Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications

Peizhong Yi, *Student Member, IEEE*, Abiodun Iwayemi, *Student Member, IEEE*, and Chi Zhou, *Senior Member, IEEE*

***Abstract*—Smart grid is an intelligent power generation, distribution, and control system. ZigBee, as a wireless mesh networking scheme low in cost, power, data rate, and complexity, is ideal for smart grid applications, e.g., real-time system monitoring, load control, and building automation. Unfortunately, almost all ZigBee channels overlap with wireless local area network (WLAN) channels, resulting in severe performance degradation due to interference. In this paper, we aim to develop practical ZigBee deployment guideline under the interference of WLAN. We identify the "Safe Distance" and "Safe Offset Frequency" using a comprehensive approach including theoretical analysis, software simulation, and empirical measurement. In addition, we propose a frequency agility-based interference avoidance algorithm. The proposed algorithm can detect interference and adaptively switch nodes to "safe" channel to dynamically avoid WLAN interference with small latency and small energy consumption. Our proposed scheme is implemented with a Meshnetics ZigBit Development Kit and its performance is empirically evaluated in terms of the packet error rate (PER) using a ZigBee and Wi-Fi coexistence test bed. It is shown that the empirical results agree with our analytical results. The measurements demonstrate that our design guideline can efficiently mitigate the effect of WiFi interference and enhance the performance of ZigBee networks.**

***Index Terms*—Active scan, energy detection, frequency agility, PER, smart grid, WLAN, ZigBee.**

I. Introduction

THE SMART GRID is an intelligent power generation, distribution, and control system. It specifies the addition of intelligence and bidirectional communication and energy flows to today's power grid in order to address the efficiency, stability, and flexibility issues that plague the grid. The smart grid facilitates services such as wide-scale integration of renewable energy sources, provision of real-time pricing information to consumers, demand response programs involving residential and commercial customers, rapid outage detection, and granular system health measurement.

All of these tasks demand the collection and analysis of real-time data, along with the control of electrical loads for energy reduction and demand response, emphasizing the importance of the communication infrastructures required to support device control and data exchange between the various domains which comprise the smart grid.

The U.S. National Institute for Standards and Technology (NIST) has defined ZigBee and the ZigBee Smart Energy Profile (SEP) as the one of the communication standards for use in the customer premise network domain of the smart grid [1]. ZigBee wireless technology is characterized by low cost, low power, low data rate, and simplicity [2]. These features, along with its operating over unlicensed spectrum and being a standardized protocol based on IEEE 802.15.4 standards, facilitate easy network deployment and implementation, and make it the most suitable wireless technology for smart grid applications. It has also been selected by a large number of utilities as the communications platform of choice for their smart metering devices as it provides a standardized platform for exchanging data between utilities and smart metering devices and appliances located on customer premises [3]. The SEP provides support for features including demand response, advanced metering support, real-time pricing, text messaging, and load control.

The Illinois Institute of Technology (IIT) Perfect Power project is a five-year project sponsored by the U.S. Department of Energy (DOE), with the objective of implementing smart grid in IIT main campus. The purpose is to improve energy efficiency throughout the campus by reducing electricity consumption by up to 11 million kWh (20% reduction) and reducing natural gas consumption by nearly 1 million therms (10% reduction) per year. One of the primary research activities of IIT Perfect Power project is the evaluation of advanced wireless technologies for real-time system monitoring, load control and reduction, energy efficiency, and building automation. In line with NIST smart grid guidelines, the IIT Perfect Power project has adopted ZigBee as the wireless communications infrastructure for energy usage monitoring, net metering, and demand response.

However, operating on the license-free industrial, scientific, and medical (ISM) frequency band, ZigBee is subject to interference from various devices that also share this license-free frequency band, ranging from IEEE 802.11 wireless local area networks (WLANs) or WiFi networks, Bluetooth, to baby monitors and microwave ovens, shown in Fig. 1. Studies have shown that WiFi is the most significant interference source for ZigBee within the 2.4 GHz ISM band [4], [5]. As the adoption of ZigBee for smart grid applications within homes, campuses, and commercial buildings becomes widespread, their usage in environments with prevalent WiFi networks introduces ZigBee and WiFi coexistence problems, serving as the motivation for this work.

In the light of this, the collocation of ZigBee and WiFi devices needs to be taken into account during ZigBee deploy-

Manuscript received April 01, 2010; revised August 12, 2010; accepted October 25, 2010. Date of publication December 20, 2010; date of current version February 18, 2011. This work was supported by the Department of Energy under Grant DE-FC26-08NT02875. Paper no. TSG-00044-2010.

The authors are with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: pyi@iit.edu; aiwayemi@iit.edu; zhou@iit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2010.2091655

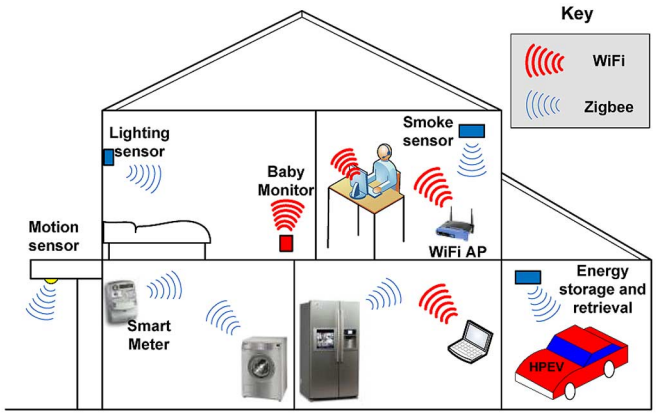

Fig. 1. ZigBee and WiFi device collocation.

ment. Despite the extensive existing research on ZigBee and WiFi coexistence, no practical and simple deployment guideline can be found in the related work, such as how far away the ZigBee should be placed from the WiFi AP and over which frequency ZigBee should operate in order to maintain certain QoS. In this paper, we aim to identify the "Safe Distance" and "Safe Offset Frequency" to guide the ZigBee deployment using a comprehensive approach including theoretical analysis, software simulation, and empirical measurement. To guide ZigBee network deployment, we first need to evaluate the impact of WiFi interference on ZigBee performance. The performance of ZigBee in the presence of IEEE 802.11 is analyzed theoretically in terms of Bit Error Rate (BER) and Packet Error Rate (PER), and a complete ZigBee and WiFi coexistence simulation system is designed and implemented in MATLAB. Moreover, performance of ZigBee subject to IEEE 802.11 interference is measured in residential environment and laboratory using off-the-shelf ZigBee products. To verify that the deployment guideline can be applied in general situations, different experiment scenarios are designed and evaluated in the paper. From those results, we identify that 8 m between ZigBee and WiFi is a "safe" distance which can guarantee the reliability of ZigBee no matter what's the offset frequency, and 8 MHz is a "safe" offset frequency (i.e., the interference is negligible) even when the distance is just 2 m.

We also need to develop techniques to mitigate WiFi interference in order to guarantee ZigBee performance when the WiFi interference is significant. We propose to adopt a frequency-agility based interference mitigation algorithm [6]. Our preliminary work has been presented in [7]. Specifically, PER, link quality indicator (LQI), and energy detection mechanisms are used to detect the presence of significant levels of interference within the current channel. Once interference is detected, the coordinator instructs all the routers to perform an energy detection scan on channels and then the measurement report's is sent to the coordinator. The coordinator selects the channel with the low noise levels and then requests all nodes in the PAN to migrate to this channel. In order to reduce the detection time and power consumption, we divide all ZigBee channels into three classes based on offset frequency. The energy detection scan will be performed from high priority class to low priority class to quickly identify the channel with acceptable interference level. The real implementation shows that the proposed frequency-agility based algorithm is simple but efficient, fast, and practical.

The rest of paper is organized as follows. Section II presents the related work. In Section III, ZigBee and WiFi standards are briefly introduced. A theoretical model of ZigBee under WiFi interference is presented in Section IV. Section V presents our proposed frequency agility-based interference mitigation scheme. Our MATLAB/Simulink-based ZigBee and WiFi coexistence simulation model is shown in Section VI. We empirically evaluate the performance of proposed scheme in a ZigBee test bed in Section VII. Finally, the paper is concluded in Section VIII.

II. Related Work

ZigBee performance has been investigated extensively using analysis and software simulation. In [8], the authors developed a ZigBee PHY layer simulation model based on the IEEE 802.15.4 standard, and evaluated ZigBee performance in the absence of interference in terms of BER. In [9], the performance of IEEE 802.15.4 under the effect of IEEE 802.11 interference is analyzed in terms of the BER, without considering the collision time during which IEEE 802.11b packets overlap IEEE 802.15.4 packets. In [5], the PER is obtained from the BER and collision time by analysis and simplified simulation.

ZigBee performance under WiFi interference has also been measured in empirical experiments. Zensys Company tested a large number of ZigBee products from the European market in the laboratory environments and generated results demonstrating that ZigBee is critically impacted by IEEE 802.11b [4]. According to two-year survey data from thousands of systems in operation today around the world containing both ZigBee and WiFi, ZigBee Alliance's report shows that the ZigBee can coexist with WiFi while still maintaining the desirable Quality of Service (QoS) [10]. In [11], the received signal strength indicator (RSSI) and PER of IEEE 802.15.4 are measured using off-the-shelf hardware. Interaction between ZigBee and IEEE 802.11g is empirically evaluated in terms of throughput in [12], with results demonstrating that ZigBee does not affect IEEE 802.11g significantly; however, the throughput of ZigBee drops significantly when the spectrum of the chosen channels of operation coincide.

However, none of the existing research specifies how to deploy the ZigBee network with WiFi present in practice. When we try to develop and deploy a Smart Grid test bed for IIT Perfect Power project, in which ZigBee-equipped sensors and actuators are used to demonstrate building automation and control, we have encountered many restrictions and constraints during real world implementation and deployments. For instance, ZigBee node placement is often restricted by the function of the node and this may necessitate placement close to WiFi APs. For example, motion sensors have to be deployed near a door, while smart meters are deployed in distribution cabinets. In such cases, appropriate channel management is the only available interference mitigation method available to us. For WPAN deployments permitting flexible node placement, the determination of "safe" locations in which we can minimize the effect of interference is paramount for optimal node

TABLE I
ZIGBEE FREQUENCY BANDS AND DATA RATES [17]

PHY (MHz)	Frequency band (MHz)	Channel Number	Spreading parameters		Data parameters	
			Chip rate (kchip/s)	Modulation	Bit rate (Kb/s)	Symbol
868/915	868-868.6	0	300	BPSK	20	Binary
	902-928	1-10	600	BPSK	40	Binary
2450	2400-2483.5	11-26	2000	OQPSK	250	16-ary Orthogonal

placement. This enables us to reserve "safe" channels for nodes which have inflexible deployment conditions.

Interference mitigation schemes have been proposed to enhance ZigBee performance. Won *et al.* [13] proposed an adaptive channel allocation scheme for ZigBee and WiFi co-existence, which allows ZigBee to utilize multiple channels in a personal area network (PAN). However, it is not practical, as ZigBee specifies that each PAN uses only one channel. An adaptive, interference-aware multichannel clustering algorithm is proposed in [14], but such scheme is not suitable for practical deployment due to significant delays it incurs. Designing the interference mitigation technique, we have to consider the practical implementation constraints, such as the specification limitation of ZigBee standards, small memory size, low computation capability, small delay requirement, etc. In other words, any proposed scheme should be simple, practical, and energy-efficient.

III. ZIGBEE/IEEE 802.15.4 AND WIFI/IEEE 802.11B OVERVIEW

A. ZigBee/IEEE 802.15.4

IEEE 802.15.4 defines the Physical Layer (PHY) and Medium Access Control (MAC) of ZigBee, while the ZigBee Alliance defines the network and application layers. The 802.15.4 standard specifies operation in the ISM 2.4 GHz, 915 MHz and 868 MHz bands and two PHY options with both adopting direct sequence spread spectrum (DSSS). The basic channel access mode employs "carrier sense, multiple access with collision avoidance" (CSMA/CA). There are 16 ZigBee channels in the 2.4 GHz band, with each channel occupying 5 MHz of bandwidth. The maximum output power of the radios is generally 0 dBm (1 mw) and receiver sensitivities are -85 dBm for 2.4 GHz and -92 dBm for 868/915 MHz. It uses binary phase shift keying (BPSK) modulation for both 868 and 915 MHz bands, and offset quadrature phase-shift keying (OQPSK) modulation for 2.4 GHz band. Transmission range is between 1 and 100 m, heavily dependent on the deployment environment [2]. Frequency band and data rate information is summarized in Table I.

IEEE 802.15.4 supports both beacon-enabled and non-beacon-enabled communication. In a non-beacon-enabled network, a device simply transmits its data frames using un-slotted CSMA/CA to the coordinator. In contrast, in a beacon-enabled network, the device uses the network beacon to identify available data transmit intervals.

TABLE II
IEEE 802.11B DATA RATES SPECIFICATIONS [5]

Data rate	Code length	Modulation	Symbol rate	Bits/symbol	System
1 Mbit/s	11 (Barker C)	DBPSK	1	1	DSSS
2 Mbit/s	11 (Barker C)	DBPSK	1	2	DSSS
5.5 Mbit/s	4 (CCK)	DBPSK	1.375	4	HR/DSSS
11 Mbit/s	8 (CCK)	DBPSK	1.375	8	HR/DSSS

ZigBee devices can be classified into two major categories, full function devices (FFDs) and reduced function Devices (RFDs) [2]. FFDs can perform network establishment, routing, and management, while RFDs only support a subset of the ZigBee device functions, making them simple and low cost. A ZigBee network usually consists of a ZigBee Coordinator, one or more ZigBee Routers, and multiple End Devices. A FFD can serve any of the three roles, while end devices tend to be RFDs. The ZigBee Coordinator is responsible for network setup and management. ZigBee Routers are used to route traffic between the network coordinator and end devices. Routers and coordinators can communicate with all the devices on the network, usually powered by main power supplies since they cannot go to sleep without adversely affecting the ability to route traffic through the network. End devices communicate with routers, incapable of peer to peer communication. They tend to be battery-powered devices and spend most of their time in sleep mode. They periodically wake up, check for any messages buffered for them at their parent router, read their attached sensors, transmit the measured data, and return to sleep mode.

B. WiFi/IEEE 802.11b

IEEE 802.11 standard specifies PHY and MAC for WiFi. It defines 13 overlapping 22 MHz wide frequency channels in the ISM 2.4 GHz frequency band. As there are only two groups of three nonoverlapping channels, one group for channels 1, 6, and 11 is adopted for use in the US while the other group for channels 1, 7, and 13 is utilized in Europe. IEEE 802.11 has several versions, among which IEEE 802.11b has been widely applied in WiFi. IEEE 802.11b has a maximum transmission rate of 11 Mbps and uses the same CSMA/CA media access method defined in the original IEEE 802.11 standard. The 802.11b PHY layer incorporates DSSS modulation. Technically, the 802.11b standard uses Barker coding and complementary code keying (CCK) as its modulation technique. It is the amendment of CCK coding that enables data rate to increase dramatically compared to original standard. Typical indoor range is 100 ft at 11 Mbps and 300 ft at 1 Mbps. Different data rate specifications are shown in the Table II.

IV. THEORETICAL ZIGBEE BER AND PER ANALYSIS

In this section, a BER and PER analysis model is introduced based on the model developed in [5]. We extend their work by including not only the interference but also noise into the PER analysis.

A. BER Analysis of ZigBee Under WiFi

The PHY of IEEE 802.15.4 at 2.4 GHz uses OQPSK modulation. For an additive white Gaussian noise (AWGN) channel, the BER can be calculated by the following equation [15]:

$$BER = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{1}$$

where E_b/N_0 is the normalized signal-to-noise ratio (SNR) and $Q(x)$ is the Q-function of Gaussian distribution

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{u^2}{2}\right) du. \tag{2}$$

When a ZigBee channel overlaps with a WiFi channel, we can consider the WiFi signal as partial band jamming noise for the ZigBee signal [16] and the SNR is replaced by signal-to-interference-plus-noise ratio (SINR) which can be defined as

$$\text{SINR} = \frac{P_{\text{signal}}}{P_{\text{noise}} + P_{\text{interference}}} \tag{3}$$

where P_{signal} is the power of the desired signal at ZigBee receiver, P_{noise} is the noise power, and $P_{\text{interference}}$ is the received interference power from WiFi signal at ZigBee receiver.

The path loss model represents the power loss between transmitter and receiver, and can therefore be used in conjunction with the transmission power to enable the calculation of P_{signal} and $P_{\text{interference}}$. We define the maximum transmission power of ZigBee as 1 mw (0 dBm). Considering that ZigBee and WiFi are most frequently deployed in the indoor environments, a simplified indoor path loss model is adopted in this paper [15]

$$L_p(d) = \begin{cases} 20\log_{10}\left(\frac{4\pi d}{\lambda}\right), & d \le d_0 \\ 20\log_{10}\left(\frac{4\pi d}{\lambda}\right) + 10n\log_{10}\frac{d}{d_0}, & d > d_0 \end{cases} \tag{4}$$

where d_0 is a break point. We set n equals to 3.3 and d_0 is 8 m [17].

Considering that the power spectrum of IEEE 802.11b is 11 times wider than ZigBee and is not uniformly distributed, in-band interference power of IEEE 802.11 cannot be simply calculated by dividing 11 [18]. An amendment parameter of in-band power factor r is added to $P_{interference}$. Therefore, (3) is modified to:

$$\text{SINR} = \frac{P_{\text{signal}}}{P_{\text{noise}} + r \cdot P_{\text{interference}}}. \tag{5}$$

To obtain the factor, the power spectral density of the IEEE 802.11b and offset frequency between the central frequency of ZigBee and WiFi are considered. Since the power is concentrated around the central frequency, r increases as the offset frequency decreases.

B. PER Analysis of ZigBee Under WiFi Interference

The PER is calculated based on BER and collision time. The IEEE standards for both IEEE 802.11 [19] and 802.15.4 [20] specify three methods of clear channel assessment (CCA) to determine the channel occupancy.

CCA Mode 1: Energy detection

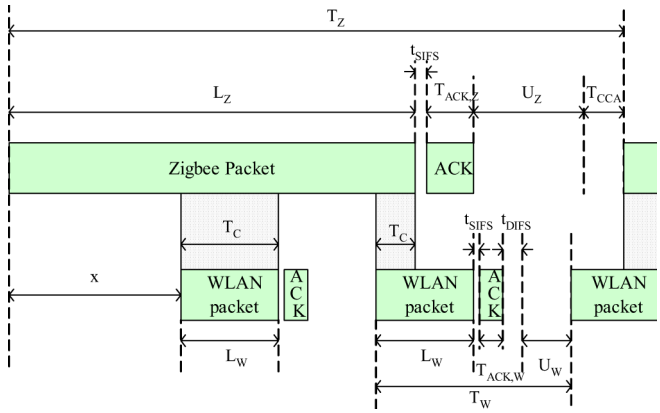

Fig. 2. Interference model between IEEE 802.11b and IEEE 802.15.4 [18].

CCA Mode 2: Carrier sensing

CCA Mode 3: Carrier sensing with energy detection.

The default mode of operation of WiFi is mode 2, in which a WiFi node considers the channel free if no other WiFi device is detected, even if some device other than WiFi may be using the channel. And we assume that both Zigbee and WiFi devices operate in CCA mode 2, meaning that they are essentially blind to each other's transmissions. This assumption therefore provides the worst case performance for WiFi and ZigBee coexistence environments. A similar assumption is made in Shin *et al.*'s paper [18]. We therefore assume blind transmissions for both IEEE 802.15.4 and IEEE 802.11b and that retransmissions are not taken into account.

The collision time model is shown in Fig. 2. Based on the assumption of blind transmission, the contention window is not modified even when ZigBee and WiFi coexist. Though both ZigBee and WiFi adopt CSMA/CA, unlike WiFi, ZigBee only detect the availability of a channel by CCA twice after backoff time. Let U_z and U_w represent the average backoff time of ZigBee and WiFi, respectively. Suppose that the backoff time is uniformly distributed between zero and their minimum contention window, so we can set the two average backoff times equal to half of the IEEE 802.15.4 and IEEE 802.11 minimum contention window respectively. Table III lists all parameters and the corresponding values commonly used. From Fig. 2, we have

$$T_Z = L_Z + T_{\text{CCA}} + \text{SIFS}_Z + T_{\text{ACK,Z}} + U_Z \tag{6}$$

$$T_W = L_W + \text{SIFS}_W + T_{\text{ACK,W}} + \text{DIFS} + U_W. \tag{7}$$

Let x be the time offset between WLAN packets and ZigBee packets. Similar to [14], we simplify the model by assuming that x is uniformly distributed in $[0, T_W)$, and then the average collision time T_c can be calculated using the following equation:

$$T_c(x) = \begin{cases} L_z - x - 2(T_w - L_w) & 0 \le x < L_z - 2T_w \\ 2L_w & L_z - 2T_w \le x < L_z - T_w - L_w \\ L_w + L_z - x - T_w & L_z - T_w - L_w \le x < L_z - T_w \\ L_w & L_z - T_w \le x < L_z - L_w \\ L_z - x & L_z - L_w \le x < L_z \end{cases} \tag{8}$$

$$T_c = \frac{\int_0^{L_z} T_c(x)dx}{L_z}. \tag{9}$$

TABLE III
PARAMETERS IN INTERFERENCE MODEL [5]

Parameter	Definition	Value
T_z	inter-arrival time between two ZigBee data packets	6186μs
L_z	duration of a ZigBee data packet	4064μs
tSIFS	t Short interframe space of Zigbee	10μs
$T_{ack,z}$	duration of a ZigBee ACK packet	352μs
U_z	Average backoff time of Zigbee	1120μs
TCCA	Clear Channel assessment time	640μs
T_w	Inter-arrival time between two WLAN data packets	1977μs
L_w	Duration of WLAN data packet	1303μs
tSIFS	Short interframe space of WLAN	10μs
tDIFS	Distributed coordination function interframe space of WLAN	50μs
$T_{ack,w}$	Duration of WLAN ACK packet	304μs
U_w	Average backoff time of WLAN	310μs
X	Time offset	Varying
T_c	Collision Time	Varying

The PER of ZigBee under WiFi (IEEE 802.11b) interference can be expressed as

$$\mathrm{PER} = 1 - \left[(1 - P_b)^{N_z - |T_c/b|} \times (1 - P_b^I)^{|T_c/b|}\right] \quad (10)$$

where P_b is the BER without IEEE 802.11 interference, P_b^I is the BER with IEEE 802.11 interference, N_z is the number of the bits in a ZigBee packet, and b is duration of a bit transmission.

V. INTERFERENCE AVOIDANCE SCHEME—FREQUENCY AGILITY

According to the theoretic model, BER depends on noise and interference power within the overlapping channel. Distance and offset frequency play a key role on interference power. If ZigBee devices can detect interference, find "safe channels," and migrate the entire PAN to a clear channel, performance will be significantly improved. The proposed solution should require minimal adjustments to the existing IEEE 802.15.4 standard, or can be implemented via a software upgrade in order to facilitate easy adoption. In addition, any proposed solution must be simple and energy efficient. Considering these factors, we propose a frequency agility algorithm for IEEE 802.15.4 cluster-tree networks which combines the star and mesh topologies, achieving both high level of reliability and scalability, and energy efficiency.

The key operations of our scheme are interference detection and interference avoidance. Each sender node measures its PER periodically. If the PER exceeds some threshold, the sender will report to router to check its link quality indicator (LQI). If LQI is below certain value, the coordinator instructs all the routers in the PAN to perform interference detection of the available channels. Interference detection is achieved by means of energy detection (ED) scans defined in the ZigBee protocol. Based on the feedback from all the ED scans, the Coordinator selects a channel which has acceptable quality and also not used by other ZigBee PAN. The final step is the migration of all the PAN devices to this "safe" channel. We elaborate on the steps involved in the proposed frequency agility scheme in the following section.

A. Interference Detection

Energy efficiency is a major feature of the ZigBee standard so it is essential that any interference detection scheme be energy efficient. In most time, it has been observed that ZigBee can provide reliable service. In order to extend device battery lifetime, interference mitigation functions should be applied as rarely as possible, unless absolutely necessary, e.g., when the received interference is too significant due to the heavy traffic.

Some interference detection schemes have been studied for sensor network including [13], [21] and [14]. In [21], Zhou *et al.* present a radio interference detection protocol (RID) to detect run-time radio interference among sensor nodes. Unfortunately their work cannot be directly applied to our scenario, as the interference we consider is from a different air interface scheme, rather than interference within the same access network. An interference detection scheme based on the ED scan results and received signal strength indication (RSSI) is proposed in [14]. In this paper, Kang *et al.* argue that RSSI is not an accurate measure of interference, as the RSSI values of ZigBee frames at a distance within 0.3 m can be very high. Kim [22] proposed an ACK/NACK-based interference detection scheme which utilizes ACK/NACK reports to detect interference. The sender sends beacon frame to receiver and counts the number of NACKs. If the value exceeds the threshold, then interference is detected. However, the ZigBee standard [2] defines that once the beacon frame is sent, all the reachable full-function devices within the communication range must respond to the beacon request. Such a system will result in significant energy waste, which is unacceptable for low power networking scheme such as ZigBee.

To improve these schemes, we propose a PER-LQI based interference detection scheme in ZigBee network. Due to ZigBee's low duty cycle which only requires a few milliseconds to transmit packets [23], a node can successfully deliver the majority of its packet by means of retransmission. To improve packet transmission and network battery life, we use regular packets rather than dedicated signaling messages such as dedicated beacons or periodic packet transmissions to perform interference detection. Each end device measures its PER over transmission period of at least 20 packets [2]. When the PER exceeds 25%, an interference detection report is sent to the parent router of that end device. The router checks the LQI between router and end device, if the LQI [24] is smaller than 100 (which maps to PER 75%,) it considers that the packet loss has occurred due to poor link quality rather than due to power outages or other problems at the End device. In this case, router will perform ED scans on the current channel to ensure that interference is the actual cause of the degradation detected

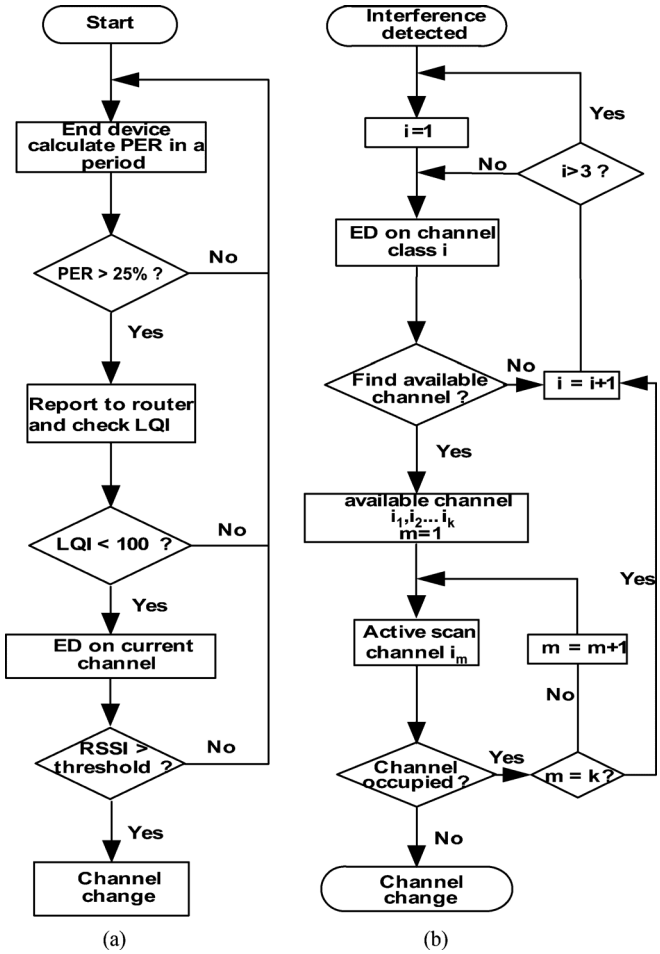

Fig. 3. Flowchart of: (a) interference detection and (b) interference avoidance.

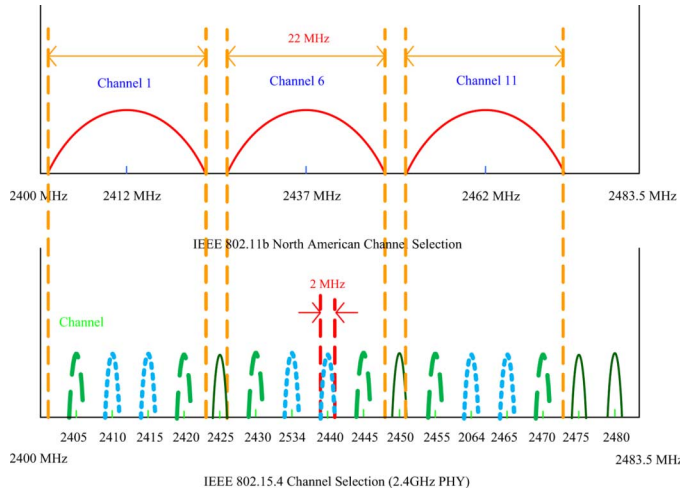

Fig. 4. ZigBee and WiFi channels in the 2.4 GHz band.

in link quality. Once the energy detection result RSSI exceeds a threshold of 35 (corresponding to a noise level between -65 dBm to -51 dBm), it considers interference has been detected and the node makes an interference report to its router which forwards the report to the coordinator. The coordinator then calls the corresponding interference avoidance scheme and initiates migration to a safe channel. The flowchart of interference detection is shown in Fig. 3(a). Our proposed scheme emphasizes simplicity and efficiency, with low network overheads.

For a specific case, in which the interference is so severe that end device can't successfully report it to router, the router still can detect interference since it periodically monitors the link LQI between itself and all its child nodes. If the LQI is quite low over multiple cycles and router doesn't receive any messages from its child nodes within the configured timeout period, the router automatically performs an energy detection scan and reports the results to the coordinator.

B. Interference Avoidance

Once interference is detected, some interference avoidance scheme needs to be applied to mitigate the effect. In [24], considering the scenario in which multiple ZigBee PANs coexist, authors suggest letting the PAN which experiences greater interference, or the PAN with lower priority, change to another channel by means of beacon requests. The coordinator determines which channel they switch to based on the responses from the beacon requests that indicate free channel. A pseudorandom-based interference avoidance scheme is proposed in [18]. All devices move to the same next channel based on the pseudorandom sequence predefined to avoid interference. This scheme doesn't take into consideration factors such as the interference source and state of other channels, instead, channel selection is randomly performed and interference detection is repeated. It is obviously that this scheme increases the delay and energy consumption. Our interference avoidance scheme utilizes energy detection and active scans to determine which channel is appropriate for all the devices to change to. ZigBee utilizes sixteen 2 MHz wide frequency channels located within the ISM band, and our test bed experiments show that when the offset frequency between ZigBee channel and the WiFi central frequency is larger than 8 MHz, the interference from IEEE 802.11b is negligible. When the offset frequency is less than 3 MHz, ZigBee experiences significant levels of interference. Our results are in line with similar research such as [21].

In order to reduce the detection time and power consumption of our protocol, we divide all ZigBee channels into three classes based on offset frequency. As shown in Fig. 4, Class 1 (solid line) consists of channels 15, 20, 25, 26 in which the offset frequency is larger than 12 MHz; class 2 (dashed line) is made up of channels 11, 14, 16, 19, 21, 24 with the offset frequency is larger than 7 MHz and smaller than 12 MHz; while class 3 (dotted line) consists of channels 12, 13, 17, 18, 22 and 23 respectively which offset frequency is smaller than 3 MHz. Class 1 has highest priority and class 3 has the lowest. Upon receipt of an interference detection report, the coordinator sends an energy detection scan request to all routers in the PAN to check the status of channels from high priority to low priority till an available channel is found. The coordinator chooses the best channel by means of weighted energy detection result. Each router is assigned a weight based on its priority, network topology, and location. Node's which are near WiFi APs or which possess a large number of child nodes is assigned larger weights. The coordinator chooses the available channels from high to low score. In a

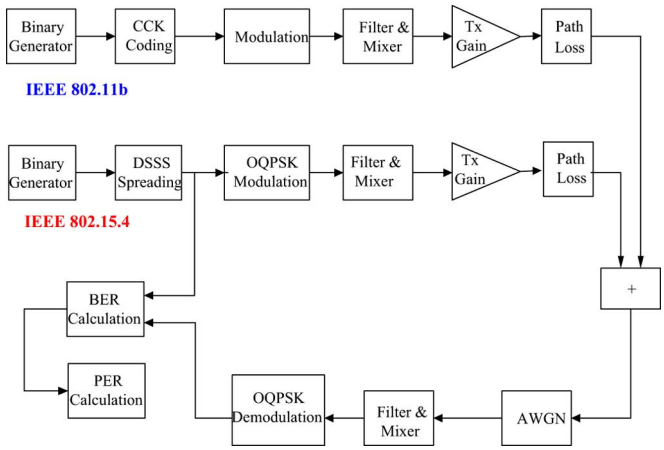

Fig. 5. IEEE 802.11b /IEEE 802.15.4 coexistence simplified simulation model.

cluster-tree ZigBee network, having all routers doing the energy detection can avoid hidden terminal problem to some extent. In comparison to having all the devices in the PAN perform an energy detection scan, our algorithm minimizes the complexity of the decision-making algorithm and is more energy efficient.

Upon completion of the energy detection scan, all routers in PAN commence an active scan on the proposed migration channel selected by the coordinator. They send out a beacon request to determine if any other ZigBee or 802.15.4 PANs are currently active in that channel within hearing range of the radio. If a PAN ID conflict is detected, the coordinator selects a new channel and unique PAN. The decision algorithm is detailed in Fig. 3(b).

VI. Simulation Model and Results

A. Simulation Model

According to theoretical model we develop a simulation model based on the IEEE 802.15.4 standard using MATLAB\Simulink, shown in Fig. 5. In accordance with IEEE 802.15.4 standards document, every four bits are mapped into a symbol and each symbol spreads to a 32-chip almost orthogonal PN sequence, thus a spreading table is set in a spreading block. Data is packed into frames, with a maximum frame size of 128 bytes as defined in the standard. The transmission rate is 250 kbps at 2.4 GHz for ZigBee, while 11 Mbps for WiFi. We utilized the IEEE 802.11b simulation module provided in MATLAB. The IEEE 802.15.4 and IEEE 802.11b signals are added together before being passed through AWGN channel. Both signals must be sampled and filtered at the same sampling rate [25]. The frequency band for both simulation systems was set to -44 to 44 MHz to satisfy the Shannon theorem. The BER is calculated based on minimum Hamming distance between data before modulation and after demodulation. The spectrum derived from the simulation in Fig. 6 is compared with the measured spectrum obtained by means of a spectrum analyzer as shown in Fig. 7. Measurements were taken in a screen room, enabling the elimination of all external signals and interference.

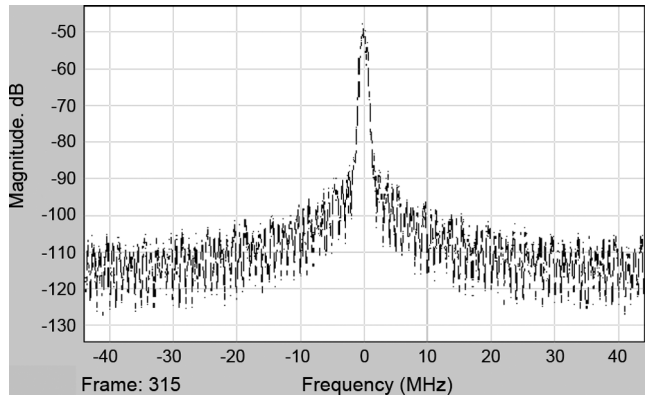

Fig. 6. Simulated power spectrum of ZigBee signal.

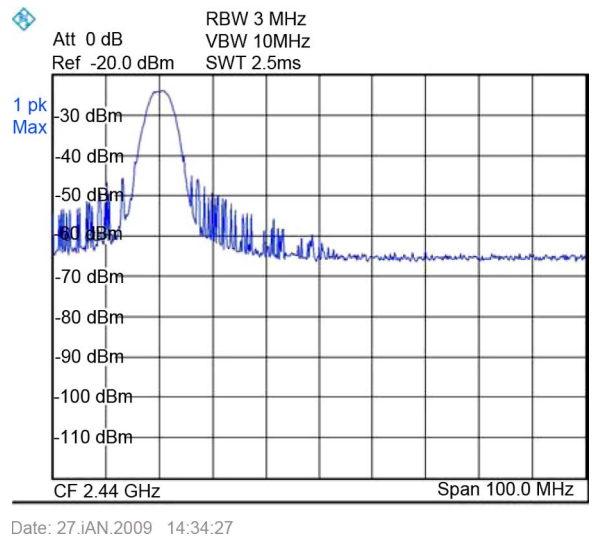

Fig. 7. Measured power spectrum of ZigBee signal.

B. Simulation Results

Theoretical analysis and simulation of BER and PER are shown in Figs. 8 and 9 respectively. The solid line represents theoretical values while the dotted lines represent the values obtained via simulation. Except for a few channels that are far away from the WiFi central frequency, most of channels overlapped with the WiFi channels have 2 MHz, 3 MHz, 7 MHz, and 8 MHz offsets from the WLAN channel frequency. We therefore perform simulations in these four scenarios.

From both the simulation and theoretical results, we find that the BER and PER drop drastically as the offset frequency increases. For the same offset frequency channel, the BER and PER decrease when the separation distance increases. BER and PER are higher when the offset frequency is 2 MHz and 3 MHz in the simulation compared to theoretic results; when the offset frequency is 7 MHz and 8 MHz, the BER is lower than theoretical result. That is because the frequency band of the IEEE 802.11b simulation model is narrower than the theoretical one, with more power concentrated on the effective band frequency.

Both graphs prove that most interference power is around the central frequency of WiFi. “Safe Distance” and “Safe Offset Frequency” are two critical parameters, which guide the ZigBee deployment in order to mitigate the WiFi interference. If the offset frequency is less than 2 MHz, the distance needs at least 8 m to efficiently minimize the effect of the IEEE 802.11b. If

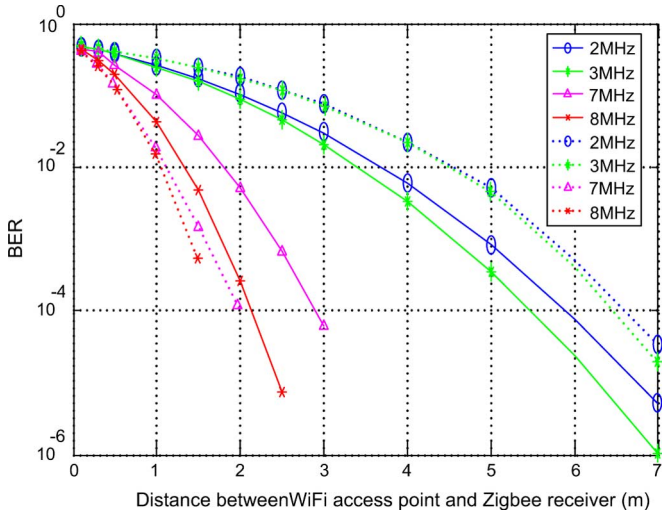

Fig. 8. Theoretical and simulation BER versus distance.

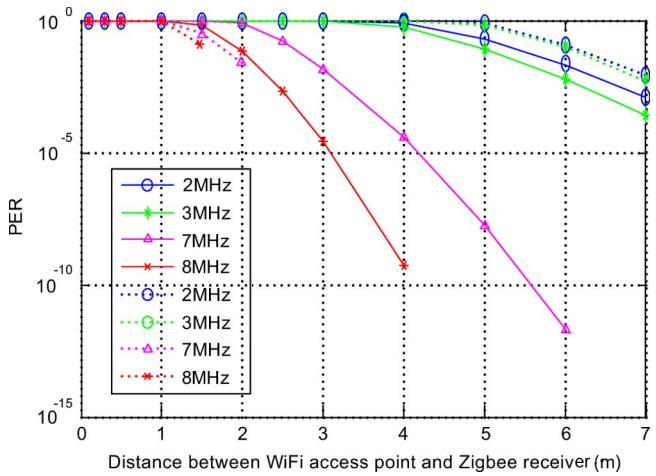

Fig. 9. Theoretical and simulation PER versus distance.

the offset frequency is larger than 8 MHz, safe distance can be decreased to 2 m.

VII. Implementation

To evaluate the performance of ZigBee under WiFi interference in real world environments as well as the performance of our scheme in terms of PER, we deploy a Zigbee-WiFi coexistence test bed, which consists of a pair of ZigBee nodes, two laptops, a PC desktop, and two Linksys Wireless G WiFi routers. In addition, a WiSpy WiFi analyzer and a Peryton ZigBee network analyzer are used to measure the performance.

A. ZigBee Performance Under WiFi Interference

We first examine the ZigBee performance under WiFi interference in a typical residential environment. Fig. 10 shows the test bed developed. A WiFi router is set as an access point, with two laptops connected to the WiFi. One laptop transmits large files constantly to the other laptop through AP. Two ATMEL RZRAVEN 2.4 GHz ZigBee boards are used to form peer-to-peer communication. The distance between the ZigBee transmitter and receiver is 1 m, while the distance between the access point and the ZigBee receiver can vary. The WiFi AP is set to channel 1 (2412 MHz). ZigBee channels 11, 12, 13, and 14

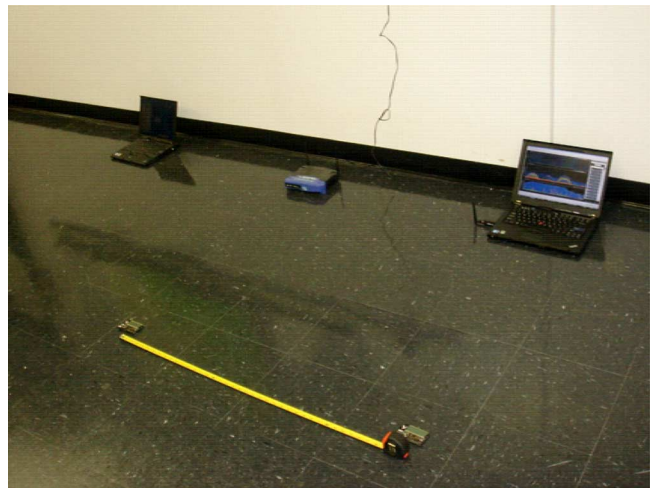

Fig. 10. Test bed.

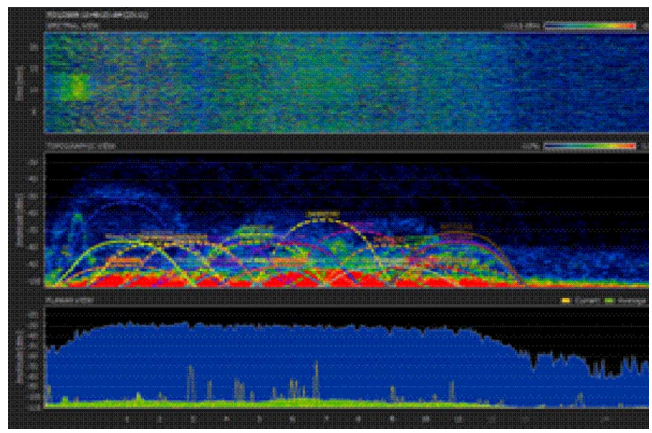

Fig. 11. Power spectrum of ZigBee and WiFi AP survey at residential environment (offset frequency 7 MHz).

are tested which correspond to offset frequencies of 7 MHz, 2 MHz, 3 MHz, and 8 MHz respectively. The PER is calculated by the receiver board as follows:

$$\text{PER} = \left(\frac{\text{Number of Failed Messages}}{\text{Number of Attempted Measurements}} \right) * 100\%. \tag{11}$$

The performance for the typical residential environment is tested at Lake Meadows Apartments, a typical residential apartment building in Chicago, which is a 22-story high-rise with 15 units per floor. Almost each unit has a WiFi Router which can cover multiple units in the physical communication range. The Internet connection is DSL with 768 kbps–3 Mbps. Fig. 11 shows the power spectrum measured within one unit. It is shown that a large number of WiFi APs coexists with overlapping spectrum and various signal power strength. We set the distance between the access point and the ZigBee receiver as 1 m. The laptop downloads files from AP at the rate of 768 kbps. The PER performance is shown in Fig. 12(a). We observe that the PER decreases as the frequency offset increases. However, although multiple WiFi APs are present, the interference impact is not significant due to the low WiFi traffic.

Since the DSL service in Lake Meadows Apartment does not support high data traffic, we use the Optical Wireless Integration Research Laboratory (OWIL) located in the basement of the

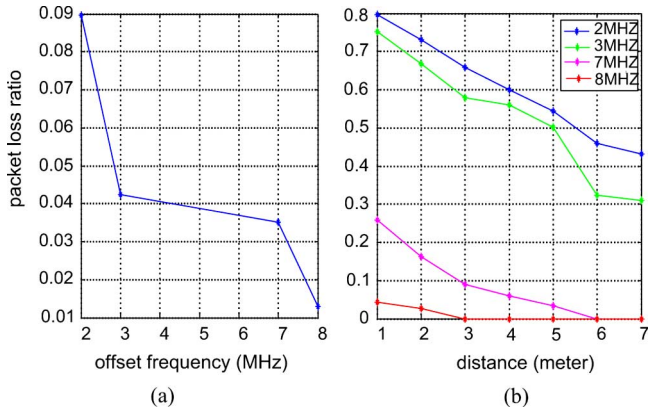

Fig. 12. PER of ZigBee measured at: (a) residential environment and (b) laboratory environment.

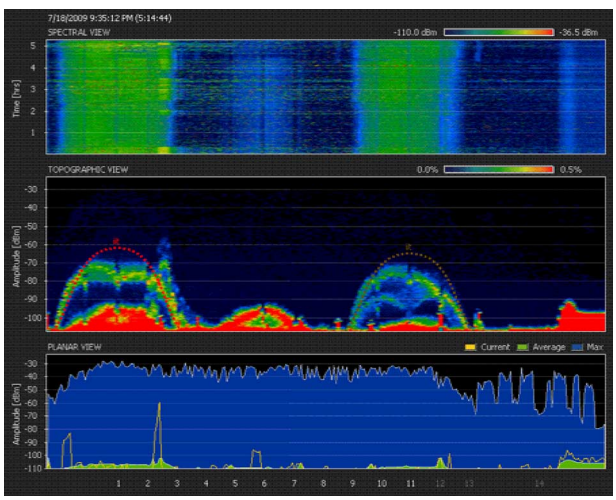

Fig. 13. Power spectrum of ZigBee and WiFi at OWIL.

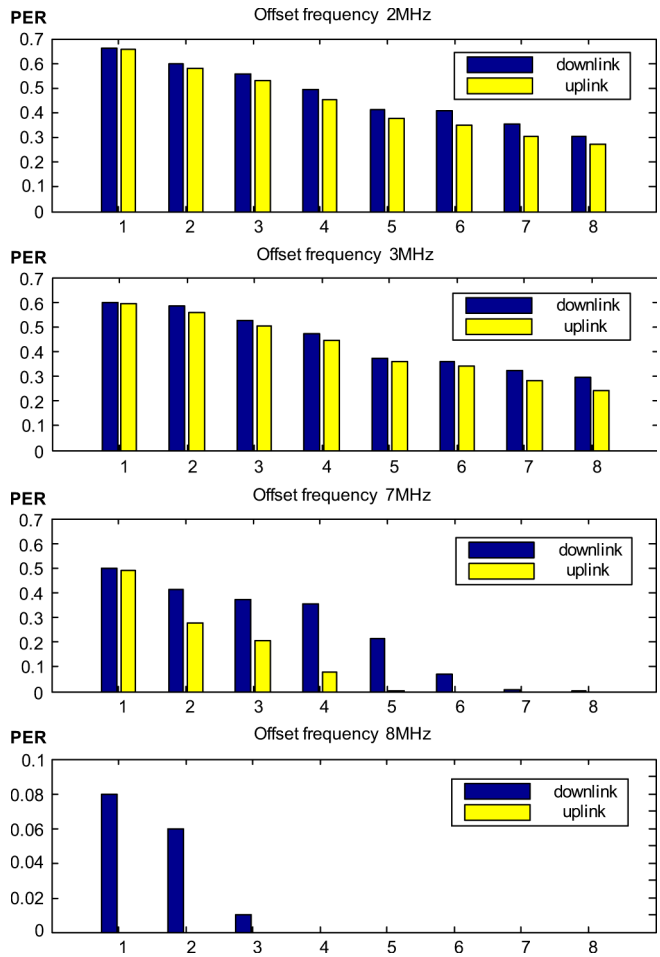

Fig. 14. PER VS. Distance (meter) at OWIL.

Siegel Hall building on the IIT Main Campus to test the performance under high interference. The whole IIT campus is WiFi enabled, with APs carefully deployed in a controlled manner to reduce the interference among multiple APs. Fig. 13. shows the power spectrum measured in the Lab, with the ZigBee signal clearly identified at 8 MHz offset from the WiFi channel center frequency. We generate heavy traffic (i.e., heavy WiFi interference to ZigBee) at the rate of 4.5 Mbps between two laptops through router and vary the distance between the access point and the ZigBee receiver from 1 m to 7 m. Fig. 12(b) shows that the PER is much higher under the heavy interference. It is also shown that when the offset frequency is set 8 MHz, the performance of ZigBee is always acceptable.

We further compare the impact from the uplink communication with the one from the downlink communication in WiFi. In this experiment, we use a pair of 2.4 GHz Meshnetics MeshBean full-function ZigBee modules to sipport more functions. Instead of using two laptops, we use one laptop and one PC desktop to connect to the WiFi network so that we only have a single wireless link for either uplink or downlink communication, but not both. To create uplink traffic, we let the laptop send file to the PC through WiFi, while to create the downlink traffic, we let the laptop download file from the PC through WiFi.

From the test results shown in Fig. 14 we observe that the WiFi downlink traffic causes more interference than the uplink traffic. This is due to the difference in the transmit power from the router and the laptop. In our experiments, the WiFi router's transmit power is set at default value, which is measured as -35.21 dBm by the WiFi spectrum analyzer. The laptop output power is measured as -42 dBm, which is lower than the router output power. Again, the results show the performance of ZigBee can be improved dramatically when the offset frequency is larger than 8 MHz.

In order to verify the developed design guideline applicable in multiple AP scenario, we extend the experiment to a two AP WiFi system. To measure the performance of ZigBee under the severe WiFi interference, we generate streaming video traffic over WiFi at 4.5 Mbps with two APs operating on the same channel. Due to the use of CSMA/CA, the maximum data rate per AP in the two-AP system is reduced to half, compared to a single AP case. Compared with ZigBee channel 12 at same distance, the PER for ZigBee channel 14 drops dramatically as shown in Fig. 15. Thus the results in a two-AP scenario are comparable to those in a single AP environment so our "safe distance" and "offset frequency" guidelines and interference avoidance scheme are applicable in multi-AP environments.

In summary, ZigBee can work well when WiFi traffic is not heavy. With increasing traffic, ZigBee needs more distance

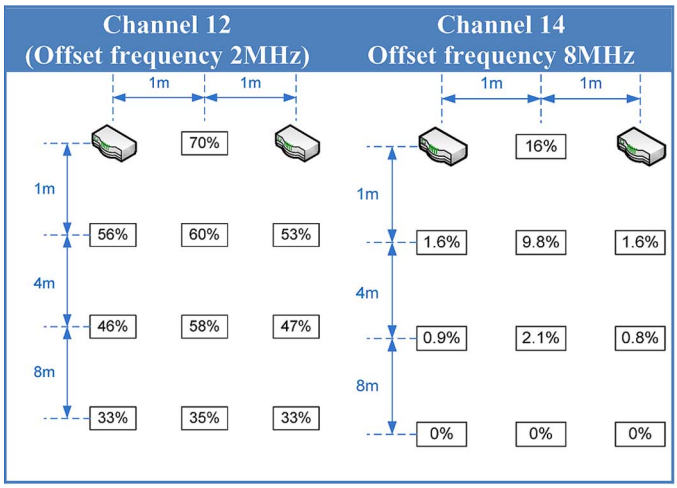

Fig. 15. PER under two WiFi APs.

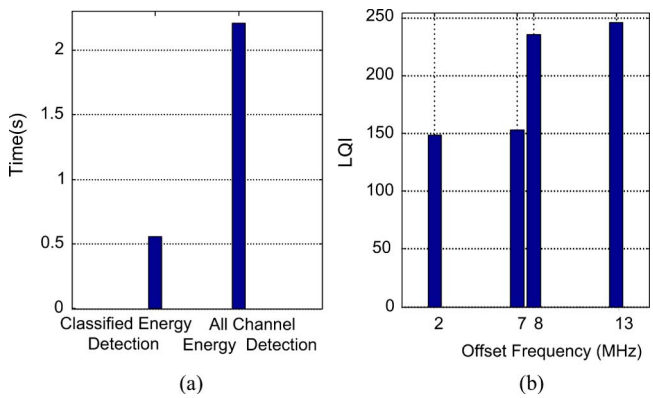

Fig. 16. (a) Energy detection duration and (b) LQI versus offset frequency.

away from WiFi or more offset frequency to avoid strong interference from WiFi. The empirical experiment results match theoretical analysis and simulation results in term of "safe distance" and "safe offset frequency."

B. Interference Detection

Obtaining accurate energy detection results within a short time is the key step to guarantee the effectiveness of any interference avoidance scheme. We conduct a large number of tests on the ZigBee nodes and find that energy detection (ED) scan duration of 138 ms provides the best balance between the scan duration and accuracy. Our tests show that 100% percent of best channel are in class 1 when we scan all 16 channels with a single WiFi AP serving as the interferer. The implication is that a scan of only class 1 channels provides the same result as a complete scan of 16 channels. We can see from the Fig. 16(a) that a scan of class 1 channels can save 75% time on energy detection.

LQI is a parameter that indicates the strength or quality of received packet. The range of LQI values is from 0 to 255 and the PER decreases as the LQI increases. The LQI measurement is performed for each received packet. If a packet is lost, the transceiver sets LQI as 0. We analyze the LQI readings from 4600 packets transmissions for each channel. Fig. 16(b) illustrates the relationship between the average LQI and the offset frequency. It shows that for ZigBee channels with a small offset frequency to the WiFi central frequency, the link quality is bad and transmission packet strength is weak. When the offset frequency is

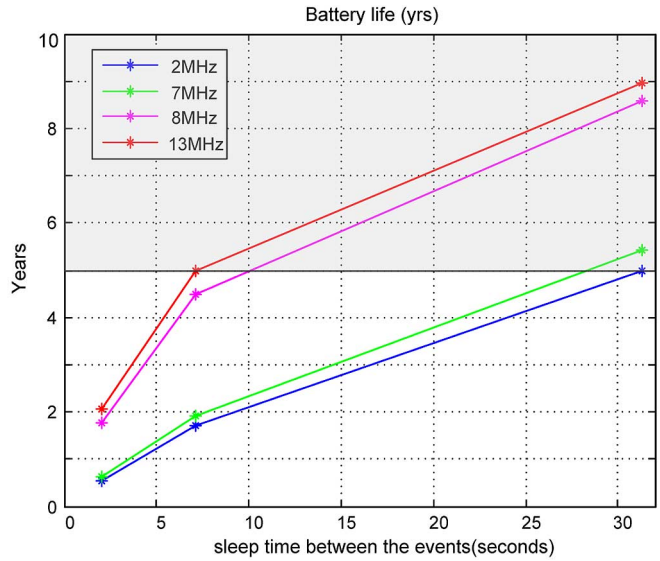

Fig. 17. Battery life performance.

larger than 8 MHz, the LQI is larger than 220, which means PER is close to 0 [26].

Energy consumption is calculated based on the PER and battery life analysis [10]. ZigBee sleep duration between active events limits to 2 s to 4000 s, while the battery life is around five years. We assume battery capacity is 1000 mAH, battery efficiency is 50% and retransmission times equal to 10. If the PAN operates under heavy interference, a high PER leads to a large amount of retransmission which results in wasted energy throughout the sensor network. Fig. 17 shows that if we choose a less interfered channel, battery life can be prolonged by up to 2–3 more years with the same sleep time between events.

VIII. Conclusion

In this paper, we have thoroughly evaluated ZigBee performance under WiFi interference for smart grid applications. A theoretical model has been introduced, followed by a corresponding simulation model which completely reflects the ZigBee and WiFi coexistence features via MATLAB/Simulink. Both analysis and simulation results show that ZigBee may be severely interfered by WiFi and that a "Safe Distance" and "Safe Offset Frequency" can be identified to guide ZigBee deployment. It is shown that 8 m between ZigBee and WiFi is a "safe" distance which can guarantee the reliable ZigBee performance regardless of the offset frequency, while 8 MHz is a "safe" offset frequency even when the distance is just 2 m. These results have been verified by means of empirical analysis and experimentation. We have shown that in general, ZigBee provides satisfactory performance when the WiFi interference is not significant. In the event of significant WiFi interference, our proposed interference mitigation scheme provides an effective and efficient means of providing reliable data service. Our system enhances the ZigBee performance to provide robust and reliable service in coexistence with WiFi networks.

Acknowledgment

The authors thank Prof. Mohammad Shahidehpour for discussions and suggestions concerning this work.

REFERENCES

[1] Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0∗ , 2010.

[2] ZigBee Alliance, ZigBee Specification: ZigBee Document 053474r17 2008.

[3] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Feb. 2010.

[4] Zensys, White Paper: WLAN Interference to IEEE 802.15.4, 2007.

[5] S. Y. Shin, H. S. Park, S. Choi, and W. H. Kwon, "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2825–2830, 2007.

[6] G. Thonet and P. Allard-Jacquin, ZigBee-WiFi coexistence white paper and test report, Schneider Electric White Paper, 2008.

[7] P. Yi, A. Iwayemi, and C. Zhou, "Frequency agility in a ZigBee network for smart grid application," in *Proc. Innovative Smart Grid Technol. (ISGT)*, 2010, pp. 1–6.

[8] K. Shuaib, M. Alnuaimi, M. Boulmalf, I. Jawhar, F. Sallabi, and A. Lakas, "Performance evaluation of IEEE 802.15.4: Experimental and simulation results," *J. Commun.*, vol. 2, no. 4, pp. 29–37, Jun. 2007.

[9] I. Howitt and J. Gutierrez, "IEEE 802.15.4 low rate—wireless personal area network coexistence issues," in *Proc. IEEE Wireless Commun. Netw. (WCNC 2003)*, pp. 1481–1486.

[10] ZigBee Alliance, ZigBee and Wireless Radio Frequency Coexistence 2007 [Online]. Available: http://www.zigbee.org/imwp/download.asp?ContentID=11745

[11] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance Study of IEEE 802.15.4 Using Measurements and Simulations," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC 2006)*, pp. 487–492.

[12] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Co-existence of ZigBee and WLAN, a performance study," in *Proc. 2006 IFIP Int. Conf. Wireless Opt. Commun. Netw.*, pp. 1–5.

[13] C. Won, J. Youn, H. Ali, H. Sharif, and J. Deogun, "Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b," in . *Proc. IEEE 62nd Veh. Technol. Conf. (VTC 2005 Fall)*, pp. 2522–2526.

[14] M. Kang, J. Chong, H. Hyun, S. Kim, B. Jung, and D. Sung, "Adaptive interference-aware multi-channel clustering algorithm in a ZigBee network in the presence of WLAN interference," in *Proc. 2007 2nd Int. Symp. Wireless Pervasive Comput.*, pp. 200–205.

[15] T. Rappaport, *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ: Prentice-Hall, 2001.

[16] R. L. Peterson, D. E. Borth, and R. E. Ziemer, *An Introduction to Spread-Spectrum Communications*. Upper Saddle River, NJ: Prentice-Hall, 1995.

[17] D. G. Yoon, S. Y. Shin, W. H. Kwon, and H. S. Park, "Packet error rate analysis of IEEE 802.11b under IEEE 802.15.4 interference," in *Proc. 2006 IEEE 63rd Veh. Technol. Conf.*, pp. 1186–1190.

[18] S. Y. Shin, H. S. Park, and W. H. Kwon, "Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b," *Comput. Netw.*, vol. 51, no. 12, pp. 3338–3353, Aug. 2007.

[19] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11-2007 Part 11, 2007.

[20] *: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Std. 802.15.4a-2007, 802.15.4a Part 15.4, 2007.

[21] G. Zhou, T. He, J. Stankovic, and T. Abdelzaber, "RID: Radio interference detection in wireless sensor networks," in *Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc.*, 2005, pp. 891–901.

[22] S. M. Kim *et al.*, "Experiments on interference and coexistence between ZigBee and WLAN devices operating in the 2.4 GHz ISM band," in *Proc. NGPC*, Nov. 2005, pp. 15–19.

[23] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Newton, MA: Newnes, 2008.

[24] R. C. Shah and L. Nachman, "Interference detection and mitigation in IEEE 802.15.4 networks," in *2008 Int. Conf. Inf. Process. Sensor Netw. (IPSN 2008)*, pp. 553–554.

[25] J. Mikulka and S. Hanus, "Bluetooth and IEEE 802.11b/g coexistence simulation," *Radio Eng.*, vol. 17, no. 3, pp. 66–73, Sep. 2007.

[26] Atmel Corp, RF230: Low power 2.4 GHz transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE and ISM applications, 2009.

Peizhong Yi (S'10) received the B.S. degree in telecommunication from Xi'dian University, Xi'an, China, in 2007, and the M.S. degree in electrical engineering from Illinois Institute of Technology (IIT), Chicago, in 2009. She is currently working toward the Ph.D. degree in the Computer Engineering Department, IIT.

Her Ph.D. research concentrates on design of interference avoidance techniques of ZigBee, design and development of self-forming and self-healing cluster-tree ZigBee systems, and deployment of ZigBee wireless network in the Perfect Power project.

Abiodun Iwayemi received the B.S. degree in electrical engineering from the University of Ibadan, Nigeria, and the M.S. degree in electrical engineering from the Illinois Institute of Technology, Chicago, in 2009. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology.

His research interests lie in wireless sensor networks for smart grid applications, network science applications for critical infrastructure protection, mobile voice over IP, and quality of service for real-time data over cellular broadband networks.

Chi Zhou received two B.S. degrees in both automation and business administration from Tsinghua University, China, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from Northwestern University, Evanston, IL, in 2000 and 2002, respectively.

Between 2002 and 2006, she was an Assistant Professor at Florida International University. Since 2006, she has served as an Assistant Professor in the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago. Her primary research interests include wireless sensor networks for smart grid application, scheduling for OFMA/MIMO systems, network coding for wireless mesh networks, and integration of optical and wireless networks.