构建 GPRS 工业监控系统的关键技术研究

袁建伟 华中科技大学材料科学与工程学院(430072)
刘从新 曾维鲁 三峡大学电气信息气学院 (443002)

Abstract

Having analyzed the implementation difficulties of construction GPRS monitor & control system,this paper puts forward some effective measures to the problems.Finally,a virtual wireless communication system based on GPRS is implemented.

Keywords:GPRS,monitor control system,communication,wireless

摘 要

分析了构建基于 GPRS 的监控系统的实现难点,给出了相应的解决办法,并设计出了实际的无线监控系统。

关键词:GPRS,监控系统,数据通信,无线

现在有许多企业都存在一些作业点分散于野外,环境恶劣,需要无人值守和远传控制,用有线来做通信媒介无论从技术或成本上来讲都不太合适,这迅速推动了无线通信技术在工业控制领域的应用和发展。本文采用 GPRS+TCP/IP 协议使得工业监控系统的监控空间延伸到了移动网+Internet。

1 GPRS 的主要特点

1) 充分利用现有资源——中国移动全国范围的电信网络(GSM),方便、快速、低成本地为用户数据提供远程接入。GPRS 数据传输速度可达到 57.6Kbps,最高可达到 115Kbps-170Kbps,完全可以满足用户应用的需求,下一代 GPRS 业务的速度可以达到 384Kbit/s;

2)接入时间短。GPRS 接入等待时间短,可以快速建立连接,平均为 2s;

3)提供实时在线功能。用户将始终处于连线和在线状态,这将使访问服务变得非常简单、快速;

4)按流量计费。GPRS 用户只有在发送或接收数据期间才占用资源,用户可以一直在线,按照用户接收和发送数据包的数量来收取费用,没有数据流量的传递时,用户即使挂在网上也是不收费的。

从上所述的 GPRS 特点可以看出 GPRS 网络特别适合于频发小数据量的实时传输。

工业的远程数据采集系统就是一个比较典型的频发小数据量的实时传输系统。

2 GPRS 监控制系统的组网方式

构建基于 GPRS 的无线数据通信系统一般有下面两种方式。

(1)外网方式(SM-MH,DH-MH)

这种方式(如图 1 所示)是指 GPRS 监控系统的某些组成部件在 Internet 上,为了支持这种方式,往往需要租用专线来满足业务的要求。工业数据采集系统的流量是间断性的,有的应用甚至以小时和天为上传周期,租用专线传输,资源的利用率不高,经济上也不合算。该种组网方案的优点是可以简化 GPRS DTU(Data Transmission Unit)的设计复杂度,系统的性能比较稳定、可靠性高。当然也可以采用 ADSL 拨号的方式来接入监控主机,但是这种方式除了存在下面将要提到的动态 IP 地址互相访问的问题外,同时还存在系统安全难以得到保障的问题。

(2)内网方式(MH-MH)

这种构建方式(如图 2 所示)是指整个监控系统的各个重要组成部件都在 GPRS 网络内部,并没有进入到 Internet。很明显按照这种方式构建的监控系统其安全性比外网方式要高得多,构建过程更加方便与快捷,构建成本也更低。

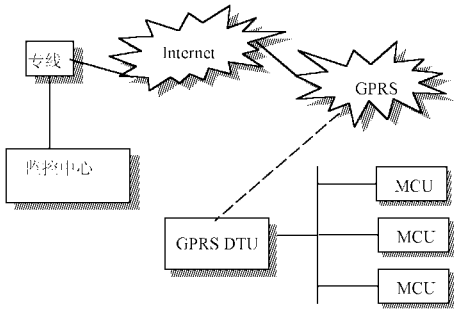

图 1 外网方式的 GPRS 系统

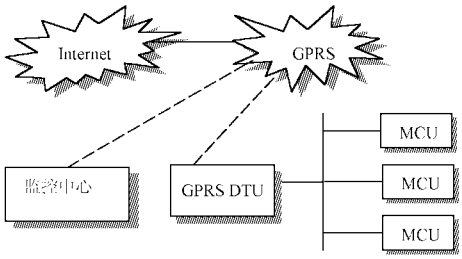

图 2 内网方式的 GPRS 系统

3 以 GPRS 内网方式构建监控系统存在的问题及其应对策略

(1)动态 IP 的互相访问的问题

从图 2 可以看出监控主机和被监控设备像手机一样都是通过拨号上到 GPRS 网络,ISP 提供给它们的 IP 地址都是动态分配的,那么一个很明显的问题就是它们之间如何寻找到对方,就算网络在初始化的时候通过人工电话解决了该问题,那么在系统的运行过程中出现主机和从机都断线后,系统将如何重建?

我们的解决方案是:SMS(Short Message Service)+邮件来确保系统在一个确定的时延内自动建立或恢复系统之间的连接。SMS 可以方便地实现系统各个部件之间的通信联络,其不足是实时性和确定性得不到保证,所以这里再增加邮件的功能可以弥补 SMS 的不足。

网络连接的构建过程可以这样描述:

从机上线,GPRS DTU (GPRS Data Transmission Unit)首先发送短消息给 GPRS AS(GPRS Access Server),并且报告其 IP 地址,在规定时延内 GPRS DTU 如果得不到 GPRS AS 的回应,其立即发送电子邮件到互联网上的一个商业电子

邮件服务器（如 263），GPRS AS 在例行时间段内没有得到 GPRS DTU 的短消息或者其采集的数据，并又无法对其实施控制，其马上到互联网上既定的电子邮件服务器取信件，从而获得对方的 IP 地址，这个方案可以使网络各部分间的联络时延限定到一个较小的确定的时间段内，系统的实时性可以得到保证。

(2)监控主机断线及软件的自动重新拨号的问题

如果成功解决了动态 IP 的互相访问题，那么这样的 GPRS 数据传输终端是否就可以进入实际应用呢？答案是不能。原因是由于 GPRS 网络的工作特点使得监控主机在接受设备群的接入时，普遍存在断线的问题，这使得 MH-MH 方式的组网方案又得增加了一个必须具备的条件，那就是要求中国移动提供静态 GPRS 内网 IP 地址给监控主机，否则当监控主机断线后，利用目前的已有产品的解决方案很难重建系统，原因是由于这些产品缺乏高层协议（针对 GPRS 链路的工作特点而制定的协议）的统一指挥，系统并不具备处理异常情况的能力，遗憾的是目前开通静态 GPRS 内网 IP 地址服务的城市还很少。退一步讲，就算在静态 GPRS 内网 IP 地址服务开通的情况下，采用目前已有的解决方案，系统的通信中断也是在所难免，系统的整体工作性能肯定会受到很大的影响。

从上段的分析可以看出，GPRS 网络的断线给系统运行的稳定性带来了很多的问题，但是还有一问题却更棘手，那就是主机断线后要靠人工拨号来重新上线，原因是 GPRS DTU 没有觉察到自己已经断线，这个问题带来的后果就是 MH- MH 组网方案的失败，从而迫使企业采用专线的方式来组建 GPRS 监控网络。

对于这个问题我们采用的应对策略是：

首先，我们将 GPRS 数据传输终端分开设计为 GPRS DTU 和 GPRS AS，见图 3。

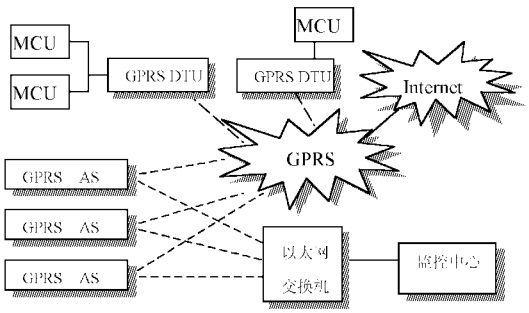

图 3 一个比较实用的 GPRS 监控系统

系统工作过程的描述：

1)平稳过渡过程：在图 3 的组网拓扑中，各个 GPRS AS 都运行自定义的 RBP(Redundancy-Backup Protocol)，当某条链路断线的时候，其所属 GPRS DTU(具备自适应机制)可以迅速切换到其它的 GPRS AS。接到别的 GPRS DTU 数据的 GPRS AS 立即发送一个指令到已经断线的 GPRS AS 要求其立即重新拨号，断线的 GPRS AS 上线后将其 IP 地址通知“加负荷”的 GPRS AS，该服务器在数据的回应包中，给出断线 GPRS AS 的新地址，收到新地址的 GPRS DTU 开始向其“原来”的 GPRS AS 发送数据。

2)平滑过渡过程(所有 GPRS AS 同时断线)：多个 GPRS AS 通过 10M/100M 的以太网互连，一直在不停地交流各自的负荷信息和各种动态表(下面将有叙述)，如果它们的负荷都为 0 的时间超过 1 个最小时限后，GPRS AS 逐个拨号上线，再通过以上相似策略，逐渐分配流量，系统过渡平滑；为了避免“短消息风暴”和误操作，GPRS DTU 在不能和 GPRS AS 群通信后等待 2~3 个最小时限，然后重新拨号上网，并主动发起和 GPRS AS 的连接。

在平稳过渡过程中整个切换过程十分自然，系统性能几乎没有受到任何影响、系统数据流量几乎没有增加，这里的依据是 GPRS AS 断线的周期要大于 GPRS AS 重新拨号上线的所用的时间；平滑过渡过程发生的概率低，流量有微弱增加，系统恢复到正常运行有一个小的时延。

(3)设备群接入规模受限的问题

其实在解决监控主机断线问题的同时，这个问题也就得到了解决，当用户要扩容的时候，只要增加 GPRS AS 的个数就能增加系统的规模，GPRS AS 的个数越多，系统的健壮性就越好。

(4)增强系统的安全性的一些技术措施

在分析了 OTP(One-Time Password)系统工作原理的基础上，我们拟采用以下面的方案来增强数据的可靠性：

1)远程操作指令格式为 ID(16bit)和操作码(16bit)。ID 是控制者的身份标识，操作码是对操作行为的 16 位编码。

2)在 GPRS AS 上建立服务器 ID、密钥(32bit)和结合策略的对应表；在 GPRS DTU 上建立服务器 ID、密钥(32bit)和逆结合策略的对应表。

3)定义一组适合 MCU 运算的加密算法(N 个)和相应的解密算法(N 个)，二者分别存储在 GPRS AS 和 GPRS DTU 上。

4)数据发送端将原始数据和相应密钥作结合运算产生结合数据包。

5)数据发送端随机产生一个(1~N)中的序号，然后用这个序号对应的算法来加密结合数据包，同时让这个序号成为 TCP 数据报的序号，数据接收端根据该序号找到相应的解密算法。

6)接收端经过两次解码运算，可以得出原始数据：ID 和操作码，检查 ID 和本地 ID 是否一样，不一样则丢弃该包，并发回 N-ACK 包；反之，则继续检查操作码是否属于本地的操作码表，是则进行操作，不是则发回 N-ACK 包；发送方在收到 N-ACK 后，又选择新的密钥和新的结合算法，重新完成 D-F。

7)如果是远动命令，则采用发送多个数据包，在接收端进行核对的方法来确保数传输的正确性。当然为避免多个包被截获后，反而成为解密的参照物，所以每个原始数据都要经过 D-F 过程。

该应对策略有如下特点：应单片机的特点，不选择复杂的加密算法，取而代之构建适合 MCU 的加密算法集合；“动态”产生加密算法，“动态”产生结合算法，“动态”产生密钥，使得同样的原始数据在网络上传输的数据包都是不一样的；本该明文传输信息也被隐蔽地隐藏在 TCP 的包头之中，基本上就不会引起攻击者的注意。

本加密策略至少确保了数据在 GPRS 链路上的完整性，当一个受损的数据包到达时候，其被拒绝的概率是：

$P=100*(1-3*20/2^{32})\%$

这里假定有 4 个 GPRS AS 和 20 种远端操作指令。

4 监控系统设计与实现

按照以上的策略，我们设计实现了一套基于 GPRS 的监控系统。

(1)GPRS DTU(GPRS Data Transmission Unit)

硬件芯片：8051、MC35(西门子的 GPRS Modem)

嵌入开发环境：μCos/II

实现的协议：TCP/IP，PPP，POP3 和 SMTP；这些协议是经过精简和扩充的，扩充的主要方面是使它们具有一定的智能，在

监控系统中断时,能自动采取既定的应对策略,迅速恢复和监控制主机间的通信。

实现的功能:将设备接入到 GPRS 网络,支持以多种工作模式(永久在线模式、定时传输模式、中心呼叫模式、数据触发模式、节电模式)上传采集到的数据,在通信异常的情况下,能迅速建立与 GPRS AS 和管理者的联系,具备接收并执行监控主机和 GPRS 服务器发来的命令、支持嵌入式程序控制的功能。图 4 是 GPRS DTU 的结构图。

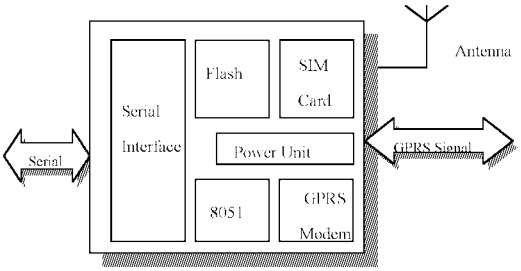

图 4 GPRS DTU 的结构图

(2)GPRS AS(GPRS Access Server)

硬件芯片:S3C4510B、MC35

嵌入开发环境:μClinux.

实现的协议:TCP/IP、PPP、POP3、SMTP、RBP (自定义的 GPRS AS 间的通信冗余的协议),这些协议也是经过改进的协议,具有一定的智能,在既定策略的控制下有条不紊的运行,整个监控系统稳定性和鲁棒性都比较强。

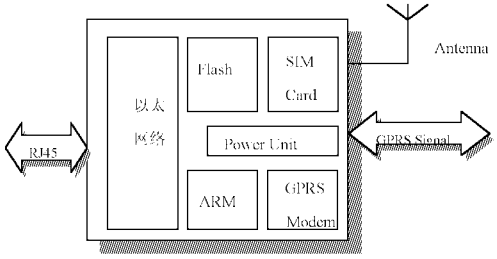

图 5 GPRS AS 的结构图

实现的主要功能:GPRS AS 是整个监控系统的通信联络中心,负责设备群的远程接入,在系统通信发生异常情况下能协调系统的各个部分,使其迅速恢复到正常的运行状态;支持多个 GPRS AS 之间流量均衡和流量的分摊,支持多个 GPRS AS 共同服务于一个或者多个监控主机。建立了 GPRS DTU IP 地址和设备 ID (Identification) 的对照表,实现了监控主机和 GPRS AS 之间数据的透明传输,如:设备 ID+监控数据、设备 ID+命令;另外,系统还"动态"地保留了和每个 GPRS DTU 连接信息,实现了 GPRS AS 和 GPRS DTU 的"永久虚连接"。

(3)监控主机中短消息模块

在本系统中,监控主机可以将采集到的重要数据以短消息的形式发送到管理者的手机。在监控主机还建立了短消息库和相应的管理工具。

(4)本系统和现有组建 GPRS 监控网络方案的技术性能和成本比较见表 1。

表 1 本系统和现有其他方案的技术性能和成本比较表

项目 / 组网方式	主机的线路费(元/月)	移动或 ISP 的特殊服务	服务提供的可能性	设备群规模	监控主机断线否	构建成本(相对)	安全性
SM-MH(专线)	2000(64K)	专线	一般	不受限	否	高	高
DH-MH(ADSL)	600(包月)	公网动态 IP	一般	不受限	断线	较高	低
MH-MH 现有方案	200(包月)	内网静态 IP	小	受限	断线	中	高
MH-MH 本系统	200-400(包月)	无要求	100%	不受限	否	低	高

(注:SM:static Host,DH:dynamic host,MH:move host,以上报价来自中国移动(宜昌))

经过上表简单的对比,我们可以发现:现在可以进入实际应用的方案只有 SM-MH 方式,我们构建的系统其稳定性和可靠性可以和 SM-MH 相比,在组网的方便性、设备群体的接入规模和成本方面却占有很大的优势,从运行成本讲,在满负荷运行下(以上面的参数为参考),同样的投入,本系统可以接入的设备群规模是 SM-MH 的 10 倍以上;在欠负荷情况下,SM-MH 要亏本;SM-MH 方式扩容成本高,若采用本系统,是否扩容掌握在用户手里,随时可以扩容,几乎没有上限,而增加的成本又比较低,所以本系统在中小型企业建设 GPRS 监控网络可能会得到比较广泛的应用。

5 结束语

目前该系统已经地应用到了本地某水利部门的防汛、防洪监控网,其性能正在进一步的测试之中。本系统的下一步工作就是扩充该系统使其具备 VPN(Virtual Private Network)的功能,为企业创建跨省的监控系统提供技术支持。

参考文献

1 哲伟. 线环境中 TCP 性能的分析和改善. 北京邮电大学硕士论文 2001

2 杜吉荣.GPRS 环境下 TCP 协议的性能分析与改进.浙江大学硕士论文,2002

3 Http://www.hongdian.com.深圳宏电科技开发有限公司

[收稿日期:2004.12.25]