Sensors & Transducers, Vol. 155, Issue 8, August 2013, pp. 107-114

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

Development Novel Organization Structure of Wireless Sensor Network Protocol Based on ZigBee Technology

[1] Zhen Liu, [2] Peng Ni, [1] Xiaoqin Ma, [1] Wenxian Xiao

[1] Network Information Center, Henan Institute of Science and Technology, Henan Xinxiang, 453003, China

[2] Luohe Medical College, Henan Luohe, 462002, China

[1] Tel.: 13613738850, fax: 0373—3693596

E-mail: liuzhenedu@163.com

Received: 13 May 2013 /Accepted: 12 August 2013 /Published: 20 August 2013

Abstract: ZigBee technology is a kind of two-way wireless communication technology in short distance, low complexity, low power consumption, low data rate, low cost, which is suitable for the automatic control and remote control. The wireless sensor network may be arranged in a hostile environment, in order to prevent the supply into the fake information to the network, need to realize the security of multicast source authentication based on wireless sensor network. Therefore, this paper presents implementation scheme of wireless sensor network technology 2.4 GHz ZigBee and 433 MHz combined. Each sensor node can be collected, simple computing environment data and to communicate with other nodes. The paper put forward development novel organization structure of wireless sensor network protocol based on ZigBee technology. The experimental results show that the terminal node has extremely low power consumption, long time work continuously, and this method has good self-organization, self-healing function. *Copyright © 2013 IFSA.*

Keywords: Wireless sensor network, ZigBee, Sensor nodes.

1. Introduction

As a result of computation, communication and sensor three technologies combined with wireless sensor network, is a novel technology about acquiring and processing information. Due to the improvement of recent micro manufacturing technology, communication technology and battery technology, ability makes tiny sensor has sensing, wireless communication and information processing. This kind of sensor not only can sense and detect the target object and environment change, and processing the data collected, and the processed data in wireless transmission mode to the data collection center or base station [1]. This tiny sensor is usually composed of sensor unit, data processing unit and communication unit, sensor, data processing unit and communication modules of tiny nodes through the self-organizing way constitute a network integrated random distribution.

As a newly emerging technology, wireless sensor network to establish a good, good robustness is still faced with many challenges. But due to some special characteristics, are very different design method of wireless sensor network and the existing wireless network. For example, since the sensor nodes in sensor network distribution is dense, so the data management and processing technology of large range. Secondly, the wireless sensor network node deployment in general human to reach and contact area is facing great challenges to maintain the sensor network node. In addition, the power consumption is a very important issue, wireless sensor node is a tiny device, with limited power, in some applications, replace the power supply is almost impossible.

ZigBee technology is a kind of two-way wireless communication technology in short distance, low complexity, low power consumption, low data rate, low cost, which is suitable for the automatic control and remote control, can be embedded in various devices, and supports for the geographical location. With respect to various wireless existing wireless communications technology, ZigBee technology will be the lowest power consumption and cost of technology. The ZigBee protocol is suite by the application of the application of high standards, convergence layer, network layer, data link layer and physical layer.

The data link layer and medium access control layer provides reliable communication channel for the neighbor nodes, in the MAC protocol, node to determine its ability to access communication channel by monitoring the neighbor node sends data. The carrier sense method is particularly vulnerable to denial of service attack is DOS. Methods using carrier sense in certain MAC layer protocol to neighboring nodes use the channel. When the channel conflict, nodes use a binary value index regression algorithm to determine the time to send data, conflict the attacker only needs to produce a byte can destroy the entire packet [2]. Because as long as part of the data conflict will cause the receiver to check data packets and do not match. In response to control information ACK receiver will send the data conflict sending node according to the binary exponential regression algorithm to choose the transmission time.

In wireless sensor networks, data processing by the node itself, the purpose is to reduce the amount of data transmitted in wireless links, only the relevant information with other nodes in the link transmission. Characteristics of data-centric is another feature of wireless sensor networks, because the nodes not planned in advance, but the node location is not determined in advance, so that there are some nodes due to the occurrence of many wrong or cannot carry out the specified task and stopped running. In order to monitor the target object in the network, configuration of redundant nodes is necessary, communication and collaboration, sharing of data between nodes that can, can guarantee to obtain the monitored object more comprehensive data. Wireless sensor network is a wireless network composed of a set of ZigBee nodes with Ad Hoc, its purpose is to perceive objects regional cooperative sensing, collecting and processing information in the network coverage, and released to the observer sensor, object perception and observation. The paper put forward development novel organization structure of wireless sensor network protocol based on ZigBee technology.

2. Structure of Wireless Sensor Network Protocol Analysis

Sensor network deployment of large-scale networks in complex environment, real-time data acquisition and processing brings hope. But at the same time, WSN is usually deployed in unattended maintenance, can not control the environment, besides the general wireless network facing the information disclosure, information tampering, replay attack, denial of service and other threats, WSN faces the sensor node easy for an attacker to physical manipulation, and get all the information stored in the sensor node, so as to control the part of the network threat. The user can not be accepted and deployed without a sensor network to solve the security and privacy issues, so in the WSN protocol and software design, should fully consider the security problem of WSN may face, and the safety mechanism is integrated into the system design. Only in this way, can promote the extensive application of sensor networks, otherwise, can only be deployed in Sensor Network Limited, controlled environments, the ultimate aim and sensor networks -- to achieve universal computing and become an important way of people's life is contrary.

The data link layer in the protocol stack usually provides two main services: media access control (MAC) and error control [3]. In a variety of MAC, carrier senses multiple accesses (CSMA) in ad-hoc sensor networks are the most commonly used. This is mainly because it is easy to implement, but more important is that it can improve the rate of channel multiplexing large network.

Wireless sensor nodes by multi-hop forwarding, through the access network gateway node, management, classification, processing of sensory information in the task manager node network, then the sensing information to the application user. Sensor nodes first acquisition such as sound, light and distance environment related data, and these data are sent to the gateway node simple processing. Wireless sensor networks usually have two kinds of application modes: active polling mode, passive mode. Active mode requires the gateway node active polling for each sensor nodes to get the news, while passive mode requires that in the event of a sensor node occurs, the gateway node can be timely response. Each sensor node data can be combined, which greatly improves the efficiency of sensor network. Of course, this also requires sensor nodes to computing ability, as is shown by equation 1.

$$\begin{aligned}\mu_{s|a} &= E\{s(k) \mid a(k)\} \\ &= \mathrm{M}^{-1}\{\beta(k)^{\mathrm{T}}\Sigma_{\varepsilon(k)}^{-1}\left(a(k)-\alpha(k)\right)+\frac{s_0(k)}{\sigma_{s(k)}^2}\}\end{aligned} \quad (1)$$

In view of the environment and structure state monitoring, we design a universal wireless sensor network hardware platform; the hardware platform is composed of a number of sensor nodes, Sink nodes with wireless receiving function and a computer. Wireless sensor nodes distributed in the monitoring area, performing data acquisition, processing and wireless communication, Sink node receives the sensor data to the wired way and sends the data to the computer.

The design goal of traditional MAC protocol is to maximize throughput, minimize the delay and fairness. About MAC layer protocol for WSNs design is to minimize the energy consumption, which determines that it should be appropriate to reduce the throughput and delay. Because the WSNs node always cooperates to complete an application task, so the usual fairness is not the main problem. In addition, some typical WSNs application also proposed is different from traditional wireless network design requirements for the MAC layer protocol.

Integrated circuits, micro electromechanical systems and the development of communication theory led to the emergence of wireless sensor networks [4]. This wireless sensor network is composed of many sensor nodes self-powered. Each sensor node can be collected, simple computing environment data and to communicate with other nodes and the outside world. The sensor node characteristics of sensor networks make many sensors can be made of high quality through collaborative work, and consists of a collection of good fault tolerance of the system. It is because of these advantages, in recent years there have been many wireless sensor network applications based on distributed detection and rescue, emergency rescue and disaster relief, intelligent home furnishing such as chemical and biological weapons attacks, as is shown by equation 2.

$$\hat{f}_n = f(u_n) = f[\sum_{k=1}^{K} w_k \sum_{m=1}^{M} x_m \psi(\frac{x_m - b_k}{a_k})] \quad (2)$$

The use of radio frequency module, there are two problems to be paid attention to: the first is when the transmission is completed, must send the enable pin and transmit data pin is set to low level. Otherwise one will consume energy, on the other hand, the RF module will always send a single carrier frequency signal, the disturbance to the surrounding nodes work; second is the wireless transmission module to transmit state from the standby state, there are about 20 s between the delay. In the meantime, input module data cannot be sent correctly, so ready to send before, should be sent to set high in advance.

Wireless ad hoc networks (mobile Ad-Hoc network) are a kind of tens to hundreds of nodes by multi-hop, mobile wireless communication network, dynamic peer-to-peer network. Its purpose is to through dynamic routing and mobility management technology, multimedia information transmission with quality of service requirements flow. Usually the node with energy supply continued. Wireless sensor networks with wireless ad hoc networks have similarities, but there is great difference. Sensor network is integration of the monitoring, control and wireless communication network system, the number of nodes is large, a network with thousands or even tens of thousands of node; node distribution is more intensive; due to the depletion of environmental impact and energy, nodes are more prone to failure; environmental interference and node failure caused by the change of the network topology; in general, most of the network node is fixed.

The majority of distributed MAC protocol uses carrier sense or collision avoidance mechanism and the use of additional signaling information to solve the hidden and exposed node problem. Competition is a random access MAC protocol based on nodes need to transmit data, using the wireless channel by means of competition. IEEE802.11 MAC protocol based on Carrier Sense Multiple Access with collision avoidance (Carrier Sensor Multiple Access with Collision Avoidance, CSMA/CA) is based on MAC protocol is a typical competition. Based on IEEES02.11 MAC protocol, the researchers put forward many sensors for sensor network contention based MAC protocol, S-MAC protocol, T-MAC protocol: for example, ARC-MAC protocol, Sift-MAC protocol, Wise-MAC protocol [5].

$$J_M R^* J_M (w_b^B)^* = J_M r_b^* = r_f = R w_f \quad (3)$$

Wireless sensor network architecture consists of three main parts: the sensor node, terminal node (Sink) and object of observation. Sensor nodes scattered collection and observation of the object of related data observed in the region, and after coordination to deal with data transfer to Sink. Sink can realize the communication of sensor network node and task management through Internet or a communications satellite.

The network layer is responsible for routing lookup and packet transmission. Since a large number of nodes in a sensor network deployment group are random, so look at the mesh network of multi-hop routing is very difficult, when the node failure or redeployment route maintenance and repair (self-healing) will be equally difficult. In the past few years there has been a large number of can support distributed routing algorithm for ad hoc mullion network. In general, these routing algorithms can be divided into two categories: active (proactive) and passive (reactive). In a proactive routing protocol, all nodes in the network are often maintained a route between the source address and destination address list, regardless of the need of these routing.

$$\sigma_\Omega^2 = \frac{1}{A_\Omega} \sum_{(x,y)\in\Omega} [(I(x,y) - \bar{I}_\Omega]^2 \quad (4)$$

Wireless sensor network consists of a large number of sensor nodes and a base station (BS), the base station node communication with other network access, environment monitoring sensor node and will collect the data to the base station. However, its limited energy, directly transmit the data to the base station will consume a lot of energy (Fig. 1). The routing method for multi-hop is not ideal, because the nodes closest to the base station will soon die for routing a received data, resulting in the later arrival

data cannot be passed to the base station. Routing method of other nodes in the PEGASIS, only with communication neighbor nodes, nodes take turns sending the fusion data to BS, ant colony algorithm considering the energy of each node in the route to choose the shortest path at the same time, based on consumption, so as to select the path more appropriate.

The hardware part of the gateway mainly consists of a central processing unit, a storage unit, frequency transceiver module and GPRS communication module, as shown in Fig. 1. The central processing unit of gateway is mainly used to treat from the data collected by sensors and finish some control function. The central processing unit of function realization is still using FPGA in Alter Cyclone series and NIOS soft core embedded processor [6]. This design makes it can complete some functions of rich applications in low cost, low power conditions. In addition, it can be integrated many peripheral interface, USB2.0 interface and Ethernet interface.

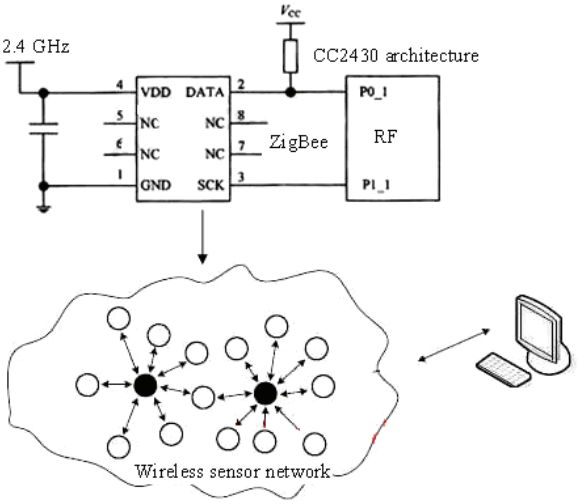

Fig. 1. The structure of Wireless sensor network based on CC2430 of ZigBee.

Wireless sensor network information with the external network or terminal connection between the need to achieve through the Sink node, Sink node is the wireless sensor network and cable connection, is responsible for sending the command (such as query, ID address allocation etc.), lower nodes receive requests and data, with data fusion, request the arbitration and the routing function, is one of the most important parts in wireless sensor networks. We design a Sink node with USB data and RS232 data, two kinds of data can be switched by a switch, for easy connection to the Sink and the external network or between terminals.

The basic features of WSN are energy limited. The MAC protocol as much as possible to save energy, such as reducing conflict and crosstalk, reduce the duty cycle and avoid long distance communication. The agreement shall also include the compromise mechanism, the user can improve the throughput, lower delay in energy saving and make a choice between. In addition, protocol designers should pay attention to energy is not readily available. Node is in a sleep state or the cause of death unknown.

The specific page programming operation is as follows: Command stage, to I/O port to send the page programming operation of the first command word (Ox80), said is page programming operation. The address phase, continuous send 4 address, K9Fl208 address register receives the address value, waiting to receive the data; when the data bus to send data, receive data until receiving continuous K9F1208, page second programming command word (0x10), that is the end of waiting to receive data state; R/B signal will remain "busy" for a period of time, then R/B is ready. The last bus issues a read status command word (Ox70), the K9F1208 command register to receive and respond to the command, said state data operation successfully to I/O port to send (Ox00) or said state data operation failure (OxO1), as is shown by equation 5.

$$f(x) = \frac{1}{nh^d} \sum_{i=1}^{n} K(\frac{x - x_i}{h}) \tag{5}$$

Nodes are battery-powered, the battery energy Co., and nodes may work in the inaccessible region, inconvenience frequent replacement battery. So in the design, energy conservation is the need to give priority to a problem [7]. First of all, SCM should perform tasks with the fastest speed, once it is possible to enter power saving mode. In the energy-saving mode, through the management circuit, will cut off the power supply device in addition to outside of the mcu. Enter power saving mode, if the monitoring center needs to access the node, through the RF transceiver module to awaken the node MCU.

Sensor nodes first acquisition such as sound, light and distance environment related data, and these data are sent to the gateway node simple processing. Wireless sensor networks usually have two kinds of application modes: active polling mode, passive mode. Active mode requires the gateway node active polling for each sensor nodes to get the news, while passive mode requires that in the event of a sensor node occurs; the gateway node can make timely response. Each sensor node data can be combined, which greatly improves the efficiency of sensor network. Of course, this also requires sensor nodes to computing ability.

Since the communication module to transmit power of wireless sensor nodes, nodes and the duty ratio is very small, a lot of data cannot be transmitted out at the same time, so it is necessary to have a manageable memory for storing the data collected, temporary or need other nodes forwarding the data collection. The 512 KB serial FLASHAT45DB041

data stored in this design. Compared with the common data memory, the chip has the characteristics of low power consumption, small volume, serial interface; the external circuit is simple, suitable for sensor nodes.

Two kinds of special security protocol in Wireless Sensor Networks: encryption protocol SNEP security network (Sensor Network Encryption Protocol) and stream authentication protocol time efficient tolerate packet loss based on TESLA. The function of SNEP is to provide node to receiver data authentication, encryption, refresh, TESLA is the function of broadcasting data authentication. Because wireless sensor networks may be arranged in a hostile environment, in order to prevent the supply into the fake information to the network, need to realize the security of multicast source authentication based on wireless sensor network [8]. But because of the wireless sensor networks, can not use public key cryptosystem, so multicast source authentication is not easy to realize. Security protocols for sensor network SP INK gives uTESL A multicast source authentication based on, the scheme is the improvement of the TESLA protocol, which is suitable for sensor networks.

Usually, in wireless sensor networks, a large number of sensor nodes are densely distributed in an area, the message may be required after a certain number of nodes to reach the destination, but also due to the dynamic nature of the sensor network, so there is no fixed infrastructure, so each node needs to have routing function. Since each node is a potential routing node, and therefore more vulnerable to attack. The main attack types of wireless sensor network.

$$\mu_{s_0} = E_{\hat{k}}\{s_0(\hat{k})\} = \sum_{\hat{k}\in\mathcal{R}_{\hat{k}}} p(\hat{k}) s_0(\hat{k}) \qquad (6)$$

Distributed routing algorithm for mobile ad hoc networks most are using and the development of mesh network, network structure based on the plane, and whether it is active or passive routing. Since the network is not stratified, each node acts as a relay of other nodes, which bear the responsibility of the same. In this flat network using full distributed routing algorithm, all nodes are not transmitted must actively monitor channel, in order to realize the relay. Therefore, power distributed routing algorithm in mesh networks have higher. Use of a star - mesh mixed structure can develop an intelligent routing, achieve high efficiency, reduce delay and enhanced connectivity.

Due to the limited routing list storage space each sensor, the passive routing can provide more compact solutions for sensor network applications. The transmission of information is to serve as a small number of nodes data collection station, which can effectively solve the time delay problem of passive routing. Each central station for communication information is collecting adjacent regions.

3. Research of Wireless Sensor Network Protocol Based on ZigBee Technology

Wireless sensor network is a computer network arises independently, its basic unit is a node, and the node integrates sensor, microprocessor, wireless interface and power module four. Computer network technology in the traditional industry has a mature solution could be used in wireless sensor networks. But the uses and advantages of wireless sensor network based on the development of special, communication protocol and routing algorithm has become a subject of urgent research in the field of the wireless sensor network.

ZigBee supports the star network; peer-to-peer network and hybrid network 3 network topology structures. Fig. 2 is a hybrid ZigBee network. Each network has its own advantages. A star network with a powerful master device is as the network center, responsible for the coordination of the whole net work and it is the master device other or from the devices in their coverage range [9]. The network control and synchronization are relatively simple, suitable for relatively few occasions' equipment quantity. Peer-to-peer network is divided into point to point and cluster tree 2, is composed of a main device connected to the. This network can provide higher reliability. Star network and peer-to-peer network is formed by the combination of the hybrid network, subnet to star connection, the main devices in a peer-to-peer manner. The network application is complex on the network request. General in the real application environment, mixed type has more practicability.

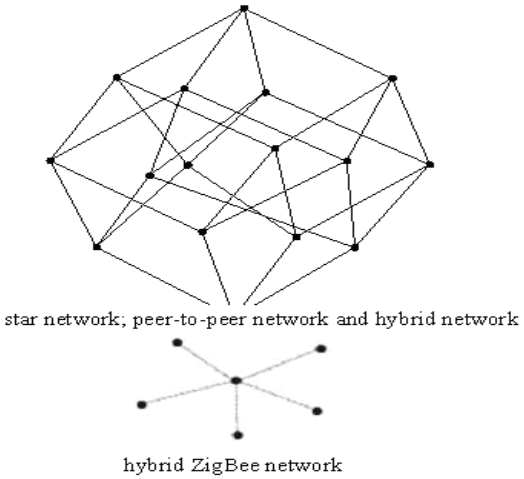

Fig. 2. The hybrid ZigBee network figure.

We design node implementation mechanism is serial communication module based on ZigBee transmission module to replace the traditional, the information collected data wirelessly sends out. The node that contains the ZigBee wireless transmission module, microcontroller module, and it is the sensor module and interface circuit, DC power supply

module and an external memory. In order to reduce the cost of sensor node, to reduce the volume of sensor nodes, data transmission and processing of our company introduced the use of highly integrated SoC chip CC2430 to realize the sensor node.

Mainly for K9F1208 to operate the page read and page programming operation. Fig. 2 is a standard page NAND Flash read timing diagram. The page read operation is as follows: Command stage, in the chip select signal CE effective, first command allows signal CLE effectively, the write signal WE, chip ready signal R/B is set high, says ready; and sending a read operation command to the I/O port (0xOO or OxO1), that is the read operation. The address phase and, at this time chip select effective, effective address enable signal ALE, the write signal WE remain effective, continuous send 4 address; K9F1208 address register receives the address value, the R/B signal will remain "busy" for a period of time, then R/B is ready [10]. The last is the data output stage, each read effective signal is asserted low effective, will output a set of data. And so on until the entire data output end, as is shown by equation 7.

$$P_{LP}(\theta)=\frac{1}{\left|G_{LP}\right|^2}=\frac{1}{\left|a^H(\theta)W\right|^2} \tag{7}$$

ZigBee technology adopts IEEE 802.15.4-2003 standards of physical layer and media access control layer as ZigBee physical layer and media access control layer, ZigBee alliance in the provisions of the framework of network layer and application layer; ZigBee technology has powerful function of the equipment of the Internet, he supported the star structure (Star), reticular formation (Mesh) and cluster (Tree) three kinds of self-organizing wireless network type, especially the network, he has the reliability of network robustness, strong.

From the point of view of maintaining routing security angle, find the safest possible route to ensure the security of network. If the routing protocol is damaged, transmitted message tampering, so no security at all for any application layer packet. This paper introduces a method called "have senses of security routing" (SAR), the idea is to find out the relationship between the real values and node, and then use the true value to generate a secure routing. The method to solve two problems and it is namely how to ensure the information security of data transmission in the safety path and routing protocol in WSN.

CC2430 is the first to comply with the ZigBee standard 2.4 GHz single chip (System On Chip, SOC), a wireless network node is suitable for various ZigBee or similar to the ZigBee, including the coordinator, router and terminal node, chip using the previous CC2430 architecture, in a single chip integrated ZigBee radio frequency (RF) transceiver, memory and the micro controller, in sleep mode, the whole chip flow consumption is less than 0.5 μ A, integrated timer and a lot of resources on chip.

The MAC layer: follow the IEEE 802.15.4 protocol for wireless, wireless data link between the equipment establishment, maintenance and end of pattern recognition, data transmission and reception, optional slot, low transmission delay, support a variety of network topology, network of each device for a 16 bit address addressing. The network layer: the establishment of a new network, the processing nodes enter and leave the network, according to the arrangement of nodes of the network type of protocol stack, the network coordinator node distribution of address, to ensure synchronization between nodes, network routing, ensure the integrity of the data, use the optional AES-128 for communication encryption, as is shown by equation 8.

$$I_\sigma(i,j)=\sigma_{\Omega_{ij}},\ \Omega_{ij}=\{(i-1)l+1\le x<il,\ (j-1)l+1\le y<jl\} \tag{8}$$

In most sensor network deployment, the network topology is unpredictable, and after deployment, role in the network topology of the whole network, sensor nodes are constantly changing, so unlike the wired network, wireless network that most of the network equipment configuration fully, pre configuration of sensor node is limited in scope, a lot of network parameters, key are formed of sensor nodes in the deployment after consultations.

In the system of larger and more complex (such as a manufacturing site), the central point of control is likely to exceed the coverage of ZigBee network, and may even be placed in another building. So, the PAN coordinator may be required for communication with a central control point through the cable connection [11]. Because the application of Ethernet in the industrial market is more and more popular, so in most cases, Ethernet is the most likely choice. Application of Ethernet has two potential implications for network design: one is to consider the required processing Ethernet interface processor bandwidth; two is to drive the Ethernet interface, the network will need the corresponding driver and protocol stack, which increase the system PAN controller needs of program memory.

4. Development Novel Organization Structure of Wireless Sensor Network Protocol by ZigBee

Sensor network is used to collect the information as the main objective; the attacker can obtain this sensitive information by eavesdropping, added illegal node forged mode, if the attacker knows how to get the related algorithm limited information from multiples information, then the attacker can be derived through the massive effective information acquisition information. The issues of private general

sensors, and not through the sensor network to obtain is unlikely to be collected information, but the attacker through remote monitoring WSN, resulting in a large number of information, and according to the specific algorithm analysis problems of the private. So the attacker does not require physical contact sensor nodes, is a low risk, anonymous access private information. Transmission of remote monitor can also make a single attacker access to multiple nodes information.

The central control center is connected with multiple sink nodes through the network, between the sink node and sensor nodes exchange information through the wireless ZigBee technology, wireless sensor nodes with a radio transceiver is responsible for sensing and processing and transmission of data to the sink node; information control center through the network to obtain the collected, realize the effective control and management on the scene.

The sink node distribution in sensor network is mainly used for reporting receiving sensor data, and the fusion processing, to the transmission module of wireless communication data, transmitted to the central control center through the network information [12]. A connection between ZigBee module and MCU through asynchronous serial port to realize the communication between them, the speed is 95.4 kB / s, MCU completes the communication the sink node and central control center control module, the sensor network in the distribution of multiple sink nodes, so a 32 bit MCU to use software interrupt for ID the sink node to upload data to the sink node polling scanning, data can be orderly, complete by MCU treatment after. As the sink nodes in sensor networks is the gateway between the sensor nodes and the network.

$$\rho(y) \equiv \rho[\hat{p}(y), \hat{q}(y_0)] = \sum_{b=1}^{m} \sqrt{\hat{p}_b(y)\hat{q}_b(y_0)} \quad (9)$$

Although the ZigBee technology is the ideal solution for wireless sensor networks, but in the actual engineering application also has the side of his lack of it. The use of ZigBee in the global range of frequency is 2.5 GHz, which belongs to the category of the characteristics of microwave, high frequency, wavelength is short, straight line, in the direction of propagation is almost not open around the obstacle, the transmit power and frequency on the ZigBee node is very low, which causes, ZigBee wireless signals PENETRATE obstacles capability is very limited. Although can be increased through the arrangement of ZigBee routing nodes to steer clear of obstacles, but this will increase the capacity of the network and network costs, and some places are not allowed to assign a network node. Therefore, this paper presents implementation scheme of wireless sensor network technology 2.4 GHz ZigBee and 433 MHz combined.

Developed a ZigBee to Ethernet module, this module is mainly through the TCP / IP protocol and uploaded to the Internet using ZigBee wireless sensor network to collect information, whether you live in that corner of the world, are available through ZigBee to Ethernet module for remote real-time monitoring. Can also through the GSM network, the system adopts TC35 as data transmission terminal, can transmit data in sensor networks quickly, reliably. Use MSP430MCU to control the TC35 module to complete the communication of the sink node and the central control center.

Wireless sensor network based on ZigBee has the advantages of low power consumption, low cost, small size, can realize the acquisition and processing the monitoring region signal in special environment. With the proposed self-organizing wireless network technology mature and new energy solutions, the application of wireless sensor networks in various areas of the life.

Modular design of various nodes in the system hardware, the ZigBee module object such as shown in Fig. 3 on the left, the CC1200 module as shown in Fig. 3 as shown in the right. The compact and reasonable is structure and small volume. In the sunny weather conditions in the open area, effective communication distance is measured between the 120 ZigBee node m, the effective transmission distance of up to 433 MHz RF module 400 m; working under laboratory conditions, ZigBee wireless signals can penetrate 1 concrete wall, 433 MHz RF signal can penetrate 4 concrete wall, effectively to overcome the 2.5 GHz RF signal penetrable weakness. In the power supply circuit of ZigBee terminal nodes connected in series 2 resistor with an oscilloscope connected, measured in the working process of the terminal node.

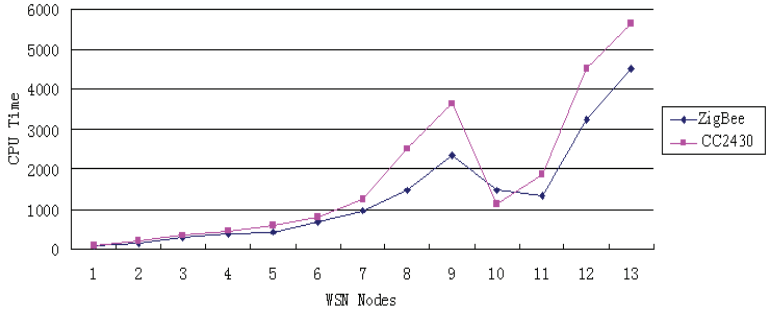

Fig. 3. Comparison organization structure of wireless sensor network protocol based on ZigBee with CC2430.

The Linux open-source is operating system. Linux is a network operating system environment, especially suitable for network application. Linux is a complete TCP/IP protocol stack, while supporting various network protocols, such as PPP protocol stack, making it easy to implement the GPRS dial function. Because the Linux open source, users can easily on the basis of the development of their applications.

The coordinator through 433 MHz RF, send the data to the concentrator, and eventually to management database. The ZigBee terminal nodes move far away, beyond the ZigBee network coverage, returned to the network coverage, can continue to work; close the router R1, again after the opening, the terminal node E2, E3 still can send data to the coordinator through R1; close the router R1, as long as the E2 the coordinator, E3 C visual range, E2, E3 can directly send data to the coordinator. The above results validated the ZigBee wireless network self-organization and self-healing characteristics of good.

6. Conclusions

Future sensor networks generally have hundreds of thousands of sensor nodes, it is difficult to monitor and protection on each node, and each node is a potential point of attack, can be an attacker to physical and logical attack. In addition, the sensors are usually deployed in unattended maintenance environment, it is more convenient for attackers to capture sensor node. The paper put forward development novel organization structure of wireless sensor network protocol based on ZigBee technology. In this paper, based on the ZigBee wireless network communication technology and 433 MHz radio communication technology is to realize the wireless sensor network. The experimental results show that, the terminal node has extremely low power consumption; long time the whole network can work continuously and stably, and has good self-organization, self-healing function.

References

[1]. Wang Guohong, He You, Yang Zhi, et al., Adaptive sensor management in multisensor data fusion systems, *Chinese Journal of Electronics,* 27, 2, 1999, pp. 125-132.

[2]. Hintz Kenneth J., McIntyre, Greg, Goal lattices for sensor management, in *Proceedings of the Signal Processing, Sensor Fusion, and Target Recognition VIII,* Orlando, FL, USA, SPIE, Vol. 3365, 1999, pp. 249-255.

[3]. Jiang Yi, Li Jianping, Xiong Anping, Certificateless Aggregate Signcryption Scheme for Wireless Sensor Network, *IJACT,* Vol. 5, No. 8, 2013, pp. 456 - 463.

[4]. Jiping Li, Shouyin Liu, Shixun Wu, A Design of Remote Computer House Monitoring and Control System Based on ZigBee WSN, *IJACT,* Vol. 4, No. 12, 2012, pp. 233 - 240.

[5]. L. Yan, B. Liu and D. Zhou, The modeling and estimation of asynchronous multirate multisensor dynamic systems, *Aerospace Science and Technology,* 10, 1, 2006, pp. 63-71.

[6]. Tan Li, Yang Minghua, Yu Chongchong, Li Xuanya, Cheng Bin, A Coverage Gap Filling Algorithm in Hybrid Sensor Network, *IJACT,* Vol. 4, No. 4, 2012, pp. 192 - 198.

[7]. Meiqian Ye, Tianding Chen, Changhong Yu, ZigBee-based Positioning and Navigation System for Robot, *JCIT,* Vol. 6, No. 1, 2011, pp. 135 - 146.

[8]. Wang Guohong, He You, Yang Zhi, et al., Adaptive sensor management in multisensor data fusion systems, *Chinese Journal of Electronics*, 27, 2, 1999, pp. 125-132.

[9]. Qian Xiao, Kangfeng Zheng, Shoushan Luo, Yixian Yang, Ling Zhang, An Efficient Algorithm for Time-Driven Data Gathering in Wireless Sensor Networks Using Inter-Session Network Coding, *JCIT,* Vol. 7, No. 1, 2012, pp. 11 - 18.

[10]. Guisong Yang, Zhongjie Wang, Chunxue Wu, Binjie Xiao, Hegang Dong, One-hop Expansion ETR Protocol for Wireless Sensor Networks, *JCIT,* Vol. 7, No. 11, 2012, pp. 169 - 178.

[11]. Zhang Chong-Quan, Zhang Li-Yong, Yang Su-Ying, etc., A Weighted Fusion Algorithm of Multi-sensor Based on the Principle of Least Squares, *Chinese Journal of Scientific Instrument,* 24, 4, 2003, pp. 427-430.

[12]. Jian Hu, Haixi Wu, Shuguang Ye, Ling Li, Gangyan Li, Research and Implementation of Taxi Calling-Response Method based on ZigBee, *JDCTA,* Vol. 5, No. 8, 2011, pp. 92 - 100.