Application of Remote Wireless Sensor Network in Power System

Hua Wang, Zijiang Yang, Yan Cong, Jing Xu, Wanchun Luan
State Grid Chaoyang Power Supply Company, Chaoyang 122000, China

Abstract. This paper mainly studies the design and research of remote wireless sensor networks. This system features low power consumption, strong anti-interference ability, large capacity, real-time acquisition, and safe and reliable data transmission. The research idea of this paper: The host connects up to 255 extensions through the wireless transmission module, and the host sends standard MODBUS (RTU) access commands to control the operation of each extension.

1. Introduction
The emerging interdisciplinary field of wireless sensor networks is a major change in the interaction between people and the environment. Its development will bring new ideas and challenges in various fields of military and civilian use. With its development, it will surely become more and more wide range of applications, so further research work has important practical significance.

2. RF bidirectional power amplifier circuit design
The existing products basically have relatively small communication distances, and relatively few two-way transmission and reception. This paper mainly studies the scheme and hardware implementation of the extended RF front-end. It mainly realizes the method of increasing the sensitivity, increasing the transmit signal power and selecting the antenna with larger gain by amplifying the received signal while implementing the two-way transmission and reception. It is used in wireless communication systems compatible with IEEE802.11b/g.

The main design specifications of the bidirectional power amplifier are shown in the table.

| Table 1. Bidirectional power amplifier main design indicators |
|-------------------------------------------------------------|
| Working frequency                                           | 2400MHz ~ 2483MHz |
| Maximum output power                                        | +30dBm (1W)       |
| Transmit gain                                               | ≥27dB              |
| Receive gain                                                | ≥14dB              |
| Receiver noise figure                                       | < 3.5dB            |
| Frequency response                                          | ≤±1dB              |
| Input minimum input power threshold                         | <15dB m            |
| With transceiver indication function and power polarity reverse connection protection |

3. Construction of communication protocol
In the MODBUS communication protocol, a typical RTU message frame format is shown in Table 2:
By analyzing the requirements of the system, a 14-byte message frame is constructed by referring to the structure of a typical RTU message frame in the MODBUS communication protocol. The frame structure is as shown in Table 3 below:

### Table 3. Message frame structure

| Start bit | Device address | Function code | Sampling channel number H | Sampling channel number L | Sampling length H | Sampling length L | CRC check L | CRC check H | Terminator |
|-----------|----------------|---------------|---------------------------|--------------------------|------------------|------------------|-------------|-------------|-------------|
| T1-T2-T3  | 0-255          | 8bit          | 8bit                      | 8bit                     | 8bit             | 8bit             | 8bit        | 8bit        | T1-T2-T3    |

Start bit: The first thing the protocol has to do is to identify the noise and data. The appearance of noise is random, and the way is not obvious. For a noise source, it should be able to generate every kind of byte information that can appear. Because of this feature, we want to find a kind of byte to be combined as a valid packet. The beginning, fortunately, noise is not ideal for us to think about. In this way, we can increase the start bit and specify that the receiving party only receives the data packet starting with the start bit.

Extension number: That is, the address field of the message frame contains one byte. The host strobes the extension by placing the extension number of the extension to be contacted into the address field in the message. The address 0xFF is used as a broadcast address so that all extensions can recognize it.

Function code: The function code field in the message frame contains one byte. Of course, some code is for all controllers, some for some controllers, and some for future use. When a message is sent from the host to the extension, the function code field tells you what action to take from the extension. For example, let the extension start sampling, read the data content of one channel, read all sampled data, and so on. There are 8 function codes in this system, as shown in Table 4:

### Table 4. Function code definition

| Function code | Name                        | Meaning expressed                      |
|---------------|-----------------------------|----------------------------------------|
| 1             | TASK_ADC_SAMP               | Sampling separately                    |
| 2             | TASK_ADC_SAMP_TRIG          | Trigger sampling                       |
| 3             | TASK_ADC_READ_ONE_CH       | Read broadcast sampling single channel data |
| 4             | TASK_ADC_READ_4_DATA       | Read broadcast samples to read 4 data |
| 5             | TASK_ADC_READ_2048_DATA    | Read broadcast samples to read 2048 data |
| 6             | TASK_ADC_READ_3_CH         | Read broadcast sampling 3 channel data |
| 7             | TASK_ADC_BROCAST_SAMP      | Broadcast sampling                     |
| 8             | TASK_SAVE_ONE_DATA         | Single point data saving               |

Sampling channel number, sampling length: tell the extension to take the first few channels and how much data to collect.
CRC check: There are two error detection methods for the standard Modbus protocol. LRC method and CRC method. Since the system selects the RTU mode as a character frame, only the CRC check can be used. The CRC field is appended to the end of the message, first added to the low byte and then to the high byte. Therefore, the high byte of the CRC is the last byte of the transmitted message. The CRC check function in this system is unsigned short CalCRC16 (unsigned char *p, unsigned short len, unsigned short crc). The special feature of this CRC program is that it can calculate discontinuous data sets, so that when the amount of data sent is relatively large, it is not necessary to store the data to be sent to a continuous memory space, thereby saving memory space. Where p is the start and end address of a small piece of continuous data, len is the length of the piece of data, crc is the previously calculated crc value, and if it is the first calculation, crc is 0.

At this point, a simple and practical communication protocol based on standard Modbus RTU is built.

4. Interface and software design

All configurations of the TRF6900A are via the SPI interface, which consists of five registers. An SPI instruction is used to determine what to do, and the SPI interface is active only in Power-down mode and Standby mode.

The five registers are: Status-Register contains data ready DR and address matching AM status; RF-Configuration Register contains transceiver frequency, output power and other information; TX-Address contains the target device address byte length, configured by Register setting; TX-Payload contains the valid data packet sent, the data length is set by the configuration register; RX-Payload contains the valid data packet received, the length of the data is set by the configurator.

(A). SPI instruction settings for the TRF6900A

The commands for the SPI serial interface are shown in Table 5 below. When the CSN port is low, the SPI interface begins to wait for an instruction, and a new instruction will start when the CSN is switched from high to low.

(B). Configuration of the RF register of the TRF6900A
In order for the TRF6900A to work properly, its RF configuration register must be configured, and the configuration in the RF configuration register of the host and the extension transceiver module must be the same, so that communication can be established normally between the two! The following describes the main parameters and basic settings of the RF configuration register of the TRF6900A, as shown in Table 6.

Table 6. RF register part byte configuration description

| Name           | Set value | Description                      |
|----------------|-----------|----------------------------------|
| CH_NO          | 0 0110 1100 | Carrier frequency is 433.2MHZ    |
| HRFEQ_PLL      | 0         | Set the PLL operating mode       |
| PA_PWR         | 11        | Output power 10dbm               |
| RX_PW, TX_PW   | 000 0001  | 1 byte valid data                |
| UP_CLK_EN      | 0         | External clock is prohibited      |
| XOF            | 011       | Crystal oscillator frequency 16M |
| CRC_EN         | 1         | Enable CRC check                 |
| CRC_MODE       | 1         | Using 16-bit CRC check           |

In the TRF6900A module, the RF register contains 10 bytes. The configuration word content will determine the operating characteristics of the RF module TRF6900A.

5. Main program flow chart
The main program flow chart is shown in Figure 1 below:

![Main program flow chart](image)

6. System debugging
The hardware debugging is mainly to debug whether the hardware has a short circuit and whether the devices can work normally. The first step in debugging is to check the quality of each component. The
second step is to check if the line is connected correctly, and check for solder joints or short circuits. The third step is to use a multimeter to measure whether the voltage at each power supply terminal is normal.

This part is the most complicated in the whole system debugging. Because the radio can't be seen or touched, in order to ensure that both parties can communicate normally, the first step: to ensure that the wireless transceiver module TRF6900A can work normally, first need to configure the register of TRF6900A, here I write the configuration word into TRF6900A first, read it out. Then compare the read value with the written value. If they are consistent, the configuration of the TRF6900A can be proved successful. Step 2: Check whether the RF register configuration of the wireless transceiver module TRF6900A of the host and the extension is consistent. The third step: using the extension to continuously send decimal numbers: 0-255, received by the host. The host sends the received number to the serial port and uses the serial port debugging assistant to observe the received data. If the data can be received, and the data is in the range of 0-255, it proves that the host and the extension communicate successfully. If no data is received, check the hardware and software design and repeat the above steps to check for the problem. In programming, pay attention to the timing between TRF6900A mode switching. It must be programmed according to the timing requirements in the data sheet. Otherwise, communication will fail!

A typical phenomenon was found in the communication between the debugging host and multiple extensions. When the host is powered off and then the host is turned on, it is found that the host cannot communicate with the extension again. After analysis, it is known that when the host is powered off and then turned on, a random data will be sent. When the host sends a MODBUS command to the extension, the command shift will occur, resulting in communication failure. The solution is to be mentioned in the previous section, which is to add a timed interrupt in the extension. When a data is received, the interrupt is immediately opened and the interrupt flag is cleared. The interrupt timing time is 1S, and the 1S timing time ensures that a MODBUS command is received! If the received command is incorrect, or the command is not received enough, the receiving data counter will be cleared after the timing time expires, and the interrupt flag will be set to ensure the next re-receive! This will solve this phenomenon!

7. Conclusion
The wireless sensor network designed in this paper has the characteristics of low power consumption, strong anti-interference ability, large capacity, real-time acquisition, long data transmission distance, safety and reliability. Finally, we analyzed the experimental and data analysis and detailed some of the irregularities of the design system.

Acknowledgements
This paper is funded by the Science and Technology Project of State Grid Liaoning Electric Power Company Ltd (2019YF-42), Research and Application of Key Technologies of Power 230MHz Low Power Wan.

References
[1] Leonard J, Durrant-Whyte H. Mobile robot localization by tracking geometric beacons [J]. IEEE Transactions on Robotics and Automation, 2016, 7 (3): 376-382.
[2] Guivant J, Nebot E. Optimization of the simultaneous localization and map-building algorithm for real-time implementation [J]. IEEE Transactions on Robotics and Automation, 2011, 17 (3): 242-257.
[3] Fox D, Burgard W, Kruppa H. A probabilistic approach to collaborative multi-robot localization [J]. Autonomous Robots, 2017, 8 (3): 325-344.
[4] Thrun S, Fox D, Burgard W, et al. Robust Monte Carlo localization for mobile robots artificial intelligence [J]. Artificial Intelligence, 2010, 128 (1): 99-141.