A software defined RTU multi-protocol automatic adaptation data transmission method

Huiying Jin¹, Xingwu Xu², Zhanfeng Wang¹,³, Weijun Ma¹, Sheng Li¹, Yong Su¹ and Yunpeng Pan²

¹Nanjing Goldwater Shang Yang Information Technology Co., Ltd, Nanjing, 211101, China;
²Nanjing Sancha River Estuary Sluice Management Office, Jiangsu Province, Nanjing City, 210036, China
³hehengw@hotmail.com

Abstract. Remote terminal unit (RTU) is the core device of the monitor system in hydrology and water resources. Different devices often have different communication protocols in the application layer, which results in the difficulty in information analysis and communication networking. Therefore, we introduced the idea of software defined hardware, and abstracted the common feature of mainstream communication protocols of RTU application layer, and proposed a uniformed common protocol model. Then, various communication protocol algorithms of application layer are modularized according to the model. The executable codes of these algorithms are labeled by the virtual functions and stored in the flash chips of embedded CPU to form the protocol stack. According to the configuration commands to initialize the RTU communication systems, it is able to achieve dynamic assembling and loading of various application layer communication protocols of RTU and complete the efficient transport of sensor data from RTU to central station when the data acquisition protocol of sensors and various external communication terminals remain unchanged.

1. Introduction

Remote terminal Unit (RTU) is the core device of hydrology and water resources monitoring system. There is a large number of RTU equipment that is made by different manufacturers or in different periods. Even in a system, the RTUs are usually not made by the same manufacturers or have different communication protocols [1][2]. The heterogeneous arisen from the arious equipment resulting in difficulties in [3][4] information analysis and communication.

At present, there are two main ways to solve this problem:

The first solution is as follows. The system owners or contractors replace all other devices with different protocols to unify the whole network protocol, such as a single protocol proposed in document [1][5]. The drawback of this approach is that it reduces the facility's availability and makes it difficult to protect and utilize the investment in the existing system. In addition, due to equipment manufacturers and the design method of hardware resource limitations, complex product series, poor versatility, the stability of the system is very difficult to guarantee and will incur high cost of construction.

The second solution is that protocol conversion is taken at the central station conversion, so that the whole network in the data application level unified [4]. There are two disadvantages of this method:
first, it increases the complexity of the central station software. Second, the whole network in the data communication level can not be interconnect, and it need take twice conversions at the application level and affect the timeliness and consistency of the data.

In order to solve the disadvantages of the above two solutions, the design can be extended by hardware and design software and protocol abstraction and modular [6][7], the development of new equipment is compatible with multi-protocol application, depends on its in abstraction framework, resides in a small amount of code, through the application layer configuration [8][9]. Based on this, a software defined embedded RTU multi-protocol automatic adaptation method is proposed, and the corresponding communication adapter is designed.

2. Design of communication protocol stack for embedded RTU application layer

2.1. RTU application layer communication protocol processing framework model

By comparing the protocols of hydrology water resources protocol, groundwater protocol and encryption protocol, proprietary protocol, we find that all the protocols are made of following parts: protocol module, control module, interface module, data buffer device interface module and hardware driver module. The main functions of each module are as follows:

1) The protocol module includes a protocol packet / cell (PDU) structure (package or package), analytical (unpacking or solution package), the data message will be sent to the responsible in accordance with the selected protocol encapsulated into PDU, and completes the command parsing the received PDU.

2) The protocol control module mainly includes connection management and transmission control. It is responsible for monitoring the commands of the upper application program, completing the connection, dismantling the connection, overtime control, sending data, receiving data and other commands.

3) The interface module includes RTU device interface equipment association and the transmission mode of management, responsible for the association binding with the RTU device support agreement, parameters of the IP address, port, and short Message, and configuration of retransmission, multicast (first multicenter transmission) and channel switching method.

4) The data buffer module includes data transmission control and buffer queue management, will be responsible to send PDU data in accordance with the requirements of the size, time interval and data types, implementation of the serial data output based on scheduling.

5) The hardware drive module includes data communication interface (COM), and configuration parameters (CON) and external equipment (USB), responsible for driving various forms of serial interface components and equipment to achieve access, and RTU bus, external computing and storage devices.

2.2. Generation and loading of embedded protocol stack

The embedded protocol stack maintains a variety of executable user protocol codes. According to the framework agreement, the function of each module of the algorithm, the standardization and modularization design code, the formation of common hydrological protocol, water resources protocol, groundwater protocol and encryption protocol, protocol such as the library, a special protocol which stored user-defined protocol. The protocol component with special embedded system named as virtual function written in the form of CPU in flash space, including the name of the protocol, the communication parameters, data types and other factors, for RTU equipment in the initialization and runtime distribution, loading. Through the embedded protocol stack, the automatic loading of different protocols and the uniform dispatch of protocol data packets are realized.

Through the input protocol and RTU device configuration parameters, the protocol is loaded and controlled. Configuration instructions include application protocol instructions, underlying communication mode instructions, native and recipient IP addresses, port numbers, MAC address bindings, SMS parameters, and so on. According to the indication of the name of the protocol, the
communication parameters, data types and parameters, select the appropriate positioning of virtual functions, according to the five steps of a module, assembled quickly into the specified application protocol, link layer protocol and the corresponding parameters associated with an external communication terminal, start the RTU initialization process, and determine the center station the way of data transmission, complete communication protocol load.

3. Design of multi protocol communication adapter for embedded RTU

3.1. Embedded RTU communication adapter function module

Using the idea of software defined hardware, the embedded RTU multi-protocol automatic adapter is composed of data transmission control module, embedded protocol stack and hardware interface driver module. The logical structure of each part is shown in Figure 1.

The data sending control module comprises a data acquisition buffer, a user application protocol and a command executing program. The data acquisition buffer receives and saves the measured data from the sensor; the user application protocol command execution procedures in accordance with the application protocol is chosen to be all kinds of sensory data in buffer package, forming a protocol data unit (PDU), and through the transceiver control program performs data transmission and retransmission function.

Embedded protocol stack consists of three parts, protocol adaptation, device connection and load control. Protocol adaptation is the basic elements, including the common protocol processing framework such as PDU data structure, connection establishment, monitoring, control, sending the information processing unit, with virtual function is stored in the adapter CPU flash space, such as hydrology, water resources protocol commonly used protocol, underground water protocol, encryption
protocol, protocol etc. algorithm, user specific protocol can be written into the private agreement in
virtual function; device interface address, the data length and other parameters of the underlying data
link protocol requirements; loading control receives the user by configuring port configuration
instructions (including the application protocol instructions, instructions, the way of communication
and the recipient of the machine IP address, port number, MAC address binding, SMS), select the
appropriate parameters of function from the library, assembled quickly into the specified application
protocol, and an external corresponding link layer protocol parameters of the communication terminal
are connected, and the RTU initialization process is started and the data transmission mode between
the central station and the central station is determined.

The hardware interface driver module includes device driver, transceiver buffer and hardware
interface. The device driver to complete the external communication terminal enable and driver,
support MODEM, VHF/UHF Ethernet card, wireless communication device, Beidou satellite,
maritime satellite, VSAT, omnitrails, global satellite, GSM/GPRS mobile communication device;
receiving buffer stored with the data link layer packet size limits the application of the data to be sent.
Layer response information receiving party and give the corresponding protocol processing unit;
hardware interface using universal serial interface to connect with the external serial communication
terminal, data transmission end.

3.2. Hardware structure of embedded RTU communication adapter
The embedded RTU communication adapter consists of CPU, data storage buffer, interface level
conversion circuit, data transceiver serial port, parameter configuration port, data acquisition port and
power supply conversion circuit. Where CPU by STM32F103ZE, CPU FLASH, RAM built-in storage
space and serial peripherals (automatic control serial baud rate); data storage buffer using SD card as
storage medium, ensure storage capacity and reliability; interface level conversion circuit to realize the
CPU to the hardware level with a data transmission device, data transceiver serial port is connected;
and the external data transmission equipment hardware; parameter configuration for port protocol
adapter internal control parameter configuration and management; data acquisition port for 485 bus
frame data acquisition, receiving all kinds of hydrology, water resources, meteorology, environmental
sensors, similar to the literature [10][11], collected original data into SD card data storage buffer;
power supply converter power supply adapter to achieve the whole. The hardware structure diagram is
shown in Figure 2.

![Figure 2. Hardware structure of embedded RTU communication adapter.](image-url)
The adapter is built in RTU, as an important component of RTU, sharing RTU power supply, through the on-board power conversion circuit to generate the required power supply, to maintain its normal work. The compiled multiprotocol adapter executable codes are written into the FLASH CPU space.

4. Data transmission based on embedded RTU adapter

4.1. Protocol initialization

Before usage of RTU equipment, according to the external sensor, data transmission equipment and the need to use the type of protocol parameter configuration by proper configuration parameters for export, RTUs can automatically load the virtual function of the library in the configuration parameters of the specified protocol and reset, so as to realize the transmission protocol of core algorithm execution.

RTU electric loading algorithm and the control parameters of the program, the data acquisition port began to receive sensor data acquisition according to the configuration needs, the original data under the control of CPU directly into the SD card data storage buffer, sending and receiving control to extract the original data in the buffer, according to the application protocol choice will be all kinds of original data buffer in the package the formation of protocol data, stored in a protocol data unit (PDU), then start sending and receiving control data sent through the virtual function call configuration parameter specifies the protocol, the protocol stack protocol adaptation function. The hardware interface driver module is connected with the external communication terminal through the serial interface to send data at the same time, the control module to the application layer of the PDU package into a data frame of data link layer, data link layer frame through the external communication terminal sends out, send and reply processing data frame.

4.2. Generating PDU

Following the byte oriented state machine protocol stack, the protocol follows the water resource monitoring data transmission protocol (SZY206-2012) to indicate the working state of the protocol at runtime. The steps for generating the protocol data unit (PDU) are as follows:

Step 1: once the agreement is loaded successfully, the system will trigger mechanism according to the sending data set (such as interruptions or other event messages), PDU package of sensor data packets actually received the Baotou identification and verification and content, and start the data transmission and control.

Step 2: according to the state machine and the corresponding loading parameters of the protocol, when receiving data processing signal, remove the set protocol number of bytes received from a data buffer, and match the packet header. When matching is not successful to discard the data, shift buffer again the number of this operation is called the packet process state (State A); when the matching is successful, it transfers to the state of protocol packet processing (State B).

In the top level state, state B is divided into three specific sub states:

1. After successful matching and buffer shift operation, Baotou enters the protocol packet processing state (status B-, sub state a);
2. After knowing the protocol packet length (L bytes), the state machine controls the access to the protocol fetch state (status B-, sub state B) for protocol fetch;
3. After reading the L byte of the data buffer, the state machine controls into the protocol check state (status B-, sub state C);
4. After the data packet is checked and verified, the data part of the whole PDU is taken away, and the protocol data processing signal is sent out to start the follow-up data processing;
5. Finally, the next protocol state machine processing process is returned to the remaining data of the received data buffer (back to state A).
4.3. Data transmission and control

The data processed by the protocol are input into the data report buffer queue, and the data sending module and the hardware interface driver module are used to complete the data sending and retransmission functions. Reported successful data is discarded in the report (after the completion of the original data storage device in advance have been deposited in the RTU) for reporting data is not successful, and opened a special supplement from the data buffer to store the difference.

The data automatic retransmission algorithm firstly send data in buffer at each time of booting, and then according to the LIFO order. In addition, the data transmission control module can reside a plurality of transmit control strategies to meet the application requirements and communication environment.

5. Conclusions

The multi-protocol embedded RTU through software definition abstract RTU application layer protocol processing framework, through the configuration automatic combination load protocol component. This method has been used for the research and development of JSSY-DCT-1001 hydrological data acquisition telemetering terminal, and put into practical system construction, improve the transmission of telemetry data in different network environment and user protocol scalability and reliability. This method can also change the user agreement and networking mode, to achieve multiple configuration loading, flexible configuration update, improve the RTU in the integrated construction of new and old system efficiency, reduce the construction period and the cost of the whole system.

Reference

[1] Hanafiah M, Raman S, Wan Jusoh W, Ghani M and Baharuddin Z 2013 J. Smart. Clean. 3 330
[2] Ghani M, Wan N, Hanafiah M, Raman S and Jano Z 2013 J. Telkomnika 4 819
[3] Xi-Dong L, Liu T and Gang L 2005 J. Tech. Auto. Appli. 7 37
[4] Motoyama, Tetsuro 2009 Method and apparatus for monitoring remote devices through a local monitoring station and communicating with a central station supporting multiple manufacturers[J]
[5] Zhang G, He M and Zhang W 2016 J. Micro. Appli
[6] Yuan S and Ying L. 2010 J. Low Vol. Appa.
[7] Wang Z, Sun H and Yi M. 2010 J. Elec. Tech 3 178-186
[8] Motoyama T C R C. 2014 P. EP1519514
[9] Garcia L, Teyeb O, Redana S and et al. 2015 P. US9113405
[10] Peng D, Zhang H, Weng J, et al. 2009 Proc. IEEE International Symposium on Industrial Electronic 2148-2152
[11] Peng D, Zhang H, Li H, and Zhou K, 2009. J. Elec. Auto. Equi. 29 115