

GPRS 在 SCADA 系统中的应用与实现

王延政,李瑞祥,王立青

(上海理工大学 光电信息与计算机工程学院,上海 200093)

摘要: 针对远程复杂环境下 RTU 设备与 SCADA 系统数据中心的通信问题,提出了一种基于 GPRS 网络的 SCADA 系统的实现方案。简要介绍了 GPRS、SCADA 的基本知识,描述了 GPRS 无线传输应用于 SCADA 系统的组网方案。

关键词: GPRS; SCADA; AT91SAM9261; 抗分组丢失

中图分类号: TP39; TN919

文献标识码: A

文章编号: 1674-7720(2011)09-0001-03

Application and implementation of GPRS to SCADA system

Wang Yanzheng, Li Ruixiang, Wang Liqing

(School of Optical-electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: Aiming at the communication question of the RTU and the data center of the SCADA system in the remote complex environment, this paper proposes a SCADA system based on GPRS network. In this paper, the basic knowledge of GPRS and SCADA is briefly introduced, and the GPRS wireless network scheme used in SCADA system is described.

Key words: GPRS; SCADA; AT91SAM9261; anti-packeting loss

随着信息技术、特别是无线网络通信技术的迅猛发展,信息的传递以及人与人之间的交流更加方便和快捷。在许多领域的 SCADA 系统中需要对大范围的 RTU 设备进行自动、及时的数据采集、传输、处理以及控制指令的下达,以便及时掌握和控制现场情况。而这些 RTU 设备大多分布范围广、数量多、分布零散、距离远且地域复杂。当前 SCADA 系统使用最广的有线或短距离无线通信方式,显然已经不能满足要求。基于 GPRS 无线网络的 SCADA 系统可以摆脱线缆的束缚,具有安装周期短、维护方便、扩容能力强、成本回收快等特点。而无线 GPRS 网络所具有的永远在线、按流量计费和传输速率高等突出特点,特别适合于 SCADA 系统这样间断、突发性的或者频繁、中小流量的数据传输系统。无线网络由网络提供商维护,遵循全球统一的技术标准和通信协议,可跨地域实现对 RTU 设备的监测与控制,是 SCADA 系统发展的趋势。

1 GPRS 技术、SCADA 简介

通用分组无线业务 GPRS (General Packet Radio Service)是在现有 GSM 系统上发展起来的一种新的承载业务,目的是为 GSM 用户提供分组形式的数据业务,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、

低成本的无线分组数据业务。GPRS 充分利用共享无线信道,实现了与标准 Internet 的无缝连接,采用 IP Over PPP 实现数据终端的高速、远程接入。GPRS 理论上可提供高达 171 kb/s 的传输速率(实际应用中大约为 20~40 kb/s)。无线 GPRS 网络所具有的永远在线、按流量计费、传输速率高以及支持 X.25 和 IP 协议等突出特点,特别适合于 SCADA 系统这样间断、突发性的或者频繁、中小流量的数据传输。

SCADA (Supervisory Control And Data Acquisition)系统,即数据采集与监视控制系统。SCADA 系统的应用领域很广,它可以应用于电力系统、给水系统、石油、化工等领域的数据采集与监视控制以及过程控制等诸多领域(在电力系统以及电气化铁道上又称远动系统)。SCADA 系统是以计算机为基础的生产过程控制与调度自动化系统。它可以对现场的运行设备进行监视和控制,以实现数据采集、设备控制、测量、参数调节以及各类信号报警等功能。

2 系统的组网方案

现场 RTU 设备采集到数据后,通过 GPRS 模块将数据发送到监控中心。而 GPRS 模块与监控中心的连接总体上有两种方案:GPRS+Internet 连接和 GPRS 内网连接。由于 GPRS 内网连接的组网方式存在着运营成本较

综述与评论 Review and Comment

高等缺点, 在本文中采用 GPRS+Internet 连接的组网方式。系统拓扑结构图如图 1 所示。

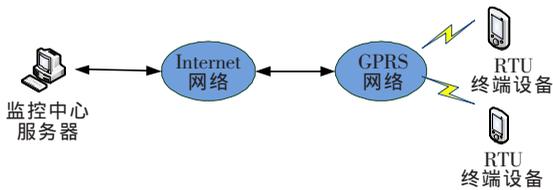


图1 SCADA网络拓扑结构图

在该方案中监控中心采用 Internet 接入, 其接入方式也有多种形式, 只要是能够获取公网 IP 地址即可。这种组网方式较 GPRS 内网连接的组网方式安全级别低, 但是可以通过由移动运营商经 VPN 隧道连接至监控中心的服务器, 这样可以大大提高系统的安全级别并且可以减少时延。由于实验条件的限制, 本监控中心服务器采用 ADSL 的接入方式。由于这种接入方式服务器的 IP 地址是随机的, 而在 RTU 设备上配置的是服务器某一时刻的 IP 地址, 因此一旦监控中心服务器的 IP 地址发生了变化, 除非马上重配置 RTU 设备(实际很难做到), 否则就没有办法访问监控中心的服务器, 系统不能工作。针对这种情况国内已提出两种解决方案——动态域名技术和端口映射技术。本文采用的是动态域名的解决方案。所谓动态域名就是当主机的 IP 地址发生了变化, 此域名(不会变)就对应这个变化的 IP 地址。动态域名技术的工作原理: 为接入 Internet 的主机申请一个动态域名, 然后在主机上安装一个软件, 随时检测主机的 IP 变化情况, 一旦有变化就访问域名服务器, 把当前 IP 地址更新到域名服务器相应数据库表单中, 这样对方只要根据这个域名到分布在 Internet 上的域名服务器上查找就可知当前对应的主机 IP 地址。

3 系统的实现

3.1 终端部分

RTU 设备在 SCADA 系统中的主要作用就是实现对现场数据获取、监控中心指令执行以及数据的传输。该部分主要由数据采集模块、控制执行模块、电源管理模块、微处理器和 GPRS 模块等部分组成。数据采集模块主要完成现场温度、湿度、光度、设备运行状态参数以及现场视场图片信息等数据的采集, 并经过微处理器处理后经由 GPRS 模块发送到系统监控中心服务器。控制执行模块主要完成系统监控中心发送的执行指令, 包括调控设备运行状态、调控现场温度等操作。电源管理模块主要是对 RTU 设备各模块供电, 并采用太阳能电池板加蓄电池的设计方案, 以实现设备在复杂恶劣环境下的自生存能力, 采用先进的电源管理方案, 实现系统的低功耗设计。GPRS 模块的主要功能是实现 RTU 设备与监控中心服务器之间的数据传输。RTU 设备终端硬件结构框图如图 2 所示。

3.1.1 终端硬件平台

采用 Atmel 公司的工业级 ARM9 处理器 AT91SAM9261,

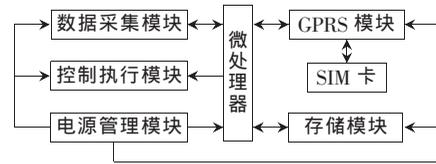


图2 RTU设备硬件结构

该处理器是以 ARM926EJ-S ARM Thumb 处理器为核心的完全的片上系统, ARM926EJ-S 属于 5TEJ 版的 ARM 架构, 针对的是多任务的应用, 包括全存储器管理, 高性能、小核心尺寸和低功耗都是其重要的特点。

3.1.2 终端软件平台

本系统 RTU 终端软件采用嵌入式 Linux 系统架构实现对终端各设备的控制管理及数据的处理和存储, Linux 提供了完成嵌入功能的基本内核和所需要的用户界面, 能够处理嵌入式任务和用户界面。Linux 作为嵌入式系统, 是一个带有很多优势的新成员。Linux 对许多 CPU 和硬件平台具有易移植、稳定、功能强大、易于开发的功能。嵌入式 Linux 操作系统的内核和文件系统都可配置, 系统能够裁剪到足够小, 以适应嵌入式系统运行和存储的空间限制。同时可通过补丁改进系统的实时性, 实现操作系统的软实时性。

3.1.3 终端数据采集

RTU 设备的主要作用就是获取现场数据并通过一定的传输方式传送到 SCADA 系统的数据中心, 以供分析与处理。RTU 设备所要获取的数据包括设备现场有关设备运行状况、环境状态等参数数据以及设备现场的图像数据信息。由于图像信息数据量大, 图像的处理、传输对硬件环境的要求相对较高, 目前常用的处理方法有以下两种: (1) 采用高速视频 A/D 转换器结合专用的同步信号提取芯片采集, 这种方法的电路较为复杂; (2) 使用专用的视频处理芯片实现模拟信号的数字化以及行、场同步信号的提取, 然后送入处理器。这种方法的特点是处理器只需对专用芯片进行配置, 而不参与采集过程。

本文中图像信息的采集是通过 USB 摄像头实现的, 因此需要将 USB 驱动加载到系统内核中。由于动态加载方式测试较为简单, 该系统采用动态加载方式。系统使用 v4l 实现对图像采集的控制。考虑到摄像头监测的是静态图像的视觉状况, 是缓变信号, 间隔时间较短的前后两幅图像具有很强的相似性, 如果直接对单幅图像进行压缩就无法利用前面已经获知的信息, 压缩效率低, 故在该系统实现中采用对差值图像进行压缩的处理方法。系统接收到 USB 摄像头拍摄的实时图, 首先将其与存储器中的基准图进行配准, 然后以像素对应的方式相减; 进行分块、DCT 量化以及熵变化, 并进行图像压缩。压缩后的数据流按最大 256 字节拆分, 并将各帧通过 GPRS 网络依次发送出去。数据中心将接收到的图像数据依次经过熵解码、反量化、IDCT 变换后恢复差值图像, 并与基准图像进行矩阵相加, 以恢复实时图像。

综述与评论 Review and Comment

3.1.4 无线数据传输的实现与传输控制

系统的无线数据传输是通过内嵌有 TCP/IP 协议的 GPRS 模块实现的。目前市场上提供的 GPRS 无线模块有 WAVECOM 的 Q2403B, 西门子的 SIEMENS、MC35i、MC39i, 摩托罗拉的 G20 等。本系统选用了西门子的 SIEMENS300C。SIEMENS300C 是高性能高稳定工业级的 GSM/GPRS 无线模块, 适合长期连续工作, 抗干扰能力强。SIEMENS300C 是新一代的 900 MHz/1 800 MHz 双频自动选择的无线模块, 内嵌有 TCP/IP 协议栈, 无需微处理器的支持即可实现基于 TCP/IP 的数据传输。其支持标准的 AT 命令及增强的 AT 命令监护数据模式, 功能强大、操作灵活方便。微处理器可以通过标准串口接口 RS232 与 SIEMENS300C 通信。它向用户提供了标准的 AT 命令接口, 为数据传输提供了快速、可靠、安全的传输通道, 方便用户进行实际应用的二次开发设计。

由于 GPRS 网络的不稳定性且基于 GPRS 网络的 IP 信道存在着很多的干扰, 丢包、不均匀延迟的情况时有发生。针对这一问题本文采用了一种无线传输的抗分组丢失算法对传输的数据做进一步的处理, 以确保数据传输的可靠性。该算法的基本思想是: 在编码效率 η 不变的前提下, 将长数据分成若干短数据, 分别进行 RS 编码, 以获得随数据长度呈线性增长的编解码时间, 但这样会减弱其抗突发干扰能力, 因此, 采用交织技术将行码序列变换为并码传输, 使信道传输过程中产生的突发错误离散化, 以达到原有 RS 纠错编码的纠错性能。算法由编码算法和解码算法构成, 数据的发送与接收过程如图 3、图 4 所示。



图 3 抗分组丢失算法数据发送过程图



图 4 抗分组丢失算法数据接收过程图

3.2 监控中心

监控中心负责接收远程监控终端传回的实时数据, 并对其进行分析、处理及储存, 同时将监控中心的指令信息发送给终端的软件控制平台。远程监控终端的数据通过 GPRS 网络经由网关传到 Internet, 然后找到监控中心的主机。监控中心是 SCADA 系统的中枢, 是整个系统可靠高效运行的关键。

监控中心的软件设计充分考虑了系统功能的完整性和扩展性以及系统的可靠性和兼容性。监控中心的软件系统主要由通信服务器、数据库服务器和 Web 服务器模块三部分组成。

通信服务器程序采用 VS2005 进行开发, 主要实现与远程终端的通信以接收 RTU 终端传回的实时数据, 同时向 RTU 设备下达监控中心的控制指令等功能。该部分程序采用 Socket 编程, 实现与 RTU 设备之间的 TCP/IP 连接以及数据的传输。同时嵌入了抗分组丢失算法的程序, 实现对传输数据的控制功能。

数据库服务器采用 SQL 2005 进行设计, 主要实现对 RTU 设备传回数据的管理、远程 RTU 设备的管理、系统管理人员数据的管理以及管理员权限的管理等功能。

Web 服务器采用 ASP 架构开发, 主要是实现监控中心实时数据的发布、报表生成以及数据的分析等功能。系统采用 B/S 架构, 管理人员只需通过浏览器登录 Web 服务器即可实现对 SCADA 系统的管理与维护, 无需安装客户端软件。系统对管理人员权限的分级审查制度确保了系统数据的安全性和稳定性。

采用 GPRS 无线传输技术进行数据传输的 SCADA 系统, 其终端具有安装部署简单、工程建设周期短、扩充性强、可靠性高、传输速率高、实时性强等优点, 从而解决了 SCADA 系统中监控点多而且分布范围广的监控难点。同时采用嵌入式高性能、低功耗的 ARM9 微处理器作为远程终端设备的微控制器, 能够更好地利用终端资源, 实现对设备现场的图像信息采集, 给管理人员提供感官上的监测数据, 同时可实现设备现场的防盗功能。

无线 GPRS 网络所具有的永远在线、按流量计费、传输速率高、支持 X.25 和 IP 协议等突出特点, 以及其终端设备安装方便、受外界环境干扰小等优点, 使得在远程复杂 SCADA 系统中采用 GPRS 技术进行数据传输成为一种趋势。伴随着国家数字移动通信技术的不断推进与成熟, 采用移动网络作为承载网络的 SCADA 系统将会得到更加广泛的应用, 也必将成为一个新的研究热点。

参考文献

- [1] 周雪松. 基于 GPRS 远程监控系统的研究[J]. 机械设计与制造, 2010(1): 148.
- [2] 刘艺. 基于 GPRS 的低压配电网远程监控的相关问题研究[J]. 电气应用, 2009(23): 52.
- [3] 张灯灿, 林春深, 万晋, 等. 用于 GPRS 无线传输的抗分组丢失算法[J]. 计算机工程, 2009(11): 283.
- [4] 黄新波. 输电线路在线监测与故障诊断[M]. 北京: 中国电力出版社, 2008.

(收稿日期: 2010-12-03)

作者简介:

王延政, 男, 1986 年生, 硕士研究生, 主要研究方向: 嵌入式系统及无线数据传输。

李瑞祥, 男, 1967 年生, 工程师, 主要研究方向: 嵌入式系统。

王立青, 男, 1984 年生, 硕士研究生, 主要研究方向: 嵌入式系统。