# Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption

Yan Li*
Computer Science and Electrical Engineering, UMBC
liy1@umbc.edu

Zicheng Chi*
Computer Science and Electrical Engineering, UMBC
zicheng1@umbc.edu

Xin Liu
Computer Science and Electrical Engineering, UMBC
xinliu1@umbc.edu

Ting Zhu
Computer Science and Electrical Engineering, UMBC
zt@umbc.edu

## ABSTRACT

Within heterogenous IoT sensor networks, users of ZigBee devices expect long-lasting battery usage due to its ultra-low power and duty cycle. In IoT networks, to demonstrate even further ultra-low power consumption, we introduce Passive-ZigBee that demonstrates we can transform an existing productive WiFi signal into a ZigBee packet for a CoTS low-power consumption receiver while consuming 1,440 times lower power compared to traditional ZigBee. Moreover, this low power backscatter radio can bridge between the ZigBee and WiFi devices by relaying data allowing heterogenous radios to communicate with each other. We built a hardware prototype and implement these devices on a commodity ZigBee, WiFi, and an FPGA platform. Our experimental evaluation demonstrates the backscattered WiFi packets can be decoded by CoTS ZigBee receivers over a distance of 55 meters in none-line-of-sight and with human movements. Our Passive-ZigBee can consume only $25\mu W$ when transferring sensor data and relay ZigBee and WiFi data compared to traditional ZigBee (36mW). Our FPGA synthesis tool demonstrated the extremely low power consumption.

## CCS CONCEPTS

• **Computer systems organization** → **Sensor networks**; • **Hardware** → **Wireless devices**; Wireless integrated network sensors; • **Networks** → *Cross-layer protocols*;

## KEYWORDS

IoT, Heterogenous Networks, Backscatter

**ACM Reference Format:**
Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. 2018. Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption. In *The 16th ACM Conference on Embedded Networked Sensor Systems (SenSys '18), November 4–7, 2018, Shenzhen, China.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3274783.3274846

*Authors contributed equally to the paper



*SenSys '18, November 4–7, 2018, Shenzhen, China*

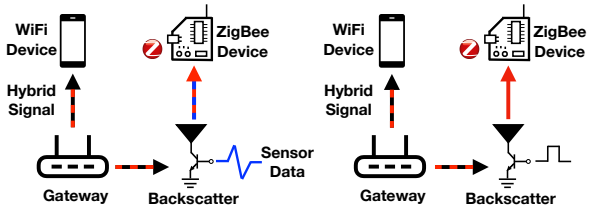
ACM ISBN 978-1-4503-5952-8/18/11…$15.00
https://doi.org/10.1145/3274783.3274846

## 1 INTRODUCTION

Gartner predicts that the Internet of Things (IoT) devices will increase to 20 billion by 2020 connecting all those devices (implanted or wearable health monitors, security locks, human trackers, etc) to the internet and each other. For these connected devices' battery to last more than 10 years or use energy harvesting technology, they must consume ultra-low power. Based on the low-power consumption needs of the IoT devices and widely-deployed existing WiFi radios infrastructure, we seek to ask: can we produce ultra-low power backscatter ZigBee devices that harvest energy from the deployed WiFi infrastructure? Traditional ZigBee offers a promising solution by consuming far less power than WiFi radios (36mW and 210 mW respectively). However, inspired by recently proposed backscatter designs, we seek to dramatically decrease power consumption. Unlike previous works, Passive-ZigBee is the first to achieve maximum standard-based network-throughput communication while harvesting energy from productive WiFi communication packets and thus consuming ultra-low energy.

We propose Passive-ZigBee, a novel backscatter communication that produces productive WiFi packets and transforms that packet to a commodity-compliant ZigBee packet instantaneously. Passive-ZigBee concurrently produces fully-compliant 802.11n WiFi and 802.15.4 ZigBee packets. We observe that WiFi devices are the most ubiquitous, dense, and powerful compared to other IoT devices. We argue that Passive-Zigee's devices require significantly lower power consumption due to 1) productive WiFi packets, 2) ultra-low power, simple, and inexpensive backscatter tags, and 3) low-power ZigBee listeners. Passive-ZigBee reuses existing WiFi and ZigBee devices thus encourages backscatter adoption. The resulting radios enable significantly longer battery life and energy harvesting devices in the sensor networks compared to a traditional ZigBee. Moreover, because of the simplistic tag design, these tags require a smaller footprint on the sensor's integrated chip. Thus, Passive-ZigBee provides a novel design for a lower-energy consumption sensor network.

In a nutshell, Passive-ZigBee 1) creates a hybrid ZigBee WiFi packet and 2) leverages backscatter to communicate to a listening ZigBee device operating in any of the industrial, scientific and medical (ISM) band. More specifically, as shown in figure 1, Passive-ZigBee operates in two modes: 1) utilizing productive WiFi to WiFi packets, low-power consumption backscatter radios transmit sensor data to listening ZigBee devices, and 2) enabling concurrent WiFi to WiFi and WiFi to ZigBee communications through a backscatter radio relay. The reason that Passive-ZigBee packets can be received




(a) Sensor (b) Relay

**Figure 1: System Overview**

by both ZigBee and WiFi devices at full network throughput is based on the observation that ZigBee spreads its energy enabling it to be robust against WiFi's multi-tone signals. While the hybrid packet does introduce higher interference levels, we find that the robustness of WiFi and ZigBee standards can recover from the introduced noise. Specifically, we make the following technical contributions:

- We design a novel Gateway to produce hybrid signals that contain concurrent ZigBee and WiFi symbols. We leverage the facts that 1) WiFi and ZigBee use vastly different Symbol and Chip rates (250 KHz and 2 MHz), and 2) 802.11n WiFi signal contains enough subcarriers such that all possible ZigBee symbols can be contained in a single WiFi packet. Thus this hybrid WiFi packet enables productive Gateway to commodity WiFi communications.
- We design a low-power and small-footprint backscatter radio that 1) receives the Gateway's hybrid packet and 2) backscatters the signal to a listening ZigBee device. We achieve this design by using a multiplier that shifts the incoming Gateway signal to different frequencies at the ZigBee symbol rate. By mapping and frequency-shifting the ZigBee symbols embedded in the wide-band WiFi, the backscatter can transmit sensor data in a customized packet to a commodity ZigBee device.
- We enable low-power consumption bridging in WiFi and ZigBee networks by embedding ZigBee to WiFi data in the hybrid gateway's packet for the backscatter to relay. We achieve this design by leveraging the inherent interference robustness built into the ZigBee and WiFi communication protocols.
- Through prototyping the hybrid gateway on both a software defined radio and a commodity radio and backscatter on an FPGA, Passive-ZigBee consumes 1,440 times less energy than traditional ZigBee transmitters according to our FPGA synthesis tool.

## 2 MOTIVATION

The increase of more than 20 billion mobile connects IoT devices that range from home automation controls to life-saving health-monitoring devices create demands for efficient energy usage. Thus, the goal of low-energy consumption, 10+ year battery life, and energy harvesting sensors and controller motivate our design to communicate to ZigBee devices. A sample application includes energy-harvesting ECG (Electrocardiogram), glucose, and Pulse-Oximetry sensors embedded in patients transmitting data to a wearable long-battery-life operated health monitor and drug delivery device which needs location and control data from a cloud server (Figure 2). The health device will only deliver drug at specific locations with certain vital sign levels and control information. Due to high-power and ubiquitous availability WiFi network, these WiFi signals are an ideal target for energy harvest in backscatter sensors and control information access.

**Limitation of Traditional ZigBee:** Current ZigBee devices operate by the generation of transmitting RF signals through a self-contained integrated chip and analog RF component with an attached battery. While these ZigBee devices are small and considered low-power, they still draw mA of current during transmission [6]. The highest energy consumptions components are the amplifiers and baseband generating digital logic. Moreover, traditional ZigBee radios were not designed to interact with existing WiFi devices in a heterogeneous network.

**Limitation of gateways:** In the ever-crowding and denser wireless networks, the main limitation of the gateways is the energy and device costs to bridge the heterogenous radios. The traditional gateway translates between the WiFi and ZigBee protocols by 1) receiving a data packet from the WiFi device and 2) then retransmitting that data using ZigBee protocols. Examining the case with multiple ZigBees sensors and control devices operating simultaneously on different channels, the gateway would need multiple additional ZigBee radios. In the case where ZigBee sensors operate on the same band, the WiFi using carrier-sense multiple access (CSMA) will back-off due to interference caused by the physical proximity of the collocated ZigBee and WiFi radios on the gateway. Thus, the 1) additional radios, 2) repetitive overhead packets, and 3) gateway deployment increases the energy consumption of the WiFi devices requiring additional infrastructure. With the case that ZigBee and WiFi operating on the same frequency bands, the WiFi must back-off due to CSMA, degrading network throughput. Additionally, the translation between WiFi and ZigBee protocols also introduces additional latency.

**Advantages of Passive-ZigBee:** By leveraging productive WiFi networks, Passive-ZigBee removes the need for the amplifiers and RF generation and therefore, consumes $\mu W$ power enabling communication between pairs of a backscatter tag and a single ZigBee receiver. Moreover, Passive-ZigBee enables WiFi and ZigBee to communicate. Because of the ultra-low current draws, Passive-ZigBee significantly improves battery and provides a framework toward battery-free energy-harvesting sensors.

## 3 DESIGN OVERVIEW AND CHALLENGES

Our design has two main players: a modified WiFi Gateway and Passive-Zigbee tags. The gateway is a router that coordinates between heterogenous IoT devices (WiFi, ZigBee, and backscatter tags). Specifically, the active wider-band gateway operating on the WiFi network's frequency has the ability to concurrently transmit WiFi and ZigBee signals. The low-power narrower-band ZigBee operate on separate frequencies to avoid Carrier-sense multiple access (CSMA) back-off. The Passive-ZigBee tag backscatters the gateway signal to 1) carry sensor data and 2) relay messages to


**Figure 2: A health-monitoring application where WiFi router provides localization data and control messages relayed by Passive-ZigBee's tag. This tag also sends glucose, oxygen saturation, and ECG data. The listener is a long-battery-life wearable ZigBee health monitoring and medicine delivery device.**

ZigBee devices. The signals produced by both devices are able to be decoded by commodity WiFi and ZigBee devices.

The rest of the section describes an overview of WiFi and ZigBee devices. We then explain how to transmit and receive hybrid WiFi and ZigBee signals. After producing these hybrid signals, we provide a theoretical design of a low-power tag which will backscatter the signals. We demonstrate how these tags can 1) send the tag's sensor data and 2) relay packets between the ZigBee and WiFi devices.

- **How does the gateway produce signals for WiFi devices and the backscatter tags simultaneously?** The design challenge for the hybrid gateway is to perform productive communication to WiFi devices and relay mode for backscatter devices. This is done by modifying the wider-band WiFi signal (described in Section 5.1).
- **How does the backscatter tag send sensor data to a listening ZigBee?** The design challenge of the backscatter tag is to reflect the WiFi Gateway signal to transmit sensor data while achieving full ZigBee network throughput and maintaining ultra-low power utilization for both the tag transmitter and receiver. This process is done by modifying the frequency of the hybrid gateway signal that contains ZigBee symbols (described in Section 6).
- **How does the backscatter create custom ZigBee frames for a commodity device?** The backscatter reflects various groups of the wider-band WiFi subcarriers that contain embedded ZigBee symbols. By selecting and reflecting specific portions of WiFi signals, the tags form customized ZigBee frames achieving full ZigBee network throughput (described in Section 6.2).
- **How does the backscatter tag relay WiFi data to the ZigBee Network?** The design challenge of the backscatter tag is to relay and bridge the WiFi gateway to ZigBee networks utilizing ultra-low energy. The tag reflects portions of the WiFi signals that contain ZigBee information to a ZigBee listener (described in Section 6.3).
- **How does a commodity WiFi device act as a hybrid WiFi ZigBee Gateway?** By embedding messages in the WiFi payload, the CoTS WiFi devices can emulate ZigBee frames in the subcarriers. With coordinated backscatter tags, we can achieve low power transmission and reception using listening CoTS ZigBee devices (described in Section 7.1.1).

# 4 BACKGROUND

First, we introduce the WiFi and ZigBee communication protocols.

## 4.1 WiFi Radio

Figure 3 shows a WiFi system overview. A WiFi radio uses multiple sub-carriers to simultaneously transmit aggregate bits in a wider-band protocol. To perform this aggregate transmission: 1) The data payload is interleaved; 2) The WiFi serial binary is parallelized and mapped into bits onto different channels; 3) On each channel, WiFi applies Quadrature Amplitude Modulation (QAM) to mapping bits to different phases in sine waves. We define the various phase states of the signals as symbols. 4) Then, WiFi uses orthogonal frequency-division multiplexing (OFDM) to sum the sine waves. 5) Between each symbol duration, a cyclic prefix is appended to reduce inter-symbol interference. 6) Before the baseband WiFi signal, a training sequence allowing for sender and receiver discovery and synchronization is added. The output signal can be written as Equation1.

$$W(t) = \sum_{n=0}^{N} \left[ \left( I(t)\cos(2\pi f t_1) - Q(t)\sin(2\pi f t_1) \right) e^{2\pi j f_s n} \right] \quad (1)$$

Where there are $N$ total WiFi subcarriers, and for each $n$ subcarrier, we defined complex symbol states at the $I(t)$ and $Q(t)$ mapped by QAM. The duty cycle of each symbol is defined by $ft_1$. We defined the subcarrier spacing frequency by $f_s$.

In the WiFi receiver, the system reverses the mapped and aggregated sine waves back to bits. 1) A correlator and a phase synchronization (Phase Locked Loop) algorithm discover the training sequence and align the demodulator's initial phase state. 2) Using the inverse FFT algorithm, the receiver recovers the aggregated sine waves while accounting for the cyclic prefix. 3) A QAM demodulator maps the phase states of the sine waves to symbols and then to bits.

## 4.2 ZigBee Radio

Passive-ZigBee reflects WiFi packets to commodity ZigBee. The ZigBee transmitter and receiver is shown in Figure 5. In summary, ZigBee radios are low power narrow-band radio that spread its bits over a narrower frequency band. 1) ZigBee uses Direct Sequence Spread Spectrum (DSSS) to spread the signal into a wider band by multiplying with a higher rate (2 MHz) shared pseudorandom noise (PN) code. 2) After the spread spectrum process, the ZigBee modulator maps the bits to sine waves by offset quadrature phase-shift keying (OQPSK) modulation which reduces the dramatic phase

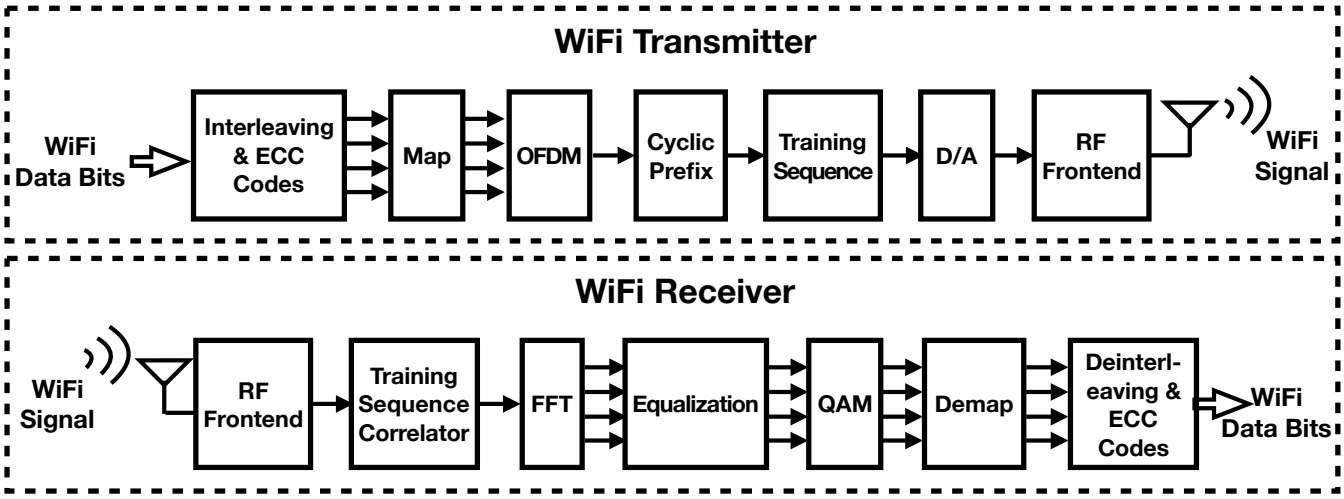


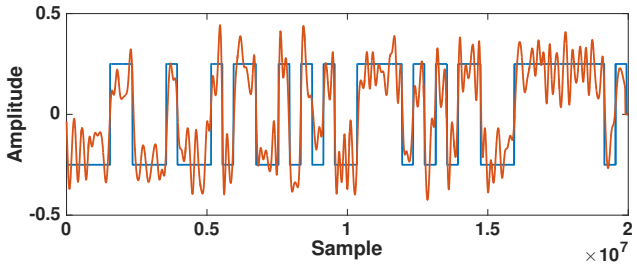

**Figure 3: The WiFi Transmitter and Receiver**

shifts by offsetting the odd and even bits by a distinct period (Equation 2). These sine waves with 4 possible states are the ZigBee chips.

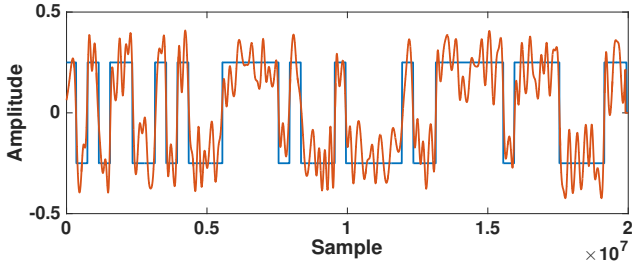
$$Z(t) = \frac{1}{\sqrt{2}} I(t)\cos(2\pi f t) - \frac{1}{\sqrt{2}} Q(t - T_s)\sin(2\pi f t) \qquad (2)$$

Where there are 4 states for I and Q describing the information carrying sine waves, and $T_s$ represents the period offset.

To receive a frame, 1) the ZigBee radio down-converts the received waveforms to baseband and digitalizes them into in-phase and quadrature (I/Q) samples using an analog-to-digital converter




(a) In-phase




(b) Quadrature

**Figure 4: A hybrid WiFi subcarrier containing added ZigBee signals**

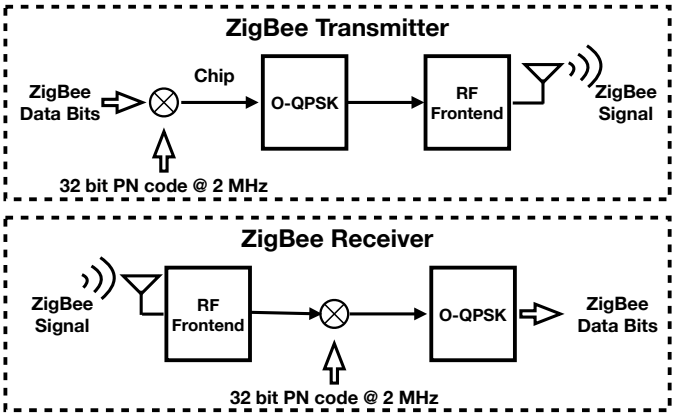



**Figure 5: The ZigBee Transmitter and Receiver**

(ADC). 2) The O-PQSK demodulator measures the changes in phase to symbols. 3). The baseband signal is multiplied by or correlated to a shared PN code which yields the encoded bits. Due to satisfying the statistical randomness property, the PN ensure that interference such as Doppler frequency shifts and multipathing can be recovered from correlations by allowing for some chip errors.

## 5 PASSIVE-ZIGBEE

The objective of Passive-ZigBee is to 1) generate a hybrid ZigBee WiFi signal that enables commodity WiFi communication and 2) using a backscatter sensor device, reflect portions of the hybrid signal to a listening commodity Zigbee device. This system enables 1) backscatter sensor to ZigBee communication and 2) relay the WiFi data to the ZigBee networks that operate on differing channels.

### 5.1 Hybrid WiFi ZigBee Gateway

Figure 4 shows an example of a single hybrid WiFi and ZigBee subcarrier that can concurrently transmit WiFi and ZigBee signals. The design of a hybrid WiFi and ZigBee signal is possible due to the

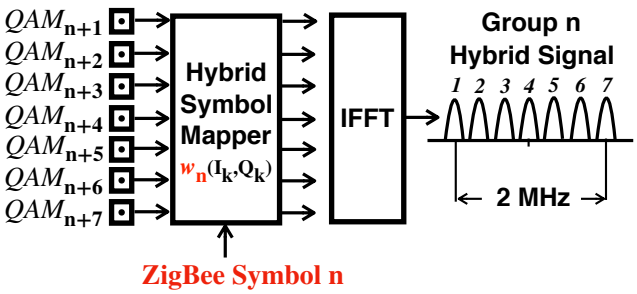



**Figure 6: Hybrid Process**

observations that 1) ZigBee chip and WiFi symbol rates operate on distinct frequencies (2 MHz and 250 KHz) and 2) 7 WiFi subcarriers overlap a ZigBee signal. The intuition is that WiFi subcarriers and ZigBee chips change its phase and amplitude states at different times with different bandwidths. This design is a form of channel sharing using different times similar to CDMA (Code Division Multiple Access). Because of filters that commodity ZigBee and WiFi radio employ, the hybrid packets can be demodulated by both devices.

To achieve the Passive-ZigBee's objective of communicating to ZigBee devices while still maintaining productive WiFi to WiFi communication, we utilize a Software Defined Radio (SDR) to produce a hybrid concurrent WiFi and ZigBee signal. The advantage of an SDR design is the custom gateway can simultaneously communicate with WiFi devices while producing all combinations of ZigBee symbols for the backscatter to reflect. This hybrid signal is achieved by solving for weights added to WiFi baseband QAM signals.

*5.1.1 Tx a Hybrid Signal.* Figure 6 shows the objective of the hybrid gateway is to embed in the wide-band WiFi subcarriers the combination of the ZigBee symbol states, such that a backscatter can choose which symbol to reflect. Thus, a combined hybrid WiFi and ZigBee frames can be received by unmodified WiFi and ZigBee devices. To transmit the signals concurrently, the output of the hybrid gateway must contain a mixture of ZigBee and desired WiFi signals. This mixture is compared to the two baseline signals: normal WiFi signal and WeBee's emulated ZigBee signal. To generate this hybrid signal, we utilize an optimization search algorithm resulting in a linear look-up table. The size of the table is based on the number of the QAM states that matches the 4 OQPSK states. With 7 subcarriers per ZigBee chip, this is a combinatorics problem with 4 objects selecting 7 samples allowing for replacements yielding 120 entries. Due to the WiFi router infrastructure, we don't expect the memory requirements from the look-up table to be an issue.

To combine the ZigBee and WiFi hybrid signal, we recognize that seven WiFi subcarriers contain a single ZigBee channel. Thus, the seven WiFi subcarriers, which operates with 312.5 KHz frequency offsets, must contain both the higher 2 MHz frequency ZigBee chips rate and the lower 250 WiFi KHz symbol rate. To combine these signals, we utilize a look-up table defined by an optimization search algorithm.

We define this optimization algorithm as a search for weights to add to while combining the WiFi subcarriers and ZigBee signals. Minimizing the output's Error Vector Magnitude (EVM) of WiFi and ZigBee symbols. EVM measures the error distance between the desired phase states of both ZigBee and WiFi symbols.

We define the cost function in Equation 3 where $I_{ref}$ and $Q_{ref}$ are the reference or expected phase states. The $I_{Meas}$ and $Q_{Meas}$ are the measured or recovered phase states.

$$C = \sqrt{\left(I_{ref} - I_{Meas}\right)^2 + \left(Q_{ref} - Q_{Meas}\right)^2} \tag{3}$$

Minimize $C_{WiFi}$ and $C_{ZigBee}$ where to $w_1$ and $w_2 \in R$ subjected to

$$\begin{aligned} I_{Meas} &= (I_n(t_1) + w_1 \cdot Z_I(t_2)) \cos(2\pi f t) \\ Q_{Meas} &= \left(Q_n(t_1) + w_2 \cdot Z_Q(t_2)\right) \sin(2\pi f t) \end{aligned} \tag{4}$$

Where $I_n$ and $Q_n$ represent WiFi symbols, and $w_1$ and $w_2$ are searchable weights to scale the ZigBee symbols $Z_I$ and $Z_Q$.

The inputs to the look-up table are a WiFi QAM phase signal and a ZigBee DSSS O-PQSK symbol, and the output is a hybrid combined ZigBee WiFi signal.

The output of the hybrid gateway will be

$$\sum_{n=0}^{N} \left[ \left( (I(t) + w_i) \cos(2\pi f t_1) - (Q(t) + w_q) \sin(2\pi f t_1) \right) e^{2\pi j f_s n} \right] \tag{5}$$

Because of the ZigBee 4 O-PQSK states, there are $2^4 = 16$ possible ZigBee chip states. Thus, the WiFi subcarriers must have all 16 possible ZigBee states embedded in the wide-band signal. Since 7 WiFi subcarriers overlap a single ZigBee symbol, we need $7\dot{k}$ WiFi subcarriers to carry all the possible $k$ ZigBee states.

The modifications to the WiFi subcarriers include the cyclic prefix, the repetitive portions of the WiFi signal to decrease intersymbol interference. Thus, the weights are different for the repetitive portions of the WiFi subcarriers, but the modification from the must not remove all the guard interval. Again mixture is moderated by the optimization algorithms. Due to satisfying the statistical randomness property, the 32-PN codes per symbol scheme ensures that interference such as Doppler frequency shifts and multipathing can be recovered from correlations.

To illustrate this process, Figure 9 demonstrates embedding the ZigBee and WiFi signals together. 1) The ZigBee symbols are spread using a shared PN code. 2) The selected ZigBee and WiFi symbols are mapped using the look-up table generating the hybrid sine waves. 3) The hybrid sine waves are spread using the IFFT algorithms. 4) The rest of the transmission scheme is the same as the standard WiFi protocol described in Section 4.1.

## 6 BACKSCATTER

Figure 1 shows an overview of our system. A WiFi radio transmits a custom packet, and the backscatter reflects the packet to a ZigBee receiver while modulating the narrowband information. When the tag backscatters the packet, it shifts the frequency of the reflected signals to select the desired ZigBee symbol. The ZigBee receiver listens on the normal ZigBee channel, receives the reflected packet, and decodes the packet using the normal ZigBee decoding mechanism. Next, we discuss the key components of our system which enable this capability, first 1) embedding sensor data on the reflecting signal, 2) bridging between the ZigBee and WiFi network operating on different frequency bands, and 3) synchronization.

## 6.1 Backscatter Coding

As shown in Equation 6 and 7, backscatter tags operate on the principles of reflecting existing signals with modifications in the amplitude, phase, and frequency. 1) A transmitter excites electrons and sends a signal. 2) The excited electrons from a transmitter are induced from an antenna onto the receiver because of the potential difference between the ground and the antenna. 3) The radio modifies the signal and re-excites transmitting the electrons.

$$\begin{aligned} S_{out} &= S_{in} \times S_{tag} \\ &= \sin(2\pi f_{in} t) \times [D + \frac{2}{\pi} \sum_{I=1}^{\infty} \frac{sin(n\pi D)}{n} cos(2\pi f_{tag} n t)] \\ &= S_{DC} + S_{shift} \end{aligned} \tag{6}$$

$$\begin{aligned} S_{shift} &= \sin(2\pi f_{in} t) \times \frac{2}{\pi} \sum_{n=1}^{\infty} \frac{sin(n\pi D)}{n} \cos(2\pi f_{tag} n t)] \\ &= \sum_{n=1}^{\infty} \frac{2sin(n\pi D)}{n\pi} [\sin(2\pi f_{in} t) \times \cos(2\pi f_{tag} n t)] \\ &= \sum_{n=1}^{\infty} \frac{sin(n\pi D)}{n\pi} \{\sin[2\pi(f_{in} - f_{tag} n)t] \\ &+ \sin[2\pi(f_{in} + f_{tag} n)t]\} \\ &= S_{left} + S_{right} \end{aligned} \tag{7}$$

$$S_{right} = \sum_{n=1}^{\infty} \frac{sin(n\pi D)}{n\pi} \sin[2\pi(f_{in} + f_{tag} n)t] \tag{8}$$

Thus, backscatter tags are extremely efficient. Because backscatter tags do not need to generate an active carrier wave, these tags require far less power. These tags reduce latency because the radio does not need for the circuits to be warm.

## 6.2 Sensor Data to Commodity ZigBee

Utilizing the hybrid ZigBee WiFi gateway, the backscatter's objective is to shift the desired symbol states embedded in the wide-band hybrid signals to the channel that the ZigBee device listens.

**Algorithm 1** Algorithm on the backscatter

**Input:** $WZ\_Sym\_Freq[K]$, $ZB\_Listen\_Freq$, $BS\_Bits[N]$
**Output:** $BS\_Sig$.

1: **for** $i = 1; 4 * i < N; i = i + 1$ **do**
2: $Symbol[i] = BS\_Bits[(1, 2, 3, 4) + i)]$
3: **end for**
4: **if** $4 * i = N$ **then**
5: $Symbol\ Number:\ M = i - 1$
6: **else**
7: $M = i$
8: $Symbol[i + 1] = BS_Bits[N + 4 - 4 * i] \mid 0000$
9: **end if**
10: **for** $i = 0; i < M; i = i + 1$ **do**
11: $Frequency\ Offset:\ F$
12: $F \rightarrow MAP(WZ\_Sym\_Freq[K],\ Symbol[i])$
13: $BS\_Sig \rightarrow Mix(F, ZB\_Listen\_Freq)$
14: **end for**

As shown in figure 7, the objective of the backscatter is to select which group of ZigBee symbols embedded in the wideband WiFi signal to reflect using frequency shifting to a listening ZigBee receiver expressed in algorithm 1. The array $WZ\_Sym\_Freq[K]$ defines the frequencies in the wide-band WiFi signal that contain the ZigBee symbols. $ZB\_Listen\_Freq$ defines the frequency of the listening ZigBee radio. The array $BS\_Bits[N]$ are the array of $N$ bits acquired from the sensor to be transmitted. The intuition is by shifting and reflecting the desired combination of ZigBee symbols embedded in the wideband hybrid gateway signal, the backscatter communicates to a listening commodity ZigBee device at full 802.15.4 standard throughput. To understand this WiFi subcarrier selecting and frequency shifting process expressed in the function $Mix$, we explain heterodyning.

Heterodyning is the process of changing the original signal frequency to another frequency by mixing the two signals together. The mathematical principle behind this process is a trigonometric identity, expressed in Equation 9.

$$\begin{aligned} &\sin(2\pi f_1 t) \sin(2\pi f_{i2} t) \\ &= \tfrac{1}{2} \left[\cos\left(2\pi \left(f_1 - f_{i2}\right) t\right) - \cos\left(2\pi \left(f_1 + f_{i2}\right) t\right)\right] \end{aligned} \tag{9}$$

Where $f_1$ is the frequency of hybrid Gateway signal, and $f_{i2}$ is the carrier frequency of the tag's clock at symbol instance $i$. Therefore, after the multiplication, there is a frequency shift $f_1 + f_{i2}$ and a phase shift as shown in figure 8. Thus, the backscatter is able to change the incoming signals' frequency to the listening receiver. Here, we ignore the DC component. We could use an existing technique to cancel one of the sidebands, such as $S_{left}$, and keep $S_{right}$ left.

Between each ZigBee symbol rate, the tag must change $f_{i2}$ to the center location of each group of the 7 WiFi subcarriers that each contain a possible ZigBee symbol state. Because there are 4 symbol states in O-QPSK signal, there is a total of $2^4 = 32$ combinations. To change the tag's carrier frequency $f_{i2}$, the clock would need to perform dynamic frequency scaling by varying the voltage level expressed in Equation 10. $P$ is the power consumed; $C$ is the clock capacitance; $V$ is the voltage; $f_{i2}$ is the tag's clock frequency.

$$P = C \cdot V^2 \cdot f_{i2} \tag{10}$$

Figure 9 demonstrates this process. 1) The WiFi gateway embeds possible ZigBee symbols in 7 subcarriers that covers ZigBee frequency band. 2) Multiple groups of the 7 WiFi subcarriers produce differing ZigBee symbols. These subcarriers contain concurrent WiFi and ZigBee data that commodity WiFi and ZigBee devices can demodulate due to the vastly differing symbol and chip rate. 3) The backscatter selects and shifts these groups of 7 subcarriers to the center frequency of the listening ZigBee radio. Figure 10 shows the hybrid process of backscatter relay.

## 6.3 Relay WiFi data to ZigBee Network

The objective of the tag is to relay WiFi data to ZigBee networks that are operating outside of the WiFi network's frequency. As an example, the hybrid gateway transmits a packet to a WiFi receiver. Embedded in that same packet, the gateway embeds ZigBee data using portions of the WiFi packet. In the relay mode, each subcarrier groups contain changing ZigBee symbols that allow the backscatter to relay and bridge to a ZigBee network operating out of the WiFi frequency band.

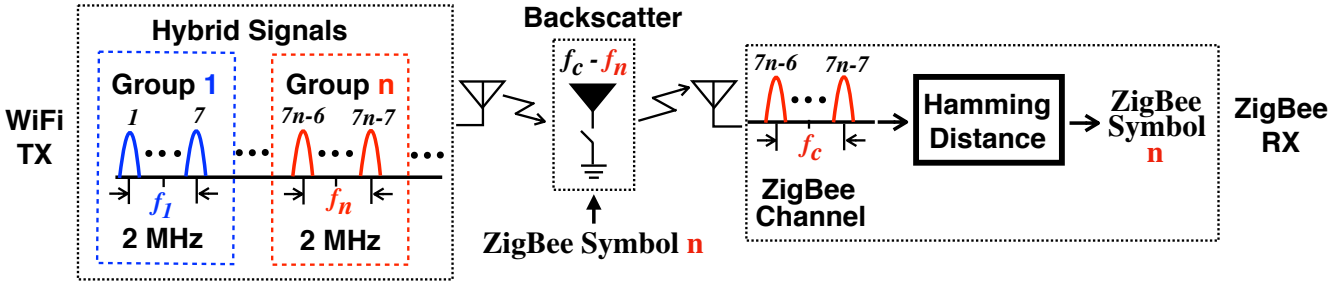



**Figure 7: 7 WiFi Subcarriers carrying concurrent WiFi and ZigBee Data**

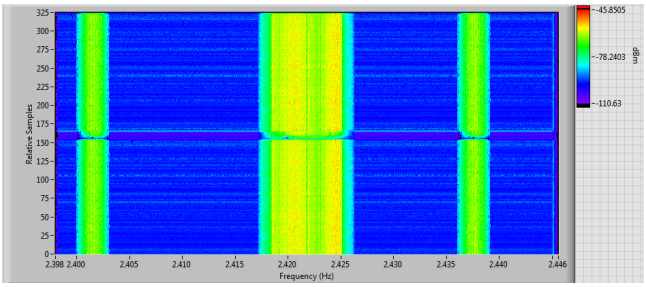


**Figure 8: Reflected WiFi Hybrid signal**

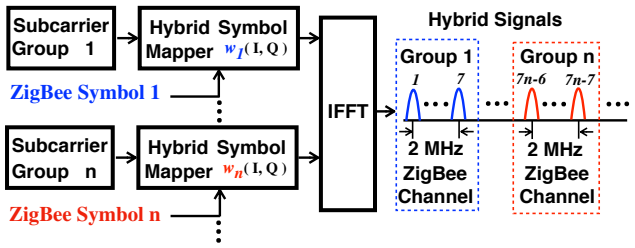



**Figure 9: The Hybrid ZigBee WiFi Gateway**

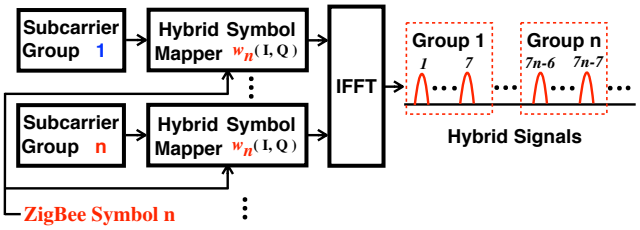



**Figure 10: The Hybrid ZigBee WiFi Gateway for relay**

Figure 10 demonstrates this relaying and bridging process. 1) The gateway embeds the WiFi to ZigBee data in all the groups of 7 subcarriers that covers ZigBee frequency band as before. 2) Multiple groups of the 7 WiFi subcarriers contain the ZigBee symbols that change in respect to the ZigBee symbol duration. Unlike the backscatter sensor data mode, the symbols remain the same for all the groups of subcarriers. 3) The backscatter relays the gateway's message to the listening ZigBee.

## 6.4 Symbol Level Synchonization

In order for the backscatter tag to shift at the rate of each symbol period, the tag must have the knowledge from the hybrid WiFi ZigBee packets symbol period. To achieve this synchronization, we leverage WiFi's training sequence. This training sequence allows for fine timing and frequency synchronization using a specialized BPSK modulation. We utilize a sliding cross-correlation on the signal envelope to seek for this marker for the beginning of symbols. This sliding cross-correlation produces spikes that a simple threshold will provide the phase alignment information. The reason why the correlation to the preamble envelope works for detecting the start is that the preamble has a much greater power level compared the data payload and the preamble is standard for every WiFi packet.

## 6.5 Channel Access

Both WiFi and ZigBee protocols adopt Carrier-sense multiple access with collision avoidance (CSMA/CA) to reduce the probability of packets' collisions among different transmitters. Basically, CSMA/CA senses the channel before transmitting. If the channel is busy, the transmitter backs off and senses again until the channel is free. To sense a particular channel, an energy consuming ADC and a bandpass filter is needed. However, as an ultra low power device, the PassiveZigBee tag is not able to power these two modules. To conduct channel sensing, we offload the sensing task to the gateway side. Specifically, the gateway senses not only the WiFi channel but the targeted ZigBee channel (i.e., the channel which PassiveZigBee shifts to) as well before transmitting the hybrid signal. By doing this, the PassiveZigBee can shift the hybrid signal without backoff.

For example, assuming the gateway communicates with a WiFi device on WiFi channel 1 and the PassiveZigBee transmits to a commodity ZigBee receiver on ZigBee channel 16 (by shifting the hybrid signal from gateway). Before transmitting, the gateway senses the both the WiFi channel 1 and ZigBee channel 16 to avoid collisions on these two channels.

# 7 IMPLEMENTATION

We built Passive-ZigBee using off-the-shelf components utilizing a Virtex 5 FPGA to provide a clock and multiplier as the backscatter. We utilized a standard Software Defined Radio (SDR) and a commodity WiFi and ZigBee devices to prototype the design.

## 7.1 Using CoTS WiFi Devices as the hybrid transmitter

The objective of Passive-ZigBee is to transmit ZigBee symbols frames in wide-band WiFi packets allowing a backscatter to select the frames and communicate with a commodity ZigBee. To achieve this objective, we can use a commodity WiFi device to emulate ZigBee symbols by embedding specific bits in the data payload. We formulate the searching of the string of bits to produce the terms of a search problem.

*7.1.1 Emulating a ZigBee Signal.* We leverage WeBee's technical contribution that was able to emulate ZigBee in WiFi packets. To emulate possible ZigBee frames, we need to first define the output of a WiFi payload in terms of a signal $S_w$. Let the data load be defined as arrays of bits as $WiFi_Payload$. We first define the possible ZigBee frames in equation 11. Where $I_k, Q_k$ is the WiFi symbols for n subcarriers. Since 7 WiFi subcarriers overlap a signal ZigBee frame, we consider the combining the subcarriers as the emulated ZigBee signal. Our search is to find a set of WiFi symbols $I_k, Q_k$ that matches the ZigBee signal $z(N)$ (Equation 11).

$$w_i\left(I_k, Q_k\right) = \sum_{n}^{n+7}\left[I_k \cos\left(2\pi f t\right) - Q_k \sin(2\pi f t)\right] e^{2\pi j f_2 n}$$
$$\max\left\{\begin{array}{c}\arg\max \\ (I_k, Q_k) \in S\end{array}\left[w_i\left(I_k, Q_k\right) * z(N)\right]\right\} \tag{11}$$

The emulation procedure is that 1) the desired ZigBee frames are mapped to a set of WiFi symbols ($I_k$ and $Q_k$). 2) The $I_k$ and $Q_k$ WiFi symbols are then mapped into WiFi bits. 3) Finally, 4) the correct position for the bits are mapped into the packet based on the WiFi devices convolutional interleaving function, such that the WiFi subcarriers produce the respective QAM states that emulate the ZigBee signal. Because of imperfections of emulating ZigBee signal due factors such as repetitive cyclic prefix, the ZigBee's demodulation frame correlation threshold has to be decreased.

## 7.2 Software Defined Hybrid WiFi ZigBee Gateway

The objective of the gateway was to transmit and receive combined and separate ZigBee and WiFi packets. We utilize National Instruments FPGA with 802.11 core to build a custom hybrid WiFi ZigBee gateway. Utilizing a multi-rate design, we synthesized a prototype compatible OFDM QAM design with embedded DSSS O-PQSK signals to transmit to commodity Zigbee and WiFi development receivers (XBee and UP Squared Grove).

## 7.3 Backscatter Tag

The objective of the backscatter tag is to reflect existing signals to the ZigBee listener. We prototyped the backscatter tag design on a National Instruments (NI) FlexRio. The design was a simple mixer that shifted frequencies from the operating frequency of ZigBee and WiFi networks. In a practical implementation, we must sense the WiFi signal through correlation threshold on the WiFi training sequence and remove the interference produced by the mixing process described in Section 6.2 as to reduce interference from non-relevant WiFi subcarriers. Otherwise, these reflected subcarriers may interfere with other ZigBee channels.

*7.3.1 Removing WiFi Subcarrier with active components.* To achieve the optional removal of reflected subcarrier interference, we must achieve the objective of the removing the extra interference signal in the backscatter signal. While removing this interference does not affect the listening ZigBee, interference may occur with other IoT devices depending on the network setup including the strength of the router signal and distance between the tag and other IoT devices. This optional process requires more active components include a low-noise-amplifier and an output band-pass filter must be used. This filter is centered around the ZigBee listener with a bandwidth of 2 MHz matching the ZigBee devices. The amplifier ensures that the signal loss from the filter does not compromise signal integrity. We prototype this design on the NI Flexrio board.

# 8 EVALUATION

We describe the evaluation of the performance of Passive-ZigBee in achieving uplink backscatter up to 55m in none-line-of-sight and mobility scenarios (Section 8.2). Our experiments demonstrate the following

Our Passive-ZigBee prototype achieves an uplink backscatter of 55m in non-of-sight scenarios (NLOS). This distance performance is due to the fact that WiFi routers output higher power than standard ZigBee. In mobility scenarios, we achieve the full 15m distance in hallways in our academic building as our signals need to pass through several (2+) human bodies that are made of mostly water that stops RF signals.

Our system is able to achieve the close to full 250 Kbps throughput in close range (under around 30m) in non-line-of-sight from the from the tag to the commodity ZigBee listener. With human bodies and movement, the ZigBee achieved around 200 Kbps.

The operational range of our WiFi ZigBee hybrid router to tag is more than 10m. Our commodity WiFi receiver is able to receive 802.11n packets at 25m.

Lastly, we show that our simple, low-power tag only consumes around 25 $\mu W$ while shifting the router signal to another frequency band. Through this shifting, we remove carrier interference caused by the all the radios thus decreasing interference. Because the receives are all commodity devices, we show that our system is compatible with existing IoT infrastructure.

We benchmark Passive-ZigBee's range using three metrics: throughput, bit error rate (BER), and received signal strength indicator (RSSI). For a baseline, we controlled the interfering signals by shielding using a Faraday cage that offered -90 dB signal isolation; we placed the router, tag, and ZigBee receiver in the Faraday cage. In our NLOS deployment, the WiFi ZigBee transmitter and the tag were placed in a room while the ZigBee device was operating in the hallway separated by a door and one or two drywall. In mobility scenarios, we attached the ZigBee receiver to the human body and received messages while moving. We moved the ZigBee and receiver away increasing from the tag and measured throughput, BER, and RSSI. Then we also move the ZigBee listener away from the tag and measured throughput, BER, and RSSI.

We evaluate Passive-ZigBee with the hybrid gateway at 2.422 GHz at 40 MHz with 108 subcarriers. Our ZigBee receivers operated at 2.405 to 2.480 GHz.

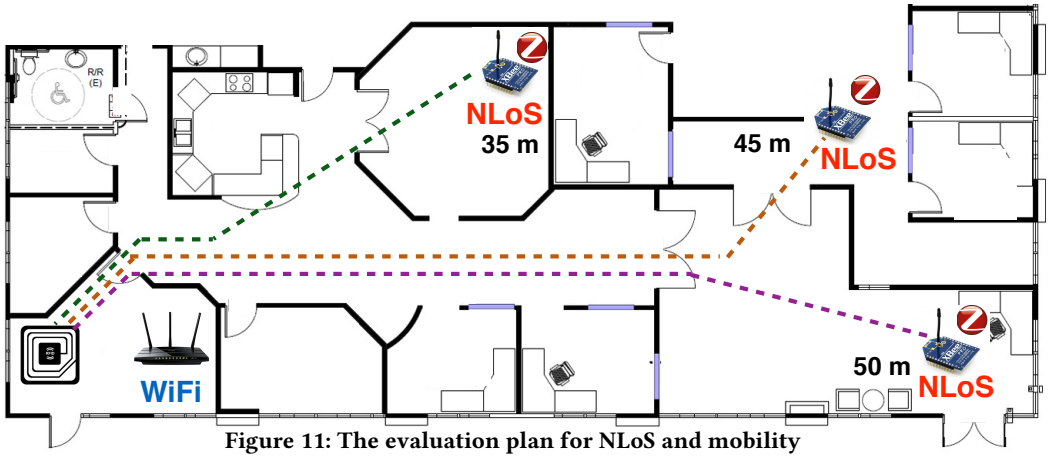



**Figure 11: The evaluation plan for NLoS and mobility**

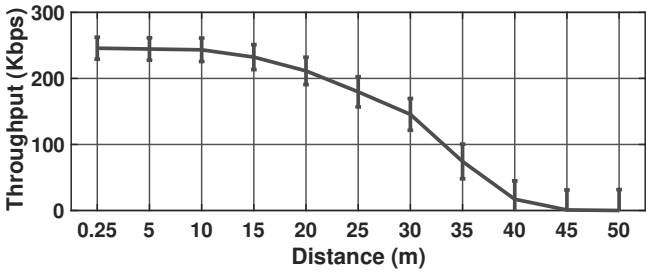



**Figure 12: Backscatter to ZigBee throughput in NLoS Passive-ZigBee has stable throughput over communication distance in NLoS scenario.**

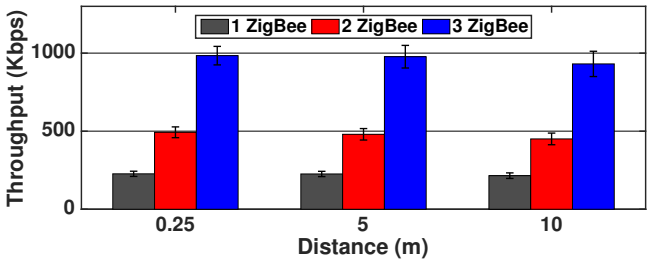



**Figure 13: Backscatter to ZigBee throughput in Mobile Scenario. Passive-ZigBee has stable throughput over communication distance.**

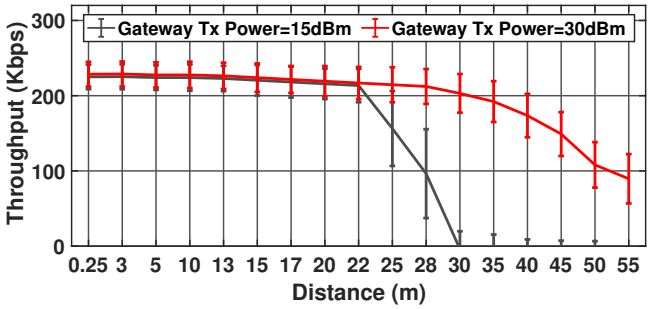



**Figure 14: Backscatter to ZigBee Throughput under different Gateway Transmission Power**

## 8.1 NLoS Performance

In this section, we evaluate the backscatter to ZigBee throughput over communication distance. Figure 12 shows the results. At 0.25 meter, the throughput achieves around 230 Kbps (note that 250 Kbps is the maximum throughput defined by ZigBee's protocol). When the communication distance increases to 10 meters, the throughput of backscatter to ZigBee communication is very stable (around 225 Kbps). We further evaluated the throughput at longer distances. At 35 meters, it still maintains around 80 Kbps. The reason is that Passive-ZigBee has simple design at the backscatter side that the low power device only needs to select the incoming signal to modulate OQPSK signal.

***Takeaway:*** *Passive-ZigBee is able to achieve low power and long-range communication.*

## 8.2 Mobility Performance

Since Passive-ZigBee is designed for low power sensors, potentially, it can be deployed on human bodies for medical or fitness applications. To investigate the performance of Passive-ZigBee on the human body, we asked up to three participants to wear the Passive-ZigBee tags in their pockets and walked around the office. Figure 13 shows the aggregated throughput across one, two, or three tags over different communication distances. Overall, for one tag, the throughput is stable when the communication distance increases from 0.25 meter to 10 meters (the results only show a slight decrease from 227Kbps to 215Kbps). The reason is that the tag shifted the signal to out-of-band ZigBee receiver. Thus, it is not affected by the original in-band WiFi signal. For two and three tags, the throughput linearly increases because the Passive-ZigBee tags can reflect the hybrid signal to different frequency channels that they do not impact with each other.

***Takeaway:*** *Passive-ZigBee shows stable throughput even attached to a human body and in mobile scenarios.*

## 8.3 Impact of Gateway Transmission Power

In this section, we test how the gateway transmission power impacts the backscatter to ZigBee throughput over communication distance. Figure 14 shows the results. When the communication distance is relatively short (less than 22 meters), the throughput under 15 dBm and 30 dBm are similar and maintains around 220 Kbps. After 22

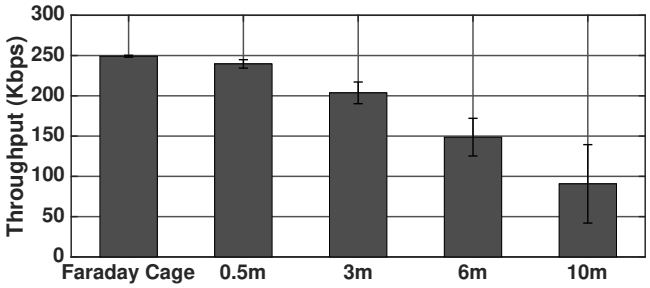



**Figure 15: The throughput of Backscatter to ZigBee in NLoS**

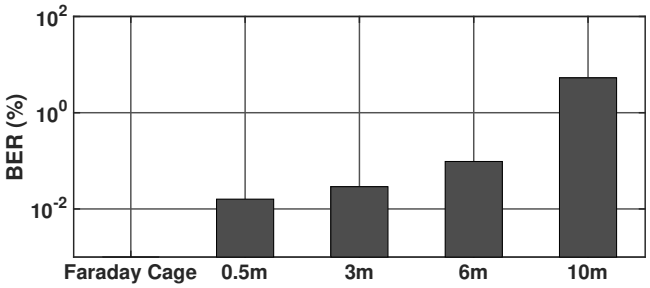



**Figure 16: BER of Backscatter to ZigBee in NLoS**

meters, the throughput under 15 dBm transmission power drops exponentially as the SNR decreases. Thus, the commodity ZigBee throughput under -30 dBm transmission power is still stable. Even at 55 meters, the throughput under -90 dBm transmission power achieves up to 88 Kbps throughput. The receiver will drop the packet when incorrect DSSS chips exceed the threshold of the demodulator.

***Takeaway:*** *When the communication range is within 22 meters, the gateway transmission power does not impact too much on Passive-ZigBee's throughput. When the communication is longer than 22 meters, the gateway transmission power shows a positive impact on Passive-ZigBee's performance.*

*8.3.1 Impact of Transmitter-Tag Distance.* Figure 15 shows the impact of increasing tag to ZigBee receiver distance to throughput, and Figure 16 shows the impact respect to BER. Our experiment demonstrates successful reception at over 10 meters non-line-of-sight. At close distances, we achieved near maximum ZigBee standard throughput (250 Kbps). The backscatter tag does significantly decrease the reflected power; but due to the robustness of ZigBee spread spectrum protocols, our experiment demonstrates more than 10 meter of reception. The exponential increase of BER is expected with DSSS and QPSK.

## 8.4 Latency

To demonstrate latency in bridging WiFi and ZigBee networks, we experimented in IoT networks comparing Gateway and Passive-ZigBee backscatter approaches. We modeled the time between when data was given to the transmitting radio to when the RF signal is received. We measured the collisions and CSMA backoff with commodity ZigBee and WiFi devices using lossless National Instruments RF recording system. In all the cases, we experimented

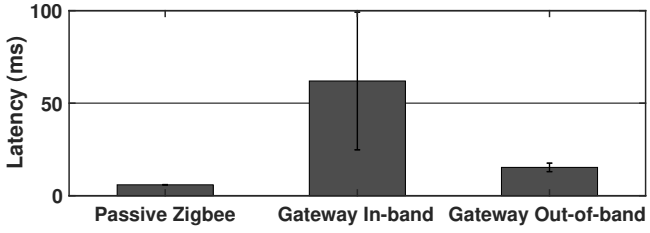



**Figure 17: Latency**

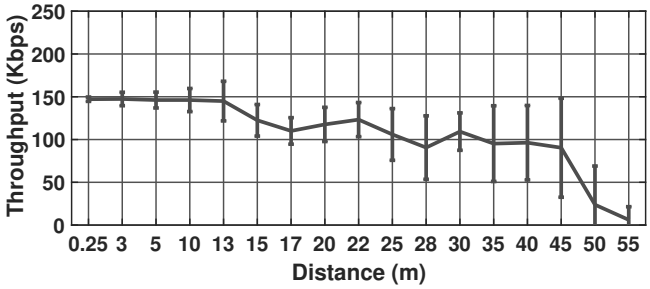



**Figure 18: Throughput of Backscattering COTS WiFi to ZigBee in NLoS.**

with ZigBee receivers that operate in both WiFi in-band and out-band networks. As shown in Figure 17, due to CSMA back-off, in-band ZigBee devices experience heavy latency (53 ms). Without out-of-band band ZigBee devices, latency (15 ms) is primarily caused by the translation between the WiFi and ZigBee protocols. The cause of low latency (6 ms) in Passive-ZigBee is the decoding logic in ZigBee receiver due to instantaneous frequency shifting method of Passive-ZigBee without having to wait for baseband generating circuits to warm.

***Takeaway:*** *Passive-ZigBee shows much lower latency compared with traditional ZigBee devices.*

## 8.5 Use of Commodity WiFi Gateway

To demonstrate that we can use commodity WiFi to emulate ZigBee signals, we used an Atheros QCA9880 802.11ac chipset due to the ability to inject packets and to fix scramble seeds. We also operated in 5 GHz with 80 MHz in increase number available subcarriers. Because of the ability to directly inject packets and monitor the signal produced, we could determine how the bits were interleaved into the FFT outputs by demodulating using a Keysight Vector Signal Analyzer. In our experiment, we were only able to synthesize 10 simultaneous ZigBee symbols due to pilot tones and firmware compatibility. Thus this limited our throughput. This limitation can be removed with newer devices and firmware. Our experiment demonstrates the framework that 180 MHz 802.11ac can generate all the possible symbol combinations. We also lowered the correlation threshold in MICAz ZigBee listener to adapt to the emulated signals. The results in Figure 18 demonstrate that at 0.5 meter, 35 meters, and 50 meters communication distance, the throughput achieves around 150 Kbps, 100 Kbps, and 25 Kbps, respectively.

***Takeaway:*** *Passive-ZigBee can use a commodity WiFi as a sender to communicate with ZigBee devices.*

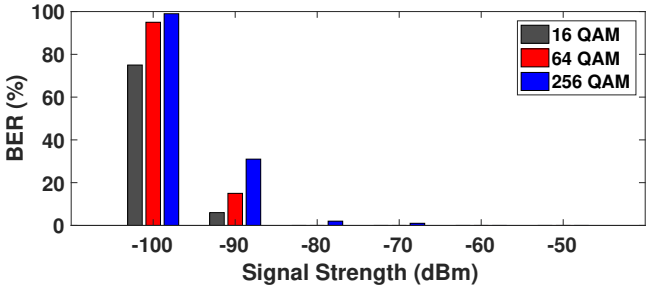



**Figure 19: Bit error rate (BER) at ZigBee Receiver Side**

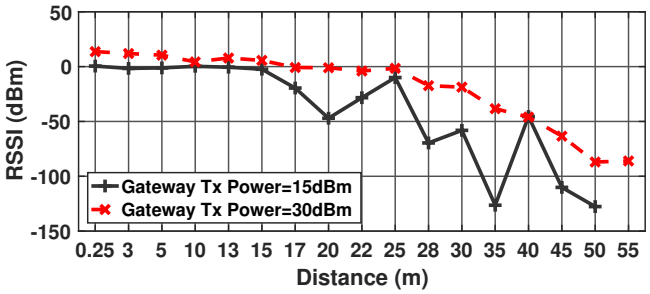



**Figure 20: RSS @ ZigBee Receiver Side**

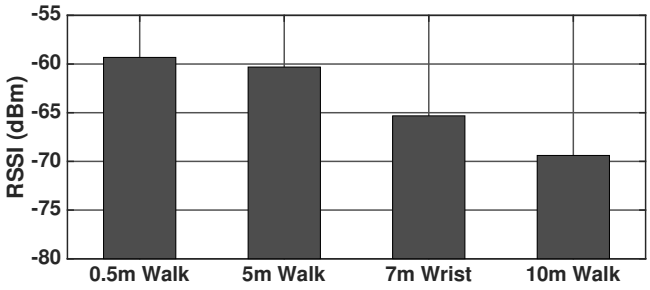



**Figure 21: Mobility RSSI**

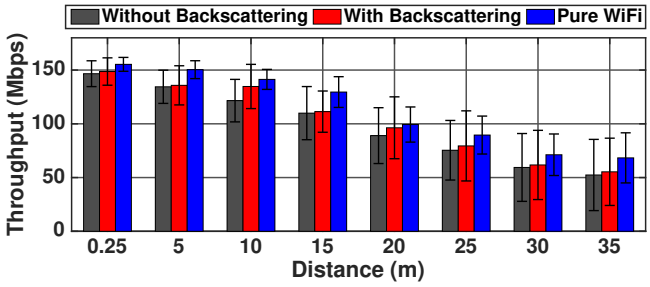



**Figure 22: The impact to On-going WiFi Communications**

## 8.6 BER

In this section, we show the results of Bit error rate (BER) at different received signal strength. Figure 19 shows the results for different WiFi modulation schemes (including 16, 64, and 256 QAM). We can observe that with lower rank modulation scheme (i.e., 16 QAM), the BER is lower and the BER is relatively high with higher rank modulation schemes (i.e. 64 and 256 QAM). The reason is that the hybrid signal needs to emulate both ZigBee and WiFi signal. Since lower higher rank modulation scheme is sensitive to SNR, the optimization scheme (introduced in Section 5.1.1) adds more weight on WiFi signal. Thus at ZigBee receiver side, the BER is relatively high compared with the lower rank modulation scheme. The results show that the BER is approaching 0 when the received signal strength is higher than -80 dBm. This ensures the backscatter to ZigBee communication at a high throughput.

***Takeaway:*** *Passive-ZigBee shows low BER when the signal strength is higher than -90 dBm regardless of the WiFi modulation scheme.*

## 8.7 RSS @ the ZigBee Receiver

We measured the received signal strength (RSS) at ZigBee receiver side and show the results in Figure 20. The figure shows the RSS with different gateway transmission power (15 and 30 dBm). Overall, we can observe that the overall RSS decreases along with the communication distance increases; this is the major reason that the throughput decreases and BER increases over distance. The received signal strength for 15 dBm (black solid curve) is lower than 30 dBm (red dashed curve). The results have some fluctuation caused by the multipath effect. We also experimented on mobility scenario measuring the RSSI levels measuring the distance between a person walking with tag and stationary ZigBee receiver. The RSSI levels demonstrate that the ZigBee receiver was able to receive messages beyond 10 meters distance at -70 dBm.

## 8.8 The impact to On-going WiFi Communications

In this section, we evaluate the impact of 1) backscatter to on-going WiFi traffic and 2) hybrid WiFi ZigBee signal. Figure 22 shows that regardless of whether backscatter presents or not, the throughput of WiFi communication decreases along with communication distance increases because the SNR decreases while communication distance increases. By comparing the scenarios with or without backscatter at the same communication distance (for example 35 meters), the results did not show an obvious difference. It is because that the backscatter shifts the WiFi signal to another channel which is far (in terms of frequency) from the original WiFi channel.

Compared to the original WiFi router, the hybrid WiFi ZigBee decreased throughput by about 10% due to interference created to the original WiFi signals. This is due to our increase in overhead bits using WiFi's native convolutional forward error correcting codes.

***Takeaway:*** *Passive-ZigBee does not make an impact to on-going WiFi traffic because it is able to shift the signal to out-of-band ZigBee channel.*

## 8.9 Energy Consumption

Table 1 shows the breakdown of the components of Passive-ZigBee. Our results are based on Xilinx Power Estimator tool. The clock does consume variable power depending desired clock speed but averages out to 11 $\mu W$. The mapping logic can be synthesized using selective NAND gates using 6 $\mu W$. Our FPGA synthesis tool shows that the critical transmitting components use around 25 $\mu W$ of

| | Clock | Logic |
|---|---|---|
| Energy Consumption (uW) | 11 | 6 |

**Table 1: Energy Consumption for Each Component**

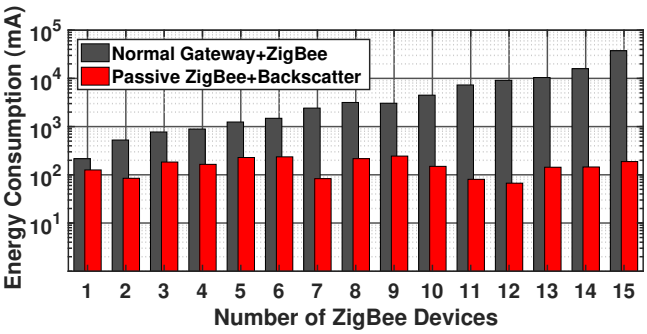



**Figure 23: Energy Consumption (the y-axis is in log scale)**

power. The power produced from energy harvesting devices produce around 100 $\mu w$ from indoor lights and temperature supporting Passive-ZigBee.

We experimented up to 15 links of backscatter to ZigBee communications as well as traditional ZigBee to ZigBee communications and estimating the energy consumption at the sender sides (backscatter or ZigBee sender). From the results shown in Figure 23 (note that the y-axis is in log scale), we observe that the average energy consumption of backscatter is 1,440 times lower than the traditional ZigBee communications while providing similar throughput.

***Takeaway:*** *Comparing to traditional ZigBee, Passive-ZigBee saves 1,440 times energy to transmit a packet.*

## 9 RELATED WORKS

The related works are divided into two categories:

**Backscatter:** Backscatter techniques enable a promising way for extremely low power sensing and computing devices due to the removal of carrier and symbols generators. Recent research demonstrates these backscatter systems, such as TV backscatter [14], full-duplex backscatter [15], turbocharing backscatter [16], LoRa backscatter [17] which works on 900 MHz to achieve longer communication distances.

Interesting works include [1, 7, 9, 10, 20–22] which utilize the ambient signals on the ISM 2.4 GHz band to enable communications between low power backscatters and pervasive receivers (e.g., WiFi, ZigBee, and Bluetooth devices). Specifically, the WiFi backscatter [9] piggybacks backscatter's data on existing WiFi signal and receives it on a cell phone using CSI (Channel States Information). Backfi [1] utilizes full-duplex technique on the WiFi receiver side to separate the WiFi and backscattered signal, which boosts the backscatter-to-receiver throughput. Passive WiFi [10] and FS-Backscatter [22] shift the backscattered signal to out-of-band to achieve higher SNR for demodulation. Interscatter [7] reflects the Bluetooth signal to commodity WiFi devices for medical applications. Hitchhike [22] uses a coding scheme to remove additional carriers so that backscatter can reflect between 802.11b compatible WiFi devices. Freerider [21] further improves the system in Hitchhike so that it works with 802.11g WiFi, ZigBee, and Bluetooth devices.

Different from current backscatter works, our PassiveZigBee achieves both productive WiFi 802.11n communications while maintaining extremely low power consumption to i) communicate with ZigBee networks; and ii) bridge WiFi networks and ZigBee networks. Meanwhile, it generates minimal impact to existing WiFi communication and achieves maximum ZigBee standard throughput.

**Cross Technology Communication (CTC):** In this category, the researchers both mitigate and utilize the interference among different wireless communication techniques (e.g., WiFi, ZigBee, and Bluetooth). Esense [2] and Gsense [23] utilize special timing features of packet length and gap duration, respectively. FreeBee [11], EMF [3], C-morse [19] and DCTC [8] use packet level modulation to improve the CTC performance. $B^2W^2$ [4] demodulates the BLE data by using the CSI at WiFi side. In WEBee [13], they propose to manipulate the WiFi payload for ZigBee signal emulation. Other proposals that demonstrated symbol level modification for CTC include PMC [5] and Chiron [12]. Reducing latency under concurrent communcation, ECT [18] changes node prioirties through network protocals.

Different from above CTC papers, our goal is to enable ultra-low power sensor which can not only communicate with ZigBee devices but forward messages from WiFi device to ZigBee device as well.

Passive-ZigBee is a novel backscatter low power radio that leverages existing commodity WiFi and ZigBee infrastructure by transforming productive WiFi packets into ZigBee packets. The backscatter uses 1,440 times lower power compared to a traditional ZigBee transmitter. Moreover, the backscatter also is capable of relaying data between WiFi to ZigBee devices. To perform the reverse communication path, we could use existing techniques such as Chiron [12].

## 10 CONCLUSION

Passive-ZigBee is a novel backscatter low power radio that leverages existing commodity WiFi and ZigBee infrastructure by transforming productive WiFi packets into ZigBee packets. The backscatter uses 1,440 times lower power compared to a traditional ZigBee transmitter. Moreover, the backscatter is also capable of relaying data between WiFi to ZigBee devices.

## ACKNOWLEDGMENTS

This project is supported by NSF grants CNS-1652669 and CNS-1539047. We also thank anonymous reviewers and our shepherd for their valuable comments.

## REFERENCES

[1] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. 2015. BackFi: High Throughput WiFi Backscatter. *SIGCOMM Comput. Commun. Rev.* 45, 4 (Aug. 2015), 283–296. DOI: http://dx.doi.org/10.1145/2829988.2787490

[2] Kameswari Chebrolu and Ashutosh Dhekne. 2009. Esense: Communication Through Energy Sensing. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom '09)*. ACM, New York, NY, USA, 85–96. DOI: http://dx.doi.org/10.1145/1614320.1614330

[3] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu. 2017. EMF: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices. In *IEEE INFOCOM 2017 - IEEE Conference on*

*Computer Communications*. 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2017.8057109

[4] Zicheng Chi, Yan Li, Hongyu Sun, Yao Yao, Zheng Lu, and Ting Zhu. 2016. B2W2: N-Way Concurrent Communication for IoT Devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM (SenSys '16)*. ACM, New York, NY, USA, 245–258. DOI: http://dx.doi.org/10.1145/2994551.2994561

[5] Zicheng Chi, Yan Li, Yao Yao, and Ting Zhu. 2017. PMC: Parallel multi-protocol communication to heterogeneous IoT radios within a single WiFi channel. In *Network Protocols (ICNP), 2017 IEEE 25th International Conference on*. IEEE, 1–10.

[6] Artem Dementyev, Steve Hodges, Stuart Taylor, and Joshua Smith. 2013. Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. In *Wireless Symposium (IWS), 2013 IEEE International*. IEEE, 1–4.

[7] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. 2016. Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices. In *Proceedings of the 2016 ACM SIGCOMM Conference (SIGCOMM '16)*. ACM, New York, NY, USA, 356–369. DOI: http://dx.doi.org/10.1145/2934872.2934894

[8] W. Jiang, Z. Yin, S. M. Kim, and T. He. 2017. Transparent cross-technology communication over data traffic. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2017.8057086

[9] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R. Smith, and David Wetherall. 2014. Wi-fi Backscatter: Internet Connectivity for RF-powered Devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM (SIGCOMM '14)*. ACM, New York, NY, USA, 607–618. DOI: http://dx.doi.org/10.1145/2619239.2626319

[10] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. 2016. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX Association, Santa Clara, CA, 151–164. https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/kellogg

[11] Song Min Kim and Tian He. 2015. FreeBee: Cross-technology Communication via Free Side-channel. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom '15)*. ACM, New York, NY, USA, 317–330. DOI: http://dx.doi.org/10.1145/2789168.2790098

[12] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. 2018. Chiron: Concurrent High Throughput Communication for IoT Devices. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 204–216.

[13] Zhijun Li and Tian He. 2017. WEBee: Physical-Layer Cross-Technology Communication via Emulation. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17)*. ACM, New York, NY, USA, 2–14. DOI: http://dx.doi.org/10.1145/3117811.3117816

[14] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. 2013. Ambient Backscatter: Wireless Communication out of Thin Air. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM (SIGCOMM '13)*. ACM, New York, NY, USA, 39–50. DOI: http://dx.doi.org/10.1145/2486001.2486015

[15] Vincent Liu, Vamsi Talla, and Shyamnath Gollakota. 2014. Enabling Instantaneous Feedback with Full-duplex Backscatter. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom '14)*. ACM, New York, NY, USA, 67–78. DOI: http://dx.doi.org/10.1145/2639108.2639136

[16] Aaron N. Parks, Angli Liu, Shyamnath Gollakota, and Joshua R. Smith. 2014. Turbocharging Ambient Backscatter Communication. In *Proceedings of the 2014 ACM Conference on SIGCOMM (SIGCOMM '14)*. ACM, New York, NY, USA, 619–630. DOI: http://dx.doi.org/10.1145/2619239.2626312

[17] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. 2017. LoRa Backscatter: Enabling The Vision of Ubiquitous Connectivity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 105 (Sept. 2017), 24 pages. DOI: http://dx.doi.org/10.1145/3130970

[18] Xin Liu Wei Wang, Tiantian Xie and Ting Zhu. 2017. ECT: Exploiting Cross-Technology Concurrent Transmission for Reducing Packet Delivery Delay in IoT Networks. In *Network Protocols (ICNP), 2017 IEEE 25th International Conference on*. IEEE.

[19] Z. Yin, W. Jiang, S. M. Kim, and T. He. 2017. C-Morse: Cross-technology communication with transparent Morse coding. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2017.8057107

[20] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. HitchHike: Practical Backscatter Using Commodity WiFi. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM (SenSys '16)*. ACM, New York, NY, USA, 259–271. DOI: http://dx.doi.org/10.1145/2994551.2994565

[21] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. FreeRider: Backscatter Communication Using Commodity Radios. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT '17)*. ACM, New York, NY, USA, 389–401. DOI: http://dx.doi.org/10.1145/3143361.3143374

[22] PENGYU ZHANG, Mohammad Rostami, Pan Hu, and Deepak Ganesan. 2016. Enabling Practical Backscatter Communication for On-body Sensors. In *Proceedings of the 2016 ACM SIGCOMM Conference (SIGCOMM '16)*. ACM, New York, NY, USA, 370–383. DOI: http://dx.doi.org/10.1145/2934872.2934901

[23] X. Zhang and K. G. Shin. 2013. Gap Sense: Lightweight coordination of heterogeneous wireless devices. In *2013 Proceedings IEEE INFOCOM*. 3094–3101. DOI: http://dx.doi.org/10.1109/INFCOM.2013.6567122