Simultaneous Bi-Directional Communications and Data Forwarding Using a Single ZigBee Data Stream

Zicheng Chi, *Member, IEEE*, Yan Li, *Member, IEEE*, Hongyu Sun, *Member, IEEE*, Zhichuan Huang, *Member, IEEE*, and Ting Zhu, *Senior Member, IEEE*

***Abstract*— With the exponentially increasing number of Internet of Things (IoT) devices and the huge volume of data generated by these devices, there is a pressing need to investigate a more efficient communication method in both frequency and time domains at the edge of IoT networks. In this paper, we present Amphista, a novel cross-layer design for IoT communication and data forwarding that can more efficiently utilize the ever increasingly crowded 2.4 GHz spectrum near the gateway. Specifically, to enable the communication from ZigBee to WiFi, we leverage WiFi's fine-grained channel state information to extract the concurrently transmitted ZigBee-to-WiFi message from time overlapped ZigBee and WiFi packet. We further leverage this unique feature and design a novel forwarding protocol that can simultaneously forward uplink (e.g., collecting sensing data) and downlink (e.g., disseminating control messages) data by using a single ZigBee data stream. Our extensive experimental results show that Amphista significantly improves throughput (by up to 400x) and reduces the latency.**

***Index Terms*— Wireless, cross-technology, CPS, Internet of Things (IoT).**

I. Introduction

THE number of Internet-of-Things (IoT) devices will grow exponentially to reach 1 trillion by 2025 [1]. Each person will touch or use 300 to 500 "smart" devices every day by 2032 [1]. These devices will also generate a huge amount of wireless traffic. Based on the Cisco Global Cloud Index [2], the data created by these devices will reach 42.3 ZB (i.e., 4.23×10^{22} bytes) per month and will be 49 times higher than the total data center traffic by 2019. Therefore, there is a pressing need for conducting the computing at the edge of the network instead of in the cloud.

In edge computing, it is extremely important to efficiently collect the huge amount of data generated by these densely deployed IoT devices at the edge (e.g., gateway) of the network. This is because most of these IoT devices are using the industrial, scientific, and medical (ISM) band. The ever-growing number of IoT devices and the huge amount of data generated by these devices will cause the ISM 2.4 GHz band to be extremely crowded. This issue is becoming worse at the gateway side because all the data from heterogeneous IoT networks needs to be sent to the gateway through the overlapped wireless channels. For example, in Figure 1, a WiFi high quality (HQ) video camera is uploading real-time surveillance video to the gateway using WiFi channel 6, which is overlapped with ZigBee channels 16 to 19. To avoid WiFi packets colliding with ZigBee packets at the gateway, traditional approaches adopt either carrier-sense multiple access (CSMA) or time-division multiple access (TDMA). These approaches can effectively reduce the packet collisions when the number of IoT devices is small.

However, with the exponentially increasing number of IoT devices and huge volume of data generated by these devices, these approaches may cause inefficient communication in both time and frequency domains. In the time domain, only one device is able to send the packets to the gateway at any given time. For example, if a ZigBee device is sending packets to the gateway, the WiFi HQ video camera needs to wait. This will introduce significant latency and an interruption to the real-time WiFi video traffic, especially when the number of ZigBee devices increases; in the frequency domain, the transmission from a narrow-band ZigBee device will prevent the wide-band WiFi device's transmission. Therefore, the spectrum utilization is extremely low. For example, in order to avoid interference, when a ZigBee device is sending packets to the gateway using a 2 MHz channel (e.g., channel 19), the WiFi HQ video camera cannot use the whole 20 MHz WiFi channel 6 that is overlapped with ZigBee's channel 19. One may argue that the WiFi HQ video camera can use another WiFi channel. However, all the WiFi channels are overlapped with ZigBee channels. As the number of IoT devices exponentially

Manuscript received June 16, 2019; revised July 7, 2020 and November 20, 2020; accepted December 27, 2020; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor M. Li. Date of publication January 29, 2021; date of current version April 16, 2021. This work was supported in part by NSF under Grant CNS-1824491 and Grant CNS-1652669, in part by the National Natural Science Foundation of China under Grant 61802451, and in part by the Fundamental Research Funds for the Central Universities under Grant 18LGPY61. *(Corresponding author: Ting Zhu.)*

Zicheng Chi is with the Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44115 USA (e-mail: z.chi@csuohio.edu).

Yan Li is with the Johns Hopkins Applied Physics Laboratory, Laurel, MD 20723 USA (e-mail: liy1@umbc.edu).

Hongyu Sun is with the College of Computer Science, Jilin Normal University, Siping 136000, China (e-mail: hongyu@jlnu.edu.cn).

Zhichuan Huang is with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510275, China (e-mail: huangzhich@mail.sysu.edu.cn).

Ting Zhu is with the Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250 USA (e-mail: zt@umbc.edu).

Digital Object Identifier 10.1109/TNET.2021.3054339

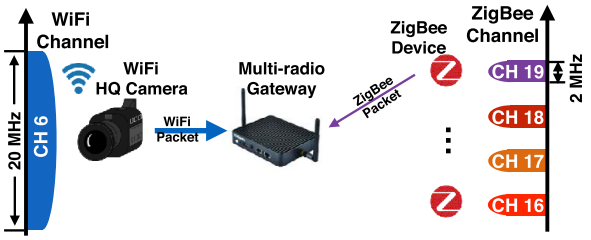


Fig. 1. Limitations of CSMA (or TDMA) -based approaches. The transmission of ZigBee packets in the 2 MHz ZigBee channel 19 to the gateway will block the WiFi packets in WiFi channel 6. Therefore, it i) introduces the delay to WiFi traffic; and ii) reduces the spectrum utilization in the 20 MHz WiFi Channel 6.

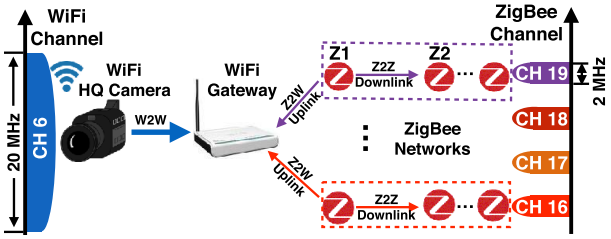


Fig. 2. Advantages of Amphista. Z2Z, Z2W, and W2W communications can be conducted concurrently.

increases, it is not possible to find a clear and designated channel that can only be used by WiFi devices.

To address this limitation, we propose a novel design across physical and network layers. Our proposed approach – Amphista enables WiFi and ZigBee devices to simultaneously transmit their packets to the gateway.

At the physical layer, Amphista embeds the ZigBee to WiFi (Z2W) data into ZigBee to ZigBee (Z2Z) communication by smartly modulating ZigBee packets' transmission power. The Z2W data can be detected by the channel state information on the WiFi gateway along with the WiFi to WiFi (W2W) transmission. As shown in Figure 2, the unique feature of Amphista is that when a ZigBee device ($Z1$) is conducting Z2W communication with the gateway (e.g., uploading sensing data), the same stream of ZigBee packets can be leveraged for forwarding the data from $Z1$ to another ZigBee device $Z2$ (e.g., disseminating control messages). By doing this, Amphista enables a ZigBee device to send out two different pieces of information to both the WiFi gateway and other ZigBee devices using a single ZigBee data stream that coexists with WiFi to WiFi communication. To summarize, Amphista supports three types of simultaneous communications: i) WiFi to WiFi (W2W), ii) ZigBee to ZigBee (Z2Z), and iii) ZigBee to WiFi (Z2W) communications at the same time within the same channel. Therefore, Amphista can provide much higher spectrum utilization than CSMA and TDMA methods.

At the network layer, we further leverage the unique physical layer communication feature and design a novel data forwarding protocol that can *simultaneously* provide **uplink** and **downlink data forwarding** using a *single* ZigBee data stream. Overall, Amphista can support 4 independent ZigBee uplink and downlink data streams that are simultaneously coexisting with the WiFi traffic. Therefore, the spectrum utilization at the gateway is significantly increased.

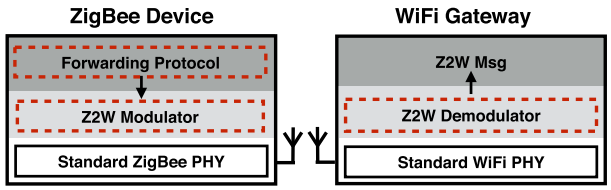


Fig. 3. System Architecture of Amphista. Our design is highlighted in red dashed boxes.

In summary, our main contributions are as follows:

- We developed a novel *simultaneous* communication method that enables three types of simultaneous communications: W2W, Z2Z, and Z2W. Different from existing approaches, our method enables the heterogeneous IoT devices to transmit their packets to the gateway at the same time and within the overlapped channel. Amphista can significantly increase the spectrum utilization and reduce the number of retransmissions due to the packets collision between WiFi and ZigBee devices.

We built a heterogeneous handshaking process (i.e., a two-way scheme to negotiate between ZigBee and WiFi devices) to minimize the cross-technology interference. Our evaluation results demonstrate that our approach introduces negligible interference to the original WiFi-to-WiFi and ZigBee-to-ZigBee communications.

- Different from existing cross-technology communication methods that only focus on the PHY layer, we designed a distributed simultaneous uplink and downlink data forwarding scheme that uses the same stream of ZigBee packets to *simultaneously* i) upload sensing data to the gateway and ii) disseminate control messages inside the ZigBee network. To the best of our knowledge, this is the first technology that can provide uplink and downlink data forwarding simultaneously. Our scheme only needs one-hop neighbors' information. Therefore, it is simple, symmetric, highly distributed, and scalable.
- We extensively evaluated our design under four different real-world settings. Amphista significantly improves throughput (by up to 400x) and reduces the latency. Moreover, Amphista's spectrum efficiency is 2.29 times higher than traditional CSMA and TDMA-based approaches.

II. Design Overview

Figure 3 shows the system architecture of Amphista, which provides the following two functions:

I) ZigBee to WiFi (Z2W) Gateway Communication. Since ZigBee and WiFi radios use fundamentally different physical layers, ZigBee cannot directly communicate with WiFi. To enable the communication from ZigBee to WiFi, we leverage WiFi's fine-grained channel state information (CSI) to decode embedded messages from time overlapped ZigBee packets. Since CSI is used to measure WiFi's physical channel, while the channel is affected by ZigBee, we can use CSI sense the existence of ZigBee packets. In other words, a concurrent message from ZigBee can be received along with WiFi messages at the WiFi gateway.

II) Forwarding Protocol. Our forwarding protocol leverages the unique feature, concurrent Z2Z and Z2W

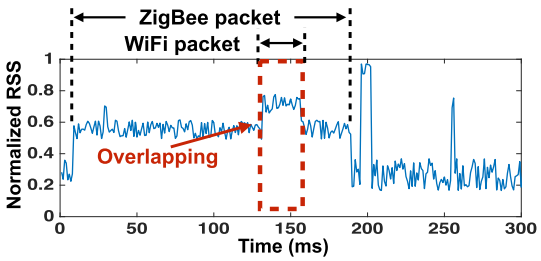


Fig. 4. Concurrent Transmissions.

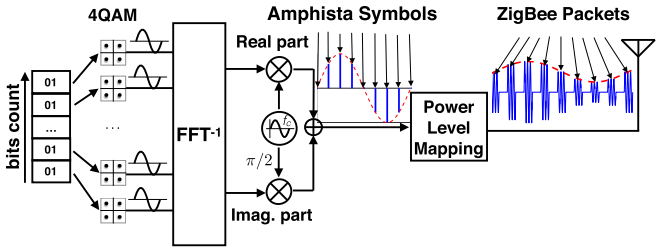


Fig. 5. 4QAM-OFDM on top of the channel state information.

transmissions, to minimize the total number of transmissions and average time delivery delay in the entire network. In this forwarding protocol, there are two main functions: i) neighbor maintenance, which maintains the throughput to each ZigBee node's 1-hop neighbors and to the WiFi gateway; ii) forwarding decision, which splits the data into three sending buffers.

III. Z2W Communication

In this section, we introduce how to achieve Z2W communication without i) affecting Z2Z and W2W communications and ii) modifying physical layers of WiFi and ZigBee. Specifically, we design novel modulation and demodulation schemes on top of the standard WiFi and ZigBee physical layers.

A. Z2W Modulation at ZigBee Sender Side

The objective of Amphista's physical layer design is to simultaneously enable Z2Z and Z2W communications. Figure 4 shows an example of a WiFi packet and ZigBee packet that is overlapped in the time domain and we can observe that the overlapped part has a different signal strength. As an overview, our design for Z2W communication is to leverage the under-utilized power transmission capabilities in commodity ZigBee radios. Therefore, by modulating the transmission power levels of each ZigBee packet, we embed information for Z2W messages in each ZigBee packet. It is worth noting that the ZigBee protocol uses a Direct-Sequence Spread Spectrum (DSSS) technique which can minimize the impact of transmission power changing on Z2Z communication. We introduce the basic modulation schemes (PAM, MSK, and 4QAM-OFDM) for embedding WiFi information in the power levels of each ZigBee packet:

Pulse-Amplitude Modulation (PAM) is the simplest solution, which directly modulates the Z2W message on the power levels of ZigBee packets. Each power level is related to symbols that represent the binary data combinations. Though PAM achieves high throughput, the bit error rate (BER) increases significantly in noisy environments.

Minimum-Shift Keying (MSK) is a phase-based modulation, which is more robust to noise. An MSK modulator maps each binary combination or symbol to 4 possible sine wave phase states. MSK is easy to be implemented on a ZigBee device as we just need look-up tables between the symbol and 4 possible sine wave phase states. However, MSK has low spectrum utilization which means lower throughput.

4QAM-OFDM divides the spectrum into multiple subcarriers and modulates the data on each subcarrier. As shown in Figure 5, since the available ZigBee's transmission power levels are limited, we use 4 Quadrature Amplitude Modulation (4QAM) for each subcarrier to modulate two bits of data (i.e., four different phases can be assigned to each subcarrier). Eight subcarriers are used to carry data. The eight subcarriers are mapped and summed into an output signal by using Inverse Fast Fourier Transform (IFFT). The output signal is mapped into the power levels for each packet. Since we use ZigBee packets' transmission power to form the OFDM signal, the maximum throughput mainly depends on factors such as packet rate (which depends on payload length) and available power level (which depends on the result from the handshaking process).

TABLE I
Comparison of Different Modulation Methods

Modulation Schemes	PAM	MSK	4QAM-OFDM
Spectrum Efficiency	High	Low	High
Sensitive to Noise	High	Low	Low
Complexity	Low	Low	High

Table I shows the comparison among these three modulation schemes. Compared to PAM, 4QAM-OFDM provides similar spectrum efficiency while it can also work under noisy environments. 4QAM-OFDM is noise immune like MSK but provides much higher spectrum efficiency. The only issue for 4QAM-OFDM is that the implementation of OFDM needs to calculate IFFT, which is difficult for ZigBee to calculate in real-time given its limited computation and energy resources. To solve this problem, we precompute a lookup table to map the data bits and modulated power levels. The size of the lookup table is $log_2 M \times S \times C$ bits, which is small and can be stored in ZigBee's memory. The M, S, and C are the number of states used to represent data, the symbol rate, and the information capacity of data bits, respectively. In our implementation, the size of the lookup table is around 64KB, which is much less than the flash size of ZigBee devices (e.g., flash size of a TelosB device is 1024KB).

B. Z2W Demodulation at WiFi Gateway

At the WiFi gateway receiver side, the Z2W demodulator's main functionalities are i) extracting the embedded Z2W message and ii) recovering the original W2W message.

1) Design of Z2W Message Extractor: In this section, we explore how to extract the embedded signals in the received WiFi packets in a noisy environment. The embedded Z2W message can be extracted by measuring the amplitude of channel state information when demodulating the WiFi signal. A threshold filter removes the channel state information

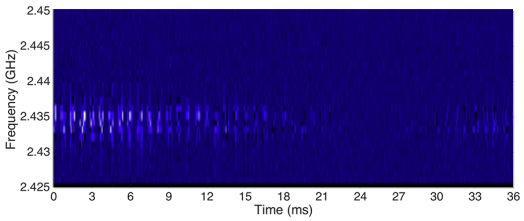


Fig. 6. Different TX power recovered by using CSI.

that does not contain embedded messages. Thus, the values passed to the demodulators are values with the embedded ZigBee message and channel interference. In the demodulation scheme, we first obtain the channel state information values defined as $x(t)$. We can then derive the quadrature symbols from the following equation:

$$b_i(t) = x(t) \cdot \cos(f_c + \phi),$$
$$b_q(t) = x(t) \cdot \sin(f_c + \phi), \tag{1}$$

where, f_c is the Nyquist frequency that is inversely proportional to the length of the ZigBee packet. The demodulation algorithm maintains the phase state ϕ. An example is shown in Figure 6, which visualizes CSI values. The white part has a high amplitude, which is affected by ZigBee packets. This example shows using CSI can extract the overlapped ZigBee packets with different TX power. After the quadrature symbols are computed, we pass the symbols into the predetermined demodulation scheme. Each modulation (PAM and 4-QAM OFDM) scheme maps the symbols using lookup tables to their respective bits.

2) Recovering the Original WiFi Message: While extracting Z2W messages, the WiFi receiver also recovers the WiFi messages. The recovering is possible because of the three techniques 1) interference cancellation, 2) equalization, and 3) bit error correcting techniques. First, from the received WiFi signal, we subtract out portions of interfering ZigBee signals. Then, we apply an equalization method on the remaining WiFi signals using a channel sensing technique. Finally, after the signals are decoded to bits, an error correcting code is applied to the bits associated with the equalized WiFi subcarriers that are overlapped with ZigBee channels.

Interference cancellation: Our interference cancellation functions simultaneously transmit data and commonly repeated wireless signals (e.g., beacons and headers) to recover original WiFi messages. By sensing the amount of interference, we are able to obtain the ZigBee packets' interference. Then, we apply the interference cancellation technique using the following equation:

$$z(t) = x(n) - \sum_{n=1}^{N} \psi_n x\left(t - \tau_n\right), \tag{2}$$

where, $z(t)$ is the recovered WiFi signal at time t, $x(n)$ is the received signal that contains noise. ψ_n is the complex coefficient describing the interfering signal. τ_n is the delay respective to the transmission time of the interferer. To determine ψ_n, we use the standard Least Mean Square (LMS) adaptive filter. We update the ψ_n variable by using the following equation:

$$\psi_{n+1} = \psi_n + \mu \sum x^*\left(t - \tau_n\right) \cdot z(t), \tag{3}$$

where, μ is the updating step size control factor. After the noise subtractions, we must correct the phase in the quadrature signals by using the frequency selective fading equalization. x^* is related to ZigBee's Pseudo Noise (PN) signal. ZigBee uses a shared PN code to spread to a wider channel becoming more resistant to interference. This PN code is a standard constant array of random-like numbers that is multiplied by the ZigBee transmitter and ZigBee and Amphista receivers. The intuition behind the LMS adaptive equalization functions is that with the shared ZigBee PN coding, we can remove ZigBee interference in the received WiFi packet.

Frequency Selective Fading Equalization: Because of human movements and objects that reflect RF signals, the WiFi channel experiences strong frequency selective fades. Existing commodity WiFi devices must recover from faded signals due to channel interference such as fading and delays using an equalizer. Since the Z2W message in Amphista's simultaneous communication also causes distortions within specific frequency bands. The commodity WiFi receiver treats the interference from ZigBee as frequency selective fading. Therefore, the native equalizer is able to recover the original WiFi signal by using the pilot tones that are signals agreed upon by the transmitter and receiver.

To define this interference, the receiver computes the channel's frequency response (H_n) for each pilot tone. The receiver is supposed to receive $\overrightarrow{X_w}$ but instead receives $\overrightarrow{y}$. Computing the difference vector $\overrightarrow{h}$, the receiver applies correction to all bits around the pilot tone's frequency. We model the interference correction process as quadrature values due to the sine wave signals. The equalization scheme for the interfered carrier correction quadrature values are defined below:

$$i'_n = H_n\left[i_n \cos\left(\theta_n\right) + j_n \sin(\theta_n)\right], \tag{4}$$
$$j'_n = H_n\left[j_n \cos\left(\theta_n\right) - i_n \sin(\theta_n)\right], \tag{5}$$

where, i'_n and j'_n are the correction quadrature values. i_n and j_n are the received pilot tone quadrature values, which are sent to the traditional WiFi OFDM demodulation systems, then the original WiFi bits are recovered.

Error Correcting Codes: After the WiFi bits are demodulated from each WiFi subcarrier, we note that the subcarriers associated with overlapped ZigBee channels may have a relatively high probability of bit error. By appending Error Correcting Codes (ECC) to the data stream during concurrent communication, we can also increase the probability of reception. Because corruption in the bit stream can be expected, as ZigBee packets are transmitted within a fixed frequency band, we can append an extra ECC to non-affected bits. We utilize the Reed-Solomon ECC as the scheme allows for variable matrix recovery sizes. We produce this matrix by encoding data chunks with a polynomial. For a message m with a length of i, we define the error correcting polynomial in the following equation:

$$m(x) = m_0 + m_1 x + m_{i-1} x^{i-1}. \tag{6}$$

The Reed-Solomon ECC depends on solving $n = i + 2s$ non-zero points, where s is the maximum number of errors. Thus, n is directly related to the number of appended ECC bits to the data stream. Intuitively, as the Z2W link quality or ZigBee signal strength increases, we increase the number of appended ECC bits. This solution is optimal because the number of appended ECC bits is directly related to the amount of ZigBee interference. From the experimental results, the number of appended ECC bits is always less than 1% of the total WiFi data.

C. Handshake Between ZigBee and WiFi

To conduct data communication between ZigBee and WiFi devices, a handshaking process is needed to i) determine ZigBee sender's transmission power range, which ensures the Z2W signals do not saturate WiFi's ADC (analog to digital converter) or are not sensible; and ii) synchronize phase for different modulation schemes.

Power Range Determination: To ensure concurrent Z2W and W2W communications, the concurrent transmissions of WiFi and ZigBee must not saturate ADC inputs of WiFi and ZigBee, but still remain above the sensitive levels. The power level handshaking scheme allows concurrent power level transmissions.

Power Range Optimization: The objective of this optimization is to coordinate transmission power of both the overlapping ZigBee and WiFi devices so that the Z2W communication generates negligible impact to original Z2Z and W2W communications. Intuitively, concurrent communication is possible because 1) both coordinated radios are aware of each other's interference, sensitivity levels, and transmission rate; and 2) the WiFi and ZigBee protocols are designed to be robust against interference. To achieve the optimal concurrent transmission powers, we first introduce a ZigBee modulation scheme, and then describe our receiver synchronizing handshaking protocol.

ZigBee modulates information using 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 transmitted signal into a wider band by multiplying it with a higher rate Pseudo Noise (PN) code, this is also known as Direct Sequence Spread Spectrum (DSSS). Since ZigBee does not modulate data on amplitude, we utilize the full range of the transmission power to communicate with WiFi and ensure that it can be sensed by WiFi's channel state information. However, this transmission power must not exceed the WiFi radio's sensitivity range. Therefore, to achieve modulating within the valid transmission power levels, we must search for the optimal transmission power of the two devices.

By understanding cross-technology receiver sensitivity, we need to control the transmission power of WiFi and ZigBee devices. We define the receiver's sensitivity for ZigBee with Equation 7 and WiFi with Equation 8.

$$S_z = \mathrm{R_{NF}} + K \cdot T \cdot Chip\_Rate + \frac{E}{N_{tx} + S_w} - \mathrm{PG}, \quad (7)$$

where $\mathrm{R_{NF}}$ is the radio's noise figure or system noise, K is the Boltzmann's constant and T is temperature. $Chip\_Rate$ is ZigBee's chip rate at 2 MHz. $\frac{E}{N_{tx}}$ is transmission's signal to noise ratio. In current transmission, the noise also includes the overlapped WiFi's signal S_w. PG is the process gain or the clock stability of the receiver and transmitter.

$$S_w = K \cdot T \cdot B + \frac{E}{N + S_z} - PG, \quad (8)$$

where B is the total bandwidth and S_z is the overlapped ZigBee signal. Therefore, S_w and S_z demonstrate the need to control the transmission power of both ZigBee and WiFi. This optimization search problem can be solved with an efficient search in the handshaking protocol. We frame the search space as the range of sequential power values given the RF propagation characteristics, receiver sensitivity, and transmitter gain. We define the search as the maximum length of sequential power levels in terms of two power array sizes. Let $P_{\min} < i < P_{\max}$, with minimum and maximum powers that allow the receiver to discriminate concurrent transmissions. With a successful handshake, the WiFi receiver responds with a predefined ACK packet thus defining a power range array:

$$A(i) = \lfloor 1 + \max\{A(j) | P_{\min} \leq j \leq P_{\max} \& a_j < a_i\} \rfloor, \quad (9)$$

where $A(i)$ is an array sized in power of two as to follow binary computing, a_i and a_j are individual elements in the array. Since the CSI amplitude may be affected by the multipath effect in real world scenarios, we need to build a channel model to combat the multipath effect. During the handshaking procedure, a channel model is built and an equalization is conducted to map between the received CSI amplitude and ZigBee transmission power based on the predefined sequence. The ZigBee transmitter confirms the ACK by sending $P_{\min}$ and $P_{\max}$. The number of elements within the array of $A(i)$ or N defines the number of symbols available for communication. The rate of change between the power modulation values provides initial phase information. Therefore, higher sensitivity WiFi receivers and ZigBee transmitters with more gain states have more symbols, thus yielding a higher bit rate.

Let P_0 be the minimum power needed for receivers to sense each other, and P_N be values that saturate. A handshake protocol will determine the values from P_0 to P_N by transmitting a series of incrementing values. The number of steps (N) is between 0 to N which determines the number of symbols for each modulation type. Therefore, we can describe N modulation symbol states using the following equation.

$$N \propto \frac{P \cdot G}{R^2 \cdot f}, \quad (10)$$

where, P is transmission power, G is digital gain and number of digitizer bits, R is distance between transmitters, and f is frequency. The intuition is that the higher N value, the more symbol states and the higher the throughput.

Phase Synchronization: 4QAM-OFDM is used to embed Z2W data in power levels that require phase synchronization to discriminate between each symbol. In our design, we maintain phase states for each symbol and account for clock drifts of the transmitter and receiver. During the handshaking protocol, the intervals between each power level measurement $\theta(t)$

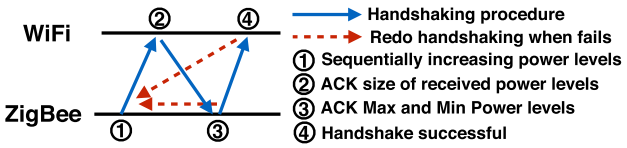
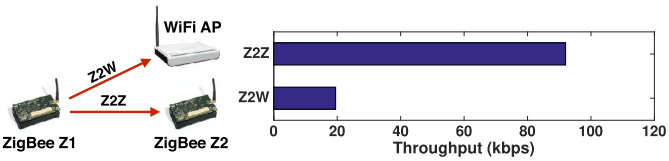


Fig. 7. Handshaking Process.



(a) Experiment Setup (b) **Experiment Results**

Fig. 8. Concurrent communications of Z2Z and Z2W.

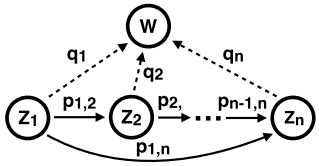


Fig. 9. Network Model.

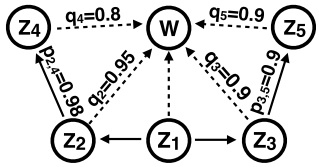


Fig. 10. EDW Example.

provides timing information that defines phase $\phi(t)$.

$$\phi(t) = \theta_{i+1}(t) - \theta_i(t). \tag{11}$$

We perform the subtraction on all the handshaking values and obtain a rate of phase change.

The process of the handshaking is shown in Figure 7. Firstly, when the communication is being established, the ZigBee transmitter provides the phase state by increasing the power levels sequentially so that modulation requiring quadrature states can be synchronized. Secondly, the WiFi receiver acknowledges ZigBee (by using WiFi to ZigBee technique such as WeBee [3]) the received maximum and minimum power levels. Finally, if the sequence is not completely detected, the acknowledgement will contain an error message to invalidate and redo the handshake.

IV. Forwarding Protocol

Current multi-hop ZigBee networks are not very efficient. Especially in a large network, the uplink experiences more transmissions, retransmissions, and longer delay. We propose to utilize the extra ZigBee-to-WiFi (Z2W) link provided by the physical layer (as introduced in Section III) to boost the sensing data uploading. Our approach deals with the uplink and downlink traffic together by taking the Z2W link into account to minimize the total number of transmissions in the network. While uploading sensing data to the gateway via Z2W link, the ZigBee devices can simultaneously disseminate control messages to the whole network, exchange networking maintenance information, or pass actuator's data to individual devices. This bi-directional communication concept provides a more efficient solution for overlapped heterogeneous networks.

In the previous sections, we showed how ZigBee devices convey data to the WiFi AP while concurrently communicating with other ZigBee devices. To demonstrate this scheme, we conduct an experiment with the setup shown in Figure 8(a) yielding results in Figure 8(b). ZigBee device Z_1 communicates to another ZigBee device Z_2 at 90kbps while concurrently communicating to the WiFi AP at 20kbps. Since different Z2Z and Z2W links suffer different fading and interference, the nodes have various packet reception rate (PRR). To utilize this unique feature of concurrent communications, we propose a new metric to measure the link quality of the heterogeneous communication and design a forwarding protocol for ZigBee networks.

A. EDW Metric

To reduce the number of transmissions and improve the throughput, we need a metric to measure the quality of different links and determine the forwarding scheme. Although routing metrics (such as ETX [4] and cETX [5]) described the link quality between sender and receiver then find the best forwarding route based on the link quality, these metrics are not able to support heterogeneous links (i.e., Z2Z and Z2W links) that these links i) have different throughput capabilities; ii) have totally different link quality because the receivers have different radios (e.g., WiFi or ZigBee). To better utilize the concurrent communication features, we propose a new metric: **expected delivery to WiFi (EDW)**. The basic idea is to use EDW to measure the "link quality" among heterogeneous devices and determine the route (e.g., forwarding to next ZigBee or upload to WiFi). Figure 9 shows the network model of concurrent communication, where Z_i ($i \in [1, n]$) is a ZigBee device and W is a WiFi device. q_i and $p_{i,j}$ are the PRR from Z_i to W and from Z_i to Z_j, respectively. EDW describes the combined neighbor's expected delivery rate of Z2W link (Z_i to W) and Z2Z link (Z_i to Z_j). Therefore, each potential forwarder can calculate the EDW to decide whether it should forward the received packets for its neighbor or not. The EDW is calculated as follows:

$$EDW_{Z_i,Z_j} = R_d q_i + R_d(1 - R_d) q_j p_{i,j}, \tag{12}$$

where R_d is the throughput ratio between link Z2W and Z2Z. We show a simple example in Figure 10. In the example, Z_2 and Z_3 are potential neighboring forwarders of Z_1. Equation 12 yields $EDW_{Z_2,Z_4} > EDW_{Z_3,Z_5}$. Therefore, Z_2 is a better forwarder of Z_1.

B. Forwarding Procedure

In the last section, we introduced the metric EDW to characterize our concurrent communication system. In this section, we present the Amphista forwarding protocol that

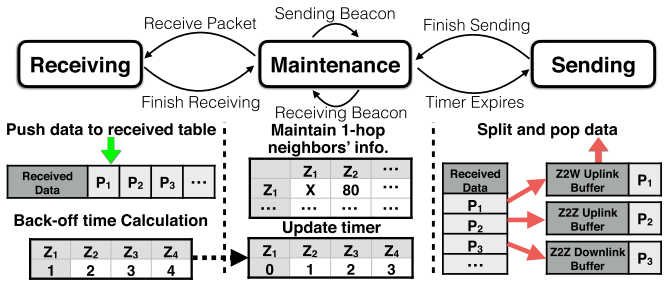


Fig. 11. State Machine Diagram of the forwarding protocol.

enables efficient concurrent uplink and downlink communications across heterogeneous IoT devices. The goal of this protocol is to minimize the number of transmissions for concurrent data uploading and dissemination tasks in IoT networks. A state machine diagram running in the ZigBee device is shown in Figure 11. Specifically, a ZigBee device is in one of three states at any time: (i) maintenance, (ii) sending, and (iii) receiving. Transitions between the states are triggered by events. In the rest of this section, we explain the operations in each state in details.

1) Maintenance State: After a ZigBee device is turned on, the device enters the maintenance state. The main purpose of maintenance state is to i) update the PRR of 1-hop Z2Z ($p_{i,j}$) and Z2W (q_i) communications; ii) calculate EDW; and iii) update the status table of received packets to decide whether to forward them or not. The throughput ratio R_d can be obtained by ACK from the WiFi device and neighboring ZigBee devices with zero overhead. To update the PRR, each ZigBee device will periodically send out small probe packets. To minimize overhead, our system only requires 1-hop neighbors' information. Another task in maintenance state is to update the timer that is set in receiving state to minimize the redundant transmissions. Once the timer of any packet expires, the device enters the sending state to decide how to send the packets through Z2Z and Z2W communications. Additionally, the new uplink and downlink requests will also be updated in maintenance state.

2) Receiving State: When a ZigBee device receives a data packet, the device enters the receiving state and adds a new entry in the received data table for the received data. The received data table contains the status of each received data. For each entry of the table, it contains the data ID, data destination and the back-off time to forward the data. Since the data is broadcasting in the ZigBee network, if a device receives a new data, there will be other ZigBee devices that can also receive the data. To minimize the redundant transmissions, each device will set a back-off time to forward the received data. The detailed design of back-off time will be discussed in Section IV-B.4. If the device receives redundant uplink data, which means that another device with shorter back-off time uploads the uplink data. Then, the back-off time of the data will be updated as infinity so that the data will not be forwarded anymore.

3) Sending State: When a device has data packets in the received data table, it enters the sending state. In this state, it selects packets to send through Z2W uplink, Z2Z uplink and downlink to minimize the overall number of transmissions in the network. The key idea is to apply concurrent Z2Z downlink and Z2W uplink communication first because its aggregated throughput is higher, and apply concurrent Z2Z and Z2W uplink communication when there are extra uplink packets after concurrent Z2Z downlink and Z2W uplink communication. Specifically, the number of packets to send through Z2W uplink (P_{AP}), Z2Z uplink (P_U) and downlink (P_D) can be calculated as:

$$P_{AP} = \begin{cases} N_U, & \text{if } \frac{N_U}{N_D} \leq \frac{U_{AP}}{D} \\ N_U - \frac{N_D U_{AP} U}{D(U_{AP}+U)}, & \text{otherwise} \end{cases} \tag{13}$$

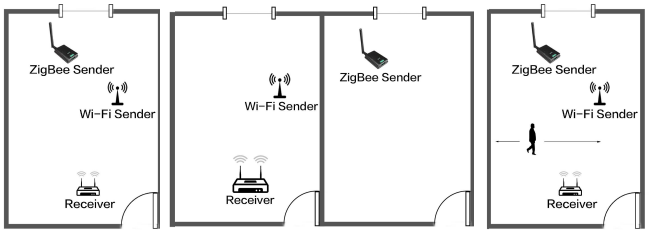
$$P_U = \begin{cases} 0, & \text{if } \frac{N_U}{N_D} \leq \frac{U_{AP}}{D} \\ (N_U - \frac{N_D U_{AP}}{D})\frac{U}{U_{AP}+U}, & \text{otherwise} \end{cases} \tag{14}$$

$$P_D = \begin{cases} N_D, & \text{if } \frac{N_U}{N_D} \geq \frac{U_{AP}}{D} \\ \frac{N_U D}{U_{AP}}, & \text{otherwise} \end{cases} \tag{15}$$

where N_U and N_D are the number of uplink and downlink packets that are ready to send based on the packet table. U_{AP}, U and D are the Z2W uplink throughput, minimum uplink Z2W throughput of device's neighbors and maximum downlink Z2Z throughput of device's neighbors. These parameters are firstly obtained during the initial state by transmitting probe packets. The probe packets are utilized to i) calculate the packet reception ratio for Equation 12; and ii) transmit the information like U_{AP}, U, and D to the neighboring devices. To deal with the dynamics, each device maintains an 1-hop neighbors' information table and updates the table with the latest neighbors' information, where the packet reception ratios are calculated after each transmission. U_{AP}, U, and D are periodically embedded in the packets.

4) Back-off Timer Design: As introduced in Section IV-B.2, since the forwarding decision is made in a distributed manner, the back-off timer is applied to reduce both the redundant uplink and downlink transmissions, and guarantee the downlink packets will be sent out to all the ZigBee devices. At a specific time while the potential forwarder receives packets from its neighbors, every forwarder calculates the priority parameter (PP) according to i) the EDW value and ii) the data size of uplink and downlink. We can divide it into three conditions to calculate the PP:

- $\mathbf{P_D = 0, P_U > 0}$**:** In this case, each device Z_i calculates all the EDW between all neighbors and pick the maximum one as PP (where $PP = \max_{j\in[1,n], j\neq i} EDW_{Z_i,Z_j}$).
- $\mathbf{P_D > 0, P_U > 0}$**:** When the forwarder has both the uplink and downlink packets in the buffer, generally, it has higher priority to forward neighbor's packets because when performing the downlink transmission, the uplink data can be sent directly to WiFi through Z2W link to eliminate uplink Z2Z transmissions. In this condition, $PP = \sum p_{i,j} + q_i$.
- $\mathbf{P_D > 0, P_U = 0}$**:** In this case, the network system cannot utilize the Z2W link to improve the performance. However,



(a) LoS (b) NLoS (c) w/ Human

Fig. 12. Three indoor experiment scenarios.

the devices can still use Z2W link to exchange control messages in order to reduce the overhead.

When a ZigBee device calculates the PP, it updates its back-off timer based on the PP value. Intuitively, the higher the PP value, the smaller the back-off timer should be because we always select the forwarder which can reduce the overall number of transmissions.

V. Experimental Evaluation

We extensively evaluated our Amphista system in an academic building, which has a lot of other WiFi access points that create interference.

A. Experimental Setup

In the experiment, in order to have the flexibility to implement our design and obtain lower level data (such as PHY throughput and BER), we implemented the WiFi system (including WiFi sender and receiver) by using USRP devices. For ZigBee devices, we used off-the-shelf TelosB nodes. We deployed the system in the following three distinct scenarios:

- **Line-of-Sight (LoS):** As shown in Figure 12(a), the sender and the receiver were within Line of Sight at distances of 0.5, 3, and 10 meters.
- **None-Line-of-Sight (NLoS):** As shown in Figure 12(b), the sender and the receiver were in different rooms with distances of 4, 7, and 10 meters.
- **Human Interference:** As shown in Figure 12(c), a person was in the middle of the sender and the receiver.
- **Mobile Scenarios:** A person was walking with a device in the pocket or on the wrist.

B. Comparison With TDMA and CSMA

To examine the efficiency of Amphista, we compared it with two traditional MAC schemes: CSMA and TDMA. We conducted an experiment by using a pair of WiFi devices and 4 pairs of ZigBee devices. Each pair consists of two devices communicating with each other. In CSMA and TDMA, we utilized a multi-radio gateway that is equipped with both ZigBee and WiFi radios. We use the following four metrics: i) **packet reception rate (PRR)**: the number of packets received divided by the total number of packets transmitted; ii) **power efficiency**: the amount of energy required to transmit a bit; iii) **spectrum efficiency**: the amount of bandwidth required to transmit a bit; and iv) **throughput**: total number of bits transmitted per second.

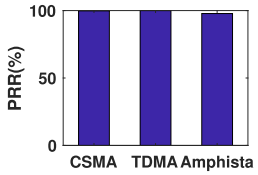


Fig. 13. Packet Reception Rate (PRR).

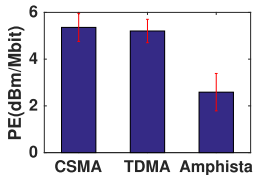


Fig. 14. Power Efficiency (PE).

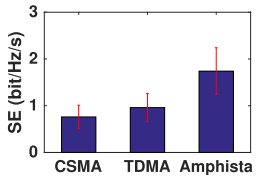


Fig. 15. Spectrum Efficiency (SE).

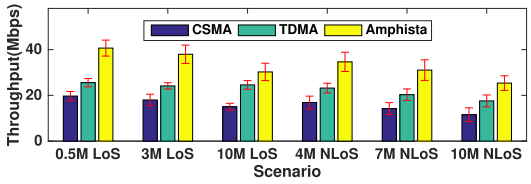
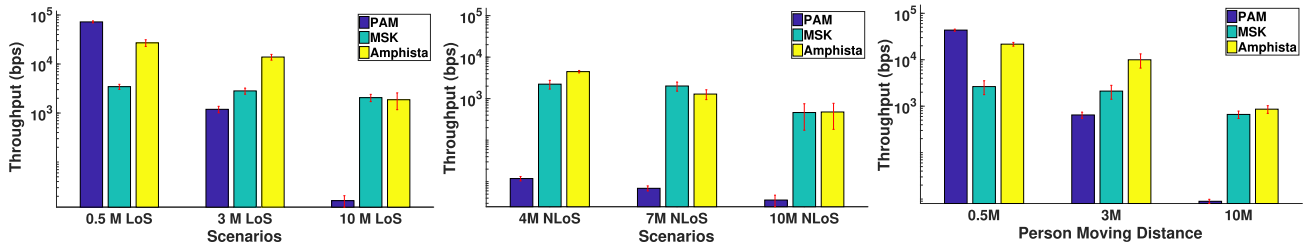


Fig. 16. Throughput.

As shown in Figure 13, the PRR of Amphista is as high as CSMA or TDMA, however, Amphista only needs 2.59 dBm to transmit 1 Megabit data comparing to 5.36 dBm/Mbit and 5.2 dBm/Mbit of CSMA and TDMA, respectively (see Figure 14). Moreover, Amphista's spectrum efficiency is 2.29 times as high as the popular CSMA scheme (see Figure 15). The error bar shows the variance across different scenarios (LoS or NLoS) and communication distances. Furthermore, as shown in Figure 16, Amphista's throughput is around **two times** as high as CSMA in different scenarios. This is because by using CSMA or TDMA, ZigBee and WiFi devices are competing for accessing the overlapped channel. When the ZigBee device is transmitting, the WiFi device will avoid collisions. Since the ZigBee device uses only 2 MHz bandwidth, compared with 20 MHz bandwidth of WiFi, the major part of the spectrum is wasted, which results the overall performance decreases. However, since Amphista enables concurrent W2W, Z2Z, and Z2W communications, ZigBee and WiFi can concurrently communicate to the gateway.

C. Z2W's Performance

In Section III-A, we proposed a discrete 4QAM-OFDM signal on top of the ZigBee's transmission power to encode the



(a) LoS (b) NLoS (c) Human Interference

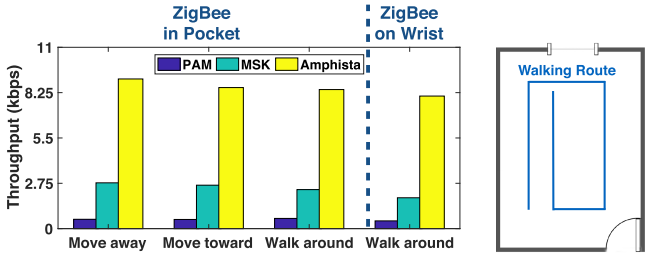
Fig. 17. Z2W Throughput.

ZigBee-to-WiFi (Z2W) message. This OFDM signal is different from traditional analog OFDM signals, where DAC, sampling, and ADC are not needed. By doing this, we can achieve considerable throughput with better anti-interference capability (when compared with PAM and MSK). Moreover, since one WiFi channel is overlapped with up to four ZigBee channels, the gateway can receive four concurrent ZigBee transmissions. In this section, to demonstrate Amphista's maximum capacity of Z2W communication, we first test the system in a controlled environment (i.e., line-of-sight, minimum noise and interference). We report the aggregated throughput for four concurrent Z2W transmissions because one WiFi channel can cover up to four ZigBee channels (as described in the introduction section). Secondly, to understand the performance of Amphista in less controlled conditions, we evaluated the system in three different scenarios: non-line-of-sight, human interference, and mobile scenarios. Finally, to make a fair comparison with the latest cross-technology communication (CTC) techniques, we also conducted the experiments in a similar setup as stated in other's works [6]–[9].

1) Line-of-Sight: The result is shown in Figure 17(a). When the distance between the WiFi and ZigBee devices increase, the signal strength decreases causing loss of WiFi sampling fidelity. We conclude that although, PAM provides 10 times better throughput, as distance increases in real world, the throughput drops exponentially which is not usable. MSK and Amphista have a relative stable performance over distance while Amphista has better throughput than MSK. The highest throughput of OFDM is 27 kbps.

2) Non-Line-of-Sight: In NLoS (see Figure 17(b)), RF signal experience diffraction, reflection, and increased fading contributing to increased multipath interference. Because of increased multipath interference, the transmission between WiFi and ZigBee contains more distortions lowering sampling fidelity. PAM cannot recover from the increased multipath interference and thus perform 100 times worse. The throughput of MSK and Amphista remain the same as expected. By embedding information in phase, MSK and OFDM modulations provide robustness against multipath and sampling fidelity loss. The highest throughput of Amphista in NLoS is 4.5 kbps at 4 meters.

3) Human Interference: Human movement introduces Doppler effect, which causes frequency shifts and thus these the received signal is distorted. At a short distance, PAM remains relatively unaffected due to the higher signal strength from the unaffected signals (see Figure 17(c)). As the distance



(a) Throughput (b) Route

Fig. 18. The performance of ZigBee to WiFi communication in four different mobile scenarios. The throughput error ranged about 15-20% which means our modulation schemes remain robust and against fading caused by human movement.

increases, PAM decreases exponentially while MSK and Amphista decrease linearly. Amphista performs 7 times better in the medium distance and equivalently in long distance. Based on these results, we conclude that Amphista is robust under human interference.

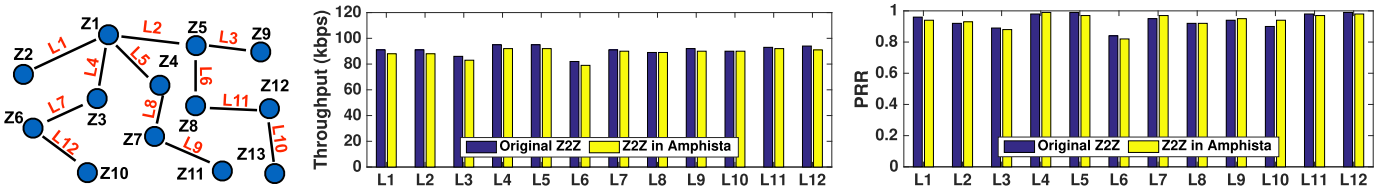
4) Mobile Scenarios: In this experiment, we evaluated the throughput (results shown in Figure 18(a)) by attaching the ZigBee device to the human body in four different mobile scenarios: i) walking toward the WiFi receiver with the ZigBee device in a pocket; ii) walking away from the WiFi receiver with the ZigBee device in a pocket; iii) walking around the office with the ZigBee device in pocket; and iv) walking around the office with the ZigBee device on wrist. The route in scenarios iii) and iv) is shown in Figure 18(b). The results show that the throughput remained stable during each scenario. The throughput error ranged about 15-20%. The phase-based modulation remains robust against fading caused by the human movements.

D. Comparison With the Latest CTC Techniques

The results (Table II) show that our design is up to 2 orders of magnitude better than the state-of-the-art approaches. This is because we i) adopt 4QAM-OFDM modulation scheme to increase the spectrum efficiency and ii) designed the handshaking protocol to minimize interference between WiFi and ZigBee devices.

E. Impact to Z2Z Communication

To evaluate the impact of concurrent communication to the original ZigBee to ZigBee (Z2Z) traffic, we deployed thirteen ZigBee devices in a tree topology (shown in Figure 19(a)).



(a) Topology (b) Throughput (c) PRR

Fig. 19. Impact to ZigBee Network is negligible in terms of throughput and packet reception rate.

TABLE II

COMPARED WITH THE LATEST APPROACHES, AMPHISTA INCREASES THROUGHPUT BY MORE THAN 170X, 20X, 10X, AND 11X, RESPECTIVELY

Approach	Amphista	FreeBee[6]	EMF[7]	C-mose[8]	ZigFi[9]
Throughput	2,500bps	14bps	120bps	215bps	215.9bps

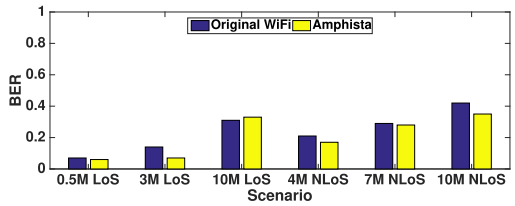


Fig. 20. Impact to WiFi to WiFi communication is negligible.

The comparison results of throughput and PRR are shown in Figure 19(b) and Figure 19(c), respectively. Overall, impact of concurrent communication to the original Z2Z traffic is negligible. The largest difference occurs on link $L5$ (i.e., the link between device $Z1$ and $Z4$), where the Z2Z throughput is only reduced by 3 kbps (or 2%) when Amphista is enabled. This is because ZigBee uses direct sequence spread spectrum (DSSS) to improve protection against interference and noise.

F. Impact to W2W Communication

We evaluated the impact of Amphista's concurrent communication to the original WiFi to WiFi (W2W) communication. Figure 20 shows the BER of WiFi to WiFi communication with and without Amphista. We can observe that the BER are under 0.5% in both scenarios. Moreover, there is negligible difference between original W2W communication and Amphista interfered W2W communication. This result demonstrates the effectiveness of our Amphista design and also explains why Amphista achieves higher power efficiency, spectrum efficiency, and throughput than CSMA and TDMA in Figures 13 to 16.

G. Performance of Handshaking

In this section, we demonstrate the effectiveness of our handshaking scheme (introduced in Section III-C) under the human interference. In our experiment, up to 3 people walked inside the room to create interference. As shown in Figure 21, with more interference (generated by individual persons), less symbol states can be used. Specifically, when there is no person interference, half of the handshaking success in 32 symbol states; when there is 1 person interference, more than half can use 8 or 16 symbol states; when there are 3 persons, most of the handshaking is in 2 symbol states.

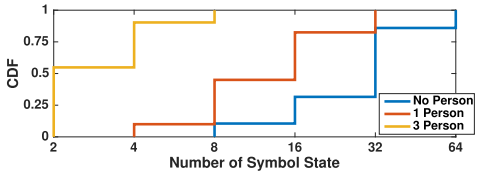


Fig. 21. CDF of the handshaking protocol during three scenarios: 0 person, 1 person, and 3 persons walking around in the room.

H. Network Layer Evaluation

In this section, we evaluate the network layer design of Amphista. The system is deployed in a 33 ft x 33 ft square area. Each sensing node is deployed and randomly assigned to one of the four channels that are overlapped with the WiFi channel. The gateway is positioned in the center of the deployment field. When the system is on, each ZigBee device sends the data packets (with payload from 1 Byte to 10 Bytes) towards the gateway as uplink; while the gateway also disseminates the data from the gateway to all the ZigBee devices as downlink. The throughput of Z2W and Z2Z links follows the empirical results from Section V-C.1. The **metrics** below are used to evaluate the network performance: i) **Packet delivery delay of downlink:** The aggregated throughput in the network divided by number of transmissions. ii) **Average uplink throughput:** The aggregated uplink throughput in the whole network divided by the number of uplink transmissions. iii) **Number of transmissions:** The total transmission number for a certain amount of data in a network.

To verify the effectiveness of our forwarding protocol, we compare our design with the baseline that does not utilize the unique feature of concurrent Z2W and Z2Z communications.

Baseline: For each ZigBee device in baseline, it has the same throughput of Z2W and Z2Z communications, however, it can only conduct either Z2W or Z2Z communication at a time.

We also compared the performance of Amphista with exiting routing metrics ETX [4] and our EDW (introduced in Section IV-A).

We evaluate the scalability of the IoT network by increasing the number of nodes from 50 to 400. For the uplink throughput (shown in Figure 22), when the device number is small, Amphista with ETX and EDW are similar to baseline. However, when the number increases, both Amphista approaches

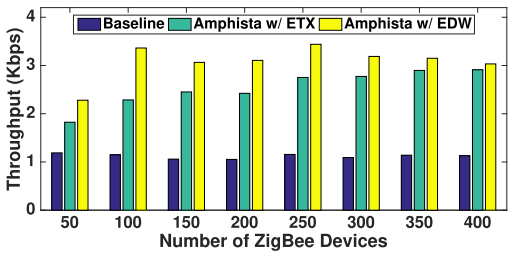


Fig. 22. Average Throughput (Uplink).

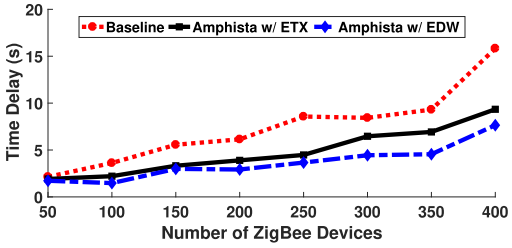


Fig. 23. Packet Delivery Delay (Downlink).

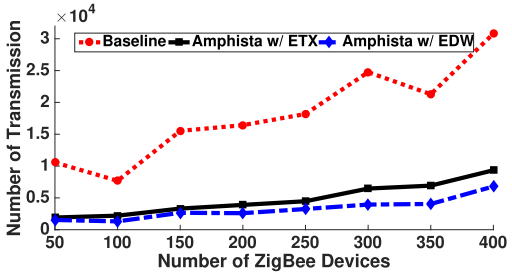
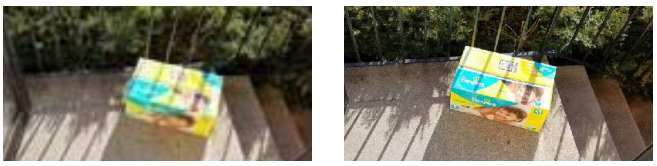


Fig. 24. Number of Transmissions.

show an increasing trend while the baseline keeps the same. This is because when there are more nodes in the network, the conflict between uplink and downlink will be more severe for baseline approach but the Amphista approachs' performance increases due to the bi-directional communications. By comparing two Amphista approaches, the one with EDW has higher throughput than with ETX because EDW metric takes the heterogeneous links (i.e., Z2Z and Z2W links) into consideration. The average uplink throughput for Amphista with EDW is close to two time of the baseline. Meanwhile, the time delay of downlink in Amphista with EDW is less than 40% than of the baseline (Figure 23) because less amount of retransmission is needed for Apmhista approach comparing with baseline approach. For the number of total transmissions in the network, our design is similar to baseline when there are only 50 nodes in the network while the number of transmissions in our design is 70% less than the number of transmission in the baseline when there are 400 nodes (Figure 24). This is because when there are more nodes in the network, the conflict between uplink and downlink will be more severe.

I. Evaluation Using a Real-World Application

We also demonstrate the effectiveness of our Amphista approach by using a real-world application in a smart home scenario. The WiFi based surveillance camera is coexisted



(a) Amphista disabled (b) Amphista enabled

Fig. 25. Comparison of surveillance camera's video quality. When Amphista is disabled, ZigBee's transmission may significantly reduce the surveillance camera's video quality and cause the face recognition failure (see Fig. 25(a)). When Amphista is enabled, the WiFi data and ZigBee data can be correctly received by the gateway simultaneously. Therefore, we can still correctly recognize the face in Fig. 25(b).

with multiple ZigBee devices (e.g., motion detectors, temperature and humidity sensors, water leak detection sensors, smoke & CO sensors, and etc). Figure 25 shows the wireless camera video quality comparison between Amphista is disabled and enabled. We note that when Amphista is disabled (Figure 25(a)), the video quality is low because the ZigBee traffic affects WiFi's transmission such that the camera is adaptively switched to a lower resolution mode. When Amphista is enabled (Figure 25(b)), since the WiFi packets can be received simultaneously with ZigBee packets at the gateway side, the video is streaming at a higher resolution to ensure the applications such as face recognition, which is critical for security and surveillance purpose.

VI. Related Work

To utilize the coexistent features of different wireless technologies within the same frequency band, researchers have proposed different technologies [10]–[13], including the CTC techniques [7]–[9], [14]–[22] which enable direct communications between WiFi and ZigBee by modify PHY or link layers parameters. BlueBee [23] and B^2W^2 [24] achieve the BLE to ZigBee and BLE to WiFi communications, respectively. [20] and [25] manipulates the PHY layer symbols to communicate between WiFi and ZigBee by using customized radios. WEBee [3] enables WiFi to ZigBee communication by using WiFi signals to emulate ZigBee signals. However, WEBee cannot enable ZigBee to WiFi communication, which is one of the novelties of this paper. Therefore, WEBee is complementary to our system.

Researchers have also proposed various techniques to improve the spectrum utilization and the performance of different wireless systems [26]–[32]. Due to the increasingly crowded 2.4 GHz ISM band, significant amount of work has been conducted to improve its spectrum utilization [33]–[36]. To further improve the performance of wireless communication, researchers have proposed various interference mitigate techniques [37], [38] and collision avoidance solutions [39]–[41].

Instead of avoiding collisions or mitigating interference, our work investigates whether it is possible to leverage the interference for concurrent communication. Our Amphista leverages the Channel State Information, which is available in several commercial devices [38], [42], for embedding ZigBee devices' messages into WiFi packets. We note that CSI has been utilized in various ways such as detecting RF interference [43], improving MIMO communication systems [35],

[44], [45], human activity recognition [46]–[48] and indoor localization [49], [50]. However, no one has utilized CSI to enable *concurrent* uplink and downlink data forwarding.

Different from the above approaches that focus on physical layer design, our approach is a cross-layer design that explores the cross-technology communication's unique feature for simultaneous uplink and downlink data forwarding using a single ZigBee data stream.

VII. Conclusion & Future Work

To facilitate edge computing with the exponentially increasing number of IoT devices and the huge amount of data generated by these devices, we propose a novel design – Amphista, which can achieve simultaneous uplink and downlink communications and data forwarding with a single ZigBee data stream. Compared with existing approaches, Amphista significantly improves throughput and reduces the latency. By applying the noise cancellation and equalization techniques, our experiments also demonstrate that Amphista has a negligible impact on the original WiFi-to-WiFi communication. Our design is compliant with WiFi and ZigBee standards. It can be deployed on commodity ZigBee devices to achieve simultaneous uplink and downlink communications and data forwarding with negligible impact to the on-going WiFi traffic. For future work, we plan to deploy Amphista on commodity WiFi devices. One way is to utilize the full CSI feature provided by some WiFi drivers (e.g., Intel 5300 NIC [51]). Another way is to utilize limited but widely available CSI amplitude information provided by WiFi drivers (e.g., Atheros chipsets [52]).

References

[1] T. Nandagopal, "Wireless research at the NSF: Current investments and emerging priorities," Nat. Sci. Found., Alexandria, VA, USA, Tech. Rep., 2016. [Online]. Available: https://sites.google.com/site/thyagaresearch/videos

[2] C. Systems, "Cisco global cloud index: Forecast and methodology, 2014–2019 white paper," Cisco Syst., San Jose, CA, USA, Tech. Rep. FLGD 12624, 2014.

[3] Z. Li and T. He, "WEBee: Physical-layer cross-technology communication via emulation," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2017, pp. 2–14.

[4] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Netw.*, vol. 11, no. 4, pp. 419–434, Jul. 2005.

[5] S. M. Kim, S. Wang, and T. He, "CETX: Incorporating spatiotemporal correlation for better wireless networking," in *Proc. 13th ACM Conf. Embedded Netw.Sensor Syst.*, Nov. 2015, pp. 323–336.

[6] S. M. Kim and T. He, "FreeBee: Cross-technology communication via free side-channel," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 317–330.

[7] 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 *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[8] Z. Yin, W. Jiang, S. M. Kim, and T. He, "C-morse: Cross-technology communication with transparent morse coding," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[9] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali, "ZIGFI: Harnessing channel state information for cross-technology communication," in *Proc. INFOCOM*, Apr. 2018, pp. 360–368.

[10] 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 Trans. Mobile Comput.*, vol. 13, no. 6, pp. 1379–1392, Jun. 2014.

[11] T. Jin, G. Noubir, and B. Sheng, "WiZi-cloud: Application-transparent dual ZigBee-WiFi radios for low power Internet access," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1593–1601.

[12] K. Chebrolu and A. Dhekne, "Esense: Communication through energy sensing," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. - MobiCom*, 2009, pp. 85–96.

[13] H. Sun, Z. Fang, Q. Liu, Z. Lu, and T. Zhu, "Enabling LTE and WiFi coexisting in 5 GHz for efficient spectrum utilization," *J. Comput. Netw. Commun.*, vol. 2017, pp. 1–17, Feb. 2017.

[14] W. Jiang, Z. Yin, S. M. Kim, and T. He, "Transparent cross-technology communication over data traffic," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[15] X. Guo, X. Zheng, and Y. He, "WiZig: Cross-technology energy communication over a noisy channel," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. .

[16] Y. Chae, S. Wang, and S. M. Kim, "Exploiting WiFi guard band for safeguarded ZigBee," in *Proc. 16th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2018, pp. .

[17] S. Wang, S. M. Kim, and T. He, "Symbol-level cross-technology communication via payload encoding," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. .

[18] W. Wang, T. Xie, X. Liu, and T. Zhu, "ECT: Exploiting cross-technology concurrent transmission for reducing packet delivery delay in IoT networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2018, pp. .

[19] Z. Chi, Y. Li, H. Sun, Y. Yao, and T. Zhu, "Concurrent cross-technology communication among heterogeneous IoT devices," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 932–947, Jun. 2019.

[20] Z. Chi, Y. Li, Y. Yao, and T. Zhu, "PMC: Parallel multi-protocol communication to heterogeneous IoT radios within a single WiFi channel," in *Proc. IEEE 25th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2017, pp. .

[21] W. Wang, X. Liu, Y. Yao, Y. Pan, Z. Chi, and T. Zhu, "CRF: Coexistent routing and flooding using WiFi packets in heterogeneous IoT networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2019, pp. 19–27.

[22] Z. Chi, Y. Li, X. Liu, Y. Yao, Y. Zhang, and T. Zhu, "Parallel inclusive communication for connecting heterogeneous IoT devices at the edge," in *Proc. 17th Conf. Embedded Netw. Sensor Syst.*, Nov. 2019, pp. 205–218, doi: 10.1145/3356250.3360046.

[23] W. Jiang, Z. Yin, R. Liu, Z. Li, S. M. Kim, and T. He, "BlueBee: A 10,000x faster cross-technology communication via PHY emulation," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2017, pp. 1–13.

[24] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2W2: N-Way concurrent communication for IoT devices," in *Proc. 14th ACM Conf. Embedded Netw. Sensor Syst. CD-ROM*, Nov. 2016, pp. 245–258.

[25] Y. Li, Z. Chi, X. Liu, and T. Zhu, "Chiron: Concurrent high throughput communication for IoT devices," in *Proc. 16th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2018, pp. 204–216.

[26] D. Halperin, S. Kandula, J. Padhye, P. Bahl, and D. Wetherall, "Augmenting data center networks with multi-gigabit wireless links," in *Proc. ACM SIGCOMM Conf. SIGCOMM - SIGCOMM*, 2011, pp. 38–49.

[27] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with Wi-Fi like connectivity," in *Proc. ACM SIGCOMM Conf. Data Commun. (SIGCOMM)*, 2009, pp. 27–38.

[28] T. Zhu, Z. Zhong, T. He, and Z.-L. Zhang, "Exploring link correlation for efficient flooding in wireless sensor networks," in *Proc. 7th USENIX Conf. Netw. Syst. Design Implement.*, 2010, p. 4.

[29] J. Jun, L. Cheng, L. He, Y. Gu, and T. Zhu, "Exploiting sender-based link correlation in wireless sensor networks," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols*, Oct. 2014, pp. 445–455.

[30] Z. Chi, T. Zhu, D. Jiang, and P. Yi, "A survey of side-channel sensing in wireless networked systems," *J. Commun. Technol., Electron. Comput. Sci.*, vol. 3, p. 32, Dec. 2015.

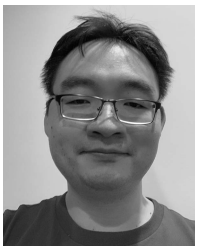
[31] S. Guo, S. M. Kim, T. Zhu, Y. Gu, and T. He, "Correlated flooding in low-duty-cycle wireless sensor networks," in *Proc. 19th IEEE Int. Conf. Netw. Protocols*, Oct. 2011, pp. 383–392.

[32] F. Chai, T. Zhu, and K.-D. Kang, "A link-correlation-aware cross-layer protocol for IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[33] S. Yun, D. Kim, and L. Qiu, "Fine-grained spectrum adaptation in WiFi networks," in *Proc. 19th Annu. Int. Conf. Mobile Comput. Netw. - MobiCom*, 2013, pp. 327–338.

[34] J. Zhang, H. Shen, K. Tan, R. Chandra, Y. Zhang, and Q. Zhang, "Frame retransmissions considered harmful: Improving spectrum efficiency using micro-ACKs," in *Proc. 18th Annu. Int. Conf. Mobile Comput. Netw. - Mobicom*, 2012, pp. 89–100.
[35] S. Kumar, D. Cifuentes, S. Gollakota, and D. Katabi, "Bringing cross-layer MIMO to today's wireless LANs," in *Proc. ACM SIGCOMM Conf. SIGCOMM*, Aug. 2013, pp. 387–398.
[36] K. Chintalapudi *et al.*, "Wifi-nc: Wifi over narrow channels," in *Proc. NSDI*, 2012, pp. 43–56.
[37] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. - SIGCOMM*, 2007, pp. 385–396.
[38] S. Sen, J. Lee, K.-H. Kim, and P. Congdon, "Avoiding multipath to revive inbuilding WiFi localization," in *Proc. 11th Annu. Int. Conf. Mobile Syst., Appl., Services - MobiSys*, 2013, pp. 249–262.
[39] S. Sen, R. Roy 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.
[40] T. Nandagopal, T.-E. Kim, X. Gao, and V. Bharghavan, "Achieving MAC layer fairness in wireless packet networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. - MobiCom*, 2000, pp. 87–98.
[41] Z. Chi *et al.*, "Countering cross-technology jamming attack," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, pp. 99–110, doi: 10.1145/3395351.3399367.
[42] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, p. 53, Jan. 2011, doi: 10.1145/3395351.3399367.
[43] Y. Zheng, C. Wu, K. Qian, Z. Yang, and Y. Liu, "Detecting radio frequency interference for CSI measurements on COTS WiFi devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[44] C. Shepard, A. Javed, and L. Zhong, "Control channel design for many-antenna MU-MIMO," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 578–591, doi: 10.1145/2789168.2790120.
[45] X. Xie, E. Chai, X. Zhang, K. Sundaresan, A. Khojastepour, and S. Rangarajan, "Hekaton: Efficient and practical large-scale MIMO," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 304–316, doi: 10.1145/2789168.2790116.
[46] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with Wi-Fi," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2014, pp. 1–12, doi: 10.1145/2639108.2639112.
[47] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: Device-free location-oriented activity identification using fine-grained WiFi signatures," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2014, pp. 617–628, doi: 10.1145/2639108.2639143.
[48] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2014, pp. 237–248, doi: 10.1145/2639108.2639111.
[49] J. Xiong, K. Sundaresan, and K. Jamieson, "ToneTrack: Leveraging frequency-agile radios for time-based indoor wireless localization," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 537–549, doi: 10.1145/2789168.2790125.
[50] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter level localization using WiFi," in *Proc. ACM Conf. Special Interest Group Data Commun.*, Aug. 2015, pp. 269–282, doi: 10.1145/2785956.2787487.
[51] *Linux 802.11n CSI Tool*. Accessed: Jan. 6, 2017. [Online]. Available: https://dhalperi.github.io/linux-80211n-csitool/
[52] *Existing Linux Wireless Drivers*. Accessed: Jan. 6, 2017. [Online]. Available: https://wireless.wiki.kernel.org/en/users/drivers/ath9k/

Zicheng Chi (Member, IEEE) received the B.S. degree from Lanzhou University, the M.S. degree from the South China University of Technology, and the Ph.D. degree from the University of Maryland, Baltimore County. He is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, Cleveland State University. He is the author and coauthor of over 20 articles in premier journals and conferences. His research interests include wireless communication, wireless sensing, cyber-physical systems, and the Internet-of-Things.



Yan Li (Member, IEEE) received the B.S. degree from Virginia Tech, the M.S. degree from Johns Hopkins, and the M.S. and Ph.D. degrees from the University of Maryland, Baltimore County (UMBC). He is currently a Researcher with the Johns Hopkins Applied Physics Laboratory. His research interests include wireless communication, RF engineering, machine learning, sensing, IoTs, signal processing, and biomedical applications and security.

Hongyu Sun (Member, IEEE) received the Ph.D. degree from Jilin University, Changchun, China, in 2017. From January 2015 to September 2016, she was a Visiting Scholar with the University of Maryland, Baltimore County. She is currently an Assistant Professor with Jilin Normal University. She has published over 20 articles in SCI/EI international conference proceedings and journals. Her research interests include wireless communication and mobile computing, RF-based sensing, privacy, and security, and the Internet of Things (IoT).

Zhichuan Huang (Member, IEEE) received the Ph.D. degree in computer science from the University of Maryland, Baltimore County, in 2017. He is currently a Research Associate with the School of Data and Computer Science, Sun Yat-sen University. His research interests include big data analytics and IoT sensing and networking.

Ting Zhu (Senior Member, IEEE) received the Ph.D. degree from the University of Minnesota, Twin City, in 2010. He is currently an Associate Professor with the Department of Computer Science and Electrical Engineering, University of Maryland at Baltimore. He has authored or coauthored over 120 articles in premier journals and conferences. His research interests include cyber-physical systems, intelligent building systems, IoT, wireless networks, and mobile systems, which are supported by the NSF, Microsoft, and other agencies. He was a recipient of the NSF CAREER Award in 2017 and the CRA Computing Innovation Fellowship in 2010. He has received a number of research awards in the areas of energy efficient smart buildings, networking, and the Internet of Things (IoT). He has served on many program committees of premier conferences. He currently serves as an Editorial Board Member for three international journals.