

一种软件定义的嵌入式 RTU 多协议 自动适配数据传输方法

金惠英, 苏 勇

(南京金水尚阳信息技术有限公司, 江苏 南京 210000)

摘要: 远程测控终端系统(RTU)是构成水文水资源监控系统的核心装置,不同的设备会有不同的应用层通信协议,从而造成信息解析和通信组网的困难。采用软件定义的方法,抽象主流 RTU 应用层通信协议共性,形成统一的协议处理框架模型。将各种应用层通信协议算法按照框架模型进行模块化分割,其可执行代码用虚函数标记,保存在嵌入式 CPU 的 flash 中,构成协议栈。根据配置指令加载及初始化 RTU 通信系统,实现多种 RTU 应用层通信协议的动态拼装与加载,在保持传感器数据采集协议与外部多种通信终端不变的情况下,采集数据从 RTU 到中心站的高效传输。

关键词: 嵌入式 RTU, 协议栈, 通信适配器, 协议加载

中图分类号: TP273

文献标识码: B

文章编号: 1007-7839 (2017) 08-0065-04

A software-defined embedded RTU multiprotocol auto-adaptation data transmission method

JIN Huiying, SU Yong

(Nanjing Jinshui Shangyang Information Technology Co., Ltd, Nanjing 210000, Jiangsu)

Abstract: Remote monitoring and control terminal system (RTU) is the core device which constitutes the hydrological and water resources monitoring system. There are different communication protocols of application layer with different devices, which causes the difficulty of information analysis and communication networking. Using the method of software definition, the mainstream RTU application layer communication protocol was abstracted, and a unified protocol processing framework model was formed. The application layer communication protocol algorithms were modularized based on the framework model. The executable codes were marked with virtual function and stored in the flash of the embedded CPU to form the protocol stack. According to the configuration instructions to load and initialize the RTU communication system, to achieve dynamic assembly and loading of a variety of RTU application layer communication protocol, to collect and transfer data efficiently from the RTU to the central station while maintaining the sensor data acquisition protocol and a variety of external communication terminal unchanged.

Key words: embedded RTU; protocol stack; communication adapter; protocol loading

收稿日期: 2017-07-10

作者简介: 金惠英 (1963-), 女, 本科, 高级工程师, 主要从事水利信息化工作。

0 引言

远程测控终端系统(RTU)是构成水文水资源监控系统的核心装置,由于使用面广量大,存在不同的RTU设备生产厂商和不同时期的RTU设备,这些不同的厂商和不同时期的设备会有不同的通信或应用协议。在实际应用中,由于多种原因,在一个系统会存在大量不同时期、不同厂家的各种设备,这些设备的应用层通信协议大多不尽相同,相应的,中心站数据接收端数据接收程序也不同,从而造成信息解析和通信组网的困难。目前解决这一问题的办法主要有两种:

第一种:系统业主或承建方规定一种协议,更换其他所有不同协议的设备使全网协议统一,比如文献^[1]中针对性的单一协议。这种方法的缺点是减少了设备的可选择性,也不容易保护和利用既有系统的投资。另外,由于厂商设备硬件资源和设计方法的局限,大部分设备都是针对不同的协议做不同的软件版本,产品系列庞杂,通用性差,稳定性很难保证,系统建设成本高。

第二种:不同的协议在中心站转换,使全网在数据应用层面统一^[2]。这种方法的缺点有两点:一是增加了中心站软件的复杂性。二是全网在数据通信层面不能互联互通,需要应用层分别二次转换,影响数据直接使用的时效性与一致性性能。

为解决上述两种办法存在的问题,可利用设备硬件设计的可扩展和软件及协议设计的抽象化、模块化,使新开发的设备能够兼容多协议应用选择,依赖其自身在抽象化的协议框架,驻留少量程序代码,通过应用层的配置,即时拼装出新的协议,并保证其运行的稳定可靠。据此提出一种软件定义的嵌入式RTU多协议自动适配方法,并设计相应的通信适配器。

1 嵌入式RTU应用层通信协议栈设计

1.1 RTU应用层通信协议处理框架模型

分析常用的水文协议、水资源协议、地下水协议以及加密协议、私有协议等的组成,将此类用户通信协议抽象成以下几个部分:协议结构模块、协议控制模块、协议—设备衔接模块、数据缓冲模块和硬件驱动模块。各模块主要功能如下:

(1)协议结构模块主要包括协议数据包/单元(PDU)的构造(组包或封装)、解析(拆包或解

封装),负责将待发送的数据报文按照选定的协议封装成PDU,同时完成对接收的PDU进行命令解析。

(2)协议控制模块主要包括连接管理和传输控制,负责监听上层应用程序的命令,完成建立连接、拆除连接、超时控制、发送数据、接收数据等命令。

(3)协议—设备衔接模块主要包括RTU设备关联和传输模式管理,负责与RTU设备支持的协议的关联绑定,设置设备IP地址、端口、短消息等参数,配置首发、重发、组播(多中心发送)和信道切换等方式。

(4)数据缓冲模块主要包括数据发送控制和缓冲队列管理,负责将待发送的PDU按照数据量大小、要求的时间间隔和数据类型,调度执行基于串口的数据输出。

(5)硬件驱动模块主要包括数据通信口(COM)、参数配置口(CON)和外接设备口(USB),负责对多种形态的串行接口部件和设备的驱动使能,实现与RTU总线、外部计算和存储设备的接入。

1.2 嵌入式协议栈的生成与加载

嵌入式协议栈保存可执行的多种用户通信协议代码。根据协议处理框架模型,将各模块的功能、算法进行标准化、模块化代码设计,形成常用水文协议、水资源协议、地下水协议以及加密协议、私有协议等的“函数库”,其中私有协议存放用户自定义的特殊协议。这些协议组件以特有的嵌入式系统的“虚函数”形式写入CPU的flash空间中,包含协议名称、通信参数、数据类型等要素,供RTU设备在初始化和运行时装配、加载。通过嵌入式协议栈来实现不同协议的自动加载和协议数据包的统一解析调度运行。

通过输入协议与RTU设备配置参数,对协议进行加载控制。配置指示包括应用协议指示、底层通信方式指示、本机和接收方IP地址、端口号、MAC地址绑定,短信参数等。根据协议名称、通信参数、数据类型等参数指示,定位选择合适的“虚函数”,按照步骤一的五个模块,快速组装成指定的应用协议,并与一个外部通信终端相应的链路层协议参数关联,启动RTU初始化过程,确定其与中心站的数据传输方式,完成通信双方的协议加载。

2 嵌入式 RTU 多协议通信适配器设计

2.1 嵌入式 RTU 通信适配器功能模块

采用软件定义的方法, 嵌入式 RTU 多协议自动适配器, 由数据发送控制模块、嵌入式协议栈和硬件接口驱动模块组成。各部分的逻辑结构如图 1 所示。

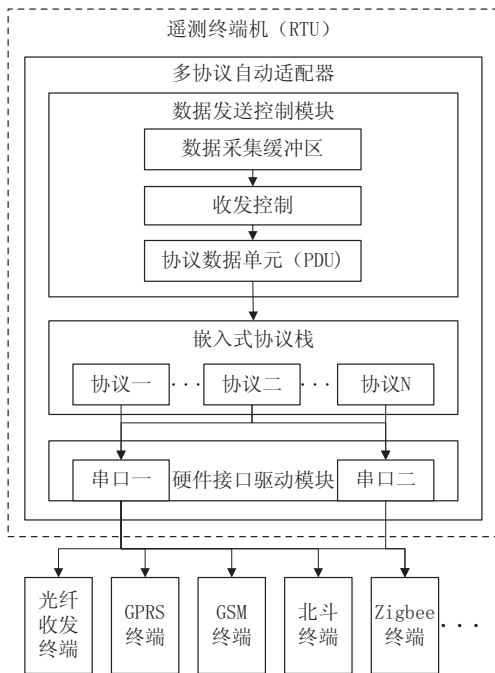


图 1 嵌入式 RTU 通信适配器功能模块逻辑结构

数据发送控制模块包括数据采集缓冲器、用户应用协议命令执行程序。数据采集缓冲器接收并保存来自传感器的实测数据; 用户应用协议命令执行程序按照所选择的应用协议将缓存器中的各类感知数据进行封装, 形成协议数据单元 (PDU), 并通过收发控制程序执行数据发送和重发功能。

嵌入式协议栈, 由协议适配、设备衔接和加载控制三部分组成。协议适配包含通用协议处理框架的基本要素, 如: PDU 数据结构、建立连接、监听、发送、控制信息处理单元, 以“虚函数”保存在适配器 CPU 的 flash 空间中, 如常用的水文协议、水资源协议、地下水协议、加密协议、私有协议等算法, 用户特殊协议可写入到“私有协议”虚函数中; 设备衔接部分提供底层数据链路协议要求的地址、数据长度等参数; 加载控制通过配置口接收用户配置指示 (包括应用协议指示、底层通信方式指示、本机和接收方 IP 地址、端口号、MAC 地址绑

定, 短信参数等), 从“函数库”中选择合适的函数, 快速组装成指定的应用协议, 并与一个外部通信终端相应的链路层协议参数关联, 启动 RTU 初始化过程, 确定其与中心站的数据传输方式。

硬件接口驱动模块, 包括设备驱动程序、收发缓冲和硬件接口。设备驱动程序完成对外部通信终端的使能和驱动, 支持 MODEM、以太网卡、无线 VHF/UHF 通信装置、北斗卫星、海事卫星、VSAT、全线通、全球通等卫星、GSM/GPRS 移动等通信装置; 收发缓冲存放符合数据链路层数据包大小限制的待发送数据, 接收对方的应用层应答信息并交给相应的协议处理单元; 硬件接口采用通用串行接口, 与外部通信终端的串口相连, 完成最终的数据传输。

2.2 嵌入式 RTU 通信适配器硬件结构

嵌入式 RTU 通信适配器由 CPU、数据存储缓冲器、接口电平转换电路、数据收发串行口、参数配置口、数据采集口及供电电源变换电路组成。其中: CPU 采用 STM32F103ZE, CPU 内置 FLASH、RAM 存储空间和串行口外设 (实现串行收发波特率自动控制); 数据存储缓冲器采用 SD 卡作存储介质, 保证存储容量和可靠性; 接口电平转换电路实现 CPU 到外接数据传输设备的硬件电平匹配; 数据收发串行口是和外接数据传输设备的硬件物理连接口; 参数配置口用于对协议适配器内部控制参数进行配置与管理; 数据采集口用于采集、接收各类水文、水资源、气象、环境传感器的原始数据类似文献^[3-4]的 485 总线构架, 采集到的原始数据进入 SD 卡做数据存储缓冲; 供电电源变换电路实现整个适配器的电源供应。其硬件组成结构图如图 2 所示。

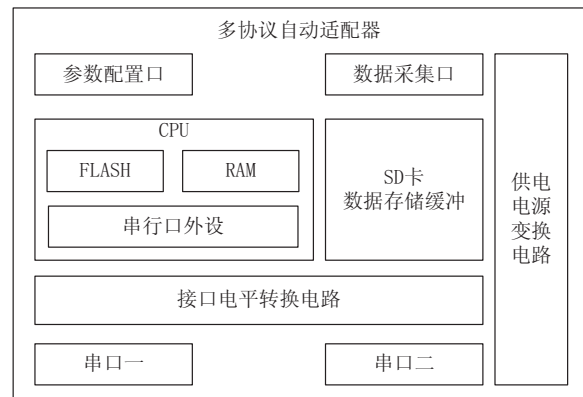


图 2 嵌入式 RTU 通信适配器硬件组成结构

该适配器内置于 RTU 中, 作为 RTU 的重要组成部分, 共享 RTU 的供电电源, 通过板载的电源变换电路生成自需的供电电源, 维护自身正常工作。封装编译好的多协议适配器可执行代码写入 CPU 的 flash 空间中。

3 基于嵌入式 RTU 适配器的数据传输

3.1 协议初始化

RTU 设备使用前, 根据外接传感器、数据传输设备和需要使用的协议类型, 通过参数配置口进行合适的参数配置, RTU 加电复位后就可以自动加载“函数库”中配置参数所指定协议的虚函数, 从而实现传输协议核心算法的加载执行。

RTU 上电加载控制参数和算法程序后, 数据采集口开始按配置需要采集外接传感器原始数据, 原始数据在 CPU 控制下直接写入 SD 卡进行数据存储缓冲, 收发控制提取缓冲器中的原始数据, 按照所选择的应用协议将缓存器中的各类原始数据进行封装, 形成协议数据, 存储入协议数据单元 (PDU), 然后, 收发控制启动数据发送, 通过调用配置参数指定协议的虚函数, 实现协议栈的协议适配功能。硬件接口驱动模块通过通用串行接口连接外部各种通信终端, 同时, 将数据发送控制模块传来的应用层 PDU 封装成数据链路层的数据帧, 数据链路层数据帧通过外接通信终端发送出去, 实现数据帧的发送和应答处理。

3.2 生成 PDU

遵循面向字节型的状态机协议栈算法遵循《水资源监测数据传输规约》(SZY206-2012), 表示协议在运行时的工作状态。生成协议数据单元 (PDU) 的步骤如下:

步骤 1: 一旦协议加载成功, 系统将根据设置的数据发送触发机制 (如中断或其他事件消息), 对实际接收到的传感器数据报文包头识别、校验和内容的 PDU 封装, 并启动数据传输与控制。

步骤 2: 根据加载的协议及其对应的状态机参数, 当接收到数据处理信号后, 从接收数据缓冲区取出协议参数设置个数的字节来进行本协议包头匹配, 协议包头匹配不成功时丢弃所取的数据, 同时进行缓冲区移位以便于再次取数, 这个操作被称为包头处理状态 (状态 A); 当协议包头匹配成功即转入协议数据包处理, 处理具体的 PDU

内容 (状态 B)。

在顶层状态 B 中又分三个具体的子状态:

(1) 包头匹配成功并进行缓冲区移位操作后进入协议包长处理状态 (状态 B—子状态 a);

(2) 知道协议包长 (L 字节) 后, 状态机控制转入协议取数状态 (状态 B—子状态 b) 进行协议取数;

(3) 读取接收数据缓冲区 L 字节后, 状态机控制转入协议校验状态 (状态 B—子状态 c);

(4) 数据包校验通过后, 取走整个 PDU 的数据部分, 并发出协议数据处理信号启动后续数据处理。

(5) 最后对接收数据缓冲区余下的数据启动下一次协议状态机处理过程 (回到状态 A)。

3.3 数据传输与控制

经过协议处理后的数据, 输入到“数据上报缓冲区”队列中, 由数据发送控制模块与硬件接口驱动模块共同完成数据发送和重发功能。上报成功的数据在上报完成后即丢弃 (原始数据事前已存入 RTU 设备的存储器中), 对于上报不成功的数据, 专门开辟了“补传数据缓冲区”来区别存放。

通过“数据自动补传”算法的控制, 每次启动上报时都是优先发送数据上报缓冲区内的数据, 待数据上报缓冲区的数据全部发完后, 再按后进先出的顺序控制发送数据补传缓冲区内的数据, 保证实时数据的优先上报。

除此之外, 数据发送控制模块可以驻留多个发送控制策略, 满足应用需求和通信环境。

4 结语

嵌入式 RTU 多协议自动适配数据传输方法, 通过软件定义的方式, 抽象 RTU 应用层协议处理框架, 经由配置确定 RTU 的通信工作模式, 自动组合加载协议组件, 使 RTU 和中心站同时初始化, 实现配置一次自动加载并永久使用。该方法已用于研发 JSSY-DCT-1001 型水文水资源数据采集遥测终端机, 并投入实际系统建设, 显著提高了遥测数据在不同用户协议和网络环境下传输的扩展性和可靠性。该方法也能在用户协议和组网方式改变的情况下, 重新配置加载, 实现多次配置灵活更新, 提高 RTU 在新老系统集成建设中的

(下转第 72 页)

效率,有效降低整个系统的建设周期和费用。

参考文献:

- [1] Zhang G, He M, Zhang W. The application of Modbus-RTU in the monitor system of water pumping station[J] . Microcomputer & Its Applications, 2016 .
- [2] Motoyama, Tetsuro. Method and apparatus for monitoring remote devices through a local monitoring station and communicating with a central station supporting multiple

manufacturers[J] . 2009 .

- [3] Peng D, Zhang H, Weng J, et al. Design and development of Modbus/RTU master monitoring system based on embedded PowerPC platform[J]. IEEE, 2009:2148-2152.
- [4] D Peng, H Zhang, H Li, K Zhou, Design and implementation of ARM embedded monitoring platform based on Modbus protocol, 《Electric Power Automation Equipment》, 2009, 29 (1): 115-119+123.

(责任编辑:华智睿)