WizBee: Wise ZigBee Coexistence via Interference Cancellation with Single Antenna

Yubo Yan*, Panlong Yang*†, Xiang-Yang Li†‡§, Yafei Zhang*, Jianjiang Lu*, Lizhao You¶, Jiliang Wang†, Jinsong Han‖ Yan Xiong**
* PLA University of Science and Technology, Nanjing, China
† MOE Key Lab, School of Software, TNLIST, Tsinghua University, Beijing, China
‡ Department of Computer Science, Illinois Institute of Technology, Chicago, USA
§ College of Computers and Software, Nanjing University of Information Science and Technology, China
¶Institute of Network Coding, Chinese University of Hong Kong
‖Department of Computer Science and Technology, Xi'an Jiaotong University, China
**School of Computer Science and Technology, University of Science and Technology of Chinay, China

Abstract—Coexistence of WiFi and ZigBee in 2.4 GHz ISM band is a long standing and challenging problem. Previous solutions either require modifications of current ZigBee protocols or WiFi re-configurations, which is not feasible in large-scale wireless sensor networks. In this paper, we present WizBee, a coexistence system using *single-antenna* sink without changing current WiFi and ZigBee design. WizBee is based on an observation that WiFi signal is about 5 dB to 20 dB stronger than ZigBee signal in symmetric area, which leaves much room for applying interference cancelation technique to mitigate WiFi interference, and extract ZigBee signals. However, we need to cancel the WiFi interference perfectly for residual ZigBee signal decoding, which needs more accurate channel coefficient across data transmissions in spite of cross technology interference. For robust and accurate WiFi decoding, we use soft Viterbi decoding with weighted confidence value over interfered subcarriers. Consequently, our solution uses decoded data for channel coefficient estimation instead of conventional training symbol based methods. The key insight is that, the signal recovery opportunity for cross technology coexistence, lies in multi-domain information, such as power, frequency and coding discrepancies. Using these information properly will improve the coexistence network throughput effectively.
We implemented WizBee in USRP/GNURadio software radio platform, and studied the decoding performance of interference cancelation technique. Our extensive evaluations under real wireless conditions show that WizBee improves ZigBee throughput up to $1.9\times$, with median throughput gain of $1.2\times$.

Index Terms—Cognitive networks, Physical Layer, Sensor Networks

1 Introduction

The past decade has witnessed a wide use of 802.15.4-based wireless sensor networks (*i.e.* ZigBee networks)[1] in the area of medical health care [24], environment monitoring [18] [26], *et al.*. In particular, there are increasing interest on deploying them to provide real-time and long-term monitoring in urban area, *e.g.*, CitySee [19]. ZigBee networks share the same 2.4 GHz-ISM band with WiFi networks, which are often widely deployed in urban area to provide ubiquitous Internet access. However, it imposes a coexistence issue with difficulty. Recent studies [17] have shown that ZigBee's performance degrades dramatically during busy WiFi traffic.

Several types of solutions have been proposed to address the cross technology coexistence. The first type of approach is to do centralized frequency planning beforehand, separating different technologies in non-overlapping spectrums. The second type of approach [8], [9], [23], [31] requires the wideband devices (*e.g.*, WiFi) to vacate the spectrum being used by narrowband devices (*e.g.*, ZigBee), thus achieving interference-free coexistence in frequency domain. The third approach designs novel ZigBee protocols (*e.g.*, predication [10], recovery [17], prevention [28], [32]), or customized preambles [22] to ensure ZigBee networks interference-free from WiFi networks in time domain.

Unfortunately, such solutions cannot be easily deployed in urban monitoring scenario for several reasons. First, WiFi networks in urban area are uncontrolled and unpredictable, especially in residential area, which makes centralized coordination and modification of WiFi devices infeasible. Second, these aforementioned novel protocol solutions either consume computation resource at weak sensor nodes, or require network coordination, leading to severe overhead. Third, some of these novel solutions mentioned above require re-programming of ZigBee nodes, and reduce the performance of WiFi networks, which are not feasible in large-scale and long-term urban monitoring scenario.

To tackle these challenges, we present WizBee (*i.e.* Wise ZigBee system), an extension to current ZigBee networks with intelligent sink node. The design of Wiz-

1. In this paper, we make no distinction between IEEE 802.15.4 standard and ZigBee, because we mainly focus on PHY/MAC layer. It also applies for IEEE 802.11 standard and WiFi.

Bee is motivated by the observation that WiFi signal is much stronger than ZigBee signal when they collide, leaving much room for applying interference cancellation technique, especially in symmetric area [17]. To recover ZigBee packet during WiFi/ZigBee collision, WizBee first extracts WiFi packet, then subtracts WiFi interference and decodes ZigBee packet. To provide such collision resolution capability, WizBee adds WiFi interference management component, and redesigns existing sink architecture. The novel design allows concurrent access of WiFi and ZigBee packets. Furthermore, the redesigned architecture is capable for connecting with multiple ZigBee networks using orthogonal channels.

Notably, such design is non-trivial and challenging. WizBee could coexist ZigBee signal with WiFi using only one antenna, which is fundamentally different from previous MIMO based scheme [4] [1], as well as other single antenna schemes needing additional aiding nodes [32]. For single antenna design, we especially need more robust and accurate WiFi signal decoding scheme, even in presence of the ZigBee interference. Also, as the decodable signal need to be reconstructed for interference cancellation, more accurate channel coefficient estimation as well as effective interference boundary detection are needed.

We use two innovative methods to address these two challenges. First, we use soft Viterbi algorithm on each subcarrier for confident interval evaluation. Cross technology interference differs from distinctive subcarrier, and this information can be leveraged for robust WiFi data decoding. Second, we use the decoded data as training sequences for frequency offset compensation in channel coefficient estimation, which differs short training symbol and long training symbol methods. We find that, for WiFi interference cancellation, the historical data can be also used for coming data correction iteratively. Our key insight in WizBee is that, for cross technology coexistence, there are opportunities in power, frequency and coding domain, because different configurations will provide multi-domain hints for interference mitigation and signal recovery. Also, the schemes in WizBee successfully close the gap between WiFi and other ISM band technologies, as ZigBee is similar to WiFi in many aspects and bearing fully semantic information.

WizBee presents several attractive properties. First, unlike previous solutions that either sacrify ZigBee performance or WiFi performance, WizBee achieves coexistence without intervention. WizBee does not need to suppress WiFi interference to ZigBee, thus improving ZigBee's throughput without affecting WiFi's network latency. Second, WizBee is a seamless solution, providing seamless backward compatibility. In spite of adding a new sink device, WizBee is a very practical solution: it requires no modification of existing ZigBee protocols and existing deployed ZigBee nodes. Also the extra cost of adding sink is likely to be small compared with redeployment of massive sensor nodes. We envision the WizBee approach could also seamlessly support future home wireless networks [21], where many WiFi-based and ZigBee-based wireless devices are equipped pervasively.

We make the following contributions in this paper:

- We revisit the coexistence problem in urban monitoring scenario, and propose a novel WizBee solution based on WiFi interference cancellation technique to enhance ZigBee networks performance. Our solution uses single antenna, leveraging the significant power discrepancy between WiFi and ZigBee signals. To the best of our knowledge, WizBee is the first system design to effectively coexist WiFi and ZigBee signals with only one antenna, where no more modifications are needed for WiFi and ZigBee devices.
- We propose an innovative interference cancellation scheme for ZigBee signal coexistence, where WiFi decoding is used for channel coefficient estimation in an iterative way. For accurate and robust WiFi decoding, we apply soft Viterbi decoding scheme across different subcarriers. As only portion of subcarrier is interfered, such scheme could evaluate different confidence among subcarriers, which helps improve the decoding robustness. Also, a data-aided channel coefficient computation scheme is put forward for frequency offset compensation.
- We have implemented WizBee in USRP/GNURadio platform, and characterized the cancellation performance. Extensive evaluations show the performance gain over existing systems. Evaluations under real wireless conditions show that WizBee can improve $1.6\times$ throughput for ZigBee networks over 80% cases, with median throughput gain of $1.2\times$. More importantly, we have presented a 'decodable' SNR range when WiFi and ZigBee signals are coexisted with only one antenna. For one antenna system, the range is 5dB to 20dB, *i.e.*, the WiFi signal is at least 5dB higher than ZigBee signal. Such constraint can be easily satisfied in symmetric range.

The rest of the paper is organized as follows. In section 2, we provide background on ZigBee and WiFi systems, and specific characteristics of WiFi&ZigBee signals. Also, We overview the system design in Section 3. After describing our system design in detail for the interference mitigation process in Section 4, and implementation in Section 5, we evaluate the performance of WizBee in Section 6. Further, we discuss the relevant MIMO design and introduce related work in Section 6.4 and Section 7 respectively. Finally, we conclude the work in Section 8.

2 PRELIMINARY

2.1 Background on 802.11 and 802.15.4

WiFi and ZigBee are targeted at different applications. WiFi is designed for high-throughput transmission, but in need of high-power. While ZigBee is designed for low-cost industry control, e.g., environment monitoring,

showing the low-power merit. WiFi (11g) can support transmission rate from 6Mbps to 54Mbps using Orthogonal Frequency Division Multiplexing (OFDM) technique[2], while ZigBee's (IEEE 802.15.4) transmission rate is only 250Kbps using Direct Sequence Spread Spectrum (DSSS) technique in 2.4GHz ISM band. Thus, for transmitting a typical WiFi packet with 1500 bytes, WiFi needs at most 2ms. For transmitting a maximum-length packet (127 bytes), ZigBee needs about 4ms. In MAC layer, both technologies use CSMA/CA mechanism to coordinate channel access, and rely on Clear Channel Avoidance (CCA) mechanism to detect whether the carrier is idle.

Recent studies have shown that ZigBee is vulnerable to WiFi, while not vice versa in necessary. Two key reasons lead to this phenomenon. First, WiFi's transmission power is about 10 to 100 times higher than ZigBee [17], [32], leading to poor sensibility of ZigBee devices to WiFi devices under threshold-based CCA mechanism. Therefore, ZigBee devices are possibly affected by high-power WiFi devices. Second, due to ZigBee's low data rate and low cost, the time resolution ability is relatively coarse and slow. For example, the backoff time slot in ZigBee system is 320μs, and CCA operation delay is 128us. The TX/RX switching time can be up to 192μs. On the other hand, for WiFi (IEEE802.11g), the time slot is 9μs, and the CCA detection time is less than 4μs. Shorter basic operation times of WiFi system make it easy to win the channel contention. The readers can refer to [17], [32] for a detailed explanation of packet confliction and resolutions schemes.

2.2 Characteristics of WiFi/ZigBee Signal

To have a deep understanding on why WizBee can deal with collision signal, we show the characteristics of WiFi and ZigBee signals in frequency and time domains. To present the signal-level signature, we use USRP/GNURadio software radios to collect real-time traces, and analyze them in off-line mode.

As we stated before, WiFi uses 20MHz spectrum bandwidth while ZigBee uses 2MHz. Besides, their central working frequencies are also different. Even though in the same 2.4GHz ISM band, there are still four orthogonal and interference-free channels from WiFi channels. Hence in one single WiFi channel, there are at most four ZigBee channels overlapping with it. Without loss of generality, we consider a particular co-channel example: WiFi uses channel 6 (with 2.437GHz as its central frequency), and ZigBee uses channel 17 (in 2.435GHz central frequency).

3 WizBee Overview

3.1 Problem Domain

The reason for investigating the one-antenna solution is two-folds. First, one antenna system is still widely existed in nowadays communication system. Although adding one or more antennas for MIMO system is beneficial and applicable, investigating the interference management capability for one antenna system is still needed, because mining the one-antenna potential capability still helps to enhance the multi-antenna system. For example, a 3-antenna system, if two antennas are leverage to receive 2 MIMO signals and the other one will also need to deal with the coexistence problem where 2 heterogeneous wireless signals are concerned.

Second, we find that, in one antenna system, the signal strength, that is, the receiving energy plays important role. And in real network deployment, when WiFi interference is heavy, and quite often, the signal strength of WiFi is significantly larger than ZigBee signal. There are fruitful of opportunities in leveraging this effect to recover WiFi signal and help to improve the ZigBee network throughput.

3.2 Design Overview

In this section, we present an overview of WizBee system. WizBee is designed to be compatible with current ZigBee and WiFi system, and do not need any protocol modification. The only requirement is to replace conventional ZigBee sink with WizBee sink. Figure 1 shows a typical scenario where WizBee, WiFi and ZigBee systems are working together. For the two sensor networks in this scenario, one uses conventional ZigBee sink (the right most ZigBee network in Figure 1), and the other uses WizBee sink (the left most ZigBee network). Sensor nodes are collecting and reporting real-time data to sink node. The WiFi access point is providing data service to WiFi clients at the same time, leading to severe WiFi interference. Obviously, the conventional ZigBee sink cannot decode the ZigBee signal in presence of WiFi interference. However, with proper WiFi interference cancellation design, WizBee sink can decode the collided signal. Therefore, the interfered signal of WizBee sensor network can be recovered, while the conventional ZigBee sensor networks suffer from interference.

Fig. 2 shows the system architecture of WizBee, including the RF front-end, spectrum component, WiFi interference management, and ZigBee physical layer (ZigBee PHY). RF front-end utilizes wide-band sampling and transmission, which can be used for managing several orthogonal ZigBee channels. Spectrum component is used to filter out samples of interested channel for decoding, or combine samples from several channels. Interference management block takes in charge of WiFi interference detection, estimation and cancellation, which is a key component of WizBee. Finally, WizBee includes standard ZigBee physical layer for modulation and demodulation.

4 Design of WizBee

In this section, we describe WizBee design in details. Before diving into details, we first illustrate how WizBee

2. WiFi in 2.4GHz ISM band includes IEEE 802.11b/g/n standard. We focus on 802.11g/n standard, since OFDM has become the standard physical layer for next-generation wireless communication (e.g., LTE, WiMAX).

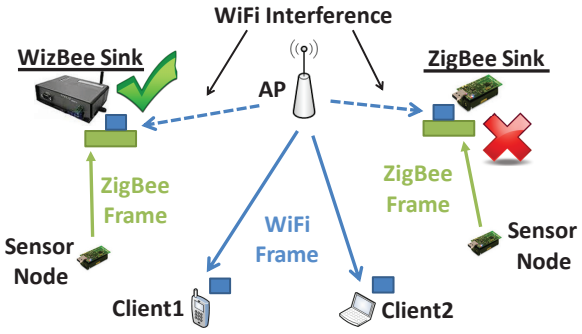


Fig. 1: Illustration of coexistence of WizBee, ZigBee and WiFi systems: under WiFi interference, conventional ZigBee sink can not decode collided ZigBee packet, while our WizBee sink can.

sink works. Taking uplink packet reception for example, WizBee sink works in following seven steps: The signal from the RF front end will be processed firstly for spectrum slicing and combining. If the WiFi interference is detected, WizBee will process the WiFi decoding, and use decoded data for accurate channel coefficient estimation. After that, the WiFi signal is mitigated by interference cancellation module, where the residual signal can be used for ZigBee decoding.

4.1 Spectrum Slicing/Combining

In order to incorporate several ZigBee orthogonal networks and WiFi signal cancellation, WizBee uses wideband RF front-end. However, wideband sampling means that the sampled signal has a wide spectrum, which can not be used for decoding directly. The spectrum slicing block tries to convert sampled signal to suitable signal for ZigBee decoding. In this paper, we use typical WiFi setup (*e.g.* WiFi channel 6: 2.437 GHz, 20 MHz bandwidth) to determine front-end parameters (complex sampling rate: at least 20 MHz).

We first assume there is no WiFi interference during ZigBee's communication. Suppose $x_z(t)$ be sampled value from ZigBee packet, and H_z be the corresponding channel coefficient of ZigBee transmission. Then we have $y(t) = H_z x_z(t) e^{j2\pi\delta_f t} + n(t)$, where y is the reception signal, and δ_f is the central frequency offset between WiFi and interested ZigBee signal, and $n(t)$ is the background noise.

The spectrum slicing/combining design includes three steps: frequency translation, FIR filtering and re-sampler. The goal of frequency translation step is to get rid of frequency offset δ_f, which can be achieved by multiplying the incoming signal with $e^{-j2\pi\delta_f t}$. Since the bandwidth of WiFi is 20 MHz, which is larger than 2 MHz (the information is not lost due to Nyquist sampling theorem), we can use $e^{-j2\pi\delta_f t} y(t)$ to extract ZigBee packet. To improve the SNR of ZigBee reception channel, we add an FIR filter to filter out unwanted out-of-band noise. Then we employ a re-sampler block lowering down the sampling rate to improve the decoding speed while retaining necessary signal information.

The spectrum combining block design in transmission chain is just the reverse process, so we omit the details. For extension to multiple orthogonal ZigBee networks, we only need to add parallel reception chain with different frequency translation parameters.

4.2 Interference Detection

In our design, WizBee invokes the interference cancellation block only if it confirms the WiFi transmission starts. To do so, we take the standard auto-correlation approach that has been widely adopted to detect WiFi packets for the WiFi interference detection. The key idea is to exploit repeated patterns in short training symbol (STS) of WiFi packet. The auto-correlation means summing up the multiplications between the received signal and its delayed form. Let r_t denote the t^{th} sample, and L denote the length of the meta-repeating. The auto-correlation output can be represented as

$$c_n = \sum_{k=0}^{L-1} r_{n+k} r^*_{n+k+L},$$

where r^*_t is the conjugate of the t^{th} sample.

In order to yield a normalized result, we need to calculate

$$p_n = \sum_{k=0}^{L-1} r_{n+k+L} r^*_{n+k+L} = \sum_{k=0}^{L-1} |r_{n+k+L}|^2.$$

The final auto-correlation result is $m_n = |c_n|^2/(p_n)^2$, which means the correlation of current samples with past samples essentially. Only when a real WiFi packet comes, the auto-correlation output m_n is about to approach 1, because the real WiFi packet includes ten repeated sequences. Otherwise, the randomized noise would not give a high m_n.

For WiFi packet boundary detection, we exploit packet length information embedded in SIGNAL symbol at the beginning of a WiFi packet. Also, the dramatic power decrease at the end of WiFi packet (in our current implementation we use 10 dB) could help us to check the packet boundary.

4.3 WiFi Decoder

There are mainly three components for WiFi decoding: synchronization, channel estimation and demodulation.

Synchronization is achieved by exploiting the preamble of WiFi frame, including Short Training Symbols (STS) and Long Training Symbols (LTS). There are three steps in synchronization: frame synchronization, carrier frequency synchronization and symbol timing synchronization. Frame synchronization and carrier frequency synchronization are performed by using the 10 repeated STS. We use auto-correlation to perform frame synchronization as described in Section 4.2. While, CFO is derived by a data-aided maximum-likelihood estimator.

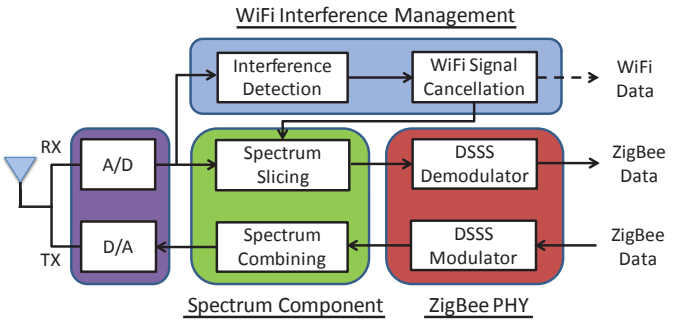


Fig. 2: System Architecture of WizBee, including RF front-end, spectrum component, WiFi interference management, and ZigBee PHY. The WiFi data is an optional output.

Let the transmitted signal be s_n, the carrier frequency offset be f_Δ, and sampling time be T_s, then the received complex baseband signal r_n is

$$r_n = s_n e^{j2\pi f_\Delta n T_s}$$

Let D be the delay between the identical samples of the two repeated symbols. Denoting $z = \sum_{n=0}^{L-1} r_n r_{n+D}^*$, we can derive

$$z = e^{-j2\pi f_\Delta D T_s} \sum_{n=0}^{L-1} |s_n|^2$$

The CFO can be estimated as

$$\hat{f}_\Delta = -\frac{1}{2\pi D T_s} \arctan z$$

.

Finally, the received signal can be compensated as

$$\hat{r}_n = r_n e^{-j2\pi \hat{f}_\Delta n T_s}$$

Symbol timing synchronization is achieved by using LTS. After CFO compensation, we use cross correlation method between LTS and the received signal for symbol level synchronization. Then the Cyclic Prefix (CP) is removed accordingly. A Fast Fourier Transform (FFT) is carried out to transform the received signal from time domain to frequency domain.

Channel estimation is performed with a frequency domain approach. The channel estimation can be calculated as

$$\hat{H}_k = (R_{1,k} + R_{2,k}) X_k^*$$

where $R_{1,k}$ and $R_{2,k}$ are the received LTS, X_k is the transmitted LTS, X_k^* is the conjugated form of X_k, and H_k is the channel response of subcarrier k.

Demodulation include phase error tracking, symbol decision, de-interleaving and Viterbi decoding. We exploit 'pilot subcarrier' for phase error tracking. After the receiver performed the aforementioned synchronization, we use soft decision technique to decide what is the most likely transmitted symbol for each received symbol. Then, de-interleaving and Viterbi decoding is performed to get the most likely bits.

For robust WiFi decoding, we use soft Viterbi algorithm. It use additional information to indicate the confidence of the input decisions, and produces a more accurate estimation of transmitted codes. Such good character enables us to design robust WiFi decoding. Note that, in frequency domain, the ZigBee signal can only interfere portion of subcarriers, and we can know the exact subcarriers through previous spectrum slicing scheme. Taking advantage of this merit, we assign different weights to subcarriers. For the interfered subcarriers, the 'ZigBee noise' should be evaluated for its SNR value. We omit the detailed soft output Viterbi algorithm design as it can be referenced in classic books [27] and web site [29].

4.4 Accurate WiFi Channel Coefficient Estimation

To estimate H_w accurately, we leverage the known long training symbols (LTS) at the beginning of a WiFi packet. The estimation algorithm is called least square algorithm, which is widely used due to its low complexity. Note that OFDM modulates bit information in frequency domain (*i.e.* subcarriers). Therefore, we estimate the frequency response of the channel as a complex value at each subcarrier. Suppose $X_m = (X_m[0], \cdots, X_m[n-1])$ is the m^{th} training symbol used in the n subcarriers, and $Y_m[k]$ be the corresponding value of k^{th} subcarrier. The frequency response of each subcarrier k can be represented as: $\hat{H}_m[k] = \frac{Y_m[k]}{X_m[k]}$.

In practice, there are several symbols used for channel estimation, and we can average over all estimation $\hat{H}_m[k]$ to get a more accurate $\hat{H}[k]$. After getting channel frequency response, we can apply the inverse fast Fourier transform (IFFT) to obtain the channel impulse response. Then the channel impact on transmission samples is easy to be emulated using a standard finite impulse response (FIR) filter.

However, there are two weaknesses when appling this approach in our scenario. First, since WiFi standard defines 64 subcarriers but only uses 52 data subcarriers, there are 12 zero subcarriers left. It is hard to estimate channel frequency response in those zero subcarriers. In other words, we cannot get accurate channel impulse response, which may lead to high residual noise. Second, the channel estimation using long train symbol is not enough, and pilot phase tracking is very important. It is difficult to apply phase rotation using FIR filter approach, which can also lead to high residual noise. Therefore, we implement signal cancellation in the frequency domain symbol by symbol. The canceled signal in frequency domain can be represented as $(H[k] - \hat{H}[k]) X_w[k]$. Then we use IFFT to obtain the signal in time domain.

We also note that, another main reason leading to inaccurate channel coefficient is frequency offset between Tx and Rx terminals. We propose a linear model for frequency offset compensation. With the accumulated symbols over time, our linear model can automatically

adjust the frequency between Tx and Rx nodes, and will not be affected by the transmission duration.

Another issue is that we need to cut Cyclic Prefix (CP) in OFDM symbol carefully. CP is an important design in OFDM systems to combat inter-symbol interference, and relax the time synchronization accuracy. However, in our interference cancellation scenario, we need to calculate the exact symbol boundary. Otherwise, we cannot reconstruct the complete OFDM symbol in time domain. We use cross-correlation technique, which means correlating incoming signal with pre-known symbol (long training symbol). When getting the maximum peak value, we can find the symbol being distorted in channel. In this way, we can judge the exact symbol boundary accurately.

4.5 Interference cancellation

The key design of WizBee is based on the observation that it is possible to decode WiFi and ZigBee packets even when they access the channel at the same time, because the signal strength of WiFi is always 5∼20dB stronger than that of ZigBee due to high transmit power [17]. Therefore, we can first regard ZigBee signal as background noise, and apply standard decoder to decode WiFi packets. Given enough SNR of WiFi signal, it is possible to first decode WiFi packet. Then, we remodulate the transmission signal, add the real channel impact, and use Interference cancellation (IC) technique [2] to subtract the strong known WiFi signal. If we can mitigate WiFi signal from the mixed signal, we can use standard ZigBee decoder to extract ZigBee packets. The overall processing is called Successive Interference Cancellation (SIC), which is a useful tool for dealing with diverse power transmissions.

In achieving higher accuracy of the signal recovery, we consider the mixed (collided) signal $y(t)$, and downsample it using central frequency with the bandwidth of WiFi system. Let $x_w(t)$ be the signal from WiFi, and $x_z(t)$ be the signal value from ZigBee. Then we have

$$y(t) = H_w x_w(t) + H_z x_z(t) e^{j2\pi\delta_f t} + n(t),$$

where H_w and H_z are the channel coefficient of WiFi and ZigBee respectively, $n(t)$ is noise, and δ_f is the central frequency offset between WiFi and ZigBee signals.

When $H_w x_w(t)$ is much larger than $H_z x_z(t)$, we can regard $H_z x_z(t) e^{j2\pi\delta_f t} + n(t)$ as new noise $N(t)$, and get $x_w(t)$ using standard WiFi decoder. Then we re-modulate the WiFi signal as $S_w = \hat{H}_w x_w(t)$, and setup a new formula as

$$Y(t) = y(t) - S_w = H_z x_z(t) e^{j2\pi\delta_f t} + n(t).$$

In this way, we can process $Y(t)$ as in Section 4.1 to get ZigBee packet.

4.6 ZigBee Decoder

The ZigBee data decoding subsystem performs frame synchronization, phase ambiguity resolution and OQPSK demodulation, chip to symbol decoding and CRC calculation. The decision-directed phase error detector of Fine Frequency and Phase Compensation subsystem has two stable lock points at $\theta_e = 0$ and $\theta_e = \pi$ and poses a π-phase ambiguity. As a consequence, the carrier phase recovery PLL can lock to the undemodulated carrier with a phase offset. We exploit the preamble to resolve phase ambiguity. Specially, we calculate the cross correlation of input signal and modulated symbol zero (Remember that, 4-bit zeros are mapped to a 32 chip sequence. The chip sequence is then modulated to 16 complex signals). Then we estimate the phase of the cross correlation result. We classify the estimated phase into 0 and π phase offset. The input undemodulated signal is corrected with this phase offset. After phase offset compensation, the received signal is demodulated to chip sequence. This chip sequence is cross correlated with the chip sequence of symbol zero. If the cross correlation result is less than a previously defined threshold (10 in our implementation), a symbol zero of preamble is considered to be found. Once we found a preamble symbol with the estimated phase offset, we continuously search the SFD (Start of Frame Delimiter) byte in the incoming signal. If SFD is found, the physical header information can be extracted and the packet can be resembled. After the resembling is completed, the CRC of this packet can be calculated.

4.7 Downlink Design

The downlink design also involves WizBee sink and computationally weak sensor nodes. We try to accomplish downlink design by only modifying WizBee sink node. Note that our architecture allows simultaneous packet transmissions in orthogonal ZigBee channels. We can adopt the design of CCS [32] to emit jamming signal, making WiFi backoff explicitly. The key issues here are: 1) to determine how long the jamming signal is, and 2) to use which power level to jam.

It is easy to deal with the first issue, since the transmission packets are generated by WizBee sink. The complex timing calculation and network coordination in CCS [32] is no longer needed. As for the second issue, note that our interference detection block can provide WiFi signal strength information, and ZigBee decoder gives us ZigBee signal strength. Then WizBee can estimate the distance between WiFi interferer and ZigBee receiver, and adjusts the transmission power to keep ZigBee downlink transmission from being interfered by WiFi transmissions.

A notable concern is whether this design degrades the WiFi performance. We argue that for environment monitoring applications, downlink traffic is mostly ACK packets [18]. In other words, very few downlink transmissions are reserved. Moreover, since we have an accurate control of the jamming signal, the WiFi performance loss is negligible.

5 IMPLEMENTATION

We use GNURadio/USRP N200 with RFX2400 daughterboard software radios to evaluate WizBee performance, because WizBee design requires complete control on wireless physical layer (*e.g.* WiFi signal-level control), which cannot be acquired using commercial network interface cards and sensor nodes. However, due to the inherently long latency between RF and hosts, software radios cannot support precise MAC layer timing control. In other words, we cannot implement the whole system currently, especially the carrier sensing and strict MAC protocol. Therefore, we use trace-driven approach. It is worth noting that, we collect real trace data and process them with our proposed procedures. Actually, it is a real experimental validation for WizBee design.

We implement the OFDM PHY layer of WiFi and 2450 MHz PHY layer of ZigBee according to IEEE Standard 802.11 [11] and 802.15.4 [12] respectively. The WiFi and ZigBee USRP transmitters are configured to span 20 MHz and 2 MHz respectively. The PHY layer of WiFi includes a modulation choice of BPSK, QPSK, 16QAM and 64QAM and convolution codes with code rates specified in IEEE Standard 802.11 [11]. The bit rates of WiFi PHY layer in our prototype span from 6 Mbps to 54Mbps. The 2450 MHz PHY layer of ZigBee employs a 16-ary quasi-orthogonal Direct Sequence Spectrum Spreading (DSSS) and Offset Quadrature Phase-Shift Keying (O-QPSK) modulation techniques. We also implement a coherent O-QPSK receiver to decode ZigBee packets.

In order to evaluate the WizBee decoding performance under WiFi interference, we need to collect collision signals. However, it is non-trivial to synchronize two USRPs, since the packet collision happens in signal-level (μs). We exploit the time stamp mechanism provided by GNURadio community to deliberately create the WiFi/ZigBee collision. For example, ZigBee packets are sent periodically every 5 ms, and WiFi packets are sent periodically every 10 ms. Since ZigBee and WiFi have different packet length, the overlapping pattern can change as packets accumulate. Since RFX2400 daughterboard does not support hardware gain control, we adopt software-tuned approach to adjust the transmission signal strength.

6 EXPERIMENT RESULTS

In this section, we show the experiment results of WizBee implementation using GNURadio/USRP testbed. Our evaluations focus on the following questions:

- Are our WiFi/Zigbee decoders accurate enough?
- How accurate is our WiFi interference detection?
- What is the performance of ZigBee decoder after the WiFi cancellation?
- What is the throughput gain achieved by WizBee?

Our goal is to show WizBee is plausible in practical wireless environment. We conduct micro-benchmark to evaluate the performance of interference detection and interference cancellation. We then show the benefit of interference cancellation by measuring the end-to-end throughput gain of WizBee in real wireless environment.

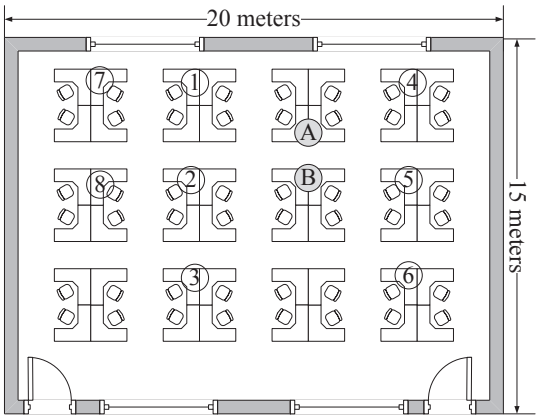


Fig. 3: Test Environment

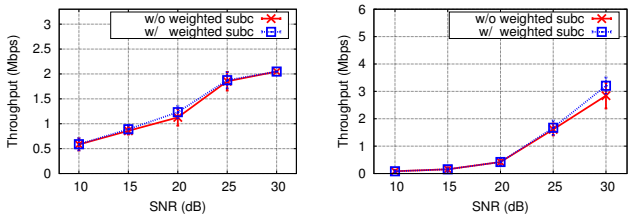
6.1 Experiment Setups

Fig. 3 shows the layout of our testing environment. It is a typical working office where tables and chair are equipped in an indoor area with walls and windows all around. Without loss of generality, we fix the channel of WiFi and ZigBee to 5 and 16, *i.e.* with center frequency of 2432 MHz and 2430 MHz. The bandwidth of WiFi and ZigBee is 20 MHz and 2 MHz respectively. In order to evaluate WizBee thoroughly, we need to collect packets with various collision patterns. However, due to the inherently unpredictable and long latency between USRP and hosts, it is non-trivial to control different USRPs to generate various collision patterns. We exploit the time stamp provided by USRP UHD driver [3] to deliberately create various collision patterns. In the following experiments, the lengths of WiFi packets are chosen from 256(BPSK), 512(QPSK) and 1024(16-QAM) Bytes according to different modulation schemes (shown after the packet length respectively), and the ZigBee packet length is set to 20 Bytes. In such a configuration, the packet transmission time is 0.36 ms for WiFi and 0.83 ms for ZigBee. The packet interval for WiFi and ZigBee packets is set to 1.5 ms and 1.612 ms respectively.

6.2 Micro Benchmark

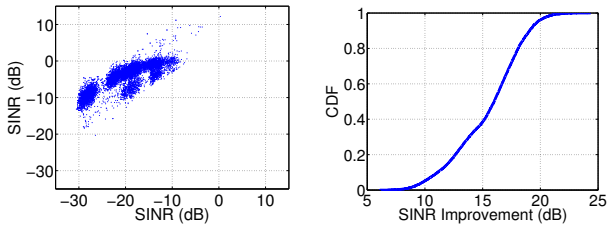
6.2.1 Interference Cancellation

We then evaluate the performance of interference cancellation with WizBee decoder. We place WizBee receiver in location A as shown in Fig. 3. The WiFi and ZigBee transmitters are placed in location 1 and 2 respectively. Due to the hardware limitations on RFX2400 daughterboard, we can not adjust the transmission gain. Thus we adjust the signal strength with software to generate signal with different SNR. The SNR values of WiFi signal are ranging from 5 dB to 30 dB. And the SNR of ZigBee packets are 5 dB and 10 dB, which are typical in real deployments [17] [18].



(a) When WiFi Modulation is QPSK (b) When WiFi Modulation is 16QAM

Fig. 4: Effects of Subcarrier Weighted Soft Viterbi Decoding



(a) SINR of WiFi Cancellation (b) CDF of SINR Improvement

Fig. 5: Performance of WiFi Cancellation. The x-axis of Fig. 5a shows SINR of the frame before the start of WiFi interference. The y-axis of Fig. 5a shows SINR after WiFi interference cancellation. The x-axis of Fig. 5b shows the SINR improvement of the frame before the start of WiFi interference.

To show the interference cancellation performance, we select modulation scheme of BPSK, QPSK and 16QAM with convolution coding rate 1/2 for WiFi nodes. The corresponding data rates are 6 Mbps, 12 Mbps and 24 Mbps for WiFi nodes, and 250 kbps for ZigBee nodes. Due to the high SINR requirement of 64QAM modulation, we omit the evaluation of this modulation scheme. Naturally, this kind of modulation may also be not suitable for transmissions in low SINR environments, especially in real network deployments.

We instruct the WiFi and ZigBee senders to transmit every 100 frames with fixed power level, modulation scheme and packet length at each trial. We dump the data at WizBee AP side. After collecting 15 traces, where 100 frames are collected in each trace, we change the transmission power, modulation and packet length for another trial.

After collecting all the traces, we exclude the traces that are severely interfered by unknown interference in our everyday working environment (*e.g.* uncontrollable WiFi APs). Then we apply interference cancellation to the overlapping frames. In evaluating the interference cancellation performance, we first remove the cases where the WiFi frame fails to decode when corrupted by ZigBee frames, since in this case, successive interference cancellation can not work. We then remove the cases where the ZigBee frame can be decoded without interference cancellation.

We defined the CSINR (cancellation based signal-to-interference-and-noise) in our study, so as to show the effectiveness of interference cancellation. CSINR is defined as $\frac{S+N}{S+I+N}$, where S is the signal energy of the first frame, I is the energy of interference frames, and N is the noise. If the interference can be successfully canceled, the ratio in our definition is 1, and the according value is 0dB. Thus, the CDF figure for IC effects will be clear.

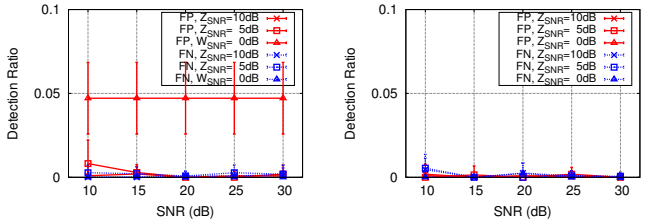
Figure. 5a shows the cancellation effects of WiFi signals. We compare the SINR value between a frame before and after the interference cancellation. It can be seen from Fig. 5a that the SINR of the frame before the start of WiFi interference are ranging from -30 dB to -10 dB, which coincides with the SNR value of WiFi frames in typical cases. After WiFi interference cancellation, the SINR are improved to -12 dB to 0 dB, which indicates that most of the WiFi interferences have been canceled effectively. It should be noted that not all the SINR before the start of WiFi interference are around 0 dB after interference cancellation. This is because ZigBee frames overlap with WiFi frames in various patterns. When the SNR of ZigBee frames is about 10 dB, and the WiFi/ZigBee frames arrive at the same time, the SINR can still around -10 dB even when the WiFi interference has been mitigated.

Figure. 5b plots the Cumulative Distribution Function (CDF) of the improvement of SINR. We can observe that interference cancellation can effectively mitigate at least 8 dB WiFi interference. Also, we can find that, most of the SINR improvement (over 80%) is around 10∼20 dB.

6.2.2 *Frame Detection*

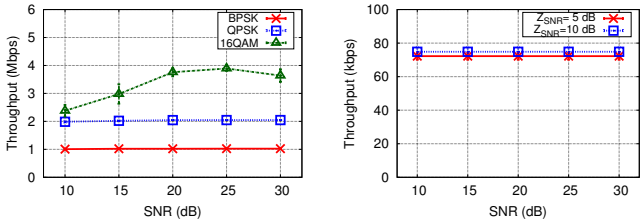
Next, we evaluate the performance of frame detection in WizBee implementation. We use the same data as in previous experiment. For each experiment case, at least 1,000 WiFi and 1,000 ZigBee frames are used for the evaluation of frame detection accuracy. We present the detection results when the modulation scheme of WiFi signal is BPSK, since the detection results of different modulation schemes are similar.

Figure. 6a presents the detection ratio of ZigBee frames under different experiment settings. FP stands for false positive rate, which corresponds to the probability that the algorithm falsely detects a frame when it does not exist. While FN stands for false negative rate, corresponding to the probability that the algorithm misses a real frame and reports nothing. Z_{SNR} is the SNR value of ZigBee frames. And notably, the SNR value $Z_{SNR} = 5$ dB represents the case where no WiFi frames are transmitted and the SNR value of ZigBee frame is 5 dB. According Fig. 6a, we can see that both false positive rate and false negative rate are negligible, except that the false positive rate when WiFi SNR is 0 dB. To achieve a lower false negative, it is reasonable and tolerable to keep false positive a little bit higher. False positive detection will make the WizBee decode packets without inference.



(a) Detection Ratio of ZigBee (b) Detection Ratio of WiFi

Fig. 6: Detection Performance of WiFi and ZigBee. FP stands for false positive rate, while FN stands for false negative rate. The x-axis shows the SNR of WiFi frames. Z_{SNR} is the SNR of ZigBee frames. $Z_{SNR} = 0$ dB is the case where no ZigBee frame is transmitted. $W_{SNR} = 0$ dB is the case where no WiFi frame is transmitted.



(a) Benchmark of WiFi (b) Benchmark of ZigBee

Fig. 7: Benchmark Throughput of WiFi and ZigBee

Naturally, we need to raise the false positive rate to ensure very low false negative rate.

Figure. 6b shows the detection ratio of WiFi frames under different SNR values. It is worth noting that, the SNR value $Z_{SNR} = 0$ dB is the case where no ZigBee frame is transmitted. We can see that for all SNR values of WiFi signal, the FP and FN detection rate of WiFi frame are extremely low, such that, they can be negligible.

6.2.3 Throughput Gain

We then evaluate the throughput performance of WizBee under different settings, and use the same data set collected in previous experiment for evaluation.

We first study the benchmark performance of throughput for both WiFi and ZigBee networks. Fig. 7a shows the benchmark throughput of WiFi networks, *i.e.* there is no ZigBee signal interference. We can see that the throughput of WiFi networks with BPSK and QPSK modulation can achieve its maximum value for all SNR values from 5 dB to 30 dB. When the SNR of WiFi is greater than 20 dB, the throughput of WiFi with 16QAM modulation can achieve its maximum value. Since 16QAM modulation is not resilient to noise, the throughput of 16QAM modulation is less stable than BPSK and QPSK modulations. Fig. 7b shows the benchmark throughput of ZigBee networks when there is no WiFi signal interference. The x-axis of Fig. 7b is not the SNR value of ZigBee frames. It is only for the purpose of plotting. We can see that there is little difference between the throughput of ZigBee networks when SNR is 5 dB and 10 dB. Both cases can achieve the maximum performance in our experiment testing. The benchmark throughput of WiFi and ZigBee networks validate our implementations on WiFi/ZigBee decoder.

The throughput gain of WizBee networks over benchmark ZigBee networks is shown in Fig. 8. According to the results we obtain the following observations.

First, WizBee effectively improves throughput gain by interference cancellation. From Fig. 8, we can see that WizBee can improve throughput gain as high as 90% than benchmark. The throughput of ZigBee networks with WizBee almost achieves 85% of the benchmark throughput, in which case no WiFi interference is presented.

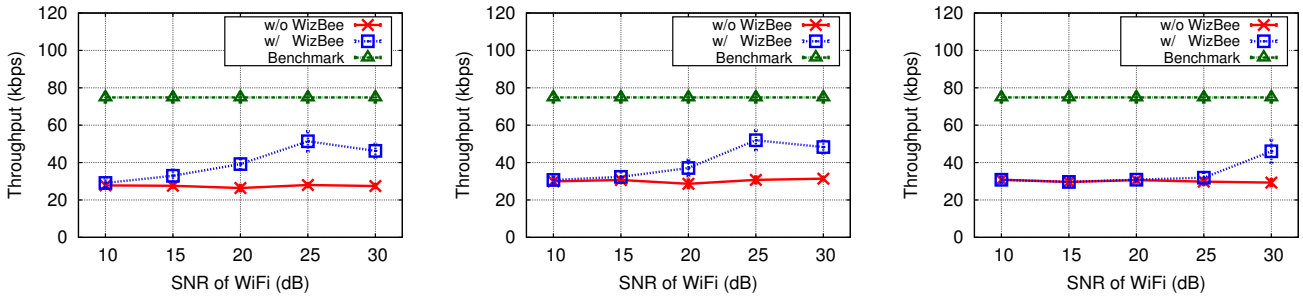
Second, the improved throughput gain increases as the SNR of WiFi increases. This is because the higher SNR value of WiFi, the more resilient to ZigBee interference. So, the successive interference cancellation can work better. In particular, when the SNR of WiFi goes too high, *e.g.* 30 dB for BPSK and QPSK modulation, the throughput gain of WizBee decreases little. This is mainly because when the SNR of WiFi goes too high, the residual noise after interference cancellation remains larger too. Thus, the throughput of ZigBee networks is affected by the residual noise of WiFi signals.

Third, the improved throughput gain reduces as the SNR of ZigBee increases. This is reasonable since higher SNR of ZigBee packets leads to poorer decoding performance of WiFi networks when the frame of the two networks collide.

Last but not least, the throughput gain reduces as the modulation order of WiFi increases. According to Fig. 8c we can clearly see that the throughput gain of WizBee become very small when the modulation of WiFi networks is 16QAM. This is accordance with the SNR requirement of higher order modulation schemes. This phenomena also reveals the limitation of WizBee, which requires large SNR difference and high interference resilient capacity for interference modulation technique.

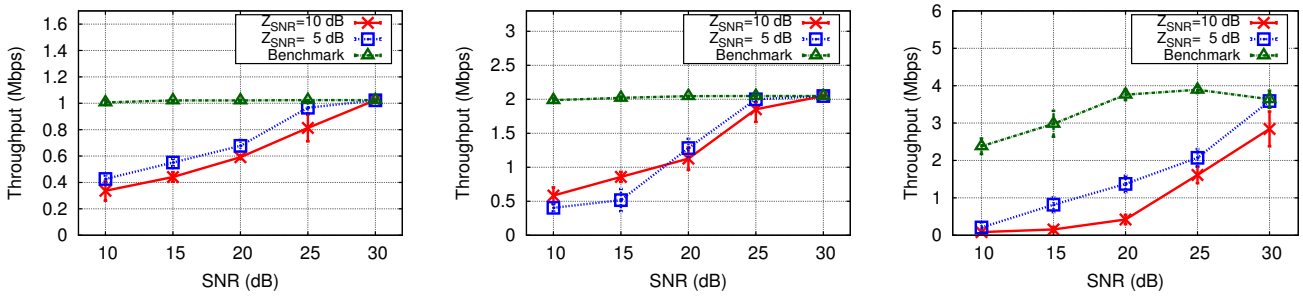
Fig. 9 shows the throughput of WiFi networks under the impact of ZigBee signals. We observe that the impact of ZigBee signal is limited when the SNR of WiFi is greater than 25 dB for BPSK and QPSK modulations. This indicates there remains a large room to improve the throughput gain of ZigBee networks with WizBee, especially for the case when WiFi networks use high SNR value and low modulation order to transmit packets.

To further examine the construction of the throughput gain, we plot the recovery ratio of different frame types in Fig. 10. The x-aixs is the ratio of correctly decoded frames of the corresponding type. The y-axis is the SNR of WiFi when WiFi and ZigBee networks coexist together. Corrupted frames are the frames that are collided with each other. Fig. 10 shows the recovery ratio when ZigBee SNR is 10 dB. We find that the recovery ratio of uncorrupted ZigBee frames is relative stable, above 0.8 in all



(a) When WiFi Modulation is BPSK (b) When WiFi Modulation is QPSK (c) When WiFi Modulation is 16QAM

Fig. 8: Throughput gain of WizBee network over ZigBee benchmark system when ZigBee SNR is 10 dB. The SNR of WiFi shows the signal strength of WiFi networks when they coexist together.



(a) Throughput of WiFi with BPSK Modulation (b) Throughput of WiFi with QPSK Modulation (c) Throughput of WiFi with 16QAM Modulation

Fig. 9: Throughput of WiFi networks

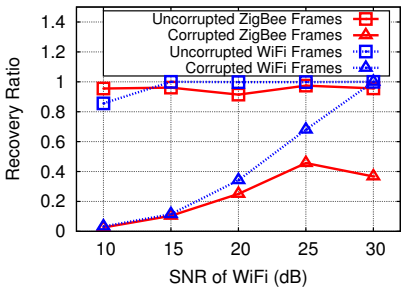
experiment settings. The recovery ratio of uncorrupted WiFi frames increase when SNR increases, which is accordance with the SNR requirement of different modulation techniques. Obviously, the recovery ratio of corrupted ZigBee frames and corrupted WiFi frames show a similar trend, *i.e.*, the recovery ratio of corrupted ZigBee frames increases with the recovery ratio of corrupted WiFi frames increases. Since the decoding results of corrupted ZigBee frames depend on the decoding results of corrupted WiFi results, interference cancellation can work only when the corrupted WiFi frames decoded correctly. It should also be notified that the trend of recovery ratio of corrupted ZigBee frames and corrupted WiFi frames go apart when the SNR of WiFi is higher than 25 dB for BPSK and QPSK modulation. This is because when the SNR of WiFi increases, the residual noise of WiFi after interference cancellation increases too. Thus, the decoding performance of ZigBee frames is affected.

6.3 Macro-benchmark

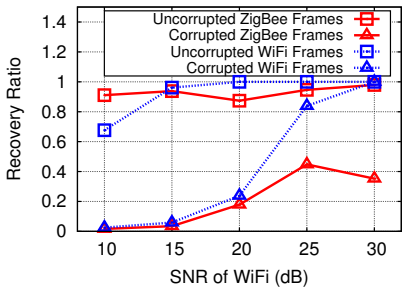
In this section, we evaluate the end-to-end throughput gain of WizBee under the testbed shown in Fig. 3. We place the WizBee sink at position A or B randomly. The WiFi and ZigBee transmitters are moved among the eight locations during our experiments, as shown in Fig. 3. We mainly compare the throughput of WiFi and ZigBee networks with and without WizBee. To measure the throughput accurately, we configure one USRP node as WiFi sender to transmit 100 packets with 256 Bytes in 2 ms, and another USRP node as ZigBee sender to transmit 100 packets with 20 Bytes in 2 ms. The data rate of WiFi networks is set at 6 Mbps, *i.e.* with BPSK modulation and 1/2 convolution code rate. The packet intervals of WiFi and ZigBee are 1.5 ms and 1.612 ms respectively. We collect 10 traces in each location pair, and change the location pairs 20 times. The column labeled with 'R' represents the location of the receiver (*i.e.* WizBee sink), and the columns labeled with 'W' and 'Z' represent the locations of WiFi and ZigBee nodes respectively. In general, 20,000 WiFi and ZigBee packets are collected in all experiment cases. These traces are sampled randomly within 3 hours.

Fig. 11 shows the SNR difference between of WiFi and ZigBee packets of different location pairs. From Fig. 11, we can see that the SNR difference various sharply according to different location pairs, ranging from -8 dB to 28 dB. Fig. 14 plots the cumulative distribution function of the SNR difference between WiFi and ZigBee networks. We can also observe that in over 90% cases, the SNR of WiFi is 15 dB higher than that of ZigBee.

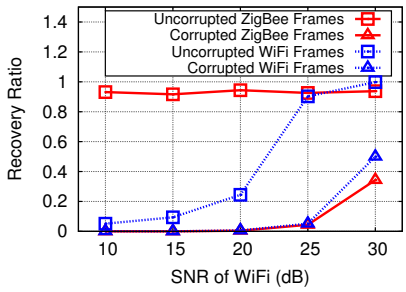
Fig. 12 shows the throughput of ZigBee with and without WizBee. It can be seen from Fig. 12 that the throughput gain of WizBee for ZigBee networks is highly dependent on the location pairs. The throughput gain of WizBee is 1.8X in location pair 7 but only 1.0X at location



(a) When WiFi Modulation is BPSK



(b) When WiFi Modulation is QPSK



(c) When WiFi Modulation is 16QAM

Fig. 10: Recovery ratio of networks when ZigBee SNR is 10 dB. The SNR of WiFi shows the signal strength of WiFi networks when they coexist together.

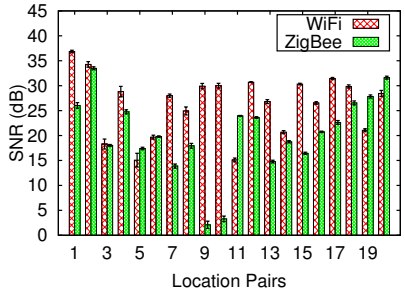


Fig. 11: SNR of WiFi and ZigBee

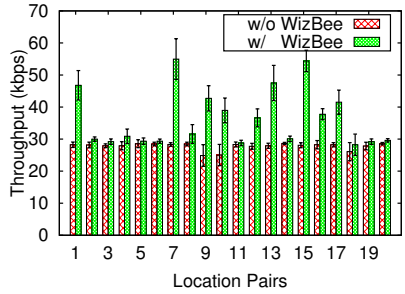


Fig. 12: Throughput of ZigBee

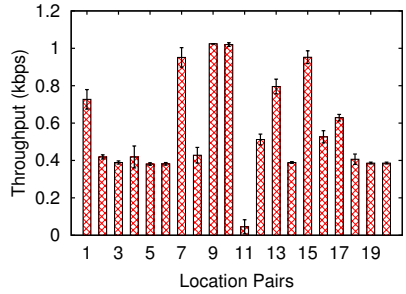


Fig. 13: Throughput of WiFi

pair 11. Fig. 15 plots the cumulative distribution function of the throughput gain of WizBee for ZigBee networks. We can observe that in 80% cases, the throughput gain of WizBee is higher than 1.6×, with median throughput gain of 1.2×.

We also show the throughput of WiFi networks in Fig. 13, in which the result indicates that the throughput of WiFi is highly dependent on location pairs, *i.e.* the SNR difference between WiFi and ZigBee networks. Note that the throughput of WiFi highly correlate with the throughput gain of WizBee. Fig. 16 shows the relationship between the throughput of WiFi and the throughput gain of WizBee. We can observe that the throughput gain of WizBee increases with the increase of WiFi throughput, which indicates a win-win solution for the coexisting WiFi and ZigBee networks with the use of WizBee.

6.4 Discussion

Cost Issue: One of the concerns is that WizBee uses wideband sampling, and the WiFi decoding algorithm is much complex than ZigBee, leading to high-cost and high energy consumption. Our argument is twofold. First the sink is owning unlimited energy budget compared to small sensors, such that the energy consumption will not be a serious concern. Second, WizBee only needs to introduce sink nodes. Although the cost is relatively high, it is still acceptable compared to the redeployment of all sensor nodes, especially in large-scale sensor networks.

Multi-Hop Networks: Wireless sensor networks used in environment monitoring are envisioned to be organized in multi-hop way. However, all we discussed in focused on one-hop networks. Actually, our WizBee sink can also serve as a relay node, and it will only be deployed in heavy WiFi traffic area. Due to the short transmission range of WiFi and long transmission range of ZigBee, the interference region could be restricted to one-hop area. In our real world network measurement study, the hidden terminal is difficult to identify [30]. The main reason is, most of the WiFi AP deployment is dense, and over equipped.

Carrier Sensing Optimization: A good property of WizBee is that sensor nodes can transmit packets with WiFi interference in uplink, which implies that they will be free from the backoff operation when sensing WiFi signals. Thus, to further improve ZigBee system performance, an aggressive solution might be used to modify sensor nodes' program to enable concurrent transmission with WiFi. We leave this attempt in our future work.

Architecture Scalability: Note that our architecture is easy to expand. For example in home wireless networks, we can add WiFi packet output in shadowed interference cancellation block. Also, it is possible to implement a full-duplex sink [1] that allows in-band simultaneous transmission and reception by adding the coexistence-enabled elements before the RF front-end and spectrum component.

Energy Consumption: Its true that the WizBee sink

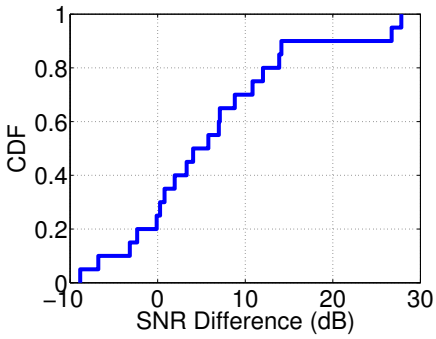


Fig. 14: CDF of SNR Difference

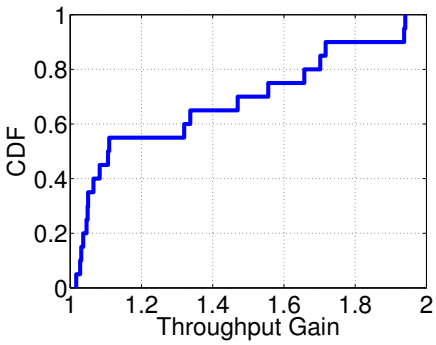


Fig. 15: CDF of Throughput Gain

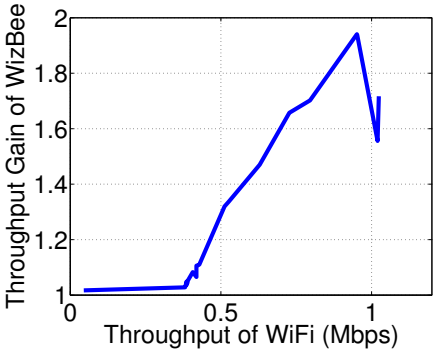


Fig. 16: Throughput of WiFi vs Throughput Gain

needs more power than conventional design. In our design, since the sensors are deployed in urban area. The public power supply is available around the sink node area, where energy consumption is not serious in our case. Moreover, even in the power supply hungry area, we could also use the solar battery to empower the cognitive radio platform. There are also other efforts having been made for low power cognitive radio platform, such as μ-SDR [14], *et al.*. Leveraging these low power design, the cognitive radio based system could also be deployed massively in large scale wireless sensor networks.

Comparing with TIMO: Comparing with TIMO, we use only one antenna, and will inevitably require the relatively high energy level of WiFi. Moreover, for TIMO network, it mainly focuses on protecting WiFi signals, and could not effectively recover both WiFi and ZigBee at the same time. Obviously, such design could not satisfy our design requirement, because large-scale urban WSNs, need to successfully recover the ZigBee and WiFi signals at the same time.

7 Related Work

Related work falls in the following areas:

Coexistence Solutions: Many solutions have been proposed to address the coexistence problem. An easy idea to enable coexistence is to do frequency planning beforehand. However, it requires centralized planning. Second, there are only three orthogonal WiFi channels in 2.4GHz ISM band. Densely deployed WiFi networks will make interference-free frequency planning hard. Hence, in this paper, we focus on co-channel coexistence scenario, and consider the corresponding design issues.

To tackle the co-channel coexistence problem, [10] first predicates the length of inter-frame interval of WiFi transmissions, and then adapts the frame length of ZigBee packet to fully utilize the "white-space" opportunity to avoid collisions. The approach presented in [17] measures the interference pattern of WiFi and Zigbee, and proposes to add redundant information (i.e., multi-header and Reed-Solomon channel code) to let ZigBee recover valid packets from WiFi interference. However, this leads to two problems: First, it does not guarantee ZigBee's performance during busy WiFi traffic, since WiFi is still the "first-class citizen". Second, it introduces extra overhead to existing ZigBee protocols, and needs re-programming existing nodes, which is difficult to be applied in existing deployed architecture.

Some efforts [28], [32] tackle the challenge by introducing new strong devices to improve the visibility of low-power ZigBee. A signaler node emits strong jamming signal [32] or fake WiFi header [28] during ZigBee transmission to let WiFi backoff explicitly. Radunovic *et al.* [22] redesign the preamble of low-power wireless technology based on a key observation that longer preamble sequence can be detected easier. In this case, WiFi will sense the presence of ZigBee, and thus backoff. The mutual visibility solutions can enhance a fair coexistence, but is not a perfect solution in urban monitoring scenario. Long-term running of mutual visibility solutions will cause WiFi's performance degradation, and WiFi can also have anti-jamming capability [20] to make such solutions infeasible. Moreover, the signaler solution requires strict timing control of ZigBee's transmission, leading to severe protocol overhead in large-scale ZigBee networks.

Exclusive use of channel by weak ZigBee will underutilize the overall network resource, since ZigBee only needs 2MHz bandwidth. Therefore, several solutions [8], [23], [31] utilize OFDM subcarrier suppressing technique to vacate spectrum that ZigBee networks are using. The strong WiFi devices first find the existence of weak ZigBee devices (either by sensing [8], [31] or learning [23]), decide which spectrum ZigBee networks use, and nullify those spectrums to enable simultaneous access. Thus, little interference or no interference is generated to ensure proper operation of low-power devices, which enables the coexistence of different technologies. Though it is a good idea to provide general coexistence, the subcarrier suppressing solution requires hardware redesign on high-power nodes, e.g., preamble design and packet detection algorithm, which limits the application if it is not compatible with existing devices.

Interference cancellation: The approach proposed in [2] employs successive interference cancellation tech-

nique to redesign the carrier sensing mechanism to improve the performance of wireless local area networks. ZigZag [5] exploits different overlap patterns and interference cancellation technique to resolve hidden terminal collisions. A few researchers [6], [25] use interference cancellation technique in multi-user MIMO scenario. Instead, we use interference cancellation technique to solve coexistence problem. Moreover, some previous works, [2], [5], [6], [25] demonstrates interference cancellation using DSSS-style communication system, while we use OFDM.

Wireless Systems using WiFi and ZigBee: Many wireless systems use WiFi and ZigBee technologies at the same time. ZiFi [33] uses low-power ZigBee radios to indentify periodical WiFi beacons, thus discovering WiFi networks. WiZi-Cloud [13] propose to use additional ZigBee radios to help WiFi clients to achieve ubiquitous connectivity, high energy efficiency, and real time inter-AP handover. WiBee [16] exploits low-cost ZigBee sensor networks to build real-time WiFi radio maps. WizSync [7] utilizes periodical WiFi beacons to synchronize ZigBee nodes. Compared with those works, we consider coexistence problem, and exploit WiFi radios to help decode ZigBee packets. Recent studies also include Picasso [9] and weeble [22]. However, Picasso [9] needs regulated spectrum usages for coexistence, where the end systems of WiFi or ZigBee need to coordinate for non-overlapping spectrum usages. Adaptive preambles [22] for coexistence are also very useful due to lightweight and high efficiency, but still suffers from device intervention.

8 Conclusion

This paper presents WizBee, a single-antenna sink based design to coexist ZigBee signals with WiFi interference without modifying terminal equipments. The key insight of WizBee is that, we can use the opportunity lies in cross technology for effective signal recovery. Leveraging multi-domain information, such as power, frequency and coding discrepancies, the interfered signals can be recovered by iterative decoding and cancellation scheme. In future work, we will focus on how to further use these information intelligently to improve the coexistence network throughput.

We implemented WizBee on the GNURadio-USRP platform using commercial compatible implementations of WiFi and ZigBee, *i.e.* IEEE 802.11g and IEEE 802.15.4. We demonstrated that, WizBee effectively improve the network throughput and make an effective recovery over interfered ZigBee signals. Our extensive evaluations under real wireless conditions show that WizBee can improve $1.6\times$ throughput for ZigBee networks over 80% cases, with median throughput gain of $1.2\times$.

Our future work is multidimensional. WizBee can be enhanced as a new form of WiFi AP for both ZigBee and WiFi signals. Also, WizBee can be applied to other WiFi standards with slight modifications, such as IEEE 802.11n. Moreover, real time decoding of WizBee is also a favorable function for real deployment in large scale sensor network. We will improve the processing ability as well as the accuracy in future investigations.Furthermore, we extend the WizBee design to some down-sized and energy-efficient software radio platform, e.g. uSDR [15], which is promising to bridge the gap between SDR-based system and WSNs.

Acknowledgment

This research is partially supported by NSF China under Grants No. 61232018, 61272487, 61170216, 61172062, 61228202, 61273210, NSF CNS-0832120, NSF CNS-1035894, NSF EECS-1247944, BK2012512. Particularly, the research work is mainly done during the authors' scholar visiting in IOT Tech-center of TNLIST, Wuxi, China.

References

[1] Choi, J., Jain, M., Srinivasan, K., Levis, P., and Katti, S. Achieving single channel, full duplex wireless communication. *in Proc. ACM Mobicom* (2010), 1–12.

[2] D. Halperin, T. A., and Wetherall, D. Taking the sting out of carrier sense: interference cancelation for wireless lans. *in Proc. ACM MOBICOM* (2008), 339–350.

[3] Ettus Research, 2013.

[4] Gollakota, S., Adib, F., Katabi, D., and S.Seshan. Clearing the rf smog: Making 802.11 robust to cross-technology interference. *In Proc. ACM Sigcomm* (2010).

[5] Gollakota, S., and Katabi, D. Zigzag decoding: combating hidden terminals in wireless networks. *in Proc. ACM SIGCOMM* (2008), 159–170.

[6] Gollakota, S., Perli, S., and Katabi, D. Interference alignment and cancelation. *in Proc. ACM SIGCOMM* (2009).

[7] Hao, T., Zhou, R., Xing, G., and Mutka, M. Wizsync: Exploiting wi-fi infrastructure for clock synchronization in wireless sensor networks. *in Proc. IEEE RTSS* (2011), 149–158.

[8] He, Y., Fang, J., Zhang, J., Shen, H., Tan, K., and Zhang, Y. Mpap: virtualization architecture for heterogenous wireless aps. In *SIGCOMM '10* (New York, NY, USA, 2010), ACM, pp. 475–476.

[9] Hong, S., Mehlman, J., and Katti, S. Picasso: Flexible rf and spectrum slicing. *ACM SIGCOMM* (2012).

[10] Huang, J., Xing, G., Zhou, G., and Zhou, R. Beyond coexistence: Exploiting wifi white space for zigbee performance assurance. In *ICNP '10* (2010), pp. 305–314.

[11] IEEE Standard for WiFi. Wireless lan medium access control (mac) and physical layer (phy) specifications, 2007.

[12] IEEE Standard for ZigBee. Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans), 2006.

[13] Jin, T., Noubir, G., and Sheng, B. Wizi-cloud: Application-transparent dual zigbee-wifi radios for low power internet access. *in Proc. IEEE INFOCOM* (2011).

[14] Kuo, Y.-S., Pannuto, P., Schmid, T., and Dutta, P. Reconfiguring the software radio to improve power, price, and portability. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems* (2012), SenSys '12.

[15] Kuo, Y.-S., Pannuto, P., Schmid, T., and Dutta, P. Reconfiguring the software radio to improve power, price, and portability. In *Sensys '12* (2012), pp. 267–280.

[16] Li, W., Zhu, Y., and He, T. Wibee: Building wifi radio map with zigbee sensor networks. *In Proc. IEEE INFOCOM* (2012).

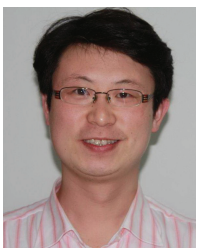
[17] Liang, C.-J. M., Priyantha, N. B., Liu, J., and Terzis, A. Surviving wi-fi interference in low power zigbee networks. In *SenSys 2010* (2010).

[18] Liu, Y., He, Y., Li, M., Wang, J., Liu, K., Mo, L., Dong, W., Yang, Z., Xi, M., Zhao, J., and Li, X.-Y. Does wireless sensor network scale? a measurement study on greenorbs. In *INFOCOM 2011* (2011).

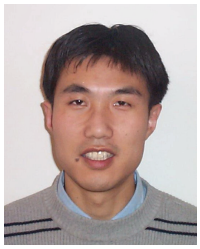
[19] Mao, X., Miao, X., He, Y., Li, X.-Y., and Liu, Y. Citysee: Urban co2 monitoring with sensors. In *INFOCOM* (2012), pp. 1611–1619.

[20] PELECHRINIS, K., BROUSTIS, I., KRISHNAMURTHY, S. V., AND GKANTSIDIS, C. Ares: an anti-jamming reinforcement system for 802.11 networks. In *CoNEXT '09* (2009), pp. 181–192.
[21] PIAMRAT, K., AND FONTAINE, P. Coordinated architecture for wireless home networks. In *HomeNets '11* (2011), pp. 49–54.
[22] RADUNOVIC, B., CHANDRA, R., AND GUNAWARDENA, D. Weeble: Enabling low-power nodes to coexist with high-power nodes in white space networks. *ACM CoNEXT* (2012).
[23] RAHUL, H., KUSHMAN, N., KATABI, D., SODINI, C., AND EDALAT, F. Learning to share: narrowband-friendly wideband networks. In *SIGCOMM '08* (New York, NY, USA, 2008), ACM, pp. 147–158.
[24] SHNAYDER, V., CHEN, B.-R., LORINCZ, K., JONES, T. R. F. F., AND WELSH, M. Sensor networks for medical care. In *SenSys '05* (2005), pp. 314–314.
[25] TAN, K., LIU, H., AND FANG, J. Sam: Enabling practical spatial multiple access in wireless lan. *In Proc. ACM Mobicom* (2009).
[26] TANG, L.-A., HAN, J., AND JIANG, G. Mining sensor data in cyber-physical systems. *Tsinghua Science and Technology 19*, 3 (2014), 225–234.
[27] VITERBI, A. J., AND OMURA, J. K. *Principles of Digital Communication and Coding*. McGraw-Hill, 1979.
[28] WANG, Y., WANG, Q., ZENG, Z., ZHENG, G., AND ZHENG, R. Wicop: Engineering wifi temporal white-spaces for safe operations of wireless body area networks in medical applications. *IEEE RTSS* (2011), 170–179.
[29] WIKIPEDIA WEB SITE, 2013.
[30] YUBO, Y., PANLONG, Y., XIANGYANG, L., YUE, T., LAN, Z., AND LIZHAO, Y. Zimo: Building cross-technology mimo to harmonize zigbee smog with wifi flash without intervention. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking* (2013), MobiCom '13.
[31] ZHANG, X., AND SHIN, K. G. Adaptive subcarrier nulling: Enabling partial spectrum sharing in wireless lans. In *ICNP* (2011), pp. 311–320.
[32] ZHANG, X., AND SHIN, K. G. Cooperative carrier signaling: Harmonizing coexisting wpan and wlan devices. *MobiHoc 2011* (2011).
[33] ZHOU, R., XIONG, Y., XING, G., SUN, L., AND MA, J. Zifi: wireless lan discovery via zigbee interference signatures. *In Proc. ACM Mobicom* (2010), 49–60.

Yubo Yan (S'10) received the B.S. degree and M.S. degree in communication and information system from the College of Communications Engineering, PLA University of Science and Technology, China, in 2006 and 2011 respectively. He is currently working towards the Ph.D. degree at the PLA University of Science and Technology. His current research interests include cognitive radio networks, software radio systems and wireless sensor networks. He is a student member of the IEEE.



Panlong Yang (M'02) received his B.S. degree, M.S. degree, and Ph.D. degree in communication and information system from Nanjing Institute of Communication Engineering, China, in 1999, 2002, and 2005 respectively. During September 2010 to September 2011, he was a visiting scholar in HKUST. Dr. Yang is now an associate professor in Institute of Communication Engineering, PLA University of Science and Technology. His research interests include wireless mesh networks, wireless sensor networks and cognitive radio networks. Dr. Yang has published more than 50 papers in peer-reviewed journals and refereed conference proceedings in the areas of mobile ad hoc networks, wireless mesh networks and wireless sensor networks. He has also served as a member of program committees for several international conferences. He is a member of the IEEE Computer Society and ACM SIGMOBILE Society.

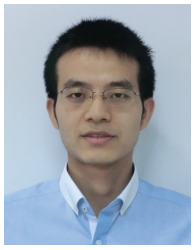


Xiang-Yang Li (SM'08) received a Bachelor degree at Department of Computer Science and a Bachelor degree at Department of Business Management from Tsinghua University, P.R. China, both in 1995. He received M.S. (2000) and Ph.D. (2001) degree at Department of Computer Science from University of Illinois at Urbana-Champaign. Xiang-Yang is an Associate Professor (since 2006) of Computer Science at the Illinois Institute of Technology. His research interests include the cyber physical systems, wireless sensor networks, game theory, and algorithms.

Yafei Zhang is currently a professor of PLA University of Science and Technology, Nanjing, China. He received his PhD degree in Computer Science from Fudan University, Shanghai, China, in 1992. His research focuses on intelligent information processing.

Jianjiang Lu is currently an associate professor of PLA University of Science and Technology, Nanjing, China. He received his PhD degree in Computer Science from PLA University of Science and Technology, Nanjing, China, in 2002. His research focuses on intelligent information processing.

Lizhao You received his B.S. and M.E. degrees from Nanjing University in 2009 and 2013, respectively. He is currently a Ph.D. student at the Department of Information Engineering, The Chinese University of Hong Kong. His research interests include wireless communication and wireless networks.



Jiliang Wang received his BE degree in computer science and technology from University of Science and Technology of China and his PhD degree in computer science and engineering from Hong Kong University of Science and Technology, in 2007 and 2011, respectively. He is currently with School of Software and TNLIST, Tsinghua University. His research interests include sensor and wireless networks, network measurement and pervasive computing.

Jinsong Han is currently an associate professor at Xi'an Jiaotong University. He received his Ph.D. degree from Hong Kong University of Science and Technology. His research interests include pervasive computing, distributed system, and wireless network. He is a member of IEEE and ACM.

Yan Xiong was born in Anhui Province, in 1960. He is a professor in School of Computer Science and Technology, University of Science and Technology of China. His research interests include distributed processing, mobile computation, and information security.