,经分析知 ISP 否认了 ACCM(02) 选项的配置参数(00 00 00 00),并指定其配置参数为 00 0A 00 00;

第 44 行:7E FF 03 C0 21 01 02 00 14 02 06 00 0A 00 00 05 06 7E CD 01 B6 07 02 08 02 C0 3C 7E,数传终端按照 ISP 发来否认包的内容作了更改后,再次封装为配置请求包;

第 45 行:7E FF 03 C0 21 02 02 00 14 02 06 00 0A 00 00 05 06 7E CD 01 B6 07 02 08 02 2B 55 7E,此为

ISP 发送的配置确认包,表明此时数传终端发送的配置选项均可识别且被接受。

对于 PAP 认证和 IPCP 配置阶段的数据包也可作类似分析,故在此便不给出分析过程。PPP 数据包如图 4 所示。对于 PPP 帧中“协议”字段的取值及含义如表 3 所示。

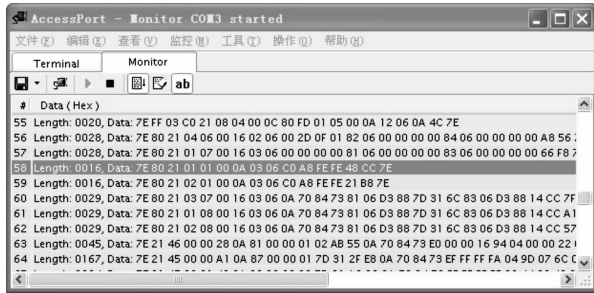


图 4 PPP 协议数据包

表 3 协议字段的取值及含义

| 取值   | 协议   | 取值   | 协议   |
|------|------|------|------|
| C021 | LCP  | C023 | PAP  |
| C223 | CHAP | 8021 | IPCP |

### 2.4 uIP 协议栈及 TCP 通信的实现

uIP 是一个仅包含三层网络层核心协议的协议栈,本身不包含任何类型的底层网络驱动和上层应用程序,它只提供接口函数供用户开发使用。因此为了完成与网络设备的交互,用户必须根据网络设备的类型在 uIP 中自行实现对底层网络设备的驱动。

由于本设计链路层采用的是 PPP 协议,用 PPP 协议作为 uIP 的底层设备驱动。uIP 提供了 3 个函数给底层系统: void uip\_init(void), uip\_input(), uip\_periodic(conn)。uIP 内核中有两个函数需要底层设备驱动程序的直接支持,一个是当网络设备驱动程序从网络层收到一个数据包时需要调用函数 uip\_input(), 设备驱动程序必须事先将数据包存放到 uip\_buf[], 包长存放到 uip\_len, 然后交由函数 uip\_input() 处理; 另一个是 uIP 内核直接提供给底层设备驱动程序的函数 uip\_periodic(conn), 此函数用于 uIP 内核对各连接的定时轮询。

此外,应用程序还必须提供一个回应函数给 uIP, 数据传输任务周期性调用宏定义 UIP\_APPCALL 处理事件的发生。uIP 系统底层与应用层之间的关系如图 5 所示。

若要以 TCP 方式实现数据传输,首先要通过调用 uIP 协议栈提供的 struct uip\_conn \* uip\_connect(uip\_ipaddr\_t \* ripaddr, u16\_t port) 函数与监控中心建立 TCP 连接,由协议栈的 void uip\_process(u8\_t flag) 完成

TCP 连接的 3 次握手。建立了 TCP 连接,数据便可以以 TCP 方式传输至监控中心。

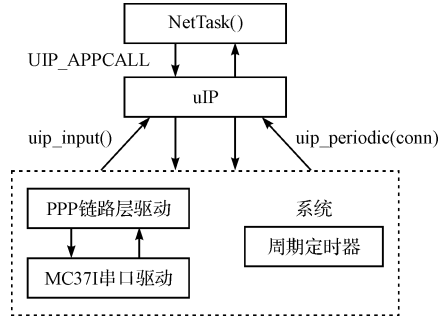


图 5 基于 uIP 实现 TCP 的软件结构

### 3 结束语

本研究在硬件设计上采用了低配置的单片机 STC12C5A56S2,既完成了 TCP/IP 协议栈 uIP 的移植,又节约了成本。整个程序约占 14 KB 的 ROM 和 400 Bytes 的 RAM,数据上传速率可以达到 19 kbps,满足了应用要求。能够利用该数传终端 GPRS 网络实现与 Internet 的连接,能够将数据采集设备采集到的污染数据实时传送至远程监控中心,可方便地应用于实践中。

### 参考文献(References):

- [1] CHAN Shun-yu, TENG Jen-hao. Multi-functional power quality monitoring and report-back system [J]. Elsevier, Electrical Power and Energy Systems, 2010, 32(6): 728-735.
- [2] 苑文举,赵孔新. 基于 GPRS 的汽车防盗无线远程报警器 [J]. 长春工业大学学报:自然科学版, 2008, 29(4): 391-394.
- [3] 汪发锋,陶维新. 基于 MC391 的电能管理终端远程 GPRS 接口设计 [J]. 合肥工业大学学报:自然科学版, 2009, 32(1): 24-27.
- [4] 刘扬. GPRS 通信技术在智能运输系统中的应用研究 [D]. 河北:燕山大学电气工程学院, 2007.
- [5] 张建霞,马南琦. 西门子 MC391 在船舶智能火灾报警系统中的应用 [J]. 船海工程, 2007, 36(3): 119-121.
- [6] 张昕,韩基荣. 基于 GPRS 的油井远程监控系统的设计 [J]. 佳木斯大学学报:自然科学版, 2009, 27(1): 10-12.
- [7] 滕志军,王晨臣. 基于 MC391 的电力设备远程监控系统研究 [J]. 东北电力大学学报, 2009, 29(6): 81-84.
- [8] FOROUZAN B A, FEGAN S C. TCP/IP 协议族 [M]. 谢希仁,译. 北京:清华大学出版社, 2006.
- [9] 陈小鹏. GPRS 在 LED 显示系统上的应用 [D]. 上海:上海海运学院电气自动化系, 2004.
- [10] GU Qing-hua, LU Cai-wu. Dynamic management system of ore blending in an open pit mine based on GIS/GPS/GPRS [J]. Elsevier, Mining Science and Technology, 2010, 20(1): 132-137.