ZIMO: Building Cross-Technology MIMO to Harmonize ZigBee Smog with WiFi Flash without Intervention

Yubo Yan[1], Panlong Yang[1,3], Xiang-Yang Li[2,3], Yue Tao[2], Lan Zhang[3], Lizhao You[4]
[1]PLA University of Science and Technology, China
[2]Department of Computer Science, Illinois Institute of Technology, USA
[3]School of Software and TNLIST, Tsinghua University, China
[4]Department of Computer Science and Technology, Nanjing University, China
yanyub@gmail.com, panlongyang@gmail.com, xli@cs.iit.edu, nightvista@gmail.com, zhanglan03@gmail.com, youlizhao.nju@gmail.com

ABSTRACT

Recent studies show that WiFi interference has been a major problem for low power urban sensing technology ZigBee networks. Existing approaches for dealing with such interferences often modify either the ZigBee nodes or WiFi nodes. However, massive deployment of ZigBee nodes and uncooperative WiFi users call for innovative cross-technology coexistence without intervening legacy systems.

In this work we investigate the WiFi and ZigBee coexistence when ZigBee is the interested signal. Mitigating short duration WiFi interference (called *flash*) in long duration ZigBee data (called *smog*) is challenging, especially when we cannot modify the WiFi APs and the massively deployed sensor nodes. To address these challenges, we propose ZIMO, a sink-based MIMO design for harmony coexistence of ZigBee and WiFi networks with the goal of protecting the ZigBee data packets. The key insight of ZIMO is to properly exploit opportunities resulted from differences between WiFi and ZigBee, and bridge the gap between interested data and cross technology signals. Also, extracting the channel coefficient of WiFi and ZigBee will enhance other coexistence technologies such as TIMO [1]. We implement a prototype for ZIMO in GNURadio-USRP N200, and our extensive evaluations under real wireless conditions show that ZIMO can improve up to 1.9× throughput for ZigBee network, with median gain of 1.5×, and 1.1× to 1.9× for WiFi network as byproduct in ZigBee signal recovery.

Categories and Subject Descriptors

C.2.1 [**COMPUTER-COMMUNICATION NETWORKS**]: Network Architecture and Design—*Wireless communication*

General Terms

Design, Experimentation, Performance

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
MobiCom'13, September 30-October 4, Miami, FL, USA.
Copyright 2013 ACM 978-1-4503-1999-7/13/09 ...$15.00.

Keywords

MIMO, Physical Layer, Sensor Networks

1. INTRODUCTION

Urban area wireless sensor networks are becoming vitally important for nowadays "smart city" programs. These grand engineering work heavily depend on sensor nodes and efficient network connections for monitoring environment. Most of the urban sensing systems are leveraging the COTS ZigBee, such as Urban sense [2], CitySee [3]. Unfortunately, in urban areas, WiFi interference is pervasive and possibly the primary factor leading to ZigBee throughput degradation [1, 4–7]. Meanwhile, it has been verified that the WiFi network performance can be affected by the ZigBee interference [8]. It is worth noting that, protecting ZigBee signal and extracting the interested data from the cross-technology noise is not trivial. Previous studies [1, 8] indiscriminately take the ZigBee signal as cross-technology interference, especially RF *smog*, which leaves a gap between WiFi and other cross-technologies for coexistence. Notably, ZigBee is similar to WiFi in sense of CSMA scheme, and apparently different from RF technologies without communication functionality, such as microwave oven.

In summary, existing solutions can not reasonably work in urban sensing sensor networks. There are several specific requirements in building an efficient ZigBee system coexisting with WiFi systems. Foremost, there should be no modification or intervention on the end nodes in either ZigBee or WiFi networks. For urban sensing, modifying the software and/or hardware on the sensor nodes is difficult and expensive. Furthermore, WiFi AP holders are reluctant to make any changes even when ZigBee nodes interfere them. Meanwhile, it is expected that the performance degradation caused by coexistence should be minimized. In our case, ZigBee is interested signal, but the WiFi transmission is expected to be pervasive. This is the key idea of harmony coexistence, where two systems can share the conflicted network resource, without harming each other.

Fully considering these design requirements, we propose ZIMO, a cross-technology MIMO sink design to harmonize the coexistence of ZigBee and WiFi networks. Different from previous studies, in our design, the sink node performs the coexistence work, and the end nodes in WiFi and ZigBee networks need not do any further modification. Adding a modified sink is relatively easy and more affordable than re-

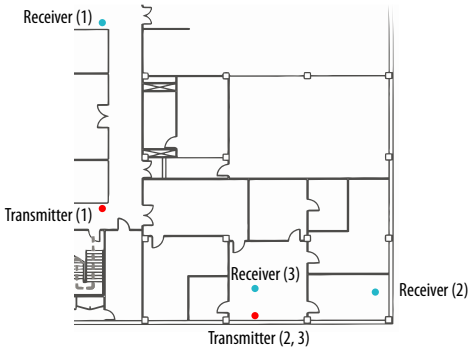


Figure 1: Indoor layout of the experiment.

programming all the deployed sensor nodes. In ZIMO, we leverage a 2-antenna MIMO system for WiFi and ZigBee interference resolution. To the best of our knowledge, ZIMO is the first implemented working system meeting the aforementioned requirements. There are several challenges that need to be addressed carefully in designing and implementing ZIMO, which are summarized as follows.

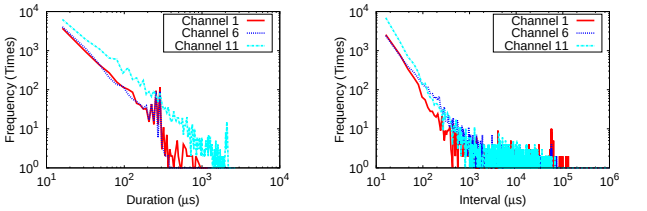
First, unpredictable and uncooperative WiFi interference will incur different interference patterns. When WiFi preamble is clear, the WiFi signal needs to be nullified first for ZigBee signal decoding. Inevitably, the WiFi channel coefficient estimation will suffer unfavorable distortions due to ZigBee interference, and will incur unsatisfiable ZigBee signal recovery.

Second, when WiFi flash is drowned in ZigBee smog, signals in two technologies are cross-affected in both time and frequency domain. For WiFi signal, there is no clear reference for accurate channel coefficient estimation. Even worse, considering the low-power ZigBee signal, more accurate and thorough interference cancelation for WiFi signal is needed. Thus, the CFO (Carrier Frequency Offset) estimation across receiving symbols are not negligible comparing with conventional interference cancelation and alignment schemes [9]. For ZigBee signal, the channel coefficient estimation should be carefully considered as the frequency offset can be possibly up to 200 KHz [10], which means accurate and fast enough synchronization should be done within ZigBee preamble time.

ZIMO addresses these challenges with two innovative techniques. For the first challenge, a blind recovery method for WiFi channel coefficient is presented, based on interpolation that exploits the continuous and steady feature in frequency domain. With this advantage, the second challenge for WiFi signal is addressed by a linear regression model used for fine frequency offset compensation across WiFi symbols. Also for ZigBee signal, an innovative ZigBee channel coefficient estimation method is proposed, where large frequency offset is estimated and compensated through modulation-independent approach.

In summary, our main contributions are as follows.

We propose ZIMO, a sink based MIMO design for harmony coexistence of WiFi and ZigBee by protecting the ZigBee data from being interfered. Our design need not modify and intervene on WiFi APs or ZigBee nodes. A key insight of the work is to properly handle the relationship between WiFi and ZigBee where opportunities in time, spectral and power domain due to cross-technology can be leveraged. The



(a) Duration of Corrupted (b) Interval between Corrupted

Figure 2: Corruption of ZigBee transmission covered by different WiFi channels at site 1 with log-log plot.

ZIMO sink can also serve as a sniffer that can recover the interfered WiFi packets. Extracting accurate channel coefficients of WiFi and ZigBee will also enhance other coexistence technology such as TIMO [1].

We implement ZIMO on USRP platform and present a working system. Comparing with SAM [11], we solve the distributed cross-technology multiplexing with virtual MIMO implementation, and recover WiFi and ZigBee data at the same time. Comparing with TIMO [1], we intelligently handle the ZigBee and WiFi signal simultaneously, leveraging the channel coefficient of the cross-technologies in data domain. In power domain, we can handle the smog-like interference in TIMO scenario [1], and the flash-like interference experienced in our experimental study in Section 8 as well. Surprisingly, we find that ZIMO can help enhance WiFi and ZigBee communications. ZIMO will help recover the interfered ZigBee signals as well as WiFi signals, leading a way from coexistence to co-prosperity.

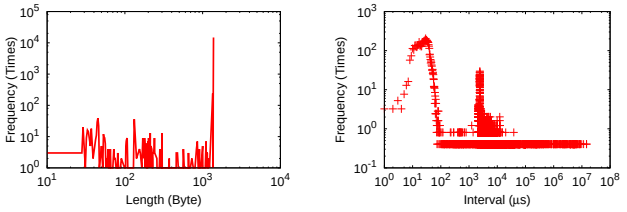
The rest of the paper is organized as follows. We conduct a comprehensive experimental study on the impacts of WiFi interference on ZigBee networks in Section 2. Section 3 provides background on ZigBee and WiFi system, as well as MIMO communication. The problem domain and system design overview are introduced in Sections 4 and 5 respectively. After describing our system design in Section 6, and implementation in Section 7, we evaluate the performance of ZIMO in Section 8. We make extensive discussions on ZIMO in Section 9, and review the related work in Section 10. Finally, we conclude the work in Section 11.

2. IMPACT OF WIFI ON ZIGBEE

2.1 Experiment Rationale and Setup

A preliminary experiment was made to investigate the interference between WiFi and ZigBee networks. Since the CSMA/CA mechanism restricts that only one pair of nodes can transmit at one time when multiple ZigBee senders are presented, in our experiment, the ZigBee networks consist only one sender and one receiver, without losing significance of the result. The transmitter repeatedly sends packets with identical content, and the interference will be represented on the received data as corrupted bytes. Note that, we've tested that, the ZigBee transmission experiences very low error rate before WiFi interference is introduced.

The experiment is conducted in a basement of the school building at IIT, with layout specified in Fig. 1. Although we are not permitted to obtain the number and locations of WiFi APs for security reasons, a scanning made on a laptop at the location of ZigBee receiver shows that more than 20 WiFi APs can be found with distinct signal strength, ranging from -65dBm to -27dBm.



(a) Length statistics (b) Interval statistics

Figure 3: Packet length and packet interval statistics of busy WiFi connection.

Both ZigBee nodes are installed with Contiki OS [12]. The sender transmits the packet every 0.03 seconds. In order to compensate the variation of WiFi interference signal, the sender changes the transmission power every 10 seconds, looping over the scale from 1 to 31. Similarly, both the sender and receiver change their channel every 600 seconds, looping over all ZigBee channels which could be affected by WiFi communication, from channel 11 to 25.

2.2 Analysis of ZigBee Corruption

Our experiment shows that the results from different locations are similar. We choose the result from one site for simplicity. Since the ZigBee channels covered by the same WiFi channel show same behavior, we separate the results of different ZigBee channels into 3 groups, which are covered by the WiFi channel 1, 6, and 11 respectively.

Fig. 2a and Fig. 2b illustrate the duration and interval of corrupted symbols using log-log plot respectively. We observed that different channels have similar patterns.

The results show that the corruption durations and intervals distribute similarly and are close to power-law distribution. As short corruption durations and intervals are far more frequent than those of long corruptions, it's reasonable to conclude that most of the short durations and short intervals of corruptions occur alternately. Thus, the results suggest that *short and frequent WiFi data transmission (i.e., flash) plays the main role of WiFi interference on ZigBee. Further, the power-law like distributions indicate shorter flashes will interfere ZigBee signal with exponentially increasing probability, which is a drastic threat for ZigBee signal.*

2.3 Analysis of WiFi Interference Behavior

We also collect the WiFi data in the same experiment, and investigate the behavior of WiFi transmission in detail. When massive data is being transmitted over a WiFi connection, the length of the data packet could be varied, while the interval between two consecutive WiFi packets is relatively short. Fig. 3a shows that most of the WiFi packets are short and the packet length is usually less than 256 bytes. Note that, there is a peak when the packet length is larger than 10^3 bytes, because 1500 bytes is also a typical WiFi frame length for TCP transmissions.

Fig. 3b shows that, most of the WiFi interval is less than 1ms, *i.e.*, $10^3\mu$s. Because the length of the data packet is usually with the full length of a WiFi frame, *i.e.*, 1406 bytes. When the WiFi is working on the max data rate, 56Mbps, a packet will last for 200μs, and the interval between two data packets is also seldom lower than 10μs. Note that, another peak shows between $10^3\mu$s and $10^5\mu$s, which shows that, even when WiFi communication is idle, the ZigBee communication can still be affected by the WiFi beacon and probe frames, because the beacon interval is typically $10^5\mu$s (*i.e.* 0.1s) long. Note that, the interval is much lower than $10^5\mu$s because there are multiple WiFi APs around (about 20), which will significantly shorten the beacon interval independently. Note that, there is a thick but extremely low line in Fig. 3b, which cannot be overlooked. This line shows that, part of the WiFi packets' intervals are evenly distributed across a wide range of values, although the frequency is low.

The results in Fig. 2 show similarity between interference intervals and durations. Also, most of the WiFi interferences are short and periodical. We conclude that *the WiFi interference is distributed across ZigBee symbols, rather than concentrated on particular positions. Hence it is not possible to avoid the interference thoroughly with MAC layer technique only. We need to resort to the signal processing techniques for fundamental solutions.*

3. BACKGROUND AND MOTIVATIONS

In this section we provide background on wireless communication fundamentals and single-user multiple-input multiple-output (MIMO) systems. We then describe the signal character of WiFi and ZigBee in a typical WiFi and ZigBee coexistence environment. The motivations are presented according to the technologies and observations mentioned above.

3.1 MIMO and Interference Nullifying

In a MIMO system, multiple antennas are coupled together and signals are transmitted over the channels, say mathematically, in a linear combinatorial manner. Here we show a 2×2 MIMO system using a simplified mathematical model, where the signal stream $s_i(t)$ is on the i-th antenna, $i = 1, 2$. The signal receiving model for MIMO system can be expressed as follows:

$$\begin{cases} y_1(t) = h_{11}s_1(t) + h_{21}s_2(t) \\ y_2(t) = h_{12}s_1(t) + h_{22}s_2(t) \end{cases} \quad (1)$$

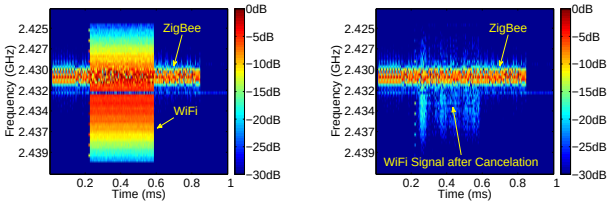
Here h_{ij} is a complex value for channel coefficient, where the magnitude attenuation and delay of a transmitted signal from antenna i to antenna j is evaluated. In each MIMO transmission, there is a previously known preamble used for channel coefficient calculation. The receiver node can compute this value according to the signal and preambles.

At the receiver side, as the 4 channel coefficient values h_{ij} are known, the transmitted signals $s_1(t)$ and $s_2(t)$ can be successfully recovered from the received signals $y_1(t)$ and $y_2(t)$. It is worth noting that, this model is applied to narrow band channel communication system, such as ZigBee. However for wideband communication system such as OFDM, the channel coefficient is a series of complex values, that is, a channel coefficient vector.

To deal with the concurrent transmissions from different stations, the interference nullifying technique can be used for unaligned signals. The key idea of the interference nullifying technique is based on Eq. (1). As for the unaligned interference signals, there are *clear part* and the *interfered part*. For the interfered part, the nullifying process is used to cancel the interference signal. For example, according to Eq. (1), the interference can be mitigated by subtracting the other interference signal when $s_1(t)$ is the interested signal.

$$s_1(t) = \frac{y_1(t) - \frac{h_{21}}{h_{22}}y_2(t)}{h_{11} - h_{12}\frac{h_{21}}{h_{22}}} \quad (2)$$

3.2 Preliminary Observations for IEEE 802.11 and 802.15.4 Signals



(a) Spectral and time domain (b) After WiFi Cancelation

Figure 4: Power Spectral Density (PSD) form of WiFi and ZigBee signals.

We demonstrate a particular co-channel example: In IEEE 802.11g, we use channel 5 (with 2.432GHz central frequency), and in IEEE802.15.4, we use channel 16 (2.430GHz). Fig. 4a shows the spectrum and time characteristics of WiFi and ZigBee signal in power spectral density (PSD), where WiFi's bandwidth is much larger than ZigBee, and they are in different central frequency.

Signals in Fig. 4a are sampled by USRP/GNURadio in WiFi channel, which conforms to the IEEE standards 802.11g and 802.15.4: WiFi's bandwidth is 20MHz, and ZigBee's bandwidth is 2MHz, while central frequency offset of WiFi and ZigBee is 2MHz. The payload of WiFi is 256 Bytes with TX rate 6Mbps, and the payload of ZigBee is 20 Bytes with TX rate 250kbps. As we can see, WiFi is faster than ZigBee, and WiFi signal is 5 to 10dB stronger than ZigBee. We only consider co-channel interference case.

The differences are just that they collide in different frequency. Here Fig. 4a shows collided WiFi and ZigBee signal in time domain. We can tell WiFi signal from ZigBee signals easily. First, the ZigBee signal is slower than WiFi due to its low bandwidth. Second, WiFi's signal is stronger than ZigBee due to its high-power. High-power implies high SNR reception at the same distance. Fig. 4b shows the PSD of ZigBee signal when WiFi interference is canceled. This demonstrates the feasibility of recovering ZigBee signal from WiFi interference.

3.3 Motivations

Basically, there are three technical points driving us to tackle the intrinsic difficulties in mitigating the WiFi flashes from the ZigBee smog.

The cross technology interference leaves opportunities in power, spectral and time domain. As shown in Fig. 4, there are opportunities for protecting ZigBee smog from WiFi flashes. First, in power domain, significantly different signal strengths may exist between WiFi and ZigBee. Second, in spectral domain, only portion of WiFi frequency band is interfered. Third, in time domain, not all signal duration is interfered, and referred signal can be leveraged for further interference mitigation and decoding enhancement. It should be noted that, except for the frequency domain, the power and temporal differences are dynamic and not easy for use.

The nullifying process on coupled antennas can deal with the power and temporal uncertainty. The MIMO design can deal with the power uncertainty easily, because signals from same node on different antennas may not have significant difference. Also, only the overlapping portion is nullified, where temporal differences can be omitted temporarily before further processing.

Harmonize ZigBee with WiFi system is possible and feasible. MIMO based sink will receive the WiFi and ZigBee signal at the same time. Preferable interference cancelation of WiFi signal relies on the accurate recovery of the WiFi signal. A 2-antenna MIMO system will also improve the possibility on WiFi signal recovery. The ZigBee and WiFi can work together as if they are from the same technology, and no interventions among systems are needed.

4. ZIMO PROBLEM DOMAIN

ZIMO deals with interference from WiFi APs and protects the ZigBee signals from being corrupted. We focus on typical situations that arise in large-scale urban sensing networks, where WiFi and ZigBee signals are severely interfering each other. In particular,

- *ZIMO tackles scenarios where the WiFi APs use antennas no more than what the ZIMO Sink has.* Typically, the WiFi transmissions use one antenna. If n-antenna system such as [13] is applied in WiFi AP, the ZIMO node should place $(n+1)$ antennas for transceiving packets. Such constraint also applies to other cross technology devices in ISM band.
- *ZIMO applies to scenarios where at least one preamble is clear when interference happens during data transmissions.* The preamble value, whether it comes from WiFi or ZigBee, should be clear for packet detection as well as channel coefficient estimation.
- *ZIMO applies to scenarios where the ZIMO empowered sink node can be deployed in the asymmetric area [6].* Considering the long-range coverage region by WiFi and the limited communication range of ZigBee devices for power saving, the asymmetric area is common in urban sensing networks. Also, even in symmetric area, the ZigBee sensor node and WiFi node can disable the CCA scheme, and transmit packets as they will.
- *ZIMO can address environments where the interference is wideband and the interested signals are narrow-band.* When WiFi and ZigBee technologies are coexisted, the reference signal for WiFi channel coefficient computation is often unavailable. Extracting ZigBee from WiFi and other cross-technology system is apparently different from previous study such as TIMO [1].

5. ZIMO DESIGN OVERVIEW

In ZIMO design, the conventional one-antenna sink node is modified to a 2-antenna MIMO system. The WiFi and ZigBee signals can be transmitted concurrently and then received by this sink.

The basic idea of ZIMO is simple. When WiFi preamble is clear, we use the interference nullification to WiFi signal directly, and leave the residual signal for ZigBee decoding. When WiFi preamble is not clear, we need to leverage the clear ZigBee preamble to nullify ZigBee signal. After that, WiFi signal can be decoded. Using the decoded data and accurate channel coefficient, we can regenerate the received WiFi signal accurately. After using the interference cancellation technique, the WiFi interference is mitigated, and the residual signal can be used for ZigBee decoding.

The working flow of ZIMO is illustrated in Fig. 5. There are basically five operation modules in ZIMO, which are

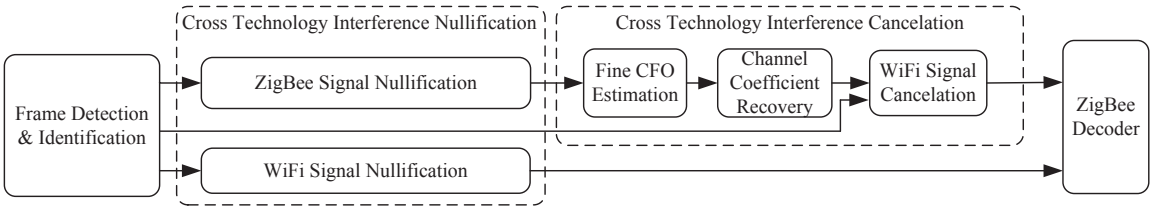


Figure 5: Working flow of ZIMO

frame detection & identification, spectrum slicing, cross technology IC (Interference Cancelation) and IN (Interference Nullification), and ZigBee decoder. When interfered signals are received, the frame detection & identification module is applied for interference pattern recognition. When WiFi preamble is clear, we first nullify the WiFi signal and send the signal to spectrum slicing module for ZigBee decoding. Specifically, when WiFi flashes (fast and short-duration WiFi transmissions) are covered by ZigBee smog (slow and long-duration ZigBee transmissions), although ZigBee signal is nullified, the estimated channel coefficient cannot be used for IC directly due to interfered WiFi signals. Thus in ZIMO, we use a linear fitting model for fine central frequency offset (CFO) estimation. After CFO is compensated, channel coefficient is recovered through blind recovery method, where missing values are interpolated by leveraging the partially interfered channel and SNR disparity in cross-technology coexistence. In summary, ZIMO extends convention MIMO system as well as virtual MIMO, such as SAM [11], from multiplexing signals in same technology to embracing cross-technology. Also, we make an extension to TIMO because ZIMO makes it possible to survive the ZigBee signal from WiFi interference. We then describe these basic functions in detail in the following sections.

6. DECODING IN THE PRESENCE OF WIFI INTERFERENCES

6.1 Spectrum Slicing and Combining

In order to incorporate ZigBee and WiFi signal for processing, ZIMO uses wideband RF frontend. However, wideband sampling means that sampled signal has wide spectrum, which cannot be used for ZigBee decoding directly. Then in ZIMO, a spectrum slicing block is used to convert the over sampled signal to appropriate signal for ZigBee decoding. In this work, we use WiFi setup (*e.g.*, WiFi channel No.5: with central frequency at $2.432GHz$, and $20Mbps$) to determine front-end parameters (complex sampling rate: at least $40Mbps$).

We take only one ZigBee transmission in our experiment study because of contention scheme in IEEE 802.15.4. The extension to multiple orthogonal ZigBee networks is possible: all we need is to add parallel reception chain with different frequency translation parameters.

6.2 Interfered Frame Processing

6.2.1 Frame Detection and Identification

The auto-correlation is a basic step for frame detection, which means a multiplication of received signal and its delayed version, and the sum of all the multiplications during the delayed period. Auto-correlation method can be used for clear header signal. However, the deferred signal can not use this method because the interference destroies the correlations among symbols.

In dealing with this difficulty, we group 80 samples for one checking window (equal to one symbol length), and make 64-point FFT for subcarrier energy detection. Once the detected energy is 5 dB (verified by our experiments in Section 8.2.3) higher than the noise, the interference signal is identified. Further, we need to identify whether the interference comes from WiFi or ZigBee. Luckily, WiFi is wideband signal and ZigBee is narrow band, we can use the occupied subcarrier number for interference identification.

6.2.2 Boundary Detection

Another important issue is boundary detection, *i.e.*, determining where the interference happens. Accurate 'clear preamble' identification is highly correlated with the packet detection and further interfered signal resolution. For signal detection, we take the standard auto-correlation approach that is widely used in packet detection. For WiFi signal, we exploit repeat patterns in short training symbol (STS) for detection. After compensating the frequency offset, we use the long training symbol (LTS) for accurate frame boundary detection. And for ZigBee signal, when preamble is autocorrelated, the frequency offset will be compensated. Thus the start of frame delimiter (SFD) can be detected through cross-correlation, which means the start of a ZigBee packet. Note when ZigBee header is interfered, the WiFi nullification process will ensure the preamble autocorrelation and reliable SFD recovery.

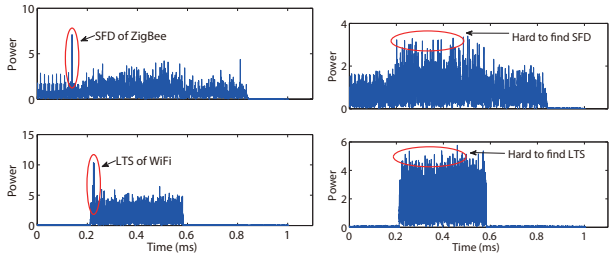
For signal detection, auto correlation is enough, and will not be affected by the frequency offset. However, boundary detection need more accuracy, which is different from signal detection with repeated patterns, e.g., the preambles. In ZIMO design, we use cross correlation instead of autocorrelation. First, we use STS for signal detection. After receiving the signal and successful frequency offset compensation, we can actually leverage the LTS, which has given and known symbols, and achieve robust boundary detection. Fig. 6 shows the effects of frequency compensation for boundary detection when WiFi signal is interfered by ZigBee. Fig. 6a shows clear WiFi and ZigBee boundary through SFD and LTS respectively. However, when frequency offset is not compensated, it is hard to identify the boundary as shown in Fig. 6b.

6.3 ZigBee Channel Coefficient Estimation

6.3.1 Frequency Offset Compensation

Compared with WiFi systems, the main challenge is that we have to use the short and simple preamble in ZigBee system with frequency bias up to $200KHz$. Thus, the key technology is frequency compensation.

The received band OQPSK signal $x(n)$ with a phase index k ($k = 0, 1, 2, 3$), frequency offset δ_f and phase offset δ_ϕ can



(a) Boundary detection for WiFi signal (b) Boundary detection without frequency compensation

Figure 6: Effects of frequency compensation for boundary detection

be expressed as:

$$x(n) = A_n e^{(j(k\pi/2+2\pi\delta_f n+\delta_\phi))} \quad (3)$$

According to Equ.3, there are three main factors affecting the received signal,*i.e.*, modulation, frequency offset and phase offset. To mitigate the modulation values from our equation, we raise our received signal with the power of 4. Note that only four cases can happen in modulated signal, *i.e.*, 0, $\frac{\pi}{2}, \pi, and \frac{3\pi}{2}$. When the subsystem raises the signal to the power of 4, the phases of the modulated signal have all been shifted to multiply of 2π, which can be eliminated from the received signals.

Therefore, to eliminate the effect of modulation,

$$x^4(n) = A_n^4 e^{(j(2k\pi+4(2\pi\delta_f n)+4\delta_\phi))} = A_n^4 e^{(j(4(2\pi\delta_f n)+4\delta_\phi)))}$$

After that, we perform an FFT on the modulation independent signal to estimate the tone at four times the frequency offset. The received signal can be corrected by:

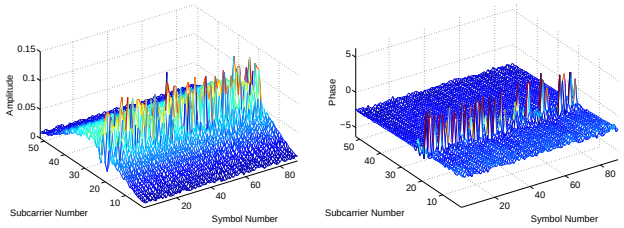
$$y(n) = x(n)e^{-j2\pi\delta_f n} = A_n e^{(j(k\pi/2+\delta_\phi))}, k = 0, 1, 2, 3$$

There is usually a residual frequency offset even after the coarse frequency compensation, which would cause a slow rotation of the constellation. In ZIMO implementation, the sample frequency $f_s = 2MHz$, and FFT size is 2048. The minimum frequency offset value is $\delta_f^{min} = 244.14Hz$ and the maximum offset $\delta_f^{max} = 250kHz$. Our evaluation results in real wireless environment show that the coarse frequency compensation is enough for channel coefficient estimation to nullify ZigBee signal.

6.3.2 *Timing Recovery*

After frequency compensation, the time recovery is needed to achieve accurate channel coefficient. The timing recovery subsystem implements a PLL (Phase Locked Loop) to correct the timing error in the received signal. The input of the timing recovery subsystem is over-sampled by two for basic over-sampling processing. Four folds or higher makes no difference as two is enough. On average, the timing recovery subsystem generates one output sample for every two input samples. The NCO (Numerical Controlled Oscillator) control subsystem implements a decrementing modulo-1 counter to generate the control signal to select the interpolations of the Interpolation Filter. This control signal also enables the Timing Error Detector (TED), so that it calculates the timing errors at the correct timing instants.

The NCO Control subsystem updates the timing difference for the Interpolation Filter, generating interpolator structure. Based on the interpolations, timing errors are generated by a zero-crossing Timing Error Detector, filtered by a tunable proportional-plus-integral Loop Filter, and fed into the NCO control for a timing difference update. The Loop Bandwidth (normalized by the sample rate) and Loop Damping Factor are tunable for the Loop Filter. The default normalized loop bandwidth is set to 0.07 and the default damping factor is set to 2, such that the PLL quickly locks to the correct timing while introducing little noise.



(a) Amplitude (b) Phase

Figure 7: Amplitude, phase of channel coefficient on overlapping ZigBee and WiFi

6.4 Interference Nullifying

In ZIMO, to remove the WiFi impact, we need to mitigate the ZigBee signal temporarily for further WiFi signal cancelation. Inspired by two antenna MIMO-based design, we use interference nullifying process for ZigBee noise mitigation. When WiFi signal is 'covered' by the ZigBee smog, we should first nullify the ZigBee smog according to Eq. (2) in Section 3.

As ZigBee signal is narrow band, for efficient computation, we estimate channel coefficient in time domain. The optimal equalizer will minimize the differences between received signal $y(t)$ and the training signal $w(t)$, where

$$\mathbf{c} = \arg\min_{\mathbf{c}} \|w(t) - \mathbf{c} * y(t)\|$$

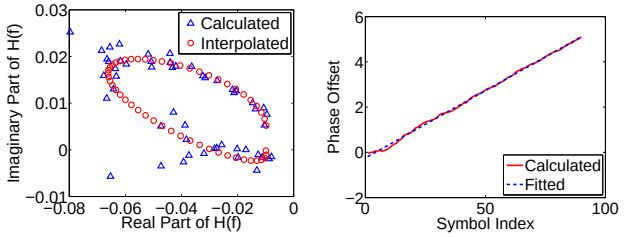
In the time domain, $\mathbf{c} = \{c_{-L}, \cdots, c_0, \cdots, c_L\}$ is a good estimation of channel coefficient $\mathbf{H}$. For WiFi signal, we compute the channel coefficient in frequency domain, using the FFT of the received signal to divide that of transmitted signal. Then the interference nullifying technology is applied for cross-technology data decoding.

6.5 Interference Cancelation

If we can separate WiFi signal from the mixed signal, we can use standard ZigBee decoder to extract ZigBee packets. The overall processing is called Successive Interference Cancelation (SIC).

6.5.1 *Fine frequency offset estimation for WiFi*

Fine carrier frequency offset (CFO) estimation is necessary to minimize the residual noise after interference cancelation (IC). Inaccurate CFO estimation will lead to increased residual noise over time. A coarse estimation in WiFi training symbols (*i.e.* STS & LTS) is not enough for IC because of limited preamble length and noise. For finer CFO estimation, we remodulate the received data, and compare the phase shifts with the received symbol. Note that, our scheme is data aided, because the remodulated symbol can be achieved after the coarse CFO estimation.



(a) Interpolation result in Real part and Imaginary part (b) Fitting line of fine frequency offset estimation for WiFi

Figure 8: Improvement methods for WiFi IC

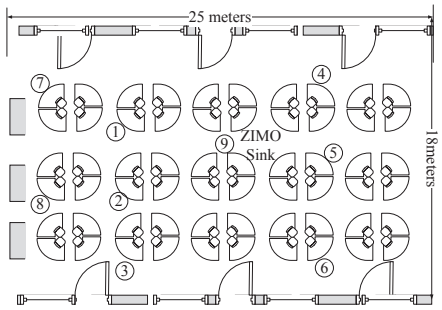


Figure 9: ZIMO test environment with 9 testing locations

As the synchronization process in preamble has successfully compensated the clock difference between sender and receiver, the phase shifts grow linearly with the accumulative symbols in a constant CFO estimation. Consequently, we use linear regression method across symbols in achieving the CFO estimation. The fitting model is based on minimizing the least squares of the noisy data. As shown in Fig. 8b, the fitting line is regressed from the calculated phase shifts over the symbols. There is also a merit in using this CFO estimation method, that is, the channel coefficient can be corrected during data transmission in any length.

6.5.2 *Blind Recovery for WiFi Channel Coefficient*

To recover the channel coefficient $\mathbf{H}_w$ for interfered WiFi signals blindly, we use the interpolation method for the missing data. Here blind means recovery channel coefficient without any additional information. The key insight is that, in cross technology coexistence of WiFi and ZigBee, the frequency occupation scheme differs. Note in frequency domain, WiFi can only *partially* overlap with the ZigBee signal as shown in Fig. 7. As ZigBee is a narrow band system while WiFi is wideband, we can reasonably recover the overlapping coefficient according to the known channel coefficient in other subcarriers. Other MIMO multiplexing schemes, *e.g.* SAM [11], can not take this advantage due to the complete frequency overlapping signals in same technology.

We interpolate the interfered parts of WiFi channel coefficient with a fourth-degree polynomial function, and the unknown fitting parameters are computed by minimizing the sum of the squares of deviations. For channel coefficient estimations, quartic-function is smooth enough. We show the interpolation result in Fig. 8a, which validates our scheme. We use the real part versus imaginary part comparison in Fig. 8a to show the relationship between calculated channel coefficient and the interpolated value. Obviously, the effect of the cross-technology interference is reduced, and a reasonably accurate channel coefficient for WiFi is recovered.

6.5.3 *WiFi Interference Cancelation with ZigBee*

To be more accurate, let us assume the mixed (collided) signal is $y_m(t)$, and the mixed signal is down-sampled using central frequency and bandwidth of WiFi setup. Let $x_w(t)$ be the packet bits from WiFi, and $x_z(t)$ be the packet bits from ZigBee. Then we have

$$y_m(t) = \mathbf{H}_w x_w(t) + \mathbf{H}_z x_z(t) e^{j2\pi\delta_f t} + n(t)$$

where $\mathbf{H}_w$ and $\mathbf{H}_z$ are the channel coefficient of WiFi and ZigBee respectively, and δ_f is the central frequency offset between WiFi and ZigBee.

Due to successful ZigBee signal nullification, we can get $x_w(t)$ using standard decoder from the WiFi signal (ZigBee signal is nullified). Then we re-modulate the WiFi signal as $S_w = \mathbf{H}_w x_w(t)$, and setup a new formula as $Y(t) = y(t) - S_w = \mathbf{H}_z x_z(t) e^{j2\pi\delta_f t} + n(t)$. Then we can process $Y(t)$ to get ZigBee packet.

6.6 ZigBee Data Decoding

The data decoding subsystem performs fine frequency offset compensation, phase ambiguity resolution, timing recovery, OQPSK demodulation, chip to symbol decoding and CRC calculation. Fine frequency offset compensation is achieved by a Phase Locked Loop (PLL). Next, we exploit the preamble to resolve phase ambiguity. Particularly, we calculate the cross correlation of input signal and modulated symbol zero. Then we estimate the phase of the cross correlation result. We classify the estimated phase ambiguity into 0, $\pm\frac{\pi}{2}$ and π phase offset. The input signal for demodulation is corrected with this phase ambiguity. After timing recovery, the received signal is demodulated to chip sequence.

Once a preamble symbol is detected, we continuously search the SFD byte in the incoming signal. If SFD is found, the PHR (PHY headeR) information can be extracted and the packet can be resembled. After that, the CRC of this packet can be calculated for verifying correctness of packets.

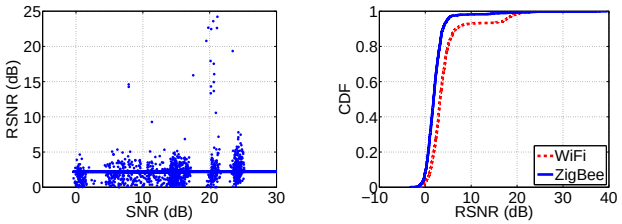
7. IMPLEMENTATION

We use GNURadio/USRP N200 software radios to evaluate ZIMO performance, because ZIMO design requires total control of wireless physical layer (*e.g.*, WiFi and ZigBee signal-level control), which cannot be accomplished using commercial network interface cards and sensor nodes. However, due to the inherent unpredictable and long latency between RF frontend and hosts, software radios cannot support precise MAC timing control. We have built a prototype of ZIMO sink with GNURadio/USRP N200, including all components described in Section 6. As in the literature we use trace-driven approach. The real-time trace is collected using USRP/GNURadio, and then fed into decoder. We not only study the physical layer performance, but also conduct network level experiments.

We implement the OFDM PHY layer of WiFi and OQPSK PHY layer of ZigBee. The bandwidth of WiFi and ZigBee is 20 MHz and 2 MHz respectively. In Section 8, we will demonstrate that, our design can ensure sufficient number of processing for every interfered patterns in our random sampling collections.

Table 1: Setup for Test-bed

No.	WiFi			ZigBee		
	Dist (Loc)	Amp	SNR (dB)	Dist (Loc)	Amp	SNR (dB)
1	5(1)	0.3	23.6-35.6	5(5)	0.15	14.7-24.5
2	5(1)	0.25	11.8-34.2	5(5)	0.1	15.8-21.8
3	5(1)	0.2	14.2-32.1	5(5)	0.05	-0.3-7.3
4	7(6)	0.2	4.2-23.4	10(7)	0.2	5.6-17.3
5	10(8)	0.2	3.4-18.4	10(7)	0.2	0.3-15.8
6	10(8)	0.3	10.0-23.0	10(7)	0.2	4.1-15.9



(a) RSNR across different SNR values

(b) CDF of RSNR, with ZigBee & WiFi signals

Figure 10: IN performance in RSNR, the solid line in 10a shows the linear regression of the data.

8. EXPERIMENTAL RESULTS

8.1 Experiment Setups

Fig. 9 shows the layout of our testing environment. It's a typical semi-open office floor with table and cubicles. For simplicity of explanation, both WiFi and ZigBee channels are assumed to be fixed. The channel number of WiFi and ZigBee is 5 and 16, *i.e.*, 2.432 GHz and 2.430 GHz. WiFi uses BPSK and $\frac{1}{2}$ channel coding rate (*i.e.*, 6Mbps), and ZigBee system is set to 250Kbps. We select the WiFi and ZigBee payload length to be 256 Bytes and 20 Bytes respectively. And in our system design, the transmission durations are 0.358ms and 0.8325ms respectively. In order to evaluate the ZIMO decoding performance under WiFi interference, we need to collect collision signal. However, it is non-trivial to synchronize two USRPs, since the packet collision happens in signal-level. 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 1ms, and WiFi packets are sent periodically every 2.5ms. Because ZigBee and WiFi have different packet lengths, the overlapping pattern can change as packets accumulate, but be retained periodically.

The ZIMO sink is fixed at location 9, while WiFi and ZigBee transmissions are randomly selected from other 8 different locations in Fig. 9. ZIMO sink captures 10 traces of the channel periodically. Each trace contains around 200 ms signal data on one 20 MHz 802.11g channel, which is equivalent to collect over 1000 packets in the air. Thus over 10,000 respective WiFi and ZigBee packets are collected, which contain various interfered patterns for validated evaluation.

The experiment is evaluated in different locations with various SNR values. Table 1 shows the configurations of USRP based WiFi and ZigBee nodes. We use 6 different location pairs in total. The 'dist' column shows the distance between ZIMO sink and the configured WiFi/ZigBee node with exact number in brackets shown in Fig. 9 accordingly, and the 'Amp' column is the amplifying factor in RF end. Notably, the 'SNR' column shows the range of SNR value in respective location. In our configuration, although distances are not very long, the SNR values are dynamic with multiple choices, which would be helpful for further evaluation tests. Comparing with the larger scale experiment setups, ours could provide more SNR levels for evaluating the effects of interference handling processes comprehensively.

8.2 Micro Benchmark

We evaluate ZIMO using GNURadio/USRP software radio testbed. Our goal is to show ZIMO is plausible in realistic environments. We conduct micro-benchmark to evaluate the three key techniques in ZIMO, including interference nullification, interference cancelation and interference detection performance. We then show the benefit of ZIMO for coexisted networks, by measuring the end-to-end throughput gain of ZIMO over conventional wireless sensor network as well as WiFi networks.

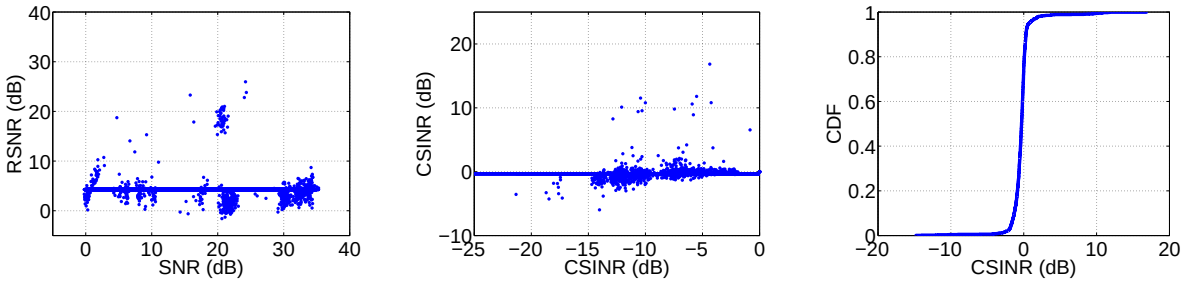
8.2.1 *Interference Nullify of ZigBee & WiFi Signal*

We first study the performance of interference nullification (IN) in the ZIMO implementation.

As stated in Section 6, the IN step of ZigBee signal is important for IC of WiFi signal. Only the well performed IC in WiFi will lead to ideal ZigBee data decoding. Similarly, the WiFi signal IN is also a fundamental step for ZigBee signal decoding. To evaluate how effective our IN algorithm performs, we examine the (Residual Signal+Noise) to Noise Ratio (called RSNR) after IN process under different SNR settings. This rule can here be applied to both WiFi and ZigBee signals. RSNR is defined as $\frac{R+N}{N}$, where R is the residual noise after IN and N is the energy of background noise. Obviously, lower RSNR in fixed background noise N means better performance of IN. Also, we need to evaluate the residual noise across different background noise.

Fig. 10a shows the result of ZigBee signal nullification. The x-axis shows the average of SNR values of the ZigBee signal with clear preamble at both antennas. Observe that the majority of frames are with SNR between 0dB to 25dB, which is the usual SNR range for ZigBee system to work reliably in practice. We also observed frames with very low SNRs. This is due to the dynamic fading effects of ZigBee channel. We notice that IN has removed a significant portion of interfering energy, and the majority of RSNR is very small, with 0 to 5dB higher than the noise. The solid line is a linear regression of the data, which shows the steady performance of IN. In practice, many wireless links work at higher SNR range than this minimal requirement. For example, in our data set, most ZigBee links have a SNR higher than 10dB. Thus, this additional noise has little impact on the following decoding process. We then evaluate the residual noise level over all SNR settings. Fig. 10b plots the Cumulative Distribution Function (CDF) of the RSNR values for ZigBee signal. We can observe that over 90% cases, IN can effectively remove the interference and the resulted RSNR is less than 4dB. There are only around 5% cases that RSNR is larger than 5dB, such that, the decoding of the WiFi may be affected.

Similar results are also shown in Fig. 11a. The WiFi signals are ranging from 0dB to 35dB, and most of the signals



(a) RSNR of WiFi Nullification (b) CSINR of WiFi Cancelation (c) CDF of WiFi Cancelation

Figure 11: WiFi nullification and cancelation.

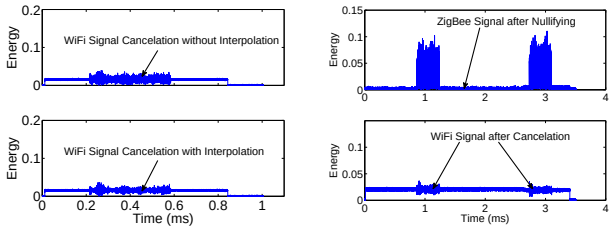
are nullified below 5dB. Notably, in Fig. 11a, small but significant portion of residual signals are around 15dB to 25dB when the input signal is around 20dB, because the WiFi preamble is interfered but can still be detected. Actually, the channel coefficient value is not accurate. As the interference detection module will not take this case as interference, the residual noise after IN is not satisfiable. When the signal is larger than 20dB, the ZigBee interference signal will not effectively affect the WiFi IN process.

8.2.2 *Interference Cancelation of WiFi Signal*

Next, we evaluate the performance of interference cancelation in the ZIMO implementation. We use the same experiment setups and same data as in the previous experiment. 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. If the interference can be successfully canceled, the line will be very close to the line '$x = 0$'. Then, we evaluate how effective our IC algorithm can improve the CSINR value of the first frame and thereby enable correct decoding.

Fig. 11b shows the CSINR of the ZigBee after canceling the interference from WiFi. The x-axis is the SINR before IC. We observed the follows. First, IC effectively improves SINR of the frame by reducing the energy from interference. From Fig. 11b, we can see that SINR has been substantially improved up to $15dB$, and most of the SINR values are around 5 to 10dB. Thereby the interfered ZigBee frames can all be decoded successfully. Second, the improved SINR value reduces as the original SINR increases. This is reasonable since SINR is a ratio between the desired signal energy and the sum of interference and noise. A larger SINR usually means the interference is small. As shown in Fig. 11c, the CDF of CSINR shows that, over 95% SINR value is around 0dB, which means the successful IC process.

Fig. 12a shows the cancelation effects between our interpolation method and original method without correction for channel coefficient. The upmost sub-figure shows the interfered ZigBee signal with WiFi flash, and there is no clear WiFi signal for reference. The middle sub-figure shows the cancelation effects of the original method. The bottom sub-figure shows that, the interpolation method has provided significantly ideal cancelation effects for ZigBee signal decoding. It will also contribute to the WiFi data recovery, which leads to co-prosperity in ZIMO.



(a) Interpolation scheme for IC (b) Multiple WiFi cancelation

Figure 12: WiFi cancellation effects

When ZigBee smog is interfered by multiple WiFi flashes, ZIMO can still work without modification. Fig. 12b shows that, in such case, after the ZigBee signal is nullified, the WiFi flashes are significantly detectable. Whether it comes from same WiFi AP or multiple APs, the cancelation process can work independently and automatically, where the WiFi interferences can be successfully mitigated.

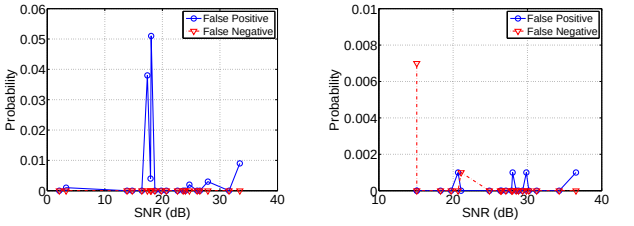
8.2.3 *Frame Detection Accuracy*

We evaluate the accuracy of frame detection of ZIMO under different SNR settings. The data is generated and collected with USRP devices. Various overlapping patterns are presented, where over 1,000 WiFi and 1,000 ZigBee frames are used for accuracy evaluation of ZIMO frame detection.

Fig. 13 shows that, the false negative (FN) rate is always negligible, even in very low SNR. This result means ZIMO can reliably detect the WiFi and ZigBee frame. The false positive (FP) values in Fig. 13a, although are relatively high in low SNR, will not affect the network performance much. For ZigBee signals, it only costs unnecessary ZIMO processing. For keeping the FN low, raising the FP value a little higher is tolerable and reasonable.

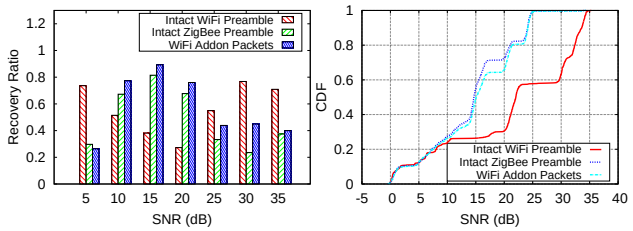
8.3 Throughput Gain of ZIMO

We then evaluate throughput gain of ZIMO under the GNURadio-USRP implementations. We mainly compare the throughput of ZIMO to a baseline system designed for comparison. We use the following method to measure the throughput of ZIMO as our current decoder cannot run in real-time due to hardware limit. The ZIMO sink node will take 100 snapshots during 3 hours randomly. Each snapshot contains 200ms data, which is equivalent to 100 frames



(a) ZigBee frame (b) WiFi frame

Figure 13: Frame detection accuracy in FP & FN



(a) Different SNR values (b) CDF versus SNR

Figure 14: Recovery ratio of ZIMO network.

in different interference patterns and 10,000 frames in total. We store the data and process it off-line. With these traces, we can estimate the throughput as well as the recovery ratio during the snapshot period.

8.3.1 Baseline System Design

Our baseline system is designed according to IEEE standards 802.11 and 802.15.4. The reference codings and procedures are validated, evaluated, and tested for standard conformance sufficiently. We omit the details due to page limit. In summary, the baseline system can successfully tranceive WiFi and ZigBee packets and can decode COTS WiFi and ZigBee packets as well.

8.3.2 Throughput Gain of ZIMO over ZigBee

Fig. 14a shows the recovery ratio of ZIMO across different levels of SNR value. In the 'x-axis', the SNR value is calculated according to the first received intact symbols. Thus, when the intact preamble is from ZigBee, the SNR value is calculated by ZigBee symbol at the receiver side. Also, SNR is accordingly computed for intact WiFi preamble. In 'y-axis', we evaluate the recovery ratio, which is the fraction of the successfully recovered ZigBee packets among all the interfered packets. Notably, for WiFi packets, we also evaluate the case where WiFi packets can be recovered when ZigBee interference exists.

The recovery ratio of ZIMO ranges from 20% to 80% when ZigBee preamble is intact, and up to 90% when WiFi preamble is intact. Note that with higher SNR value, the benefits of ZIMO degrade. For WiFi network, this degradation is due to the interference of ZigBee. Fig. 14b shows the CDF of the recovery ratio for the cases mentioned above.

Fig. 15a shows the throughput gain of ZIMO comparing with the baseline system. We observe that for all cases, ZIMO significantly improves the network throughput compared to ZigBee. It shows that coexisting WiFi and ZigBee signals with MIMO can make full use of two antennas by overlapping two concurrent transmissions from cross technology. Three cases are listed for clear evaluation and categorization. The 'intact ZigBee preamble' and 'intact WiFi preamble' means reliable detection of the packets because the preamble is not affected. These two cases are used to illustrate the performance of ZIMO in different processes. It is 'IN+IC+Decoding' comparing with the 'IN+Decoding'. Interestingly, to show the effects of the harmonizing process, where WiFi data can be recovered for the IC process, we take the 'WiFi add on packets' for evaluation, showing the recoverability of the interfered WiFi signals during ZIMO process. Note that, it is a special case of 'intact ZigBee preamble', because only in this case, the WiFi data can be recovered as a co-prosperous gain under the favorable 'IN+IC+Decoding' process.

In Fig. 15a, the 'x-axis' is location pair, which is labeled with $\langle i, j \rangle$, denoting WiFi node at location i, and ZigBee node at location j, as shown in Fig. 9. In 10 location pairs of our experiment, ZIMO makes over 3-folds throughput gain.

8.3.3 Throughput Gain of WiFi Network

We then evaluate the throughput gain of WiFi network, which is illustrated in Fig. 15b. There are about 200kbps to 400kbps throughput gain across location pairs. Except for location pair 2, where the gain is not significant. The main reason is, the WiFi signal (from location 1) strength is comparatively much higher than ZigBee signal (from location 2). Thus, the ZigBee will not make effective interference, *i.e.* corruptions, on WiFi signal.

We thus claim that ZIMO enables co-prosperity in coexisting cross-technology systems with only one MIMO sink node. Note that, comparing with the asymmetric regions, the ZigBee interference is relatively weak. However, the WiFi data corruptions are not negligible. In some location pairs, *e.g.*, location pairs 3, 9, 10, the throughput gain is nearly 2-folds to the baseline system.

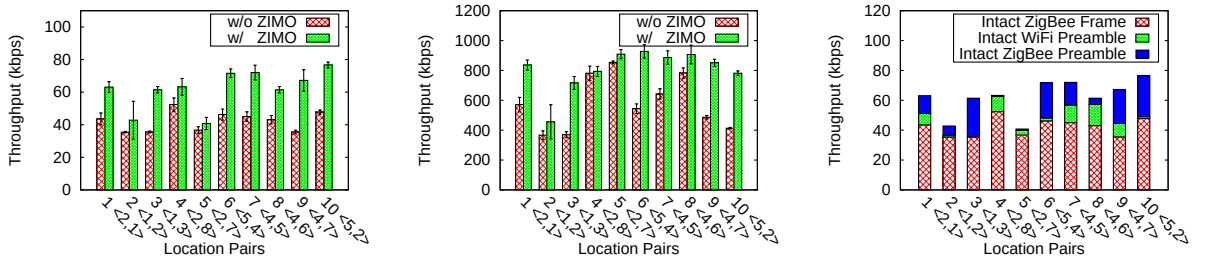
8.3.4 Structural Analysis for Interference Patterns

Fig. 15c shows the throughput of ZIMO, also with the statistical result for different interference patterns (InPs). It is shown that, in most location pairs, three InPs, including intact WiFi preamble, intact ZigBee preamble and intact ZigBee frame (no interference) are well distributed, *i.e.* no significant difference on the number of interfered packets among InPs, which shows that our configurations on packet length and interval are reasonable. The structural analysis will provide us information about the InPs and help us know how the ZIMO performs. For example, if we know the InPs, there are two potential enhancements: one is for the optimal placement of ZIMO sinks, while the other is for the optimal number of ZIMO sinks. Obviously, the structural analysis is more precise than conventional spectrum sensing schemes for ensuring good throughput performance.

9. DISCUSSIONS

9.1 Fundamental Differences from TIMO

Applying TIMO technology [1] directly to Sink node will not help us solve the coexistence problem. Actually, ZIMO is fundamentally different from TIMO. The main difference is, when WiFi and ZigBee signals are interfering each other, successful WiFi decoding will not ensure successful ZigBee signal recovery. When we need to recover ZigBee signal un-



(a) ZIMO over ZigBee baseline system (b) ZIMO over WiFi baseline system (c) Fractions of interference patterns

Figure 15: Throughput gain of ZIMO network over baseline system in distinctive location pairs

der WiFi interfere, decoding WiFi is not enough, because we have to achieve a more accurate channel coefficient under the CFO (Central Frequency Offset). The main challenge is to make a finer and more accurate channel coefficient estimation for WiFi decoding, tackling the relatively large CFO and interfered channel coefficient values. Note that, in interfered signals, achieving accurate CFO evaluation directly is extremely difficult. In tackling these difficulties, we use the frequency offset estimation method and channel coefficient interpolation to recover ZigBee data from WiFi interference.

9.2 Coexisting with Multiple WiFi and Other Cross-technology Signals

Our concern originates from a real deployed large-scale wireless sensor network, CitySee [3], the world largest environment monitoring network based on wireless sensors. When these sensors are deployed in city scale, especially in residential area, shopping mall, and railway stations, etc, the WiFi interference became the No.1 interference source to ZigBee network transmission and forwarding. On the other hand, numerous sensor nodes (For GreenOrbs and CitySee projects in WuXi, China [3], there will be up to 4,000 wireless sensor nodes at the end of 2013, and over 10,000 ZigBee-based sensors before 2015!) make the modifications on either software or hardware extremely difficult. It is also very interesting and challenging to deal with Bluetooth and other cross technology devices. We will focus on this topic in future work.

9.3 Extension to Multihop Scenario

Our scheme only works in one hop away for WiFi and ZigBee transmission. Extending our solution to multi-hop network will need multiple or dynamic ZIMO sink deployment. It's similar to cellular network deployment and optimizations, which has been widely studied. Moreover, adding ZIMO sink will be easy and affordable, especially for densely deployed WSNs.

The only difficulty lies in the site survey for interference between cross technology devices. Fortunately, there are some candidate solutions in recent studies. For example, Zhou *et al.* [14] propose an instructive method for mining the practical conflict graphs for dynamic spectrum distribution, especially in outdoor scenario. Also, inspiring works are leveraging the crowdsourcing data [15] [16] to characterize the signal and interference map for indoor scenario.

10. RELATED WORK

In most of the previous studies, WiFi is the interested signal, and other mixed signals are eliminated as interference [1,5]. In technology independent multi-output receiver design, *e.g.*, TIMO [1], the ZigBee transmissions are treated as same band interference with microwave interference. Solutions making the WiFi network aware of the existence of ZigBee are not bandwidth efficient [7, 17], because the high speed WiFi node is suppressed by the ZigBee notification. Suppressing subcarriers will also lead to performance reduction [7, 18]. Leveraging the silent duration between WiFi transmissions is a passive method [4], where the ZigBee transmissions depend on WiFi networks. Liang *et al.* [6] proposed multi-header (for handling symmetric regions) and payload redundancy (for handling asymmetric regions) to protect the ZigBee data, but the sensor node needs to be reprogrammed. Another inspiring and creative work is Picasso [19], a full duplex wireless system with only one antenna, providing adaptive and efficient RF and spectrum slicing. Such technology can be used for efficient coexistence only when spectrum usages are not conflicting or overlapping. Such constraint makes Picasso not suitable to address our concern without intervening or modifying deployed WiFi and ZigBee systems.

Special signaler devices were introduced to improve the visibility of low-power ZigBee in [17, 20]. A special node emits strong jamming signal [20] or fake WiFi header [17] during ZigBee transmission to let WiFi backoff explicitly. Radunovic *et al.* [21] redesigned 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 performance degradation, and WiFi can also have anti-jamming capability [22] 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.

Then several solutions [7, 18, 23] utilized 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 [7,18] or learning [23]), decide which spectrum ZigBee networks are using, and nullify those spectrum to enable simultaneous access. The subcarrier suppressing solution requires hardware redesign of high-power nodes, *e.g.*, preamble design and packet detection algorithm, which limits the application if it is not compatible with existing devices.

Inspiring works SAM [11] and IAC [9], used interference cancelation technique in multi-user MIMO scenario. Moreover, [9,24,25] demonstrated the interference cancelation using DSSS style communication system, while we use OFDM.

WiZi-Cloud [26] proposed to use additional ZigBee radios to help WiFi clients achieve ubiquitous connectivity, high energy efficiency, and real time inter-AP handover. WiBee [27] exploited low-cost ZigBee sensor networks to build real-time WiFi radio maps.

11. CONCLUSIONS

We presented ZIMO, a cross-technology MIMO design to harmonize ZigBee smog with WiFi flash without modifying legacy systems. We implemented ZIMO on the GNURadio/ USRP platform using commercial compatible implementations of WiFi and ZigBee. Our experiment results showed that, up to 80% interfered signals are effectively recovered by ZIMO. Moreover, 30% to 90% interfered WiFi signals are effectively recovered in the process, which demonstrates the co-prosperity goal in ZIMO design.

ZIMO enables the sink node to protect WiFi and ZigBee signal in one framework. In future design, ZIMO could be enhanced into a composite AP for both ZigBee and WiFi networks. Thus, downlink design is needed for effective communications. For large-scale wireless sensor networks, ZIMO sinks can be deployed in asymmetric areas for multi-hop support. Placement of ZIMO sinks depends on interference relationship between WiFi and WSN deployments, which makes optimal placement an interesting and challenging work for future research. Also, in symmetric area, clear carrier sensing scheme can be encouraged to be disabled for concurrent transmissions. Finally, ZIMO can be applied to other WiFi standards with slight modifications, such as IEEE 802.11n.

12. ACKNOWLEDGMENTS

This research is partially supported by NSF China under Grants No. 61003277, 61232018, 61272487, 61170216, 61172062, 61228202, 61273210, NSF CNS-0832120, NSF CNS-1035894, NSF EECS-1247944, China 973 Program under Grants No. 2009CB320400, 2010CB328100, 2010CB334707, 2011CB302705. We thank all the reviewers for their insightful comments and valuable suggestions, and Prof. Kannan Srinivasan for shepherding the final revision of the paper in dedication. Particularly, the research work is mainly done during the authors' scholar visiting in IOT Tech-center of TNLIST, Wuxi, China.

13. REFERENCES

[1] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the RF smog: making 802.11n robust to cross-technology interference," in *Proc. of ACM SIGCOMM*, 2011.

[2] R. Murty, G. Mainland, I. Rose, and M. Welsh, "CitySense: An Urban-Scale Wireless Sensor Network and Testbed," in *Proc. of IEEE HST*, 2008.

[3] X. Mao, X. Miao, Y. He, T. Zhu, J. Wang, W. Dong, and X. Li, "CitySee: Urban CO2 Monitoring with Sensors," in *Proc. of IEEE INFOCOM*, 2012.

[4] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance," in *Proc. of IEEE ICNP*, 2010.

[5] R. Zhou, Y. Xiong, G. Xing, L. Sun, and J. Ma, "ZiFi: Wireless LAN Discovery via ZigBee Interference," in *Proc. of ACM MobiCom*, 2010.

[6] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving wi-fi interference in low power ZigBee networks," in *Proc. of ACM SenSys*, 2010.

[7] X. Zhang and K. Shin, "Adaptive Subcarrier Nulling: Enabling partial spectrum sharing in wireless LANs," in *Proc. of IEEE ICNP*, 2011.

[8] S. B. S. Rayachu, A. Patro, "Airshark: Detecting Non-WiFi RF Devices using Commodity WiFi Hardware," in *Proc. of ACM IMC*, 2011.

[9] S. P. S. Gollakota and D. Katabi, "Interference alignment and cancelation," in *Proc. of ACM SIGCOMM*, 2009.

[10] IEEE Standard, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," 2006.

[11] K. Tan, H. Liu, and J. Fang, "SAM: Enabling Practical Spatial Multiple Access in Wireless LAN," in *Proc. of ACM MobiCom*, 2009.

[12] *Contiki website*, http://www.contiki-os.org.

[13] C. Shepard, H. Yu, N. Anand, L. Li, T. Marzetta, Y. Yang, and L. Zhong, "Argos: practical base stations with many antennas," in *Proc. of ACM MobiCom*, 2012.

[14] X. Zhou, Z. Zhang, G. Wang, X. Yu, B. Y. Zhao, and H. Zheng, "Practical conflict graphs for dynamic spectrum distribution," in *Proc. of ACM Sigmetrics*, 2013.

[15] Z. Yang, C. Wu, and Y. Liu, "Locating in fingerprint space: wireless indoor localization with little human intervention," in *Proc. of ACM MobiCom*, 2012.

[16] G. Shen, Z. Chen, P. Zhang, T. Moscibroda, and Y. Zhang, "Walkie-Markie: Indoor Pathway Mapping Made Easy," in *Proc. of USENIX NSDI*, 2013.

[17] Y. Wang, Q. Wang, Z. Zeng, G. Zheng, and R. Zheng, "WiCop: Engineering WiFi Temporal White-Spaces for Safe Operations of Wireless Body Area Networks in Medical Applications," in *Proc. of IEEE RTSS*, 2011.

[18] Y. He, J. Fang, J. Zhang, H. Shen, K. Tan, and Y. Zhang, "MPAP: virtualization architecture for heterogenous wireless APs," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, Jan. 2011.

[19] S. S. Hong, J. Mehlman, and S. Katti, "Picasso: flexible RF and spectrum slicing," in *Proc. of ACM SIGCOMM*, 2012.

[20] X. Zhang and K. G. Shin, "Cooperative Carrier Signaling: Harmonizing Coexisting WPAN and WLAN Devices," *IEEE Trans on Networking*, 2012.

[21] B. Radunovic, R. Chandra, and D. Gunawardena, "Weeble: Enabling low-power nodes to coexist with high-power nodes in white space networks," *ACM CoNEXT*, 2012.

[22] K. Pelechrinis, I. Broustis, S. Krishnamurthy, C. Gkantsidis, B. Radunovic, R. Chandra, and D. Gunawardena, "ARES: an anti-jamming reinforcement system for 802.11 networks," in *Proc. of CoNEXT*, 2009.

[23] H. Rahul, N. Kushman, D. Katabi, C. Sodini, and F. Edalat, "Learning to share: narrowband-friendly wideband networks," in *Proc. of ACM SIGCOMM*, 2008.

[24] D. Halperin, T. Anderson, and D. Wetherall, "Taking the sting out of carrier sense: interference cancellation for wireless LANs," in *Proc. of ACM MobiCom*, 2008.

[25] S. Gollakota and D. Katabi, "Zigzag decoding: combating hidden terminals in wireless networks," in *Proc. of ACM SIGCOMM*, 2008.

[26] T. Jin, G. Noubir, and B. Sheng, "WiZi-Cloud: Application-transparent dual ZigBee-WiFi radios for low power internet access," in *Proc. of IEEE INFOCOM*, 2011.

[27] W. Li, Y. Zhu, and T. He, "WiBee: Building WiFi radio map with ZigBee sensor networks," in *Proc. of IEEE INFOCOM*, 2012.