论文题目：基于GPRS的数据集中器设计

专　　业：微电子与固体电子学

硕 士 生：　　（签　名）_____

指导教师：　　（签　名）_____

摘　要

目前远程电力抄表系统成为电力部门管理、分析和处理各种电量数据的一种重要选择措施。随着人民生活水平的提高和国民经济、房地产产业的迅速发展，居民住宅的质量和档次越来越高，住户对住宅环境、物业管理水平和数字信息化水平的要求也日益提高。对供水、供电、供气部门和用户来说，传统的人工抄表方式已经远不能满足当今社会需求。这种落后的方式，消耗大量的人力、物力，给居民和供应部门带来极大的不便，因此国内很多城镇逐步出现了以计算机为基础的自动抄表系统来取代传统的人工抄表。

自动抄表系统集电子、计算机、通信、自动控制及计量技术于一体，具有抄表速度快、计算精度高、抄收方便等突出的优点。基于综合考虑，本文提出了一种无线抄表系统即基于GPRS无线智能抄表系统，本文研究的是基于GPRS无线智能抄表系统中的集中器部分。

智能抄表系统由电表、集中器和后台管理三个部分构成，其中集中器工作流程为：接受主站的控制指令，然后将电表数据保存并上传至主站后台管理系统。课题研究的目标：利用嵌入式技术，针对远程抄表系统控制要求，深入研究集中器的软硬件设计思想，为实际系统的开发提供较为全面的理论和技术支持。

回顾GPRS技术发展和最新进展，并根据集中器的功能要求，结合国内外相关技术的发展现状，提出了基于GPRS无线技术的集中器的设计方案和实现方法。在硬件上包括CPU、存储单元、电力线载波通讯、GPRS通讯、串口通讯和电源管理单元六个功能部分。利用流行的嵌入式技术，采用AMR7单片机，搭载外围扩展部件，构建硬件系统，并对系统进行相关模件的调试。使系统基本达到集中器的硬件平台的要求。在软件上，通过进行软件程序的编写，实现了两个基本功能模块：集中器与电表的通信和控制模块、后台与集中器的通信以及控制模块的软件系统的设计。充分考虑实际使用中的各种异常处理方法，保证集中器准确可靠地运行。通过本课题的研究，基本满足了集中器的功能要求和指标性能要求，并在系统选型、软件实现等环节，进行较为系统的研究，为实际装置的设计提供重要的参考依据。

关键词 ： GPRS技术 集中器 通讯协议 主站

研究类型：应用研究

Subject : GPRS-based Data Concentrator Design

Speciality : Microelectronics and Solid state electronics

Name :Chen Xin (Signature)_____

Instructor : Sun Longjie (Signature)_____

ABSTRACT

At present the remote electric power meter reading system a power department management, analysis and processing all kinds of quantity of electricity data is a kind of important choice measures. With the improvement of people's living standard and national economy, the rapid development of real estate industry, residential the quality and grade of the more and more high, residents of residential environment, property management level and digital informatization level requirement also is increasing day by day. On the water supply, the power supply, gas supply departments and users, the traditional artificial meter reading way already far cannot satisfy the needs of society. This kind of way behind, use a lot of manpower and material resources to residents and supply authorities inconvenient, so many domestic town gradually appeared to the computer for the foundation to be automatic meter reading system to replace the traditional artificial meter reading.

Automatic meter reading system set electronic, computer, communication, automatic control and measuring technology in a body, has the meter reading speed, high precision, copy is convenient wait for a outstanding qualities. Based on the comprehensive consideration, this paper puts forward a wireless meter reading system is based on GPRS wireless intelligent meter reading system, this paper is based on GPRS wireless intelligent meter reading system of concentration in the device.

Intelligent meter reading system electric meter, concentration, and by management background three components, including concentrators, workflow to: accept the Lord control instruction, and then will electric meter data save and upload to host background management system. Subject research goal: the use of embedded technology, in view of long-distance meter reading system control requirements, the in-depth study of the concentration of the software and hardware design thinking, and to the development of practical system provides a comprehensive theory and technical support.

Review of the technical development and the latest progress of the GPRS, and according

to the concentration of function requirement, combined with the domestic and foreign relevant technology development present situation, proposed based on GPRS wireless technology is the focus of the design and realization method. In the hardware including CPU, storage unit, power lines carrier communication, GPRS communication, serial communication and power management unit six functional parts. Using popular embedded technology, using AMR7 microcontroller, carrying peripheral expansion parts, construction hardware system, and the system related module commissioning. The system is to focus on the basic requirements of the hardware platform. In software, through a software program compiling, and realize the two basic function module: focus on sensor and meter communication and control module, the background and concentrators, communication and control module of the design of the software system. Full consideration of the actual use of various exception handling method, ensure the accurate on reliably. Through this topic research, satisfy basically concentrators, the function requirement and index performance requirements, and in the system selection, software to realize such links, the systematic research for the actual device design provides important reference.

Key words: GPRS technologies The concentration of a single-chip microcomputer Communication protocol Host

Thesis ： Application Research

目 录

1 绪论

1.1 选题的背景及研究的意义

科技的发展动力及重要目标之一就是给人们的生活带来便利。随着信息技术的飞速发展，家具设施、工业控制的智能化、自动化水平越来越高，将各种信息数据用无线进行传输及采集已经成为人们追求的目标。传统的有线数据传输方式、繁琐的布线规则严重制约了其工作效率和应用范围。在信息化和自动化迅猛发展的今天，无线传感网络，在各行各业都有着广泛的应用，尤其是工业测量、控制方面，各种需要集中传感与控制的现场对于无线传感网络表现出了极大的需求。

以GSM、CDMA为主的数字蜂窝移动通信和以Internet为主的分组数据通信是目前信息领域增长最为迅猛的两大产业，正呈现出相互融合的趋势。GPRS可以看作是移动通信和分组数据通信融合的第一步。移动通信在目前的话音业务继续保持发展的同时，对IP和高速数据业务的支持已经成为第二代移动通信系统演进的方向，而且也将成为第三代移动通信系统的主要业务特征。GPRS包含丰富的数据业务，如：PTP（Point To Point，点对点）数据业务，PTM-M（Point To Multipoint，点对多点）广播数据业务、PTM-G（Point To Multipoint－Group，点对多点群呼）数据业务、IP-M广播业务。这些业务已具有了一定的调度功能，再加上GSM phase II+中定义的话音广播及话音组呼业务，GPRS已经能够完成一些调度功能。GPRS主要的应用领域可以是：E-mail电子邮件、WWW浏览、WAP业务、电子商务、信息查询、远程监控等[1]。

数据远程通讯技术是实现远程传输系统可靠运行的关键，常用的数据远程传输方式多依靠电台、数传机等无线通讯方式实现，这些方式不仅容易受到外界干扰，在使用过程中经常出现数据传输速度较慢、易丢失、准确性不高等问题，而且若系统所处位置地势较为起伏，也会较大程度的影响通讯效果。在监测点分散广、外界干扰大、数据实时性要求高的情况下，上述的远程传输方式不是最佳选择。GPRS无线数据传输方式的出现为数据远程传输带来了新的技术革命，它是目前通信体系中最成熟、最完善、覆盖面积最广的GSM系统上发展出来的一种数据承载业务。GPRS允许用户在端到端分组转移模式下发送和接收数据，而不需要利用电路交换模式的网络资源，从而提供了一种高效、低成本的分组数据业务。特别适合用于简短的、突发性的、频繁的、少量的数据传输，也适合于偶尔的数据量传输。具有实时在线、按量计费、高速传输等优点。

基于GPRS的监控系统终端常用两种方法实现：一种是个监测点采用Modem分别与监控中心通信；另一种是设计专门的集中器，通过RS-232总线、电力载波等通信方式采集各监测点数据，由集中器通过Modem与控制中心通信。第一种方法虽然在数据传输的

实时性和稳定性上略高于第二种方法，但是系统造价高，维护工作也较繁重。考虑到系统的成本、实现方式、实时性等因素，本文提供一种使用GPRS方式和RS-232总线通讯方式组合的集中器设计方案。该方案成本低，通用性强，具有一定的应用前景[2]。

1.2 本课题研究领域国内外的研究动态及发展趋势

目前全世界已有近百个运营商开通了GPRS商用系统、试商用系统或实验系统。较为著名的有英国的BTCELLNET、德国的T-MOBILE、中国香港的SMARTONE、中国台湾的TSL以及法国、西班牙、葡萄牙、芬兰、捷克、丹麦、比利时、意大利、俄罗斯、澳大利亚、新加坡、菲律宾等国家和地区的运营商。可以说，GPRS已经被所有GPRS运营商所关注，亟待投入商业运行。

国内动作比国外要平缓，但是也取得了相应的进展。2002年南京的GPRS网络已在试运行中；2002年5月初，北京移动也在该地区开通了GPRS网络；中国移动2001年7月9日也已开始了酝酿已久的GPRS业务，在全国16个省（市）的25个城市投入试商用。 尴尬也好、争议也好、炒作也好、实战也好，总之GPRS仍旧在沿着轨迹前进着。

我国GPRS行业发展速度较快，受益于GPRS行业生产技术不断提高以及下游需求市场不断扩大，GPRS行业在国内和国际市场上发展形势都十分看好。虽然受金融危机影响使得GPRS行业近两年发展速度略有减缓，但随着我国国民经济的快速发展以及国际金融危机的逐渐消退，我国GPRS行业重新迎来良好的发展机遇。进入2010年我国GPRS行业面临新的发展形势，由于新进入企业不断增多，上游原材料价格持续上涨，导致行业利润降低，因此我国GPRS 行业市场竞争也日趋激烈。面对这一现状，GPRS行业内企业要积极应对，注重培养创新能力，不断提高自身生产技术，加强企业竞争优势，于此同时GPRS 行业内企业还应全面把握该行业的市场运行态势，不断学习该行业最新生产技术，了解该行业国家政策法规走向，掌握同行业竞争对手的发展动态，只有如此才能使企业充分了解该行业的发展动态及自身在行业中所处地位，并制定正确的发展策略以使企业在残酷的市场竞争中取得领先优势[3]。

GSM是当前全球使用最为广泛的移动电话系统。目前以GSM为基础的GPRS作为向第三代移动电话系统发展过程中的一个至关重要何必不可少的一步，已成为迈向第三代移动通信部署的基石，并开启了无线数据市场的大门。事实上，传统的话音服务和其带来的利润增长现在已经出现了停滞不前。而以GPRS为基础的通信增值业务，包括手机上网、E-mail等Internet业务等正在急速上升。

GPRS已经为运营商提供了开辟全新市场的能力。通过部署GPRS网络，运营商可以开辟新兴市场以及增加收入来源。分组交换使它能够有效地使用现有的网络容量。GPRS技术将支持开展创新服务，以便吸引新的客户，从而提高客户的忠诚度并降低处理成本。由于GPRS网络使用的是现有的GSM网络，所以其可以一举在全国范围内推出。这样，

运营商将会拥有一个新的机会，使其在新型服务合作伙伴关心的基础上与互联网服务提供商或信息提供商合作。新的市场带来的另一个新商机就是GPRS将会有新终端，这无疑为终端设备制造商提供了一个新的市场增长点。

目前将GPRS无线传输技术应用于工业远程监控系统的数据传输是当前比较热门的研究课题。采用GPRS-Internet通信网络，使工业远程监控系统的监控空间延伸到了公用通信网络和Internet，在保证系统实时性、可靠性的同时又降低了系统的开发成本以及运营费用。GPRS技术在国内外已广泛的应用于电力、交通、医疗、勘探、供热暖等领域的工业远程监控系统中[4]。

1.3 研究内容

1.3.1 研究的主要内容

远程电力抄表系统由电表、集中器和主站管理系统三个部分构成。集中器通常安装在用户配电变压器出线侧，负责管理多个电表，并与之进行通信，获得电表读数和传送控制电表电源的指令，同时与主站中心通信，向主站中心传送用户电表读数，接收主站控制中心对用户电表下达的指令，起承上启下的作用。针对已有的具体目标，这次系统建设的主要内容就是：集中器的设计，然后将采集到信息传送到集中器，再由各集中器上传数据到主站管理系统。

1.3.2 集中器的研究方案及准备采取的技术路线

集中器除了接收电表传来的信息外，还要将接收的信息通过某种方式传送给主站管理系统，以便分析计算和决策使用。由于电网分布的广泛性，用户配电变压器安装位置往往远离电力管理和调度中心，也就是说：集中器远离电力管理中心。因此，集中器与电力管理中心的通信方式也必须加以研究，以解决集中器与管理系统的远距离通信问题，尽可能减小运营成本。

基于 GPRS 技术的通用数据集中器主站的上行通信方式采用 GPRS 无线网络实现数据的远程传输，集中器的下行通信方式采用低压电力线载波实现数据的读取。其实现方法是在集中器与主站的上行通信段、数据采集终端、中继器中集成 GPRS 通信模块，并在各无线设备中集成近距离 GPRS 通信协议，使这些设备以集中器为网络中心，构建近距离无线通信自组网络如图 1.1 所示：

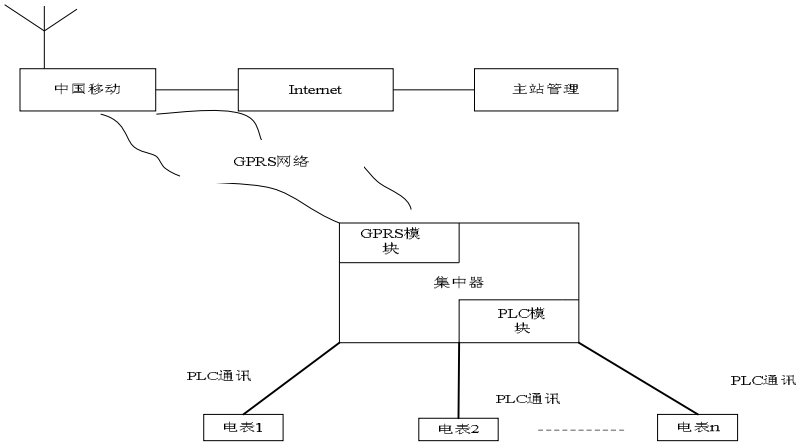


图 1.1 集中器系统结构示意图

集中器系统主要是由采集器（数据采集模块和采集终端）、集中器、主站（数据处理中心）以及将这些设备连接起来的高效、可靠的数据传输通信方式组成的系统。

数据传输系统是指由主站通过传输媒介 GPRS 网络将各个终端的信息进行传输，通过这种方式实现系统主站和集中器之间的数据通讯，具有远程传输和监控等功能。一个系统，其总体设计往往包含有多方面，并且各方面的连接有不同的组合方案。在总体设计上，以软硬件结合设计为主线，软硬件结合仿真调试为辅线，主要分为硬件架构和软件架构。

1.3.3 拟解决的关键问题

本课题拟解决以下问题：集中器的设计(软件硬件的设计)、集中器和主站之间的通信以及数据的传输，集中器与电表之间数据采集和传输。

1.3.4 研究目标

本课题研究的目标：利用GPRS技术，针对远程抄表系统控制要求，深入研究集中器控制装置的软硬件设计思想，为实际系统的开发提供较为全面的理论和技术支持，最终完成集中器与主站之间的数据传输，集中器与电表之间数据的采集。

2 GPRS 技术

2.1 GPRS 简介

GPRS---(General Packet Radio Service)，即通用分组无线业务的简称，是欧洲电信协会GSM系统中有关分组数据所规定的标准。GPRS具有充分利用现有的网络、资源利用率高、始终在线、传输速率高、资费合理等特点。目前世界上有大约10亿普通电话用户，3亿无线通信用户和1亿互联网用户。世界电信业的发展趋势将会是无线语音业务的发展速度超过普通电话业务，两者也在不断融合。未来的网络将是一个有线、无线和互联网三者合一的数字化全球网络，其覆盖将超越一切地理障碍，使信息无处不在。2005年大约就有10亿无线互联网用户，中国的互联网用户数在2003年就有6千万。GPRS是目前解决移动通信信息服务的一种较完善的业务[5] 。

与GSM CSD业务不同的是，GPRS业务将以数据流量计费，而GSM CSD业务则以时间计费，GPRS这一计费方式更适应数据通信的特点。此外，GPRS业务的速度较GSM CSD业务也有很大提高，GPRS可提供高达115Kbit/s的传输速率(最高值为171.2Kbit/s)，下一代GPRS业务的速度将可以达到384Kbit/s。

GPRS一个较大的优势是能够充分利用现有的GSM网络，可以使运营商在全国范围内推出此项业务。相信在数年内，通过便携式电脑，GPRS用户将能以与ISDN用户一样快的速度上网浏览，同时也使一些对传输速率敏感的移动多媒体应用成为可能。

GPRS用户只有在发送或接收数据期间才占用资源，意味着多个用户可高效率地共享同一无线信道，从而提高资源的利用率。同时，用户只需按数据通信量付费，而无需对整个链路占用期间付费。实际上，GPRS用户可能连接的时间长达数小时，却只需支付相对较少的连接费用，可使用户的使用费用大大降低。GPRS通信模块就是为使用GPRS服务而开发的无线通信终端设备。可应用到下列系统集成中：远程数据监测系统、远程控制系统、自动售货系统、无线定位系统、门禁保安系统、物流管理系统等。

2.2 GPRS 技术

2.2.1 GPRS 网络单元

GPRS系统通过在原有的GSM系统中引入分组数据单元来提供无线系统上的数据业务。作为承载网络，GPRS系统本身采用IP网络结构，并对用户分配独立地址，将用户作为独立的数据用户，从而实现了从网络到移动用户端到端的数据应用。

为了实现数据承载，GPRS系统引入了几种新的网络单元，如PCU，SGSN，GGSN，

以及其他辅助进行数据业务管理和应用的单元，如DNS和DHCP服务器、网络时间协议（NTP）、计费网关（CG）等。只有通过对各功能单元特性的了解以及协议结构的认识，才可能为进一步的系统维护和优化打好基础。

典型的GPRS网络结构如图2.1所示。

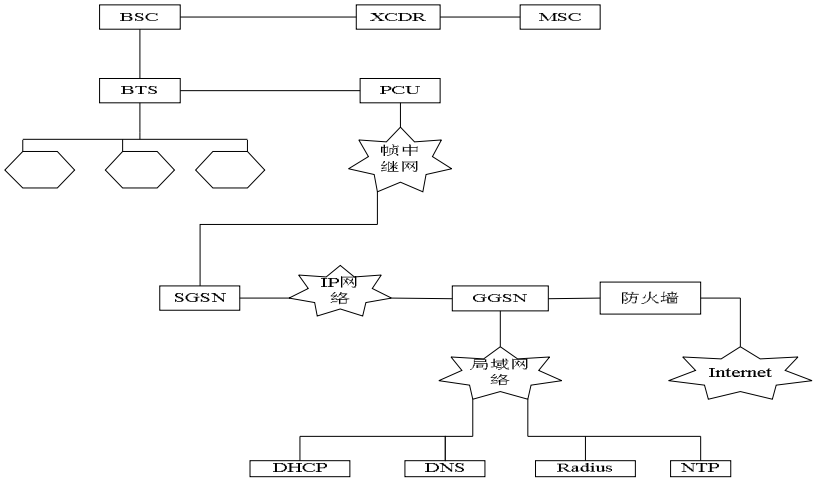


图 2.1 GPRS 系统网络结构

GSM 系统是我们通常所说的基于时分交换的无线移动系统中的第二代系统，它以提供话音业务为主；GPRS 系统作为移动 2.5G 系统，则主要用于提供低速数据业务；目前处于试验和测试阶段的第三代系统（如 WCDMA）则主要用于提供高速数据业务。GPRS 系统在向第三代移动通信系统演进的过程中至关重要，因为第三代系统可以充分利用 GPRS 网络的核心网络系统，如 SGSN，GGSN，DNS，Radius，NTP 等网络技术和设备以及计费系统。另外，运营商可以充分利用在 GPRS 网络运营基础上积累的运营维护经验、业务种类和客户群，尽快达到收益最大化的效果。由此可见，了解 GPRS 网络和技术不仅仅有利于目前的工作，更能够为个人进一步的技术进步打好基础。

(1)GPRS 网络单元功能

简单来讲，GPRS 系统中新引入的网络单元可区分为无线部分和数据部分两大类。其中 PCU 属于无线管理部分，SGSN 属于无线管理和数据管理公用部分，GGSN 则完全属于数据管理部分。其他一些辅助单元虽然在 GPRS 系统中未给出定义，但在数据网络中必不可少，因而也是 GPRS 网络的一部分，如域名解析服务器（DNS）、动态地址分配服务器（DHCP）、网络时间协议（NTP）服务器、认证与鉴权服务器 Radius 等。

(2)PCU

PCU 是分组数据处理单元，它与 BSC 协同作用，提供无线数据的处理功能，如逻辑链路与物理链路的映射、数据包的拆封、数据包的确认、无线数据信道的分配等。PCU 可作为模块单元插入 BSC 中，或者作为独立于 BSC 的单元存在，它与 BSC 之间的接口方式规范未给出定义。

PCU 与 SGSN 之间 Gb 接口采用帧中继协议。PCU 具有 Gb 接口管理的功能。

(3) SGSN

SGSN 即 GPRS 服务支持节点，它通过 Gb 接口提供与无线分组控制器 PCU 的连接，进行移动数据的管理，如身份识别、加密、压缩等；通过 Gr 接口与 HLR 项链，进行用户数据库的访问及接入控制；通过 Gn 接口与 GGSN 相连，提供 IP 数据包到无线单元的传输通路和协议变换等功能；SGSN 还可以提供与 MSC 的 Gs 接口连接，以及 SMSC 的 Gd 接口连接，用以支持数据业务和电路业务的协同工作和短信收发等。

(4) GGSN

GGSN 负责 GPRS 网络与外部数据网的连接，提供 GPRS 与外部数据网之间的传输通路，进行移动用户与外部数据网之间的数据传送。

GGSN 与 SGSN 之间的接口为 Gn 接口，采用 GTP 协议类型；GGSN 与外部数据网之间的接口为 Gi 接口，采用 IP 协议类型。

对于网络发起的数据单元传送业务，GGSN 需要通过 Gc 接口到 HLR 查询用户相关信息；对于计费信息的传送工作，GGSN 通过 Ga 接口完成[6]。

2.2.2 GPRS 网元之间相互作用

GPRS 系统中各个网元相互作用，完成协议处理和呼叫处理等功能。只有了解了网元之间的相互关系，才能对系统有一个完整的认识，从而更好地了解 GPRS 协议栈和进行系统故障分析。

在 GPRS 系统中，最常用也是最基本的系统功能包括用户附着和激活 PDP 上下文。移动用户在进行数据传送时，首先需要进行网络附着，即进行位置和身份登记，然后通过 PDP 激活请求信息申请网络接入，系统根据接入申请信息中的 APN 信息进行处理，如通过 DHCP 服务器进行用户地址分配及通过 Radius 服务器进行用户身份认证等，最终使合法用户得到 IP 地址。作为数据用户，用户在进行数据传送与接收时拥有独立的 IP 地址，是一个真正意义上的 IP 或数据用户。得到 IP 地址后，用户可以建立数据连接，进行数据收发。

在用户附着过程中，主要涉及无线系统，如 PCU，SGSN，MSC 和 HLR 等业务单元，与数据单元（如 GGSN 等）无关；在激活 PDP 上下文过程中，涉及数据单元与无线单元的配合，如 PCU，SGSN，GGSN，DNS 服务器，DHCP 服务器，Radius 服务器等之间的配合。各个单元的相互配合和作用是完成系统功能的基础。

(1)移动用户附着过程

移动台（MS）通过附着过程登录到 GPRS 网络从而能够进行位置区的更新，以及发起数据传送和接收过程，其附着过程如图所示。MS 在附着过程中，通过 PCU 进行接入控制和信道分配，通过 SGSN 和 HLR 进行鉴权管理，并从 HLR 中获得用户签约信息，

最终在 MS，HLR 与 SGSN 内部形成有关用户的移动管理信息（MM Context）,如图 2.2 所示：

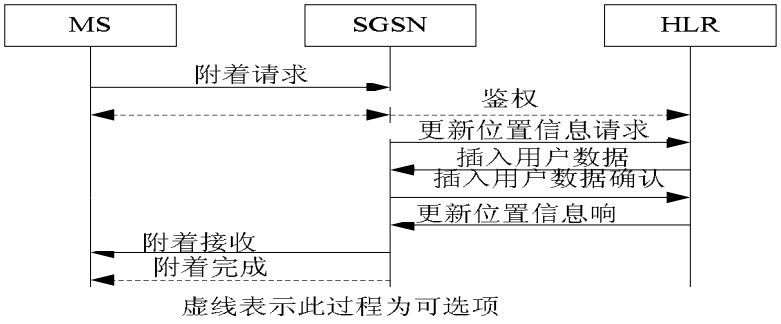


图 2.2 GPRS 系统用户附着过程示意图

MS 在未进行附着之前脱离 GPRS 网络，处于空闲（idle）状态，不能进行任何数据业务操作。附着之后用户得到临时身份识别号 TLLI，并在 MS 与 SGSN 之间建立起逻辑链路，变为就绪（ready）状态，可以进行 PDP 上下文激活过程，进行 IP 地址的申请。

(2)移动用户激活 PDP 过程

PDP 指分组数据规程,PDP 上下文包含与某个接入网络（APN）相关的地址映射及路由信息。移动用户通过激活 PDP 上下文得到动态地址并可随时通过 GGSN 接入特定数据网络[12]。

PDP 上下文激活过程如下图所示，MS 发送 PDP 上下文激活请求信息到 SGSN，SGSN 根据 APN（接入点名称，它与特定的业务类型和企业网相关）判断可接入性，并通过 DNS 得到相应的 GGSN 地址，再通过 Gn 接口转发 PDP 激活请求信息到 GGSN，由 GGSN 控制进行动态地址分配和接入认证过程。如果 APN 接入允许，MS 将得到 IP 地址，并在 MS 与相应的 SGSN 和 GGSN 中形成 MS 的相关 PDP 上下文信息。

对于激活 PDP 上下文过程中各网元的详细作用如图 2.3 所示：

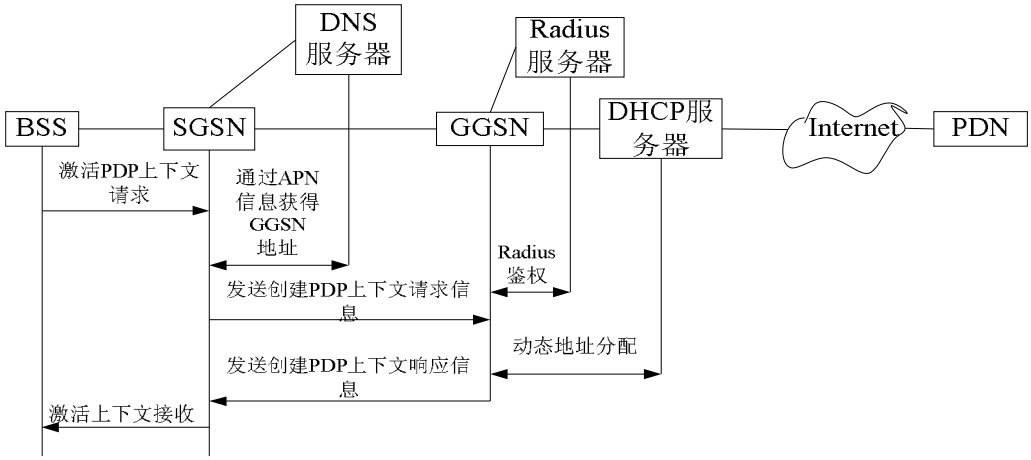


图 2.3 GPRS 系统激活 PDP 过程示意图

2.3 GPRS 协议规程

2.3.1 GPRS 协议规程概述

GPRS 协议规程体现了无线和网络相结合的特征。其中既包含类似局域网技术中的逻辑链路控制（LLC）子层和媒体接入控制（MAC）子层，又包含 RLC 和 BBSGP 等新引入的特定规程。各种网络单元所包含的协议层次有所不同，如 PCU 中规程体系与无线介入相关；GGSN 中规程体系与数据应用相关；SGSN 规程体系则涉及两个方面，它既要连接 PCU 进行无线系统和用户管理，又要连接 GGSN 进行数据单元的传送。SGSN 与 PCU 侧的 Gb 接口上采用帧中继规程，与 GGSN 侧的 Gn 接口上则采用 TCP/IP 规程。SGSN 中协议低层部分（如 NS 和 BSSGP 层）与无线管理相关，高层部分（如 LLC 和 SNDCP 层）则与数据管理相关。

GPRS 协议规程结构具体表述如图 2.4 所示：

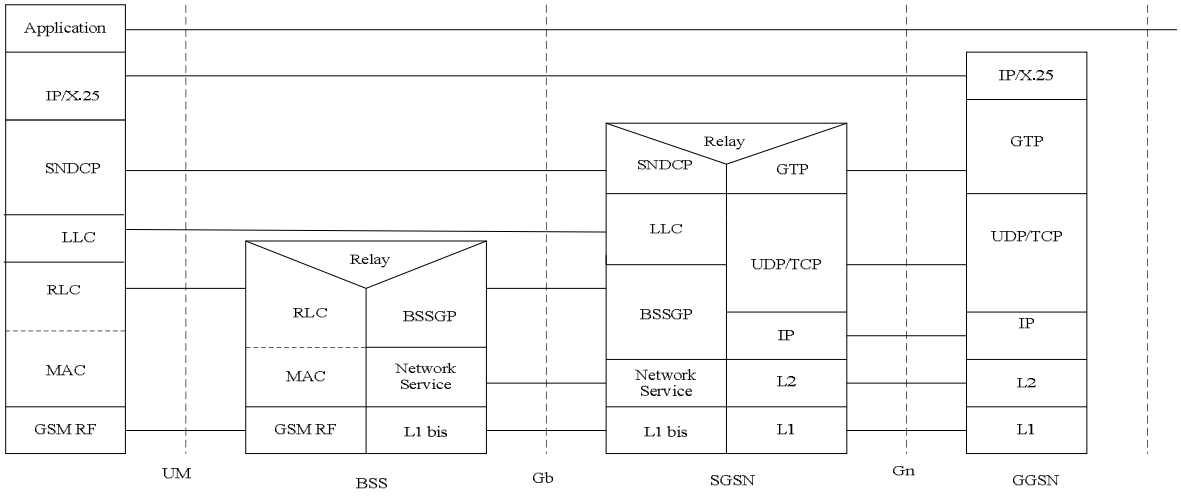


图 2.4 GPRS 规程结构

由 GPRS 系统端到端的应用协议结构可知，GPRS 网络是存在于应用层之下的承载网络，它用以承载 IP 或 X.25 等数据业务。由于 GPRS 本身采用 IP 数据网络结构，所以基于 GPRS 网络的 IP 应用规程结构可理解为两层 IP 结构，即应用级的 IP 协议及采用 IP 协议的 GPRS 系统本身。

GPRS 系统中，GPRS 隧道规程（GTP）协议用以进行 Gn 接口上的数据封装；子网汇聚（SNDC 盘）层用以实现不同协议种类的接入功能，进行数据报中数据和控制部分的压缩、封装；逻辑链路控制（LLC）层可以提供 MS 与 SGSN 之间稳定的逻辑链路，并通过确认机制保证数据的可靠传送；无线链路控制（RLC）层将 LLC 数据包变为 RLC 数据包，以进行无线接口上的传送，并采用 ARQ 机制予以传送确认；媒体接入控制（MAC）层执行接入控制功能，提供多个 MS 共享同一物理信道的控制机制；无线层提

供无线信道用以进行 MS 与 PCU 之间信息的传送。

通过到某个 MS 的下行数据流的传送过程，可以大致了解到每个协议层的具体作用。

如果 GGSN 接收到一个需要传送到某个 MS 的 IP/X.25 数据包，则它需要将数据传送到 MS 所在位置区的 SGSN 中去。假设此时 MS 已激活 PDP，即 MS 已经在 SGSN，GGSN 及 MS 中形成 PDP Context，则 GGSN 保存 MS 的位置区、IP 地址、相应 SGSN/GGSN 地址等信息，GGSN 由此可得知 MS 所在的 SGSN，并进一步将数据进行 GTP 封装后传送至 SGSN。

GTP 封装是将数据包头部添加 GTP 包头，以便区分不同 MS 或同一 MS 的不用网络接入进程，其包头格式为 TID=IMSI+NSAPI，IMSI 用于区分某个移动用户，NSAPI（网络接入点）则用以区分同一用户的不同 PDP 进程。

数据在 SGSN 与 GGSN 之间经由 Gn 接口上的 IP 网络进行传送。

GTP 数据单元进入 SGSN 后，SGSN 拆除 GTP 包头，将数据包送入 SNDCP 层，通过 SNDCP 层的协议 组合和压缩封装，以及 LLC 层的数据包切割之后，形成标准的 LLC 包。LLC 层还进行逻辑链路管理，它对 MS 分配临时身份识别号 TLLI，并采用不同服务质量的信道（用 SAPI 表示）进行 LLC 帧的传送。TLLI 和 SAPI 共同表示 LLC 层与特定 MS 之间的独立逻辑链路。

BSSGP 层提供 PCU 和小区管理功能，以及 SGSN 与 PCU 之间 Gb 接口的管理功能，如 Gb 链路之间的负荷分担等。NS 层用以在帧中继网络基础上提供逻辑虚连接，以保证 Gb 接口信息的正确传送。LLC 数据包在 SGSN 中经由 NS 层提供的 PVC 在 BSSGP 的控制下传送至正确 PCU 中的特定小区。

2.3.2 GPRS 功能单元与接口

GPRS 功能单元与接口如图 2.5 所示：

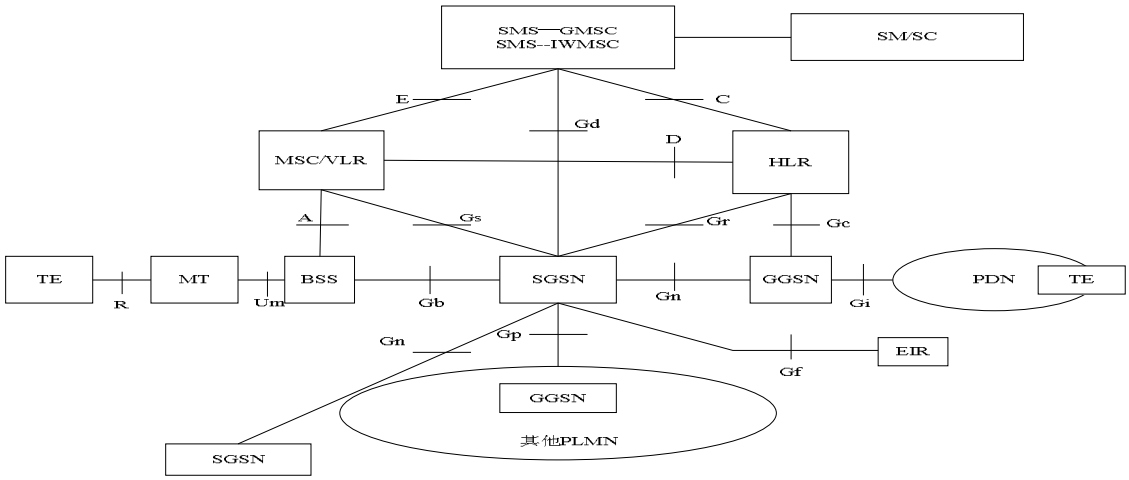


图 2.5 GPRS 功能单元与接口

GPRS 系统中 SGSN 系统包括 SNDCP，LLC，BSSGP，NS 以及 GTP 协议层，并提供 Gn 和 Gb 接口；GGSN 包括 GTP 协议及 IP 协议结构，并提供 Gn 和 Gi 接口；PCU 包括 BSSGP，NS，RLC，MAC 以及无线信道协议规程，并提供 Um 和 Gb 接口；MS 则包括 RLC，MAC，LLC，SNDCP 以及应用层功能。

SGSN 进行用户数据管理、安全性管理、位置管理以及接入控制等。

SGSN 通过 Gn 接口提供与网关服务节点 GGSN 的连接，进行数据包与外部网络的传送或路由区的更新；通过 Gr 接口提供与 HLR 的连接，提供用户数据的存取和鉴权管理；通过 Gs 接口提供与 MSC 的连接，进行话音与数据业务的协同工作。

(1)SGSN

SGSN 控制建立和管理附着用户的相关信息数据库，以及就绪 Ready 状态下用户的相关 PDP 信息。

在无线侧 SGSN 与 PCU 连接，进行 PCU 和小区管理，通过 Gb 接口上的逻辑信道采用虚电路进行到 MS 的分组数据传送，并提供数据流的流量控制。

在用户附着阶段，SGSN 通过 Gr 接口与 HLR 建立信令连接，提取用户信息，参与鉴权与加密过程，并存储用户相关数据，形成用户数据库；在用户激活 PDP 阶段，SGSN 负责进行用户 APN 的选择和控制，并通过与 DNS 的协同工作得到 APN 所属 GGSN 的地址，然后在与相关 GGSN 进行 QoS 协商的基础上建立连接，获得用户动态地址，从而形成用户的 PDP 相关数据；在用户就绪状态，SGSN 控制路由区的更新；在数据传送过程中，SGSN 负责数据包的压缩、封装、分组重组，以及相关逻辑链路的建立、释放和负荷分担工作。

在 Gs 接口存在的情况下，SGSN 将负责与 MSC 的寻呼控制协调和处理，执行经由 SGSN 本身的 LA/RA 联合更新、IMSI 附着/去附着等功能。

SGSN 还完成相关的 S-CDR 与 M-CDR 等计费信息的收集和传送。

(2)GGSN

GGSN 根据 APN 信息进行 GPRS 系统到外部网络的连接和路由选择，并配合 DHCP 服务器完成用户动态地址分配。GGSN 还进行 Gn 接口和 Gi 接口管理，完成外部数据包的传送工作。

GGSN 在激活 PDP 上下文阶段，根据用户所需接入的网络信息（APN）从 DHCP 服务器获得动态用户地址，并配合 SGSN 在 MS/SGSN/GGSN 中形成用户的 PDP 数据，其中包括 IMSI，NSAPI,APN,IP 地址，以及相关的 SGSN/GGSN 地址等，从而保证后续数据传送过程的顺利进行。

在下行数据传送阶段，GGSN 进行数据包的包头封装，并根据 PDP 相关数据或通过 HLR 获得的 MS 所在 SGSN 的地址，将数据经 Gn 接口的 GTP 隧道协议传送至 SGSN；对于上行数据的传送，GGSN 去 GTP 封装并将数据经 Gi 接口路由至相应的服务器或地

址。

GGSN 还提供相关的 G-CDR 计费信息的收集和传送工作。

(3)PCU

PCU 负责无线信道的管理与分配及无线信道到逻辑信道的映射，它控制多个 MS 共享同一无线信道或一个 MS 使用多个无线信道进行接入，并进行多个用户之间的碰撞控制；PCU 可以根据无线环境决定不同编码方式的使用与转换，并提供 RLC 层数据传送的确认；它还用以进行小区 GPRS 功能管理，执行小区与 MS 数据流量控制等。

(4)Gb 接口

Gb 链路提供 BSS 与 SGSN 之间的连接，传送小区管理和路由区切换信息，并进行 MS 与 SGSN 之间的数据传送。Gb 接口规程结构如图 2.6 所示：

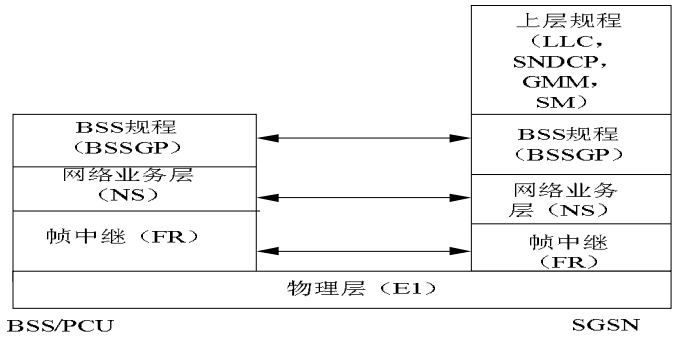


图 2.6 Gb 接口规程结构

(5)Gr 接口

Gr 接口指 GPRS 系统中 SGSN 与 HLR 之间的接口，用于传送 MS 的加密信息、鉴权信息和用户数据库信息等如图 2.7 所示。

(6)Gn/Gp 接口

如图所示，Gn 是同一个 PLMN 内部 GSN 之间的接口，Gp 是不同 PLMN 中 GSN 之间的接口，Gn 与 Gp 接口都采用基于 IP 的 GTP 协议规程，提供协议规程数据包在 GSN 节点间通过 GTP 隧道协议传送的机制。Gn 接口一般支持域内静态或动态路由协议，而 Gp 接口由于经由 PLMN 之间路由传送，所以它须支持域间路由协议。GTP 规程仅在 SGSN 与 GGSN 之间实现，其他系统单元不涉及 GTP 规程的处理，如图 2.8 所示。

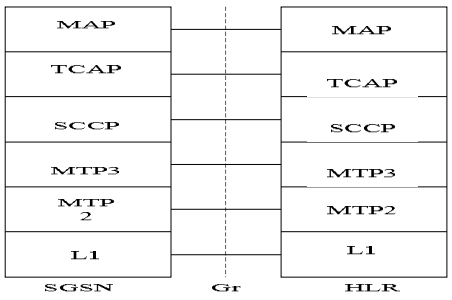


图 2.7 Gr 接口规程栈

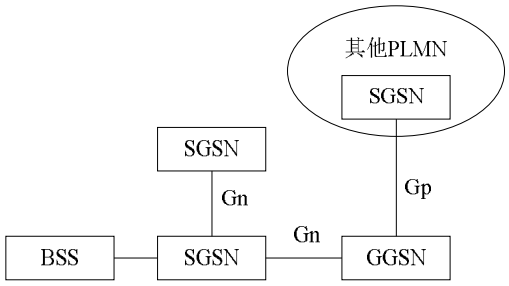


图 2.8 Gn 与 Gp 接口

(7)Gi 接口

Gi 接口是 GPRS 网络与外部数据网络的接口点，它可以采用 X.25 协议、X.75 协议或 IP 协议等接口方式，其中与 IP 接口方式餐见图 2.9。在 IP 网络中，子网的连接一般通过路由器进行。因此，外部 IP 网认为 GGSN 就是一台路由器，它们之间根据客户需要考虑采用何种 IP 路由协议如图 2.9 所示。

另外，根据协议和 IP 网络的基本要求，可由运营商在 Gi 接口上配置防火墙，进行数据和网络安全性管理；配置域名服务器进行域名解析；配置动态地址服务器进行 MS 地址的分配；配置 Radius 服务器进行用户接入鉴权等。

(8)Gs 接口

Gs 接口为 SGSN 与 MSC 之间的接口，如图 2.10 所示。在 Gs 接口存在的情况下，MS 可通过 SGSN 进行 IMSI/GPRS 联合附着和 LA/RA 联合更新，并采用寻呼方式对通过 SGSN 进行 GPRS 附着用户的电路寻呼进行协调，从而减少对系统无线资源的占用时间，减少系统信令链路负荷，有效提高网络性能。

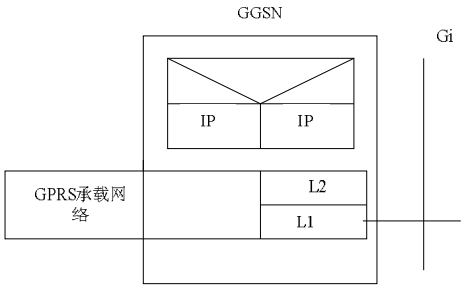


图 2.9 Gi 接口

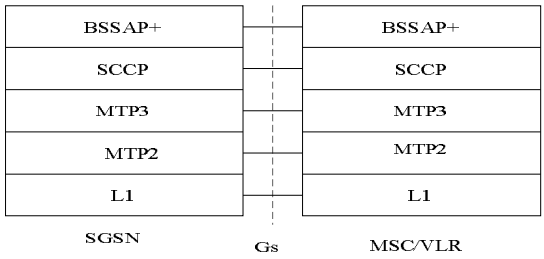


图 2.10 Gs 接口

2.4 数据传送过程

上行数据块的传送采用不同的媒体接入控制方式，如动态分配、扩展动态分配和静态分配方式等。MS 所采用的媒体接入方式由分组下行设定（Packet Downlink Assignment）信息中的 MAC_mode 参数标定，并取决于分组上行设定（Packet Downlink Assignment）信息中所包含的动态分配（Dynamic Allocation Struct）和静态分配（Fixed Allocation Struct）信息[7]。

MS 通过一步或两步接入法完成冲突检测和解决过程之后，将进入分组传送模式，启动数据传送过程。

在上行数据块传送之前，网络将通过分组上行设定（Packet Uplink Assignment）信息或分组时隙重新配置（Packet Timeslot Reconfigure）信息设定以下内容：

①TFI,在 TBF 的所有无线块中将惟一使用此值

②用于上下传送的一组 PDTCH

③TBF 起始时间指示

2.4.1 动态分配方式下的上行 RLC 传送过程

动态分配方式下的上行 RLC 传送过程如图 2.11 所示。MS 通过上行无线块进行上行数据的传送，网络侧将在 PACCH 上采用分组上行确认/非确认信息进行接收确认，在数据传送过程中网络还将通过分组上行设定信息进行上行资源分配。

MMMS 也可以通过发送分组控制确认信息进行接入信息的发送。如图 2.11 所示：

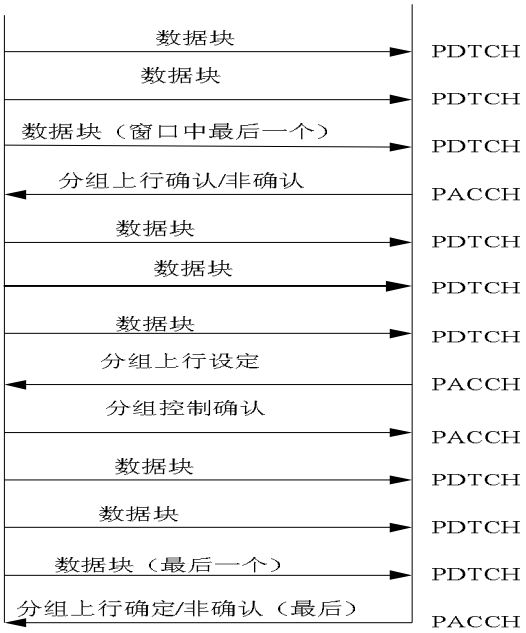


图 2.11 动态分配方式下的上行数据传送过程

上行 RLC 数据块传送过程:

如果 MS 所接收的上行设定信息中不包含 TBF 起始时间，则 MS 应在 B（（x+3）mod12）期间内开始监视所设定 PDCH 上的 USF 信息。

如果上行设定信息中包含 TBF 起始时间，MS 将在 TBF 起始时间到达后开始使用网络所设定的上行 TBF 参数进行数据传送。如果 MS 在所设定的 PDTCH 上检测到所设定的 USF 信息，MS 将在同一个 PDTCH 上传送 1 个或最多 4 个 RLC/MAC 数据块（由 USF_Granualarity 参数决定）。MS 通过 T3180 监视 USF 的分配情况，当 MS 发送一个 RLC/MAC 数据块到网络时，它将启动 T3180，当它接收到 USF 信息时，将复位 T3180。如果 T3180 超时，MS 将执行 TBF 异常释放。

网络侧接收到合法的 RLC/MAC 数据块后，将复位计数器 N3101.如果在所分配的无线块中没有接收到数据，网络将增加 N3101 计数器值。N3101 最小值应该大于 8，如果 N3101 等于 N3101 的最小值，网络将停止从 MS 接收 RLC/MAC 数据块，并启动 T3169，T3169 超时后，网络将重新使用 USF 和 TFI 值。

2.4.2 下行数据传送过程

下行数据采用“分组数据块”信息进行传送，网络通过轮询来请求 MS 侧发送“分组下行确认/非确认”信息予以接收确认，对于没有正确接收的数据块，网络侧将进行重传。所涉及的相关信息类型和流程如图 2.12 所示[8]。

下行数据传送过程:

如果 MS 所接收的上行设定信息中不包含 TBF 起始时间，则在 B（（x+3）mod 12）期间内，MS 应开始监视所设定 PDCH 上的 USF 信息。

如果分组下行设定信息中不包含 TBF 起始时间，MS 将启动 T3190 并解码所设定 PDCH 上的每个下行块。

如果分组下行设定信息或时隙重新配置信息中包含 TBF 起始时间，并且目前没有下行 TBF，但有上行 TBF，则 MS 将停留在所设定的 PDCH 上，直到 TBF 设定时间指示的 TDMA 帧号到达为止，然后 MS 启动 T3190 并立即开始对所设定的 PDCH 进行编码。

如果分组下行设定信息或分组时隙重新配置信息中包含 TBF 起始时间，并且目前有下行 TBF，则 MS 将继续使用当前 TBF 的参数，直到 TBF 设定时间指示的 TDMA 帧号到达为止，然后 MS 开始使用新设定的下行 TBF 的参数。

如果在等待起始帧过程中，MS 接收到一个新的下行设定信息，则它将忽略前一个下行设定信息，接收新的设定信息如图 2.12 所示。

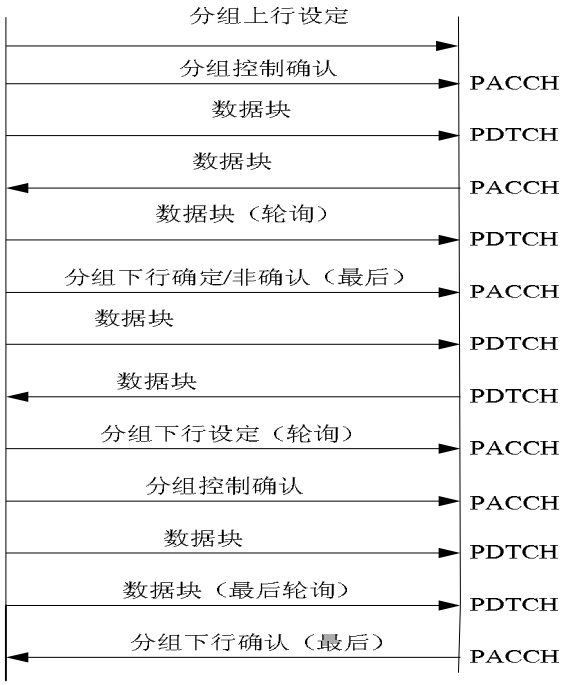


图 2.12 数据下行传送过程

下行控制信息传送过程:

下行 RLC/MAC 控制块格式如图 2.13 所示：

USF 在下行 RLC/MAC 块上传送，用于指示同一个时隙上下一个上行无线块的分配与使用。USF 为 3bit，可以表示 8 种不用的 USF 值，其中 111（USF=FREE）表示相应的上行无线块作为 PRACH 使用。

R 表示 MS 可以发送一次或多次信道请求信息

SI 表示 MS 的 RLC 传送窗口已经满，这种情况在接收方不能及时应答时将会产生。

S/P 表示 RRBP 域是否合法。

RRBP 表示一个用于传送 Packet Control Ack 或 PACCH 的上行无线块。

图 2.13 下行 RLC/MAC 控制块格式

如表 2.1 所示控制块中其他信息字段（如 CV 表示倒计数值，有效负荷类型表示信息类型，TBF 标识 TFI，功率减少指示 PR，地址控制 AC，最后封装指示位 FS，方向指示 D，无线事务指示 RTI，BSN 号等）。

表 2.1 用 RRBP 表示的传送上行 RLC/MAC 块之前需要等待的 TDMA 帧数

比特	全速率 PDCH	半速率 PDCH
65	用 TDMA 帧号表示的上行数据块	用 TDMA 帧号表示的上行数据块
00	（N+13）模 2715648	保留
01	（N+17 或 N+18）模 2715648	（N+17 或 N+18）模 2715648
10	（N+21 或 N+22）模 2715648	保留
11	（N+26）模 2715648	（N+26）模 2715648

2.4.3 TBF 清除过程

上行 TBF 的释放由网络侧或 MS 发起。以下以确认模式为例解释上行 TBF 释放过程[9]。

网络侧通过在 PACCH 上发送分组 TBF 释放（Packet TBF Release）信息启动上行 TBF 释放过程。如果为正常释放，MS 将根据倒计数过程清除 TBF；如果为异常释放，则 MS 立即停止数据传送，释放 TBF 和相关资源，并转到 CCCH 或 PCCCH 进行新上行 TBF 的建立。

MS 在所发送的 RLC 上行数据块中存在一个倒计数值 CV，以表明当前上行 TBF 中尚未传送的数据块。CV 是包含在上行 RLC 包头中的 4bit 信息位，其最大值为 15。MS

在所发送的数据块中设定 15，直到未发送的 RLC 块等于系统所设定的 BS_MAX_CV 个 RLC 数据块，直到 CV=0，然后进行 TBF 释放。只有在网络侧接收到包含 CV=0 的 RLC 数据块，并且所有的 RLC 数据块都已经被确认完成后，它才发送包含最后确认指示位为 1 和包含合法 RRBP 的 Packet Uplink Ack/Nack 消息。MS 接收到此上行确认信息后，将传送 Packet Control Acknowledge 消息并释放 TBF。网络侧接收到分组控制确认消息后，它就可以重新使用 TFI 和 USF 资源。

下行 TBF 的释放一般由网络侧发起。以下以确认模式为例解释下行 TBF 释放过程。

网络侧通过发送包含最后指示位 FBI=1 及包含合法 RRBP 的 RLC 数据块，启动下行 TBF 释放过程。所发送的 RLC 数据块必须是下行 TBF 中的最后一个 RLC 数据块。MS 在接收到此 RLC 数据块之后，将发送分组下行确认/非确认消息并继续监视所设定的 PDCH 信道。如果 MS 接收到 FBI=1 的消息并且已经接收完 TBF 中所有 RLC 数据块，它将发送包含最后确认位 FAI 为 1 的分组下行确认/非确认消息。网络侧接收到分组下行确认/非确认消息后，如果没有数据需要重传，则启动 T3193.在 T3193 超时后，网络将释放 TBF。

网络侧可以通过在 PACCH 上发送分组 TBF 释放消息对下行 TBF 进行异常释放。MS 在接收到分组 TBF 释放消息后将立即停止监视所设定的下行 PDCH。如果在分组 TBF 释放消息中包含合法的 RRBP 域，MS 将在特定的上行无线块中传送分组控制确认消息。如果不存在上行 TBF，则 MS 将进入分组空闲模式[10]。

2.5 GPRS 系统关键性能指标

2.5.1 吞吐量

吞吐量定义为系统平均每秒传输的数据率。GPRS 系统吞吐量通常指 RLC/MAC 层吞吐量。CS1 到 CS4 的吞吐量分别为 9.05kbps,13.4kbps,15.6kbps 和 21.4kbps,但是实际测试过程中所能得到的吞吐量远小于理论值，主要是由于各协议层的数据包头开销造成的。因此，进行具体量化分析将有助于更好地了解系统的实际性能[11]。

应用层数据（如 FTP，HTTP 数据）在通过 GPRS 网络进行传送时，首先进行 IP 封装，再经过 SNDCP 封装，最后经由 LLC 和 RLC/MAC 层封装后采用无线信道进行传送。

(1) GPRS 各协议层包头

①IP 包头

IP 协议包头的典型长度为 20 字节，若添加其他选项，则其长度将会相应增加，具体长度值可通过 Internet 包头长度（IHL）来表示，该字段存放的是 IP 包头中 4 字节“字”的个数，即将 IP 包头的长度除以 4 所得到的值。为避免出现小数，必须将 IP 包头填充为 4 字节的整数倍。若采用 20 字节的 IP 包头，则 IHL 字段的长度为 5（即 20/4）。IHL

的长度为 4bit,其最大值为 15，也就是说 IP 包头的最大长度为 60（即 15*4）字节（如图 2.14 所示）。

图 2.14　IP 包头

②TCP 包头

TCP 包头的标准长度为 20 字节。如果有选项，例如数据最大段长度 MSS，则包头的长度会超过 20 字节（如图 2.15 所示）。

图 2.15 TCP 包头

③UDP 包头

UDP 包头的标准长度为 8 字节（如图 2.16 所示）

图 2.16 UDP 包头

④SNDCP 包头

每个 SN-PDU 包含若干个证书字节，即包头部分和数据部分。有两种不同的 SN-PDU 格式，一种是 SN-DATA PDU，用于确认型数据传送方式，一种是 SN-UNITDATA PDU，用于非确认型数据传送方式。

SNDCP 包头一般为 3-4 字节（如图 2.17 和图 2.18 所示）。

比特位	8	7	6	5	4	3	2	1
字节1	X	F	T	M	NSAPI			
2	DCOMP				PCOMP			
3	N-PDU号-确认模式							
.....	数据分段							
N								

图 2.17 SN-DATA PDU 格式

比特位	8	7	6	5	4	3	2	1
字节1	X	F	T	M	NSAPI			
2	DCOMP				PCOMP			
3	分段号				N-PDU号，非确认模式			
4	N-PDU号，非确认模式（续）							
.....	数据分段							
N								

图 2.18 SN-UNITDATA PDU 格式

⑤LLC 包头

LLC 帧包括地址域、控制域、信息域和帧校验序列等项。地址域一般为 1 字节，而控制域和信息域则为可变长字节（如图 2.19 所示）。

图 2.19 LLC 帧格式

控制域：进行 LLC 层数据传送时，非确认模式下采用 UI 进行传送，控制字段的长度为 2 字节；确认模式下采用 U 进行数据传送，控制字段为 1 字节（如图 2.20 所示）。

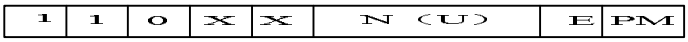


图 2.20　LLC 控制域格式

信息域：N201 设定 LLC 数据包中数据最大长度。N201U 用于非确认模式传送，N201I 用于确认模式传送，目前一般设定为 500 字节。

⑥RLC 包头

下行 RLC 数据块格式如图 2.21 所示。在某些情况下，长度指示位可以忽略，则 RLC 包头典型为 2-3 字节。

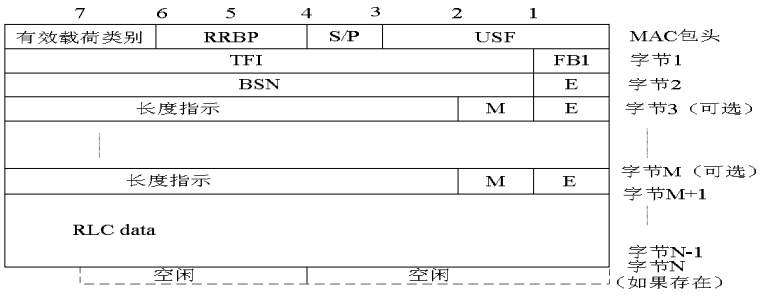


图 2.21 RLC/MAC 数据包格式

对于不同的编码方式，规定 RLC 数据块的最大长度不同，如 CS1 数据块长度为 22 字节，CS2 则为 32 字节。增加空闲位之后数据长度有所变化，具体值如表 2.2 所示。

表 2.2　RLC 数据块大小

信道编码方式	不包含空闲位的 RLC 数据块的大小/字节	空闲比特位数	RLC 数据块大小/字节	
CS1	22	0	22	7/8
CS2	32	7	32	7/8
CS3	38	3	38	3/8
CS4	52	7	52	7/8

RLC 帧头一般为 2-3 字节。对于某个 LLC 帧的第一个 RLC 数据包，由于不包含 LI 字节用于 LLC 帧分界（只有 TBF 中任何 LLC PDU 的最后分段才在相应 RLC 数据块中以 LI 表示），所以 RLC 包头为 2 字节。后续帧中可能包含用于帧分界的 LI 信息，RLC 帧头为 3 字节。

(2) 各种编码方式下的理论速度

MAC 层进行封装时，增加 1 字节的 MAC 包头。

RLC/MAC 数据包经过添加校验位和魏比特，之后分别进行 USF 和数据的编码，形成 456 位的数据，经由交织过程，形成 4 个 114 比特的突发脉冲[22]。

在对 RLC/MAC 数据块进行无线编码时，3 比特的 USF 独立编码，剩余部分作为有效负荷进行编码，在 20ms 长的时间内进行发送。由此可推算不同编码方式下的理论速率如下：

CS1：$(22+1)\times 8-3=181\,\text{bit}$　　181bit/20ms=9.05kbps　　(式 2.1)

CS2: $\left[32\frac{7}{8}+1\right]\times 8-3=268\,\text{bit}$　　268bit/20ms=13.4kbps　　(式 2.2)

CS3: $\left[38\frac{3}{8}+1\right]\times 8-3=312\,\text{bit}$　　312bit/20ms=15.6kbps　　(式 2.3)

CS4: $\left[52\frac{7}{8}+1\right]\times 8-3=428\,\text{bit}$　　428bit/20ms=21.4kbps　　(式 2.4)

(3) GPRS 信道实际编码效率计算

以太网上运行的 TCP/IP 的默认数据段的长度为 1460 字节，采用 Ethernet 封装。加上 20 字节长的默认 TCP 包头和 20 字节长的默认 IP 包头，总共为 1500 字节，正好是一个以太网帧的最大载荷。如果把数据段的长度设置成大于 1460 字节，TCP 会把这个由于太长而不能放入一个以太网帧的数据段交给 IP，导致 IP 包的分解[23]。如图 2.22 所示：

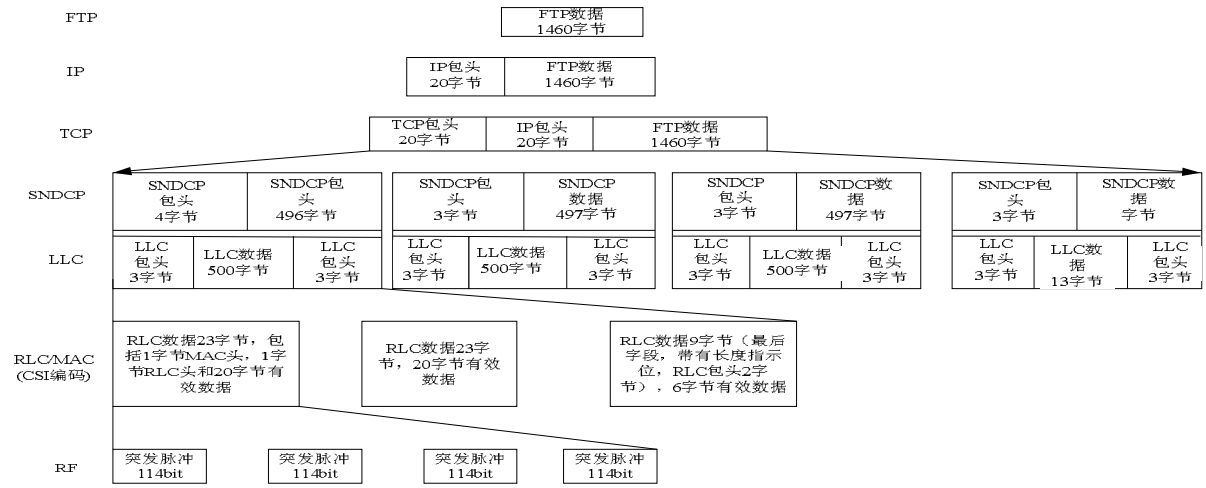


图 2.22 GPRS 协议层有效载荷

根据以上分析，IP 数据经过各个协议层的封装处理，有效载荷将有所增大，所以数据速率有所下降，

(4) SNDCP/LLC 层效率

当采用 500 字节 LLC 数据帧时，增加 6 字节的 LLC 帧头后，RLC 层所接收到的数据包长度将为 506 字节。考虑到其中还有 4 字节的 SNDCP 帧头开销，则 LLC 层传送效率为 496/(496+4+6)=98%.

(5) RLC 层有效吞吐量

RLC 有效吞吐量与数据包大小、编码方式等因素有很大关系。

假设 LLC 数据帧为 506 字节，如果采用 CS1 编码方式，包长为 20 字节的 RLC 帧为 25 个（506 除以 20 去整），包长为 19 字节的 RLC 帧为 1 个（最后一个包）。如果采用 CS2 编码方式，包长为 30 字节的 RLC 帧为 16 个（506 除以 30 并取整），包长为 29 字节的 RLC 帧为 1 个（最后一个包）。两种编码方式下 RLC 包的有效负荷及编码速率分别为：

CS1 时的平均 RLC/MAC 负荷为(20*25+19*1)/(25+1)=19.96 字节/RLC 块，吞吐量为 19.96*8/20=7.984kbps/TS.

CS2 时的平均 RLC/MAC 负荷为(30*x16+29*1)/(16+1)=29.94 字节/RLC 块，吞吐量为 29.94*8/20=11.976kbps/TS.

可见，考虑包头负荷之后，CS1 的有效速率为 7.984，相对于 9.05 的理论速率而言，约为 88%，而 CS2 编码方式在考虑了包头负荷之后相对于理论速率也仅为 89%。通过分析，使得我们对实际测试中的数据传送速率有了深入认识。

同样方法可以计算不同大小 LLC 数据包下的 RLC 速率。

吞吐量通常通过 FTP 或 UDP 等方法进行测试，由于 UDP 协议包头较少，所以采用 UDP 协议测试更为准确。

(6) 吞吐量变化相关因素

GPRS 系统中吞吐量与无线环境和 TCP/IP 作用机理有很大关系，其影响因素概述为：

① 无线环境影响造成的编码方式改变将对吞吐量造成影响；

②丢包将引起 TCP 慢启动或者阻塞控制，从而影响吞吐量；

③网络拥塞对系统吞吐量造成影响；

④MS 处理能力或者 bug 造成用户吞吐量降低；

⑤ 测试过程中频繁的路由切换也可能造成吞吐量降低；

⑥ TCP/IP 规程特性将对网络吞吐量产生很大影响；

2.5.2 延时

系统延时是指数据包在数据收发设备之间传送所需的时长。GPRS 网络中的时延包括网络内部时延以及外网时延两个方面。

对于 FTP 数据传输来讲，GPRS 中主要有时延系统间传送时延和系统处理时延，数据传送时延和 TBF 建立释放时延。其中系统处理时延和系统间传送时延基本固定，从而影响时延的最大因素为数据传送过程中的 TBF 建立时间和数据传送时延。

TBF 建立是指从发送立即指配到已接收到第一个 UL/DL RLC 数据块的时间，因此采用一步接入法和两步接入法时 TBF 的建立时间有所不同。

RTT 指系统端到端的时延，一般用 Ping 进行测试。

2.5.3 Ping 定义

GPRS 系统中一般采用 Ping 进行延迟测试。

(1)Ping 的理论意义

Ping 程序用于检测远端主机是否可达，它控制发送 ICMP 报文，并根据应答报文的类型确定发送方与主机之间路由的通达性。另外，它可以通过计算报文发送与接收到应答之间的时延，即到目的主机的往返时间来表示源主机与目的主机之间的距离。因此，Ping 常用来分析链路时延。但是在某些情况下，某些主机或网络出于安全考虑，会将 Ping 包屏蔽，这时候虽然显示目的主机不可达，但是它们之间仍是相通的。

Ping 在发送 ICMP 报文请求时，将发送序列号顺序加一，应答信息也同样标识序列号，所以通过观察 Ping 包的回应消息可以观察到链路状况，如分组丢失、分组重复和错序等。由于 Ping 采用 UDP 方式进行传送，所以上述 3 种情况有可能发生。

Ping 的测试方法：

(1) 对于采用 Window 系统的计算机来讲，可以采用 DOS 下命令行的方式来进行测试。

(2) Agnettool 等工具提供 Ping 的简单工具，所以可以通过简单设置测试次数以及数据包大小等进行测试。

Ping 与数据包大小的关系：

由于 GPRS 系统中 LLC 和 RLC 层都规定了数据包的大小，所以数据包大小由于包头负荷不一样，其传送效率也不相同。小的数据包一般一个 LLC 帧即可传送，其占用的 RLC 数据块也少，如 10 字节数据包采用 CS1 编码方式时，考虑各协议层包头负荷后将占用两个 RLC 数据帧；500 字节的 LLC 帧 CS1 方式下将占用 26 个 RLC 数据块，CS2 方式下将占用 17 个 RLC 数据块。进行系统性能测试时需根据不用测试目的考虑采用不同大小的数据包。

① 如果只是为了了解 GPRS 系统的最小时延，则建议采用小的数据包，如 CS2 时采用 10 字节数据包(包含 2 个 RLC 数据块，1 个 LLC 帧)。但是在 CS1 的情况下，10 字节数据包将包含 3 个 RLC 数据块，从而增加时延。

②如果为了测试 IP 包的 RTT，则建议使用大的数据包，通常可考虑采用 500 字节的数据包(CS2 方式下包含 17 个 RLC 数据块，2 个 LLC 帧)。标准的 DOS 命令下 Ping 采用 32 字节的 ICMP 包，在 CS2 下 RLC 层约为 3 个 RLC 数据包。其长度可以采用开关 Ping<ip-address>-1<payload>予以调整。10 字节与 32 字节的延迟差别可根据 RLC 数据块进行估算。CS2 时 10 字节包需要 2 个 RLC 块，而 32 字节包需要 3 个 RLC 块，因此上 UL 需要多传送一个 RLC 包，延迟有所增加，下行方向与上行方向作用原理相同。Ping 与发送间隔的关系 Ping 间隔是指前一个 Ping 包响应与下一个 Ping 包发送之间的时间间隔。在 GPRS 系统中，由于上下行数据的传送需要分别建立 TBF,所以合理的 Ping 间隔设置需考虑 TBF 的建立释放过程以及相关的定时器值(如 T3192)。T3192 指接收到最后一个下行数据块之后延迟释放 TBF 的时间，如果 T3192 还没有超时，则系统可以直接使用前一个 TBF，因此在连续数据包传送时需考虑 T3192 的作用。

如果接收到网络侧所发送的 RLC 数据块中指明 FBI=0，则 MS 侧准备释放 TBF 并启动 T3192 期间内，MS 继续监视 PDTCH，如果有下行数据传送，网络可以立即发起下行 TBF 建立过程，若 T3192 过期，则 MS 需监视寻呼信道。

因此为了减少 T3192 的影响，Ping 间隔时间应大于 T3192 值(默认为 500ms),以确保 TBF 的建立于释放。

2.6 本章小结

本章主要详细介绍 GPRS 技术的一些概念以及 GPRS 的网络功能，简述了 GPRS 的通信规约，以及 GPRS 技术的一些性能指标和上行下行传输的过程，然后对其关键性能指标进行简单的阐述。

3 集中器

集中器是管理中心与电表进行通信的桥梁，是收集各采集终端的数据，并进行处理储存，同时能和主站进行数据交换的设备。其中通信部分主要由两个无线通信模块组成：GPRS 无线模块负责跟 Internet 连接的主站进行通信，完成数据的传输和交换；PLC 模块完成集中器和电表之间数据的传输和交换[12]。校园智能抄表系统中至少有一台集中器，安装位置一般在中心处。

3.1 集中器的通信机制

集中器主要由微控制器与 GPRS 无线模块和 PLC 模块构成。在 GPRS 模块中插入 SIM 卡以后，能获得一个动态 IP，并自动上线，接入移动公司的 GPRS 网络。此处的 PLC 为采集器，起到采集数据的作用。主站管理软件将要发送的命令根据协议的规定生成数据帧，然后将数据帧打包成 IP 数据包，通过 Internet 发送到移动公司内部网络。移动网络通过 GPRS 内部 SIM 卡的标识找到相应的 GPRS 模块，然后将 IP 包发送过去。GPRS 模块收到 IP 包以后，提取出数据帧，然后将其发送到主站，然后数据帧通过 GPRS 网络到达相应的采集终端。采集终端按指令要求采取相应操作，并将操作的结果生成数据帧，按相反的路径返回主站计算机。

集中器对被测数据的采集有两种方式：

(1)主站采用查询的方式，向被测目标发送数据采集指令，采集每个被测目标的数据。具体的过程是：主站通过连接 Internet 网络到移动公司，移动公司通过 GPRS 网络找到集中器中的 SIM 卡号，发送一条传输指令给集中器，集中器响应之后返回一条指令，完成主站跟集中器之间的通信。采集终端根据指令完成相应任务，然后返回相应的参数，发送至集中器，经由集中器将数据由远程网络传送给主站，主站对采集到的数据进行处理。例如，主站发送一条采集指令给集中器，集中器响应之后发送一条指令给电表，将电表度数和电表功率通过GPRS网络将数据传送给主站，主站将收到的信息显示并保存。

(2)集中器根据系统设定的时间对每个被测目标采集数据，并将采集到的数据存储在自身的存储器中，主站只要访问集中器即可得到所有的目标数据。这种通信方式可以很大程度上节省数据通信的时间。

图 3.1 所示为 GPRS 数据集中器系统框图：

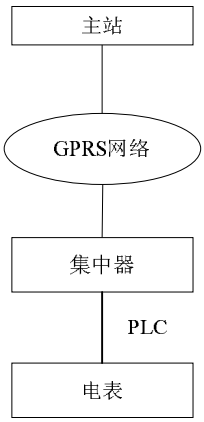


图 3.1　GPRS 数据集中器系统框图

从集中器的角度讲，从集中器到主站的通道为上行信道，上行通道通过 GPRS 将主站和集中器连接起来；从集中器到电表之间的通道为下行信道，下行通道通过 PLC 将集中器和电表连接起来。

3.2 集中器通信规约分析

3.2.1 MODBUS 协议

MODBUS 是 OSI 模型第 7 层上的应用层报文传输协议，它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信。MODBUS 是一个请求/应答协议，并且提供功能码规定的服务。MODBUS 功能码是 MODBUS 请求/应答 PDU 的元素。MODBUS 是一项应用层协议，用于在通过不同类型的总线或网络连接的设备之间的客户机/服务器通信[3]。

MODBUS 协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。

特定总线或网络上的 MODBUS 协议映射能够在应用数据单元（ADU）上引入一些附加域如图 3.2 所示：

图3.2　通用MODBUS帧

启动 MODBUS 事物处理的客户机创建 MODBUS 应用数据单元。功能码向服务器指示将执行哪种操作。

MODBUS 协议建立了客户机启动的请求格式。

用一个字节编码 MODBUS 数据单元的功能码域。有效的码字范围是十进制的 1-255（188-255 为异常响应保留）。当从客户机向服务器设备发送报文时，功能码域通知服务器执行哪种操作。

向一些功能码加入子功能码来定义多项操作。

从客户机向服务器设备发送的报文数据域包括附加信息，服务器使用这个信息执行功能码定义的操作。这个域还包括离散项目和寄存器地址、处理的项目数量以及域中的实际数据字节数。

在某种请求中，数据域可以是不存在的（0 长度），在此情况下服务器不需要任何附加信息。功能码仅说明操作。

如果在一个正确接收的 MODBUS ADU 中，不出现与请求 MODBUS 功能有关的差错，那么服务器至客户机的响应数据域包括请求数据。如果出现与请求 MODBUS 功能有关的差错，那么域包括一个异常码，服务器应用能够使用这个域确定下一个执行的操作。

串行链路上第一个 MODBUS 执行的长度约束限制了 MODBUS PDU 大小（最大 RS485ADU=256 字节）。

因此，对串行链路通信来说，MODBUS PDU=256-服务器地址（1 字节）-CRC（2 字节）=253 字节。

从而：

RS232/RS485 ADU=253 字节+服务器地址（1 byte）+CRC(2 字节)=256 字节。

TCP MODBUS ADU=249 字节+MBAP（7 字节）=256 字节。

MODBUS 协议定义了三种 PDU。他们是：

MODBUS 请求 PDU，mb_req_pdu

MODBUS 响应 PDU，mb_rsp_pdu

MODBUS 异常响应 PDU，mb_excep_rsp_pdu

定义 mb_req_pdu 为：

mb_req_pdu={function_code,request_data},其中

function_code-[1 个字节]MODBUS 功能码

request_data-[n 个字节]，这个域与功能码有关，并且通常包括诸如可变参考、变量、数据偏移量、子功能码等信息。

定义 mb_rsp_pdu 为：

mb_rsp_pdu={function_code,response_data},其中

function_code-[1 个字节]MODBUS 功能码

response_data-[n 个字节]，这个域与功能码有关，并且通常包括诸如可变参考、变量、数据偏移量、子功能码等信息。

定义 mb_excep_rsp_pdu 为：

mb_excep_rsp_pdu={function_code,response_data},其中

function_code-[1 个字节]MODBUS 功能码+0x80

exception_code-[1 个字节]，在下表中定义了 MODBUS 异常码。

3.2.2 数据编码

MODBUS 使用一个‘big-Endian’表示地址和数据项。这意味着当发射多个字节时，首先发送最高有效位。

MODBUS 以一系列具有不同特征表格上的数据模型为基础。四个基本表格为表 3.1 所示：

表 3.1 MODBUS 数据模型表格

基本表格	对象类型	访问类型	内容
离散量输入	单个比特	只读	I/O系统提供这种类型数据
线圈	单个比特	读写	通过应用程序改变这种类型数据
输入寄存器	16-比特字	只读	I/O系统提供这种类型数据
保存寄存器	16-比特字	读写	通过应用程序改变这种类型数据

输入与输出之间以及比特寻址的和字寻址的数据项之间的区别并没有暗示任何应用操作。如果这是对可疑对象核心部分最自然的解释，那么这种区别是可完全接受的，而且很普遍，以便认为四个表格全部覆盖了另外一个表格。

对于基本表格中任何一项，协议都允许单个地选择 65536 个数据项，而且设计那些项的读写操作可以越过多个连续数据项直到数据大小规格限制，这个数据大小规格限制与事务处理功能码有关[4]。

很显然，必须将通过 MODBUS 处理的所有数据放置在设备应用存储器中。但是，存储器的物理地址不应该与数据参考混淆。要求仅仅是数据参考与物理地址的链接。

MODBUS 功能码中使用的 MODBUS 逻辑参考数字是以 0 开始的无符号整数索引。

3.2.3 功能码分类

有三类 MODBUS 功能码如图 3.3 所示。它们是：

(1) 公共功能码

是较好地被定义的功能码；

保证是唯一的；

MODBUS 组织可改变的；

公开证明的；

具有可用的一致性测试；

MB IETF RFC 中证明的；

包含已被定义的公共指配功能码和未来使用的未指配保留供功能码；

(2)用户定义功能码

有两个用户定义功能码的定义范围，即 65 至 72 和十进制 100 至 110；

用户没有 MODBUS 组织的任何批准就可以选择和实现一个功能码；

不能保证被选功能码的使用是唯一的；

如果用户要重新设置功能作为一个公共功能码，那么用户必须启动 RFC，以便将改变引入公共分类中，并且指配一个新的公共功能码；

(3) 保留功能码

一些公司对传统产品通常使用的功能码，并且对公共使用是无效的功能码

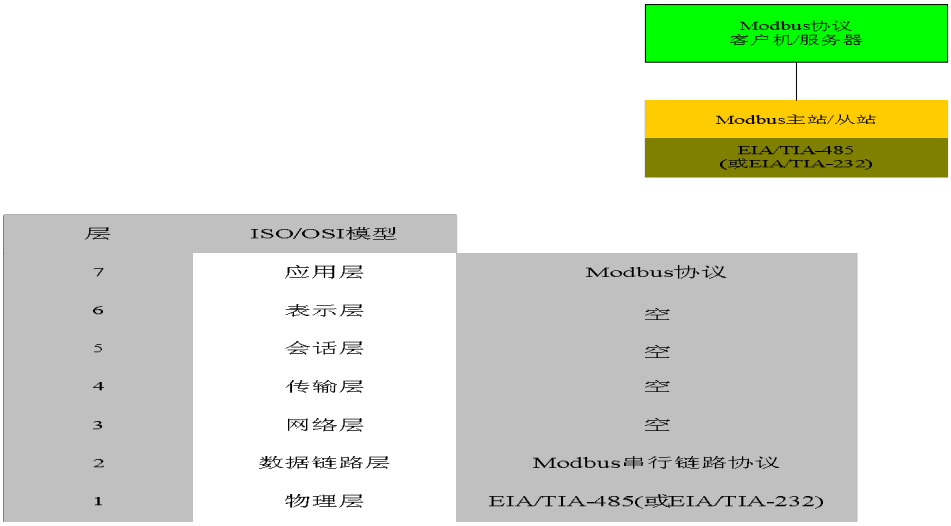
图3.3 MODBUS功能码分类

3.2.4 MODBUS 串行链路协议

MODBUS 串行链路协议是一个主/从协议，该协议位于 OSI 模型的第二层。

一个主从类型的系统有一个向某个“子”节点发出显示命令并处理响应的节点（主节点）。典型的子节点在没有收到主节点的请求时并不主动发送数据，也不与其它子节点通信[5]。

图 3.4 给出了 Modbus 串行通信栈对应于 7 层 OSI 模型的一般关系。



层	ISO/OSI模型	
7	应用层	Modbus协议
6	表示层	空
5	会话层	空
4	传输层	空
3	网络层	空
2	数据链路层	Modbus串行链路协议
1	物理层	EIA/TIA-485(或EIA/TIA-232)

图3.4　Modbus协议和ISO/OSI模型

位于 OSI 模型第 7 层的 Modbus 应用层报文传输协议，提供了连接于总线或网络的设备之间的客户机/服务器通信。在 Modbus 串行链路上客户机的功能由主节点提供而服务器功能由子节点实现。

(1) Modbus 主站/从站协议原理

Modbus 串行链路协议是一个主-从协议。在同一时刻，只有一个主节点连接于总线，一个或多个子节点（最大编号为 247）连接于同一个串行总线。Modbus 通信总是由主节点发起。子节点在没有收到来自主节点的请求时，从不会发送数据。子节点之间从不会互相通信。主节点在同一时刻只会发起一个 Modbus 事务处理[6]。

主节点以两种模式对子节点发出 Modbus 请求：

在单播模式，主节点以特定地址访问某个子节点，子节点接到并处理完请求后，子节点向主节点返回一个报文（一个‘应答’）如图 3.5 所示。

在这种模式，一个 Modbus 事务处理包括 2 个报文：一个来自主节点的请求，一个来自子节点的应答。

每个子节点必须有唯一的地址（1 到 247），这样才能区别于其他节点被独立的寻址。

在广播模式，主节点向所有的子节点发送请求如图 3.6 所示。

对于主节点广播的请求没有应答返回。广播请求一般用于写命令。所有设备必须接收广播模式的写功能。地址 0 是专门用于表示广播数据的。

单播和广播模式的区别在于一个多点的结构下更加易于理解。

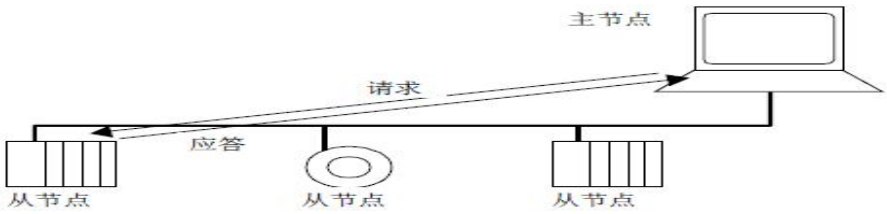


图3.5　单播模式

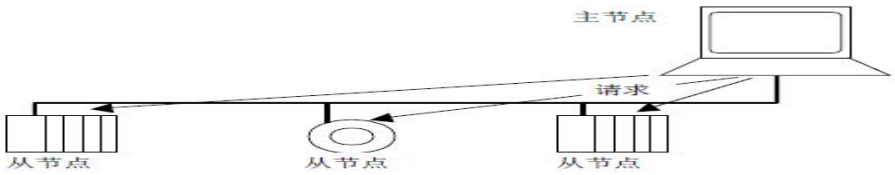


图3.6　广播模式

(2) Modbus 地址规则

Modbus 寻址空间有 256 个不同地址。

0	1-47	248-55
广播地址	子节点单独地址	保留

地址 0 保留为广播地址。所有的子节点必须识别广播地址。

Modbus 主节点没有地址，只有子节点必须有一个地址。该地址必须在 Modbus 串行总线上唯一。

Modbus 帧描述：

Modbus 应用协议定义了简单的独立于其下面通信层的协议数据单元，如图 3.7 和 3.8 所示：

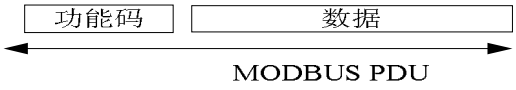


图3.7　Modbus协议数据单元

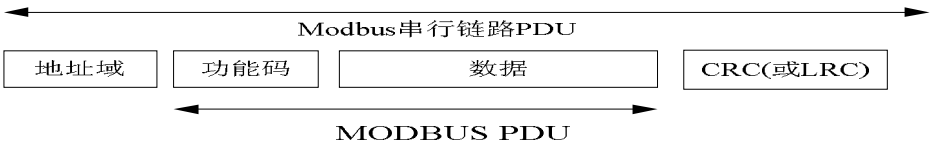


图3.8 串行链路上的Modbus帧

在 Modbus 串行链路，地址域只含有子节点地址。

如前文所述，合法的子节点地址为十进制 0-247。每个子设备被赋予 1-247 范围中的地址。主节点通过将子节点的地址放到报文的地址域对子节点寻址。当子节点返回应

答时，它将自己的地址放到应答报文的地址域以让主节点知道哪个子节点在回答。

功能码指明服务器要执行的动作。功能码后面可跟有表示含有请求和响应参数的数据域[7]。

(3) 主站/从站通信时序图

图 3.9 显示了主/从通信的 3 种典型情况。

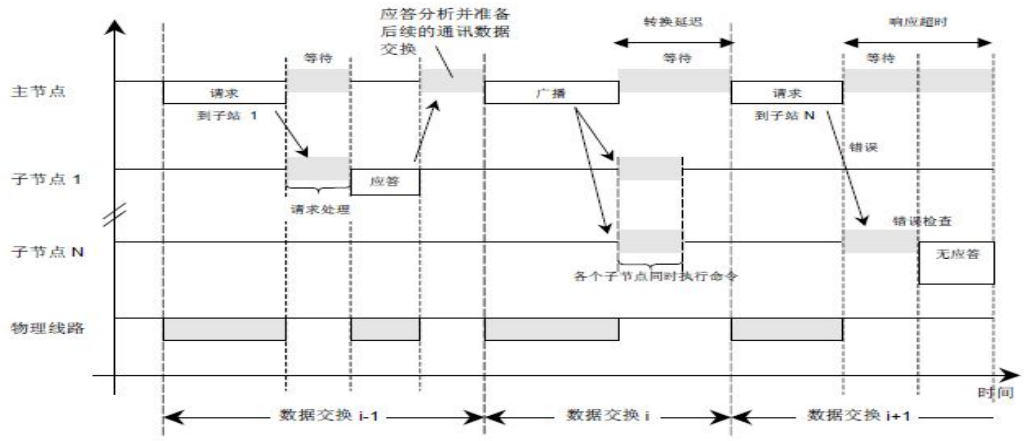


图3.9　各种情形的主/从通信时序图

注：

（1）请求，应答，广播阶段的持续时间依赖于通信特征（帧长度和吞吐量）

（2）等待和处理阶段的持续时间取决于子节点应用的请求处理时间。

3.2.5 两种串行传输模式

有两种串行传输模式被定义：RTU 模式和 ASCII 模式。

它定义了报文域的位内容在线路上串行的传送。它确定了信息如何打包为报文和解码。

Modbus 串行链路上所有设备的传输模式（和串行参数）必须相同。

(1) RTU 传输模式

当设备使用 RTU 模式在 Modbus 串行链路通信，报文中每个 8 位字节含有两个 4 位十六进制字符。这种模式的主要优点是较高的数据密度，在相同的波特率下比 ASCII 模式有更高的吞吐率。每个报文必须以连续的字符流传送。

RTU 模式每个字节（11 位）的格式为：

编码系统： 8-位二进制

报文中每个 8 位字节含有两个 4 为十六进制字符（0-9，A-F）

Bits per Byte: 1 起始位

8 数据位，首先发送最低有效位

1 位作为奇偶校验

1 停止位

字符是如何串行传送的：

每个字符或字节均由此顺序发送（从左到右）：

最低有效位（LSB）….最高有效位（MSB）如图 3.10 所示

图3.10　RTU 模式位序列

设备配置为奇校验、偶校验或无校验都可以接受。如果无奇偶校验，将传送一个附加的以填充字符帧如图3.11所示：

图3.11 RTU模式位序列（无校验的特殊情况）

帧检验域：　　循环冗余检验（CRC）

帧描述如图3.12所示：

子节点地址	功能代码	数据	CRC
1字节	1字节	0 到 252 字节	2字节 CRC低，CRC高

图3.12　RTU报文帧

(2) CRC校验

在RTU模式包含一个对全部报文内容执行的，基于循环冗余校验算法的错误检验域。CRC域检验整个报文的内容。不管报文有无奇偶校验，均执行此检验。

CRC包含由两个8位字节组成的一个16位值。

CRC域作为报文的最后的域附加在报文之后。计算后，首先附加低字节，然后是高字节。CRC高字节为报文发送的最后一个字节。

附加在报文后面的CRC值由发送设备计算。接收设备在接收报文时重新计算CRC的值，并将计算结果于实际接收到的CRC值相比较。如果两个值不相等，则为错误。

CRC的计算，开始对一个16位寄存器预装全1.然后将报文中的连续的8位字节对其进行后续的计算。只有字符中的8个数据位参与生成CRC的运算，起始位，停止位和校验位不参与CRC计算。

CRC的生成过程中，每个8位字符与寄存器中的值异或。然后结果向最低有效位（LSB）方向移动（Shift）1位，而最高有效位（MSB）位置充零。然后提取并检查LSB：

如果LSB为1，则寄存器中的值与一个固定的预置值异或；如果LSB为0，则不进行异或操作。

这个过程将重复直到执行完8次移位。完成最后一次（第8次）移位及相关操作后，下一个8位字节与寄存器的当前值异或，然后又同上面描述过的一样重复8次。当所有报文中字节都运算之后得到的寄存器中的最终值，就是CRC。当CRC附加在报文之后时，首先附加低字节，然后是高字节。

(3) ASCII 传输模式

当Modbus串行链路的设备被配置为使用ASCII模式通信时，报文中的每个8位字节以两个ASCII字符发送。当通信链路或者设备无法符合RTU模式的定时管理时使用该模式。

ASCII模式每个字节（10位）的格式为：

编码系统：　　十六进制，ASCII字符0-9，A-F。

　　报文中每个ASCII字符含有1个十六进制字符

Bits per Byte:　1 位起始位

　　7 位数据位，首先发送最低有效位

　　1 位作为奇偶校验

　　1 位停止位

偶校验是要求的，其他模式（奇校验，无校验）也可以使用。为了保证与其它产品的最大兼容性，同时支持无校验模式是建议的。默认校验模式必须为偶校验。

字符是如何串行传送的：

每个字符或字节均由此顺序发送（从左到右）：

最低有效位(LSB)……最高有效位（MSB）如图3.13所示：

图3.13　ASCII模式位序列

设备配置为奇校验、偶校验或无校验都可以接受。如果无奇偶校验，将传送一个附加的停止位以填充字符帧如图3.24所示：

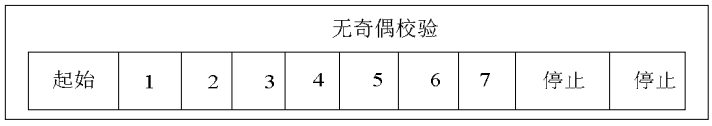


图3.14　ASCII模式位序列（无校验的特殊情况）

3.3 本章小结

本章主要阐述了集中器的一些通信机制，以及集中器的设计系统框架，分析了集中器与主站之间利用GPRS网络进行通信，工作方式为主站通过连接Internet到移动公司，然后移动公司通过GPRS网络找到集中器的SIM卡号，与集中器进行通信连接，完成主站与集中器之间的通信过程，另外讲述了集中器与主站之间的通信协议，研究了集中器通信协议的一些分类和传输模式，以及其一些特点。

4 集中器硬件电路设计

4.1 集中器电路芯片的选择

考虑到集中器的低功耗、经济高效、性能稳定、接口电路简单和自动化程度高等特点，因此选择合适的电路芯片是至关重要的。

4.2 系统硬件总体设计结构

系统以LPC2148为核心；采用EM310为GPRS通信模块；采用青岛鼎信公司的低压线电力载波模块（PLC）进行数据采集，可实时采集系统模块的电压和电流、工作环境温度等；电源管理模块，匹配了系统各模块的供电电压。硬件电路总体框架如图4.1所示：

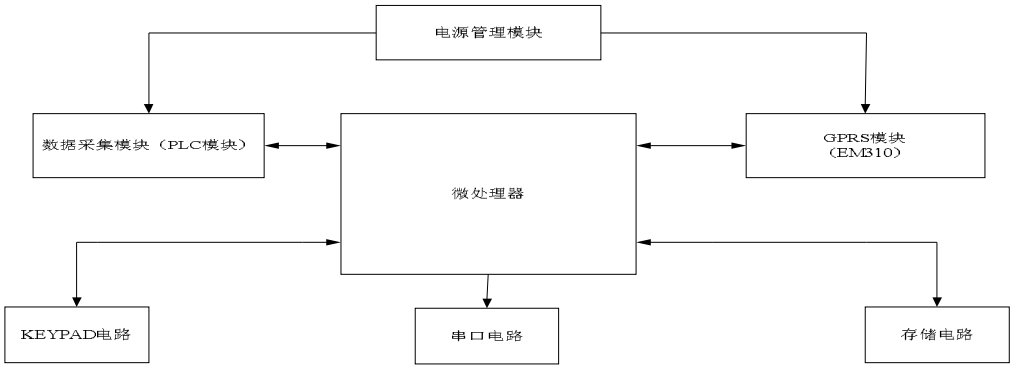


图4.1　集中器硬件总体电路框架图

4.2.1 ARM7 主控芯片选型及外围电路设计

(1) ARM7芯片介绍

单片机技术的不断进步，使其在控制方面的优势正在逐渐被相对高端的微处理器芯片所代替。ARM(Advanced RISC Machines)是32位的微处理器核，由ARM公司设计开发，自1985年出现至今已有20多年的历史。ARM公司是一家微处理器的行业的知名企业，设计大量高性能、廉价、低能耗的RISC(Reduced Instruction Set Computer)处理器。在嵌入式芯片的设计开发中，公司采用IP授权的方式，本身不直接从事芯片的生产，允许其他半导体公司生产基于ARM核的处理器芯片。IP授权的经营方式使得ARM技术得到快速的发展和推广，同时得到更多的第三方工具、制造商。开发软件的支持。目前很多半导体公司都结合自身的优势生产出各具特色的ARM芯片，并占据32位和64位嵌入式处理器的大部分市场[13]。

ARM公司开发很多系列的ARM处理器核，目前最新的是ARM11，应用最为广泛的

是ARM7系列。ARM7系列包括ARM7TDMI、ARM7TDMI-S两种类型。

ARM7TDMI是一个通用的32位微处理器，采用冯•诺依曼结构。指令和数据共用一条32位总线。装载、存储和交换指令可以对存储器中的数据进行访问。数据长度可以是字节(8位)、半字(16位)或者字(32位)。处理器具有标准32位ARM指令和16位Thumb指令两个指令集，支持三级流水线。

系统采用的主控芯片为LPC2148由菲利普公司生产，是一个支持实时仿真和嵌入式跟踪的32位ARM7TDMI-S CPU，芯片特性如下：

16/32位ARM7TDMI-S 微控制器，超小LQFP64封装；

8kB-40kB的片内静态RAM和32kB-512kB的片内Flash程序存储器。128位宽度接口/加速器可实现高达60MHz工作频率；

通过片内boot装载程序实现在系统编程/在应用编程(ISP/IAP)。单个Flash扇区或整片擦除时间为400ms。256字节编程时间为1ms；

EmbeddedICE RT和嵌入式跟踪接口提供实时调试个高速跟踪指令执行；

USB2.0全速设备控制器具有2kB的端点RAM。此外，LPC2148提供8kB的片内RAM，可被USB的DMA控制器访问；

1个或2个10位ADC转换器，提供总共6/14路模拟输入，每个通道的转换时间低至2.44us；

1个10位的D/A转换器提供可变的模拟输出；

2个32位定时器/外部事件计数器、PWM单元和看门狗；

低功耗实时时钟(RTC)具有独立的电源和特定的32kHz时钟输入；

多个串行接口，包括2个UART(16C550)、2个高速 I^2C 总线(400kbit/s)、SPI和具有缓冲作用和数据长度可变功能的SSP；

向量中断控制器(VIC)。可配置优先级和向量地址；

多达45个可承受5V电压的通用I/O口；

多达9个边沿或电平触发的外部中断管脚；

通过一个可编程的片内PLL(100us的设置时间)可实现最大为60MHz的CPU操作频率；

片内集成振荡器可操作频率为1-30MHz的外部晶体或频率高达50MHz的外部振荡器；

低功耗模式：空闲和掉电；

可通过个别使能/禁止外围功能和外围时钟分频来优化额外功耗；

通过外部中断，USB，掉电检测(BOD)或实时时钟(RTC)将处理器从掉电模式中唤醒；

单电源，具有上电复位(POR)和掉电检测(BOD)电路：--CPU操作电压范围：

3.0V-3.6V(3.3V±10%)；

(2) LPC2148 适合集中器的应用

①芯片存储管理

LPC2148具有512KB片内Flash，可以存放用户程序而不用外扩程序存储器；芯片具有40KB片内SRAM，不用外部扩展SRAM也可以满足需要。芯片的片内存储器容量和外部存储控制器的特性适合本系统的应用。

②对外接口

系统是一个远程通讯设备，对通讯口的数量需求较多，并且采用异步通信方式。LPC2148包含2个16C550工业标准UART，具有16字节的收发FIFO(First In First Out)缓冲区，内置波特率发生器，支持异步通讯方式，经过电平转换可以传输比较远的距离。在本系统中将UART转换为RS-485总线方式。芯片的对外通讯接口适合本系统的应用。

③芯片仿真

芯片支持的调试功能适合提高系统用户软件的稳定性。芯片的Embedded ICE RT和嵌入式跟踪使能断点和观察点，通过片内Real Monitor软件对代码进行实时调试和高速跟踪特点可以提高系统用户软件的开发效率。在51系列8位单片机的开发过程中，仿真调试很困难，并且仿真器的价格非常昂贵。LPC2148芯片支持JTAG仿真，调试器价格低廉，大大降低开发成本，有利于提高系统的可靠性[31]。

(3) GPRS模块的选型

在 GPRS 模块的选型，初步也有多样选择，市面上常见的 GPRS 模块有西门子公司的 MC35I，华为公司的 EM310 以及 Wavecom 公司的 Q2406B。三种模块都具有低功耗等优点。且接口都较为丰富。但最终从系统的设计角度来衡量，EM310 能很好的兼容 STC 系列的单片机，两者结合比 MC35I 和 Q2406B 能更好的降低功耗，且开发效率较快。

(4) 低压电力线载波模块选型

TCC081C 芯片实现了基于电力线通信网络的电子终端设备之间可靠的数据交换，具备通信中继能力，可自动实现载波节点侦听、主动上报等网络功能。

TCC081C 芯片进行鼎信规约的电力载波信号和标准 DL/T645-1997/2007 协议的串口信号之间的转换，支持数据透明传输模式；串口可以连接电表节点和电量显示模块，完成物理层、数据链路层、网络层、传输层四层网络功能。电路图如图 4.2 所示

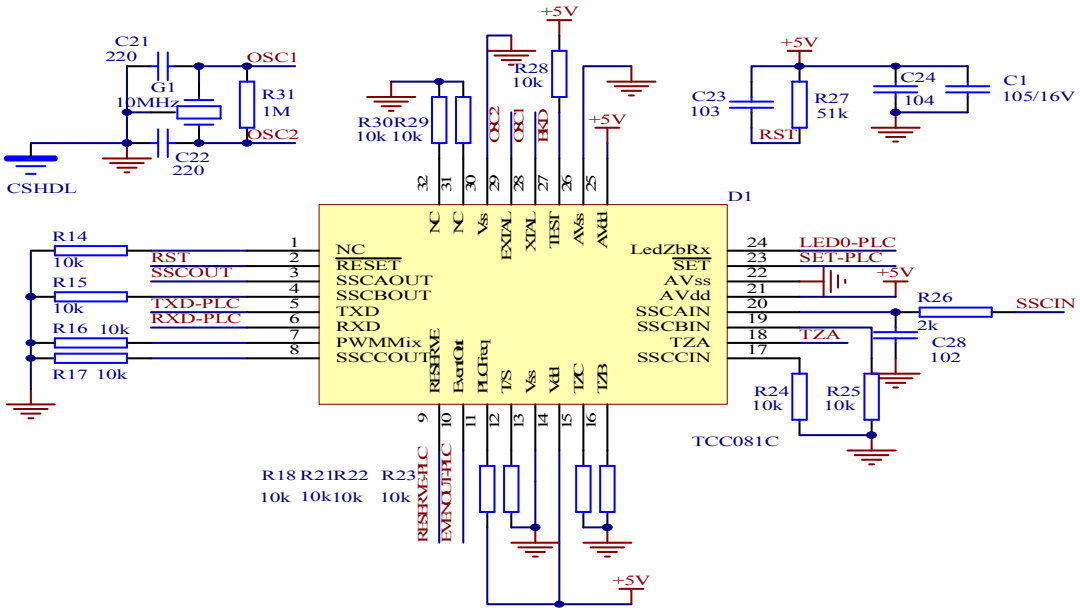


图 4.2 载波控制电路

(5) 电源转换电路

REG1117 系列稳压器有可调版与多种固定电压版，设计用于提供 2A 输出电流且工作压差可低至 1V。在最大输出电流时，REG1117 器件的压差保证最大不超过 1.3V，并随负载电流的减小而逐渐降低。

REG1117 的片上微调把基准电压调整到 1%的误差以内，而且电流限制也得到了调整，以尽量减少因稳压器和电源电路超载而造成的压力。电源转换电路如图 4.3 所示。

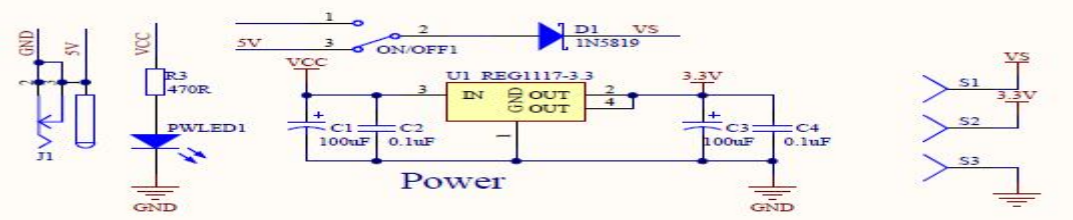


图 4.3 电源转换电路

4.2.2 实时操作系统 μC/OS-II

(1) 实时操作系统 μC/OS-II

系统程序采用一个无限循环完成，通过中断等方式提供对外围设备服务的用户软件系统称为前后台系统或超循环系统。循环中，后台为任务级，调用相应的函数完成相应的操作，前台为中断级，采用中断服务程序处理异步事件[14]。

嵌入式实时操作系统 RTOS(Real Time Operating System)可以提供多任务的任务调度、时间管理、任务间通信和同步以及内存管理 MMU(Memory Manager Unit)等重要服务[34]。目前在嵌入式应用中使用 RTOS 已经成为嵌入式应用的一个热点。

嵌入式实时操作系统的引入，可将系统功能分解成多任务，多任务设计方法会简化数据采集系统的软件设计。用户程序分成多任务，每个任务相对独立。任务中设置超时函数，时间用完以后，任务交出 CPU 的使用权。这样在系统遇到较强的干扰时部分任务死锁甚至被破坏，其它任务的运行不会受到影响[35]。系统可以通过运行系统监控进程对其进行修复，或者把有问题的任务清除掉，从而提高系统的实时性、稳定性、可靠性。

①实时操作系统简介

操作系统分为通用操作系统、实时操作系统两种。实时操作系统除满足应用的功能需求外，更重要的是满足应用提出的实时性要求。一个实时系统包括多个对于实时性要求各不相同的任务，任务之间有一些复杂的关联和同步关系，如执行顺序限制、共享资源的互斥等。因此实时操作系统的设计原则是：采用各种算法和策略，始终保证系统行为的可预测性，在系统运行的任何时刻，在任何情况下，实时操作系统的资源调配策略都能为争夺资源的多个任务合理地分配资源，使每个任务的实时性要求能得到满足[36]。

②实时操作系统的选择

在目前市场比较流行的实时操作系统中，nuClear 源代码收费的，在国内应用有限。QNX 和 WinCE 都更注重于 GUI 图形界面方面的功能体现，不提供源代码，不能根据具体的需求修改操作系统。主要用来设计开发机顶盒、手持设备、GPS 设备等对人机界面要求比较高的地方。PSOS 和 VxWorks 是目前市场上最成熟的 RTOS。系统不会死锁，运行稳定。

与上述实时操作系统不同，μC/OS-II 和 uClinux 操作系统不仅性能优良，运行稳定，并且源码公开，是免费嵌入式实时操作系统，可以作为研究实时操作系统和非实时操作系统的典范。

μC/OS-II 适合小型控制系统，具有执行效率高、占用空间小、实时性能优良、可扩展性强等特点，内核提供任务调度与管理、时间管理、任务同步与通信、内存管理和中断服务等功能；μClinux 是 Micro-Conrol-Linux 的缩写，继承标准 Linux 的特性，针对嵌入式处理器的特点所设计的操作系统，系统稳定，具有较强的网络功能和出色的文件系统，其编译后目标文件在几百 KB 两级[37]。

从实时操作系统的特点、硬件资源限制和控制成本开发周期等多方面考虑。本设计采用 μC/OS-II 实时操作系统完成开发任务，将用户程序全部放在片内 Flash 中，μC/OS-II 是可裁剪的操作系统，其所需要的存储空间，芯片内部就可以满足。

(2) μC/OS-II 的应用

μC/OS-II 内核按照其功能可以划分为任务管理模块、时间管理模块、信号量管理模块、事件管理模块、消息邮箱和队列管理模块和内存管理模块。

由于 μC/OS-II 只免费提供内核，主要的任务是完成多任务之间的调度和同步，并为设备驱动和系统服务程序提供信号量、邮箱、消息队列的服务。而操作系统的其他部

分，如文件系统、网络、窗口系统、输入输出管理程序、调试器等都没有提供，因此需要自行设计和实现软件系统的其他部分。

μC/OS-II 中的每一个任务都有独立的堆栈空间，可以分别定义大小，启动过程简单，内核是和应用程序放在一起编译成一个文件的，把这个文件转换成 HEX 格式，写入 ROM 中，上电后，嵌入式系统会像普通的嵌入式程序一样运行。

(3) μC/OS-II 的调度机制

在移植入μC/OS-II 的系统中，已经准备就绪的高优先级任务可以剥夺正在运行的低优先级任务的 CPU 使用权，只要把数据处理程序的优先级设定的高一些，并在中断服务程序中使它进入就绪态，中断结束后数据处理程序就会被立即执行，可以把中断响应时间限制在一定的范围内，保证系统的实时性。

内核的核心任务是任务调度机制。在μC/OS-II 中，一个任务通常是一个无限循环，一个任务就像其他 C 函数一样，而且没有返回任何的数据。

μC/OS-II 下每个任务可以有如下五种状态：

①休眠态(dormant):指任务驻留在程序空间中，还没有交给内核管理

②就绪(Ready):当任务一旦建立，这个任务就处于就绪态准备运行

③运行(Running):准备就绪的最高优先级的任务获得 CPU 的控制权，从而处于运行态

④等待或挂起(Pending):正在运行的任务由于调用延时函数或等待事件信号量的来临而将自身挂起，因而处于等待或挂起态

⑤中断态(Interrupt):正在运行的任务可以被中断，除非是该任务将中断关闭。被中断的任务进入中断服务程序(ISR)。如果中断服务程序使一个更高优先级的任务准备就绪，这中断服务程序结束后，则更高优先级的任务开始运行程序

任务被创建后，状态用 8 位字节变量表示，目前只用低四位。如果某位置为 1，表示任务正在等待该位表示的事件；可以复合使用这些标志，表示任务在同时等待多个事件的发生；如果所有位均为 0，表示任务处于就绪状态，一旦优先级最高，即可投入运行。

μC/OS-II 是剥夺型实时多任务内核，优先级最高的任务一旦准备就绪，则拥有 CPU 的所有权，开始投入运行。每个任务的优先级不同且是唯一的，所以任务调度的工作是查找准备就绪的最高优先级的任务并进行上下文切换，进行任务调度。

某个任务在某端代码的执行期间不能被其他任务所抢占，可以调用函数来给调度器上锁以禁止调度，之后在调用开锁允许调度。

4.2.3 开发环境 ADS 开发套件简介

ADS(ARM Developer Suite)集成开发环境是 ARM 公司推出的 ARM 微控制器集成开

发工具，成熟版本是 ADS1.2。ADS1.2 支持 ARM10 之前的所有 ARM 系列微控制器，支持软件调试 JTAG 硬件仿真调试，支持 ASM、C、C++源程序，可以在 Windows98、WindowsXP、Windows2000 以及 Linux 上运行，具有编译效率高、程序库功能强等特点。

ADS1.2 集成开发环境包括：代码生成工具、集成开发环境、调试器、指令模拟器、ARM 开发包、ARM 应用库。用户一般直接操作的是 Code Warrior IDE 集成开发环境和 AXD 调试器。

(1) CodeWarrior IDE 简介

CodeWarrior IDE 集成开发环境集成 ARM 汇编器、ARM 的 C/C++编译器、Thumb 的 C/C++编译器、ARM 连接器、工程管理器、代码生成接口等。

CodeWarrior IDE 通过工程项目来组织用户的源文件、库文件、头文件以及其它的输入文件。这些文件可以按照某种逻辑关系进行分组，一个工程项目中还可以包含其它的子工程项目，一个工程项目中至少包含一个生成目标，每个生成目标定义一组选项，用于生成特定的目标文件。

(2) AXD 调试器简介

AXD(ARM Extended Debugger)为 ARM 扩展调试器，支持硬件仿真和软件仿真(ARMulator)。AXD 能够装载映像文件到目标内存，具有单步、全速、断点等调试功能，可以观察变量、寄存器和内存的数据。

AXD 是 ADS 的调试器，独立于 ADS，属于交叉编译器。运行在 Windows 操作系统下，为 ARM 目标板生成运行程序，包含下列基本调试功能。

①下载目标映像文件到系统中，如果目标系统支持，还可以将映像文件烧入到系统的 Flash 存储器中；

②在目标程序中设置断点，包括程序断点和数据断点；查看和修改断点处处理器状态，查看和修改断点处存储器内容，查看和修改目标程序中标量的值；

③单步执行目标程序，可以显示反汇编和源程序代码，可以调试 C 和 C++程序。

4.2.4 集中器硬件电路图

图 4.4 所示为集中器硬件电路图：

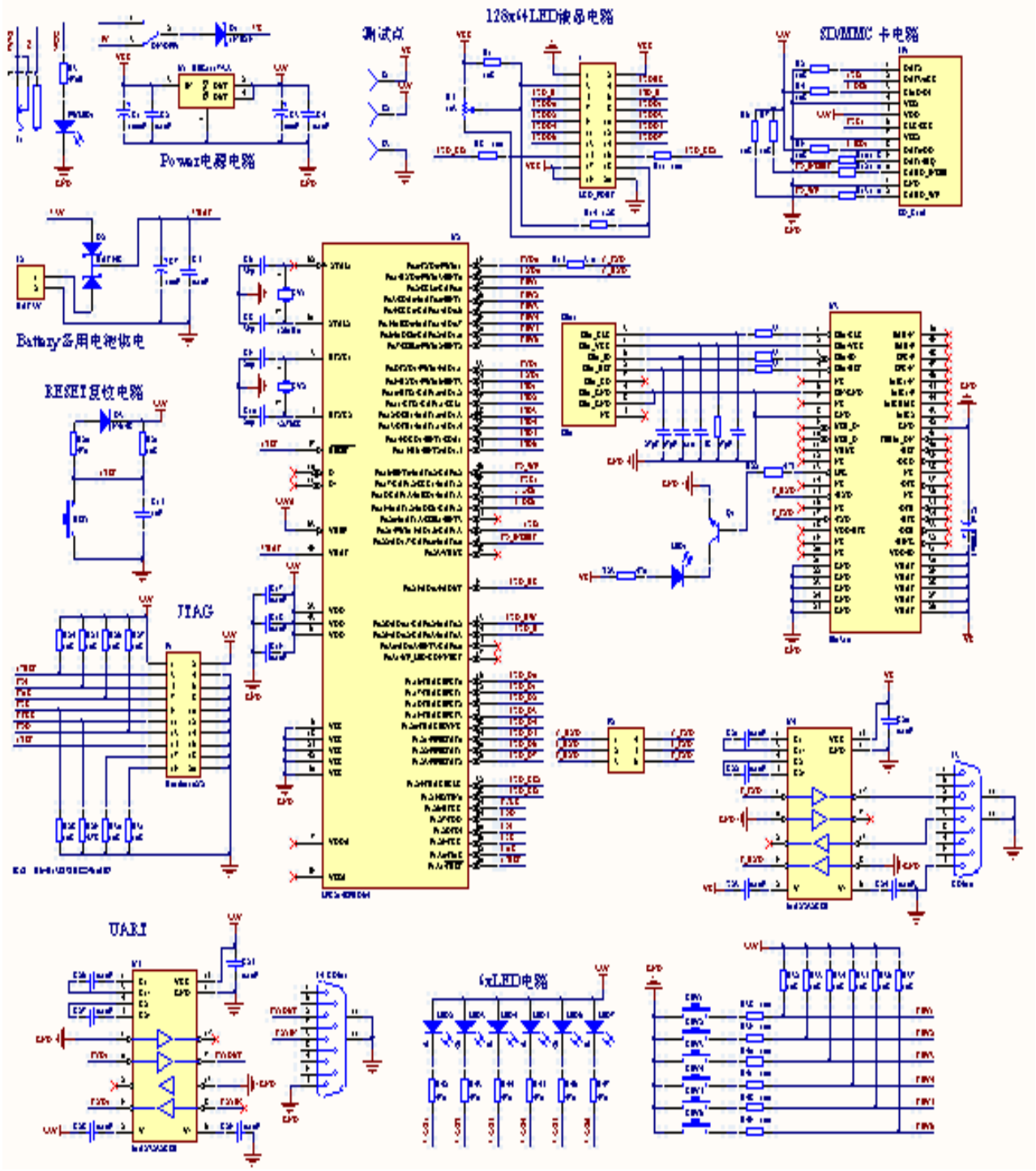


图4.4 集中器电路图

如图4.4所示为集中器硬件电路图，电源部分输入为5V电压，输出为3.3V给EM310供电，LPC2148通过TXD和RXD通过P2跳线分别跟EM310的TXD和RXD相连接，以使LPC2148单片机跟EM310模块进行通信。ARM7具有两个UART口，分别为UART0和UART1，,128*64液晶用来显示电表的数据，如：电压、电流等。

4.2.5 集中器 PCB 版图设计

PCB(Printed Circuit Board，印制线路板)设计是其从原理图变成一个具体产品必经的一道设计工序，其设计的合理性与产品生产及产品质量紧密相关。本设计中采用 Altium Designer 10 来完成电路的原理图设计和 PCB 设计。Altium Designer 10 是 Altium 公司开发的基于 Windows 环境下的电路板设计软件，该软件功能强大，人机界面友好，易学易用，是业界人士首选的电路板设计工具[24]。

(1) PCB 设计步骤

①确定 PCB 板的外形及尺寸。根据所设计的 PCB 在产品的位置、空间的大小、形状以及与其它部件的配合来确定 PCB 的外形与尺寸。在 MECHANICAL LAYER 层用 PLACETRACK 命令画出 PCB 的外形。

②制作元器件封装。在 PCB 设计过程中如果使用一些元器件库中不存在的特殊器件，例如本采集器 PCB 设计中用到的 LPC2148 芯片和 EM310 无线模块，则在布局之前需先进行这些元器件封装的制作。

③布局及布线。元器件封装制作完成后，在线路板上对元器件进行布局及布线，这是 PCB 设计的主要工作，将在下面重点介绍。

④检查。这一方面包括电路原理的检查，另一方面还必须检查相互间的匹配及装配问题。电路原理的检查可以人工检查，也可以采用网络自动检查(原理图形成的网络与 PCB 形成的网络进行比较即可)。

(2) 元器件的布局

由于 SMT(Surface Mounted Technology，表面贴装技术)一般用回流焊来实现元器件的焊接，因而元器件的布局影响到焊点的质量，进而影响到产品的成品率。而对于射频电路 PCB 设计而言，电磁兼容性要求每个电路模块尽量不产生电磁辐射，并且具有一定的抗电磁干扰能力，因此，元器件的布局还直接影响到电路本身的干扰及抗干扰能力，这也直接关系到所设计电路的性能。因此，在进行射频电路 PCB 设计时除了要考虑普通 PCB 设计时的布局外，主要还须考虑如何减小射频电路中各部分之间相互干扰、如何减小电路本身对其它电路的干扰以及电路本身的抗干扰能力。根据经验，射频电路效果的好坏不仅取决于射频电路板本身的性能指标，很大部分还取决于与 CPU 处理板间的相互影响，因此，在进行 PCB 设计时，合理布局显得尤为重要。

元器件应尽可能沿一方向排列，通过选择 PCB 进入熔锡系统的方向来减少甚至避

免焊接不良的现象：根据经验元器件之间最少要有 0.5mm 的间距才能满足元器件的熔锡要求，若 PCB 板的空间允许，元器件的间距应尽可能宽。对于双面板一般应设计一面为 SMD(Surface Mounted Devices，表面贴装元件)元件，另一面则为分立元件。在布局中应注意：

①首先确定与其它 PCB 板或系统的接口元器件在 PCB 板上的位置，必须注意接口元器件间的配合问题(如元器件的方向等)。

②因为线路板体积很小，元器件间排列很紧凑，因此对于体积较大的元器件，必须优先考虑，确定出相应位置，并考虑相互间的配合问题。

③认真分析电路结构，对电路进行分块处理(如电源电路、无线通信电路、存储器电路等等)，尽可能将强电信号和弱电信号分开，将数字信号电路和模拟信号电路分开，完成同一功能的电路应尽量安排在一定的范围之内，从而减小信号环路面积；各部分电路的滤波网络必须就近连接，这样不仅可以减小辐射，而且可以减少被干扰的几率，提高电路的抗干扰能力。

④根据单元电路在使用中对电磁兼容性敏感程度不同进行分组。对于电路中易受干扰部分的元器件在布局时还应尽量避开干扰源(比如来自数据处理板上 CPU 的干扰等)。

(3) 元器件的布线

在基本完成元器件的布局后，就可开始布线了。布线的基本原则为：在组装密度许可情况下后，尽量选用低密度布线设计，并且信号走线尽量粗细一致，有利于阻抗匹配。对于射频电路，信号线的走向、宽度、线间距的不合理设计，可能造成信号传输线之间的交叉干扰；另外，系统电源自身还存在噪声干扰，所以在设计射频电路 PCB 时一定要综合考虑，合理布线。在布线时要注意：

①所有走线应远离 PCB 板的边框(2mm 左右)，以免 PCB 板制作时造成断线或有断线的隐患。电源线要尽可能宽，以减少环路电阻，同时，使电源线、地线的走向和数据传递的方向一致，以提高抗干扰能力；所布信号线应尽可能短，并尽量减少过孔数目；各元器件间的连线越短越好，以减少分布参数和相互间的电磁干扰；对于不相容的信号线应尽量相互远离，而且尽量避免平行走线，而在正向两面的信号线应相互垂直；布线时在需要拐角的地址方应以 135°角为宜，避免拐直角。

②与焊盘直接相连的线条不宜太宽，走线应尽量离开不相连的元器件，以免短路；过孔不要画在元器件上，且应尽量远离不相连的元器件，以免在生产中出现虚焊、连焊、短路等现象。

④在射频电路 PCB 设计中，电源线和地线的正确布线显得尤其重要，合理的设计是克服电磁干扰的最重要的手段。PCB 上相当多的干扰源是通过电源和地线产生的，其中地线引起的噪声干扰最大。采集终端的 PCB 布局布线图如图 4.5 所示。

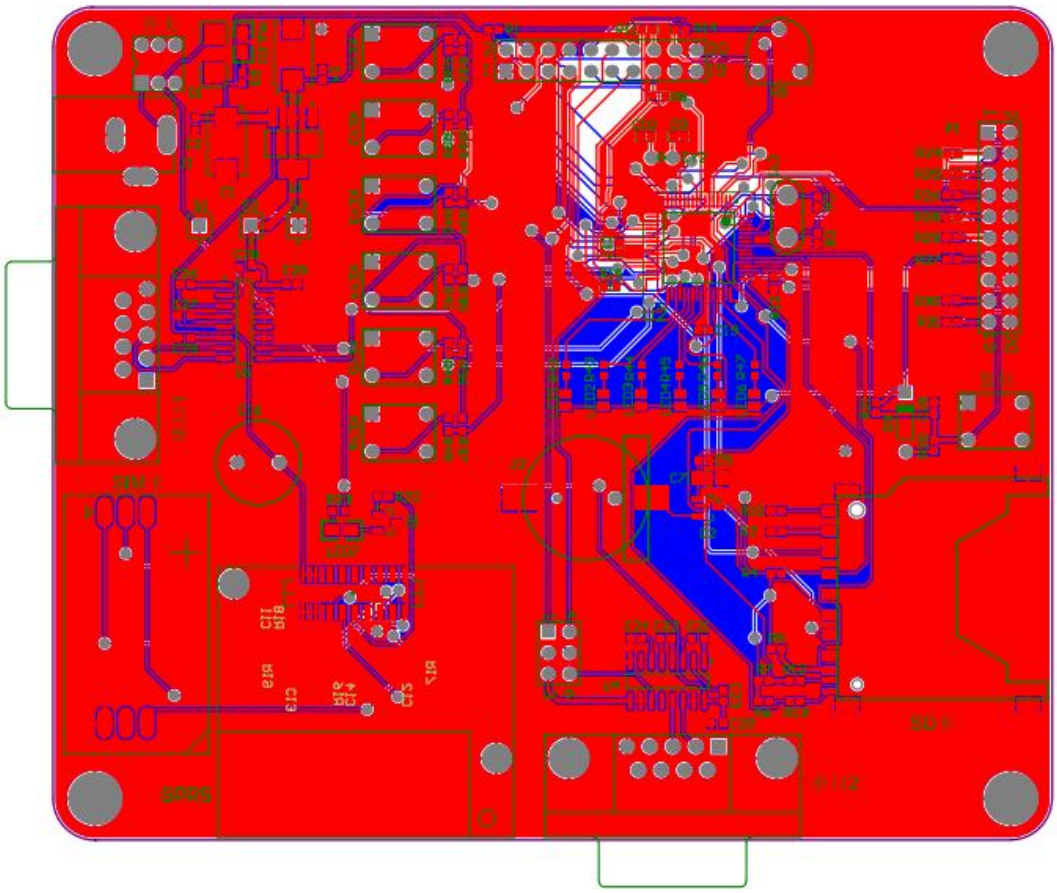


图 4.5 集中器 PCB 版图

4.2.6 集中器性能指标

输入电压：5-12V
输入电流：2A
输出电压：5V
输出电流：2A
工作频率：50Hz
串口速率：9600bps
丢包率：<5%
延迟时间：<2s
无线通信：GPRS
485 通信：MODBUS TCP/IP

4.3 本章小结

基于 GPRS 的集中器硬件设计，主要是从电路设计入手，通过 PCB 设计，到实现电路板的制作，搭建出一个硬件平台通过实验测试来达到预期的结果。在测试中发送短消息中发送成功率达到 60%以上。但发送出现延迟或失败现象，其主要集中在下午 6 点以后，由于发送短消息的太多，导致 GPRS 网络拥塞，出现发送延迟和丢包现象。由实时性实验结果的数据表明，短消息的发送、接收及与网络连接的延迟的耗时小于 5 秒。性能分析、实验结果和实际的使用效果比较令人满意符合系统设计的性能要求，满足实际使用的需求。

5 集中器软件设计

5.1 系统软件设计概述

本系统中，根据功能要求必须要具备两个基本功能模块—GPRS模块-集中器与主站的通信和控制模块、电力载波-后台与集中器的通信和采集模块。因为集中器的核心是由三部分组成的：通信、控制、采集。保证集中器管理多个用户载波抄表器电度表，并与之通信，获得电度表读数和传动控制电表电源的指令，同时与管理中心通信，向管理中心传送用户电表读数，接收控制中心对用户电表下达的指令，起承上启下的作用，便于装置做出可靠地决策。而流程反应了集中器流程控制的基本过程，它贯穿综合控制过程中的各个环节，是装置执行的基本保证[15]。

5.2 集中器与主站通信之间的软件设计

5.2.1 μC/OS-II 的移植

在实时操作系统移植中，主要完成数据类型的重定义、堆栈结构的设计、任务切换时的状态保存与恢复等工作[16]。

(1)数据类型的重定义

μC/OS-II 不使用 C 语言中的 short、int、long 等数据类型的定义、它们与处理器类型有关，隐含着不可移植性强的数据类型，直观又可移植，不过这就成为必须移植的代码。数据类型重定义为：

```
typedef      unsigned char          BOOLEAN ;     /*布尔变量*/
typedef      unsigned char          INT8U;        /*无符号 8 位整形变量*/
typedef      signed char            INT8S;        /*有符号 8 位整型变量*/
typedef      unsigned short         INT16U;       /*无符号 16 位整型变量*/
typedef      signed  short          INT16S;       /*有符号 16 位整型变量*/
typedef      unsigned int           INT32U;       /*无符号 32 位整型变量*/
typedef      signed  int            INT32S;       /*有符号 32 位整型变量*/
typedef      float                  FP32;         /*单精度浮点数 32 位长度*/
typedef      double                 FP64;         /*双精度浮点数 64 位长度*/
```

(2)堆栈结构的设计

当统一操作系统应用于不同的处理器时，由于各个应用系统所追求的性能特点不同，这就要求堆栈结构的设计与本系统追求的性能一致，uC/OS-II 使用常量

OS_STK_GROWTH 中指定堆栈的生长方式，置 0 表示堆栈从下往上；置 1 表示堆栈从上往下[17]。

ARM 处理器核对于两种方式均支持，但 ADS 的 C 语言编译器仅支持一种方式，即从上往下长，并且必须是满递减堆栈，因此在本移植代码中 OS_STK_GROWTH 为 1. 代码实现为：#define OS_STK_GROWTH 1[18]。

(3)任务切换时的状态保存与恢复

任务切换时的状态保存与恢复是实时多任务操作系统的主要任务，是操作系统正常运行的前提。系统采用的 ARM7 芯片，其具有两个指令集，任务可以应用系统模式和用户模式，组合起来有 4 种方式，为使底层接口与处理器状态无关，并且调用相应切换函数时不需要知道函数的位置，移植代码将使用软中断指令 SWI 作为底层接口，以不同的功能号区分不同的函数[19]。

```
__swi(0x00)void OS_TASK_SW(void);       /*任务级任务切换函数*/
__swi(0x01)void_OSStartHighRdy(void);    /*运行优先级最高的任务*/
__swi(0x02)void OS_ENTER_CRITICAL(void); /*关中断*/
__swi(0x03)void OS_EXIT_CRITICAL(void);  /*开中断*/
__swi(0x40)void *GetOSFunctionAddr(int Index); /*系统服务函数入口*/
__swi(0x41)void *GetUsrFunctionAddr(int Index); /*自定义服务函数入口*/
__swi(0x42)void OSISR Begin(void);              /*中断开始处理*/
__swi(0x43)void OSISRNeedSwap(void);            /*判断中断是否需要切换*/
__swi(0x80)void ChangeToSYSMode(void);      /*任务切换到系统模式*/
__swi(0x81)void ChangeToUSRMode(void);     /*任务切换到用户模式*/
__swi(0x82)void TaskIsARM(INT8U prio);      /*任务代码是 ARM 代码*/
__swi(0x83)void TaskIsTHUMB(INT8U prio);   /*任务代码是 THUMB*/
```

移植代码的功能是解决 uC/OS-II 在 ARM7 应用中存在的上述三个问题，部分代码采用 C 语言实现，部分代码采用汇编语言实现，具体工作如下[20]：

①OS_CPU_A.ASM 编写四个汇编语言的函数；

OSStartHighRdy():调度执行最高优先级任务；

OSCtxSw(): 通过软件中断切换任务；

OSIntCtxSw(): 清理任务堆栈，使被中断任务堆栈结构满足系统需要；

OSTickISR(): 使能系统时钟节拍中断功能。

②OS_CPU_C.C 需要用 C 语言编写六个函数；

OSTaskStkInit(): 初始化堆栈函数；

OSTaskCreateHook(): 任务建立中重新定义 hook 函数；

OSTaskDelHook(): 任务删除重定义 hook 函数；

OSTaskSwHook(): 任务切换重定义 hook 函数；

OSTimeTickHook(): 时钟节拍重定义 hook 函数[21]。

5.2.2 集中器中 GPRS 通信流程图

软件设计方面主要对 GPRS 管脚功能有所了解，并且要对 AT 命令有所了解这样才能激活 GPRS 模块，才能实现数据的收发如图 5.1 所示[22]：

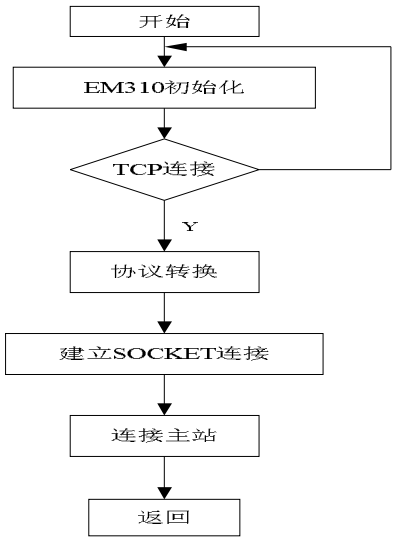


图 5.1 GPRS 模块工作流程图

如图 5.1 所示，GPRS 无线数据终端上电或复位后，首先等待参数配置命令。如果收到配置命令，则进入配置状态；否则读取片内 Flash 中保存的配置信息。接着通过串口向 GPRS 无线模块发送相应的 AT 指令，GPRS 终端开始进行拨号和 TCP 连接过程。当 TCP 连接成功，无线模块登录网络成功后，系统通过加在 PPP/TCP/UDP/IP 等协议，同主站建立起 SOCKET 连接，数据的双向传输通道建立，系统进入发送、接收用户数据[23]。

5.2.3 集中器与主站之间通信协议解析

集中器上行通信协议首先要从数据帧接收开始，从图 5.3 所示可以发现数据帧的正确接收要经过对上通讯任务，数据帧接收是以最小帧单元的长度为基础，不断接收，再根据协议中的长度解析，最终确定帧的长度，从而找到主站发送的数据帧，完成集中器跟主站之间的上行通信。流程图如图 5.2 所示[24]：

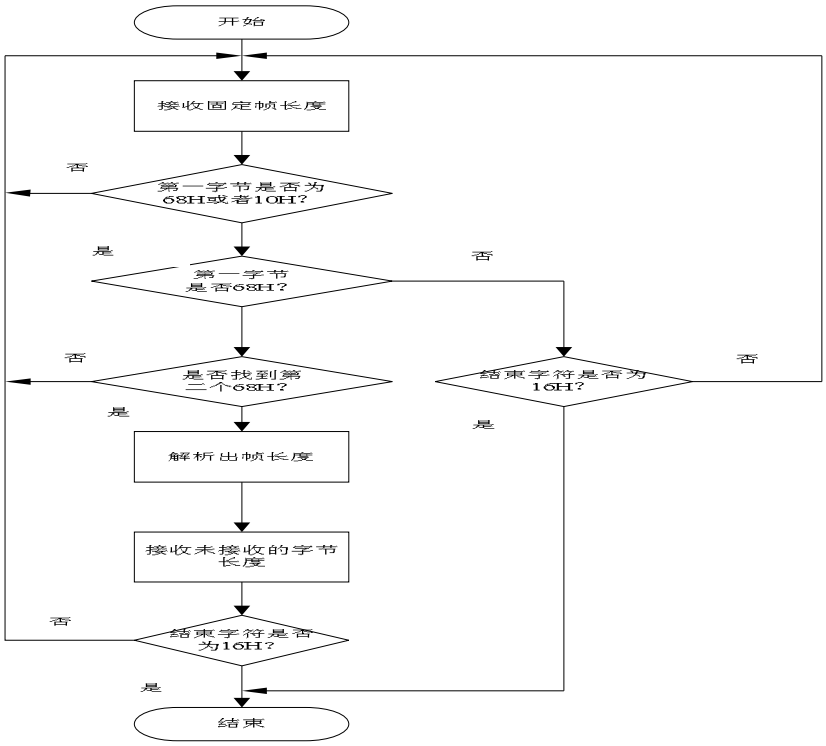


图 5.2 数据帧接收流程图

当数据接收结束时，把收到的数据帧交给解析任务，协议解析任务则分为变帧接受判断、固定帧接收判断、可变帧解析和固定帧解析。可变帧接收判断和固定帧接收判断主要负责是否是完整的帧，判断其帧头完整、帧尾完整等基本信息。流程图如图 5.3 所示[25]：

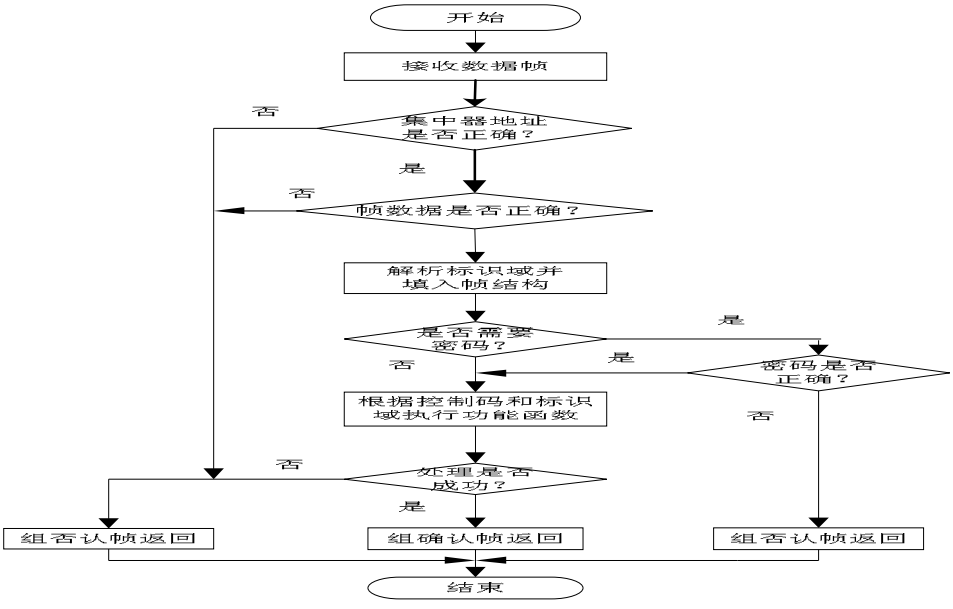


图 5.3 数据帧解析流程图

5.2.4 集中器与电表之间的通信

集中器与电能表之间交换数据遵守 DLT645-2007 多功能电能表通信协议。该规约是我国电力行业的标准，该规约的制定是为了统一和规范多功能电能表的费率装置与数据终端设备进行数据交换时的物理连接和协议，是自动抄表系统实现的协议基础。该规约适用于本地系统中多功能电能表的费率装置与手持单元(HHU)或其它数据终端设备进行点对点的或一主多从的数据交换方式，规定了它们之间的物理连接、通信链路及应用技术范围[26]。

多功能电能表通讯规约的帧格式

帧是传送信息的基本单元。无论是主站请求数据，还是从站应答数据，都严格遵循数据帧格式。多功能电能表通讯规约中的数据帧格式如表 5.1 所示[27]。

表 5.1 多功能电能表通讯规约中的数据帧格式

说　　明	代　码
帧起始符	68H
地址域	A0
	A1
	A2
	A3
	A4
	A5
帧起始符	68H
控制码	C
数据域长度	L
数据域	DATA
校验码	CS
结束符	16H

终端节点程序流程

TCC081C 第一次上电后发将按照四种串口通信速率向从节点按顺序发送三种读地址命令。

读地址命令：

(1)DL/T645-07 全 AA 通配符读地址 68 AA AA AA AA AA AA 68 13 00 DF 16H

(2)DL/T645-97 全 99 广播（GB）读地 68 99 99 99 99 99 99 68 01 02 65 F3 C1 16H

(3)DL/T645-97 全 AA 通配符读地址 68 AA AA AA AA AA AA 68 01 02 65 F3 27 16H

串口通信速率：1200bps、2400bps、4800bps、9600bps；具体流程图如图 5.4 所示：

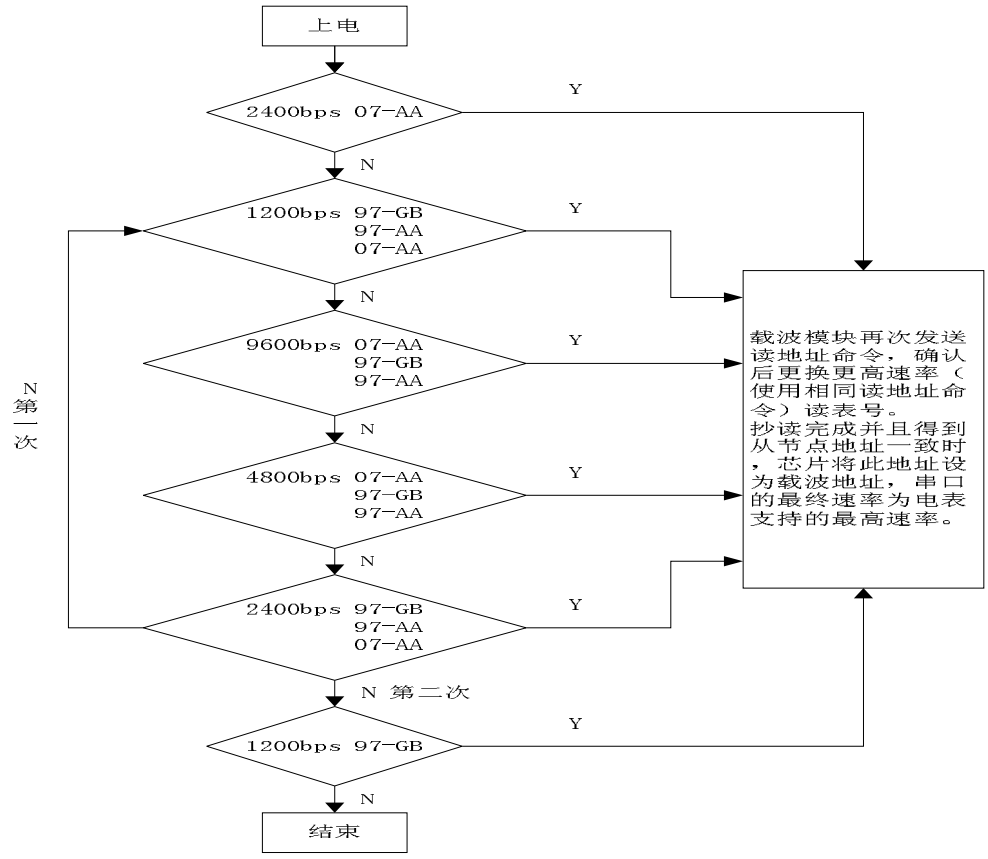


图 5.4 第一次上电读表号流程图

在往后的上电过程中，TCC081C 将按记录的串口通信速率发送记录的相应规约的读地址命令：如果返回的从节点地址和 TCC081C 记录的载波通信地址一致时，芯片立即进入正常工作状态；当两个地址不一致时，TCC081C 会重新进行上电读表号流程。

在下列两种特殊情况下，需要打断上电读表号过程而对 TCC081 进行载波通信地址和串口速率的设置，从而保证载波通信的正常进行[28]。

a)终端不支持上电读表号，且芯片默认的串口速率和实际通信速率不符；

b)终端支持上电读表号，但用户电表没有表号（即 6 个字节的 FFH）。

上电读表号时序和流程如图 5.5 所示：

TCC081C 上电 2s 后将进入上电读表号过程。TCC081C 向串口下发读表号命令后，从节点的响应延迟需大于 20ms，且响应必需在 500ms 内完成，随后 TCC081C 将下发下一条上电读表号命令，直至整个读表号过程结束。每条读从节点地址的命令在响 TCC081C 时不需要额外增加延时，否则可能造成上电读表号通信失败。

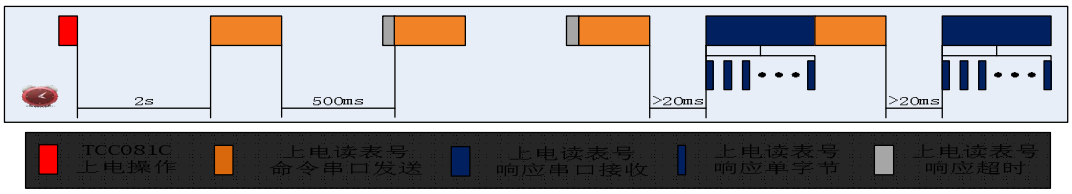


图 5.5 上电读表号时序图

单相抄读工作时序如图 5.6 所示：

TCC081C 向串口转发命令后，节点收到命令后的响应需在 1.2s 时间内回完。但在 500ms 内 TCC081C 未收到响应的第一个字节，则 TCC081C 串口等待超时。如 TCC081C 打开了额外延时，响应可延长在 4.2s 时间内回完，TCC081C 串口等待超时也延长到 3.5s。串口接收 DL/T645 规约响应，如果响应帧长度大于 12 字节时，TCC081C 将同时启动载波发送。

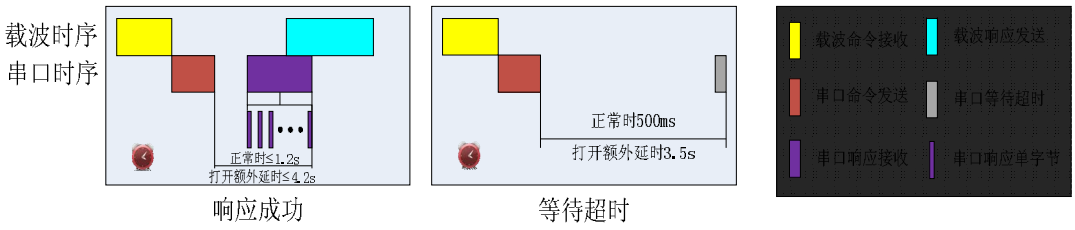


图 5.6TCC081 单向工作时序图

5.3 本章小结

本章主要讲述了集中器软件设计的流程以及集中器与主站之间的通信协议解析过程，集中器与电表之间的数据采集过程，以及传输集中器与主站和电表之间数据的传输过程。

6 集中器的测试与实现

6.1 集中器硬件测试

系统硬件都连接好后，开始进行系统测试，以看看系统设计是否一切功能正常，符合设计要求。

6.1.1 EM310 GPRS 模块的测试

下面是对 EM310 的 GPRS 数据传输测试：

在进行 GPRS 数据传输之前必须对 EM310 进行测试，检查 EM310 设备是否正常。先运行 EM310 专用工具（如图 6.1）：

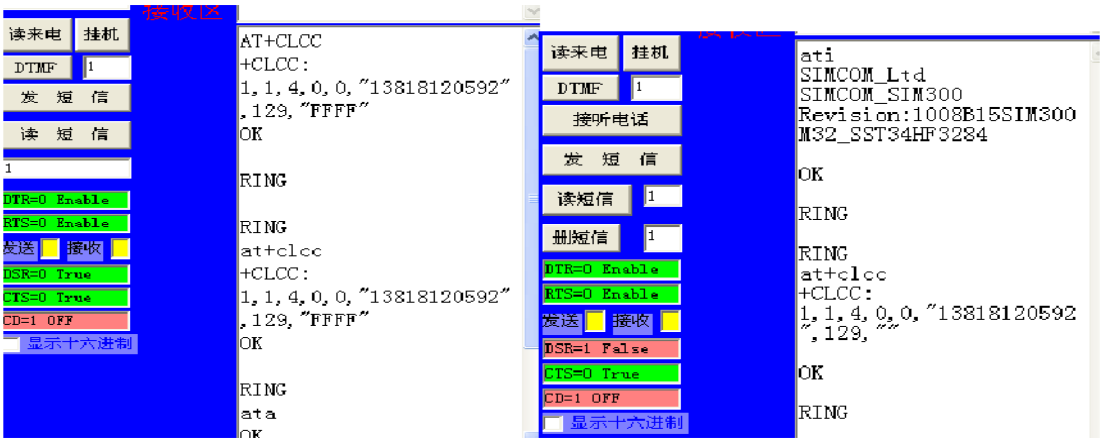


图6.1 运行EM310工具

将串口数据传输率设为9600bps，打开端口，再进行EM310设备初始化。

1、点"设备初始化" 软件会自动向模块发初始化指令,如果成功后,接收区会显示如下:

ATI

SIMCOM_Ltd

SIMCOM_SIM300

Revision:1604B09SIM300M32_SST34HF3284

OK

这说明一切正常。

2、检查SIM卡状态.点“SIM 卡”键,如果返回代码是

AT+CPIN?

+CPIN: READY

OK

说明运行正常。

如果显示是其他状态时,就要检查SIM卡是否插好,重新插好再进行上述操作。

3、信号和注册状态查询, 点“信号”如果返回代码是

AT+CSQ;+CREG?

+CSQ: 18,0 信号值18

+CREG: 0,1 已注册成功还有一个+CREG: 0,5 其它说明没有注册上去

OK

这说明系统一切正常[29]。

6.1.2 LPC2148 与 GPRS 模块通信测试

如图 6.2 所示 LPC2148 通过和 GPRS 模块连接对其进行控制，通过发送 AT 命令对其进行操作和控制，完成集中器与主站的通信。通过单片机发送 AT 指令，GPRS 模块收到后返回 OK[30]。

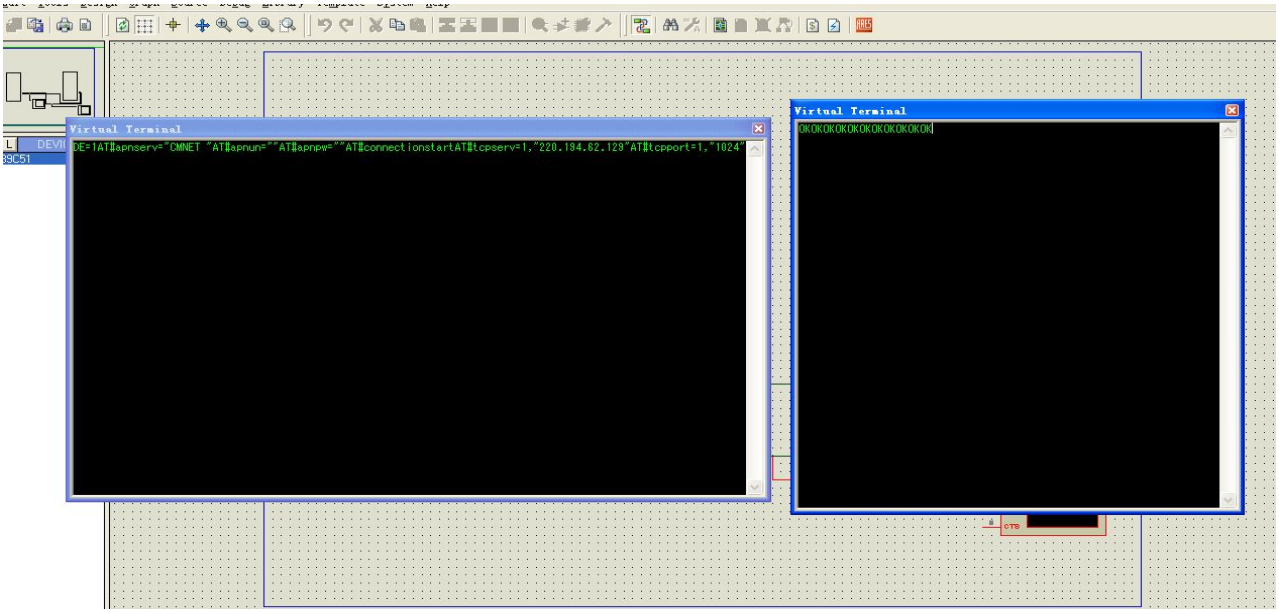


图 6.2 集中器控制 GPRS 仿真图

仿真结果表明：LPC2148 单片机通过发送 AT 指令来对 GPRS 模块进行操作和控制，完成单片机数据的发送和传输,但是在数据传输的时候有延迟，通过测试一般延迟时间为 1-2s,满足延迟的性能指标。

6.2 系统的软件测试与实现

6.2.1 连接测试

打开超级终端，利用 AT 命令设置 GPRS 模块，将 GPRS 挂到网络上，开通集中与主站之间的通道，以保证集中器与主站之间的数据传输[31]。如图 6.3 所示：

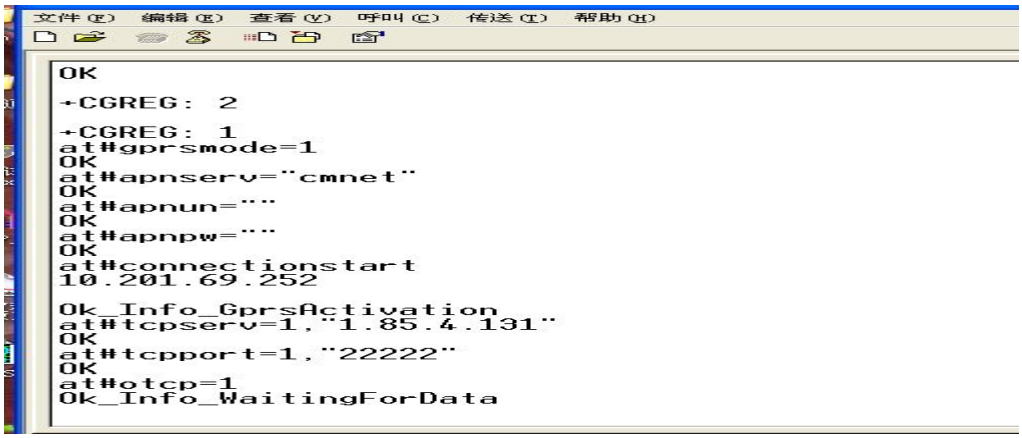


图 6.3 GPRS 模块连接到网络

表 6.1 通过测试 GPRS 与网络连接时的丢包率

8:30—10:00	丢包率约为4%	用户量非常少，丢包率非常小，吞吐量大
10:00—11:00	丢包率约为8%	用户量较小，丢包率较小，吞吐量较大
11:00--13:00	丢包率约为10%	用户量较多，丢包率较高，吞吐量较小
14:00--16:00	丢包率约为7%	用户量较小，丢包率较小，吞吐量较大
18:30—20：30	丢包率约为20%	用户量大，丢包率高，吞吐量小

6.2.2 通信数据传输测试

在我的计算机里面输入对方 IP 地址 1.85.4.131 和对方端口号 22222 点击连接 GPRS 模块就可以与主站进行通信测试如下图 6.4 所示[32]：

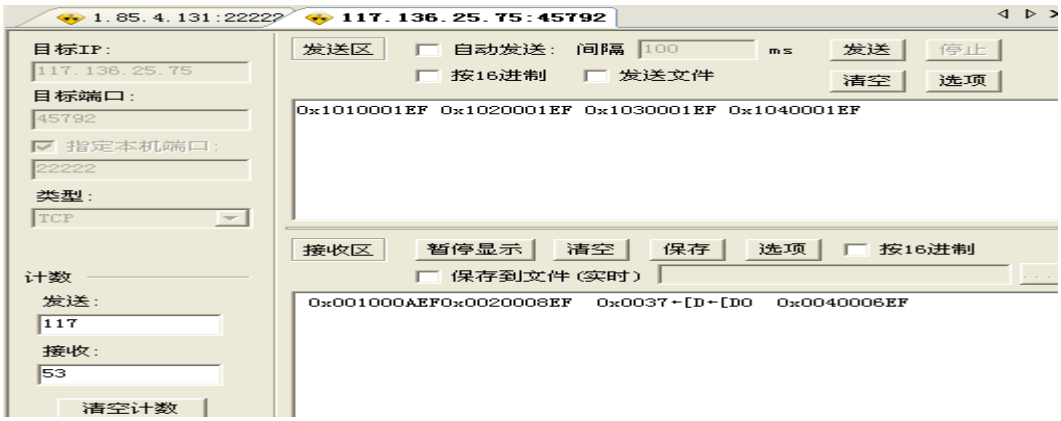


图 6.4 主站与集中器进行数据传输

测试结果表明：通过集中器与主站之间的数据传输，经过大量的测试，其中传输 20 个数据，大约会有 1 个出错，出错率约为 5%，属于正常的指标返回内，网络延迟约为每 100 个数据延迟大约 0.3 秒，符合延迟指标。

6.2.3 集中器采集与传输数据实现

对遵循 ModBus 协议的虚拟电表进行定时采集，并回传采集到的数据值上位机进行显示[33]。

如图 6.5 所示分别在虚拟电表端输入三相电压为 A：1V；B：2V；C3C；三相电流 A：4A；B：5A；C：6A。则在相应的采集器端将会收到电表的度数为三相电压为 A：1V；B：2V；C：3V；三相电流 A：4A；B：5A；C：6A；电能为 18888。

图 6.5 主站显示的电表数据

测试表明：集中器与电表之间的数据采集过程，以及传输集中器与主站和电表之间数据的传输过程，完成集中器与主站之间的数据传输，集中器与电表之间的数据采集，并在主站进行显示。性能分析、实验结果和实际的使用效果基本满意，符合系统设计的基本性能要求，满足实际使用的基本需求[34]。

6.3 集中器在校园中的应用

未来打算将集中器应用于高新学院的宿舍楼和教学楼中来管理和监测整栋楼的用电量情况，表 6.2 为变压器主要分布情况。

表 6.2 变压器分布情况

1#变压器　630KVA（集中器 1）	2#变压器　315KVA（集中器 2）	3#变压器　630KVA（集中器 3）
北区 1#公寓楼（分表 1）	北区 2#公寓楼（分表）	南区 1#教学楼（分表）
北区 3#公寓楼（分表）	6#基建楼（分表）	南区 2#教学楼（分表）
北区 1#教学楼（分表）	变频水泵房（分表）	南区 1#公寓楼（分表）
北区锅炉房（分表）		南区 2#公寓楼（分表）
学生第二食堂（分表）		南区 3#公寓楼（分表）
金工实习车间（分表）		南区 4#公寓楼（分表）

目前已经将集中器应用与南区 1#宿舍楼和南区 1#教学楼用于试点，本论文取南区 1#宿舍楼作为监测点如图 6.6 所示：

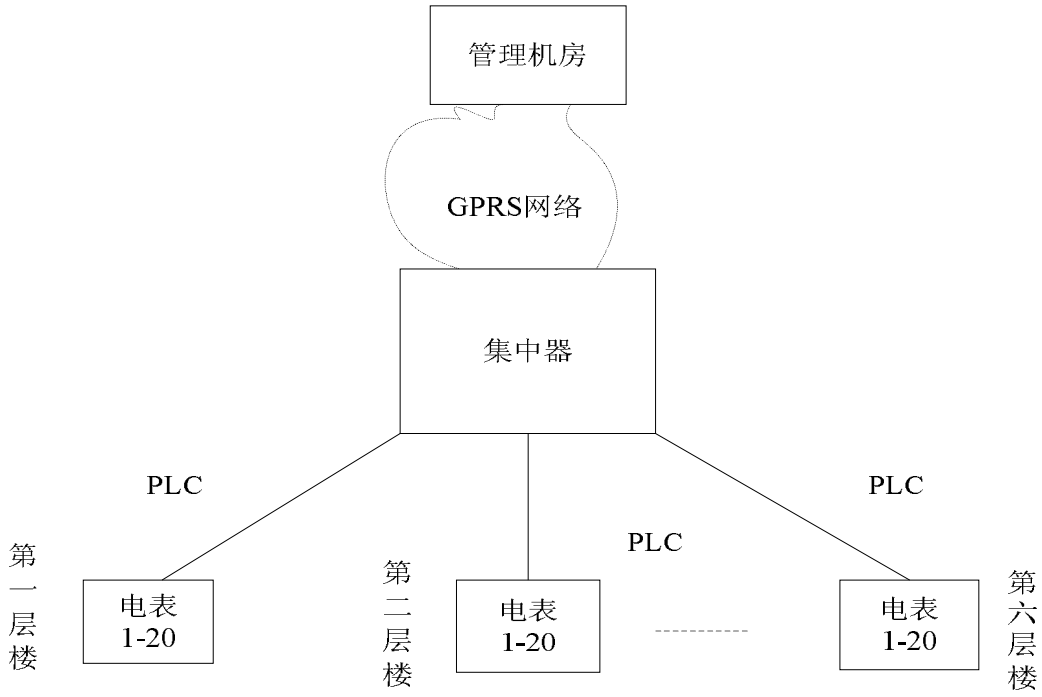


图 6.6 南区 1#宿舍楼无线抄表系统框图

图 6.7 为南区 1#宿舍楼第二层所有智能电表

图 6.7 南区 1#宿舍楼第二层所有智能电表

选取南区 1#宿舍楼二层的电表作为被测对象选取第五个表的电量度数，将当前的电量发送给集中器端并在集中器中显示出来如图 6.8 所示

图 6.8 集中器采集到第五个表的电量读数

通过实际操作测试能得到一些数据如：第 2 层宿舍楼的第 5 个表的在 10:53:38 的用电量为 2.18kw，完成了电表数据的读取，并能在主站对齐进行显示。将集中器用于南区 1#宿舍楼的电量管理上，可以实时的管理各个宿舍以及整个楼的用电情况，能准确的检测出各个时间段的峰值功率和实时电量，统计出哪个时间段的用电量最大，哪个时间段的的用电量最小，当发现哪个宿舍有大功率用电情况时及时对其进行断电，另外能统计出每个月整栋楼的所有用电量和功率，也估算出电量的损耗情况，能对其进行有效的管理。与传统的人工抄表相比，它组网灵活，成本低廉，消除了开槽、穿墙等繁琐的工作程序。

6.4 本章小结

本章主要完成集中器的硬件测试以及软件测试，最终完成集中器的实现，主演完成了集中器与主站之间的数据传输，集中器与电表之间的数据采集，通过实地测试能得出各个用户各个时间段的用电情况，将其用于校园电表管理中能对校园的用电情况进行有效地管理。

7 总结与展望

7.1 全文总结

随着国民经济的发展、人民生活水平的提高和房地产产业的迅速发展，居民住宅的质量和档次越来越高，住户对住宅环境、物业管理水平、数字信息化水平的要求也日益提高，传统的人工抄表方式已经远不能满足当今社会需求，因此国内很多城镇逐步出现了以计算机为基础的自动抄表系统取代传统的人工抄表[35]。本文应用 GPRS 无线技术、嵌入式技术以及网络编程技术，针对目前的智能抄表网络设计了一个基于 GPRS 的数据集中器，并把其应用在校园网中的一些地方用于对校园的电量进行智能化管理。本文所做工作如下：

(1) 集中器硬件电路设计

对集中器功能进行分析，通过各种方案对比选择一个较为理想的方案进行设计，对齐内部硬件组成部分进行了分析和设计，通过对其性能指标的设定，对硬件电路进行了测试，搭建出一个硬件测试平台，最后完成集中器硬件电路的设计过程。

(2)对硬件电路进行了 PCB 版图的绘制

首先确定 PCB 板的外形及尺寸。根据所设计的 PCB 在产品的位置、空间的大小、形状以及与其它部件的配合来确定 PCB 的外形与尺寸，其次进行元器件封装，第三步进行 PCB 布局和布线，最后检查电路原理图，完成 PCB 版图的制作。

(3)对集中器进行软件设计

首先进行集中器与主站之间的通信协议设计，通过对 MODBUS 协议进行分析，设计出一个上行通信协议，完成集中器与主站之间的通信；下行通过对 DLT645-2007 规约进行分析和研究，设计一个下行通信协议来完成集中器与电表之间的数据采集。

(4)对集中器进行软件测试

通过利用软件对集中器的各种性能进行测试，最终达到设计的目的

(5)将集中器应用在校园中

目前已经将集中器应用在高新学院的一些宿舍楼中，对学生宿舍楼的用电量进行有效的智能化管理。

7.2 工作展望

基于 GPRS 的通用数据集中器的研究设计是一件非常有意义的工作，之得我们进行下一步的研究。由于集中器设备大多数是由厂商生产，而厂商为减少成本，会尽可能减少硬件成本，这对集中器的发展带来制约因素。硬件改进将会影响到软件的改进，软硬

件是不可分割的，要不断对其方案进行完善与进一步的研究：

(1) 增加以太网接口

在集中器设计中，可以给集中器增加以太网通信方式，既可以提高主站和数据终端之间通信稳定性，又能增加主站和集中器之间进行大量数据传输的可能性。这将对集中器上行通信协议提出更高的要求，而集中器上行通信协议为适应以太网，也会有更多的更改，远程升级速度会更快，更加可靠。

(2)进一步对硬件电路方面进行更加深入的研究，这才是做好集中器工作的根本。

(3) 本无线采集系统的功能还有待进一步扩充，如通过上位机操作主动采集，电路布局和抗干扰方面还有很大的提升空间。

参考文献

[1] 范闻博，姚远，张其善.基于 GPRS 的数据采集远程网络监控系统的设计.无线电工程，2005(1):21-24

[2] 蔡锐丹，许少云，甘义成.GPRS 无线数据传输系统的设计.电子质量， 2004(1):19-21

[3] 文志成.通用分组无线业务—GPRS.北京：电子工业出版社，2004

[4] 王红红，李仁俊.远程自动抄表系统中的通信方式.电力系统通信， 2003(11):47-50

[5] 蔡锐丹，许少云.GSM/GPRS 通信在配电自动化系统中的应用.电子应用技术，2004(3):66-70

[6] 何小荣，钱清泉，陈维荣.GPRS 在工业监控中的应用.铁道机车车辆，2004,24(1):20-22

[7] GSM 03.60: Digital cellular telecommunications system(Phase 2+)；General Packet Radio Service(GPRS)；Service description；Stage 2(version 7.3.0 Release 1998)

[8] Adrian Burian.GPRS Radio Interface:Medium Access Control details in GPRS.Signal Processing Laboratory,Tampere University of Technology

[9] Roger Kalden.Ingo Meirick and Michael Meyer.Wireless Internet Access Based on GPRS,Ericsson Research.Ericsson Eurolab Deutschland

[10] Xavier Lagrange 等著.GSM 网络与 GPRS.顾肇基译.北京：电子工业出版社,2002

[11] Juan Li.LINK ADAPTATION IN GENERAL PACKET RADIO SERVICE (GPRS). Helsinki University of Technology

[12] 任子真.王洋.李琳 基于 GPRS 的智能电表的设计 2007

[13] 田泽.嵌入式系统开发与应用[M].北京:北京航空航天大学出版社,2005.05

[14] Jean J.Labrosse 著，邵贝贝译.嵌入式实时操作系统 uC/OS-II[M].北京:北京航空航天大学出版社,2005.06

[15] 吕晶.基于 ARM 的无线 GPRS 电力负荷控制系统[D].西安：西安电子科技大学，2007.0 王兴杰.李允.江浩.李涛. 基于 Linux 嵌入式交叉开发技术 2008(1)

[16] T.Sridhar 著,彭甫阳译.嵌入式通信软件设计[M].北京:北京航空航天大学出版社,2004.11

[17] 李莉.基于 ARM 处理器和嵌入式实时操作系统的数据采集装置设计[D].太原:太原理工大学,2006.04

[18] 杨法 嵌入式系统中 Bootloader 的编译与移植 2007(1)

[19] 梁联冠.冯太合.陈立定.谢青延 嵌入式 Linux 文件系统的研究与应用

[20] 金昆善，孙志毅等.单片机控制集中抄表系统[J].微计算机信息(嵌入式与 SOC),2005 年第 21 卷 11-2 期,20-22 页

[21] Tan,T.k.Embedded operating System Energy Analysis and Macro-modeling Computer Design.2002

[22] Payne J M, Parker D and Bradley R F. Rangefinder with fast multiple range capacity .Review of Science Instrument, 1992,63(6)

[23] Paker D H. A status report on the GBT laser demonstration at the 140 foot telescope. Report on the Green Bank Telescope of NRAO,1996-08-28

[24] Olav Queseth,etc.Algorithms for Link Adaption in GPRS.Sensors and Systems Royal Institute of Technology,Sweden

[25] The PPP internet protocol control protocol(IPCP)

[26] PPP internet protocol control protocol extensions for name server address

[27] 国标：DL/T 645-1997 《中华人民共和国电力行业标准 多功能电度表通讯规约》[S] 1998 年

[28] Roger.s.Pressman.软件工程[M].北京：电子工业出版社，2002 年

[29] Payne J M and Schiebel D. Slant range tests of ouadrant detector. Repont on the Green Bank Telescope of NRAD,1996-09-26

[30] 张靖武，周灵彬.单片机系统的 Proteus 设计与仿真.北京：电子工业出版社，2007.

[31] RF communication in a multi-user environment 2003

[32] David Seal.ARM Architecture Reference Manual,Second Edition[J].

[33] 范闻博，姚远，张其善.基于 GPRS 的数据采集远程网络监控系统的设计.无线电工程，34(1):21-24

[34] 唐枫.基于.NET 平台的动态信息发布系统[D].武汉理工大学，2006 年

[35] 吕晶.基于 ARM 的无线 GPRS 电力负荷控制系统[D].西安：西安电子科技大学，2007.01