

基于嵌入式系统的串行设备远程监控系统^①

刘小虎 黄以平 (桂林电子科技大学 机电工程学院 广西 桂林 541004)

摘要: 本文借鉴了 IT 领域中常见的远程监控的实施方案。从应用的角度出发设计出了一种实时、可靠的串行设备远程监控系统,使原本不具备联网功能并分散各地的串行设备连接到以太网中,充分利用现有的 Internet 资源进行数据传输和管理。通过研究嵌入式 S3C2440 模块的串口以太网通讯,设计了软件的实现方案,在串口以太网通讯中应用多线程技术,实现了串行设备的串行协议与 TCP/IP 协议的转换。方案中利用 OpenVPN 建立远程隧道链接,通过 telnet 远程登陆嵌入式平台,对嵌入式端进行监控。经过实验测试,串行数据在远程监控的计算机上具有良好的一致性,实现了对串行设备的监控。

关键词: 嵌入式; 串口; 以太网; 协议转换; 多线程; 串行设备

Serial Device Based on Embedded System Remote Monitoring System

LIU Xiao-Hu, HUANG Yi-Ping

(Mechanical and Electrical Engineering College, Electronic Technology of the Guilin China University, Guilin 541004, China)

Abstract: This article draws on domain of common IT remote monitoring of the implementation of the plan. From the application point of view to design a real-time and reliable serial device remote monitoring system, causes not to have the networking function originally and to disperse the regional serial devices is connected in the ethernet, make full use of existing Internet resources for transmission and management of data. Through studies the embedded S3C2440 the module of serial port ethernet communication, designed a software program to realize, serial port ethernet communication applications in the multithreading technology, achieved serial device serial protocol and TCP/IP protocol conversion. In the program establish a remote tunnel link using OpenVPN, remote login through telnet embedded platform to monitor the embedded end. The experimental test serial data in remote monitoring and control of the computer has a good consistency and achieved the monitoring of serial devices.

Keywords: embedded; serial port; ethernet; protocol conversion; multithreading; serial device

1 引言

随着互联网的快速发展,互联网总线技术在现代工业的各个领域中都得到了广泛的应用,传统的工业控制中使用的串行总线技术对于分散于各个的现场的串行设备难于进行集中管理,控制手法单一及系统运行可靠性低。这就需要对传统的串行控制总线进行升级,以太网总线以其高速的数据传输和可靠的技术成为首选,使用嵌入式设备连接若干个串行设备,把串行数

据转换成以太网上传输的数据,将方便远端机接收和管理^[1]。因此,必须设计出一种通信协议转换机制,能将 RS232/485 串行总线的数据格式与以太网 TCP/IP 数据进行转换,无需淘汰现有设备,节约了投资成本,且对监控程序无需作任何修改,能非常快捷便利的将传统的串行控制总线送入流行的以太网通道。

而现代工业生产智能化的不断发展,除要求企业将分布式生产设备和测量仪器相互连接,并能实现生

^① 收稿时间:2010-03-04;收到修改稿时间:2010-04-16

产数据和管理数据共享外,还要生产人员能在办公室或更远端对现场的设备仪表进行远程监控,远程监控已成为工业控制领域发展的必然趋势。

远程监控系统是近年来工业自动化控制领域的一个研究热点。远程监控是指通过计算机网络实现对远程受控对象的监视和控制。远程监控系统是由本地和远端共同构成的能够实现远程监控功能的软硬件系统。远程监控系统是信息网络与控制网络结合的产物,它集中了现代计算机技术、网络通信技术、传感器技术、自动控制技术和人机交互系统技术等,在许多领域有广泛的应用,如生产过程实时监控、图像远程监控、电力综合监控、动力设备集中监控、水利系统监控等。数据通信是远程用户与现场设备的连接中枢,用户与控制现场进行数据交互才能实现对现场设备的远程监控。

针对上述情况,本文设计了一种基于 **s3c2440** 和 **linux** 操作系统的串口以太网转换的远程监控系统的实现方案。总体框图如图 1 所示。

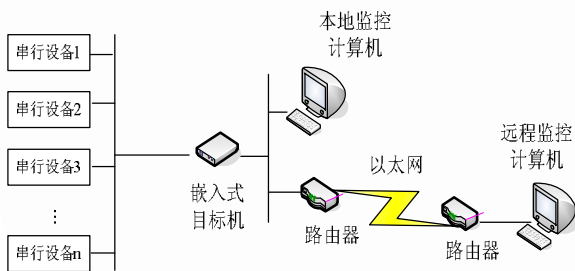


图 1 串行设备远程监控系统总体框图

2 串行设备远程监控的串口以太网通讯构建

串行设备远程监控的嵌入式系统主要功能是实现串口数据和网络数据的处理与转发。嵌入式硬件平台使用的是 **s3c2440**, **s3c2440** 是韩国三星公司生产的一款 32 位 RISC 处理器,具有低功耗、高性能、成本低和使用简单的特点,提供 3 个独立的异步串行 I/O 端口,每个都可以在中断或 DMA 模式下工作,每个 UART 通道包含 2 个 64 字节的 FIFO 部件,分别用来接收数据和发送数据。嵌入式目标机的工作方式:目标机将要发送的串口数据以及对应串口号等信息转换为以太网络数据,发送到以太网上,而接收到经以太网传送过来的数据后,从中提取串口数据以及串口号等信息,而后转发到相应串口设备。

嵌入式软件系统设计则是本文主要研究重点,

主要是网口数据与串口数据相互转发和远程传输软件设计。软件设计采用客户机/服务器(C/S)模型,在目标机上实现串口以太网的通讯功能并把此功能应用在嵌入式硬件环境下,避免因为硬件不同而须重新设计软件。系统采用 **Linux** 操作系统,它具有成熟的 **TCP/IP** 网络协议支持以及多线程应用程序处理能力,保证了串行设备数据的可靠性及实时性。数据转发程序主要是基于通讯协议转换及多线程程序技术。

2.1 串口以太网通讯协议转换和传输的实现

串行设备的远程监控嵌入式系统实现首先针对串行链路和网络接口之间的通信数据进行判断、转换与传输,对来自串行设备的数据帧进行处理,使之成为可以在网络中传输的数据帧;对来自网络接口的数据帧进行判断,转换成串行数据帧并送往串行设备。程序编写前要对网络数据帧和串口数据帧有所了解,要实现网口与串口透明传输通讯功能,首先要定义串口帧格式,要在以太网上传输就必须加上 **TCP** 包头及 **IP** 包头,转换为串口以太网数据帧格式。串口网络数据帧格式如表 1 所示。

串口网络数据帧				
IP头	TCP头			
	串口数据帧			
	起始位 (1)	数据位 (8)	奇偶位 (1)	停止位 (1)

表 1 串口网络数据帧格式

远端机收到网络数据帧后,解析出串口数据帧,传输给相应的应用程序。应用程序发送数据的过程与此相反,只须将串口数据打包成网络数据包,经过远程传输后在目标机上解析出串口数据帧发送到串行设备。

为了确保数据收发的实时及可靠,本文对来自串行设备的数据采取了一定的策略进行打包。由于串行设备发送到远端主机的数据量在某些时间段具有很大的不确定性,所以在对来自串行设备的数据进行打包,使之成为可以在以太网络中传播的网络数据帧时,要充分考虑到数据包的大小以及数据传送前的等待时间,在确保数据实时传送的同时也要防止系统数据量过大。本文设计了待发送的数据包的大小,该数值通常为用 **TCP/IP** 协议传输时一个数据包的最大值。在收到串行设备发送的串口数据后,数据打包进行网络传输前的等待时间取值为通过串口传送大约 100 个数据

所需的时间, 该时间随串口属性设置的变化而变化。根据系统运行的实际情况, 等待时间的具体取值还可以进行一定的调整。

以太网采用 TCP/IP 协议传输数据, 因此在传输数据之前远端主机与目标机建立 TCP 连接, 如果连上的目标机不是预设的 IP 地址, 则断开该连接; 如果连上的目标机符合预定设置, 则发送该网络远端主机的数据。当有符合预定设置的新的网络远端主机连接到数据端口时, 系统都会将该远端主机发来的数据送往串行设备。当网络远端主机与本地目标机断开连接时, 关闭本端 socket 连接, 将 socket 描述符从列表中删除。这些为在线参数配置过程中系统关闭所有 Socket 连接以及结束相应子线程提供了保证。由于数据传输采用 TCP/IP 协议, 只有在该特定主机与目标机建立连接之后才能将串行设备的数据送往该主机。这里用全局变量来判断远端服务器是否已经与目标机建立连接, 当符合预设 IP 地址以及端口号的网络客户端连接到设备的数据端口后, 系统会修改全局变量标志通知负责串口至网口数据传输的线程, 自此串行设备的数据可以被发往该目标机, 当与网络目标机断开连接之后, 系统会修改全局变量标志通知负责串口至网口数据传输的线程, 串行设备的数据传输将结束[2]。

2.2 多线程技术在串口以太网通讯中应用

Linux 是一个多用户、多任务的操作系统, 很早就实现了进程机制, 但是使用进程存在很多弊端, 如进程间需要采用一定的手段才能实现数据的通信。相对进程而言, 线程是一个更加接近执行实体, 可以与进程中的其它线程共享数据, 拥有自己的栈空间, 拥有独立的执行序列, 是程序执行的最小单位。多线程作为一种多任务、并发的工作方式, 具有共享资源、高程序响应速度、多 CPU 使用更加有效、能改善程序结构等优点。为实现串口和以太网之间的双向同时数据传输, 本文设计采用 linux 下多线程技术。Linux 的多线程遵循 POSIX 线程接口, 采用多线程的方式灵活高效、收发互不影响。任务主要由 4 个线程来完成: 串口接收数据线程、以太网络发送数据线程、以太网接收数据线程、串口发送数据线程。对线程通讯则采用了互斥锁和信号量的控制机制。通过创建两个数据缓冲区来暂存从网络和串口收发的数据[3]。串口以太网通讯多线程的应用方案如图 2 所示。

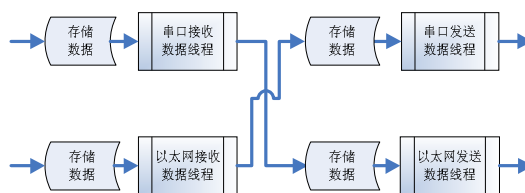


图 2 串口以太网通讯多线程的应用方案

3 串行设备远程监控的嵌入式网络平台构建

网络监控根据距离不同大致分为局域网监控和 Internet 监控。局域网有较高稳定性, 技术也非常成熟, 相对而言, 实际的 Internet 受接入方式和路由限制, 网络延迟大、掉包多、不稳定。因此, 本文应用 VPN 技术建立稳定加密隧道通信, 在嵌入式目标机上启用 Telnet 远程登陆服务, 使服务器可以监控远端嵌入式系统。

3.1 VPN 技术在嵌入式网络平台上的实现

虚拟专用网 VPN(virtual private network)是利用开放式公共网络上建立专用数据传输通道的专用网络技术, 本质上是一种网络互联技术, 在公共的网络基础架构满足企业互联需求和共享网络资源, 并具有与专网一样保证网络用户的安全。VPN 既可以构建于因特网或互联网运营商的 IP 网络之上, 也可以构建于帧中继(FR)或异步传输模式(ATM)等网络基础架构之上, 通过相应的加密和认证技术保证用户的内部数据在公网上安全传输, 实现网络数据传输的专有性[4]。

目前有两种 VPN 不同的实现方式: IPsec VPN 和 Secure Sockets Layer(SSL) VPN。必须根据的实际情况, 选择最适合的安全管理实现方式。目前, 由于 IPsec VPN 提供了对任意传输数据的加密功能, 可有效地保护 IP 数据包的安全, 大多数的 VPN 都采用了 IPsec 的解决方案。而电子商务以及网上银行的快速发展, 网络安全技术取得了长足的进步, SSL VPN 在一些应用中有逐渐取代 IPsec VPN 的趋势。当用户发送访问应用服务器的请求时, 请求并没有被直接发送给应用服务器, 而是被 SSL VPN 接收, 接收后的数据首先被 SSL VPN 进行协议解析, 然后执行身份认证和访问控制等安全策略, 最终再将数据转换为适当的后端协议, 传送给应用服务器。由于在执行安全策略后才允许数据流进入应用服务器, 从而有力地保护了专用网络。

OpenVPN 提供了一个实现 SSLVPN 全部功能的 VPN 解决方案。使用 OpenVPN 可以在任意的 IP 子网

之间建立隧道连接，也可以通过单独的 UDP 或 TCP 端口在任意的网卡之间建立隧道连接。并且可以配置一个具有可扩展性的、带有负载平衡功能的 VPN 服务器，用它可以处理来自不同地方的、成千上万的 VPN 客户端的动态连接请求。OpenVPN 提供了包括 DES、3DES、BLOWFISH、IDEA 等加密算法，利用这些加密算法和认证机制来保护 VPN 中的数据在互联网上的传输。

OpenVPN 作为一种具备完全 SSLVPN 特征的加密技术，是一种工作在网络二三层的 VPN 技术。OpenVPN 通过使用工业标准 SSL/TLS 协议实现了 OSI 二层及三层安全网络扩展，支持灵活证书、智能卡的客户端认证方法，允许通过在 VPN 虚拟接口上应用防火墙规则实现用户及组访问控制。OpenVPN 使用 TUN/TAP 驱动程序将二三层的数据包传送到用户空间，然后使用应用层 SSL/TLS 技术加密传输，从而实现隧道功能。TUN/TAP 驱动程序包含字符设备驱动和网卡驱动。网卡驱动可以接收来自 TCP/IP 协议栈的网络包，或将收到的网络包传输给协议栈；字符驱动实现网络包在内核与用户空间之间的传送，模拟物理链路的数据接受和发送。OpenVPN 使用加密的技术，必须预先知道加密的 Key，使用公开密钥对数据进行加密，首先 Server 和 Client 要有相同 CA 的证书，双方通过交换证书验证合法性以决定是否建立 VPN 连接，使用对方 CA 把自己目前使用的数据加密后发送给对方，由于使用对方 CA 加密的 key，所以只有对方 CA 对应的 key 才能解密，保证了此密钥的安全性，并且此密钥定期改变。

在远程监控的嵌入式网络平台上移植 OpenVPN，移植的过程如下：

(1) 在对 Linux 内核进行编译时，需要 TUN/TAP 设备支持，必须选择 Universal TUN/TAP device driver support 选项；

(2) 下载并安装 SSL VPN，SSL VPN 的主要功能是一种算法库，通过交叉编译为 OpenVPN 提供密码算法库；

(3) 下载并安装 OpenVPN，通过交叉编译生成在嵌入式目标机上启动的执行文件；

(4) 配置 OpenVPN 启动运行的脚本文件，主要包括了设备支持及证书路径；

(5) 在嵌入式目标机上启动 OpenVPN；

(6) 通过网络查看，可以知道是否和远端 PC 建立了虚拟网络连接。

3.2 远程登陆 TELNET 在嵌入式网络平台上的实现

当完成嵌入式目标机和远程监控服务器的连接后，还需要在目标机上启用 Telnet 远程登陆服务，使管理人员可以远端监控目标机。

对于 Linux 操作系统来说，远程登陆 Telnet 是 Internet 最常用的完全控制目标机的实现方式之一，用户可以在任何一台与目标机连接的监控端登陆到被控端系统。在以太网上，几乎每个 TCP/IP 的实现都提供了 Telnet 的标准远程登陆服务，能够运行在各种不同的操作系统中。而在嵌入式系统平台上应用该服务，要求移植 Telnet，移植的过程如下：

(1) 首先下载并安装 busybox，编译时要选择 telnetd；

(2) 系统启动后查看/dev/ptmx 是否存在，没有的话要自己建立 mknod -m 666 dev/ptmx 52；

(3) 建立/dev/pts 文件夹 mkdir /dev/pts；

(4) 在嵌入式平台的/etc/inted.conf 里面写有 telnetd 的位置、权限、工作模式；

(5) 把 devpts 挂上去，devpts 必须要和 /dev/pts 关联起来；

(6) 启动 telnetd 服务，这样可以登陆到嵌入式平台。

以上过程结束后，串行设备远程监控的嵌入式网络平台构建完成，远端服务器 PC 通过 VPN 隧道，通过 Telnet 登陆远程嵌入式平台，其实现的原理如下图 3 所示。

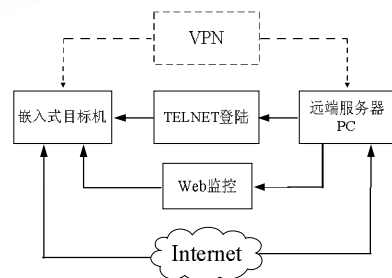


图 3 串行设备远程监控的应用方案

4 Linux 平台的虚拟串口

对远端机的而言，在以太网传输的网络数据并不能直接被应用程序接收，但是，现实中存在的大量串口设备应用程序都是直接操作串口驱动程序的，即使

用串口 API 函数或一些封装了的组件来与串口设备交互数据。因此,有必要采取一些方法,在网络驱动程序与串口设备应用程序间建立一个接口,即虚拟串口,如图 4 所示。考虑到串口设备应用程序是运行在 Linux 操作系统中,所以本文主要是在 Linux 平台下实现虚拟串口。虚拟串口软件位于串口通讯的管理软件与以太网总线驱动层之间,实际上是一个虚拟串口驱动程序,负责管理软件和以太网总线之间的信息转换。

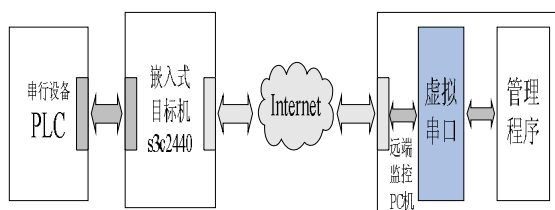


图 4 虚拟串口的应用方案

虚拟串口软件由 3 个部分组成: (1)面向 Server 的服务程序,是一个标准的设备驱动程序,作用是将从 Service 服务程序收取来的以太网上信息进行传输; (2)通讯线程程序,将传递数据保存起来,再进行数据的转发; (3)串口应用接口程序,提供标准的串口设备接口,作用是将从通讯线程传来数据以串口方式进行传输。虚拟串口软件整体框架如图 5 所示。

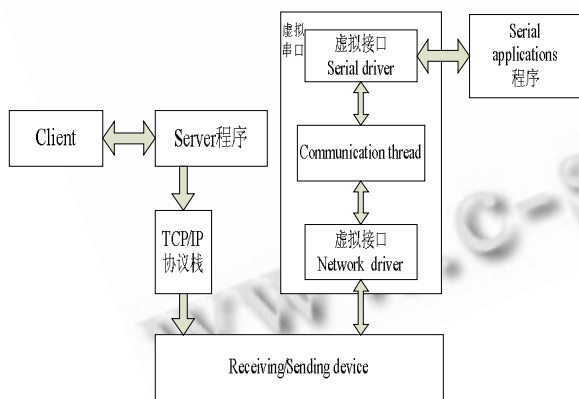


图 5 虚拟串口的软件整体框架

虚拟串口和真实串口没有任何区别,通过虚拟串口,原有的管理软件和现场的串行设备都感觉不到中

间存以太网总线,实现了原有的基于串口通讯的管理应用程序平滑移植到以太网总线的体系中^[5]。

5 测试硬件平台及结果

本文提出的嵌入式串口设备远程监控测试环境如下:目标机的硬件环境采用基于 ARM9 架构的 S3C2440 开发板,该开发板具有 3 个串口、1 个 DM9000EP 网络接口、2MB NOR Flash、64MB NAND Flash、64MB SDRAM;宿主机的硬件环境是 Pentium E2180 CPU 2GHz, 2G 的内存;两台无线路由器;一台串口可编程控制器。

测试内容:串行设备数据发送到目标机,目标机上的程序将数据转换,然后发送到以太网上;宿主机上网络应用程序负责接收目标机端数据,再通过虚拟串口把数据转发给管理程序。在此情况下,必须把本文实现的串口以太网协议转换与远程监控程序移植到目标机,实验结果表明,基于本文框架实现了对串行设备的远程监控,在普通的 Internet 网络环境下,测试效果正常。

本文提出的框架能够有效地适用于嵌入式网络环境,弥补当前串口以太网通讯在嵌入式系统中移植性差的缺点,而且在可维护性和可扩展性方面比较有优势,但还需进一步增加嵌入式系统网络安全,增强交互功能,完善平台的实用性。

参考文献

- 1 权宁一.串口服务器及其在工业以太网中的应用.福建电脑,2008,4:84-79.
- 2 徐荣珍,张敏聪,李从心.基于 ARM 和 TCP/IP 协议的嵌入式串口网络转换器设计.电子器件,2006,29(3):909-912.
- 3 许振山,张智超,刘峥嵘等.嵌入式 Linux 应用开发详解.北京:电子工业出版社,2007.
- 4 Intel Corporation.Embedded Intel architecture in virtual private network design,2006.
- 5 沙涛,王钦友,杭建军.虚拟串口软件程序结构及其接口.现代电子技术,2004,23:60-62.