Design and Research of Security System in University Laboratory

Ding Li
School of Health Services Management
Xi'an Medical University,
Xi'an, Shaanxi, China
E-mail: dingli@xiyi.edu.cn

Zhang Dujuan
School of Health Services Management
Xi'an Medical University,
Xi'an, Shaanxi, China
E-mail: ZhangDj1981sx@162.com

Shi Xuerong
School of Health Services Management
Xi'an Medical University,
Xi'an, Shaanxi, China
E-mail: 39480919@qq.com

Su Yulei
School of Health Services Management
Xi'an Medical University,
Xi'an, Shaanxi, China
E-mail: 541952030@qq.com

***Abstract*—The laboratory is an important place for teaching and scientific research in major universities, and plays an important role in the work of universities. The resources equipped by the laboratory occupy a large part of the resources of the entire school. The laboratory security system plays an important role in ensuring the safety of the laboratory and preventing the loss of equipment. Today's laboratory security systems have factors such as low automation, insufficient management, and inadequate safety in the experimental environment. Moreover, most security systems are built using wired methods, which have problems such as cumbersome wiring, aging lines, and difficult maintenance. In view of the many problems in the current laboratory management, this paper proposes a security system designed and implemented by the ZigBee technology of the Internet of Things. The system uses a wireless network to monitor laboratory access control and the environment, realizing the intelligence of the laboratory security system.**

Keyword-Internet of Things (IoT); Sensor; Security

I. INTRODUCTION

In the field of security, with the diversification of networking methods, hardware and software platforms and application technologies, the implementation of security systems has become more and more diverse. At present, the laboratory security system has a large number of alarm constraints and redundancy, and poor real-time monitoring. In response to this series of problems, this paper uses the Internet of Things and other related technologies to carry out research work on the laboratory security system design, and proposes a set Networked laboratory security system. The system uses sensor design nodes to form a ZigBee wireless sensor network to realize the collection of environmental information in the laboratory, thereby automatically monitoring the occurrence of some security risks.

II. IOT TECHNOLOGY

Internet of Things (abbreviation: IoT) originated in the media field and is the third revolution of the information technology industry[1]. The Internet of Things refers to connecting any object with the network through information sensing equipment according to the agreed protocol, and the objects exchange information and communicates, through the information transmission medium to achieve intelligent identification, positioning, tracking, supervision and other functions. There are two key technologies in IoT applications, namely sensor technology and embedded technology[2]. Unlike traditional networks, the terminal of the Internet of Things technology is no longer a PC, and its terminal is an embedded computer system and its supporting sensors. The Internet of Things technology is widely used in industrial, medical, transportation and other fields.

III. NETWORK TOPOLOGY

A typical ZigBee network supports three topologies, namely a star network topology, a tree network topology, and a mesh network topology. The star network topology is composed of a network main coordinator and multiple terminal equipment nodes. The main coordinator node is an FFD device. In a star topology, each terminal node can only communicate with the coordinator node, and each terminal node cannot transmit data. The tree topology is composed of a network coordinator and multiple terminal equipment nodes and routing nodes. The main coordinator and the routing node can have their own child nodes, and the terminal device node can autonomously choose to join the coordinator or the router node. The tree structure follows the order of parent node and child node, that is, each terminal node has its fixed parent node, which must be passed through the parent node layer by layer. The advantage of this topology is that the network coverage is large, but if one of the parent nodes is damaged, all the child nodes connected to it will be unable to communicate. The mesh topology is also composed of a coordinator node, multiple terminal device nodes and router nodes. This structure is different from the tree network structure in that all routing nodes can communicate with each other, and there is no strict communication sequence. When a routing node fails, data can be transmitted through other routing nodes. This topology not only reduces the delay of information transmission, but also improves the routing efficiency and reliability. Through the corresponding routing algorithm, the best path can be found.

According to the current status of the laboratory, the range of experiments that need to be monitored is large, and the types of data monitored are many. From a practical point of view, the wireless network that needs to be established can dynamically delete and add nodes at any time. According to these characteristics, choosing a mesh topology is more suitable for the current laboratory system. The mesh topology has a strong stability and has a strong advantage in a large-scale laboratory monitoring system.

IV. STRUCTURE DESIGN OF LABORATORY SECURITY SYSTEM

The laboratory security system mainly relies on the monitoring of the laboratory environment to determine potential safety hazards or the presence of suspicious persons[3]. Various types of sensors are arranged in the monitoring range. These sensors are connected to the terminal nodes and placed in different locations in the laboratory. The system uses infrared sensors to monitor whether there are people in the room, door magnetic sensors to detect whether someone breaks into the window, smoke and temperature sensors to detect the presence of fire in the laboratory, and harmful gas sensors to detect the leakage of pharmaceutical reagents. When an abnormality occurs, the sensor in the detection unit will send out an alarm signal, and the alarm signal will be transmitted through the communication unit to the monitoring center software via the ZigBee network. The structure of the laboratory security system is shown in Figure 1.

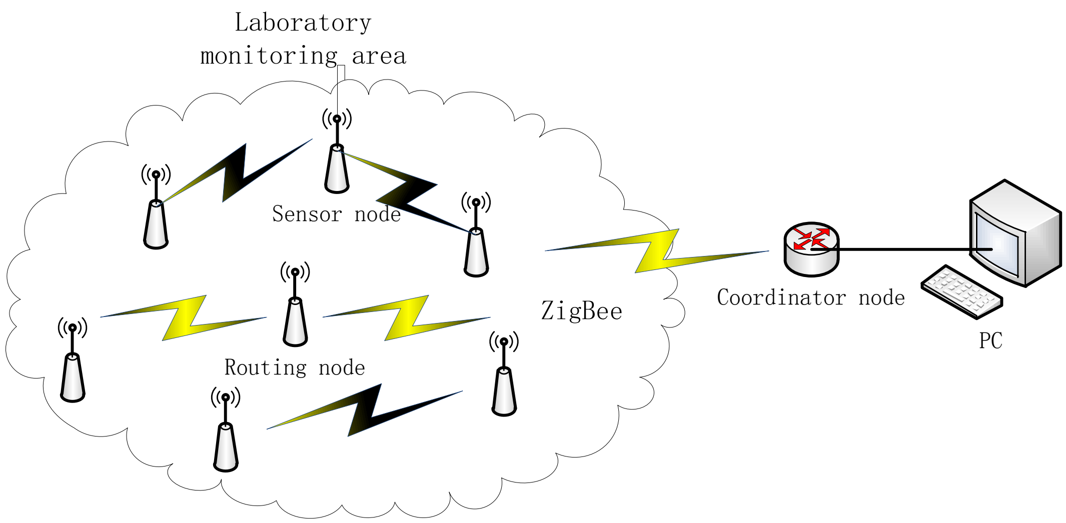

Figure 1. Laboratory security system structure

V. SYSTEM HARDWARE DESIGN

A. Monitoring unit design

The detection unit is mainly composed of an infrared sensor, a door magnetic sensor, a smoke sensor, a temperature sensor, a harmful gas and a combustible gas sensor module. The infrared sensor is mainly used to detect whether there are outsiders in the laboratory. The system uses a pyro electric infrared sensor, which mainly detects the infrared radiation radiated by the human body in a non-contact manner to determine whether someone is in the surveillance area.

This system uses the human body infrared sensor module HC-SR501. This module is fully automatic. When someone enters the sensing range, the module will automatically output high level. If it can always feel the presence of the person, it will always output high level. ，After detecting the existence of human, it will switch from output high level to output low level. The wireless door magnetic sensor is a device commonly used in security systems, mainly used to detect whether the doors and windows are opened or closed illegally. When the wireless door sensor collects the signal that the door sensor is open, it sends an alarm signal. The combustible gas sensor is a detector used to detect the combustible gas content in the air. The system uses the MQ-9 sensor to measure the combustible gas concentration[4]. When the sensor detects that the combustible gas content in the air reaches or exceeds the threshold, it sends an alarm signal. The temperature sensor adopts DS18B20 digital sensor, which is small in size and easy to use. The interface mode is single wire, which can realize the networking function of multiple sensors. The harmful gas sensor module minds the effective detection of many gases such as ammonia, sulfide, methane, and carbon monoxide. The MQ135 sensor is used for the detection of harmful gas content[5].

B. Communication unit design

The communication unit is mainly responsible for data transmission in the wireless sensor network environment monitoring system, which is the core part of the entire system. Data is transmitted through a large number of wireless sensor network nodes arranged in the network. The mutual communication between the various nodes realizes the communication of the entire network and forms the communication unit of the system. The node structure designed in the wireless sensor network is shown in Figure 2. It is mainly composed of three parts: wireless node module, sensor module and power intelligent main board.

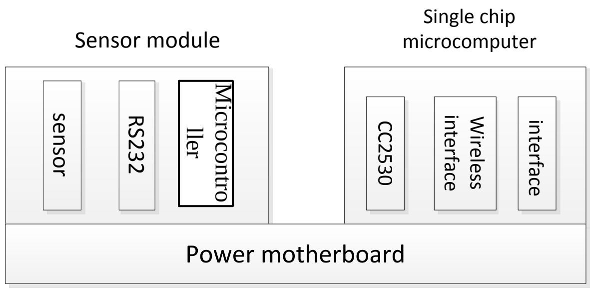

Figure 2. Wireless sensor network node

The microcontroller in the sensor module selects STC89C52RC produced by STC. The controller has the characteristics of high speed and low power consumption. It uses an enhanced 51 core, the calculation speed is higher than the ordinary 8051. The controller can wake up the idle mode at any time to reduce power consumption and ensure that the end node power supply is used for a longer time.

The wireless node module selects CC2530 chip as the microcontroller of the module. The CC2530 chip is compatible with various ZigBee standards, and has the characteristics of stable performance, low power consumption, and strong anti-interference ability[6]. The sensor module is arranged in the monitoring environment and is responsible for data collection and transmission in different areas, and transmits the collected data information to the coordinator. If it cannot be directly transmitted, it is transmitted to the coordinator in a multi-hop manner.

The design part of the power module chooses to use an input voltage of 9v, and the microcontroller and various sensors on the front-end measurement version use a 5v power supply[7]. The ZigBee module CC2530 uses a 3.3V power supply, so the system uses a 7805 voltage regulator to convert the 9V voltage It is 5V voltage. At the same time, the 5V voltage is reduced to 3.3V through the 1117 voltage regulator tube, which is used to provide power for the ZigBee module.

VI. SYSTEM SOFTWARE DESIGN

ZigBee is a wireless transmission technology based on the IE802.15.4 standard specification[8]. It has the characteristics of self-organizing network, low cost, low power consumption, and enemy complexity [9]. It does not need to apply for authorization for the working frequency band, which is convenient and cost-effective to use. The system uses ZigBee to develop a set of wireless sensor networks according to the actual monitoring needs in the laboratory, and the data transmission between the nodes in the network is transmitted using the ZigBee protocol.

The laboratory monitoring system mainly includes terminal node coordinator, terminal node and routing node. The coordinator is responsible for forming a network, collecting data, and providing an interface with a computer to realize the formation of a sensor network and the establishment of a data transmission channel. The terminal node is responsible for collecting data information in the laboratory, including temperature, smoke, and harmful gases. These data are processed by the microcontroller, transmitted to the ZigBee network via the wireless network module, and finally transmitted to the coordinator, which is then transmitted to the monitoring center to realize the collection and transmission of laboratory environmental data. The routing node is responsible for the signal enhancement and forwarding of the data. Because the monitoring area is large, some data may be lost during the transmission process. To avoid this situation, a routing node is designed in the network to enhance and forward the data signal. , To ensure the stability and accuracy of data transmission throughout the network..

A. Terminal node design

1) Design of sensor data acquisition module

The system data acquisition module uses 51-microcontroller, through C language programming, to achieve sensor status and data acquisition, judgment and so on. These data are sent to the wireless network through the ZigBee module and transmitted to the coordinator. The flow chart of the sensor data acquisition module software design is shown in Figure 3.

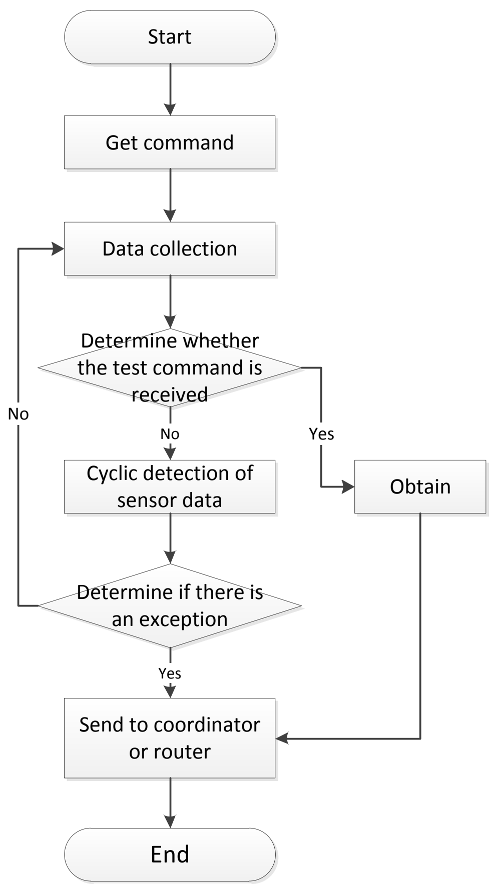

Figure 3. Software design flow chart of information collection module

After the data acquisition module software is running, it reads the background from the serial port of the ZigBee module to obtain background commands, collects the status of the sensors connected to the module, and sends the data to the network. If there is no background acquisition command, the program cyclically executes the acquisition sensor status command, and judges whether there is an abnormal situation in the laboratory through the sensor status data. If abnormal data appears, send laboratory status data to the monitoring center, and if there is no abnormality, continue to collect laboratory sensor data.

2) Wireless network module design

The information collected by each terminal node in this system is different. According to different sensors, multiple data will be collected within the scope of laboratory monitoring. In order to realize the data transmission in the system, it is necessary to establish a network and add these terminal nodes to it. In this system, the terminal node sends a request to join the network to the coordinator. The coordinator determines whether to allow joining according to the situation, responds to the request and sends it to the terminal node, so as to join the network and perform data transmission. The flow chart is shown in Figure 4.

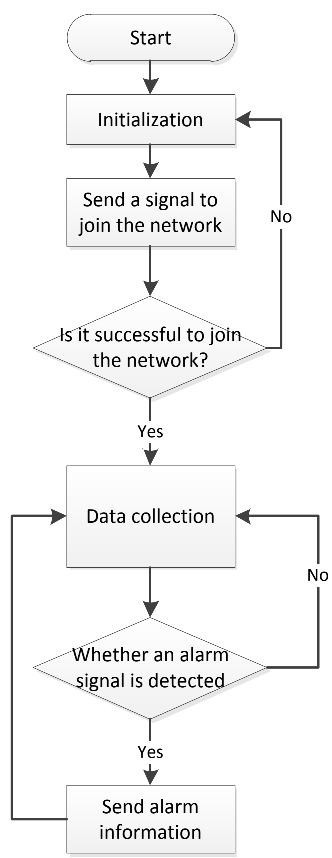

Figure 4. End node flow chart

The terminal node first finds the coordinator node in the network, and scans again if it is not found until it is found. Then send the association request command, wait for the coordinator to process, if you agree, then join the network, and get a short 16-bit address assigned, the terminal node sends data to the coordinator through the network.

B. *Coordinator node design*

The main role of the coordinator is to create the entire network and serve as a bridge between the terminal nodes and the control center. It needs to receive all kinds of data collected by terminal nodes and routing nodes through ZigBee wireless communication protocol, and then send it to the monitoring center. In the entire system, the coordinator must be a full-function device, and there can only be one coordinator node in a network, so the coordinator initialization setting is required at the time of design. The flow chart is shown in Figure 5.

The coordinator in the network is responsible for constructing the entire network, and adopts the method of ad hoc network to construct.

1) *Determine network coordinator*

The process is to determine whether the node is an FFD node, and then to determine whether the FFD node is in another network or whether a coordinator already exists in the network[9]. Through active scanning, send a beacon request command, and then set a T_scan_duration, if no beacon is detected within the scanning period, then it is considered that FFD does not have a coordinator in the entire network, it can build your own ZigBee network, and as this The network coordinator continuously generates beacons and broadcasts them.

2) *Carry out the channel scanning process*

It includes two processes: energy scanning and active scanning. First, perform energy detection on the specified channel or the default channel to avoid possible interference. Then carry out active scanning to search for network information within the communication radius of the node. This information is broadcast on the network in the form of beacon frames. The node obtains these beacon frames through active channel scanning, and then selects a suitable channel based on this information.

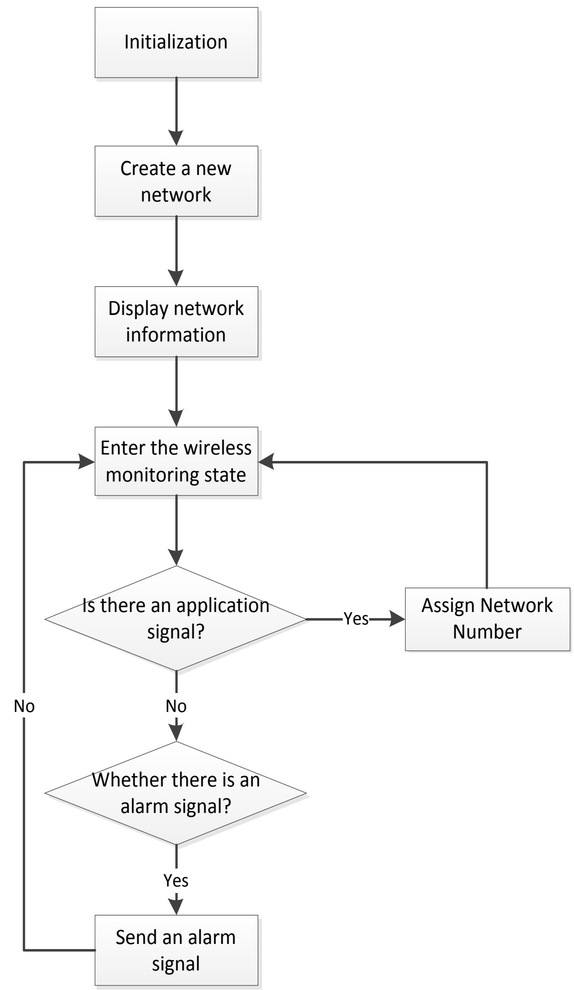

Figure 5. Coordinator node program flow chart

3) *Set the network ID*

After finding a suitable channel, the coordinator will select a network identifier (PAN ID) for the network. There are two address modes in the ZigBee network: extended address (64-bit) and short address (16-bit), where the extended address is assigned by the IEEE organization and is used for unique device identification.

After the above steps are completed, the ZigBee mesh network is successfully initialized, and then waits for other nodes to join. After the node successfully joins the network, it will get a short network address and send and receive data through this address. The flow chart of ad hoc network is shown in Figure 6.

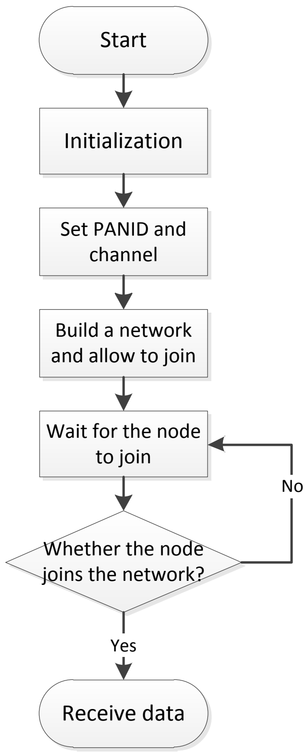

Figure 6. Coordinator ad hoc network flow chart

C. *Design of routing nodes*

As a relay node of the entire detection system, routing nodes are suitable for environmental monitoring in a large area. In wireless sensor networks, it may not be possible to connect and communicate because of the long distance between nodes. At this time, the routing node acts as a relay station to connect the terminal node and the coordinator. When setting up a routing node, you need to first initialize the CC2530 device and protocol stack, send a signal to join the network, the front-end coordinator will respond accordingly, agree to join the network, and assign a network address. After the routing node joins the network, it starts the function of data forwarding, thereby ensuring the transmission of data throughout the network. The program flow Figure 7 is shown.

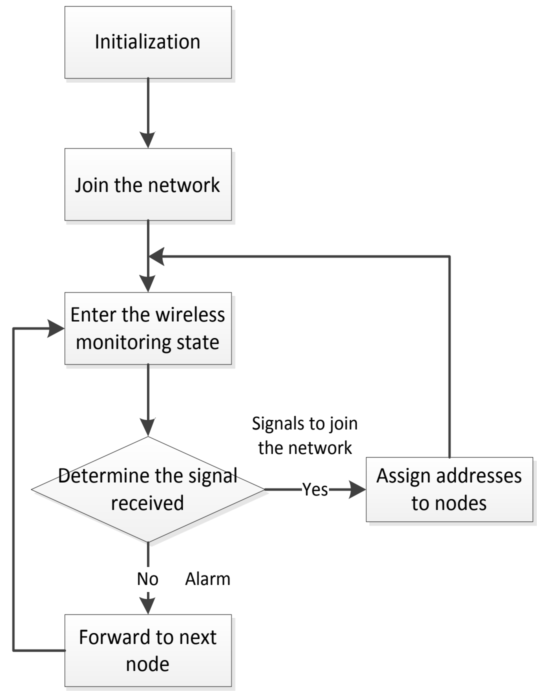

Figure 7. Routing node flow chart

VII. COMMUNICATION PROTOCOL DESIGN

Communication protocol refers to the rules and conventions that both entities must follow to complete communication or services. The protocol defines the format used by the data unit, the information and meaning that the information unit should contain, the connection method, and the timing of information transmission and reception, so as to ensure that the data in the network is smoothly transmitted to the determined place.

This system uses wireless communication, a specific communication rule designed for communication in the formulation of protocols. In the formulation of the transmission module protocol, according to the ZigBee communication protocol and the needs of the actual system, the communication protocol of this system was formulated. The single transmission format is shown in Table 1.

TABLE I. TRANSMISSION DATA FORMAT

FD	length	target address	Date 1	Date 2	Date 3	……..

FD indicates that ZigBee sends data point to point, and the length indicates the total length of the piece of data. This length can determine how many bits of data need to be read, which is convenient for taking out the data. The target address stores the ZigBee address of the received information. The following data 1 represents the laboratory number, data 2, 3, 4 and so on represent the data collected by the sensor. Each node sets different data according to its sensor.

The single data receiving format is shown in Table 2.

TABLE II. TRANSMISSION DATA FORMAT

FD	length	target address	Date 1	Date 2	Date 3	……..	Source address

FD means ZigBee point-to-point transmission. The length represents the total length of the data, and the target address represents the ZigBee address of the received message, that is, the node address to which the data needs to be sent. Data 1 represents the laboratory number. Data 2 represents the data information received by the sensor. Data 3 and data 4 are also the information received by the sensor. The amount of this information depends on the number of sensors at the terminal node. The source address represents the ZigBee address of the sent message, that is, from which node the message was received.

VIII. CONCLUSION

The laboratory security monitoring system mainly monitors the environment in the laboratory to alert the abnormal situation in time to avoid the economic loss caused by aging equipment or human negligence. The development of such a system has a positive effect on the laboratory construction of colleges and universities, and has certain application prospects.

REFERENCES

[1] ZHANG Hui YUAN Yong-zhe WANG Wen-jun "Security and intelligent system for buses based on mobile internet of things "Electronic Design Engineering. 2020, 28(9) 37-40.

[2] SUN Qi-bo LIU Jie LI Shan FAN Chun-xiao SUN Juan-juan" Internet of Things:Summarize on Concepts,Architecture and Key Technology Problem" JOURNAL OF BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS. 2010, 33(3).1-2.

[3] LIU Qiang CUI Li CHEN Hai-ming "Key Technologies and Applications of Internet of Things" COMPUTER SCIENCE. 2010, 37(6).1-4.

[4] HAN Tuanjun YIN Jiwu ZHANG Panfei ZHENG Xu ZHENG Zhengbing." Design of remote laboratory safety management system based on GPRS and Zigbee" Experimental Technology and Management. 2019, 36(11) 240-244.

[5] YAN Yaling LI Bo LIU Weijie." ZigBee-based Laboratory Fireproof Remote Monitoring System". 2019, 38(5) 282-285.

[6] Jiang Yunchen." Monitoring and managing system of laboratory based on campus LAN and ZigBee technology" EXPERIMENTAL TECHNOLOGY AND MANAGEMENT. 2010, 27(7).104-106.

[7] FAN Yan YU Yang LI Yong-yi DING Yi-xing "Research on Remote Monitoring System Based on ZigBee Wireless Sensor Network" Research and Exploration in Laboratory. 2016, 35(1).80-84.

[8] ZHANG Pan HUO Lian-song "Design of An Wireless Temperature Monitoring System Based on ZigBee" Sensor World. 2018, 24(8).23-27.

[9] WANG Sihua ZHENG Shuqiang DING Yihua "Discussion on ZigBee Sensor Network Technology and Its Application" Radio Engineering. 2020, 50(5).415-417.