An Interference Avoidance Strategy for Zigbee Based WeHealth Monitoring System

Lichen Lee†, Guixia Kang*, Xidong Zhang‡, Xiangyi Li, Longfeng Chen
Key Laboratory of Universal Wireless Communications, Ministry of Education
Wireless Technology Innovation Institute (WTI), Beijing University of Posts and Telecommunications
Beijing, P. R. China, 100876
email:†lichenlee1987@gmail.com, *gxkang@bupt.edu.cn, ‡st0rm@bupt.edu.cn

***Abstract*—With the unprecedented aging of population, chronic disease become a serious problem in modern medical area. Recent advances of wireless technology make the health monitoring in home to be more convenient for the chronic disease. Reducing the influence of the interference from the other wireless equipment is one of the most important problems in wireless physical parameter monitoring device in healthcare field, as reliable data transmitting is vital in medical care. In this paper, we propose a novel interference avoidance strategy that can greatly reduce the influence of the interference from other wireless equipment to wireless physical parameter monitoring devices in the hospital or home environment. Experimental results show that the strategy has good effect on interference avoidance and reduce the package loss rate.**

***Index Terms*—Interference Avoidance, Zigbee, health monitoring**

I. Introduction

The proportion of aging people in today's total population grows rapidly with the growing extent of aging society. It is assumed that the number of aging people (people whose age is larger than or equal to 60) would exceed youngsters for the first time in human history in 2050[1]. Chronic diseases such as hypertension, high cholesterol, and high blood sugar are typical threatening for elderly. However, the morbidity of these diseases is unpredictable so far as they have no regularity. For this reason, the elderly need long time nursing. Current social healthcare resources such as hospitals and nursing home are far from meeting the need of elderly with chronic diseases. Thanks to the development of the technology of Internet of Things (IoT), the Wireless electronic Healthcare (WeHealth) has been widely applied in the field of healthcare. In WeHealth system, the sensors that are worn on human body to acquire physical parameters form a Wireless Sensor Network (WSN), they have low power consumption and they can help doctors to watch the physical condition of several patients remotely at same time. It has greatly enhanced the efficiency of elderly nursing [1].

As a typical WSN standard, Zigbee has been widely followed by devices used in WeHealth system. Those devices work in the 2.4GHz unlicensed Industrial, Scientific and Medical (ISM) band, coexisting with other wireless equipment such as WiFi, WLAN, whose transmitting power are usually much larger than WeHealth devices. Furthermore, reliable data transmitting is vital in WeHealth as the precision of medical data is extremely important in the field of healthcare. For this reason, how to reduce the influence of the interference from the other wireless equipment has become a problem that must be considered in WeHealth.

There are many researches on the interference between Zigbee and WiFi/WLAN. The existing solution for interference problem can be divided into two categories, collaborative approach and non- collaborative approach. In the former approach, a central controller is used, who can monitor the distribution of Zigbee and WiFi signal, and arrange certain time slot for each type of signal according to some algorithms. [1] proposed a WiFi and Zigbee collaborative mechanism which is a typical collaborative approach. These approaches have good effect on in-system interference, but they can do nothing to the out-system interference. The non-collaborative approaches base on the channel detection and performance measurements, including packets received ratio measurements, bit or frame error rate, signal strength or signal to interference ratio to detect the presence of WiFi interference. And the interference avoidance algorithms consist of transmission power control, adjusting packet length and dynamic channel allocation. Transmission power control has little effect because transmission power of WiFi is extremely greater than that of Zigbee. Adaptive packet length selection based on channel condition is also a mechanism, but [4] shows that it does not always result in better PER performance. The method of dynamic channel allocation makes WiFi and Zigbee work in non-overlapping frequency. Kang [5] proposed a Pseudo Random Sequence Generator to select the aimed channel. Zigbee nodes need not to exchange the channel information, but may not adjust to the none-interference channel. Yuan [6] also proposed an interference-avoidance algorithm which change the channel with a interval of 4 channels. This may performs badly when the situation of WiFi interference is complex.

In this paper we firstly study the performance of WeHealth monitoring system through a set of experiments, and then we propose a WiFi avoidance mechanism applied to WeHealth monitoring system. The rest paper is arranged as follows: in section II we will briefly introduce the WeHealth monitoring system and an analysis of the impact of WiFi interference on our system will be given. In section III, we will give a set of experiments to measure the impact of WiFi interference.

978-1-4577-2040-6/12/$26.00 ©2012 IEEE

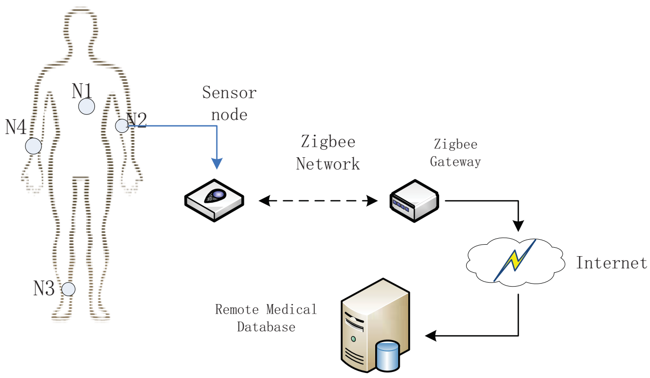

Fig. 1. Architecture of the WeHealth monitoring system

The avoidance strategy is proposed in section IV and a corresponding evaluation test is in section V. Section VI contains our conclusions.

II. WeHealth Monitoring System and Interference Problem

A. Architecture of WeHealth monitoring system

Figure 1 shows the typical architecture of the WeHealth monitoring system in family environment. Patients being monitored wear a set of medical sensors collecting different physiological signals, mainly including blood pressure, blood oxygen, blood glucose levels, heart rate and electrocardiogram. The physiological signals collected by the medical sensors will be sent to the Zigbee gateway through the configured Zigbee module. In this system, Zigbee star topology is selected by the system. The sensors are equipped with a Zigbee reduced function device which will send the collected data directly to the coordinator (Zigbee gateway in the figure). The Zigbee coordinator provides primary judgment of the physiological signals to detect the signals outside the health range (emergency signals) and provides the interface as a gateway between a Zigbee network and other networks, such as the Internet. The patient's physiological information is then transmitted over the Internet to remote medical database. The physician or the nurse can access the database to observe the physiological indicators of the patient and give the correct advice in time.

There are two modes for the sensors to transmit the physiological data, normal monitoring mode and emergency monitoring mode. Sensors collect the physiological signals periodically and transmit the data by access the Zigbee channel using Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) in the normal monitoring mode. When the coordinator detects the emergency signals, it will notify the sensor nodes to enter the emergency mode. In the emergency mode, the sensor nodes will collect required emergency signals with a higher frequency and transmit data with the Guaranteed Time Slot (GTS) which is a mechanism in the IEEE 802.15.4 MAC layer [7]. Sensors can access the channel without CSMA-CA and the data rate will be higher than that with CSMA-CA. The superframe for the WeHealth system is shown in Figure 2.

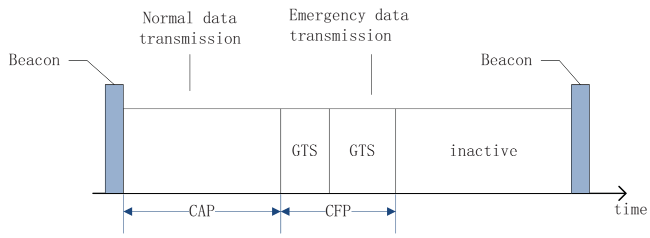

Fig. 2. Superframe of the WeHealth monitoring system

B. Analysis of the impact of WiFi interference

The accuracy and real-time feature are vital for the transmission of physiological signals. The interference will lead to great packet error rate (PER) ,the retransmission of the data and the transmission delay which will greatly reduce the quality of medical service.

Zigbee use IEEE 802.15.4 as the physical and MAC layers. IEEE 802.15.4 define 16 channels in the 2.4G ISM band , where one Zigbee channel occupies 3MHz bandwidth with the channel spacing of 5MHz. Channels are all none-overlapping channels with a 2MHz protected bandwidth. In the MAC layer, when sensor want to access the channel, it firstly estimate the channel with twice Clear Channel Assessment (CCA), if the channel is idle, the sensor can access the channel and send data. The WiFi channel which occupies 22MHz bandwidth will overlap 4 channels of Zigbee channels, so the 4 overlapping channels may suffer the WiFi interference theoretically.

The impact of the WiFi interference is different at the Zigbee sender and the receiver. Because the transmission power is far greater than that of Zigbee, the WiFi cannot sense the Zigbee signals occupying the channel in most situations. When WiFi is transmitting data in the overlapping channel, the CCA mechanism of Zigbee will always sense busy which cause the channel accessing failure of the Zigbee transmitter. As to the receiver node, because the WiFi device cannot sense Zigbee signal, data collision may occur even when transmitter transmit data successfully. If the signal to interference ratio is not great enough, packets will be error and be discarded.

III. Experimental Modeling of Interference from WiFi Signal

In this section, we will introduce the experiment tests which are used to study the transmission performance of WeHealth monitoring system under the WiFi interference. In the following tests, we will set one WeHealth sensor node sending data to the coordinator. The sensor is equipped with Zigbee chip of TI CC2530 [8]. The transmission power is set to 0dBm, and the transmission rate is 10 packets/s. The packet length is 31 bytes which contain a payload of 16

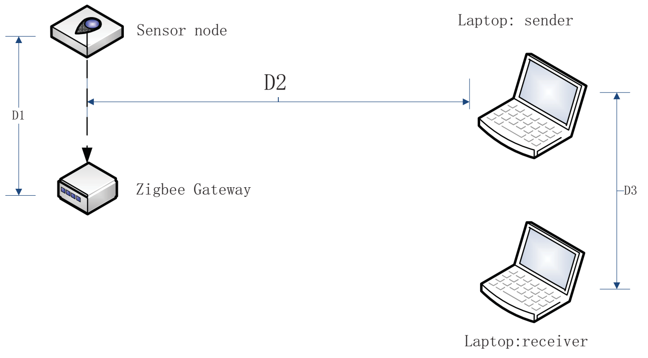

Fig. 3. The deployment of experiment test

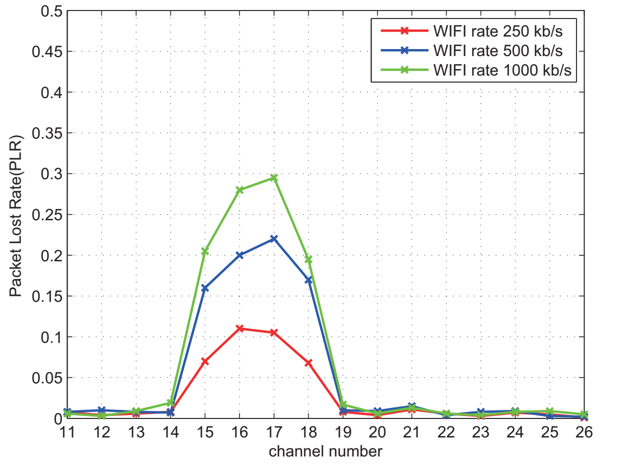

Fig. 4. PLR of Zigbee channels under WiFi channel 5 at the WiFi interference rate of 250, 500 and 1000 kb/s

bytes. There is serial number in the payload used by the receiver to determine the number of the lost packets. Intended to test the packet loss rate (PLR), the lost packet will not be retransmitted. We will implement two laptops with the WiFi module as the WiFi interference source. The physical implement is depicted in Figure 3. D1 is the distance between sensor node and the coordinator while D3 is that between two WiFi laptops. D2 is the distance between the WiFi sender laptop and the Zigbee nodes.

A. Channel Measurement under WiFi Interference

In this measurement, WiFi transmission is set at channel 5 with source data rate of 250, 500 and 1000kb/s. The distance of D1, D2 and D3 is set as 3m, 5m and 3m. Zigbee sensor will send 1000 packets on all of the 26 channels and the PLR will be recorded for each channel. The result is shown in Figure 4 with the average value of several experiments. We can see channel 15-18 are clearly interfered by WiFi signal with PLR upper to15%. The impact on channel 16 and 17 is greater than channel 15 and 18 for the different frequency offset. WiFi interference have little effect on the other channels. This result confirm the analysis in Section II and is in line with the conclusion of [9], there should be at least 7MHz offset between the operational frequencies to have satisfactory performance of Zigbee. The impact decreases as the WiFi traffic rate is lower. It can be inferred that lower WiFi rates result in a reduction of the probability of channel access failure.

B. Performance of CSMA-CA and None at Different Strength of Interference

The deployment of this experiment is similar to the experiment A. Zigbee communication channel is fixed to channel 16. We first set the D2 to 16m, and then reduce the distance by 1m for one PLR test. The other parameters are the same as the previous experiment. We test the transmission with and without the CSMA-CA mechanism to evaluate the transmission performance in GTS. The result is shown in Figure 5. When the D2 is less than 12m, the PLR of transmission using CSMA-CA increases significantly. The WiFi signal strength measured by the WiFi analyzer is -75 dBm while the default energy detection threshold for CCA is - 77dBm. The channel

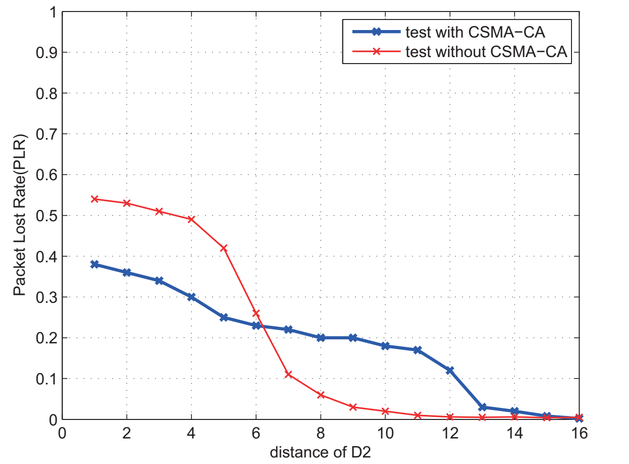

Fig. 5. PLR with different value of D2, WiFi at channel 5, and Zigbee at channel 16

state sensed by CCA will be busy. In contrast, the PLR of transmission without CSMA-CA begin to be clearly visible at the distance of 8m, and rapidly rise to more than 0.5. When D2 is at 8m, the Received Signal Strength Indicator (RSSI) of Zigbee node is -55dBm while the WiFi signal strength is -65dBm. The signal to interference ratio (SIR)is nearly 10dBm. When distance of D2 is between 8m to 10m, transmission with CSMA-CA will be blocked because the WiFi signal strength is always greater than Zigbee CCA energy threshold and the sensor node will always sense busy at the channel. So at this distance range performance of the transmission without CSMA-CA is better than that with CSMA-CA, which is similar to the conclusion of [10].

When the transmission goes into the emergency mode, for the absence of CSMA-CA mechanism, the sensor node should measured the SIR. Transmission using the GTS mechanism

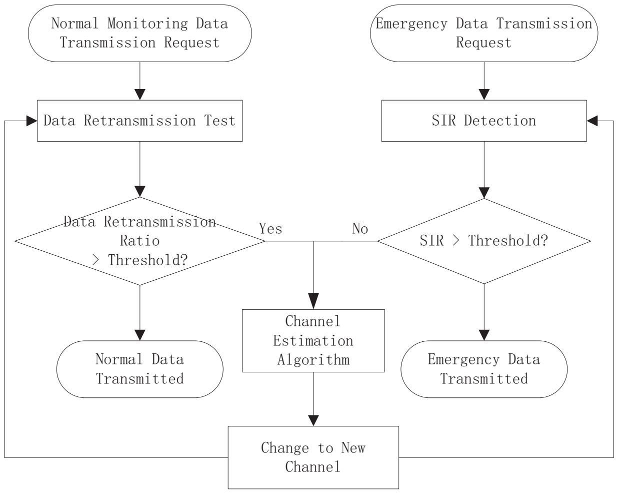

Fig. 6. Flowchart of the proposed Interference Avoidance Strategy for WeHealth

can be carried on successfully when the SIR is greater than 10dB.

IV. Interference Avoidance Strategy

According to the feature of the WeHealth monitoring system and the interference model, we propose a interference avoidance strategy aimed to the WeHealth system. Figure 6 shows the approximate flow of our avoidance strategy. In the normal monitoring cycle, every node will record the Data Retransmission Rate (DRR) of the recent N packets. The DRR is denoted as the ratio of number of packets retransmitted to N. The retransmission may caused by failure of channel access or the failure of reception of the ACK frame. When the DRR is greater than a threshold TH_{DRR} , that means the transmission of the current channel has been unable to carry out the normal monitoring data upload of communication. Then the medical sensor node will send the request of changing communication channel.

When the coordinator detects the emergency physiological data, it will notify the corresponding nodes to enter the emergency mode and allocate the appropriate GTS for each node. When the node receives the notification, it immediately implements SIR detection. The process is like this: the sensor node divides the GTS in the first M_f super frames into two periods. In the first period, the node will send a number of test packets for the coordinator to get the RSSI value, denoted as $RSSI_{data}$. The energy detection will be implemented by coordinator in the second period in which the sensor node will stop sending. The ED value will be approximately obtained by read the RSSI register for several times which can indicate the energy strength of the channel [11], denoted as $RSSI_i$. We take the highest value off as the energy strength of Interference. Then the SIR can be easily obtained. We also set a threshold for the SIR, denoted as TH_{SIR}. If the SIR is greater than this threshold, the communication can be implemented in the current channel with the GTS mechanism. If not, the coordinator then starts to change the communication channel.

There will be a channel estimation to select channel with best performance before the changing implementation. We propose a method for the WeHealth monitoring system of adding a simple WiFi model with an interface to the Zigbee coordinator which can scan the environment getting the information of WiFi networks. We set the strength of the scanned WiFi signal as $Pw[c_w]_n(mW)$ in c_w WiFi channel in the n^{th} scan cycle, which is expressed in mW. Similarly we denote $Dz[c_z]_n$ which indicates the degree of channel being affected by interference. Due to the overlapping channels of the WiFi, the Zigbee interfered channel can be divided into two groups, as follow:

$$\begin{aligned} C_{zw1} &= \{c_w + 11, c_w + 12\}\ , \\ C_{zw2} &= \{c_w + 10, c_w + 13\} \\ where\quad c_w &\in \{\ 1, 2...13\ \} \end{aligned} \tag{1}$$

According to relationship between the interference and the frequency offset, and the test result of Section II, channel in the group C_zw1 have the offset of 2M and 3M and suffer greater interference while the channel of group C_zw2 have the bigger frequency offset. The interference degree of Zigbee channel after the k^{th} scan is based on the equation (2).

$$\begin{aligned} Dz[c_z]_{k+1} = \alpha Dz[c_z]_k + (1-\alpha)\lambda Pw[c_w]_{k+1} \\ where \qquad k \in \{1, 2..., N_k\} \\ \alpha \in (0, 1) \\ c_z \in \{11, 12...26\} \\ \lambda \in \{0, \beta, 1\} \end{aligned} \tag{2}$$

The initial value of $Dz[c_z]_1$ is given the result of $\lambda Pw[c_w]_1$, which is the WiFi interference power acquired in the first WiFi interference scan. The α is the coefficient of scan used to weight mean of previous interference strength and most recent values. Due to the different Zigbee channel groups, the λ will have three values, 0 for the un-interfered channels, β for the C_{w2}, and 1 for the C_{w1} . So after the N_k scan of the WiFi signals, the interference degree $Dz[c_z]$ of all the Zigbee channels will be obtained according to the equation (2). When more than one WiFi signal overlap one Zigbee channel, probability of the Zigbee channel being interfered will be high, so the $Dz[c_z]$ will be the sum of all the WiFi strengths. The coordinator will establish a interference strength list of channels for choosing the best channel to communicate.

When the target channel is determined due to the interference strength list, the coordinator sends the notification packets to the sensor nodes. The nodes that received the notification packets then send ACK frame to acknowledge the reception, after that the node will wait the second confirm packet from coordinator until it changes its communication channel. When the coordinator has received all ACK frame and send all the second confirm packets, it changes to the target channel and start to establish the new Zigbee PAN network for the health monitoring.

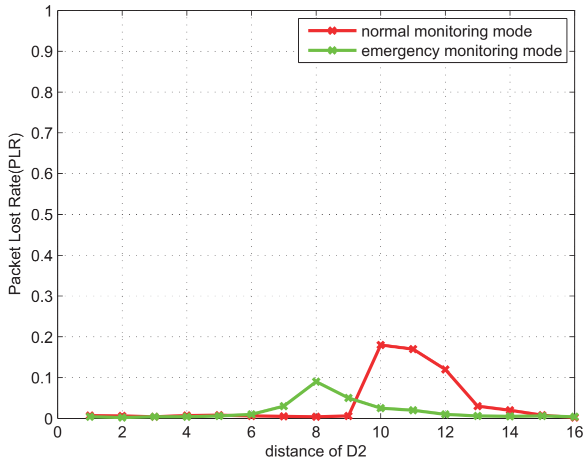

Fig. 7. PLR of the transmission in normal and emergency mode with interference avoidance strategy

V. Evaluation Test and Result

Our evaluation test experiment make use of WeHealth sensors equipped with TI CC2530 Zigbee modules. One node is connected to simple WiFi module and is appointed as the coordinator of WeHealth network. The parameters for the strategy are as follows:

TABLE I
PARAMETERS FOR THE STRATEGY

$\alpha = 0.5$	$M_f = 16$
$\beta = 0.8$	$N_k = 8$
$TH_DRR = 0.2$	$TH_SIR = 10dBm$

We firstly set the experiment which is similar to Test B in Section III, the transmitter and the receiver are moving from a distance to near the WiFi enabled laptop, that is , the distance D2 is set from 16m to 1m for this experiment to test When can the sensor sense the harmful interference. The working channel, data rate, payload of WiFi and Zigbee are equal to the Test B in Section III. The data transmission of the normal mode and the emergency mode are tested in this experiment.

Figure 7 shows the result of the experiment. With the reduction of D2, the WiFi signal strength become greater. In the transmission of normal monitoring mode with CSMA-CA mechanism, PLR begin to increase in the distance of 12m. At the distance of 9m, the PLR goes down. We can get that the coordinator changed the Zigbee channel to channel 25 which is selected by the channel estimation algorithm, for the reason that the DRR is greater than TH_{DRR}. Then even the Zigbee nodes are closer to the laptop, the data transmission successfully avoid the interference.For the emergency mode, the channel changing occurred when the D2 is 7m which the tested SIR is lower than TH_{SIR}. And the coordinator adjusted to the channel 12 with no interference.

VI. Conclusion

In this paper, we introduced the WeHealth monitoring system and the interference problem caused by the WIFI network. We analyzed the impact of the WIFI interference on the normal monitoring mode and emergency monitoring mode of the system, and found that at some situation the transmission in GTS for emergency monitoring is less affected when the SIR is greater than a threshold.

Based on the test and analysis, we proposed our strategy for the system. Both in the normal and the emergency mode, monitoring sensor can detected and estimated the interference. Then the coordinator can changed the communication channel. The coordinator estimated the interfered degree of all the Zigbee channels using the proposed algorithm. Finally, we tested the performance of the strategy and proved that the system can significantly avoid the interference.

Acknowledgement

This work was partly supported by the National High Tech. Research and Development of China (863 Program No. 2009AA02Z412), the International Science and Technology Cooperation Project (2010DFA11590) and the New Century Excellent Talents in University (NCET).

References

[1] Min Li Huang,Sin-Chong Park, ”A WLAN and ZigBee coexistence mechanism for wearable health monitoring system ”, The 9th International Symposium onCommunications and Information Technology (ISCIT),Sept.2009, Icheon, South Korea.

[2] C. Won, et al., ”Adaptive Radio Channel Allocation for Supporting Coexistence of 802.15.4 and 802.11b,” in Proc. VTC, Vol. 4, pp. 2522 - 2526, Sep. 2005.

[3] Fang Yao, Shuang-Hua Yang, Wei Zheng, ”Mitigating interference caused by IEEE 802.11b in the IEEE 802.15.4 WSN within the environment of smart house”, IEEE International Conference on Systems Man and Cybernetics (SMC), Oct. 2010, Istanbul, Turkey.

[4] N. Golmie, ”Coexistence in Wireless Networks, Challenges and System-Level Solutions in the Unlicensed Bands,” University Press, Cambridge, 2006.

[5] Min Suk Kang, Jo Woon Chong, Hyesun Hyun, Su Min Kim, Byoung Hoon Jung, Dan Keun Sung, ”Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference ”, The 2nd International Symposium on Wireless Pervasive Computing (ISWPC), Feb. 2007, San Juan, South Korea.

[6] Wei Yuan, et al, ”Distributed Adaptive Interference-Avoidance Multi-channel MAC Protocol for Zigbee Networks”, Proc. Of IEEE international Conference on Computer and Information Technology, June, 2010.

[7] IEEE 802.15.4 Specification, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), Oct. 1, 2003.

[8] Chipcon from Texas Instruments, CC2530 Transceiver datasheet: http://www.ti.com.cn/cn/lit/ds/symlink/cc2530.pdf

[9] M. Petrova, I Riihijarvi, P Mahonen, and S Labella, ”Performance study of IEEE 802.15.4 using measurements and simulations”. Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE

[10] Bertocco, M.,Gamba, G., Sona, A., ”Is CSMA/CA really efficient against interference in a wireless control system? An experimental answer”, IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sept. 2008, Hamburg, Germany.

[11] Ruitao Xu, Gaotao Shi, Jun Luo, Zenghua Zhao, Yantai Shu, ”MuZi: Multi-channel ZigBee Networks for Avoiding WiFi Interference”, 4th International Conference on Internet of Things and Cyber, Physical and Social Computing.Publication (iThings/CPSCom), Oct. 2011, Dalian, China.