EMF: Embedding Multiple Flows of Information in Existing Traffic for Concurrent Communication among Heterogeneous IoT Devices

Zicheng Chi, Zhichuan Huang, Yao Yao, Tiantian Xie, Hongyu Sun, and Ting Zhu

Department of Computer Science and Electrical Engineering

University of Maryland, Baltimore County

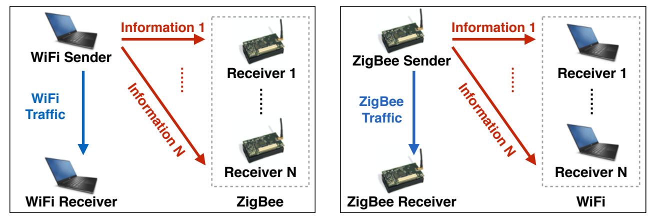
Email: {zicheng1, zhihu1, yaoyaoumbc, xtiant1, hongyu, zt}@umbc.edu

***Abstract*—The exponentially increasing number of IoT devices makes the unlicensed industrial, scientific, and medical (ISM) radio bands (e.g., 2.4 GHz) extremely crowded. Currently, there is no efficient solution to coordinate the large amount heterogeneous IoT devices that have different communication technologies (e.g., WiFi and ZigBee). To fill this gap, in this paper, we introduce embedded multiple flows (EMF) communication method, which (i) embeds different pieces of information in existing traffic and (ii) concurrently sends out these information from one IoT sender to multiple IoT receivers that have a different communication technology from the sender. By doing this, our EMF method (i) enables cross-technology communication among heterogeneous IoT devices, (ii) does not introduce any extra control traffic, and (iii) is transparent to the higher layer applications. Our approach is implemented on USRPs and commercial off-the-shelf (COTS) ZigBee devices. We also conducted extensive experiments to evaluate our approach in real-world settings. The evaluation results show that EMF's throughput is more than 14 times higher than the latest cross-technology communication technique (i.e. FreeBee[1]).**

I. Introduction

Based on Gartner, 6.4 billion Internet-of-Thing (IoT) devices will be in use in 2016, and the number of IoT devices will exponentially increase and reach 20.8 billion in 2020 [2]. On these IoT devices, WiFi or ZigBee is widely used. WiFi and ZigBee both operate in the same frequency band (i.e., 2.4 GHz). Therefore, the exponentially increasing number of IoT devices introduce severe communication interference among these devices. In order to reduce the interference and increase spectrum utilization, more efficient communication coordination among these devices is needed. However, WiFi and ZigBee cannot directly communicate with each other because they have totally different physical layers.

Traditionally, communication between wireless technologies is achieved indirectly via gateways equipped with multiple radio interfaces. This approach suffers from several issues including : (i) the cost to purchase the gateway hardware, (ii) traffic overhead flowing into and from gateways, and (iii) deployment complexity related to positioning the gateway in a way that satisfies user requirements. To address these issues, only a handful cross-technology communication (CTC) techniques have been proposed, including Esense [3], GSense [4], HoWiES [5], and FreeBee[1]. These approaches have their own limitations. Both Esense and HoWiES need to insert dummy packets which introduce extra traffic to already crowded 2.4 GHz spectrum and reduce the spectrum utilization. GSense need customized hardware platform which prevent it to be widely adopted. FreeBee only utilize beacon for



(a) WiFi-to-ZigBee (b) ZigBee-to-WiFi

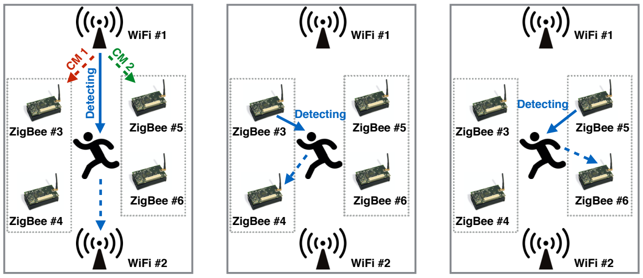
Fig. 1: Example of bi-directional EMF communication (i.e., WiFi to ZigBee and ZigBee to WiFi). Figure 1(a) shows that the WiFi sender can embed N pieces of information into its regular WiFi traffic and concurrently send out these information to N ZigBee receivers when the WiFi sender is communicating with the WiFi receiver. Similarly, Figure 1(b) shows the reverse direction.

cross-technology communication, therefore it has extremely low throughput and high latency.

In this paper, we take a dramatically different approach by leveraging existing traffic for concurrent cross-technology communication. Specifically, we introduce embedded multiple flows (EMF) communication method (shown in Figure 1), which (i) embeds different pieces of information in existing traffic and (ii) concurrently sends out these information from one IoT sender to one or multiple IoT receivers that have a different communication technology from the sender. By doing this, our EMF method (i) enables cross-technology communication among heterogeneous IoT devices, (ii) does not introduce any extra control traffic, and (iii) is transparent to the higher layer applications. In summary, the main contributions of this work are as follows:

• We propose a novel modulation mechanism that embeds information in existing traffic by slightly shifting the packets and/or flipping the packet-order to form a unique pattern that can represent arbitrary strings of data. By doing this, we enable two devices with totally different radios (i.e., WiFi and ZigBee) communicate with each other and do not introduce dummy traffic or modify the hardware. To the best of our knowledge, this is the first work that leverages data traffic for cross-technology communication.

• To further improve the spectrum utilization, our advanced design leverages the independency among different window sizes for embedding different pieces of information in a string of existing packets. In this way, our approach enables one IoT sender simultaneously transmits multiple pieces of information to multiple IoT receivers that have different radios than the sender. For example, one WiFi device transmits three pieces



(a) Time slot 1 (b) Time slot 2 (c) Time slot 3

Fig. 2: Human activity or gesture recognition through coordinated IoT devices: In time slot 1 (see Figure 2(a)), WiFi device #1 sends packets to WiFi device #2. These packets also carry embedded control messages CM1 and CM2 to tell ZigBee devices #3 and #5 starting their transmissions in time slots 2 and 3, respectively. After receiving these embedded control messages, ZigBee devices start to transmit packets at their own time slots (i.e., slots 2 and 3 in Figures 2(b) and 2(c), respectively). All the traffic from WiFi and ZigBee devices can be leveraged for sensing as well. In this way, we can also minimize the interference among WiFi and ZigBee devices due to their overlapped channels.

of message to three different ZigBee devices.

• Our approach is symmetric and generic. It enables the bi-directional communication between WiFi and ZigBee devices (i.e., WiFi to ZigBee and ZigBee to WiFi). Moreover, our approach does not require any modifications on the hardware and is compatible with the commercial off-the-shelf (COTS) devices. We implemented our approach on WiFi and ZigBee platforms and conducted extensive evaluation under real-world settings. The evaluation results show that EMF's throughput is more than 14 times higher than the latest cross-technology communication technique (i.e. FreeBee[1]). Moreover, EMF is robust against the environmental noise. The throughput is very stable across different communication ranges (from 0.5 meter to 40 meters).

II. Motivation

In this section, we first introduce the potential applications that motivate our design, then describe the main observation that provides the foundation for our design.

A. Motivating Applications

In this section, we introduce two different applications which demonstrate a wide range of benefits the EMF technology has to offer.

• **Human activity or gesture recognition through coordinated IoTs:** Human activity or gesture recognition through radio frequency (RF) sensing has been investigated by multiple researchers [6], [7], [8]. In order to achieve continuous monitoring over time, these recognition systems need to continuously send out the radio signals, which includes the artificial traffic that will interfere with the surrounding IoT devices. To address this problem, we need to coordinate the radio signals across multiple IoT devices for the RF sensing over time. Figure 2 illustrates the example of coordinating WiFi and ZigBee devices' traffic for human activity recognition by using our EMF communication method, which enables multiple flows from WiFi to ZigBee devices.

• **Augmented Reality (AR):** As shown in Figure 3, the computer needs to transmit huge volume of high quality

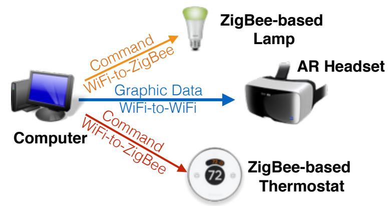


Fig. 3: Augmented reality application

Application	Latency Tolerance (ms)
Regular Websites (e-mail, news)	100-800
Heavy Websites (javascript, images)	50-400
Web Based Remote Systems	30-300
Casual Games (Facebook, flash)	200-1000
Action Games (first person shooters)	10-150
Remote Administration	50-500

TABLE I: Latency tolerance range of network applications [9]

graphic data to the AR headset. These graphic data will occupy the channel all the time and prohibit the communications of nearby ZigBee devices that have overlapped frequency band as the WiFi devices. To address this problem, we can use our EMF communication method that embeds the commands from the WiFi sender (i.e., computer in Figure 3) to ZigBee devices in the WiFi traffic (i.e., graphic data packets). In this way, we can control the ZigBee-based smart lamp and smart thermostat by using regular WiFi traffic and do not need explicit control traffic or customized hardware (e.g., gateway for WiFi to ZigBee communication).

B. Motivating Observation

In this section, we introduce the main observation that provides foundation for our design.

Observation: *Most of the network applications have wide range of latency tolerance (from tens of milliseconds to hundreds of milliseconds, see Table I). Therefore, slightly shifting the packet transmission will not affect the performance of these applications.*

Based on the above observation, we can slightly shift the packet transmission or flip the packet transmission order. Our goal is to embed the cross-technology messages in existing traffic and with negligible impact on the original traffic. For example, we want to enable the concurrent communications from WiFi to multiple ZigBee devices using existing WiFi traffic and introduce minimum delay to the existing WiFi traffic. By doing this, our approach (EMF) will not affect the higher layer applications. Similarly, we can do the ZigBee to WiFi communication. Since most of the ZigBee applications have less restriction on the delay, it is more flexible to send out ZigBee packets.

III. Design Challenges and System Overview

In this section, we first discuss the design challenges and then provide overview of EMF to address these challenges.

A. Challenges

In order to achieve the multiplex cross-technology communication, we have to address the following challenges:

C1. How to efficiently transmit information between WiFi and ZigBee devices? Since WiFi and ZigBee use totally different physical layer, they cannot directly communicate with each other. The most latest technique (i.e., FreeBee [1]) enables WiFi to ZigBee communication by using beacons instead of data packets (due to the complexity of data packets). However, the major part of wireless traffic is data packets. Therefore, FreeBee has extremely low throughput (i.e., as low as 7 bps). To enable efficient communication between WiFi and ZigBee, we need to utilize all the traffic. Unlike beacons, the challenge is that the data packets' size and transmission time are dynamically changing over time. To address this challenge, we propose a novel packet reordering scheme that contains two parts: packet shifting and packet order flipping (detailed in Section IV-B).

C2. How to minimize the bit error rate under unpredictable traffic? Other than throughput, bit error rate (BER) is another important metric that is used in communication systems. BER usually depends on Signal-to-Noise Ratio (SNR) and modulation schemes. It reflects the discrimination ability of different states. Since we utilize the existing traffic, which is unpredictable, to convey embedded messages, the two states (representing "1" and "0") themselves are not stable. Therefore, it will introduce high BER without a careful design of the modulation scheme. To address this challenge, we propose a novel packets scheduling algorithm in our modulation scheme to minimize the BER and have minimum impact to existing traffic (detailed in Section IV-B).

C3. How to enable multiple flows of information from WiFi to ZigBee devices and vice versa with one stream of existing traffic? In order to more efficiently utilize the spectrum, it will be better if we can embed multiple pieces of information in existing traffic and send them to different receivers. However, the challenge is that we only have one stream of existing traffic. To address this challenge, we propose an advanced design that utilizes the independency of multiplied window sizes to convey different messages on a single outgoing packets series to transmit to either multiple receivers or one single receiver (detailed in Section V).

B. System Overview

In this section, we introduce the system architecture of EMF (shown in Figure 4). We first describe the basic design for one-to-one communication (i.e., one WiFi device communicate with one ZigBee device and vice versa), then introduce the advanced design for one-to-many communication (i.e., one WiFi device sends out multiple messages to different ZigBee devices and vice versa). In the rest of the paper, unless explicitly stated otherwise, we will use WiFi as the sender and ZigBee as the receiver to describe the WiFi to ZigBee EMF communication just for clarity purpose. By exchanging the terms "WiFi" and "ZigBee", we can get the ZigBee to WiFi EMF communication.

One-to-one communication: As shown in Figure 4, the WiFi to ZigBee EMF communication contains two parts: modulation at the WiFi sender side and demodulation at the ZigBee receiver side.

• On the WiFi sender side, we add an EMF modulator (detailed in Section IV-B) which rearranges the packets' sending orders within the buffer based on the information needs to be sent from the WiFi device to the ZigBee device. As described in Section II-B, if we can control the packets' latency (detailed in Section VI) within the applications' wide tolerance range, EMF makes negligible impact on the transmission of existing WiFi traffic. Therefore, EMF is transparent to the upper layers (i.e., network and application layers).

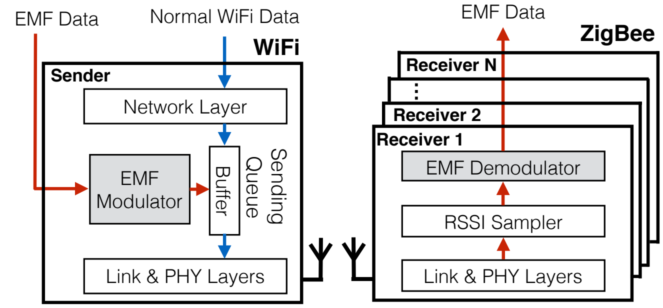


Fig. 4: Overview of WiFi to ZigBee EMF system architecture. By exchanging the terms "WiFi" and "ZigBee" in the above figure, we can also get the ZigBee to WiFi EMF system architecture.

• On the ZigBee receiver side, since the noise floor measurement or received signal strength (RSS) measurement module (for channel detection purpose) is popular on off-the-shelf radios, we utilize the RSS reading sequence from the sampler (shown on the right hand side of Figure 4) to demodulate the embedded information from WiFi sender (detailed in Section IV-C).

One-to-many communication: The most attractive feature of EMF one-to-many communication is that it can embed multiple pieces of information in existing WiFi traffic and send them to different ZigBee devices (shown in Figure 4) with minimum impact to original WiFi traffic. To enable this feature, the WiFi sender needs to adjust the data packets to embed different messages based on different window sizes and the ZigBee receivers will measure the RSS readings with corresponding window sizes (detailed in Section V).

IV. Basic Design: One-to-One Communication

In this section, we introduce the detailed design of one-to-one communication. The definitions of notations used in the rest of this paper are listed in Table II.

A. Communication Establishment

The main purpose of communication establishment is to synchronize the receiver with the sender. We use a simple *folding* approach which is originally proposed to search for weak pulsars in the radio noise picked up by telescopes [10].

In wireless communication system, beacons are periodical packets to announce the presence of a wireless device for others to discover it. We utilize this periodic feature of beacons to synchronize the receiver with the sender, so the first step is to identify the beacons. Without loss of generality, the measured received signal strength (RSS) values over time can be represented as $RSS(t)$. When these RSS readings are chopped with time period P, they can form a matrix $RSS'(i,j)$, where $i \in [1,P]$, $j = t/P$. Then, we build the histogram $h(i)$ of $RSS'(i,j)$ by using the following equation:

$$h(i) = \sum_{n=1}^{j} RSS'(i,n) \tag{1}$$

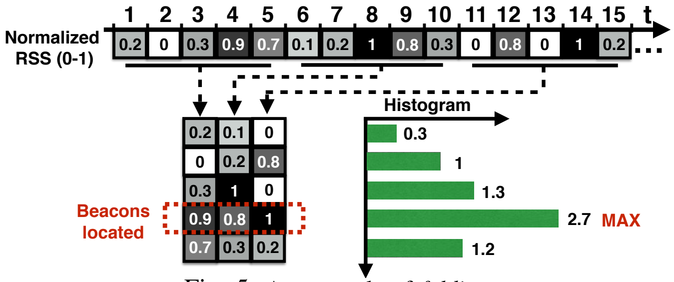


Fig. 5: An example of *folding*

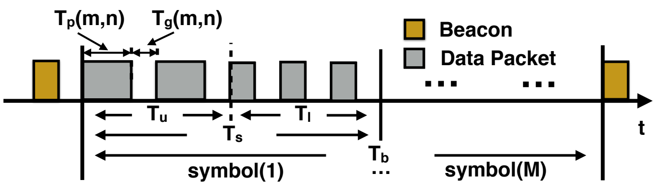


Fig. 6: Modulation of EMF

Based on the maximum value of $h(i)$, we can identify the location of beacon $i = \arg\max_k(h(k))$, because only the periodical beacons' RSS are aggregated together after folding. Therefore, we can synchronize the receiver with the sender.

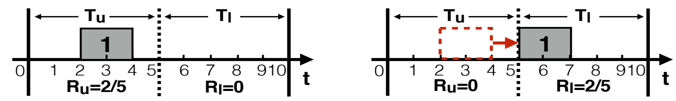
Figure 5 shows an example of the *folding* process to locate the beacons. By looking at the original time series, it is hard for the receiver to identify the beacons. After dividing the whole series by the period $P = 5$ and calculate the histogram, it is easy to identify the maximum value where the index is the location of beacons.

B. Modulation

In this section, we introduce the modulation scheme of EMF by leveraging the existing WiFi packets. Due to various network applications and protocols, the length of packets and packets transmission intervals are dynamically changing, which introduce challenges and also opportunities for our design. As described in Section IV-A, the receiver can identify when the sender's periodical beacons come. Therefore, the sender takes the beacon as a time synchronization flag to modulate data. As shown in Figure 6, the duration between two adjacent beacon is denoted as T_b, which can be divided into M pieces and each piece is called symbol duration window size T_s, where $T_s = T_b/M$ and symbol is the minimum transmission unit (i.e., each symbol represents 1-bit information from the sender to the receiver). We further divide T_s into two parts, where the duration of upper half and lower half is denoted as T_u and T_l, respectively. For clarity purpose, we define the traffic occupancy ratio R to help us describe the modulation scheme.

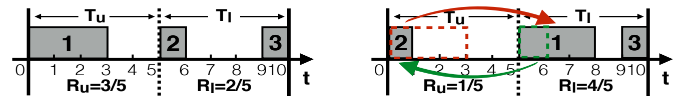
Notations	Definitions
T_b	Time duration between two adjacent beacons
T_s	Symbol duration window size
T_u	Time duration of upper half within one symbol
T_l	Time duration of lower half within one symbol
R_u	Traffic occupancy ratio of upper half
R_l	Traffic occupancy ratio of lower half
T_p	Time duration of transmitting a packet
T_g	Time interval between two packets
λ	Symbol value
τ	Lower bound of T_g

TABLE II: Definitions of Notations



(a) λ=1 (b) Shifted, λ=0

Fig. 7: An example of the shifting operation



(a) λ=1 (b) Flipped, λ=0

Fig. 8: An example of the flipping operation

Definition: *The traffic occupancy ratio R denotes the ratio of total packets duration to the total time duration which can be calculated by using the following equation:*

$$R(m) = \frac{\sum_{n=1}^{N} T_p(m,n)}{\sum_{n=1}^{N} T_g(m,n) + \sum_{n=1}^{N} T_p(m,n)} \quad (2)$$

Where $T_p(m,n)$ is the time duration of transmitting the nth packet and $T_g(m,n)$ is the packet transmission interval between the nth and $(n+1)$th packets ($n \in [1, N]$, N is the total number of packets transmitted during time interval T). $m \in [1, M]$, M is the total number of symbols need to be transmitted by the sender.

With the above definition, we can modulate one symbol by comparing the traffic occupancy ratio within the upper half time duration (T_u) and lower half time duration (T_l) to decide whether this symbol is "1" or "0" using the following equation:

$$\lambda(m) = \begin{cases} 1 & \text{if } R_u(m) > R_l(m) \\ 0 & \text{if } R_u(m) \leq R_l(m) \end{cases} \quad (3)$$

Where $\lambda(m)$ is the value of the mth symbol, $R_u(m)$ and $R_l(m)$ is the traffic occupancy ratio of the upper and lower half of the mth symbol, respectively. Figures 7(a) and 8(a) illustrate simple examples of one symbol. In Figure 7(a), since $R_u = 2/5$ and $R_l = 0$, $R_u > R_l$. Therefore, the symbol value $\lambda = 1$. Similarly, in Figure 8(a), $R_u = 3/5$, $R_l = 2/5$, and $R_u > R_l$, therefore $\lambda = 1$.

Since the packet length and intervals between packets are determined by network and upper layers, in order to transmit an arbitrary bit, we need to change the traffic occupancy ratio. We propose a novel modulation scheme which combines the following two operations:

- **Shifting:** As shown in Figure 7(a), if the original packet-order yields $\lambda = 1$, but the sender wants to transmit "0", the sender needs to shift the packet from the upper half to the lower half (as shown in Figure 7(b)) as shown in Figure 4. Similarly, if the original packet-order yields $\lambda = 0$, but the sender wants to transmit "1", the sender also can shift the packet from the lower half to the upper half. Shifting operation works when there exists enough packets interval (i.e., white space). If the white space is limited, we need to use the flipping operation.
- **Flipping:** As shown in Figure 8(a), if the original packet-order yields $\lambda = 1$, but the sender wants to transmit "0", the sender needs to flip the packet(s) from the upper half to the

Algorithm 1 One-to-one communication scheduling

Input: $\mathbf{D} = \{T_p(1), \cdots, T_p(n)\}$, T_s, τ, and λ.
Output: $\mathbf{Y} = \{T_b(1), \cdots, T_b(n)\}$.

1: **if** $\sum_{i=1}^{n}(T_p(i) + (i-1)\tau) \leq T_s/2$ **then**
2: $\quad \mathbf{S} = 1$;
3: **else**
4: $\quad L = 0, \mathbf{S} = 0$;
5: $\quad$ **while** $L < T_s/2$ **do**
6: $\quad\quad i = \arg\max_k (T_p(k))$;
7: $\quad\quad L = L + T_p(i) + \tau$, $S(i) = 1$, $\mathbf{D} = \mathbf{D} - \{T_p(i)\}$;
8: $\quad$ **end while**
9: **end if**
10: $T_u = 0, T_l = T_s/2$;
11: **for** $i = 1$ **to** n **do**
12: $\quad$ **if** $\lambda = S(i)$ **then**
13: $\quad\quad T_b(i) = T_u$, $T_u = T_u + T_p(i) + \tau$;
14: $\quad$ **else**
15: $\quad\quad T_b(i) = T_l$, $T_l = T_l + T_p(i) + \tau$;
16: $\quad$ **end if**
17: **end for**

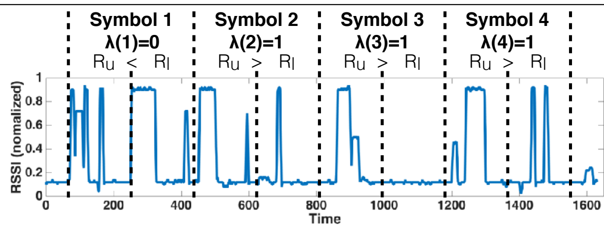


Fig. 9: An example of demodulation with empirical data

lower half (shown in Figure 8(b)). Similarly, if the original packet-order yields $\lambda = 0$, but the sender wants to transmit "1", the sender also can flip the packet(s) from the lower half to the upper half.

To generalize our modulation scheme and minimize its overhead, we propose a lightweight algorithm (see Algorithm 1) to decide how to schedule the packets in the outgoing buffer for modulation purpose. Where τ is the minimum time interval between two packets that is determined by the physical layer. In order to minimize the bit error rate, we need to maximize the difference between R_u and R_l. We first decide whether flipping operation is needed (Line 1). If the sum of n packets' lengths and $n-1$ number of minimum packet intervals is equal or less then half of a window size (i.e., $T_s/2$), flipping is not required. This is because all the packets can be transmitted within $T_s/2$ which results in the highest difference between R_u and R_l. Otherwise, we calculate the possible combinations of packets to reach the potential maximum traffic occupancy ratio for half a window size $T_s/2$ and leave the rest packets to the other half of window size (Lines 4 to 8). Finally, we perform the combination of shifting and flipping operations based on the symbol value (λ) (Lines 10 to 17). The time complexity of Algorithm 1 is $O(n)$ which can easily be implemented on common IoT devices. Where, n is the number of packet during window size T_s. The shifting and flipping operations will introduce delay. Their impacts on the performance will be analyzed in Section VI.

C. Demodulation

In this section, we introduce how to demodulate the message by leveraging the widely available received signal strength (RSS). By using the communication establishment technique described in Section IV-A, the receiver can be synchronized with the sender. After measuring the RSS values for a duration of T_b between two adjacent beacons, the receiver can divide the measured RSS values into two parts (i.e., the upper half and lower half over time) by using the same method we described in the modulation section, then calculate the upper half's and lower half's traffic occupancy ratios (i.e., $R_u(m)$ and $R_l(m)$, respectively) by applying Equation 2. Finally, the receiver is able to demodulate all the symbols by applying Equation 3.

Figure 9 shows an example of the demodulation process. The RSS readings are measured by a ZigBee compliant TelosB device and the signal is transmitted by a WiFi device using 802.11g compliant USRP. As shown in the figure, within the time duration of symbol 1, R_u is less than R_l. Thererfore, the TelosB device gets $\lambda(1)$ = "0". By applying the same method, the TelosB device gets λ = "0111".

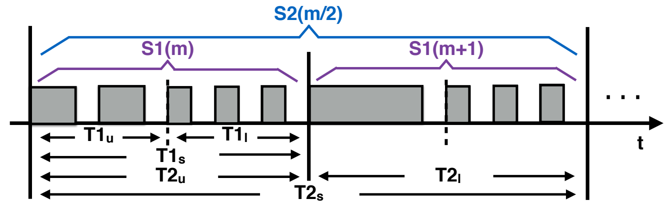


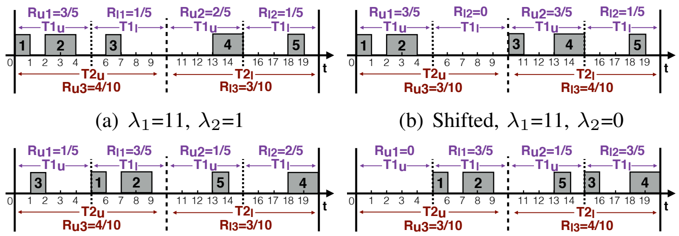
Fig. 10: Modulation of one-to-many EMF

V. Advanced Design: One-to-Many Communication

Build on top of the one-to-one communication described in Section IV, we introduce one-to-many communication which is one of the unique features of our EMF method. Due to the space constraint, we only introduce the modulation of one-to-many communication in this section. The communication establishment is the same as one-to-one communication in Section IV-A. When the receivers demodulate the signal, they choose different window size T_s to obtain corresponding message from the sender and apply the same scheme as described in Section IV-C.

As shown in Figure 10, the symbol sequence $S1(m)$ has symbol duration $T1_s$, which can be divided into upper half duration $T1_u$ and lower half duration $T1_l$. We can also embed another symbol sequence $S2(m/2)$ which has twice of the symbol duration as S1 (i.e., $T2_s = 2 \times T1_s$ and $T2_u = T2_l = T1_s$). Because of the independence of symbol duration T_s with a factor of 2 and the feature of relative difference between traffic occupancy ratio of upper half R_u and traffic occupancy ratio of lower half R_l, we can modulate S1 and S2 on the same original traffic without interfere with each other.

Figure 11 shows an example of our one-to-two modulation scheme. The corresponding detailed description of different cases is shown in Table III. Because $S2$'s time duration is twice of $S1$'s time duration, $S2$ includes two bits of symbols while $S1$ includes one bit. We show four different combinations to illustrate the independence of S1 and S2. The number of messages can be further expanded to three or more. We propose the general algorithm that can modulate m pieces of messages in Algorithm 2. The initial symbols $\mathbf{\Lambda}'$ are calculated with given $\mathbf{D}$ and τ based on Equation (3) (Line 1). Where $\mathbf{D}$ is the set of packet transmission duration and



(a) λ_1=11, λ_2=1 (b) Shifted, λ_1=11, λ_2=0

(c) Flipped, λ_1=00, λ_2=1 (d) Shifted & flipped, λ_1=00, λ_2=0

Fig. 11: An example of one-to-two modulation: two messages $S1$ and $S2$ are transmitted by using windows sizes 5 and 10, respectively. With different shifting and/or flipping operations for packets #1 to #5, arbitrary λ_1 and λ_2 can be transmitted. For example, in Figure 11(a), the original $\lambda_2 = 1$. In order to transmit $\lambda_2 = 0$, we need to shift packet #3 (shown in Figure 11(b)). More detailed combinations are shown in Table III.

Case Figure	Ratio R of S1(1)	Ratio R of S1(2)	Ratio R of S2(1)	λ_1	λ_2
11(a)	$R_{u1} > R_{l1}$	$R_{u2} > R_{l2}$	$R_{u3} > R_{l3}$	"11"	" 1"
11(b)	$R_{u1} > R_{l1}$	$R_{u2} > R_{l2}$	$R_{u3} < R_{l3}$	"11"	" 0"
11(c)	$R_{u1} < R_{l1}$	$R_{u2} < R_{l2}$	$R_{u3} > R_{l3}$	"00"	" 1"
11(d)	$R_{u1} < R_{l1}$	$R_{u2} < R_{l2}$	$R_{u3} < R_{l3}$	"00"	" 0"

TABLE III: Four different cases of transmitting two pieces of arbitrary information

τ is the minimum time interval between two packets that is determined by the physical layer. For each piece of message, if the initial symbol values $\lambda_i^{'}$ do not equal to λ_i and the packets can be shifted, we shift the shortest packet until $\lambda_i^{'} = \lambda_i$ (Lines 2-6). Otherwise, we flip the packets between upper half and lower half (Lines 7-10). Finally we apply Algorithm 1 for all minimum windows (Lines 11-13). The time complexity of Algorithm 2 is $O(nlogn)$, which can easily be implemented on common IoT devices. Where n is the number of packet during window size T_s.

VI. Performance Analysis

In this section, we mathematically analyze different factors that will affect the communication performance and the impact on existing transmission.

RSS sampling rate: To ensure the capture of the smallest packets and intervals between two packets, the RSS sampling rate must meet the following requirement:

$$f_{rss} \geq 2 \cdot MAX(\frac{1}{min(T_p(m,n))}, \frac{1}{min(T_g(m,n))}) \tag{4}$$

Where f_{rss} is the RSS sampling rate, $min(T_p(m,n))$ and $min(T_g(m,n))$ are the transmission time duration of the minimum packet length and minimum transmission interval between two packets, respectively.

The COTS IoT radios usually provide relatively high RSS sampling rate. For example, CC2420 (a common ZigBee radio) provides RSS sampling rate up to 64 kHz [11], which is corresponding to 15.6 μs sampling period that is far less than a WiFi packet transmission duration. For example, the minimum packet duration in 802.11g is 192 μs [12].

Latency: As mentioned in Section IV-B, EMF may introduce latency due to the packet(s) shifting and/or packet-order flipping. To minimize the impact on existing WiFi traffic, ideally, we need to ensure that the introduced latency is less than

Algorithm 2 One-to-many communication scheduling

Input: $\mathbf{D} = \{T_p(1), \cdots, T_p(n)\}$, $\mathbf{\Lambda} = \{\lambda_1, \cdots, \lambda_m\}$, T_s, and τ.
Output: $\mathbf{Y} = \{T_b(1), \cdots, T_b(n)\}$.

1: Calculate $\mathbf{\Lambda}^{'}$ with $\mathbf{D}$ and τ based on Equation (3);
2: **for** $i = m$ to 2 **do**
3:   **while** $\lambda_i^{'} \neq \lambda_i \wedge \tau * i + R_u + R_l \leq T_s * i$ **do**
4:     Shift shortest packet between upper and lower half;
5:     Update $\lambda_i^{'}$ based on shifted results;
6:   **end while**
7:   **if** $\lambda_i^{'} \neq \lambda_i$ **then**
8:     Flip the upper half and lower half;
9:   **end if**
10: **end for**
11: **for** $i = 1$ to 2^m **do**
12:   Apply Algorithm 1 for time slot $[T_s * (i-1), T_s * i]$;
13: **end for**

the lower bound in Table I under different applications. The latency is directly related to the time window T_s. The expected latency of flipping and shifting operation is $1/4T_s$ and $1/2T_s$, respectively. Therefore, to minimize the impact on the existing traffic, ideally, we need to ensure that the maximum latency $1/2T_s$ is less than the lower bound of different network applications in Table I. However, we also note that most of the network applications have wide range of latency tolerance (shown in Table I).

Aggregated throughput: After satisfying Equation 4, we can achieve the expected $Throughput = 1/T_s$. Because the particular modulation we use (introduced in Section V), we are able to transmit N pieces of message simultaneously (one-to-many EMF). So the aggregated throughput is as follows:

$$Aggregated\_throughput = \sum_{n=1}^{N} \frac{1}{T_s/2^{n-1}} \tag{5}$$

VII. Evaluation

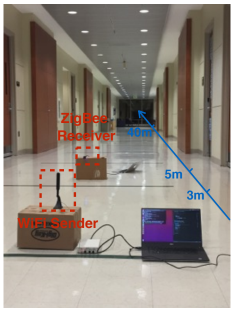
In this section, we first introduce the experimental setup, then evaluate one-to-one EMF with different window size T_s and communication range under different scenarios. We also evaluate the performance of one-to-many EMF. The following two metrics are used to evaluate the wireless communication performance:

• **Throughput:** The number of correctly received data in terms of bit per second (bps).

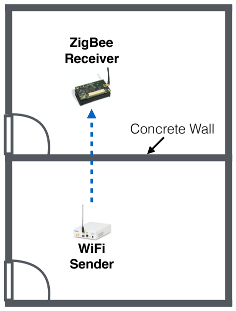
• **Bit error rate (BER):** The number of bits not correctly received divided by the total number of transmitted bits during the cross-technology communication.

A. Experimental Setup

To prove the concept, we implemented the EMF modulation and demodulation scheme on 802.11g [13] WiFi compliant USRP B210 and ZigBee compliant TelosB devices. The using of USRP can help us to better evaluate the performance of our system since we can fully control the PHY layer. In the WiFi to ZigBee communication experiments, the USRP continuously transmitted packets with varying packet lengths (from 100 bytes to 1,500 bytes) based on the traces of real-world WiFi traffic that we collected. The ZigBee devices sample the received signal strength and establish the communication by



(a) Line-of-Sight



(b) None-Line-of-Sight

Fig. 12: Experiments Setup

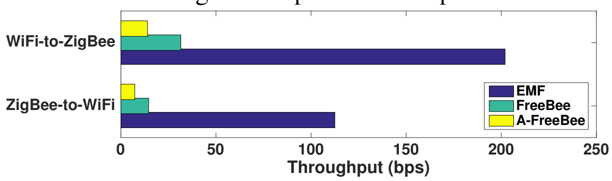


Fig. 13: Comparison between EMF and state-of-the-art cross technology communication FreeBee [1].

applying beacon folding (detailed in Section IV-A). After the communication is established, the receivers demodulate (detailed in Section IV-C) the signal and get the received data. We compare the received data with the originally transmitted data to calculate the bit error rate.

We evaluated our EMF system in an engineering building, which has a lot of other WiFi access points that create interference. To evaluate the robustness of our approach, the USRP uses the most popular WiFi channel 1 and the transmission power is 25 dBm. The ZigBee channel is set to be channel 12, which is overlapped with WiFi channel 1. ZigBee devices sample the RSSI with 32 kHz sampling rate. In each experiment, 4,000 symbols are transmitted. The experiment is repeated for 10 times. Two scenarios are evaluated as follows:

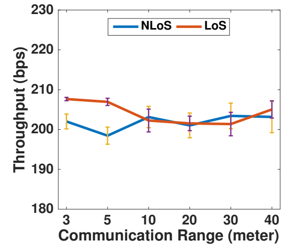
Line-of-Sight (LoS): As shown in Figure 12(a), the LoS scenario is a hallway which is 45 meters long and 4.3 meters wide. We fixed the WiFi sender at one end of the hallway and move the ZigBee receivers so that they are 0.5m, 3m, 5m, 10m, 20m, 30m, and 40m away from the sender.

Non-Line-of-Sight (NLoS): As shown in Figure 12(b), in this scenario, the sender and receiver are deployed in two adjacent rooms which are separated by a concrete wall.

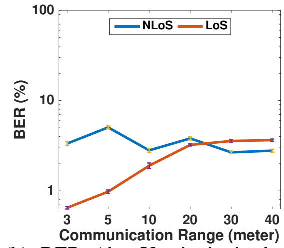
B. Evaluation of one-to-one EMF Communication

In this section, we first compare our approach with the most latest technique (i.e., FreeBee[1]), then evaluate the performance of our approach under diverse settings.

1) Comparison with state-of-the-art: Since our work is the first work that enables the multiple flows of information in cross-technology communication, the state-of-the-art research is complementary, but provides no appropriate baseline for comparison. Therefore, we can only compare our work with the most related and latest work (i.e., FreeBee[1]) under the same setting with one flow of information. The results are shown in Figure 13. Based on these results, EMF is 6.4 and 14.4 times better than the FreeBee and A-FreeBee in terms of throughput during the WiFi to ZigBee communication. During the ZigBee to WiFi communication, EMF is 7.7 and 15.4 times better than the FreeBee and A-FreeBee in terms of throughput. This is because we leverage the data traffic instead of just using beacons. Moreover, our approach can concurrently send multiple packets with *different information* to different ZigBee devices, while FreeBee does not support it.

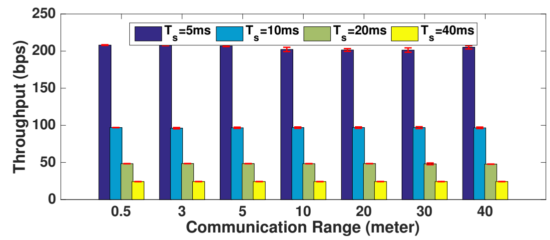


(a) Throughput

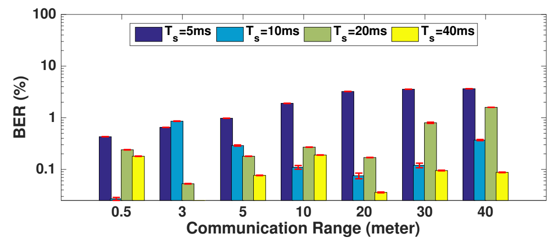


(b) BER (the Y-axis is in log scale)

Fig. 14: Throughput and BER of one-to-one EMF: The performance in NLoS scenario is slightly lower than in LoS in most circumstances, but they are very close to each other when distance increases.



(a) Throughput

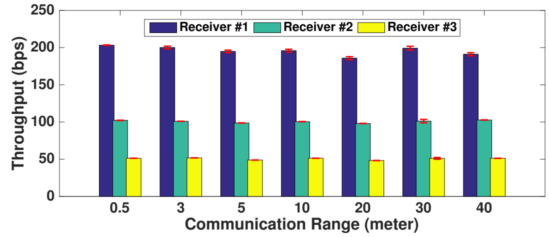


(b) BER (the Y-axis is in log scale)

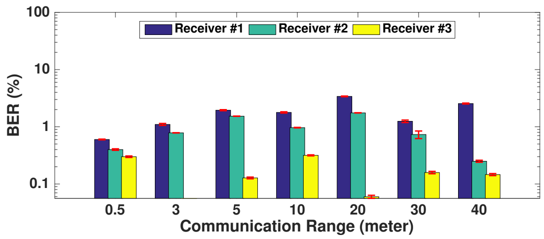
Fig. 15: Impact of window size T_s: The throughput is half when the window size T_s doubled (because the modulation mechanism we used) and it is very stable across all the communication range (from 0.5m to 40m) which shows our EMF modulation scheme is robust.

2) Performance in LoS and NLoS Scenarios: As shown in Figure 14(a), the throughput under NLoS scenario does not have significant difference comparing to LoS scenario. We think it is also because of the robustness of the EMF modulation scheme as we mentioned before. An interesting observation is the BER (as shown in Figure 14(b)) has 2.5% difference between NLoS and LoS (i.e., NLoS>LoS). However, when the distance increases, the difference is less than 1% and the trend is inversed (i.e., LoS>NLoS). We also notice that the standard deviation of both throughput and BER in NLoS scenario is larger than that in LoS scenario. These might be because of that the attenuation and multipath fading in NLoS scenario is more complicated than in LoS scenario.

3) Impact of Window Size T_s: We first investigated the impact of window size T_s (in LoS scenario) which is the most important parameter related to the communication per-

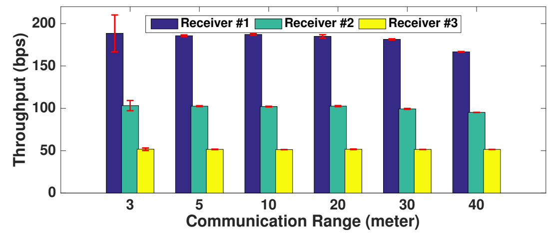


(a) Throughput

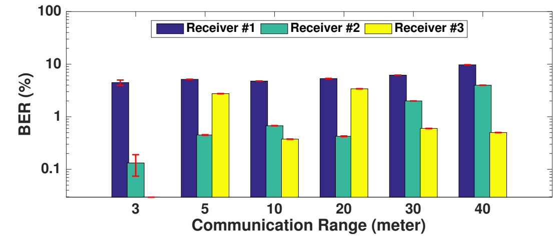


(b) BER (the Y-axis is in log scale)

Fig. 16: Throughput and BER of one-to-many EMF in LoS scenario: the relationship of throughput for three receivers is as expected that the throughput of the first receiver is two and four times of the second and third receiver (as mentioned in Section V), respectively, across all the communication ranges. The stability shows the robustness of the modulation scheme.



(a) Throughput



(b) BER (the Y-axis is in log scale)

Fig. 17: Throughput and BER of one-to-many EMF in NLoS scenario: we note that the throughput has the trend of decreasing and the BER has the trend of increasing. We can see the concrete wall has big impact on one-to-many communication

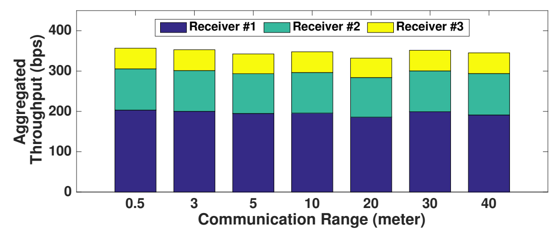


Fig. 18: Aggregated throughput of three ZigBee receivers: the highest aggregated is 356 bps at 0.5m communication range and the throughput is 344 bps at 40m.

formance (as discussed in Section VI).

As shown in Figure 15(a), the throughput is halved when the window size T_s is doubled (because the modulation mechanism we used). The highest throughput is 208 bps ($T_s = 5ms$). The throughput is very stable from 0.5m to 40m. The result shows that our EMF modulation and demodulation scheme is robust. This is mainly because the scheme is based on the relative traffic occupancy ratio and this ratio is widely detectable even when the signal strength is getting lower.

Figure 15(b) shows the BER of different window size. We can observe the trend that the BER slightly increases when the range increases. The BER is less than 1% when the range is shorter than 10 meters and less than 4% when the range is shorter than 40 meters. At a same range, basically, the BER decreases when the window size T_s increases, this is because the longer the window size is, the more packets can be operated which yields large difference on R_u (traffic occupancy ratio of upper half) and R_l (traffic occupancy ratio of lower half).

C. One-to-many EMF Performance

The most attractive feature of EMF is one-to-many communication. In this section, we show the results of one-to-many communication.

1) Line-of-sight Scenario: As shown in Figure 16(a), the highest throughput is 203 bps, 102 bps and 51 bps for three receivers at 0.5m and 191 bps, 98 bps and 48 bps at 40m, respectively. The BER does not exceed 1% for all the ranges. We notice the throughput changing trend of one-to-many along communication range is as stable as in one-to-one communication, but the BER (as shown in Figure 16(b)) is a little bit higher than in one-to-one communication. Intuitively, it is because managing three transmission makes the packet-order control less flexible than managing one transmission so that the difference of two traffic occupancy ratios (R_u and R_l) is smaller. In Algorithm 2, the shifting and flipping operations for larger window size may slightly reduce the BER for smaller window size.

2) Non-line-of-sight Scenario: In NLoS scenario, the highest throughput in NLoS scenario is 188 bps, 103 bps and 51 bps for three receivers at 0.5m and 166 bps, 95 bps and 51 bps at 40m, respectively (as shown in Figure 17(a)). The BER increases along with the communication range which reaches 19% at 40m (as shown in Figure 17(b)). The results show the concrete wall in the middle of sender and receivers makes relative high impact on one-to-many communication. We think this is because of that the multipath fading reduces the difference between two traffic occupancy ratios R_h and R_l in NLoS scenario.

For the three receivers at the same communication range, we observe the performance of the first receiver decreases when the third receiver is relative stable due to larger window size.

3) Aggregated Throughput: Theoretically, EMF can support much more concurrent receivers to receive different messages. In our evaluation, we evaluated three concurrent receivers and the experimental results are shown in Figure 18. The figure shows the aggregated throughput of three ZigBee receivers can achieve 356 bps when receivers are close to the sender and 344 bps when receivers are even 40m far away from the sender. The green and yellow parts are the benefits by using our one-to-many scheme.

VIII. Related Work

The most related work are in the following two categories:

Networking performance optimization within one communication technology: In the most crowded 2.4GHz ISM band, researchers have investigated how to improve spectrum utilization [14], [15], [16], [17], [18]. Another bunch of papers investigated on the collision avoidance methods [19], [20], [21]. Instead of avoiding interference by channel sensing type of scheme, our work investigate how to establish the communication link across technologies by leveraging the RSSI framework which is widely available on COTS devices. We note that RSSI and CSI have been utilized in various applications such as indoor localization [22], [23], [24], [25], [26], human activity recognition [6], [7], [8], and cross-technology communication.

Cross-technology communication systems: Many works utilize the coexistence of different technologies on a same band (e.g., WiFi and ZigBee are on the same 2.4GHz band) to help each other [27], [28], [29]. And several cross-technology communication systems [3], [5], [1], [4] have been introduced. Esense [3] and HoWiES [5] enables WiFi to ZigBee communication by modulating on the packet length of WiFi packets. GSense [4] uses special preamble to deliver coordination messages. FreeBee [1] leverages beacons for cross-technology communication. B^2W^2 [30] enables multiple BLE to WiFi communications by using of CSI.

Different from the above approaches, we explore the possibility of embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices. Our approach has the potential to concurrently coordinate multiple IoT devices and enable multiple applications simultaneously.

IX. Conclusion

The increasing number of IoT devices and limited available spectrum motivate us to leverage existing traffic for concurrent cross-technology communication with multiple flows of information. Specifically, we introduce EMF communication method, which (i) embeds different pieces of information in existing traffic and (ii) concurrently sends out these information from one IoT sender to multiple IoT receivers that have a different communication technology from the sender. By doing this, our EMF method (i) enables cross-technology communication among heterogeneous IoT devices, (ii) does not introduce any extra control traffic, and (iii) is transparent to the higher layer applications. We conducted extensive experiments to evaluate our approach in real-world settings. The evaluation results show that EMFs throughput is more than 14 times higher than the latest cross-technology communication technique (i.e. FreeBee [1]). Moreover, our approach can concurrently send multiple packets with *different information* to different ZigBee devices, while FreeBee does not support it.

Acknowledgment

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

References

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

[2] "http://www.gartner.com/newsroom/id/3165317."

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

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

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

[6] Y. Li and T. Zhu, "Gait-Based Wi-Fi Signatures for Privacy-Preserving," in *ASIACCS*, 2016.

[7] Y. Li and T. Zhu, "Using Wi-Fi Signals to Characterize Human Gait for Identification and Activity Monitoring," in *CHASE*, 2016.

[8] Z. Chi, Y. Yao, T. Xie, Z. Huang, M. Hammond, and T. Zhu, "Harmony: Exploiting coarse-grained received signal strength from iot devices for human activity recognition," in *ICNP*, 2016.

[9] "https://www.citycloud.com/city-cloud/some-interesting-bits-about-latency/."

[10] R. LOVELACE, J. SUTTON, and E. SALPETER, "Digital search methods for pulsars," *Nature*, vol. 222, pp. 231–233, Apr 1969.

[11] "http://www.ti.com/lit/ds/symlink/cc2420.pdf."

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

[13] "https://github.com/bastibl/gr-ieee802-11."

[14] 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.

[15] J. Jun, L. Chen, L. He, Y. Gu, and T. Zhu, "Exploiting Sender-based Link Correlation in Wireless Sensor Networks," in *IEEE ICNP*, 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] Luo, Hongyao and Huang, Zhichuan and Zhu, Ting, "A survey on spectrum utilization in wireless sensor networks," *Journal of Sensors*, vol. 2015, 2015.

[18] S. Kumar, D. Cifuentes, S. Gollakota, and D. Katabi, "Bringing cross-layer mimo to today's wireless lans," in *SIGCOMM, 2013*.

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

[20] 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.

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

[22] Q. Zhang, Z. Zhou, W. Xu, J. Qi, C. Guo, P. Yi, T. Zhu and S. Xiao, "Fingerprint-free Tracking with Dynamic Enhanced Field Division," in *IEEE INFOCOM*, 2015.

[23] P. Yi, M. Yu, Z. Zhou, Q. Zhang, W. Xu, and T. Zhu, "A Three-Dimensional Wireless Indoor Localization System," *Journal of Electrical and Computer Engineering*, 2014.

[24] D. W. Z. Zhong, T. Zhu and T. He, "Tracking with Unreliable Node Sequence," in *IEEE INFOCOM*, 2009.

[25] J. Jun, Y. Gu, L. Cheng, B. Lu, J. Sun, T. Zhu, and J. Niu, "SocialLoc: Improving Indoor Localization with Social Sensing," in *ACM SenSys*, 2013.

[26] Q. Zhang, W. Xu, Z. Huang, Z. Zhou, T. Zhu, P. Yi, and S. Xiao., "Context-Centric Target Localization with Optimal Anchor Deployments," in *IEEE International Conference on Network Protocols*, 2015.

[27] T. Hao, R. Zhou, G. Xing, M. W. Mutka, and J. Chen, "Wizsync: Exploiting wi-fi infrastructure for clock synchronization in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 6, pp. 1379–1392, June 2014.

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

[29] R. Zhou, Y. Xiong, G. Xing, L. Sun, and J. Ma, "Zifi: Wireless lan discovery via zigbee interference signatures," in *MobiCom, 2010*.

[30] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B^2W^2: N-way concurrent communication for iot devices," in *SenSys*, 2016.