PMC: Parallel Multi-protocol Communication to Heterogeneous IoT Radios within a Single WiFi Channel

Zicheng Chi, Yan Li, Yao Yao, and Ting Zhu
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County
{zicheng1, liy1, yaoyaoumbc, zt}@umbc.edu

***Abstract*—The exponentially increasing number of Internet of things (IoT) devices introduces spectrum crisis to the widely used industrial, scientific, and medical (ISM) frequency band. Since IoT devices use heterogeneous radios with different bandwidths (e.g., 20 MHz for WiFi and 2 MHz for ZigBee), traditional interference avoidance methods, such as time-division multiple access (TDMA) and carrier-sense multiple access (CSMA), have very low spectrum utilization. This is because TDMA and CSMA allocate the packets at time domain, without considering the bandwidth difference of different IoT radios. To address this issue, we propose PMC, a novel communication system that enables *parallel* multi-protocol communication to heterogeneous IoT radios (i.e., WiFi and ZigBee) within a single WiFi channel. Our extensive evaluations show that PMC achieves the throughput of up to 121.02 kbit/s and 319.76 Mbit/s for parallel communication to ZigBee and WiFi, respectively. Compared with TDMA and CSMA, the spectrum utilization of PMC is increased by 2.3 and 1.8 times, respectively.**

I. Introduction

Gartner estimates the number of Internet of things (IoT) devices will exponentially increase from 6.4 billion in 2016 to 20.4 billion by 2020 [1]. Due to different requirements on cost, data-rate, communication-range, and energy-consumption, these IoT devices use heterogeneous wireless communication radios and protocols. For example, WiFi (which typically has 20 MHz bandwidth) is used by mobile devices to achieve high-data-rate while ZigBee (which has 2 MHz bandwidth) is used by low-power and low-data rate sensor devices. However, most of these IoT devices work within the same industrial, scientific, and medical (ISM) frequency band (e.g., 2.4 GHz). Therefore, the exponentially increasing number of IoT devices introduces the spectrum crisis.

Traditional interference avoidance methods, such as time-division multiple access (TDMA) and carrier-sense multiple access (CSMA), are only designed to avoid the interference among wireless devices. Therefore, these methods have very low spectrum utilization, especially when the IoT devices are using heterogeneous radios. As shown in Figure 1, which is a waterfall figure obtained from a spectrum analyzer, ZigBee and WiFi devices are competing for the overlapped channel access. Since the ZigBee device uses only 2 MHz bandwidth (compared to 20 MHz bandwidth of WiFi), when the ZigBee device is transmitting (the red colored box in Figure 1), the WiFi device is trying to avoid collisions (the black colored box in Figure 1) because of the CSMA scheme. Thus, when the ZigBee device is transmitting, the spectrum from 2.432 GHz to 2.447 GHz (highlighted in the white color dashed box in Figure 1) is wasted.

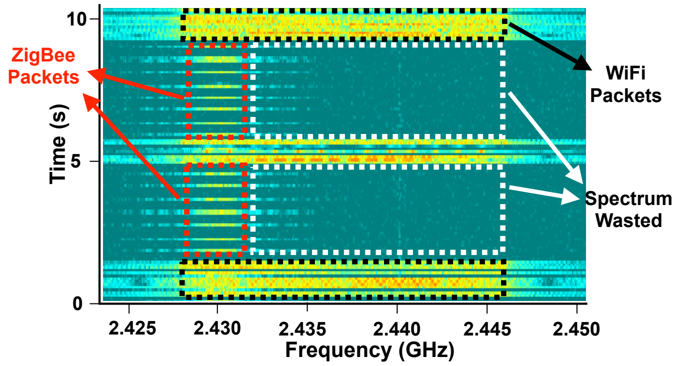


Fig. 1: A waterfall figure to demonstrate the low spectrum utilization among WiFi and ZigBee devices.

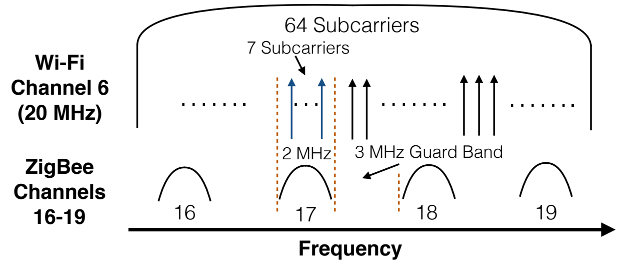


Fig. 2: Overlapped channels of ZigBee and WiFi

To address this problem, we propose PMC which explores the possibility of parallel multi-protocol communication to heterogeneous IoT radios within a single WiFi channel so that the spectrum utilization can be significantly improved. The key idea is to use some WiFi subcarriers' signal to imitate ZigBee's Offset quadrature phase-shift keying (OQPSK) modulation by leveraging the overlapped channel between WiFi and ZigBee devices. For example, as shown in Figure 2, WiFi channel 6 is overlapped with four ZigBee channels (i.e., 16, 17, 18, and 19). Within WiFi channel 6, there are 64 subcarriers with 7 subcarriers opverlapping with the ZigBee channel 17. Therefore, we explore the possibility of using these 7 subcarriers to imitate ZigBee's OQPSK modulation while keeping the other 57 subcarriers intact. By doing this, we can enable the parallel communication to 1 ZigBee and 1 WiFi devices.

In summary, our main contributions are as follows:

978-1-5090-6501-1/17/$31.00 © 2017 IEEE

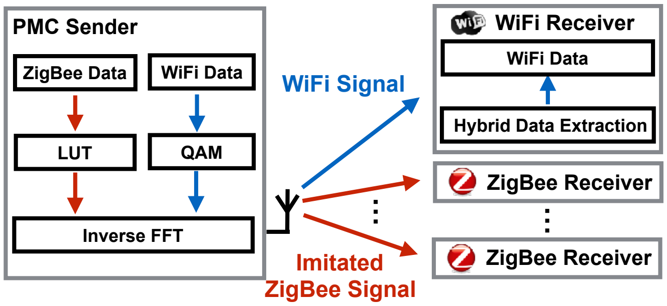


Fig. 3: System Overview

- To the best of our knowledge, this is the first work that enables *parallel* multi-protocol communication among heterogeneous IoT radios within the overlapped channel. Specifically, we develop a novel *parallel* multi-protocol communication (PMC) system, which uses some WiFi subcarriers' signal to imitate ZigBee's OQPSK modulation to achieve parallel communication from one WiFi device to another WiFi and multiple ZigBee receivers within a single WiFi channel. Moreover, both WiFi and ZigBee receivers do not need any hardware modification.
- Our design is generic and can be extended to support parallel multi-protocol communication to multiple ZigBee devices and 1 WiFi device with different data packets. To achieve this, we only need to use WiFi's subcarriers, which are overlapped with ZigBee channels, to imitate ZigBee's OQPSK modulation. With 40 MHz WiFi channel, PMC can support parallel unicast to 4 ZigBee devices and 1 WiFi device.
- We implemented PMC system using USRP and conducted extensive experiments by evaluating our design under one ideal setting (i.e., Faraday cage) and two real-world settings (i.e., Line-of-Sight and Non-Line-of-Sight). Compared with TDMA and CSMA, the spectrum utilization of PMC is increased by 2.3 and 1.8 times, respectively.

II. System Overview

The design goal of PMC is to enable parallel multi-protocol communication from the PMC sender to: i) one WiFi receiver and ii) one or multiple ZigBee receivers. To achieve this design goal, we propose the PMC system architecture (shown in Figure 3), which contains three parts: i) PMC sender; ii) conventional WiFi receiver and iii) conventional ZigBee receiver(s).

PMC sender: Our PMC sender design enables parallel transmission of data streams to heterogeneous IoT receivers (i.e., ZigBee and WiFi). Specifically, we developed a search algorithm which maps the desired ZigBee's OQPSK signal to different states of WiFi signal's QAM modulation. We store this map in a look-up table (LUT), which only contains 4 entries. Then, ZigBee data goes through the LUT and gets the QAM states for the subcarriers that overlapped between ZigBee and WiFi. At the same time, WiFi data bits go through the QAM modulation on the subcarriers that are not overlapped between ZigBee and WiFi. Then, we get the hybrid ZigBee and WiFi signal by using an inverse FFT module. The whole process is detailed in Section III.

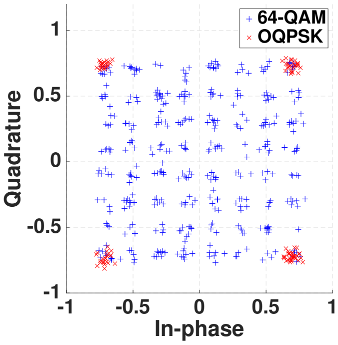


Fig. 4: Comparison between 64-QAM and OQPSK states

Conventional WiFi receiver: In order to use a conventional WiFi receiver to demodulate the received hybrid signal without any hardware modification. The main challenge is to extract the WiFi data from the hybrid data (which contains both ZigBee and WiFi data). To address this challenge, we leverage the parallel transmission feature of WiFi's OFDM modulation scheme for obtaining the WiFi data stream (detailed in Section IV).

Conventional ZigBee receiver(s): By using the feature of DSSS scheme in conventional ZigBee receivers, we overcome the minor mismatch between the desired ZigBee's OQPSK signal and WiFi imitated ZigBee signal. Our approach does not need any hardware modification (detailed in Section V).

We note that the main focus of this paper is to improve the spectrum utilization by enabling parallel multi-protocol communication from the PMC sender to WiFi and ZigBee receivers. For the reverse path (i.e., from ZigBee and WiFi to the PMC sender), we can use the existing concurrent cross-technology communication techniques (e.g., B^2W^2 [2]) to improve the spectrum utilization.

III. PMC Sender

The design goal of the PMC sender is to improve spectral utilization by imitating a narrow band ZigBee signal using the overlapped wide-band WiFi subcarriers. Thus, this design enables parallel ZigBee and WiFi communications. The intuition behind this design is that WiFi's QAM has multiple states that are like the OQPSK phase states (shown in Figure 4). The design challenges are: i) how to imitate ZigBee's OQPSK signal using specific WiFi's subcarriers which use QAM; and ii) how to deal with the different symbol rate between WiFi and ZigBee.

In the following sections, we briefly introduce the background of conventional WiFi and ZigBee senders, then describe our PMC sender.

A. Conventional WiFi and ZigBee Senders

WiFi modulates information using Quadrature Amplitude Modulation (QAM) by mapping bits to different phases and amplitude states in sine waves. To combine the sine waves efficiently, WiFi adopts Orthogonal frequency-division multiplexing (OFDM) by utilizing an inverse Fourier transform (IFFT). The duty cycle that the IFFT operates defines the

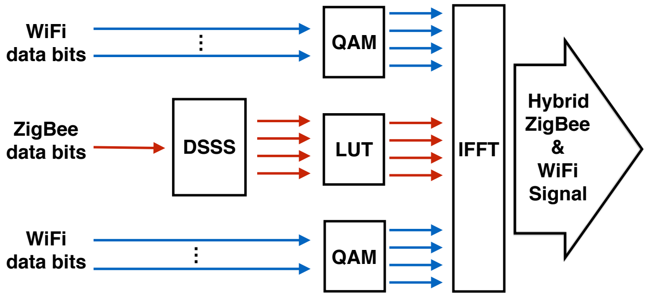


Fig. 5: Structure of PMC Sender

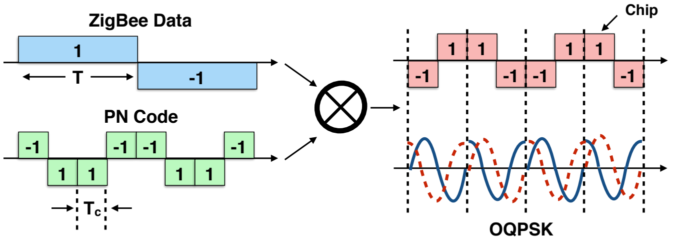


Fig. 6: Example of DSSS process

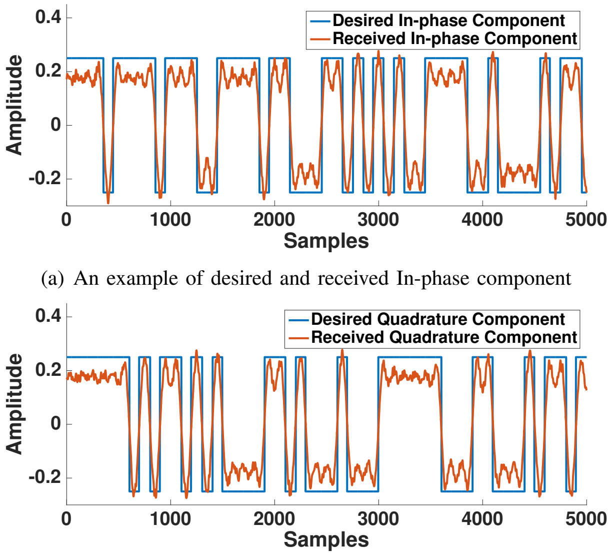
symbol duration. The signal output from the IFFT is defined as the baseband WiFi signal. Thus, in a conventional WiFi sender, the baseband signal is then up-converted to the desired transmit frequency, amplified, filtered, and radiated by the antenna.

ZigBee modulates information using Direct Sequence Spread Spectrum (DSSS) and Offset quadrature phase-shift keying (OQPSK) by mapping bits into four distinct phase states of a sine wave. To reduce signal interference, ZigBee spreads the transmit signal into a wider band by multiplying with a higher rate pseudo noise (PN) code. This PN code is shared between the sender and receiver. To map the bits to sine waves spread by the PN code, OQPSK modulation reduces the dramatic phase shifts by offsetting the odd and even bits by a distinct period of time. The output of the OQPSK signal is the ZigBee baseband signal. The output of the modulators is transmitted in the same manner as the WiFi.

B. Detailed Design of PMC Sender

To imitate the ZigBee signal using WiFi signals, the output of the IFFT must contain similar signals as the output of the ZigBee modulator. Thus, a portion of the signals from the WiFi QAM modulator must be replaced. Figure 5 shows the structure of the PMC sender. In this figure, the blue arrows indicate the flow of WiFi data while the red arrows indicate the flow of ZigBee data. The ZigBee data first goes through a DSSS module which spreads the data using a pseudo noise (PN) code for anti-noise purpose. Figure 6 shows an example of the DSSS module. By multiplying a pre-defined PN code (green blocks), the ZigBee data (blue blocks) is converted to chips (red blocks). Each chip is corresponding to an OQPSK wave (including the in-phase and quadrature components). The OQPSK wave is the desired signal can be demodulated by a conventional ZigBee receiver.

To imitate the OQPSK wave, we utilize a look-up table (LUT). The inputs to the LUT are the ZigBee chips (which is produced by the DSSS module). The outputs are the matched QAM points which allow the IFFT to imitate the ZigBee's signal at the specific subcarriers. Finally, the output of the LUT is injected in the IFFT with other QAM symbols from the WiFi data. Figures 7(a) and 7(b) show an example of the desired in-phase and quadrature components (the blue lines) and the received in-phase and quadrature components (red lines) generated by PMC sender.



(a) An example of desired and received In-phase component

(b) An example of desired and received quadrature component

Fig. 7: Desired ZigBee signals v.s. PMC sender generated signals

To generate the LUT that maps the desired ZigBee OQPSK signal to different state combinations of WiFi QAM symbols before the IFFT, we develop a search algorithm. Before introducing the algorithm, we list the equations that we will use. A ZigBee signal can be represented as follows:

$$S(t) = \frac{1}{\sqrt{2}} d_I(t)\cos(2\pi f_z t) + \frac{1}{\sqrt{2}} d_Q(t)\sin(2\pi f_z t) \qquad (1)$$

Where $S(t)$ is the actual ZigBee signal with $n = 4$ states, $d_I(t)$ and $d_Q(t)$ are the data on in-phase and quadrature components. f_z is the ZigBee's symbol rate. The following equation defines the WiFi Signal:

$$S_q(k) = I(k)\cos(2\pi f_w t) - Q(k)\sin(2\pi f_w t) \qquad (2)$$

Where S_q is the QAM signal on each subcarrier. f_w is the WiFi's symbol rate. $I(k)$ and $Q(k)$ are the possible states of in-phase and quadrature components defined as a complex number. Since WiFi adopts OFDM, multiple QAM signals on different subcarriers are aggregated together by the following IFFT equation:

$$S'(t) = \int_{n}^{n+z} S_q(k) e^{2\pi jkt} dk \qquad (3)$$

Where $S'(t)$ is the output of IFFT. From n to $n + z$ is the number of subcarriers which are overlapped with ZigBee. The intuition why the iFFT (Equation 3) allows each subcarrier to be packed closely together in the time domain without interfering with each other is that each data carrying tone $(S_q(k))$ is mapped to a specific frequency slot through efficient divide and conquer multiplications. To imitate the ZigBee signal, we need to find the minimum difference between $S(t)$ and $S'(t)$ for each ZigBee chip. Thus, we propose the following search algorithm to generate the LUT:

Algorithm 1 Search Algorithm for LUT Generation

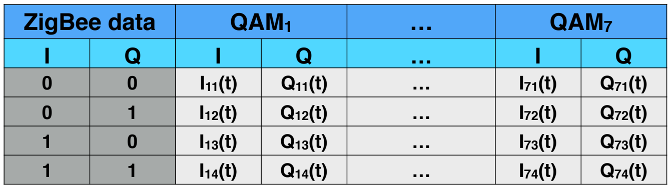
Input: $\mathbf{d_I(t), d_Q(t)}$
Output: $\{\mathbf{I_1(t), Q_1(t)}\}, \cdots, \{\mathbf{I_z(t), Q_z(t)}\}$

```
1:  Calculate $S(t)$ by Equation 1 with $d_I(t)$, $d_Q(t)$;
2:  $err = |S(t)|$;
3:  for $n = 1$ to $z$ do
4:      for every QAM state $I_j$ in I component do
5:          for every QAM state $Q_k$ in Q component do
6:              Calculate $S'(t)$ by Equation 2 and 3;
7:              if $err > |S'(t) - S(t)|$ then
8:                  $err = |S'(t) - S(t)|$, $I_n(t) = I_j$, $Q_n(t) = Q_k$;
9:              end if
10:         end for
11:     end for
12: end for
```

This search algorithm is a simple iteration through all the possible QAM phase states for the WiFi's subcarriers that are overlapped with ZigBee's channel. Line 1 calculates the desired ZigBee signal using Equation 1 based on the input ZigBee data. Line 2 initiates the err value which is used to store the temporary result. Lines 3-12 are the iteration to go through all QAM states. Line 6 calculates the aggregated OFDM signal using Equation 2 and 3. Lines 7-8 save the I and Q states for the minimal err value. Thus, this algorithm runs in O $(N \cdot z)$ because of the requirement to iterate through each of the QAM states for every WiFi's subcarriers that are overlapped with ZigBee's channel. We note that this algorithm only needs to be run offline to produce the LUT.

In run time, we only need to use LUT that maps the outputs of DSSS OQPSK to QAM. With N input phase states, the LUT outputs M subcarriers yielding an $N \times M$ look-up table. Each M outputs of the LUT contains a valid QAM symbol. For the PMC sender, there are 4 phase states from the conventional ZigBee radio that has 2 MHz bandwidth. Each WiFi subcarrier uses 312.5 kHz bandwidth. Therefore, we need 7 WiFi subcarriers each with 64-QAM phase states to imitate the ZigBee signal. The sum of the subcarriers spanning the bandwidth must represent the ZigBee signal.

Figure 8 shows the structure of LUT which contains four inputs (i.e., four possible values of an OQPSK signal) and seven outputs (corresponding to seven subcarriers overlapped with ZigBee channel). The input is the desired ZigBee data's I and Q values, the output is the QAM states that can imitate the ZigBee signal after IFFT.



ZigBee data		QAM$_1$		...	QAM$_7$	
I	Q	I	Q	...	I	Q
0	0	$I_{11}(t)$	$Q_{11}(t)$	...	$I_{71}(t)$	$Q_{71}(t)$
0	1	$I_{12}(t)$	$Q_{12}(t)$	...	$I_{72}(t)$	$Q_{72}(t)$
1	0	$I_{13}(t)$	$Q_{13}(t)$	...	$I_{73}(t)$	$Q_{73}(t)$
1	1	$I_{14}(t)$	$Q_{14}(t)$	...	$I_{74}(t)$	$Q_{74}(t)$

Fig. 8: Structure of the LUT

WiFi also attaches a training sequence and a header with different modulation schemes; and WiFi includes in a cyclic prefix. To address the problem of different modulation schemes in the fast-transient preamble, we employed concurrent transmission with the non-ZigBee overlapped subcarriers and overlapped subcarriers. Because the preamble is short, utilizes simple modulation schemes (BPSK), and is more powerful, both WiFi and ZigBee devices should recover their respective messages. We acknowledge that WiFi cyclical prefix increases the noise in the embedded ZigBee signal, but it only contains 8 ZigBee chips which do not introduce significant interference due to the robustness of DSSS. Our evaluation results in Section VII also demonstrate the robustness of our design.

IV. WiFi receiver

In Section III, we introduce the detailed design of PMC sender which transmits the hybrid signal that contains both WiFi and imitated ZigBee signals within a single WiFi channel. In this section, we introduce how to use a conventional WiFi receiver to demodulate the received hybrid signal without the hardware modification. Specifically, we introduce our solutions for addressing the following challenge: how to extract the WiFi data from the hybrid signal.

Since the symbol rates of WiFi and ZigBee are different, the conventional WiFi receiver cannot demodulate the imitated ZigBee signal in the hybrid signal. Therefore, it is challenging for the conventional WiFi receiver to extract the WiFi data from the hybrid signal without hardware modification.

To address this challenge, we utilize OFDM's unique feature that divides a data stream into N parallel pieces and modulates it in N subcarriers (e.g., $N = 48$ in a 20 MHz WiFi channel). Because of the subcarriers transmit data in parallel, the data collision or loss in one or more subcarriers does not affect other subcarriers.

Figure 9 shows the demodulator of a conventional WiFi receiver. After fast Fourier transform (FFT), the input signal is

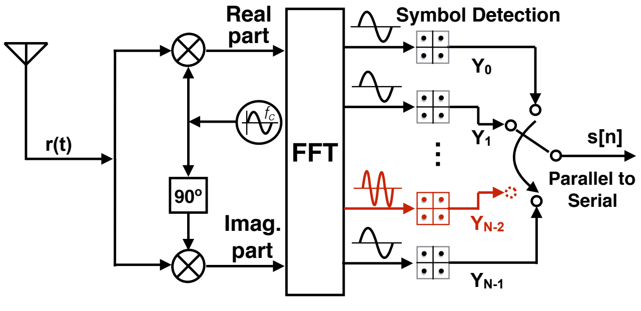
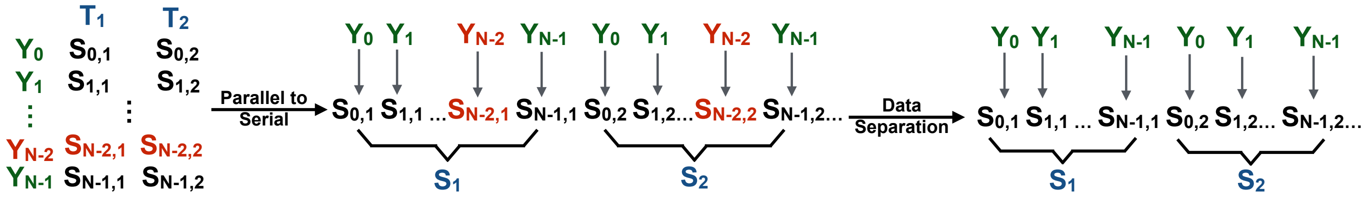


Fig. 9: Demodulation at the conventional WiFi receiver side


T1
T2
Y0
Y1
⋮
YN-2
YN-1
S0,1
S1,1
SN-2,1
SN-1,1
S0,2
S1,2
⋮
SN-2,2
SN-1,2
Parallel to Serial
Y0 Y1 YN-2 YN-1 Y0 Y1 YN-2 YN-1
S0,1 S1,1 ...SN-2,1 SN-1,1 S0,2 S1,2...SN-2,2 SN-1,2...
S1
S2
Data Separation
Y0 Y1 YN-1 Y0 Y1 YN-1
S0,1 S1,1 ... SN-1,1 S0,2 S1,2... SN-1,2...
S1
S2

(a) Data Matrix Output of Symbol Detection

(b) Hybrid Data Stream

(c) Separated Data Stream

Fig. 10: Example of extracting WiFi data from the hybrid data frame by removing the red colored bits at the link layer without hardware modification.

divided into N streams which go into the symbol detector. The output of each symbol detector is the value of bits (from Y_0 in the first subcarrier to Y_{N-1} in the last subcarrier). By using a parallel to serial converter, all the bits are composed to be a stream which is the modulated data. When the conventional WiFi receiver receives the hybrid signal from the PMC sender, part of the subcarriers contains WiFi data while the rest contain ZigBee data. In Figure 9, without loss of generality, we assume that the $N-2$ subcarrier (the red colored one) contains ZigBee data. Since ZigBee's symbol rate is higher than WiFi and their modulation schemes are different, the conventional WiFi receiver is not able to demodulate the ZigBee data. Moreover, after going through the parallel to serial converter, the ZigBee data part is mixed with the WiFi data coming from other subcarriers. Thus, we must remove the ZigBee data part and form the correct WiFi data stream which is designated for the conventional WiFi receiver.

Without loss of generality, Figure 10 shows a simplified example, which explains how to achieve this without any hardware modification on the conventional WiFi receiver. To simplify the case, assuming the WiFi is using 16 quadrature amplitude modulation (16-QAM) on each subcarrier (one symbol represents four bits data). Note that this method can also be applied to another modulation scheme, such as 64-QAM and 256-QAM. In Figure 10(a), the matrix is the output of the symbol detection (shown in Figure 9). Each row (Y_0 to Y_{N-1}) is corresponding to each subcarrier and each column (T_1 to T_2) is corresponding to a single symbol at time T_n. Since the $N-2$ subcarrier (red colored) is designated for ZigBee, the data in this row cannot be demodulated by the conventional WiFi receiver. However, we can not direct mask this row because we can not modify the physical layer (i.e., we can only access the output of the parallel to serial converter). Figure 10(b) shows the data stream after the parallel to serial converter. Since the parallel to serial converter picks each symbol (S_i) in forward order from each subcarrier (Y_n), we can periodically remove the corresponding bits (the red colored bits) from the signal data stream and form the designated WiFi data (only by the black colored bits). Figure 10(c) shows the separated bits which is the correct WiFi data stream.

To generalize our approach, the WiFi receiver is notified by a few bits (which have very tiny overhead) that the ZigBee data is embedded, then the WiFi data stream $\mathbb{S}'[m]$ can be formed based the original the output ($\mathbb{S}[n]$) of parallel to serial converter by using the following equation:

$$\mathbb{S}'[m] = \mathbb{S}[n] - \sum_{i=a}^{a+\Delta} \mathbb{S}[nN+i] \tag{4}$$

Where a to $a+\Delta$ are the subcarriers designated for conventional ZigBee receiver. N is the total number of subcarriers.

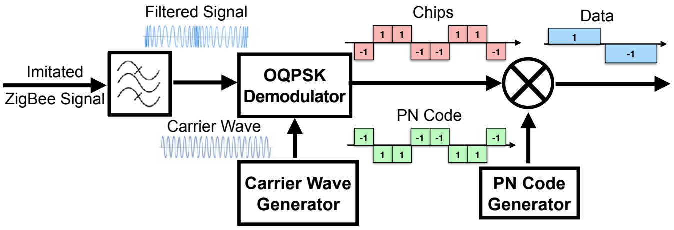


Fig. 11: Demodulator of Conventional ZigBee

V. ZigBee receiver

In this section, we introduce how to use conventional ZigBee receiver to demodulate the data from the PMC sender. Figure 11 shows the structure of a conventional ZigBee receiver. The received imitated ZigBee signal goes through the band-pass filter and gets the in-band signal, which goes into the OQPSK demodulator. The demodulator separates the baseband signals from the carrier wave by multiplying the signal from a carrier wave generator then track the phase changes of in-phase and quadrature components to decide the chip value. As described in Section III, the look-up table tries to map the desired ZigBee signal to WiFi's QAM states. Since the mapping is not always perfect, it introduces noise to the imitated ZigBee signal, which is received by the ZigBee receiver. To improve protection against interference and noise, conventional ZigBee protocol adopts Direct Sequence Spread Spectrum (DSSS) which spreads the energy into a wider band by multiplying a pseudo-random sequence at the sender side. At the receiver side, the chips are multiplied by the same pseudo-random sequence to get symbols which are used to represent ZigBee data. We evaluate the bit error rate (BER) in Section VII and demonstrate that DSSS scheme can effectively recover the data.

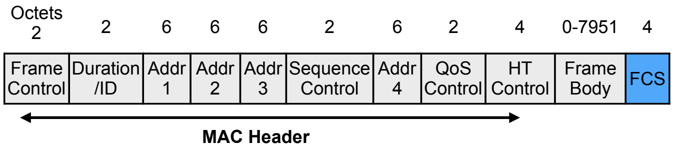


Fig. 12: WiFi Frame Format

VI. Practical Issues

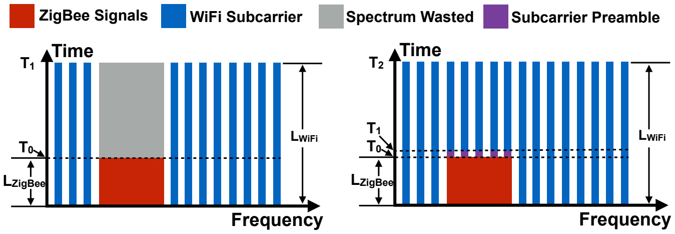
In this section, we discuss two practical issues: i) how to pass the frame check sequence (FCS) validation at the conventional WiFi receiver side; and ii) how to further improve the spectrum utilization when the frame lengths of WiFi and ZigBee are unequal.

A. Passing the FCS Validation

To ensure the receiver correctly receives a frame, the conventional WiFi sender adds a frame check sequence (FCS) field at the end of each frame (see the blue box in Figure 12). The conventional WiFi sender calculates a 32-bit cyclic redundancy check (CRC) over all the fields of the MAC frame and puts the remainder in the FCS field. After receiving the frame, a conventional WiFi receiver validates the data by performing the 32-bit CRC check over all the frame (including the FCS field). If the remainder does not equal to zero, the receiver treats the frame as a corrupted frame. When parallel multi-protocol communication is conducted, without hardware modification, a conventional WiFi receiver will not get a zero remainder during the FCS validation because the WiFi receiver demodulates signals from all the subcarriers. As we described in Section IV, we should extract the WiFi data from the hybrid data frame because the ZigBee data cannot be demodulated by the conventional WiFi receiver due to different symbol rates (i.e., ZigBee's symbol rate is higher than WiFi). For FCS check, the inherent algorithm calculates the 32-bit CRC value for all the received data which will yield wrong result.

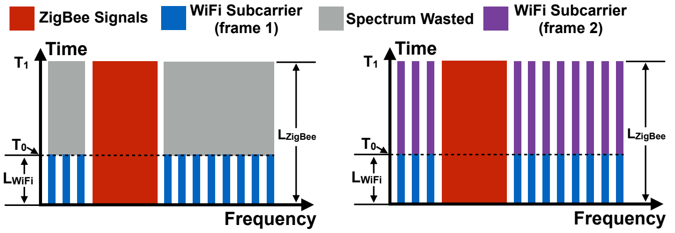
To deal with this problem, we propose to manipulate the FCS field at the PMC sender side. We only calculate the 32-bit CRC value for the valid WiFi data excluding the ZigBee data. At the WiFi receiver side, instead of dropping the frame through the original FCS check, the receiver only needs to calculate 32-bit CRC value with the manipulated FCS field after the WiFi and ZigBee Signals Separation (Section IV).

Specifically, at the WiFi and ZigBee parallel transmitter side, the 32-bit CRC calculation only includes the MAC Header and data for WiFi receiver (excludes the data for ZigBee receiver). Then the 4-byte remainder of the calculation is put into the FCS field (instead of the original FCS which calculates over all the subcarriers). After the WiFi receiver received and failed the check of the original FCS check (at hardware layer) because of the including of the meaningless ZigBee data, it separates the WiFi data (the subset $\mathbb{S}'[m]$) from WiFi and ZigBee hybrid data stream (Section IV). By having the subset $\mathbb{S}'[m]$, the WiFi receiver calculates another 32-bit CRC over MAC Header, the extracted Frame Body and the FCS field at software layer, if the result is zero, the receiver will accept this frame. By doing this, we can pass FCS validation when receiving a frame from the PMC transmitter.



(a) Spectrum wasted issue (b) Solution without spectrum wasted

Fig. 13: WiFi's frame length is longer than ZigBee



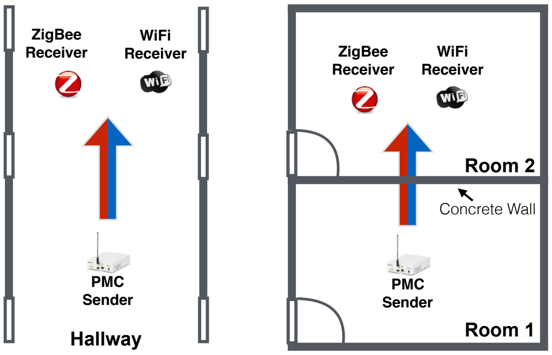
(a) Spectrum wasted issue (b) Solution without spectrum wasted

Fig. 14: ZigBee's frame length is longer than WiFi

B. Unequal Frame Length

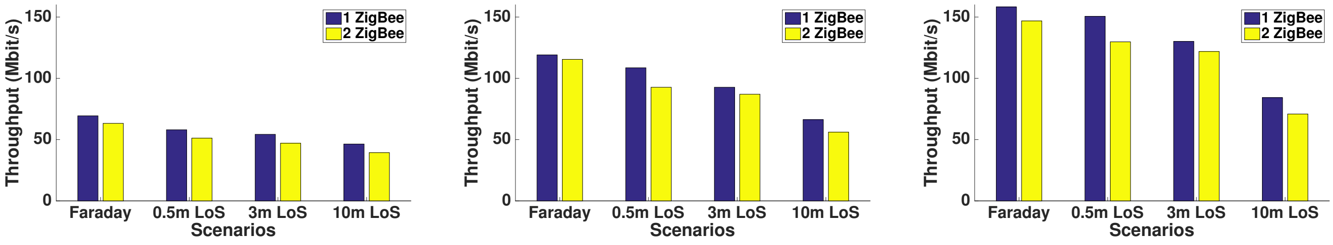
Since WiFi and ZigBee have different physical and MAC layers, it is highly possible that the frame lengths (in terms of time duration) of WiFi and ZigBee are different. For example, according to IEEE 802.11n [3] and 802.15.4 [4] standard, WiFi's frame length is from $1\mu s$ to $10ms$ while ZigBee's frame length is between $200\mu s$ and $4ms$. In this section, we introduce how to deal with this unequal frame length problem, which can be divided into two categories: i) WiFi's frame length is longer than ZigBee (i.e., $L_{WiFi} > L_{ZigBee}$); and ii) ZigBee's frame length is longer than WiFi (i.e., $L_{ZigBee} > L_{WiFi}$).

- $\mathbf{L_{WiFi} > L_{ZigBee}}$: As shown in Figure 13(a), ZigBee's frame (red block) length L_{ZigBee} is shorter than the WiFi L_{WiFi} (blue blocks). The ZigBee frame ends at time T_0. Thus, from time T_0 to T_1, if the PMC sender only transmits WiFi data using part of the subcarriers (shown in blue blocks), part of the spectrum (gray block) is wasted. To address this issue, we propose to transmit WiFi signals (on the overlapped subcarriers) immediately after the end of a ZigBee frame (shown in Figure 13(b)). However, we need to address two challenges: i) how does the conventional ZigBee receiver know the end of a frame; and ii) how does the conventional WiFi



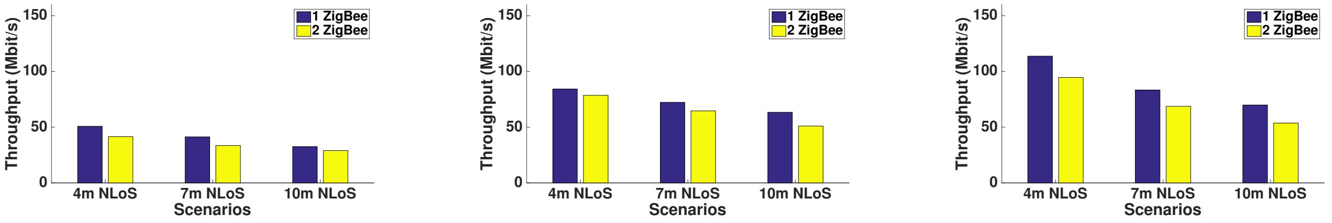
(a) Line-of-Sight (b) None-Line-of-Sight

Fig. 15: Experiment Setup



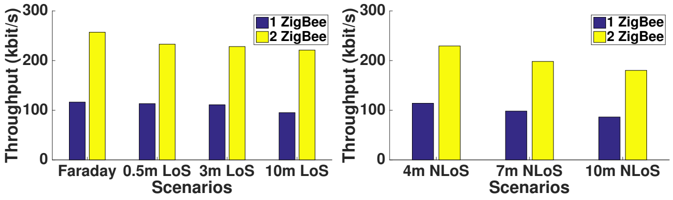
(a) 16-QAM (b) 64-QAM (c) 256-QAM

Fig. 16: In **LoS** scenario, conventional WiFi receiver's throughput in a 20 MHz WiFi channel with different modulation schemes (16-QAM, 64-QAM, and 256-QAM) slightly decrease over distance. When conducting parallel transmission to one and two ZigBee receivers, conventional WiFi receiver's highest throughput are 174.38 Mbit/s and 146.82 Mbit/s, respectively.



(a) 16-QAM (b) 64-QAM (c) 256-QAM

Fig. 17: In **NLoS** scenario, conventional WiFi receiver's throughput in a 20 MHz WiFi channel with different modulation schemes (16-QAM, 64-QAM, and 256-QAM) slightly decrease over distance. When conducting parallel transmission to one and two ZigBee receivers, conventional WiFi receiver's highest throughput are 107.94 Mbit/s and 94.62 Mbit/s, respectively.



(a) LoS (b) NLoS

Fig. 18: Conventional ZigBee receiver's throughput in a 20 MHz WiFi Channel. In LoS, the highest aggregated throughput from PMC sender to one ZigBee receiver and two ZigBee receivers are 116.39 kbit/s and 257.14 kbit/s, respectively. In NLoS, the conventional ZigBee receiver's throughput is similar to LoS. This is due to the low order modulation and DSSS scheme used by ZigBee protocol. It demonstrates the robustness of our approach.

receiver know the starting point of the WiFi frame on these overlapped subcarriers.

The first challenge is relatively easy to address because in a ZigBee frame, a frame length field is used to specify the length. Furthermore, at the end of a frame, there is a trailer which can help locate the last bit in a frame. Thus, the conventional ZigBee receiver exactly knows where is the end of a frame even if the WiFi signals are sent after the ZigBee frame.

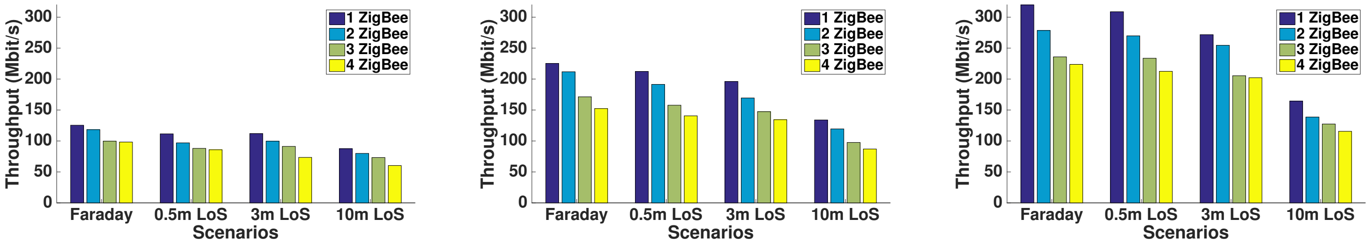
To address the second challenge, we insert subcarrier level preamble (the purple block in Figure 13(b)) on each WiFi subcarrier after the end of the ZigBee's frame at the PMC sender side. The subcarrier level preamble is a predefined sequence (e.g., a zero-one alternate sequence 01010101). At the WiFi receiver side, as stated in Section IV, the receiver will extract the WiFi signals from hybrid signals received from the PMC sender. To better utilize the spectrum, a monitor is used to locate subcarrier level preamble on each subcarrier. In the extraction process (Section IV), instead of removing all the ZigBee bits, this monitor will try to match the ZigBee bits with the predefined preamble. When the monitor locates the preamble, the separation process stops, and the WiFi receiver accepts the data from all the subcarriers.

- $\mathbf{L_{ZigBee}} > \mathbf{L_{WiFi}}$: As shown in Figure 14(a), if the ZigBee's frame (red block) length L_{ZigBee} is longer than the WiFi's frame (blue blocks) length L_{WiFi}. Most of the spectrum is wasted (gray block). To more efficiently utilize the spectrum, we propose to reuse the Aggregate MAC Service Data Unit (A-MSDU) of IEEE 802.11 [3], which is supported by IEEE 802.11e and its successor. Originally, A-MSDU is used to reduce the overhead introduced by MAC layer header by grouping two or more physical layer frames into one large frame.

As an example, Figure 14(b) shows the aggregation of two frames. Specifically, the PMC sender decides to group two frames together if it finds the first frame (blue blocks) will end (at time T_0) earlier than the ZigBee frame (red block). Then, the sender groups the first frame with the second frame (purple blocks) and sends the aggregated frame along with the ZigBee frame. At the WiFi receiver side, since the WiFi protocol naturally supports this technique (i.e., A-MSDU), the conventional WiFi receiver only needs conduct the same action to extract the WiFi data (detailed in Section IV).

VII. Evaluation

To extensively evaluate different aspects of PMC under a wide range of settings, the PMC sender and WiFi receiver are implemented using an NI RF testbed which consists of a signal digitizer (PXIe-5622), signal generator (PXIe-5652),



(a) 16-QAM

(b) 64-QAM

(c) 256-QAM

Fig. 19: In **LoS** scenario, conventional WiFi receiver's throughput in a 40 MHz WiFi channel with different modulation schemes (16-QAM, 64-QAM, and 256-QAM) slightly decrease over distance. When conducting parallel transmission to 1, 2, 3, and 4 ZigBee receivers, conventional WiFi receiver's highest throughput are 319.76 Mbit/s, 278.51 Mbit/s, 235.88 Mbit/s and 223.77 Mbit/s, respectively.

down-converter (PXIe-5601), up-converter (PXIe-5450), and streaming raid. We acquire high signal to noise ratio (SNR) signals using a RF-over-Fiber system. We utilized off the shelf ZigBee-compliant TelosB devices installed with TinyOS to receive the OQPSK signals from the PMC sender. To evaluate the system under different communication distances, we placed the devices on a rolling chair (at a 40 cm height) and moved them away from the PMC sender. For each throughput data point, we transmitted and received around 3 million symbols.

We conducted experiments in the following three scenarios:

- **Faraday cage:** To explore the optimal performance of PMC, we utilized a Faraday cage to attenuate 90 dB of the environmental interference.
- **Line-of-sight (LoS):** The sender and receivers are within line of sight and the distance between them are 0.5, 3, and 10 meters (shown in Figure 15(a)).
- **None-line-of-sight (NLoS):** The sender and receivers are in different rooms at a distance of 4, 7, and 10 meters (shown in Figure15(b)).

A. Performance within a 20 MHz WiFi Channel

We first evaluate PMC within a 20 MHz WiFi Channel, which is a popular configuration for WiFi devices working in the 2.4 GHz ISM band. As shown in Figure 2, one WiFi 20 MHz channel can be overlapped with four ZigBee channels. However, due to the implementation of four pilot tones (transmitting predefined message for environmental adapting) and one null tone (reserved tone) in IEEE 802.11n and its successor, the PMC sender can only concurrently send two different ZigBee data streams to two ZigBee devices in parallel.

Figure 16 shows the WiFi receiver's throughput in LoS scenario, the total throughput increases when the modulation scheme changes from 16-QAM (Figure 16(a)) to higher order modulation schemes 64-QAM (Figure 16(b)) and 256-QAM (Figure 16(c)). However, when the communication distance increases, the decrease rate of higher order modulation (256-QAM in Figure 16(c)) is faster than lower order modulation (16-QAM in Figure 16(a)). Compared with the scenario that the PMC sender transmits to two ZigBee receivers and one WiFi receiver, when the PMC sender transmits to one ZigBee and one WiFi receiver, the throughput of the WiFi receiver (the yellow bars in each figure) increases. This is because each ZigBee data stream occupies 7 WiFi subcarriers.

The NLoS results are shown in Figure 17. Compared to LoS, in NLoS scenario the throughput is affected by the multipath effect. Especially for the higher order modulation (256-QAM in Figure 17(c)), the throughput decreases by approximately 30%. However, the WiFi receiver's throughput can still reach 107.94 Mbit/s and 94.62 Mbit/s when the PMC sender transmits to one and two ZigBee receivers, respectively.

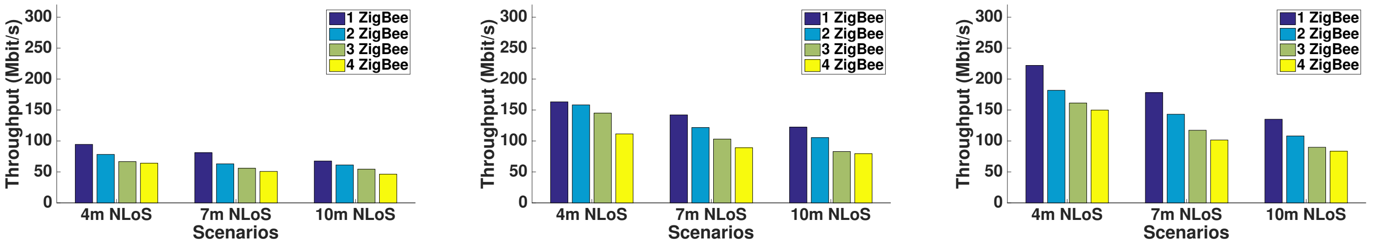
Figure 18 shows the throughput of ZigBee receivers. Within a 20 MHz WiFi channel, the PMC sender can transmit data streams to two ZigBee receivers (with the parallel transmission to a WiFi receiver). The results show that the highest aggregated throughput for one and two ZigBee receivers are 116.39 kbit/s and 257.14 kbit/s (see Figure 18(a)), respectively, which is compatible with the throughput using conventional ZigBee to ZigBee communication. We also note that the overall throughput of ZigBee receivers in NLoS only decrease 6% compared with the throughput in LoS scenario. This is because that ZigBee uses DSSS, which is robust to the environmental interference.

B. Performance within a 40 MHz WiFi Channel

One 40 MHz WiFi channel may be overlapped with eight ZigBee channels. But due to the implementation of six pilot tones and two null tones in IEEE 802.11n, the PMC sender can send ZigBee signals up to four ZigBee devices in parallel.

Figure 19 shows the throughput between the PMC sender and WiFi receiver on a 40 MHz WiFi channel in LoS. The overall throughput for different modulation schemes are approximately doubled compared with a 20 MHz channel. The results also show the trend that higher order modulation scheme provide higher performance but decrease slightly faster than lower order modulation scheme when communication distance increases. By having more ZigBee receivers (from one to four), the throughput decreases only a small portion, this is because one ZigBee occupies 7 subcarriers. Even parallel four ZigBee signals are transmitting, the throughput to WiFi receiver can still achieve up to 223.77 Mbit/s.

Even affected by the multipath effect in NLoS, the throughput (the results are shown in Figure 20) still can achieve up to 222.08 Mbit/s, 181.87 Mbit/s, 161.25 Mbit/s and 149.82

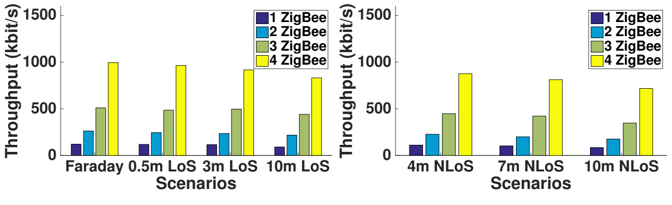


(a) 16-QAM

(b) 64-QAM

(c) 256-QAM

Fig. 20: In **NLoS** scenario, conventional WiFi receiver's throughput in a 40 MHz WiFi channel with different modulation schemes (16-QAM, 64-QAM, and 256-QAM) slightly decrease over distance. When conducting parallel transmission to 1, 2, 3, and 4 ZigBee receivers, conventional WiFi receiver's highest throughput are 222.08 Mbit/s, 181.87 Mbit/s, 161.25 Mbit/s and 149.82 Mbit/s, respectively.



(a) 40MHz WiFi Band LoS

(b) 40MHz WiFi Band NLoS

Fig. 21: Conventional ZigBee receiver's throughput in a 40 MHz WiFi Channel. In LoS, the highest aggregated throughput from PMC sender to 1, 2, 3, and 4 ZigBee receivers are 121.02 kbit/s, 262.51 kbit/s, 510.87 kbit/s and 996.02 kbit/s, respectively. In NLoS, the conventional ZigBee receiver's throughput is similar to LoS. This demonstrates the robustness of our approach.

	PMC	FreeBee	A-FreeBee
Throuhgput	121.02 kbps	≈ 14 bps	≈ 7 bps

Fig. 22: Comparison of ZigBee receiver's throughput with state-of-the-art cross-technology communication (CTC) approach. PMC's throughput is $8,644$x and $17,288$x higher than FreeBee and A-FreeBee, respectively. We note that our design goal is not specific for the cross-technology communication. However, our design can also significantly improve the latest CTC's throughput by up to 4 orders of magnitude.

Mbit/s when the PMC sender parallel transmits to one, two, three, and four ZigBee devices, respectively.

Figure 21 shows the throughput from PMC sender to ZigBee receiver. As mentioned before, a 40 MHz WiFi channel can support up to four parallel ZigBee transmissions (along with the transmission to WiFi receiver). Since these four ZigBee devices work on different channels, the parallel throughput is independent. Thus, the results in both LoS (Figure 21(a)) and NLoS show a linear increasing when the number of ZigBee receivers increase from one to four.

C. ZigBee Throughput Compared with State-of-art Cross-Technology Communication (CTC)

Figure 22 compares ZigBee receiver's throughput with state-of-the-art cross-technology communication (CTC) approach (i.e., FreeBee and A-FreeBee in [5]) under the same configuration with 1 ZigBee device. The result shows that PMC can also significantly improve the latest CTC's throughput by up to 4 orders of magnitude. We note that our design goal is not specific for the cross-technology communication.

D. Bit Error Rate

Figure 23 compares the bit error rates at the conventional ZigBee receiver side and conventional WiFi receiver side

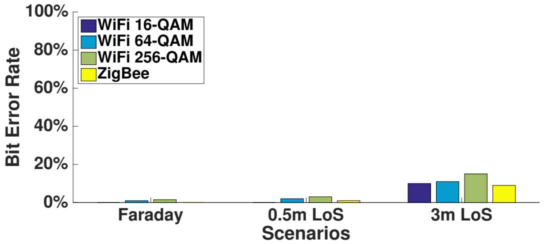
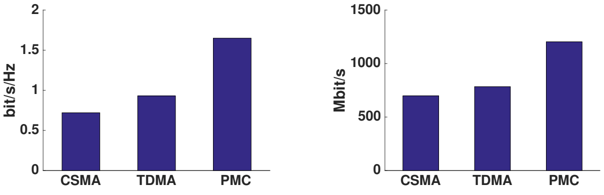


Fig. 23: BER at conventional WiFi and ZigBee receivers.



(a) Spectrum Efficiency

(b) Network Throughput

Fig. 24: Spectrum efficiency and network throughput. The spectrum utilization of PMC is 2.3 and 1.8 times higher than CSMA and TDMA approaches, respectively.

which uses 16, 64, and 256-QAM. As expected, the lower the number of phase states for QAM, the better the performance. Because of the DSSS and low phase states of OQPSK, ZigBee's signals are the most robust against noise. Thus, the results validate out design.

E. Spectrum Utilization

We compare PMC's spectrum utilization based on solely bits transmitted with CSMA and TDMA based using a common 40 MHz bandwidth 24. To compare efficiency with respect to the transmit schemes, we examine the spectral utilization efficiency and throughput. Because of the inability for the wider bandwidth (WiFi) to use the band while the narrow band (ZigBee) is transmitting we use the following metrics: spectral efficiency (bit/sec/Hz) which is the number of bits transmitted and received using the 40 MHz frequency band per second. Throughput (Mbit/sec) is the total number of bits transmitted and received using the 40 MHz frequency band. Since PMC can conduct parallel transmission to both WiFi and ZigBee receivers, the spectrum utilization (see Figure 24(a)) of PMC is 1.65 bit/s/Hz which is 2.3X and 1.8X higher than CSMA (which is 0.72 bit/s/Hz) and TDMA (which is 0.93 bit/s/Hz), respectively. Compared with CSMA and TDMA approaches, the average throughput (see Figure 24(b)) of PMC is increased by 72% and 53% respectively.

VIII. Related Work

Existing work to improve the spectrum utilization can be divided into the following two categories:

Improving performance within the same protocol: Due to the increasingly crowded 2.4 GHz ISM band, different methods [6], [7], [8], [9] have been proposed to improve its spectrum utilization. To further improve the performance of wireless communication, researchers have proposed various interference mitigate techniques [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21] and collision avoidance solutions [22], [23], [24], [25], [26].

Instead of improving spectrum utilization within the same protocol (i.e., WiFi or ZigBee), our work takes a holistic approach by exploring the possibility of increasing the spectrum utilization when heterogeneous radios with different protocols are communicating together. Specifically, our approach enables the full spectrum utilization over time within the same WiFi channel.

Cross-technology communication systems: To utilize the coexistent features of different wireless technologies within the same frequency band, several cross-technology communication systems [27], [28], [5], [29], [2] have been introduced. Esense [27] and HoWiES [28] enable WiFi to ZigBee communication by sensing the packet length of WiFi packets. GSense [29] uses special preamble to coordinate heterogeneous devices. FreeBee [5] achieved communication among WiFi, ZigBee and Bluetooth by modulating periodical beacons. EMF [30] support communication between WiFi and ZigBee devices by utilizing regular data packets. B^2W^2 [2] enables BLE to WiFi transmission by using CSI of WiFi system.

Different from the above approaches, our approach concurrently enables two types of parallel communication: i) cross-technology communication from 1 WiFi device to multiple ZigBee devices; and ii) traditional communication from 1 WiFi sender to 1 WiFi receiver in unicast mode or 1 WiFi sender to multiple WiFi receivers in broadcast mode. Our approach has the potential to significantly improve the spectrum utilization among heterogeneous IoT networks.

IX. Conclusion

The exponentially increasing number of heterogeneous IoT devices introduces a pressing requirement for more efficient spectrum utilization. In this paper, we explore a novel communication paradigm that can conduct parallel multi-protocol communication to heterogeneous IoT radios. Our extensive evaluation results demonstrate that our PMC system can significantly improve the spectrum utilization. Compared with TDMA and CSMA, the spectrum utilization of PMC is increased by 2.3 and 1.8 times, respectively. Our PMC system provides a new way to manage heterogeneous IoT networks with high spectrum utilization and conduct high throughput cross-technology communication.

Acknowledgment

This project is supported by NSF grants CNS-1503590, CNS-1652669, and CNS-1539047.

References

[1] "http://www.gartner.com/newsroom/id/3598917."

[2] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2w2: N-way parallel communication for iot devices," in *Sensys, 2016*.

[3] "http://standards.ieee.org/findstds/standard/802.11-2016.html."

[4] "http://standards.ieee.org/findstds/standard/802.15.4-2015.html."

[5] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *MobiCom 2015*.

[6] L. Deek, E. Garcia-Villegas, E. Belding, S.-J. Lee, and K. Almeroth, "The impact of channel bonding on 802.11n network management," in *CoNEXT, 2011*.

[7] D. Jiang, Y. Han, L. Miao, T. Zhu, and X. Ge, "Dynamic access approach to multiple channels in pervasive wireless multimedia communications for technology enhanced learning," *Journal of Intelligent Fuzzy Systems*, vol. 31, no. 5, pp. 2497–2509, October 2016.

[8] Z. Huang, D. Corrigan, S. Narayanan, T. Zhu, E. Bentley, and M. Medley, "Distributed and Dynamic Spectrum Management in Airborne Networks," in *IEEE Military Communications Conference*, 2015.

[9] H. Luo, Z. Huang, and T. Zhu, "A survey on spectrum utilization in wireless sensor networks," vol. 2015, pp. 1–13, 03 2015.

[10] N. Prasad, M. Arslan, and S. Rangarajan, "Enhanced interference management in heterogeneous cellular networks," in *ISIT, 2014*.

[11] L. Cheng, Y. Gu, J. Niu, T. Zhu, C. Liu, Q. Zhang, T. He, "Taming Collisions for Delay Reduction in Low-Duty-Cycle Wireless Sensor Networks," in *INFOCOM*, 2016.

[12] F. Chai, T. Zhu, and K. Kang, "A Link-Correlation-Aware Cross-Layer Protocol for IoT Devices," in *IEEE ICC*, 2016.

[13] J. Jun, L. Chen, L. He, Y. Gu, and T. Zhu, "Exploiting Sender-based Link Correlation in Wireless Sensor Networks," in *IEEE ICNP*, 2014.

[14] S. Ren, P. Yi, T. Zhu, Y. Wu, and J. Li, "A 3-hop Message Relay Algorithm for Connected Dominating Sets in Wireless Ad-hoc Sensor Networks," in *IEEE ICCC*, 2014.

[15] S. Ren, P. Yi, D. Hong, Y. Wu, and T. Zhu, "Distributed Construction of Connected Dominating Sets Optimized by Minimum-Weight Spanning Tree in Wireless Ad-Hoc Sensor Networks," in *IEEE CSE*, 2014.

[16] S. Guo, S. Min Kim, T. Zhu, Y. Gu, and T. He, "Correlated Flooding in Low-Duty-Cycle Wireless Sensor Networks," in *IEEE ICNP*, 2011.

[17] T. Zhu and D. Towsley, "E2r: Energy efficient routing for multi-hop green wireless networks," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2011.

[18] T. Zhu, Z. Zhong, T. He, and Z. Zhang, "Exploring Link Correlation for Efficient Flooding in Wireless Sensor Networks," in *USENIX NSDI*, 2010.

[19] Y. Gu, T. Zhu, and T. He, "ESC: Energy Synchronized Communication in Sustainable Sensor Networks," in *IEEE ICNP*, 2009.

[20] C. Zhou and T. Zhu, "A Spatial Reusable MAC Protocol for Stable Wireless Sensor Networks," in *IEEE WiCOM*, 2008.

[21] C. Zhou, T. Zhu, "Thorough Analysis of MAC Protocols in Wireless Sensor Networks," in *IEEE WiCOM*, 2008.

[22] J. Shi, E. Aryafar, T. Salonidis, and E. W. Knightly, "Synchronized csma contention: Model, implementation and evaluation," in *INFOCOM, 2009*.

[23] S. Sen, R. R. Choudhury, and S. Nelakuditi, "Csma/cn: Carrier sense multiple access with collision notification," *IEEE/ACM Trans. Netw.*, vol. 20, no. 2, pp. 544–556, Apr. 2012.

[24] T. Nandagopal, T.-E. Kim, X. Gao, and V. Bharghavan, "Achieving mac layer fairness in wireless packet networks," in *MobiCom 2010*.

[25] N. Singh, D. Gunawardena, A. Proutiere, B. Radunovi, H. V. Balan, and P. Key, "Efficient and fair mac for wireless networks with self-interference cancellation," in *WiOpt, 2011*.

[26] R. Merz, J. Widmer, J.-Y. Le Boudec, and B. Radunovic, "A Joint PHY/MAC Architecture for Low-Radiated Power TH-UWB Wireless Ad Hoc Networks," Tech. Rep., 2004.

[27] K. Chebrolu and A. Dhekne, "Esense: Communication through energy sensing," in *MobiCom, 2009*.

[28] Y. Zhang and Q. Li, "Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices," in *INFOCOM, 2013*.

[29] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *INFOCOM, 2013*.

[30] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu, "EMF: Embedding Multiple Flows of Information in Existing Traffic for Concurrent Communication among Heterogeneous IoT Devices," in *INFOCOM*, 2016.