Advances in Computer, Signals and Systems (2026)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2026.100206
ISSN 2371-8838 Vol. 10 Num. 2

Design and Implementation of a Smart Community System Based on Multi-Node Cooperative Sensing and Edge Control

Xilin Chai[1], Zhaoyong Shao[2], Qingxiao Song[1], Xin Chai[1], Yingjie Ren[1]

[1]Lanzhou Petrochemical University of Vocational Technology, Lanzhou, Gansu, 730060, China
[2]PetroChina Lanzhou Petrochemical Company, Lanzhou, Gansu, 730060, China

Keywords: Smart Community; Multi-Node Collaboration; Multi-Source Data Fusion; Embedded Systems

Abstract: To address the issues of isolated sensing nodes and decentralized control and decision-making in traditional smart community management systems, we have designed and implemented a smart community control system based on multi-node collaborative sensing and control. The system employs a master-slave dual-MCU distributed architecture, integrating multi-source sensors such as temperature, smoke, infrared heat detection, and light sensors, and incorporating modules such as RFID and IC card readers. It comprises five sub-control nodes: lighting, fire and theft prevention, access control, parking management, and Bluetooth relay control. Through multi-source data fusion via edge MCUs, the system enables fire risk assessment and graded alarms for the residential community. Joint hardware and software testing results indicate that all nodes function normally, data transmission is stable, control is effective, and measurement errors for all sensor monitoring values are within acceptable limits. Under multi-parameter joint evaluation, the system effectively suppresses false alarms and accurately triggers the highest-level alarm in simulated open-flame scenarios. This solution provides a feasible reference for the construction of low-cost, highly reliable smart residential communities.

1. Introduction

With the rapid advancement of IoT and embedded technologies, the development of smart communities now demands enhanced multi-node collaborative sensing and control capabilities. Current community management systems often suffer from isolated sensing terminals, decentralized control decisions, and delayed emergency response coordination [1-2]. To address these challenges, this study designs and implements a multi-node collaborative sensing and control system based on high-performance MCUs. The system integrates contactless IC card access control with parking management systems, combines infrared pyroelectric, temperature, and smoke detection for fire and theft prevention, incorporates human motion and light-sensitive monitoring for lighting control, utilizes Bluetooth wireless relay control, and features hazard alarm mechanisms. Through multi-node data fusion and collaborative decision-making algorithms, information sharing and coordinated control are achieved among sensing terminals and execution units [3-4]: When both

smoke and infrared signals are triggered simultaneously, the system automatically activates audio-visual alarms; human motion and light-sensitive modules work in tandem with relays to optimize energy-efficient lighting in public areas, while contactless IC cards synchronize access control and parking management. Experimental results demonstrate that this solution significantly reduces deployment costs, accelerates emergency response times, and enhances user convenience, providing an effective reference for building low-cost, highly reliable, and scalable smart communities.

2. Overall System Architecture Design

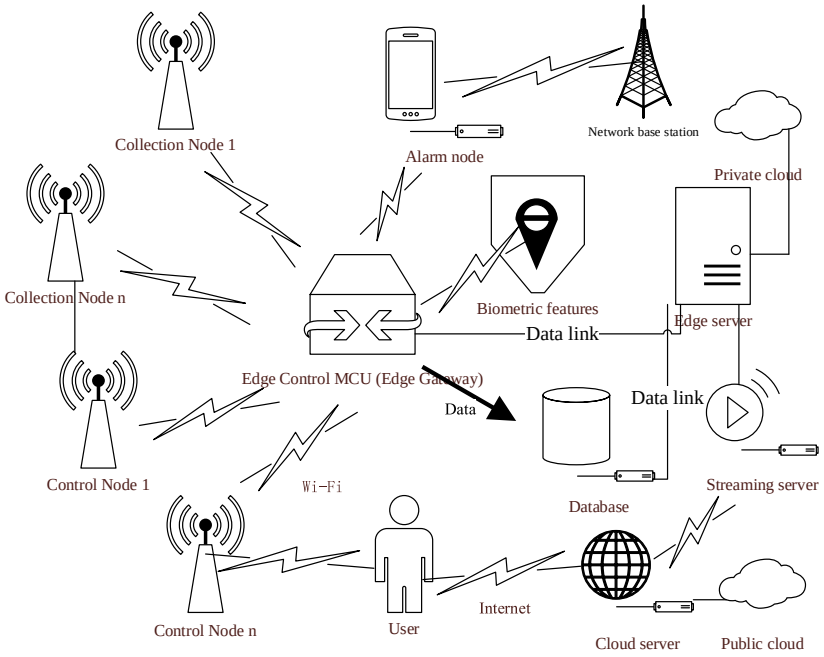

Figure 1: Overall System Architecture Design

Based on the IoT architecture, the overall system design is illustrated in Figure 1 [5]. At the sensing layer, data acquisition nodes are constructed using various sensors including temperature, smoke, photosensitive, infrared pyroelectric, and human motion detectors. At the control layer, execution control nodes are established by utilizing relays to operate access control systems, barrier gates, and lighting equipment. All acquisition and control units employ the ESP8266 as their core component, connecting to the edge gateway via Wi-Fi communication protocols and serial buses. The edge gateway manages node operations and communication aggregation within the wireless sensor network, integrating Wi-Fi or 4G/5G modules for remote wireless data transmission while utilizing Ethernet interfaces for wired data forwarding, serving as a bridge between sensor nodes and the monitoring center [6]. The network layer aggregates and packages collected data, transmitting it to servers through serial interfaces for processing by the data center, enabling IoT device management and environmental status monitoring. The application layer features both public and private cloud platforms that balance data security with hierarchical access controls, allowing users to access the data center via computers or mobile devices to view real-time field data and remotely operate various IoT devices.

3. System Hardware Design

3.1 System Hardware Block Diagram

This system employs a master-slave dual-tier MCU distributed processing architecture, enabling modular division and coordinated operation of sensing, control, and management functions [7-8]. As shown in Figure 2, the system centers around the main control MCU and functional node control MCUs, achieving integrated operation for smart community environmental monitoring, security management, and equipment control through task hierarchy and data interaction. A multi-node distributed hierarchical control framework coordinates the parallel operation of four subsystems: lighting, security, access control, and parking. By integrating temperature/humidity, smoke, and identity recognition data, it forms a multi-source sensor array that enables intelligent environmental monitoring and closed-loop emergency management. The embedded control algorithm framework implemented in C language, with its high execution efficiency and excellent portability, provides robust operational support for the system's underlying logic.

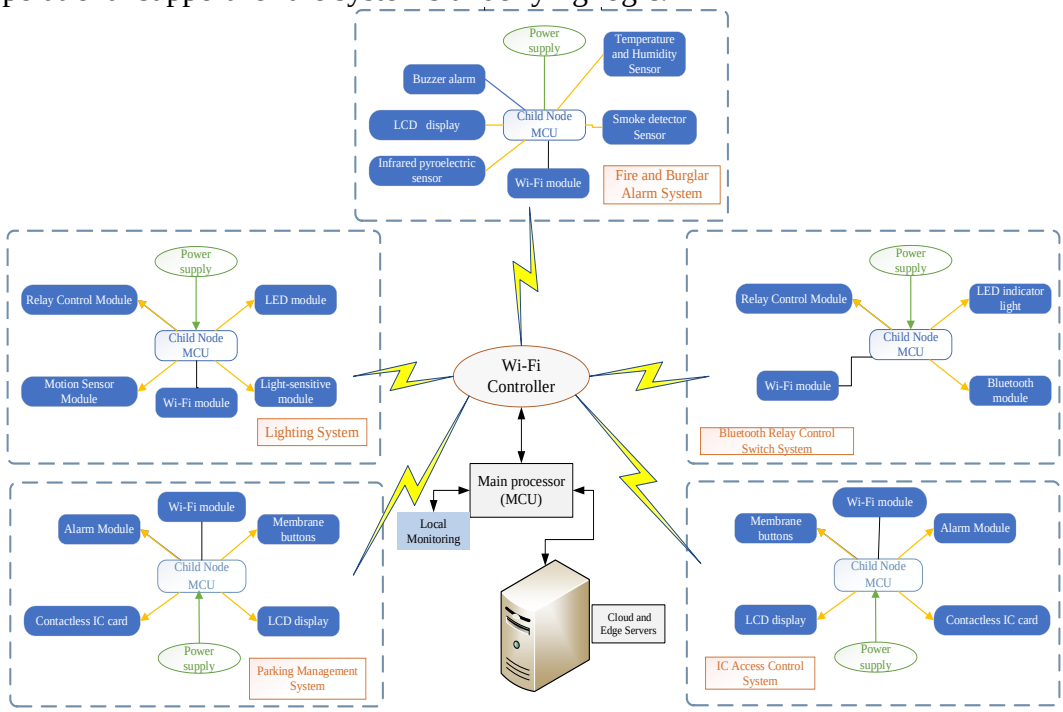

Figure 2: System Hardware Design Block Diagram

3.2 Interface Circuit Design for Each Infection Control Node

The interface circuit design of each node is tailored to meet the collaborative sensing and control requirements of smart residential communities, centered around a master-slave distributed microcontroller that integrates sensing, control, and management functions. The microcontroller combines CPU, memory, I/O ports, timers/counter, and interrupt systems on a single chip, offering advantages such as compact size, high integration, and robust reliability, making it widely used in smart home and automation control applications. In the lighting node control circuit, the HC-SR501 pyroelectric infrared sensor detects human movement by outputting high/low voltage levels to indicate presence, while the photoresistor provides environmental brightness signals via the LM393 comparator, enabling adaptive lighting control. The relay drive interface engages when the node microcontroller outputs a low voltage level, controlling lighting load activation/deactivation. The

fire and theft sub-node incorporates temperature, infrared pyroelectric, and smoke sensors: the DHT11 digital temperature and humidity sensor transmits data to the main controller via a single-bus interface, while the MQ-2 smoke sensor outputs analog signals converted by the ADC0832 into digital values processed by the node microcontroller. The node control system also features a dedicated keyboard and LED/buzzzer alarm modules for temperature, smoke, and intrusion alerts respectively. The Bluetooth relay control switch employs a low-power Bluetooth module requiring PIN verification during initial pairing, enabling wireless command-based relay operation for sub-node system control. All node circuits integrate the ESP8266 module for Wi-Fi network transmission. In summary, each hardware module centers around the microcontroller, integrating multi-source sensor data acquisition, signal conditioning, and drive execution to form a closed-loop perception-decision-control system, providing a stable and reliable hardware foundation for intelligent community collaborative management. The interface circuit designs of the system's sensing and control nodes are illustrated in Figure 3.

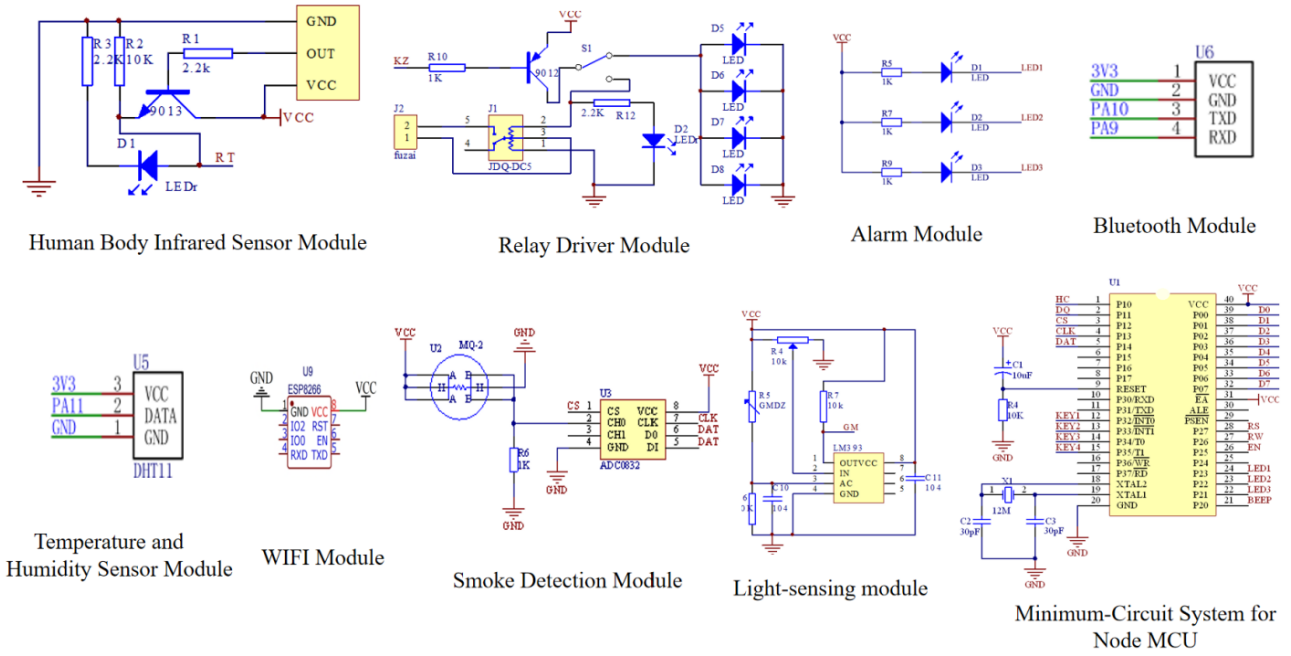

Figure 3: Design of the Interface Circuit for Major Nodes

3.3 Radio Frequency Identification (RFID)

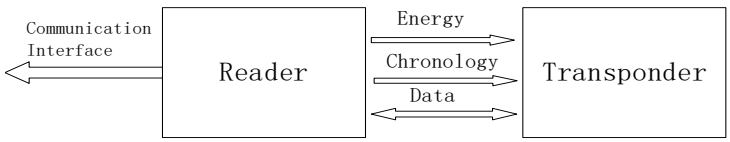

Figure 4: Basic schematic diagram of RFID

Radio Frequency Identification (RFID) belongs to the category of contactless automatic identification technologies. Its core principle utilizes the spatial coupling effect of radio frequency signals to enable contactless data exchange, thereby facilitating the identification and tracking of target objects. RFID is an integration of multiple technologies, including wireless communication and integrated circuits. The basic operational mechanism is illustrated in Figure 4: The reader supplies the necessary energy to the electronic tag (transponder) and, through precise timing control, enables bidirectional information exchange between them. Specifically, when a tag enters the

reader's magnetic field coverage area, it receives the radio frequency signal emitted by the reader. Energy supplied by an induced current activates the tag, which then transmits its stored product code information. In certain applications, the tag may also actively transmit signals at specific frequencies; the reader receives and decodes these signals before uploading the valid information to a central information system for comprehensive processing. Currently, RFID technology has found widespread application in logistics and warehousing, supply chain traceability, smart home security systems, and identity verification.

4. System Software Design

4.1 Main MCU Program Design

The flowchart of the system's main control program is shown in Figure 5. Upon power-on, the system completes initialization of all modules, then cyclically collects data from sensors such as temperature, smoke, and infrared detectors to determine whether alarm conditions are triggered. If triggered, an audio-visual alarm is activated and alarm data is uploaded to the server; otherwise, only routine monitoring data is transmitted. The program continuously monitors threshold configurations issued by the control terminal and dynamically updates operational parameters. Upon alarm occurrence, the event is recorded and enters a hold/untrigger decision phase. At the end of the loop, a watchdog refresh operation is executed before returning, ensuring stable system operation. This process enables closed-loop control with multi-node collaborative sensing, real-time alarms, and remote configuration capabilities.

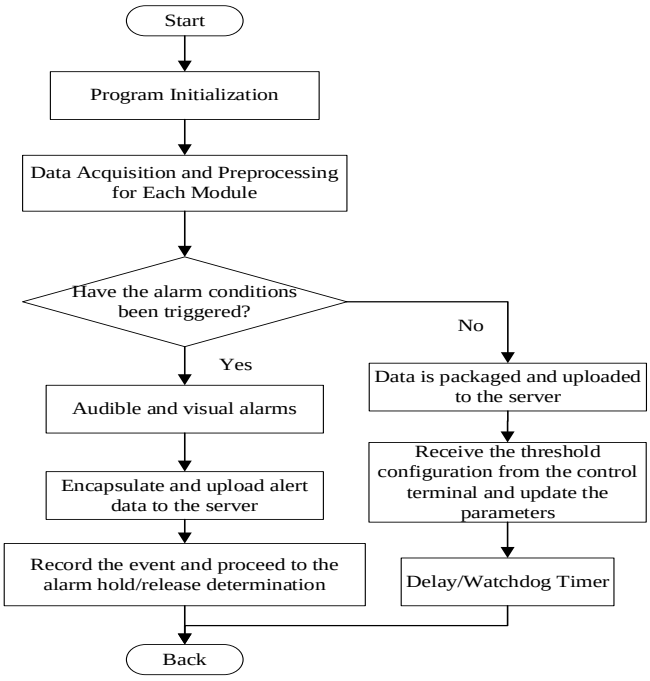

Figure 5: Main Program Control Flow

4.2 Communication Subroutine Design

The flowchart of the communication subroutine is shown in Figure 6. Upon power-on, the system first completes program initialization, then activates the WiFi module and configures the

access password. The program verifies successful network connection: if connection fails, it attempts repeatedly until successful; if successful, it reads the local IP address, processes and encapsulates the collected multi-node sensor data, and sends it to the server, thereby concluding the communication process. This subroutine ensures reliable data transmission between the system and the cloud platform.

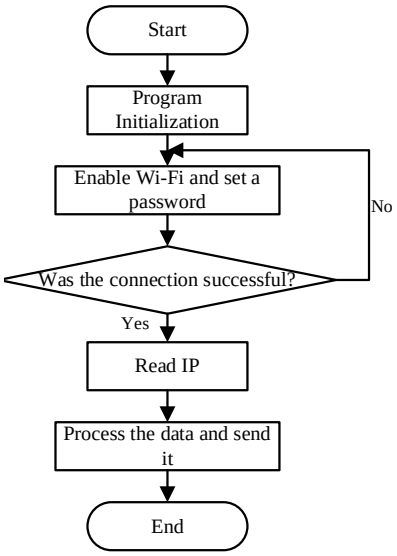

Figure 6: Communication subroutine design flowchart

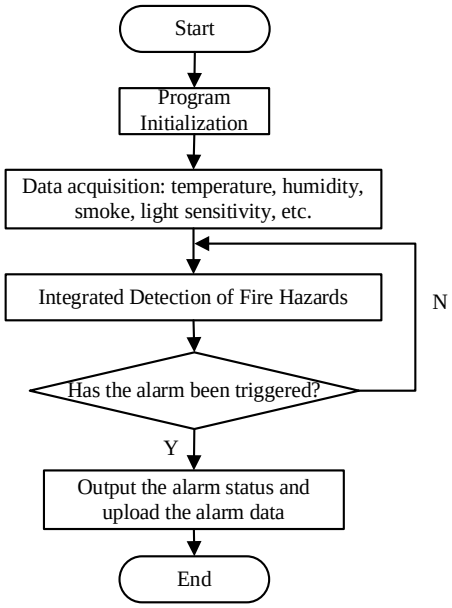

Figure 7: Flowchart of the sensor fusion subroutine design

4.3 Sensor Fusion Subroutine Design

The sensor fusion subroutine flow is illustrated in Figure 7. Upon initiation, the program first performs initialization operations, then synchronously collects multi-source sensor data including temperature, humidity, smoke, and photosensitive readings. Based on this information, the system conducts fusion analysis to assess the fire risk level of the residential area [9]. If alarm conditions are triggered, the system outputs an alarm status and uploads the alarm data to the server; otherwise,

it terminates the process immediately. Through multi-node collaborative sensing and data fusion, this subroutine enables rapid identification and reporting of fire risks in residential areas.

4.4 Design of the Local Server for the Monitoring System

This system employs a Raspberry Pi based on the ARM Cortex-A53 architecture as the core video streaming server. Its motherboard integrates 1 to 4 USB interfaces and a 100 Mbps wired network port, supporting keyboard, mouse, and network connectivity with network access capabilities equivalent to those of a personal computer. Powered by the Linux operating system, it establishes a local area network server while deploying the same configuration environment as a cloud server. Even in the event of WAN failures, the system continues data reception and storage via the local LAN, automatically synchronizing cached data to the cloud server upon communication restoration, thereby ensuring the integrity and reliability of monitoring data and significantly enhancing operational reliability. Additionally, the integration of a video streaming server within the Raspberry Pi, combined with FRP (Forwarded Proxy) technology for internal network penetration, provides remote access capabilities for security protection, further strengthening the campus's security safeguards.

5. Effectiveness of System Hardware and Software Design

5.1 Software Debugging

In this system design, the system program was developed and debugged using Keil C programming software. First, the program was compiled in Keil C, yielding zero errors and warnings. The resulting HEX file was then downloaded to the MCU nodes. The program execution flow is illustrated in Figure 8.

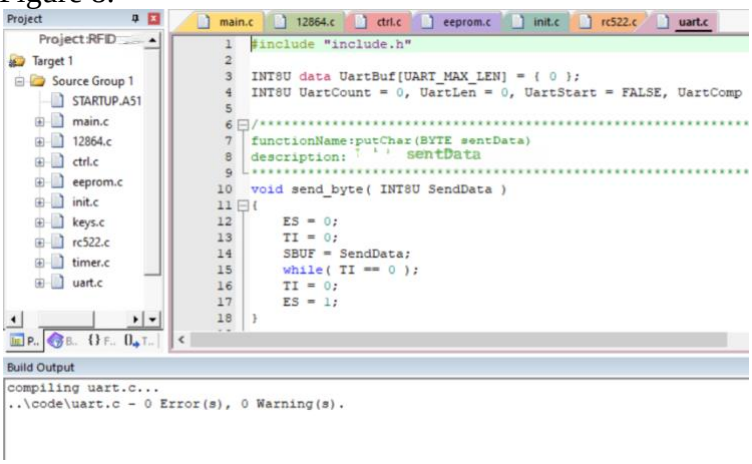

Figure 8: Example of node software debugging and execution process

5.2 Hardware Debugging

During the hardware debugging phase, first visually inspect the soldering quality and polarity of all components. Then, power on the device and use a multimeter to measure the minimum system supply voltage of the microcontroller, which reads 5V, indicating normal operation of the main control circuit. The test results for each node module are as follows.

(1) Lighting Node Module: Upon power-on, the measured voltage across the LED indicator is 4.3 V, deviating 0.7 V from the nominal value of 5 V; the measured current is 0.2 mA, while the

theoretical static current is 0 mA, resulting in a deviation of 0.2 mA. The lower voltage is primarily due to actual current consumption in the parallel branch and the voltage drop across the driver transistor, whereas the static current deviation may be attributed to the MCU port's default output state or leakage current generated by external pull-up or pull-down resistors. During actual lighting tests, the LED emits light normally, and the lighting functionality meets requirements.

(2) Fire and Theft Detection Module: The HC-SR501 infrared human body sensor has a detection angle of approximately 120 ° and a maximum detection range of 7 m. Tests indicate that sensitivity is high within 1-2 m, decreases to acceptable levels at 4 m, diminishes significantly at 5-6 m, and shows no response beyond 8 m. The DHT11 sensor measures temperature from 0-50 ℃ with an accuracy of ±2 ℃, and humidity from 20-90% RH with an accuracy of ±5% RH. It operates with a measurement cycle of approximately 5 seconds and a relatively slow response speed, resulting in an average measurement error of about ±7%. The smoke sensor requires a 4-minute preheating period before normal operation, detects concentrations ranging from 300 to 10,000 ppm, and has a response time of approximately 1 second. These deviations are caused by a combination of the sensor's inherent accuracy, ambient temperature fluctuations, and analog-to-digital conversion errors.

(3) IC Card Access Control and Parking Management Node Module: The hardware verifies normal MCU power supply, proper card reading, correct LCD display, and reliable relay control, successfully enabling IC card identity verification, access control operation, parking space management, and vehicle entry/exit management [10].

(4) Bluetooth Relay Switch Control Node Module: During initial pairing, the Bluetooth module verifies the PIN code and controls relay activation/deactivation via wireless commands, thereby coordinating the switching operations of the remaining four subsystems (including lighting and access control). Testing confirmed proper functionality of the Bluetooth remote control.

The actual performance of the system's hardware and software debugging and operation is shown in Figure 9.

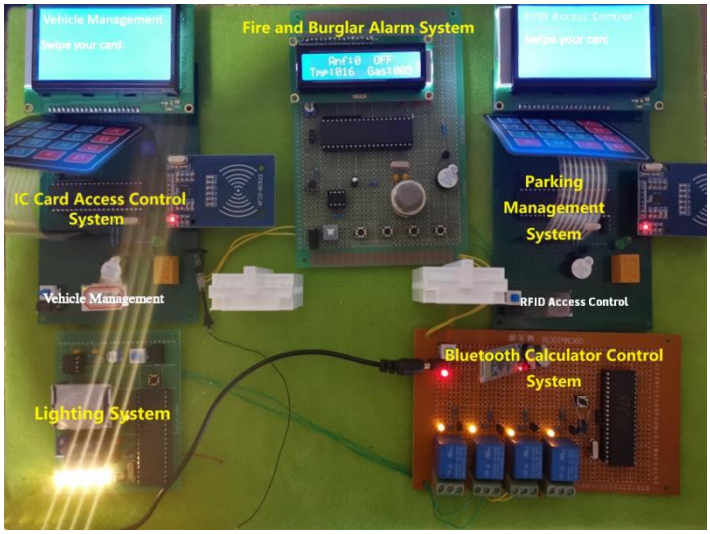

Figure 9: Practical performance of multi-node system hardware-software joint debugging and operation

5.3 Information Fusion of Multi-source Sensors at the Node

For the intelligent residential community fire detection task, a fuzzy inference method incorporating multi-source sensor data fusion is introduced. The fire probability inference model is constructed using four input parameters collected by nodes: temperature, humidity, smoke

concentration, and illumination intensity. Multiple simulations were conducted using MATLAB/Simulink to simulate sensor readings under various environmental conditions and obtain the fire probability output by the fuzzy system. The algorithm was then deployed on the edge MCU, where filtered and stabilized data were fed into the model for testing. The system's fire probability outputs and alarm levels under five simulated scenarios are presented in Table 1.

Table 1: Output Fire Probability and Alarm Levels

Test Scenario	input parameter (T,H,Smoke,Light)	Output fire probability	Alarm Level	Result Judgment
normal environment	(0.26,0.63,0.12,0.42)	0.38	alarm free	safe
high-temperature drying	(0.82,0.18,0.15,0.75)	0.71	Intermediate Alert	Medium Risk
Overcast and damp	(0.28,0.88,0.10,0.15)	0.20	alarm free	safe
Smoke interference	(0.48,0.52,0.78,0.38)	0.65	Intermediate Alert	Medium Risk
Open flame simulation	(0.92,0.15,0.85,0.90)	0.87	Advanced Alarm	highrisk

Experimental data demonstrate that the technical approach adopted by this system enables efficient integration of diverse sensor data. Taking the "high-temperature drying" and "smoke interference" scenarios as examples, the system issued medium-level alerts, highlighting the advantages of multi-parameter joint analysis and effectively reducing false alarms caused by individual parameter anomalies. Under the "open flame simulation" scenario, multiple fire characteristic indicators simultaneously escalated to high-risk levels, allowing the system to accurately assess a high fire probability and trigger the highest-level alarm.

6. Conclusion

This study addresses the collaborative sensing and control requirements for multiple nodes in smart communities, completing the overall system design, hardware selection, software programming, and joint testing. Centered around master-slave dual-level MCUs and Raspberry Pi, the system achieves closed-loop control encompassing sensor data acquisition, edge processing, and cloud interaction. The system operates reliably and meets its intended design objectives. Experimental results demonstrate that infrared sensing, temperature detection, and smoke detection functions satisfy security requirements; the data fusion algorithm effectively integrates four parameters-temperature, humidity, smoke, and illumination-and generates medium-level alerts under high-temperature/dry conditions or smoke interference scenarios, while triggering high-probability alarms in simulated open flame environments. Future work should focus on optimizing sensor deployment and wireless communication protocols to enhance the system's robustness and scalability in complex environments.

Acknowledgement

This work was supported by Gansu Provincial Education Science "14th Five-Year Plan" Research Project (GS[2023]GHB1468)

References

[1] Edge Computing Industry Alliance. Edge Computing Reference Architecture 3.0, White Paper of the Edge Computing Industry Alliance. [R]. 2018.

[2] Zhao Yuelin, Wang Ying, Shang Junling, Xu Bing. Design of a Smart Campus Security Alert Information Push System Based on Dynamic Data Aggregation [J]. Cybersecurity and Informatization, 2026, (03):85-86.
[3] Li Yanrong. Dynamic lighting environment design for smart parks driven by digital twins: Lighting demand prediction and multi-scenario adaptive control [J]. China Lighting & Electrical Appliances, 2026, (02):24-27.
[4] Miao Jieyu, Liu Liyuan, Sun Keke, Song Can, Song Mingxuan, Zhu Xiangxuan. Design and Application of a 5G Smart Campus Security System with Cloud-Edge Collaboration [J]. Fujian Computer, 2026,42(02):88-92.
[5] Li Guoxin, Chai Xilin. Design of a Multi-Node Distributed Smart Agricultural Greenhouse Monitoring System [J]. Software, 2022,43(05):56-60.
[6] Gan Peichao. Research on Simulation and Layout Technology for Communication Network Nodes in Smart Parks [J]. Industrial Control Computer, 2025,38(12):107-108.
[7] Bin Xu, Wenguang Zhao, Xiaoming Wang, Bo Gao, Wei Ma. R& D and Application of Smart Park Energy Control Platform Combined with MLM Technology[J]. Applied Mathematics and Nonlinear Sciences,2024,9(1).
[8] Ma Shizi, Liu Haishi, Pan Nan, Wang Sheng. Study on an autonomous distribution system for smart parks based on parallel system theory against the background of Industry 5.0[J]. Journal of King Saud University-Computer and Information Sciences,2023,35(7).
[9] Chen Hong, Jiang Wenxian, Huang Liping, Yu Chongchong. Research on Feature Fusion Methods for Multi-source Data in Wireless Sensor Networks [J]. Journal of Sensor Technology, 2024,37(12):2131-2136.
[10] Yunxin Kuang, Yuling Liu. Analysis and Design of the Smart Park Entry Logistics Vehicle Management System[J]. Journal of Engineering System,2023,1(2).