

Research and Realization of HART Protocol Based on Wireless Short Range Network Technology

Kaiyuan Meng^{1, a}, Qingnian Cao^{2, b}

¹School of Computer Science, Xi'an Shiyou University, Xi'an 710065, China

²School of Computer Science, Xi'an Shiyou University, Xi'an 710065, China

^aemail: kymeng@126.com, ^bemail: qncao@126.com

Keywords: HART; Wireless Short Range Networks; Communiation Protocol; RTU

Abstract. In this paper, through the research on the application layer command of HART protocol, according to the characteristics of wireless network in enterprise information network system, the system network structure based on short range wireless network was constructed, the communication control module RTU was also designed. Combined with the practical application, the monitoring software of host computer and the communication control module were programmed to achieve the basic HART protocol communication function, which based on the wireless transceiver module driver and the HART message structure and command.

Introduction to the Short-range Wireless Network HART Technology

In industrial control, wireless network communication technology is mainly focused on two aspects of wireless LAN and short-range wireless network. At present, the short distance wireless communication technology has become an important branch of wireless communication technology, and short-range wireless network with peer to peer communication, short distance, low rate, low power consumption, low cost, low complexity and other characteristics.

Application of short range wireless network technology in the industrial control, it mostly includes data acquisition, video surveillance, to help users realizing the communication between the mobile device and the fixed network or mobile communication equipment. It is suitable for various industrial environments, even in extremely execrable circumstances to ensure the safety and reliability of the network. In the device layer, live sensor, detector, card reader or other device are connected to each other to form a wireless sensor network.

HART (Highway Addressable Remote Transducer) protocol is the 4~20 mA analog signal to digital signal transition protocol. The analog signal is superimposed on a digital signal in the traditional 4~20 mA standard.

HART communication protocol was launched in 1985, for field intelligent instruments and control room equipment. The HART device is provided with a relatively low bandwidth, moderate response time. Wireless HART adopts 2.4GHz band. In order to avoid the interference of 2.4GHz frequency band, wireless HART specially opened for the band of unused channel search function, can be controlled at any time to avoid mutual interference. Wireless HART is based on the HART protocol, which is a kind of special communication protocol of wireless mesh network for process automation application design.

Each wireless HART network includes three main components, link process or wireless field device, the host computer communication application program gateway and the network manager. The network manager can be integrated into the gateway, the main application program or process automation controller [1][2].

HART Protocol Analysis

The HART protocol uses the FSK technology, the measurement of the analog signal is superimposed on a frequency signal 4~20 mA signal process, which made the analog and digital bidirectional communication can be carried out at the same time, and do not interfere with each

other. HART can also communicate with all digital way in a twisted pair line, supported by 15 field equipment multi station network, and can clearly describe the characteristics of the instrument. The characteristic of HART protocol is similar to the system structure of the fieldbus, with its open interconnection model of international organization for standardization as the reference, using OSI 1st, 2nd 7th layer. Table 1 shows the application of HART protocol in wireless network is the application layer of the HART command [3].

HART communication protocol allows two kinds of communication mode, namely "question and answer" and "production mode".

Table 1 Comparison of the wireless HART and HART hierarchical structure

Hierarchy	OSI level	wireless HART level	HART level
7	application	HART command	HART command
6	presentation	not used	not used
5	session	not used	not used
4	transport	wireless protocol	not used
3	network	wireless protocol	not used
2	data link	wireless protocol	protocol specification
1	physical	802.15.4	Bell 202

The application layer is the third layer of the HART protocol, which is also the highest level to provide a programming interface to application layer HART protocol command format, all read / write operations in order to complete the form. In addition, some of the features of link management protocol is realized by the command.

Each command of HART protocol is marked by the command. In communications, a command assembled into a complete HART frame according to the command format. In the data link layer in the provisions of the HART frame format, but the data link layer does not explain the the meaning of data segment in the HART frame, the work done by the application layer of HART protocol.

The Overall System Design

In the industrial control now, wireless information network has become critical infrastructure to connect to all segments of industrial control. Wireless network monitoring system based on sensor technology is a set of system and data acquisition, storage, transmission, processing technology in a body. Figure 1 depicts the industrial control network system structure based on wireless network. This system is composed of the field control layer, process control layer and management layer between the layers of the workstation, through the exchange of information, to complete the task [4][5].

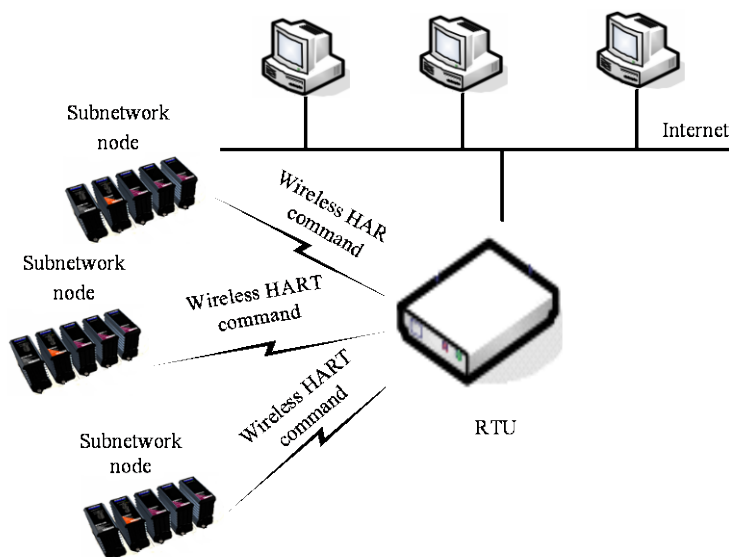


Fig.1. Network system structure diagram of wireless industry field

System Hardware Design

Design scheme of the wireless monitoring system network structure as shown in figure 2.

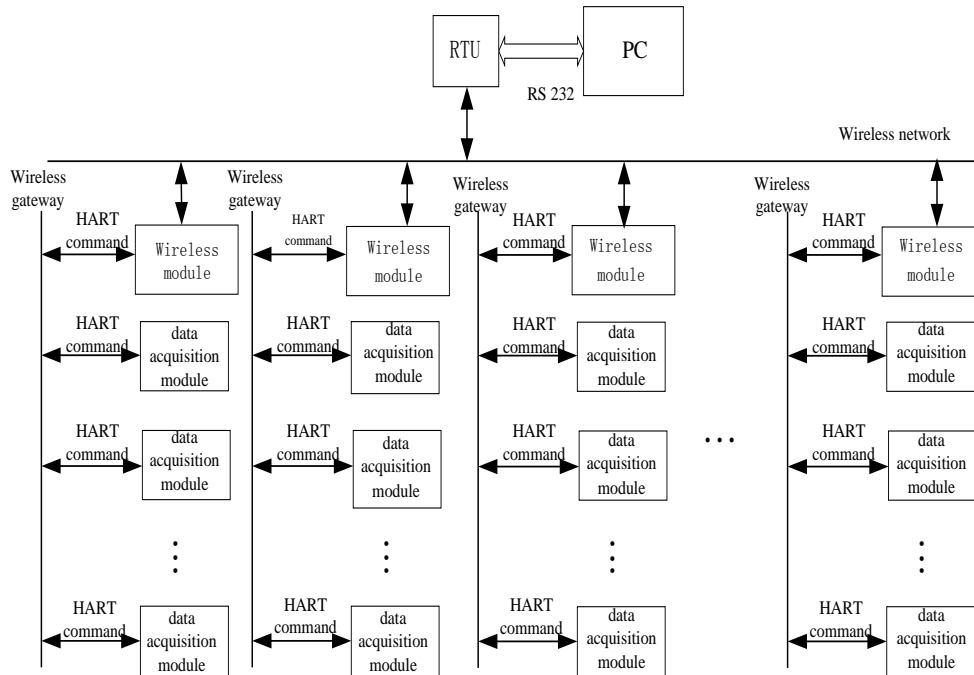


Fig.2. Structure diagram of monitoring network communication system

The embedded data acquisition module (slave node), and the communication control module RTU (Remote Terminal Unit) were designed for the system. Each node transmits the data through the wireless module. The data acquisition module data acquires and controls field data, connecting through the input and output interfaces and field instrument. In the wireless network, the HART adopts bus master/slave work mode. Through the wireless module RTU can monitor and confige distributed in different locations of the nodes in real-time of, so as to form a distributed network system.

Communication control module RTU as an important function of the master node is the network management, monitoring the working state of the data acquisition module. Communication control module RTU is connected with the host computer through the PC's serial port, observing data through the host PC software. The data acquisition module is responsible for sending the collected sensor signal to RTU, according to the transmission mode of HART protocol over the wireless network.

The data acquisition module exchange field acquisition data with RTU through the wireless HART network. Master RTU gathers in each sub node data and together transmits to host PC. The data center transmits the control data to each node in wireless HART networks through the reverse link. RTU hardware block diagram is shown in figure 3.

This system uses ATMEL's AT91SAM7X256 as the core processor of RTU, is also equipped with the reset circuit, EEROM circuit, JTAG interface circuit and the RS-232 serial port emulator. Input and output channels have an important function of the slave node to connect conveniently.

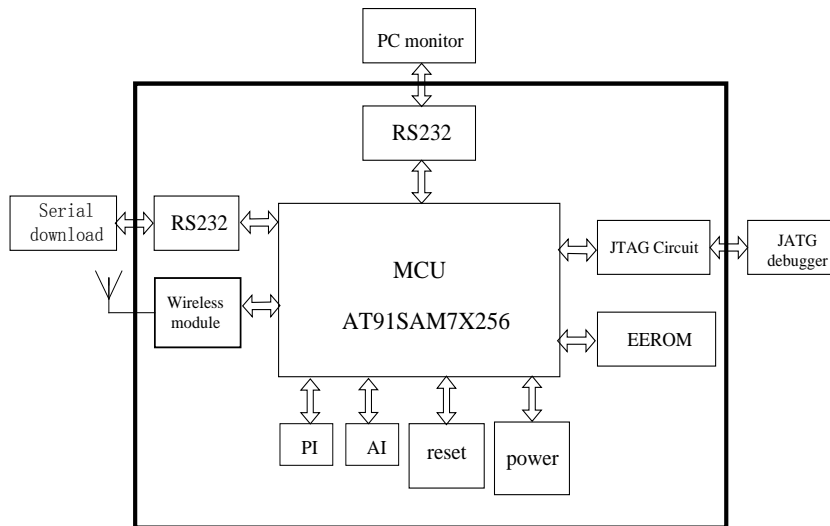


Fig.3. RTU hardware block diagram

The Overall Software Framework

Software design is based on embedded real-time operating system $\mu\text{C}/\text{OS-II}$ platform. Based on the research of HART commands and information model of HART protocol, HART protocol of short-range wireless network was achieved.

In this design using $\mu\text{C}/\text{OS-II}$ as a real-time multi task kernel, after the $\mu\text{C}/\text{OS-II}$ operating system successfully being transplanted to the AT91SAM7X256 microprocessor, the development of driver program in wireless communication module is the key software design. The wireless communication bottom driver program is the basic realization of HART protocol in wireless network [6].

The main task of software design is to realize the data communication based on short-range wireless network between the RTU and the data acquisition module. In addition, each module and serial communication with host PC. The $\mu\text{C}/\text{OS-II}$ embedded operating system provides a good platform for task scheduling, which is the basis of application software to be reliable operation. Software design of the control module and I/O module communication is generally divided into three parts: the transplanted of embedded operating system $\mu\text{C}/\text{OS-II}$, wireless module and HART, as shown in figure 4.

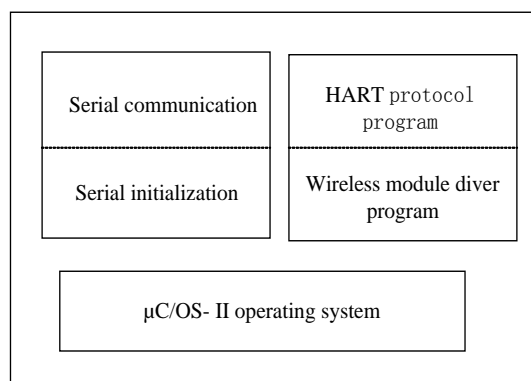


Fig.4. Software overall framework diagram

The RTU serial communication includes sending and receiving, and the data acquisition module only sends message to the RTU through the serial port output, can also receive command from host PC.

In this design, the wireless module selects the Xbee OEM RF Modules chip of DIGI company. The Xbee chip needs the necessary drivers so as to distinguish the various sites in the network and realize the normal communication with RTU.

Wireless Communication Module Program Design

Data of RTU and data acquisition module transmits through wireless network. After the initialization of the wireless module, it transmits data according to the communication protocol of HART to. HART message frame format is shown in table 2.

Table 2 HART message frame format

Leader symbol	start byte	address	command	length of data bits	Data	Check-out bits
---------------	------------	---------	---------	---------------------	------	----------------

HART communication command was chosen for wireless transmission between the RTU and the node data acquisition module. When the RTU receives the data, it is the host machine. When the RTU sends data, it is the slave machine. It's working mode needed to be judged in the wireless communication program of RTU, whether it is now in the receiving or sending data. Receiving and sending data are carried out through the serial port, using the HART communication protocol in the whole process. Data transmission process is illustrated in figure 5.

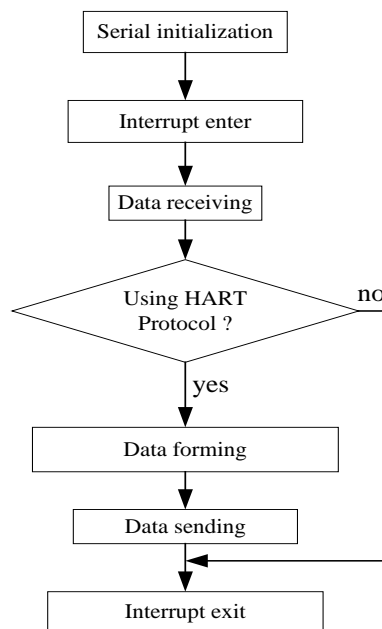


Fig.5. Data sending and receiving flow diagram

Conclusion

The short-range wireless network is a new network technology, compared with the prior existing technology, which saves the cost and constructs the network more conveniently. A wireless network monitoring system was constructed, which based on HART protocol commands and short-range wireless network technology. Using AT91SAM7X256 as the main controller core, the embedded communication control module and I/O module were designed to realize data communication between each module. Selecting the open source real-time embedded operating system $\mu\text{C}/\text{OS-II}$, it has of high efficiency and low cost. The system in this paper is stable, reliable and has application value.

Reference

[1] Peng Yu. Application prospect analysis of factory automation and process automation in short-range wireless network and wireless local area network, Shanghai Industrial Automation Instrument Research Institute, 2006

[2] Peng Yu, Recent development of short-range wireless communications in industry environment. The Zhongkong technology forum, 2007

<http://www.supcon.com/supcon/jsp/zkjslt/zkjslt08/zkjslt08.zjsd.jsp>

[3] Wireless HART Technical DataSheet, http://www.hartcomm2.org/hart_protocol/

[4] Lang Xigui, Yu Hongbiao. Short-range wireless network application and practice [J], Computer and modernization, 2009(7) 98-100

[5] Zuo Yun, Ling Zhihao. The short-range wireless network application in industry and the development [J], the ninth session of the industrial instrumentation and automation conference, 2008, 328~334

[6] ATMEL Corporation, AT91SAM7X256_datasheet.pdf