智能电网终端通信方案及安全策略研究

技术总结报告

1. 项目概述

智能电网计划是国家电网公司2009年5月21日首次公布的，其内涵是以坚强网架为基础，以通信信息平台为支撑，以智能控制为手段，实现电力系统从发电、输电、变电、配电、用电和调度各个环节的智能感知、智能识别、智能控制的功能，实现“电力流、信息流、业务流”的高度一体化融合。智能电网中的每一个用户和节点都得到实时监控，通过电子终端将用户之间、用户和电网公司之间形成网络互动和即时连接，实现数据读取的实时、高速、双向的总体效果。智能电网可以整合系统中的数据，优化电网的管理，将电网提升为互动运转的全新模式，提高整个电网的可靠性、可用性和综合效率。

建立高速、双向、实时、集成的通信系统是实现智能电网的基础，没有这样的通信系统，任何智能电网的特征都无法实现。智能电网的数据获取、保护和控制都需要高速、可靠的通信系统的支持，因此建立安全快捷的通信系统是迈向智能电网的第一步。同时，要完成用户终端的智能控制，通信系统要和电网一样深入到千家万户，从而形成两张紧密联系的网络：电网和通信网络，以实现智能电网的建设目标。高速、双向、实时、集成的通信系统使智能电网成为一个动态的、实时信息和电力交换互动的大型的基础设施。当这样的通信系统建成后，它可以提高电网的供电可靠性和资产的利用率，繁荣电力市场，抵御电网受到的攻击，从而提高电网价值。

研究智能电网的通信平台和终端接入机制，需要兼顾现有条件、标准和应用需求。在这一技术领域主要有两个方面的技术需要重点关注，其一就是开放的通信架构，它形成一个“即插即用”的环境，使电网元件之间能够进行网络化的通信；其二是统一的技术标准，它能使所有的传感器、智能电子设备(IEDs)以及应用系统之间实现无缝的通信，也就是信息在所有这些设备和系统之间能够得到完全的理解，实现设备和设备之间、设备和系统之间、系统和系统之间的互操作功能。为此，研究用户终端的接入方案具有重要意义。面向用户终端的通信接入具有典型特征：节点众多，避免复杂布线；覆盖区域大；实时通信，速度快；安全可靠。随着无线通信技术的发展，尤其是宽带无线局域网的广泛应用，一些先进的无线通信技术可以应用于智能电网的终端接入。

目前，在无线接入方面是多种标准并存的局面，并处于更新、演化之中。由美国英特尔公司开发的Wi-Fi是一个无线局域网(WLAN)的国际标准，占领了无线接入领域的大部分市场。从早期的802.11a,b到后来的802.11g，又到现在深受用户和厂商关注的802.11n标准，Wi-Fi协议的每个动作都引来多方面的关注。然而，Wi-Fi身份认证和加密机制存在安全隐患，为推广我国自主研发的WAPI无线技术，维护国家利益，政府规定进入我国的无线数码产品取消Wi-Fi功能。在WAPI成为国际标准得到认可后，允许两种模式并存。目前已有集802.11系列协议的安全标准WEP、WPA、WPA2以及WAPI为一体的无线通信芯片问世，比如北京中电华大电子公司推出的HED06W03SP芯片，提供安全多模能力，支持WAPI/WEP/WPA/WPA2 安全标准，并具有完全自主知识产权。应用具有多模能力的无线通信芯片构建基于Wi-Fi的终端接入方案，既可以利用Wi-Fi的产业链优势和成熟的技术成果，又能提高安全性能，是智能电网终端无线接入的优选方案。考虑到Wi-Fi传输的距离限制，只能适用于局部范围内的终端接入，构成无线传感网络；在远程数据传输方面，可以采用GPRS、3G等现有无线通信网络实现，见图1。

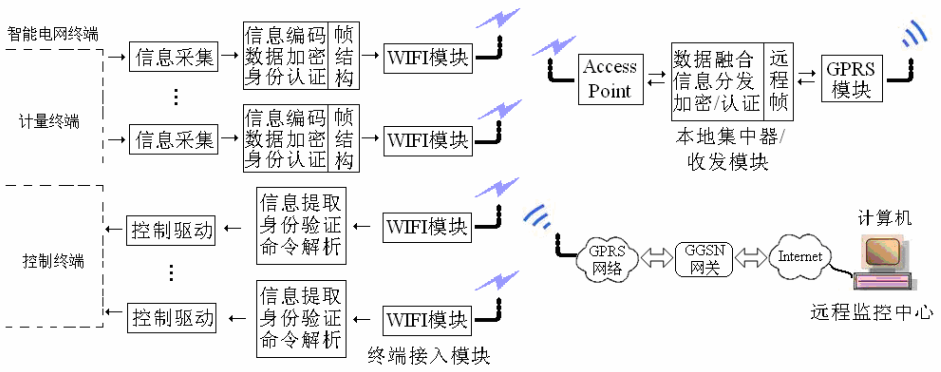

图 1 智能电网终端接入与远程通信平台初步方案

因此，在智能电网终端通信方案研究中，首先需要分析终端接入方案的安全性能与缺陷，寻求解决措施；其次，要定义设备描述信息模型，实现即插即用；最后，需要在现有无线通信网络环境下，实现信息的远程传输。

2. Wi-Fi 技术的安全性能分析

Wi-Fi 是一种短距离的无线通信技术，主要应用于局域网中，除个别版本使用 5GHz 频段外，主要使用 2.4GHz 频段，采用 802.11 协议族，实现对有限网络的延伸。Wi-Fi 技术定义在 OSI 七层网络模型的物理层和数据链路层的 MAC 子层，对于数据的安全性，Wi-Fi 使用 WEP 和 WPA 加密方法来实现数据加密和身份验证。

2.1 WEP 的安全性能分析

WEP（Wired Equivalent Privacy，有线等效保护）是无线局域网协议 802.11 中的第一个安全加密机制，定义在数据链路层，用于无线通信中的访问控制和数据加密。

2.1.1 WEP 的加密策略

当无线工作站要访问 AP（Access Point）时，首先要进行身份验证。无线工作站发出认证请求，AP 收到请求后，生成随机内容传回。无线工作站将随机内容采用 RC4 算法加密后传给 AP。AP 将收到的内容与自身根据随机内容和加密算法计算出的数据进行比对，若相等则验证成功，并通知无线工作站通过身份认证。

在通过身份认证后传输数据的过程中，仍采用 WEP 方式加密，通过共享密钥实现。WEP 加密方法定义在数据链路层的 MAC 层和逻辑链路层(LLC)之间，具体实现过程参见图 2，3。

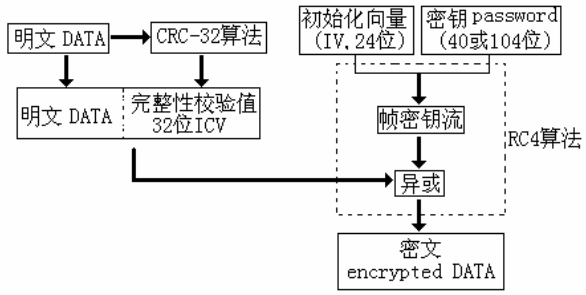

图 2 WEP 加密过程

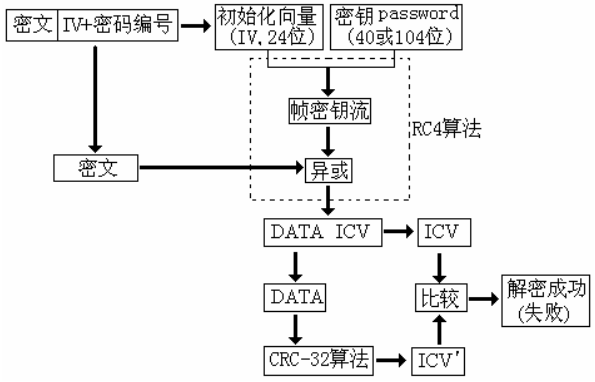

图 3 WEP 解密过程

2.1.2 WEP 的安全缺陷

WEP 算法希望达到三个目的：首先是在无线工作站和 AP 之间实现身份认证；其次是通过数据加密保证通信安全，防止窃听；第三是通过 CRC-32 算法进行完整性验证，防止数据被篡改。但该加密算法存在明显的安全隐患。

（1）32位的循环冗余校验算法CRC-32是信息的线性函数，可以被攻击者篡

改加密信息，通过修改ICV使数据包合法，不能根本保证数据完整性。

（2）24位的初始化向量(IV)和固定的密钥容易引起密钥重用攻击，因此不能保证数据传输的机密性。

（3）RC4算法的弱密钥和运行模式问题。因为RC4算法采用对称流密码算法，即加密与解密使用相同的密钥，造成了密钥分发和管理的困难。流加密即串行加密，这意味着特定的明文对应于加密后的特定密钥串，这就给黑客破译密钥提供了方便。同时由于WEP密钥是固定的，它与所形成的RC4密钥具有某种相关性，从而降低了安全性。

（4）WEP 没有定义密钥管理机制，无线工作站和 AP 的密钥需要手工分发，更改比较麻烦，一般较长时间不会更改。如果 WLAN 中一个用户丢失密钥，会殃及整个网络的安全。

（5）采用的密钥长度固定，分别是 64 位或 128 位，其对应的用户密钥为 40 位或 104 位，即 5 个字符(10 个十六进制数)或 13 个字符(26 个十六进制数)，由于用户在设定密码时有一定的固定模式，从而降低了破解难度。

（6）WEP协议中规定的身份认证是单向的。即访问节点AP对申请介入的移动站点STA进行身份验证，而STA并不对AP的身份进行验证，也会造成安全隐患。

2.2 WPA 的安全性能分析

2.2.1 WPA 的加密策略

为了应对WEP的安全缺陷，Wi-Fi联盟于2002年10月推出了一种新的加密方式WPA(Wi-Fi Protected Access)来弥补，这一安全性被设计为兼容现在的802.11产品并与802.11i标准兼容。WPA提供了增强型的数据加密、健壮的密钥管理系统、数据来源认证以及数据完整性保护等新的安全机制，从而提高WLAN的安全性。

WPA加密算法包括两个版本:

WPA = 802.1x + EAP + TKIP + MIC（工业级，需要认证服务器）

= Pre-shared Key + TKIP + MIC（家用级，不需要服务器）

802.11i(WPA2)= 802.1x + EAP + AES + CCMP

= Pre-shared Key + AES + CCMP

其中，802.1x+EAP(Extensible Authentication Protocol，可扩展认证协议)，Pre-shared Key(PSK，预置共享密钥)是身份校验算法（WEP没有设置身份验证机制），TKIP(Temporal Key Integrity Protocol瞬时密钥集成协议)和AES(高级加密标准Advanced Encryption Standard)是数据传输加密算法（类似

于WEP加密的RC4算法）,MIC(Message Integrity Code信息完整性编码)和CCMP(Cipher Block Chaining with Message Authentication Code Protocol，即CBC-MAC Protocol,密码分块链接报文认证码协议)是数据完整性编码校验算法（类似于WEP中CRC-32算法）。

WPA安全机制的健壮性来源于TKIP加密和802.1x+EAP作为认证机制，其安全性比WEP要强得多。TKIP采用保护性增强的密钥序列,它还增加了信息完整性验证,以阻止伪造的数据包。表1是WPA与WEP的加密技术指标对比。

表1 WPA与WEP对比

加密机制	密钥长度	加密方式	密钥发放	认证方式
WEP	40	静态加密	人工分发	密钥自行认证
WPA	128	动态会话加密	自动分发	802.1x+EAP 增强用户认证

WPA 的认证分为两种：第一种采用 802．1x+EAP 的方式，用户提供认证所需的凭证，如用户名密码，通过特定的用户认证服务器(一般是 RADIUS 服务器，RADIUS：Remote Authentication Dial In User Service，远端用户拨入认证服务)来实现。在大型企业网络中，通常采用这种方式。但是对于一些中小型的企业网络或者家庭用户，架设专用认证服务器代价太高，维护也很复杂，因此 WPA 也提供一种简化的模式，它不需要专门的认证服务器。这种模式即为 WPA 预置共享密钥(PSK)，仅要求在每个 WLAN 节点(AP、无线路由器、网卡等)预先输入一个密钥即可实现。只要密钥吻合，客户就可以获得 WLAN 的访问权。由于这个密钥仅仅用于认证过程，而不用于加密过程，因此不会导致使用 WEP 密钥来进行 802．11 预共享认证那样严重的安全问题。

在通过了802．1x身份验证之后，AP会得到一个与STA(无线工作站)相同的会话Key，AP与STA将该会话Key作为PMK(Pairwise Master Key，对于使用预共享密钥的方式来说，PSK就是PMK)。随后AP与STA通过EAPOL-KEY进行WPA的四次握手(4-Way Handshake)过程。在这个过程中，AP和STA均确认对方是否持有与自己一致的PMK，如不一致，四次握手过程就告失败。为了保证传输的完整性，在握手过程中使用了名为MIC(Message Integrity Code)的检验码。在四次握手的过程中，AP与STA经过协商计算出一个512位的PTK(Pairwise Transient Key)，并将该PTK分解成为五种不同用途的密钥。其中前128位用做计算和检验EAPOL-KEY报文的MIC的密钥，随后的128位作为加密EAPOL-KEY的密钥；接下来的128位作为AP与该STA之间通信的加密密钥的基础密钥(即为该密钥再经过一定的计算后得出

的密钥作为二者之间的密钥)；最后两个64位的密钥分别作为AP与该STA之间报文的MIC计算和检验密钥。

2.2.2 WPA 的安全隐患

WPA比WEP要更为安全，但也并非无懈可击，仍存在一些安全问题。包括黑客从无线传输中截取关键信息、破解无线网络的安全密钥等。WPA的问题集中在对PSK的使用上，PSK是为那些不愿意使用单独的认证服务器的小企业和家庭用户准备的认证工具，并且完全具备802.1x的关键架构。WPA设备用来执行“握手”或交换信息的方式，让那些不知道PSK的黑客可以通过字典攻击(dictionary attack)进行破译。在字典攻击中，黑客在AP和无线工作站之间截获数据流，然后使用特殊的软件来猜测密钥。短于20个字符的口令很难抵挡住字典攻击，那些未得到4个数据包的黑客可以无线AP进行一个新的握手，并且把那些包发送给黑客，而一旦经知道了PSK并已作为一个信任成员加入无线网络的黑客，可以进一步利用WPA握手中的缺点，以此来猜测另一个用户的独特的会话密钥，该会话密钥可以使这个黑客进入那个用户的无线会话。

目前，一家俄罗斯公司公布了WPA的破解工具，他们出品的EWSA软件，宣称可以快速攻破WPA和WPA2的PSK密码。

2.3 WAPI 的安全性能分析

WAPI是WLAN Authentication and Privacy Infrastructure的英文缩写，与802.11b类似，是针对WLAN的一种无线传输协议，但相对WEP具有更好的安全性能。WAPI是中国无线局域网国家标准GB15629.11中提出的WLAN安全解决方案。同时，本方案已由ISO/IEC授权的机构IEEE Registration Authority（IEEE注册权威机构）审查并获得认可，分配了用于WAPI协议的以太类型字段，这也是中国目前在该领域惟一获得批准的协议。

WAPI针对802.11存在的安全漏洞和隐患，利用基于数字证书的双向认证，在客户端和无线接入点间建立了相互验证机制。WAPI包括WAI（WLAN Authentication Infrastructure）和WPI（WLAN Privacy Infrastructure）两部分。WAI负责认证，采用基于椭圆曲线的公开密钥证书体制，无线客户端和接入点通过认证服务器进行双向身份鉴别；WPI负责数据加密，采用国家商用密码管理委员会的对称密码算法进行信息的加解密。此外，WAPI从应用模式上分为单点式和集中式两种，可以彻底扭转目前WLAN采用多种安全机制并存且互不兼容的现状，从根本上解决安全问题和兼容性问题。所以我国

强制性地要求相关商业机构执行WAPI标准，以便能更有效地保证数据的安全。

虽然 WAPI 具有良好的安全性能，但没有无坚不催的矛，也没有坚韧无比的盾。安全漏洞的出现通常要比标准问世晚 5 年时间。随着时间推移，WAPI 也体现出一些安全隐患，同时，其版本也不断完善，从而弥补不足。最新研究表明，WAPI(2006 年版)在证书鉴定和密钥协商过程中仍存在安全隐患，可能被攻击者利用以进行被动攻击和反射攻击。但总体来说，WAPI 在算法上目前没发现安全隐患，加上我国具有自主知识产权，是一项在无线局域网终端接入中值得信赖的安全标准。

3. 基于物联网架构的智能电网终端接入方案

物联网的概念是在 1999 年提出的，其英文名称为“The Internet of Things”。意为“物物相连的互联网”。物联网是在互联网基础上延伸和扩展的网络，将用户端拓展到了任何物品，并实现信息交换，其任务是把最新通信技术充分运用到各行业之中，即把感应器嵌入到包括能源、交通、医疗、家用电子产品等各类物件中，通过 RFID、云计算等各种智能化技术手段，使这些物体被普遍连接起来，实现智能感知、智能识别和智能控制功能，形成物联网。

3.1 构建物联网架构的智能电网终端通信平台

物联网作为新一代信息通信技术，引起了广泛关注，其相关产业发展已被纳入国家战略，国家科技部、工业与信息化部先后在多项国家重大科技专项中设立课题支持物联网技术研究及产业化。物连网的通信模型可分为三个层次：一是传感网络层,即以二维码、RFID、传感器为主,实现对物体及其环境状态的识别；二是传输网络层,即通过现有的互联网、广电网、通信网,实现数据的传输和计算；三是应用网络层,即输入输出控制终端,包括电脑、手机、通用家电等终端。

物体之间的信息感知是物联网的基础，也是其产业链的重点。物联网终端肩负这项功能，实现数据采集、信息封装、加密和识别等功能，其特点是物体之间的智能感知和自动识别,做到即插即用,这正符合智能电网终端设备的应用需求。为此，建立物联网架构的智能电网终端接入与数据通信平台，可以充分利用物联网的研究成果，加快智能电网的建设速度，促进二者产业链的融合，具有强大的市场潜力，见图 4。

智能电网的建设目标，是通过终端传感器在客户之间、客户和电网公司之间

形成即时连接的网络互动，实现数据读取的实时、高速、双向的效果，从而整体提高电网的综合效率。智能电网实现电力流、信息流、业务流高度一体化的前提，在于信息的实时采集、安全快速传输、准确识别、合理应用，最终实现发电、输电、配电、用电的智能控制、智能调度、智能管理。

在智能电网的各环节中，用电终端是直接面向用户的，直接体现了电力网络的服务水平，而且数量众多，管理复杂。国家电网公司提出了“面向应用、立足创新、形成标准、建立示范”的研究指导思想，在物联网的专用芯片、应用系统开发、标准体系、信息安全、无线宽带通信、软件平台、测试技术、实验技术等方面进行了全面部署，力争尽快实现物联网技术在电力系统应用多项核心技术的突破，形成若干项有重大影响的创新性科研成果，成为在国内外有重要影响的从事智能电网物联网技术研究和应用的研发中心和产业化基地。

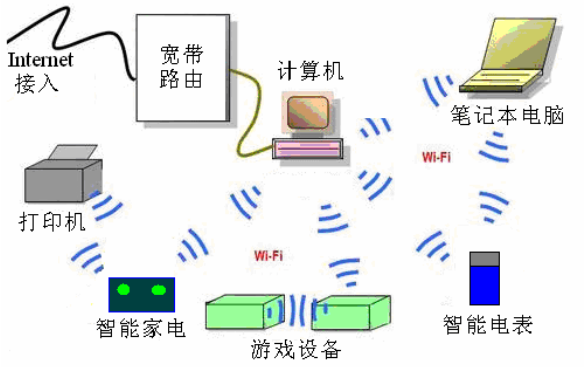

图 4 物联网架构的智能电网终端通信平台

3.2 智能电网终端通信信息模型研究

构建合理的通信信息模型，是智能电网终端接入和通信平台建立的基础。智能电网的建设目标，表现在用户终端环节是实现各种用电设备间的智能感知与识别。在终端通信信息模型建设中，必须实现即插即用的设备互联机制，结合物联网结构和协议规范，建立电力信息传输和设备间互联的数据模型，实现设备的感知、身份鉴别和控制，定义设备信息传输过程中的协议解析规范。对设备底层的信息进行封装，在会话层、表示层和应用层定义设备鉴别原则，抽取重要的身份与状态信息组成统一帧格式，并确立快速解析方法，实现设备的互操作。

因此，每种设备都需要广播自身的特点、用电需求和运行状况，同时要接收其它用电设备的相关信息。智能电网络终端设备中，智能电表研究是实现用电智能化的关键环节，需要汇报当前各种电力能源的接入情况、电能质量、实时资费等信息。同时，根据终端设备的用电需求，进行科学计算，合理调度。

图 5 是一个初步的终端通信的信息模型。

附加信息	加密信息 校验信息 专用信息
高级信息	运行状况 电能来源 资费状况
扩展信息	用电请求 预计时长 紧急程度
基本信息	设备功率 设备ID 设备类型

图 5 用电终端通信信息模型

信息模型具有典型的层状结构，各层信息的加密与传输可以根据需要取舍。其中最底层是基本信息，这是一种广播信息，被物联网范围内的所有设备所接收和感知。这部分信息将会定时发送，也是各设备实现即插即用的基础。同时，各设备也接收其它设备的广播信息，了解所有“在线”设备的基本状况。第二层扩展信息，主要用于用电请求，可能来源于用户操作或智能控制，需要给出请求信号，预计时间长度和请求级别，供调度程序分析处理。第三层是高级信息，一般是应答信息，来源于其它设备，尤其是用电管理设备的查询请求，该设备作出回应，发送当前运行状况、电能来源、实时资费等信息。附加信息除了该设备发送给专用设备的特殊信息外，主要用于信息的应用层加密与校验，加强信息传输的可靠性。

4．配电变压器远程监测系统

智能电网的一项主要功能是实现设备的远程监测，本项目以配电变压器远程监测为目标，研究了从信息采集、远程传输到处理的实现方法，开发了相应的实验装置，编写了相关的软件。

配电变压器对配电网和用户的用电可靠性、安全性有着直接的影响。为保证配电变压器的安全运行，必须加强配电变压器的运行监视以便及时采取措施，防止事故发生。但是由于配电变压器安装位置分散，传统的对配电变压器运行监视方法工作量大，安全环境差，实时性差，很多异常情况不能及时发现，造成了事故的发生。建设配电变压器远程监视系统可实现配电变压器的实时监测，提高监测的工作效率和数据准确性，为配电变压器的安全运行提供了有力的保障。配电网通信有终端节点多而分散、通信距离长等特点。传统的配电网监控一般都采用

光纤、屏蔽双绞线、电力线载波等介质的通信方案，这在布线、投资成本、日常运行费用等方面有很大的缺陷。构造安全、高效、经济、应用方便的远程通信系统成为配电变压器远程监测系统的关键。

配电变压器监测点与远程监控中心间相距可能较远，目前可以利用的通信平台主要有电信、互联网络以及移动通信网络。由于远程数据传输由任务请求而触发，数据量和实时性要求较高，加上一些特殊环境中布线受到影响，宜采用覆盖范围广、免布线的移动通信网络实现远程数据传输。

GPRS（General Packet Radio Service，通用分组无线业务）是在现有的GSM移动通信系统基础之上发展起来的一种移动分组数据业务。GPRS 通过在GSM 数字移动通信网络中引入分组交换功能实体，以支持采用分组方式进行的数据传输。GPRS 系统可以看作是对原有的GSM 电路交换系统进行的业务扩充，以满足用户利用移动终端接入Internet 或其它分组数据网络的需求，其速度最快可达172kbps。

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。

GPRS方案用于配电变压器的远程数据传输，具有组网方便，开发周期短，覆盖范围大的优势；在传输速度方面，由于数据经过了本地数据集中器及远程监控中心的处理，并按任务请求或报警需要实现信息传输，可以有效压缩数据量，同时也降低了通信资源占用，减少了流量费用，可以满足应用需求。另一方面，GPRS做为2.5G无线通信技术，是一项向3G网络的过渡技术，随着3G产品的广泛应用和相应开发手段的成熟，GPRS可以很容易过渡到3G，从而利用更宽的带宽，满足未来大数据量的实时传输，具有良好的发展潜力。

4.1 系统的组成和功能

配电变压器远程监测系统包含监测点数据采集系统、远程通信系统和主站系统。主站系统主要进行整个系统的管理和控制，完成人机交互工作及网络数据链路的建立，实现配电变压器运行参数的计算、分析和故障判别；通信系统进行通信协议转换，完成信息的上送与下发；数据采集系统主要完成前端信号的处理、滤波和信息的采集，其结构如图 6 所示：

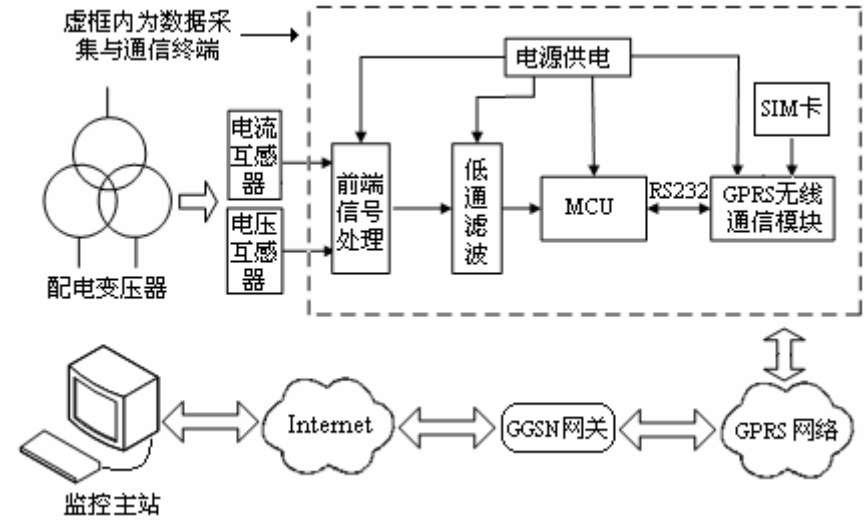

图 6 配电变压器远程监测系统组成结构图

4.1.1 主站系统

主站系统可以是一台通过固定 IP 地址连接互联网的计算机，也可以是由多台计算机构成的局域网络，通过路由器与互联网连接。为方便 GPRS 通信终端的连接，路由器的外网 IP 地址应固定，内部局域网上的计算机在路由器上建立端口映射。GPRS 通信终端采用“IP：端口”方式连接监控主站计算机，实现数据的双向传输。局域网中还可以采用多台计算机协同工作的方式，其中实现远程连接的计算机称为前置机，主要负责网络数据链路建立和数据收发，维护联入的每个终端的 IP 地址和 RTU 号，根据需要在前置机和各个终端之间建立点对点的连接和身份认证，并将数据进行分析和处理和转发。局域网中还可建立专用的数据库服务器和工作站，构建管理信息系统，便于查询、分析统计和用户交互。

4.1.2 通信系统

通信系统进行通信的管理、通信协议转换及信息传输，主要包括通信通道及相关设施。配电变压器监控系统的通信通道，目前主要有无线、GSM、光纤以及 GPRS 等方式。无线方式除了每年的频点费以外，平时运行无需额外费用，可靠性和实时性较好，但设备的安装、调试以及维护较麻烦。GSM 短消息方式安全性

和稳定性较好，但由于是按条收费，运行费用高，而且在节假日短消息中心服务器繁忙时延时相当长。光纤通信稳定可靠，但是成本投入大。 GPRS 是通用分组无线业务的简称，采用的是基于 GSM 系统的无线高速数据分组传输技术，传输速率快，数据量大，费用低，适用于间断的、突发的、频繁的以及少量的数据传输，是配电变压器监控系统的首选。

4.1.3 数据采集系统

数据采集系统主要包括终端及辅助设施。终端主要完成配电变压器监测点的信号调理、数据采集、存贮和对数据加密，对数据进行初步分析，产生异常报警信号即时上传到监控主机；接收并解析主站命令并能按照主站的指令进行帧结构组织与传输见图 7。

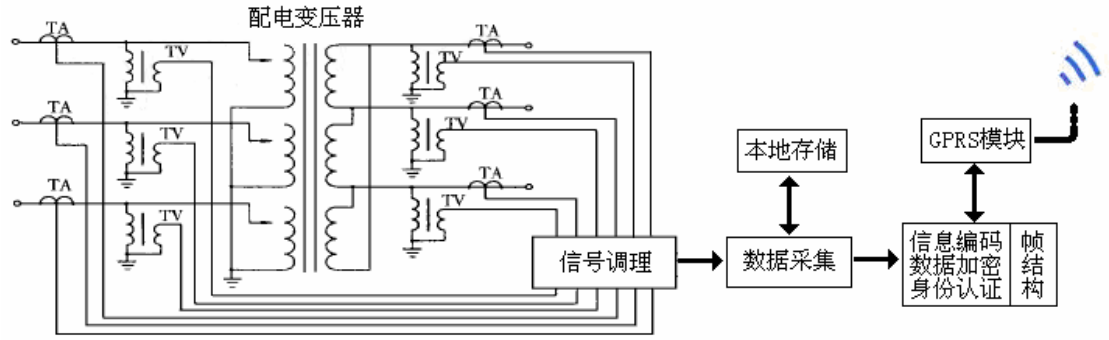

图 7 数据采集系统构成

数据采集系统安装在变压器现场，通过电压互感器（PT）和电流互感器（CT）对变压器源边和副边的三相电压、电流电气参数进行采集监测；同时，分析记录采集数据，并在变压器三相电力参数出现异常事件时主动上传告警信息。采集终端包括三大功能：一是电力参数采集模块，对变压器三相电气参数进行实时采集，存储历史数据，以便监测中心要了解变压器的电压、电流、功率等参数时，可以通过预先设定的查询历史数据命令获取，然后通过监测中心软件分析形成曲线报表等；二是智能监测与 GPRS 通信管理模块，该模块监测与分析采集模块送出的实时参数，如果发现电压电流超限或断电来电，则启动 GPRS 通信模块的监测中心发送报警信息；三是当上位机软件发起通信请求时，还要负责握手和建立通信链路，完成数据的封装与传输。

本系统采用MG8型电流互感器，如图8所示。在现场测量变压器电流信号时，可以直接将其接入配电变压器输出端，相比传统的零序电流互感器在安装和操作上显得更加方便和快捷，性能指标如下：

- 变比：2500：1；

- 测量范围：0~20A；
- 测量精度等级：0.1级；
- 工作温度：-40℃ ~ +80℃；

本系统采用TR1102-C型电压互感器，如图9所示。该互感器电压是直接输入和输出，具有外围电路简单、线性度好和测量精度高的特点，能满足现场工作环境要求，性能指标如下：

- 额定输入电压：0~380V；
- 二次输出：0~0.7V；
- 精度等级：0.1级；
- 工作温度：-25℃ ~ +75℃；

图 8 MG8 型钳式电流互感器

图 9 TR1102-C 型电压变换器

4.1.4 监测中心软件

监测中心软件首先要完成与数据采集终端通信链路的建立，进行网络侦听，接受 GPRS 模块上传的信息并将用户请求通过网络传到终端设备。其次，中心软件应为用户提供一个可视化的监测界面，让用户直观、方便、快捷地了解变压器的运行状态，通过此界面，用户可以及时发现变压器出现的故障。通过数据分析与参数计算，可以自动汇报变压器的运行状况，提供报警信息。同时，用户通过查询历史数据库，可以调出变压器的历史运行状态曲线，从而预测变压器的负荷情况。

4.2 配电变压器远程监测系统硬件设计

4.2.1 电压采集前端处理电路

电压前端采集电路的主要功能是将高电压信号按比例变换并对其进行直流偏置，以匹配ADC模块的测量电压。这部分包含了电压转换电路、直流偏置电路和反相电路，如图10所示。

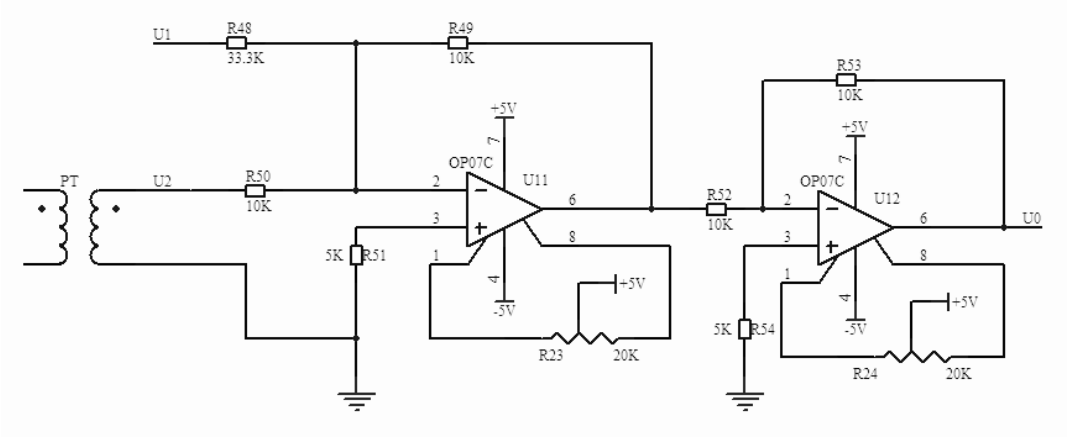

图 10 电压采集前端处理电路

C8051F020内部集成A/D转换器的输入电压是0~3.3V，所以信号的直流偏置电压选择其中间值1.5V，电路参数的计算关系式如下：

$$U_0 = -U_1 \times \frac{R_{49}}{R_{48}} - U_2 \times \frac{R_{49}}{R_{50}}$$

根据经验，R_{50}选择为10K，对变换后的电压信号只需要做电平抬升，所以R_{49}也取10K。正电压信号U_1取5V，经过运放两次反相后变为正电压叠加在信号中，通过计算可得R_{48}电阻值为33.3K。运算放大器OP07C具有较好的稳定性，第1脚和第8脚之间接入20k电位器可以消除自激振荡。

4.2.2 电流采集前端处理电路

电流采集前端处理电路是将电流转换为电压信号，并对其进行直流偏置和反相变换，使其满足C8051F020的模数转换范围。

变压器电流信号经过电流互感器CT（Current Transformer）输出后由精密多圈电位器R_{14}将电流转换为电压，其幅值大小可通过电位器调节，直流偏置电路原理和反相电路原理与电压采集前端处理电路相同。

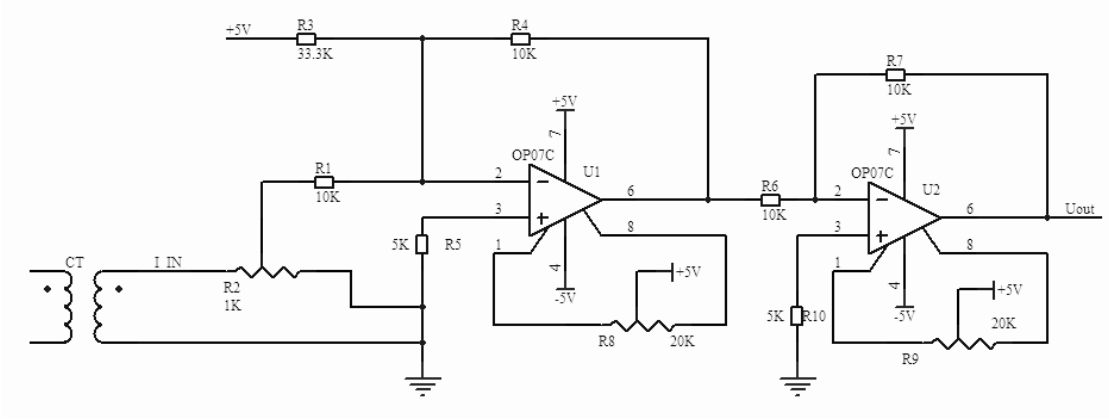

图 11 电流采集前端处理电路

4.2.3 低通滤波电路

低通滤波电路的作用是滤除信号的高频部分，防止信号混叠和干扰。本系统采用巴特沃斯二阶低通滤波器，其特点是通频带内的频率响应曲线最大限度平坦，而在阻频带则是逐渐下降为零，电路如图12所示。

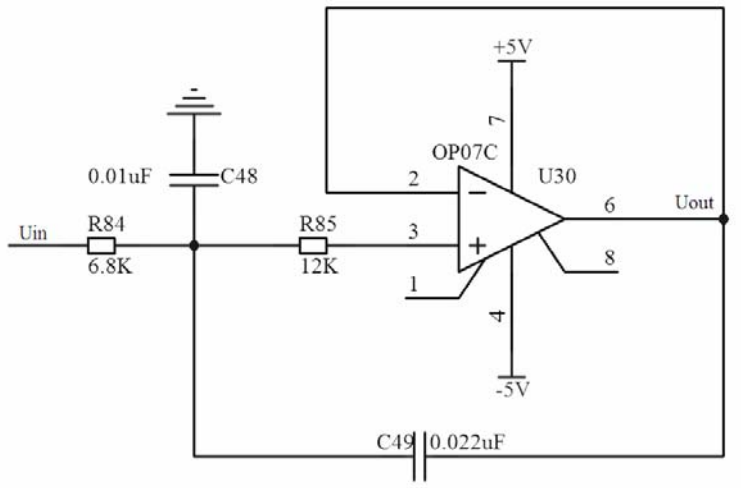

图 12 低通滤波电路

滤波器的幅频特性如图13所示，该图描绘了滤波器输入信号频率与输出信号衰减幅度之间的对应关系，可以看出大于1kHz的信号沿着固定斜率逐渐衰减。由于所采集的谐波电流频率最大不超过750Hz，低通滤波器1kHz的截止频率不会影响到谐波电流测量。每个A/D转换通道都采用了相同滤波电路，所以由滤波器引起的相位偏差很小，不会影响谐波电流的测量。

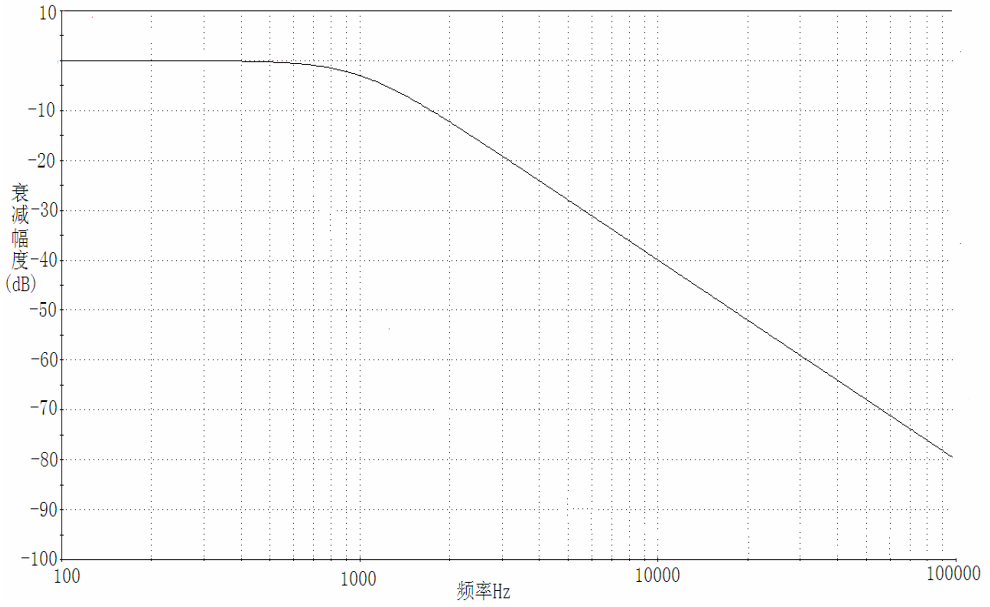

图 13 滤波电路的幅频特性

4.2.4 单片机电路设计

C8051F020 单片机是集成在 1 块芯片上的混合信号系统级单片机,具有与 MCS-51 内核及指令完全兼容的微控制器。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,主要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、SMBus/I2C、UART、SPI、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,且该单片机内部具有 JTAG 和调试电路,通过 JATG 接口可以使用安装在最终应用系统产品上的单片机进行非侵入、全速及在系统调试。

本系统中，单片机主要用于前端监测信号的数据采集和初步处理，并使用串口控制 GPRS 模块并实现数据传输。其主要电路包括：时钟电路、复位电路、JTAG 仿真口电路；串行接口电平转换电路；电源电路等。

C8051F020 单片机的电源包括 3.3V 的数字电源和模拟电源，由 LM2937IMP-3.3 产生。LM2937 是安森美半导体公司生产的三端低压差稳压器，具有过电流保护、过热保护、调整管安全工作区保护等功能，还增加了“反装电池保护”功能，见图 14。

单片机外围电路包括时钟电路、复位电路和 JTAG 仿真口电路。时钟采用 22.1184MHz 无源晶振,复位电路支持上电复位和按键复位。JTAG 接口电路利用单片机内部的边界扫描测试电路引脚加上上拉电路构成，见图 15。

单片机串行接口电路实现232电平转换。采用单片机的P0.0、P0.1、P4.0、P4.1实现串行接口，采用SP3223E电平转换芯片实现单片机的TTL电平与232电平转换，见图16。

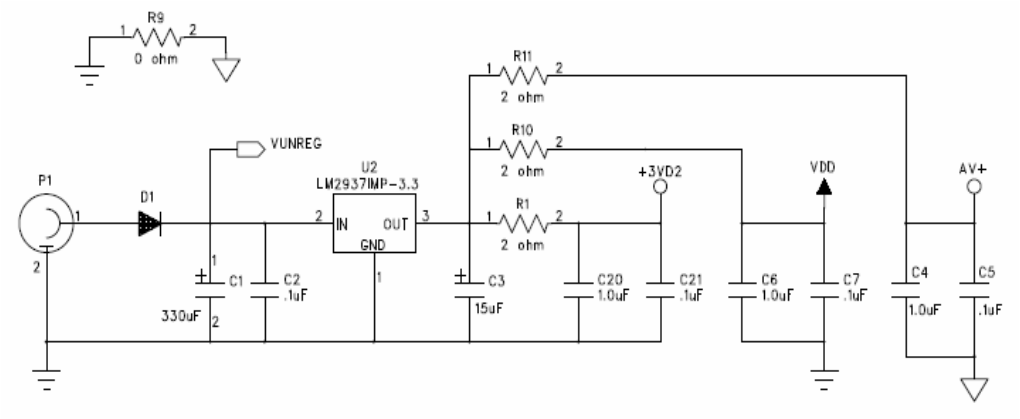

图 14 单片机电源电路

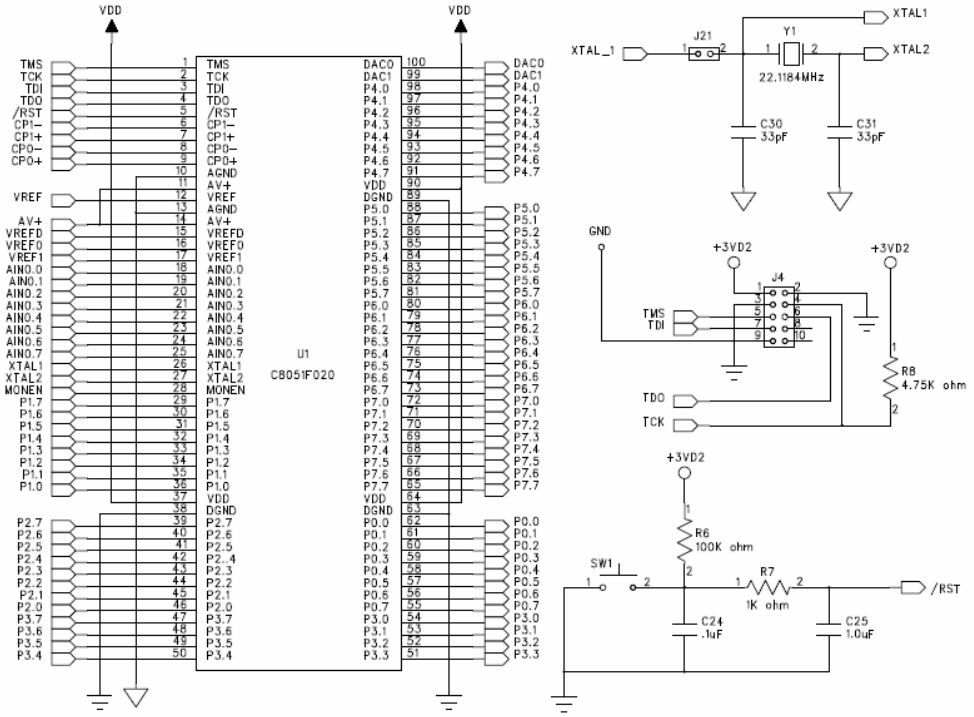

图15 单片机外围电路设计

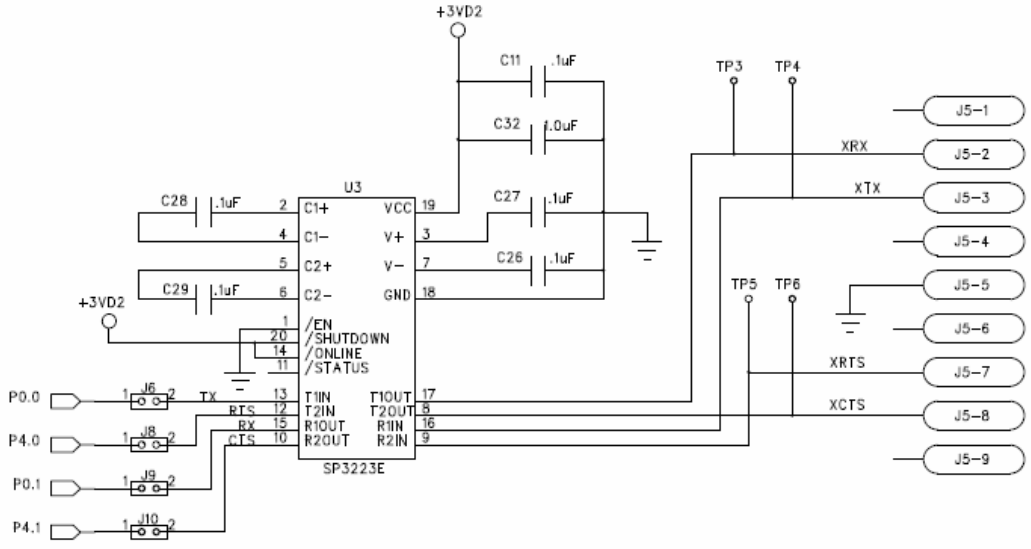

图16 单片机串行接口电平转换电路

4.2.5 GPRS 模块外围电路设计

MC52i无线模块是当今市场上尺寸最小的双频GSM/GPRS模块，适用于亚洲和欧洲的GSM网络。MC52i内嵌TCP/IP协议栈，易于集成，用户可以在短的时间内开发出GPRS无线上网终端，广泛应用于远程监控、无线公话、车载终端、无线POS终端等领域。在本系统中，MC52i无线模块是通信核心，通过SIM卡接口电路连接SIM卡实现身份验证，并由串行接口接收由单片机传送的命令及数据信息。

GPRS模块外围电路包括电源电路、GPRS模块启动信号发生电路和SIM卡接口电路、电平转换电路。

电压转换芯片采用ASM1117正稳压集成电路，为GPRS模块接口电路板提供3.3V的数字电源。多个电容用于对输入输出电源进行滤波处理，两个发光二极管，其中一个用来指示电源的供给状态，另一个应用GPRS的SYNC引脚指示GPRS的通信状态，如图17所示。

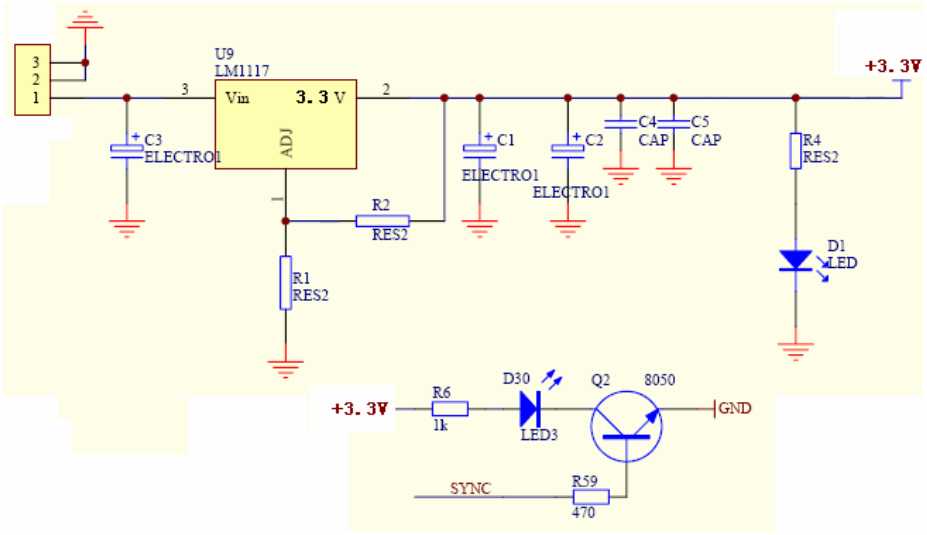

图17 GPRS电源电路

SIM卡接口电路实现GPRS模块与SIM卡的接口。GPRS模块的启动信号IGT发生电路由芯片CAT1161产生，为GSM模块的IGT引脚提供了一个大于100ms且电平下降持续时间小于1ms的启动脉冲信号，使其加电后进入工作状态，如图18所示。

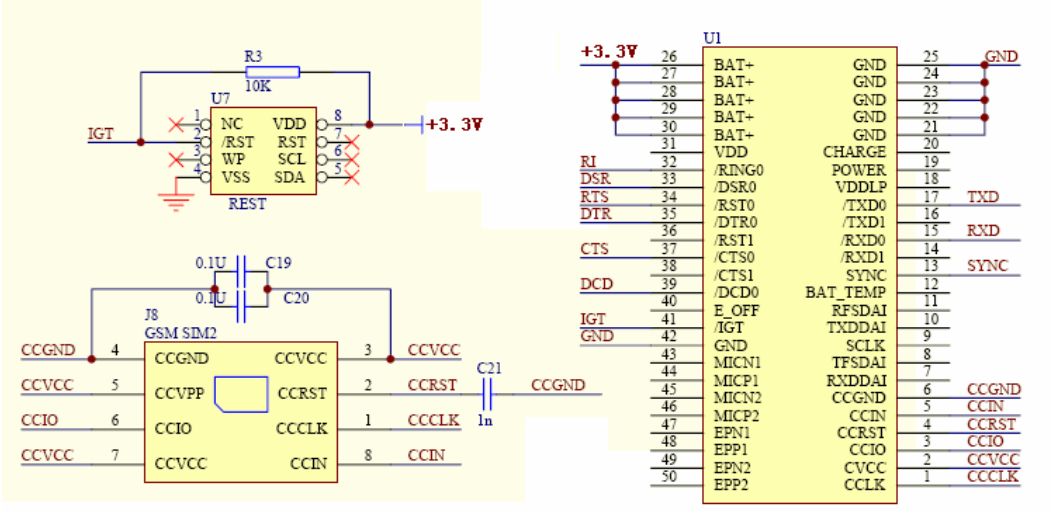

图18 SIM卡接口电路

SP207E将模块0~5V的TTL电平转换为-10~+10V的RS232电平，以便在调试环节与PC机进行通信，同时也可以与前面的单片机系统进行通信，见图19。

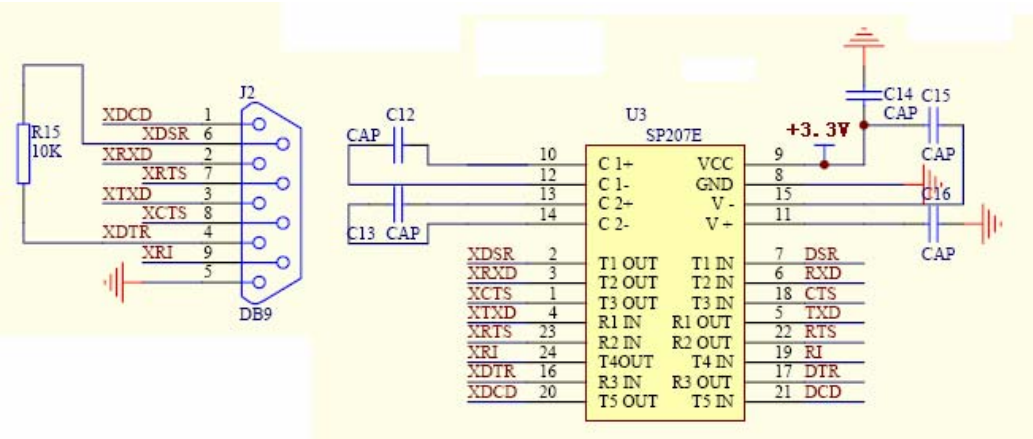

图19 GPRS模块串行口电平转换电路

经过上述设计，形成了基于单片机的数据采集板和GPRS模块通信扩展板，两个电路板都具有RS232串行口，可以与PC机连接，便于单独调试，实现性能优化。同时，两个板可以通过串口电缆连接，形成脱机系统独立工作，见图20。在系统软硬件运行成熟后，可以考虑将两块板一体化设计，一方面可以减小体积，降低功耗，同时也提高系统稳定性。

图20 数据采集与通信硬件电路板实物图

4.3 配电变压器远程检测系统软件设计

4.3.1 通信终端设计

通信终端完成数据采集和通信控制，其核心是 MC52i GPRS 通信模块，在单片机控制下实现协议解析和远程连接，并根据主机请求将单片机 ADC 采集的多通道信息进行数据封装，附加标志码组成信息帧发送到 GPRS 网络，并通过 GPRS 网关进入 Internet 由远程主机接收。

（1）MC52i 通信控制方法

MC52i 是 Cinterion 公司（原西门子）最新推出的工业级 GPRS 无线通信模块，MC52i 是 2 波段（900MHz/1800MHz）的 GPRS 模块，内部带有 TCP/IP 协议栈，目前广泛运用于智能公交、无线数传（DTU)、远程无线抄表等系统应用中，可在-40° C 到+80° C 的环境下正常工作，功耗低、可靠性高、性价比高。MC52i 包括了 MC35i、MC39i、TC35i 的所有功能，引脚和指令完全兼容 MC55/MC56，采用 AT 命令集实现协议解析和通信连接。MC52i 模块支持以下 Internet 服务：1）Socket Client and Server for TCP, Client for UDP；2）FTP Client；3）HTTP Client；4）SMTP Client；5）POP3 Client。

根据 MC52i 的协议需求，系统采用下面 AT 命令实现通信连接和信息收发：

设置配置文件：

AT^sics=0,contype,gprs0　　；配置文件 0 ，连接方式是 GPRS

AT^sics=0,user,cms　　；配置文件 0 ，设置用户名

AT^sics=0,passwd,gprs　　；配置文件 0 ，设置密码

AT^sics=0,apn,cmnet　　；配置文件 0 ，设置 APN

设置服务平台：

at^siss=1,srvType,socket　　；服务平台 1，服务类型为 socket

at^siss=1,conID,0　　；服务平台 1，使用配置文件 0

at^siss=1,address,"socktcp://远程主机 IP 地址:端口号"　;服务平台 1，设置服务器 IP 地址及端口

at^siso=1　　;服务平台 1，开始工作

上面 AT 命令如果运行成功，就可以进行数据收发了。在此之前可使用命令 at^siso?查看远程连接是否成功，运行该命令后 GPRS 模块将返回：

^SISO: 1, "Socket","4","2","0","0","本地 IP:端口号","远程 IP:端口号"

通常若 GPRS 模块已被分配到本地 IP 地址，则表明连接成功了，可运用下面 AT 命令进行数据收发：

at^sisw=1,n

使用服务平台 1 发送 n 字节数据，若 GPRS 模块响应^SISW: 1, n，则可以输出 n 字节数据,并以回车键结束。若远程有数据传来,GPRS 模块会给出提示^SISR: 1, 1,此时需要发读命令 at^sisr=1,m,然后读取数据。若通信完毕，可根据需要使用 at^SISC=1 命令关闭该服务平台。

（2）C8051F020 单片机实现数据采集与通信

MC52i 的 AT 命令接收及与终端的数据交换都通过串口进行，系统中采用 C8051F020 单片机编程实现。C8051F020 除通过串口向 MC52i 发送 AT 命令外，还完成数据采集、封装及远程命令解析任务。同传统 AT89C51 相比，C8051F 具备多项优势，包括采用 CIP-51 内核大力提升 CISC 结构运行速度、I/O 从固定方式到交叉开关配置、从引脚复位到多源复位，以及低功耗等。C8051F 单片机被称为智能产品高速路上微处理器中的奔驰，其应用领域涵盖三相电度表、电力系统监控、智能仪器仪表和医疗仪器等多种应用。

C8051F020 内部带有数据采集所需的 ADC 和 DAC，其中 ADC 有两个，一个是 8 路 12 位逐次逼近型 ADC，可编程转换速率，最大为 100 KS/s。可通过多通道选择器配置为单端输入或差分输入，内有可编程增益放大器 PGA 用于将输入的信号放大，提高 A/D 的转换精度。另一个是 8 路 8 位 ADC，可编程转换速率最大为 500kS/s，可满足本系统的需要。

此外，C8051F020 外设还增添了三个串行口，可同时与外界进行串行数据通信，其中的两个增强型 UART 串口可应用于与 GPRS 模块的连接。C8051F020 具有基于 JTAG 接口的在系统调试功能，片内的调试电路通过 JTAG 接口可提供高速、方便的在系统调试。根据上述特点，我们采用 C8051F020 单片机的监测系统终端主控器。

C8051F020 的程序由 C 语言编写，包含数据采集和通信控制两部分。通信控制程序完成系统初始化，建立网络连接，解析远程主机请求，将指定数据源加上标志信息和验证信息构成数据帧并发送，其程序流程如下：

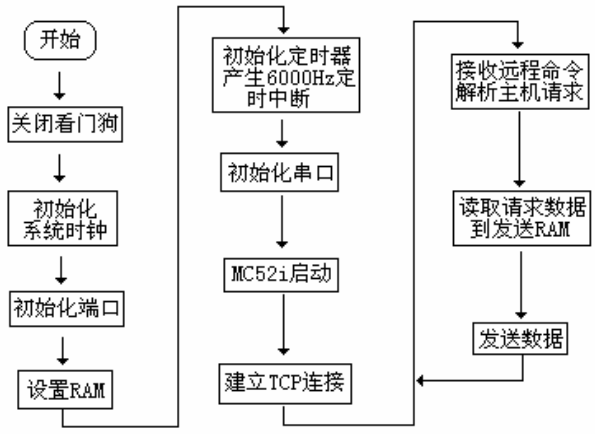

图 21 终端控制与通信程序流程图

数据采集程序完成对各通道数据的采集与存储，为通信模块提供数据源。系统中针对三相配电变压器原副边的三相电压和电流，采用电压和电流互感器获得

运行信息，对共计 12 路模拟信号经滤波后送到单片机，利用 C8051F020 的内部 ADC 完成采样，采样频率由定时器控制。由于工频信号为 50Hz，为综合考虑数据存储与传输需求,对每路信号用 500Hz 及 8 位采样,则定时器溢出频率取 6000Hz，在定时器产生中断时对各通道轮流采样。

C8051F020 单片机内部有 4352 字节的内部 RAM，可用于存放临时数据。系统分配 3900 字节用于数据存储与传输。该空间分成 13 块，每块 300 字节，其中 12 块对应于存放各通道的采样数据。由于一个工频周期采样为 10 个点,所以 RAM 中的临时数据始终保留了各通道最近 30 个周期的数据。对各通道设置位置指针变量，用于新点对旧点的覆盖及为数据传输时提供起始位置。另一块 300 字节空间用于发送缓冲区，当通信模块得到请求需要传输数据时，将指定通道的数据快速移入缓冲区中等待发送，同时在数据转移期间设置标志，以防止被覆盖破坏数据顺序。数据采集程序中断程序流程如下：

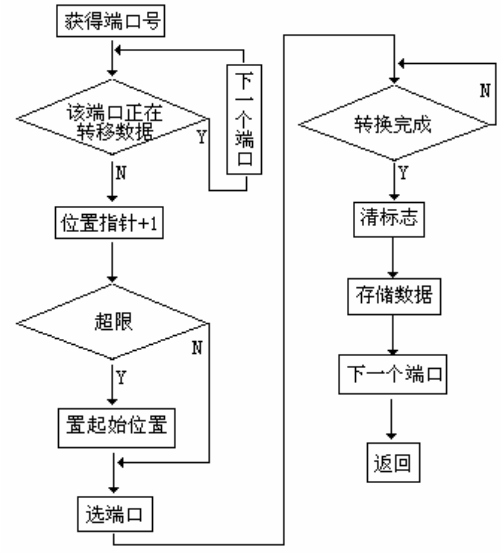

图 22 数据采集定时中断程序流程图

4.3.2 远程主机监控程序设计

远程主机监控程序由 VC++编程，负责与 GPRS 终端建立通信联络，发送来自用户操作或自动产生的服务请求，接受远程数据并根据约定进行验证，进行数据运算与处理，将监控结果汇报给用户。主机程序还在数据库支持下提供数据的存储、查询和业务需要的管理功能。

Microsoft 的 Windows Sockets API 是 Windows 下的网络应用程序接口，Microsoft Visual C++ 6.0 提供了用于 Windows Sockets 编程的 Winsock 控件，该控件为用户提供了访问 TCP 和 UDP 网络的途径，并适用于 Microsoft Access、Visual C＋＋等多种可视化环境。通过 Winsock 控件编制 C/S 程序，程序员无须

了解 TCP 或低级 Winsock API 调用实现的细节便可直接进行数据的传送。在 TCP 应用中，为了建立一个网络连接的服务器端，只需设置本地服务端口号，然后服务器调用方法 Listen 进入阻塞状态，等待来自客户的连接请求。服务器接收到客户请求时，事件 ConnectionRequest 被触发。如服务器愿意提供服务，则可调用 Accept 方法接受连接。一旦连接建立，可使用 SendData 或 GetData 进行数据的发送或接收。当收到数据时，事件 DataArrival 将被触发，可以进行数据存储、处理并通过用户界面进行参数的波形显示。程序的主要流程如下：

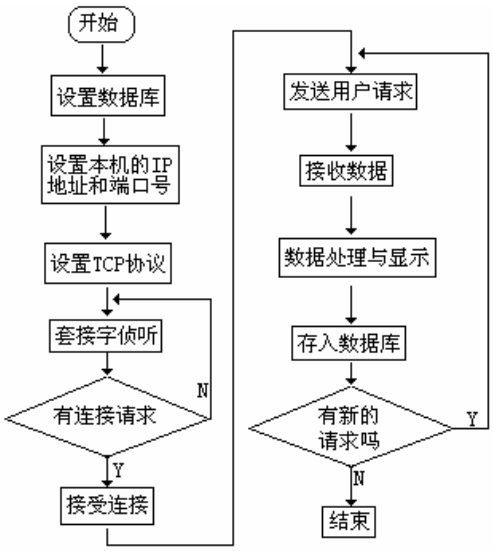

图 23 主机的监控程序流程图

项目组编写实验软件对通信系统进行了测试，实现了监控主机与数据采集终端之间的双向数据传输，见图 24。监控软件可以显示与终端的连接状态，当成功连接后，定义以每帧 80 个字节接收数据，对其进行存储、分析处理，并实现实时波形显示。通过监控软件界面可以发送命令实现通道选择，当终端收到命令后由单片机完成通道切换，实现帧结构组织与传输。

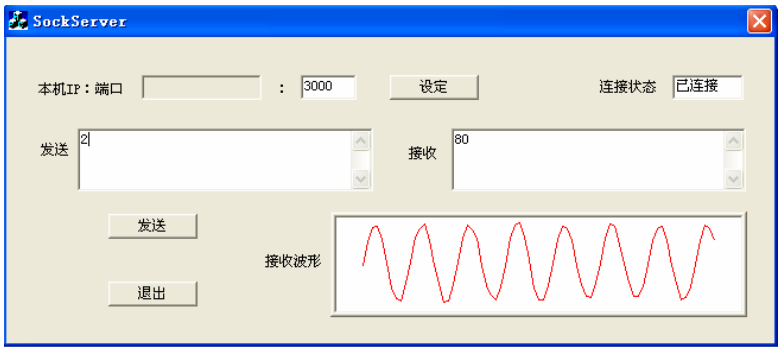

图 24 主机监控程序实验软件界面

4.4 GPRS 网络的安全性能分析及解决措施

通用分组无线业务（GPRS）是一种对GSM网进行改进的数据传输标准，在GSM

上提供分组交换和分组传输能力，利用现有GSM站点的基础设备，能以高达115kbps甚至170kbps的传输速率实现端对端的分组交换数据业务。无线应用协议（WAP）等高层协议可以基于GPRS来实现移动互联。GPRS核心网络采用了IP技术，即可以与迅速发展的IP网络（Internet/Intranet）互联，又顺应通信网的分组化发展趋势，逐步向第三代移动通信系统演进。

GPRS是在GSM网络的基础上增加GPRS服务节点（SGSN）、GPRS网关节点（GGSN）以及一系列标准接口来实现的。

4.4.1 GPRS 用户的身份验证方法

GPRS的用户身份验证过程与GSM中的验证过程由SGSN完成。验证机制中使用了一个三元组，包括一个128位的随机数RAND、用于用户验证的A3算法结果SRES（32位）以及由A8算法计算所得的64位密钥K_c（将用于身份验证结束后数据传输中使用的GPRS加密算法GEA）。在网络侧，这个三元组由SGSN从归属位置寄存器（Home Location Register, HLR）处获取并存储于SGSN内部。

用户身份验证方法简述如下：见图25。其中K_i是存储在SIM卡和HLR中的用户身份验证密钥，长度为128位。首先，移动用户终端向SGSN提出验证请求，SGSN接收到请求后，向HLR发送一个验证信息。HLR接收到该信息后，用随机数发生器产生一个在0和$2^{128}-1$之间的128位随机数RAND，并利用该随机数以及自身存储的用户验证密钥K_i，使用A3算法得到结果SRES，使用A8算法得到GPRS加密算法（GEA）的密钥K_c，并将随机数、SRES、K_c作为一个三元组发送回SGSN。然后，SGSN将三元组存贮起来，并将其中的随机数发送给用户移动终端。用户终端使用该随机数以及存储在自身SIM卡中的验证密钥K_i，利用A3算法计算出结果SRES并发送回SGSN；最后，SGSN将内部存储的三元组中的SRES与用户发回的SRES进行比较，如果二者相等，则移动用户终端通过了身份验证。随后，SGSN将与终端进行是否需要对数据传输进行加密的协商和设定，并保证SGSN与移动终端之间加密解密的同时进行。协商成功后，用户身份验证过程结束。

由图可见，A3和A8算法在用户移动终端和HLR中独立进行，其数据来源是HLR中产生的随机数和用户身份密钥K_i。由于随机数是明文传输，存在被盗风险，GPRS网络中的所有安全功能都建筑在用户验证密钥K_i之上，因此，身份保护是至关重要的。

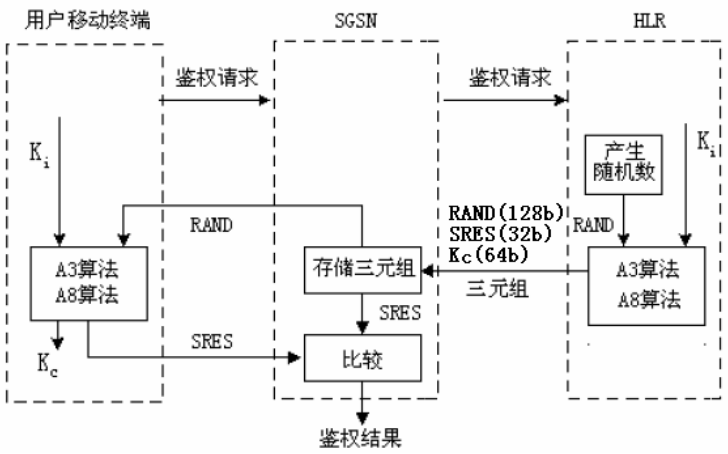

图 25 GPRS 用户身份验证及密钥计算过程

4.4.2 GPRS 数据加密方法

在移动终端身份验证成功之后，就可以进行数据传输了。在GPRS网络数据传输过程中，数据和信令是受加密算法保护的，这种GPRS加密算法（GEA）是保密的，处于逻辑链路控制（LLC）层。在GPRS网络中，数据和信令受到加密算法保护的范围是从SGSN到用户终端，比GSM中从基站到用户终端的范围要大。

GPRS加密算法的密钥K_c的传送是不受加密算法保护的。为了保证K_c的安全性，GPRS和GSM网络中均使用了间接传送的方式，如图25所示，即网络只向用户终端传送随机数RAND，用户和网络都利用RAND和K_i，使用A8算法来计算密钥K_c。

密钥K_c的长度为64位，为保证数据传输的安全性，可以在数据传输过程中随时更新，即HLR重庆生成随机数，连同Ki用A8算法重新计算K_c，网络和移动终端中始终保持最新的K_c。为了正确传递数据，SGSN和移动终端中的密钥K_c必须保持同步，这在GPRS网络通过LLC包的序列号以及数据传送方向来保证，见图26。

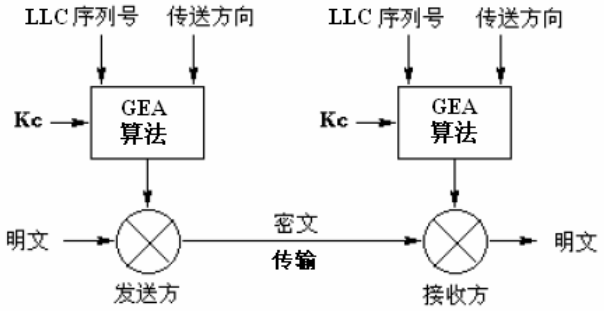

图 26 GPRS 数据及信令的加解密过程

4.4.3 GPRS 网络的安全性能分析

由于本项目中GPRS移动终端通过Internet与远程监控主机交换信息，需要重点分析GPRS与IP网络互联时的安全性能。GPRS网络通过使用GGSN的Gi参考点能够支持与IP网络的互联。Gi参考点位于GGSN与外部IP网络之间，对外部IP网络而言，

GGSN相当于一个普通的IP路由器。因此，为保证GPRS网络系统的安全性，需要完善IP网络的安全防范措施，包括采用防火墙，正确配置DHCP和DNS，在保证GPRS的合法用户访问外部网络基础上，限制外部网络对GPRS网络的某些操作。

GPRS网络为用户提供了两种访问外部IP网络的机制：透明访问方式和不透明访问方式。在移动终端使用透明访问外部IP网络时，GPRS网络为移动终端分配静态或动态IP地址，GGSN用此IP地址与移动终端想要访问的外部IP网络节点进行通信，并将返回的信息传递给相应的GPRS移动终端。在透明访问方式下，GPRS网络不保证用户在外部IP网络上的身份和数据安全，此时用户只能通过使用IP层或更高层上的安全协议（如IPsec）来保证重要信息的安全。

在移动终端使用不透明访问外部IP网络时，由外部Intranet或ISP为移动终端分配静态或动态的IP地址。GGSN用此IP地址与外部Intranet或ISP进行通信，并将返回的信息正确传递给相应的GPRS移动终端，此时需要GGSN与外部IP网络或ISP的地址分配服务器相连。用户对Internet等外部IP网络的访问通过Intranet或ISP进行。在这种方式下，GPRS网络与外部Intranet或ISP之间，用户数据的安全性可以通过双方协商的方法（比如专线连接、隧道方式、使用IPsec协议等）来保证。

4.4.4 GPRS 网络的安全威胁及防范措施

通过对GPRS的安全性能分析，GPRS网络的安全威胁主要来自以下几个方面：

（1）用户终端的身份验证依赖于SIM卡的身份密钥K_i，必须对该密钥重点保护，防止被盗。

（2）在 GPRS 网络的信息传输过程中，三元组信息都采用明文传输，其安全性可能受到威胁。

（3）产生身份验正信息SRES的A3 算法，产生数据加密密钥K_c的A8 算法和GPRS数据加密算法GEA是保密的，无法评估其安全性能。

此外，GPRS终端通过GGSN与外部IP网络实现互联后，还会受到来自网络的安全威胁：

（1）GPRS网络中的用户信息以及路由表信息都是明文保存的，有可能受到非法窃取和破坏，需要受到严密的保护。

（2）外部网络可以向GPRS用户发送数据。由于GPRS按流量计费，大数据量的电子邮件将给用户造成经济损失。

（3）来自GPRS网络内部的恶意用户或用户移动终端中的病毒程序可以发送

GPRS数据和信令消息来影响GPRS网络及其用户的行为。

为了解决这些安全隐患，GPRS网络必须正确配置SGSN和防火墙，禁止外部网络对它们的配置操作，并严格管理内部网络数据。同时，GPRS还必须不断改进自身的安全机制，采用更先进的安全技术，同时采用不公开的应用层加密策略提高系统安全性。

为保证GPRS网络中数据传输的安全性，除充分利用GPRS自身的安全措施外，还可以采用个性化的应用层加密策略。在发送方和接收方定义密钥和相关算法，该密钥不需要传输，同时算法不公开。加密算法需要完成两个目标，其一是按照约定的方法验证数据的合理性，感知数据被窜改并采取相应措施；其二是数据加密，即使在GPRS本身的数据加密方法被攻陷后，传输的数据仍具有保密特性，防止信息被窃听。