Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 17, No. 3, 2025

Wireless monitoring and transmission system for multi-sensor environmental data

Shuangxin Yang *, Dan Liu, Xinyu Li

China Electronics Technology Group Corporation Twentieth Research Institute, Xi'an, China

* **Corresponding author**

Abstract: This paper employs multi-sensor devices to design a system for collecting and monitoring environmental information, as well as for wireless encrypted transmission. The system adopts a distributed architecture with one master and multiple slaves. First, multi-channel slave device data processing boards are used to collect and display real-time environmental information such as temperature, humidity, smoke, PM2.5 concentration, and fire through sensors. Based on the requirements of different environmental scenarios, different threshold ranges are set to determine whether parameters fall within the threshold range. If any parameters are abnormal, an audio-visual alarm is triggered. Secondly, an improved encryption algorithm is used to encrypt the raw data after collection, and a wireless transmission module is employed to transmit the data, conveying environmental information from different areas to the main device's data processing board. Finally, the main device's information processing board card performs data decryption, processing, aggregation, and reporting functions. This achieves 24/7 real-time monitoring, encrypted transmission, and abnormal alarm functionality for environmental information across different scenarios.

Keywords: MCU; Sensors; Data encryption; Wireless transmission.

1. Introduction

This system uses a Microcontroller unit (MCU) [2]as its core component, enabling real-time remote monitoring of environmental parameters in various scenarios. It features the following functions: measurement and display of temperature, humidity, smoke, PM2.5 concentration, and fire detection; data encryption; wireless data transmission; audio-visual alarms when collected data exceeds alarm thresholds; storage of abnormal data; and upper-level computer display and control functionality.

Working principle: The device collects operational parameters through multiple sensors within its designated responsibility module area. The collected parameters are first displayed, then encrypted, and transmitted to the host via a wireless communication module [3]. The host aggregates and displays the received data on an LCD screen. If the collected data exceeds the alarm threshold, the host triggers an audible and visual alarm, stores the abnormal data, and sends the collected data in real-time to the upper-level computer software via a serial port. The system's working principle is illustrated in Figure 1.

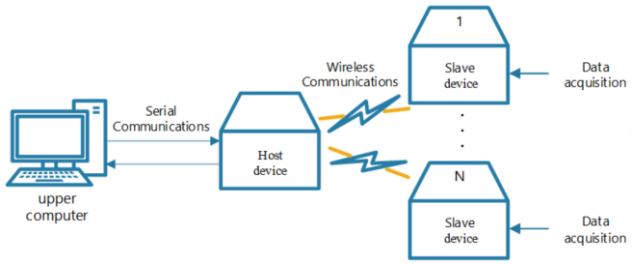

Figure 1. System working principle diagram

2. Detailed Design

2.1. System Hardware Design

From the hardware design framework of the device：The device first collects environmental working parameters within the relevant area, then displays the collected data via a screen display module, encrypts the raw data using an improved algorithm, and finally transmits it to the main device via a wireless module. The hardware block diagram of the device is shown in Figure 2.

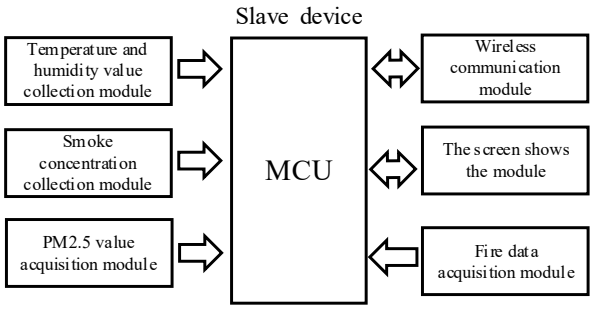

Figure 2. From the device hardware block diagram

Main Equipment Hardware Design Framework: The main device is responsible for acquiring data from the slave device, receiving data via a wireless communication module, decrypting and displaying the data, and then transmitting the data to the host computer via an RS232 serial communication module for display. When the acquired data exceeds the set threshold range, the main device enables the audio-visual alarm circuit to sound an alarm and stores the abnormal data. The hardware block diagram of the main device is shown in Figure 3.

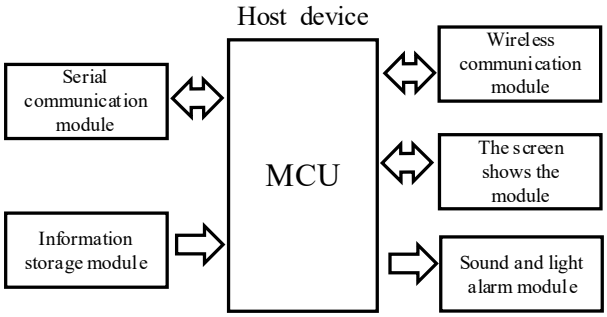

Figure 3. Main equipment hardware block diagram

2.2. System Program Design

System from device main program: The system's program design for the device mainly completes the initialization of various sensor modules, data collection, encryption algorithm encryption processing, wireless transmission, and other tasks. The program flow chart is shown in Figure 4:

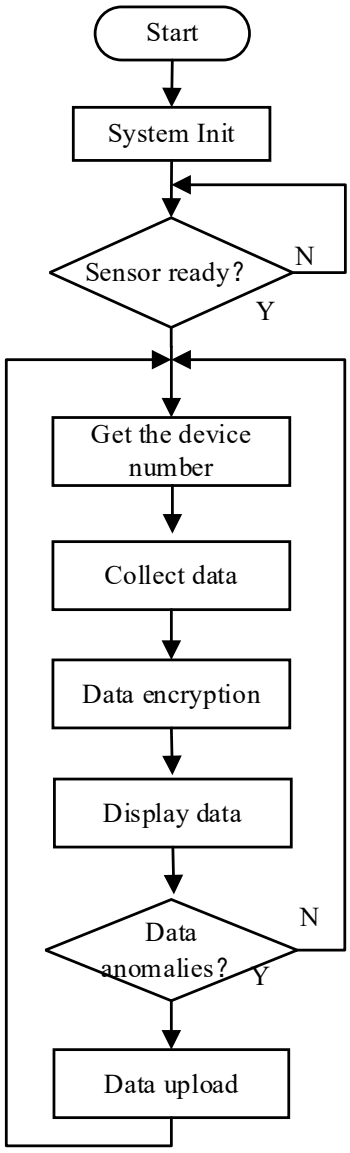

Figure 4. From the device main program flowchart Tables

System main device main program: The program design of the system's main equipment mainly involves decrypting and processing data reported wirelessly by various slave devices, reporting parameters to the host computer software, and determining whether to trigger audible and visual alarms and store abnormal information based on preset parameter ranges. The program flowchart is shown in Figure 5.

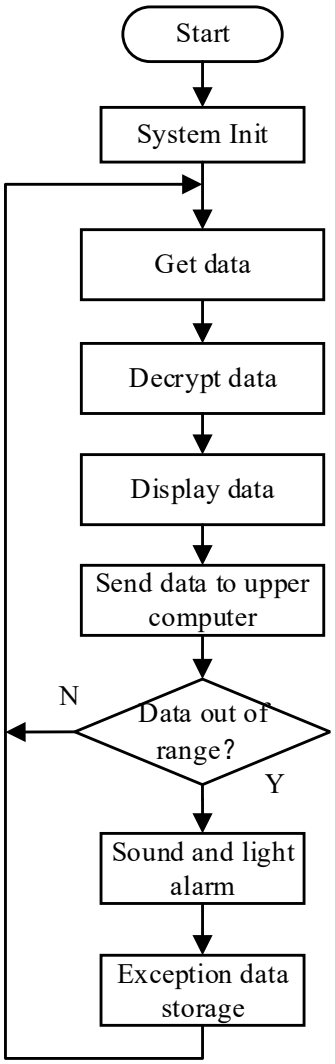

Figure 5. Main Equipment Main Program Flowchart

2.3. Improving cryptographic algorithm design

The improved AES [4] encryption algorithm consists of three stages: data preprocessing and encryption, data transmission, and data decryption. First, the plaintext data A to be transmitted is obtained, and the corresponding data preprocessing operations are performed. The data is then input into the AES encryption algorithm to complete the first step of encryption, resulting in the ciphertext data B1. The serial number of the device's data processing board is used as the seed input to the pseudorandom number generator to generate a random bit stream, completing the second encryption step to obtain ciphertext data B2. The results of B1 and B2 are then added together to form the final ciphertext data B for transmission. This approach enhances the reliability of the encrypted data results without significantly compromising data processing real-time performance; Next, the ciphertext data B obtained in the previous step is processed using the MD5 algorithm to calculate the MD5 value C of the transmitted data. Then, the ciphertext data B and the calculated MD5 value C are transmitted to the main device's data processing board. Upon receiving the data B' and C', the main device processes B' using the MD5 algorithm to obtain the corresponding MD5 value D. A verification decryption mechanism is introduced to ensure that data is not

tampered with during transmission, thereby enhancing data security; Finally, a comparison and verification of C' and D before and after transmission is performed. If the comparison is correct, the next step of decryption is carried out, which is the inverse process of encryption; if the comparison and verification fails, the data is discarded, and an acknowledgment (ACK) is sent back to the slave device unit 1, ensuring the reliability of data transmission. The algorithm flowchart is shown in Figure 6

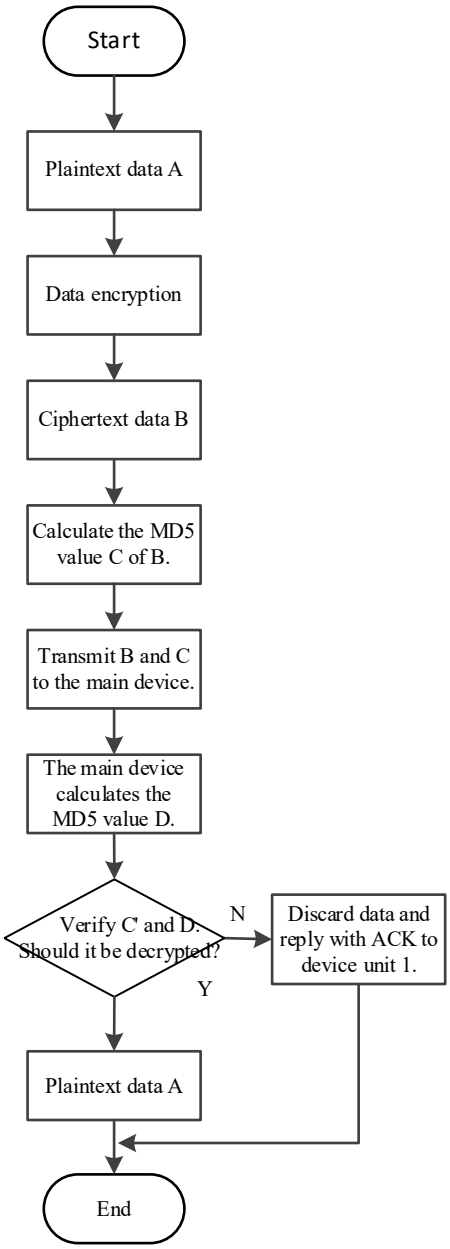

Figure 6. Encryption Algorithm Processing Flowchart

2.4. Host computer display control design

The PC-based [5] monitoring software uses the RS232 serial communication protocol to obtain real-time data uploaded by the lower-level machine, making it convenient for users to view and manage. The overall functional diagram of the PC-based monitoring software is shown in Figure 7.

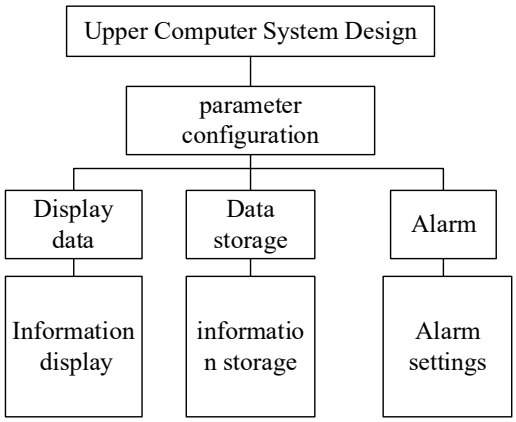

Figure 7. Overall functional diagram of host computer software

The form interfaces that need to be designed for PC-based monitoring software mainly include: login form design, system configuration form design, information display form design, database form design, and information alarm form design. Next, we will introduce the design of each form one by one.

2.4.1. Login Form Design

The login interface of the PC-based monitoring software primarily implements password-based login to enhance system security. It also features an automatic prompt function for users who have forgotten their passwords. Typically, users can access other system functions by entering their login credentials on this interface. If a user forgets their password, they can click the “Forgot Password” button, and the system will display a pop-up window with instructions for the user.

2.4.2. System Configuration Form Design

The system configuration window of the PC-based monitoring software will configure the required parameters based on the system configuration interface.

2.4.3. Figures. Information display form design

The information display window of the PC-based monitoring software. This interface primarily enables the PC-based monitoring software to display RS232 serial port data in real time after acquisition. After connecting the RS232 serial port cable to the main device's processing board, users first select the personnel information they wish to view in this interface, then click to view the information. This interface also features an information alarm light, which turns red and emits an alarm sound when an information alarm occurs.

2.4.4. Database Form Design

The information display window of the PC-based monitoring software. This interface primarily enables the real-time storage of environmental data obtained by the PC-based monitoring software. Click “View Database” on this interface, then click the name of the corresponding database table to display all contents of the currently selected database. Click “Delete Data Table” to delete the corresponding data table.

2.4.5. Information Alarm Settings Window Design

The information display window of the PC-based monitoring software. This interface primarily enables users to set the upper and lower limits for alarm information and determine whether to enable sound alerts in the PC-based monitoring software. Selecting “Enable Alarms” and clicking ‘Save’ completes the alarm information settings. The system automatically locks all alarm information. If any alarm parameter settings are incorrect, users can click “Reset” to unlock the alarm information settings, then reconfigure and

save them.

3. Summary

This paper takes multi-sensors as the starting point and designs a complete system for data collection, algorithm encryption, data transmission, and host computer display. This system can provide convenience for industrial control in certain scenarios, freeing up human and material resources to a certain extent and enhancing data reliability. However, due to limitations in hardware processing capabilities, there are still some deficiencies in real-time performance when calling algorithm parsing. Further research will be conducted in this area in the future.

Acknowledgements

I would like to thank my colleagues Liu Dan and Li Xinyu for their contributions to the algorithm research in this article.

References

[1] Antić M, Papp I, Ivanović S, et al. Learning from smart home data: Methods and challenges of data acquisition and analysis in smart home solutions[J]. IEEE Consumer Electronics Magazine, 2020, 9(3): 64-71.

[2] Khalifeh A, Mazunga F, Nechibvute A, et al. Microcontroller unit-based wireless sensor network nodes: A review[J]. Sensors, 2022, 22(22): 8937.

[3] Fang S, Zhu X, Hou M, et al. Research and design of distributed online monitoring system for power capacitor in substation based on WiFi wireless communication[C]//International Workshop on Automation, Control, and Communication Engineering (IWACCE 2022). SPIE, 2022, 12492: 68-74.

[4] Nechvatal J, Barker E, Bassham L, et al. Report on the development of the Advanced Encryption Standard (AES)[J]. Journal of research of the National Institute of Standards and Technology, 2001, 106(3): 511.

[5] Lu Z, Mohamed H. A complex encryption system design implemented by AES[J]. Journal of Information Security, 2021, 12(2): 177-187.

Qin H, Dang R, Dang B. Design of upper computer for wellhead multi-parameter detection based on LabVIEW[C]//2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP). IEEE, 2022: 1240-1244.