Enabling ZigBee Backscatter Communication in a Crowded Spectrum

Zhaoyuan Xu and Wei Gong*
University of Science and Technology of China
xzyjyx@mail.ustc.edu.cn, weigong@ustc.edu.cn

***Abstract*—To piggyback information, the instantaneous-phase shift (IPS) modulation toggles discrete phases on ambient RF carriers, which is popular with advanced backscatter systems. However, IPS has poor spectrum efficiency. It produces serious spectrum sidelobes and prevents the formation of large networks. In this paper, we propose frequency-phase shift (FPS) modulation, a fine-grained RF switches toggling that modulates carriers with a continuous phase shift. The phase continuity suppresses spectrum sidelobes without disturbing the demodulation results. We first apply FPS to optimize a ZigBee backscatter tag. ZigBee signals, consisting of a non-single-tone header and a single-tone payload, are transmitted as RF carriers. The backscatter tag leverages FPS to modulate the single-tone for phase-continuity data transmission. Further, the tag recycles the non-single-tone header using sub-symbol codeword translation to improve carrier utilization.**

Through extensive experiments and field studies, we demonstrate that FPS enables ZigBee transmissions with a bandwidth of 2.4 MHz, which is 3x lower than that of Interscatter [1] and much closer to active radios. The system prototype consists of a microchip transmitter, a backscatter tag, and a commodity receiver. Specifically, when the transmitter-to-tag distance is within 5 centimeters, the system enables a goodput of 16.6 kbps at a channel capacity of 16.8 kbps, and the communication distance can be extended to 17 meters.

***Index Terms*—System; IoT; Backscatter; ZigBee**

I. INTRODUCTION

The Internet of Things (IoT) is promising to build large networks and supports upper applications with big data [2] [3] [4]. However, active IoT radios are power-hungry and cannot work sustainably. An active IoT radio generally consumes tens of milliwatts and requires battery replacement frequently [5] [6] [7]. It uses a local oscillator to produce an internal radio-frequency (RF) carrier. The low-frequency (LF) baseband signal containing upper information is mixed with the carrier for wireless transmission. Both the local oscillators and RF mixers are power-expensive, which limits the deployment of active IoT radios.

In recent years, backscatter technology has attracted a lot of interest for its ultra-low power consumption ([8], [9], [10], [11], [12], [13], [14]). The backscatter tag modulates ambient signals (e.g., Wi-Fi, ZigBee, Bluetooth, LoRa, etc.) for RF carriers and generally consumes tens of microwatts. The tag is capable of reflecting ambient signals which pass across the backscatter circuit. Backscatter works by producing baseband signals and correspondingly toggling the reflection coefficient. It modifies the information (e.g., amplitude, phase, frequency) of the carrier and retransmits the modified carriers over the air.

*Corresponding author: Wei Gong

978-1-6654-8234-9/22/$31.00 ©2022 IEEE

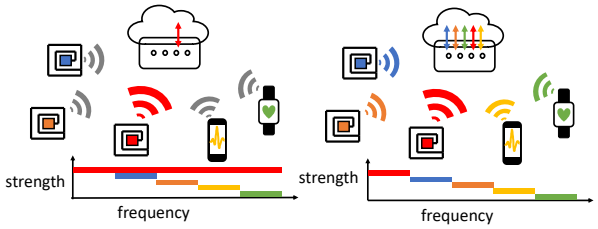


Fig. 1. Application snapshot. On the left, the tag occupies much more spectrum and does interference with neighbor IoT radios. Specifically, when its power is high enough, neighbor IoT radios fail to communicate with each other. On the right, the spectrum-efficient backscatter tag works concurrently with multiple IoT radios. A number of radios share spectrum resources and transmit data concurrently.

The instantaneous-phase shift (IPS) modulation is popular with advanced backscatter systems, such as Interscatter [1]. To piggyback information, IPS toggles discrete phase shifts (e.g., $0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}$) on ambient RF carriers. The discrete phase shift sequence (e.g., $+\frac{\pi}{2}, -\frac{\pi}{2}, +\frac{\pi}{2}, -\frac{\pi}{2}, ...$) produces serious sidelobes and has poor spectrum efficiency, which worsens the crowded spectrum. As shown in Fig.1, the spectrum-inefficient backscatter tag does interfere with neighbor IoT radios. Specifically, when its power is high enough, neighbor IoT radios fail to communicate with each other. On the contrary, the spectrum-efficient backscatter tag works concurrently with multiple IoT radios. Our evaluations in Section V demonstrate that Interscatter enables ZigBee transmissions with a bandwidth of 8.31 MHz, which greatly exceeds protocol regulations.

In this paper, we present Frequency-Phase Shift (FPS) modulation, a fine-grained RF switches toggling that produces phase continuity to suppress spectrum sidelobes. Instead of using a power-expensive pulse-shaping filter, the toggling signal is binarized into square waves with various frequencies and phases. Our evaluations show that FPS enables ZigBee transmissions with a bandwidth of 2.4 MHz. Specifically, the phase shift ($\phi_0 \rightarrow \phi_1$) is achieved using a square wave with an initial phase (ϕ_0) and frequency ($f = f_{shift} + \frac{\phi_1 - \phi_0}{2\pi\Delta T}$). Frequency is the ratio of phase shift over time ($f = \frac{\Delta\phi}{2\pi\Delta T}$). f_{shift} indicates the frequency shift to avoid carrier interference.

ΔT is the transition time. Since active receivers generally demodulate signals with the sign (positive or negative) of phase shift ($\phi_1 - \phi_0$), FPS does not disturb the demodulation results. Further, it is applicable for multiple wireless protocols (e.g., ZigBee, Wi-Fi, BLE).

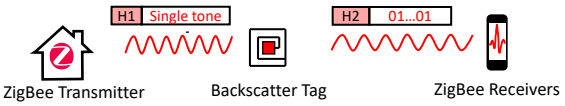


Fig. 2. System overview. The ZigBee transmitter provides RF carriers for signal excitation. The backscatter tag takes FPS to modulate ZigBee single-tone. Since RF carriers are dedicated resources for backscatter communication, the tag also translates the non-single-tone header (H1) into another (H2) to improve carrier utilization.

An FPS-based ZigBee backscatter system is shown in Fig. 2. It consists of a commodity ZigBee transmitter, a backscatter tag, and a commodity ZigBee receiver. The transmitter transmits ZigBee signals, consisting of a non-single-tone header (H1) and a single-tone payload, as an RF carrier. The carrier is powerful and does interfere with the backscatter communication. To eliminate carrier interference, the tag uses an additional frequency shift (f_{shift}) to produce signals on the neighbor ZigBee channels [1] [11] [15]. Further, the tag leverages FPS to modulate the single-tone for phase-continuity ZigBee transmissions in a crowded spectrum. Due to the scarcity of RF carriers, the tag recycles the non-single-tone header using sub-symbol codeword translation to improve the utilization, which re-customizes the header (H1) into another (H2).

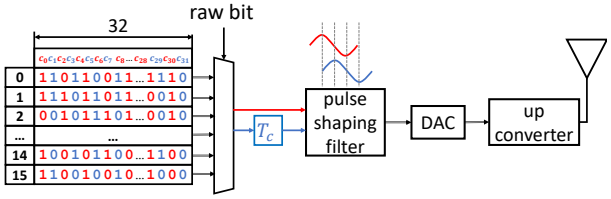
When the transmitter-to-tag distance is within 5 centimeters, our evaluations in Section V show that our tag enables a goodput of 16.6 kbps when the channel capacity (i.e., single tone + non-signal tone) is limited to 16.8 kbps. Further, the communication distance can be extended to 17 meters under indoor line-of-sight scenarios. We believe that our system can be applied effectively to enable ZigBee backscatter in a crowded spectrum. In this paper, we make the following contributions:

- We present FPS modulation, which is designed for RF switch toggling and capable of improving spectrum efficiency. In Section III-A, we demonstrate FPS design in detail and take ZigBee transmissions to validate its bandwidth efficiency. Our evaluations show that FPS enables ZigBee transmissions with a bandwidth of 2.4 MHz.
- We apply FPS practically to a ZigBee backscatter system and improve carrier utilization. A transmitter transmits ZigBee signals consisting of a non-single-tone header and a single-tone payload for the RF carrier. The sub-symbol codeword translation is introduced to recycle the non-single-tone header.
- We build a hardware prototype on an FPGA platform and perform comprehensive experiments to validate the system's effectiveness.

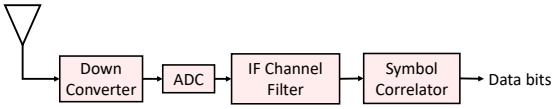
II. PRELIMINARIES

A. Active ZigBee transceiver

Active ZigBee transmitter ZigBee physical layer (PHY) is IEEE 802.15.4 [16]. It supports data transmission of 250 kbps. An active ZigBee transmitter, as shown in Fig. 3(a), spreads every four bits into one of the pseudo-random noise (PN) chip sequences $(c_0, c_1, ..., c_{30}, c_{31})$, which is known as the direct-sequence spread spectrum (DSSS). $c_i (0 \leq i \leq 31)$ has a value of either 0 or 1. Branch I indicates an in-phase component $(c_0, c_2, ..., c_{28}, c_{30})$, and branch Q indicates a quadrature-phase component $(c_1, c_3, ..., c_{29}, c_{31})$. The chip duration in each branch is $2T_c$ ($T_c = 0.5\mu s$) and there is a time offset (T_c) in branch Q.



(a) Architecture of active ZigBee transmitter



(b) Architecture of active ZigBee receiver

Fig. 3. Architecture of active ZigBee transceiver.

A pulse-shaping filter translates an input chip into a digital half-sinusoidal waveform and its expression is shown in (1). $\frac{1}{T_s}$ is the filter sampling rate and nT_s is the sample time.

$$p(nT_s) = \begin{cases} sin(\pi \frac{nT_s}{2T_c}), nT_s \in [0, 2T_c] & input = 1 \\ -sin(\pi \frac{nT_s}{2T_c}), nT_s \in [0, 2T_c] & input = 0 \end{cases} \quad (1)$$

As shown in (2), the filter enables two characters for the combination of branch I/Q: i) the phase shift between consecutive chip units (T_c) is limited within $\{+\frac{\pi}{2}, -\frac{\pi}{2}\}$, and m counts it. ii) there is an additional frequency (f_i) that enables a continuous phase shift over time. ϕ_i represents the baseband signal phase.

$$\begin{aligned} & I(nT_s) + j * Q(nT_s) \\ & = \pm sin(\pi \frac{nT_s}{2T_c} + \frac{m\pi}{2}) \pm j * sin(\pi \frac{nT_s - T_c}{2T_c} + \frac{m\pi}{2}) \\ & = e^{j(\pm\pi \frac{nT_s}{2T_c} + \frac{k\pi}{2})} \\ & = e^{j(2\pi f_i(nT_s) + \phi_i)} \\ & m \in \{0, 1\}, k \in \{0, 1, 2, 3\}, \\ & f_i \in \{+\frac{1}{4T_c}, -\frac{1}{4T_c}\}, \phi_i \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \end{aligned} \quad (2)$$

The baseband signal is then transformed into analog using a digital-to-analog converter (DAC). Finally, it is up-converted to radio-frequency (RF), and transmitted through an antenna.

ZigBee Receiver A simplified ZigBee receiver is shown in Fig. 3(b). It is a transmitter reverse engineering. The signal demodulation is based on the sign of phase shift between consecutive chip units. The RF signal is first down-converted to extract the baseband signal $s(t) = I(t) + jQ(t)$. Then, an Analog to Digital Converter (ADC) is used to obtain digital I/Q samples $s(n) = I(n) + jQ(n)$. An IF channel filter takes I/Q samples as input and functions to eliminate out-of-band noise. Finally, a symbol correlator calculates the sign of phase shift sequence between consecutive chip units (T_c) by $sign(arctan(s(n) \times s^*(n-1)))$, where $s^*(n-1)$ denotes the conjugate of $s(n-1)$. The sequence is correlated with that of standard ZigBee symbols. The closest symbol, which has the minimum Hamming distance with the input sequence, is despreaded into a bit stream.

B. Backscatter communication

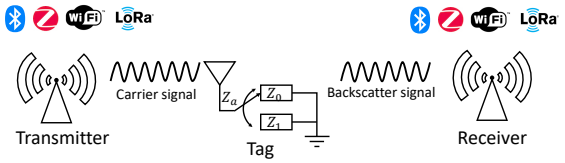


Fig. 4. A conventional backscatter system architecture.

Transforming the LF baseband signal to the RF is power-consuming. An active transmitter takes a local oscillator to produce an internal RF carrier. The baseband signal is mixed with the carrier so that the resulting signal is transformed to the RF and contains baseband information. The process generally consumes tens of milliwatts [5] [6] [7].

Fig. 4 shows a conventional backscatter architecture, which consists of a carrier transmitter, a backscatter tag, and a backscatter receiver. The transmitter provides ambient signals (e.g., Wi-Fi, ZigBee, BLE, LTE, etc.) for the RF carrier, whose expression is shown in Eq. (3). A_c, f_c ,and ϕ_c are the amplitude, phase, and frequency of the carrier. The carrier is reflected when passing across the backscatter circuit. The backscatter tag mixes the carrier with the digital baseband signal by modifying the reflection coefficient ($\Gamma(t)$) [8] [11] [17], which is shown in Eq. (4) and (5). Z_L and Z_a are the load and antenna impedance, respectively. $*$ is the complex-conjugate operator.

$$C(t) = A_c e^{j(2\pi f_c t + \phi_c)} \tag{3}$$

$$\Gamma(t) = \frac{Z_L - Z_a^*}{Z_L + Z_a^*} \tag{4}$$

$$B(t) = \Gamma(t)C(t) \tag{5}$$

In terms of RF carriers, the advanced ZigBee backscatter systems can be classified into two classes: single-tone ZigBee backscatter systems and non-single-tone ZigBee backscatter systems. Non-single-tone ZigBee backscatter systems [11] [17] use codeword translation to piggyback information, which translates the carrier codeword into another codeword from the same codebook. Two receivers are required for the carrier and backscatter demodulation, which increases the deployment cost. Further, the systems are productive-data dependent [15]: the tag data is extracted by comparing the signal differences. When the carrier signal is corrupted, we cannot extract tag data even if the backscatter signal is error-free.

In comparison, a single-tone signal is an excellent candidate for an external RF carrier. It has a constant amplitude, phase, and frequency during the modulation. The resulting signal can only be modified by the RF switch toggling. Thus the backscatter tag is able to produce a signal arbitrarily without knowing the carrier payload, which is attractive for a number of backscatter systems [1] [8] [18].

C. Interscatter design

Interscatter [1] is known for exploiting BLE single-tone to produce PSK-based signals, such as Wi-Fi and ZigBee. The backscatter tag binarizes the baseband operations of active radio and correspondingly generates a square wave sequence. The sequence producing signals with discrete phase shifts is referred as instantaneous phase shift (IPS) modulation in this paper. Specifically, a square wave ($T(t)$) with a constant frequency (Δf) and various phase shifts (ϕ_T, e.g., $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$) is used for RF switch toggling. It can be written as a combination of multiple sinusoidal signals ($\frac{4}{\pi}\sum_{n=1,3,5,7,...}^{\infty}\frac{1}{n}(sin(2\pi n\Delta f t + \phi_T))$). Only the first harmonic is the desired term. Other terms can be canceled out by the receiver channel filter, so that has been crossed out in Eq. (6). The backscatter signal generation ($B(t)$) for Interscatter is shown in Eq. (7).

A_c, f_c, and ϕ_c denote the carrier amplitude, frequency, and phase, respectively. All of them remain constant during the modulation. f_{shift} shifts the backscatter signal to neighbor channels such that avoids carrier interference. ϕ_T denotes the tag bit information, which keeps constant during one chip unit and transfers its state instantly.

$$\begin{aligned} T(t) &= A_T((cos(2\pi f_{shift}t + \phi_T) \\ &\quad + \sum_{n=3,5,7,...}^{\infty}\frac{1}{n}\cancel{cos(2\pi n f_{shift}t + \phi_T)} \\ &\quad + jsin(2\pi f_{shift}t + \phi_T) \\ &\quad + \sum_{n=3,5,7,...}^{\infty}\frac{1}{n}\cancel{jsin(2\pi n f_{shift}t + \phi_T)})) \\ &= A_T e^{j(2\pi f_{shift}t + \phi_T)} \end{aligned} \tag{6}$$

$$\begin{aligned} B(t) &= C(t)T(t) = A_c e^{j(2\pi f_c t + \phi_c)} A_T e^{j(2\pi f_{shift}t + \phi_T)} \\ &= A_c A_T e^{j(2\pi(f_c + f_{shift})t + (\phi_c + \phi_T))} \\ &\phi_T \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \end{aligned} \tag{7}$$

The IEEE 802.15.4 [16] cumulates a phase shift ($+\frac{\pi}{2}$ or $-\frac{\pi}{2}$) every T_c, which contributes to signal demodulation. The blue lines in Fig. 5, modulating part of the ZigBee symbol "0000", show IPS phase shifts on channel $f_c + f_{shift}$.

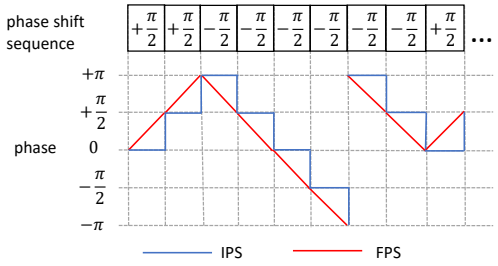


Fig. 5. Phase shift of IPS and FPS.

Specifically, when it comes to modulating $+\frac{\pi}{2}$, IPS introduces a positive phase shift $\phi_{T_i} = \phi_{T_{i-1}} + \frac{\pi}{2}$ instantly to the carrier. And when it comes to modulating $-\frac{\pi}{2}$, a negative phase shift $\phi_{T_i} = \phi_{T_{i-1}} - \frac{\pi}{2}$ is conducted. Since an active ZigBee receiver takes the sign of consecutive phase shifts for signal demodulation, IPS enables receiver-compliant wireless transmissions successfully.

Poor spectrum efficiency However, IPS has poor spectrum efficiency. For example, the waveform of constant phase shifts $(+\frac{\pi}{2}, +\frac{\pi}{2}, +\frac{\pi}{2}, ...)$ on channel $f_c + f_{shift}$ is shown in Eq. (8). It has a $4T$ cycle. Eq. (9) shows the Fourier analysis with infinite terms, that produces serious spectrum sidelobes. The spectrum simulation in MATLAB is shown in Fig. 6(a). It has a signal strength reduction of 15 dBm and 25 dBm on neighbor BLE and ZigBee channels, respectively. It is known that commodity BLE and ZigBee receivers generally have a sensitivity of -97 dBm and -100 dBm [19]. This indicates that the signal strength of IPS must be lower than -82 dBm and -75 dBm to work concurrently with neighbor IoT devices. We deploy an indoor ZigBee backscatter system and measure the signal strength in various locations in Fig. 17. It demonstrates that only 30% and 38% of locations satisfy the requirement. Other devices suffer from poor spectrum efficiency.

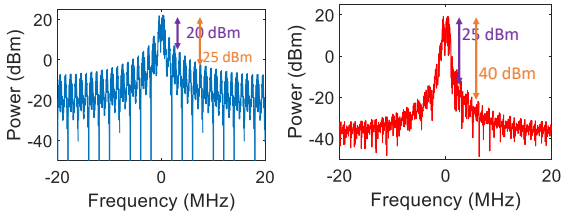
$$s(t) = \begin{cases} e^{j(-\frac{\pi}{2})}, & 4kT \le t < (4k+1)T \\ e^{j(0)}, & (4k+1)T \le t < (4k+2)T \\ e^{j(\frac{\pi}{2})}, & (4k+2)T \le t < (4k+3)T \\ e^{j(\pi)}, & (4k+3)T \le t < (4k+4)T, k \in Z \end{cases} \tag{8}$$

$$= \sum_{k=\pm1,\pm2,\pm3,...} (\frac{1}{j2k\pi}(1+2sin^2(\frac{k\pi}{2})e^{-j\frac{k\pi}{2}})e^{j(\frac{k\pi}{2T})t} + \frac{1}{2k\pi}(1+2sin^2(\frac{k\pi}{2})e^{j(-\frac{k\pi}{2})})e^{k\frac{\pi}{2T}(t-T)}) \tag{9}$$

III. SYSTEM DESIGN

We introduce a novel modulation to improve the backscatter spectrum efficiency. In this section, we first present the modulation design and then show its practical application for ZigBee backscatter. Commodity ZigBee radios provide carriers consisting of a non-single-tone header and single-tone payload. The tag leverages single-tone for reliable data transmission. It also recycles the non-single-tone header using sub-symbol codeword translation to improve carrier utilization.

A. FPS Design



(a) IPS spectrum (b) FPS spectrum

Fig. 6. IPS and FPS spectrum.

We present a novel modulation that produces continuous phase shifts on neighbor channels. The advantages of producing baseband with continuous phase shifts have been widely demonstrated in literature [20] [21]. A continuous phase shift helps to suppress spectrum sidelobes while the neighbor channel communication eliminates carrier interference. Specifically, it takes a square wave with various frequencies $(f_{shift} \pm f_{FP})$ and phases (ϕ_T) for the RF switch toggling. The RF switch toggling parameterized with frequencies and phases is denoted as FPS modulation. Its expression is shown in (10), where the first component is the desired term and the others can be eliminated by the receiver channel filter. Further, the backscatter signal generation is shown in (11).

$$\begin{aligned} T(t) &= A_T((cos(2\pi(f_{shift}+f_{FP})t+\phi_T) \\ &+ \sum_{n=3,5,7,...}^{\infty} \frac{1}{n} cos(2\pi n(f_{shift}+f_{FP})t+\phi_T) \\ &+ jsin(2\pi(f_{shift}+f_{FP})t+\phi_T) \\ &+ \sum_{n=3,5,7,...}^{\infty} \frac{1}{n} jsin(2\pi n(f_{shift}+f_{FP})t+\phi_T))) \\ &= A_T(cos(2\pi(f_{shift}+f_{FP})t+\phi_T) \\ &+ jsin(2\pi(f_{shift}+f_{FP})t+\phi_T)) \\ &= A_T e^{j(2\pi(f_{shift}+f_{FP})t+\phi_T)} \end{aligned} \tag{10}$$

$$\begin{aligned} B(t) &= C(t)T(t) \\ &= A_c e^{j(2\pi f_c t+\phi_c)} A_T e^{j(2\pi(f_{shift}+f_{FP})t+\phi_T)} \\ &= A_c A_T e^{j(2\pi(f_c+f_{shift}+f_{FP})t+(\phi_c+\phi_T))} \end{aligned} \tag{11}$$

- f_{FP} is introduced to describe the rate of phase shift over time, i.e., $f_{FP} = \frac{\Delta\phi}{2\pi\Delta T}$. Toggling an RF switch at a frequency (f_{FP}) over ΔT indicates that the backscatter signal achieves a phase shift $(2\pi f_{FP} * \Delta T = \Delta\phi)$. Specifically, when it comes to modulating phase shift $(\phi_T \to \phi_G)$ over T_c, the backscatter signal is set to have a frequency deviation $(f_{FP} = \frac{\phi_G - \phi_T}{2\pi T_c})$ on the basis of phase ϕ_T.
- f_{shift} functions to eliminate carrier interference. It backscatters signals to neighbor communication channels such that the receiver channel filter helps to suppress out-of-band noise (including signals on the carrier channels).

Further, f_{shift} is generally much higher than a baseband modulation frequency, which avoids the failure of RF switch impedance toggling. For example, when it comes to modulating ZigBee, f_{shift} can be set to 5 MHz, whose signal cycle is calculated as $0.2\mu s$ (t_2). $\frac{t_2}{2} \ll T_c$ indicates a success of backscatter signal generation.

The red lines in Fig. 5 show FPS phase shifts on channel $f_c + f_{shift}$ to modulate ZigBee, which is continuous between consecutive chip units. Specifically, when it comes to modulating $+\frac{\pi}{2}$ on the basis of ϕ_0, we set the frequency deviation to be $f_{shift}+f_{FP} = f_{shift}+\frac{\pi}{2(2\pi T_c)}$ and $\phi_T = \phi_0$. Both of them keep constant over T_c. Similarly, if we want to modulate $-\frac{\pi}{2}$ on the basis of ϕ_1, the frequency deviation is $f_{shift} - f_{FP} = f_{shift} - \frac{\pi}{2(2\pi T_c)}$ and $\phi_T = \phi_1$.

Spectrum efficiency FPS produces signals with phase continuity. The continuous phase shift helps to reduce the spectrum sidelobes, which improves the spectrum efficiency. For example, when it comes to modulating the waveform of continuous phase shifts (in Eq. (12)) on channel $f_c + f_{shift}$, FPS has a single Fourier term in Eq. (13), which greatly suppresses the spectrum sidelobes compared with Eq. (9). For ZigBee transmissions, FPS has a spectrum simulation shown in Fig. 6(b). The signal strength decreases over 25 dBm and 40 dBm on neighbor BLE and ZigBee channels. To avoid interference on neighbor IoT channels (e.g., ZigBee, BLE), the signal strength of FPS must be no more than -72 dBm and -60 dBm, respectively. Our measurements shown in Fig. 17 demonstrate that over 50% and 95% of locations satisfy this requirement. Section V evaluates the backscatter spectrum of FPS-enabled ZigBee transmissions. Further, the signal strength decreases over 60 dBm at a frequency distance of 20 MHz. We believe that FPS is a brilliant candidate to improve the spectrum efficiency for backscatter communications.

$$s(t) = \begin{cases} e^{j(\frac{\pi}{2T}t - \frac{\pi}{2})}, & 4kT \le t < (4k+1)T \\ e^{\frac{\pi}{2T}t + j(0)}, & (4k+1)T \le t < (4k+2)T \\ e^{j(\frac{\pi}{2T}t + \frac{\pi}{2})}, & (4k+2)T \le t < (4k+3)T \\ e^{j(\frac{\pi}{2T}t + \pi)}, & (4k+3)T \le t < (4k+4)T, k \in Z \end{cases} \tag{12}$$

$$= e^{j(\frac{\pi}{2T}t)} \tag{13}$$

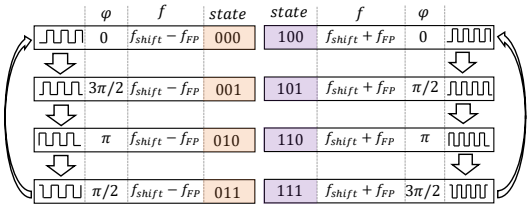


Fig. 7. FPS state machine.

State machine FPS-based ZigBee transmissions consist of a sequence of phase shifts. It requires scheduling multiple square waves for the backscatter signals generation. We first produce square waves with two groups of frequencies ($\{f_{shift}+f_{FP} = f_{shift}+\frac{\pi}{2(2\pi T_c)}, f_{shift}-f_{FP} = f_{shift}-\frac{\pi}{2(2\pi T_c)}\}$) and design a state machine to get their states transformation, which is shown in Fig. 7. All of them are pending for the RF switch toggling. Group one is marked with "0xx" and group two is "1xx". The first bit represents the sign of frequency deviation subtracted by f_{shift} while the others represent their phase states. Fig. 7 specifies their mapping rules in detail. Further, a toggling signal transfers its state due to the integral of frequency deviation ($\pm f_{FP} = \pm\frac{\pi}{2(2\pi T_c)}$) over T_c.

To select the right toggling signal, our tag first picks the signal group according to the sign of frequency deviation. Then, a toggling signal in the group is selected based on the backscatter signals phase state transformation. For instance, to backscatter the ZigBee symbol "0000" in Fig. 5, our tag first enables a toggling signal noted with "100" to produce a frequency deviation $f_{shift}+f_{FP}$ at an initial phase 0. For the next chip unit, a signal noted with "101" produces a frequency deviation $f_{shift} + f_{FP}$ on the basis of phase $\frac{\pi}{2}$. Further, a signal noted with "010" is used to modulate a frequency deviation $f_{shift} - f_{FP}$ at a phase of π.

B. Single Tone Generation

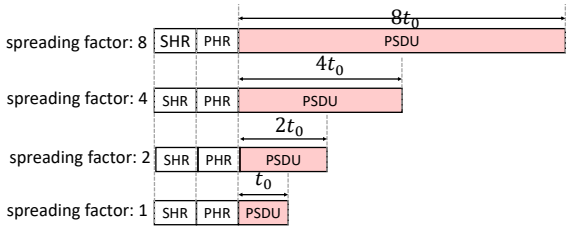


Fig. 8. Spreading factors and packet length for ZigBee transmissions.

We apply FPS for the first time to build a novel ZigBee backscatter system in the crowded spectrum. As shown in Fig. 2, our system consists of a commodity ZigBee transmitter, a ZigBee backscatter tag, and a commodity ZigBee receiver. The transmitter provides the tag with an ambient ZigBee carrier. The FPS-based backscatter tag modulates the carrier to produce ZigBee. The receiver is able to demodulate the backscatter signal without any modification. In the section, we show the details of ZigBee carrier generation. We follow the basic idea of Interscatter [1], which provides the tag a single-tone carrier using a commodity BLE. The advantages of single-tone carriers have been shown in the preliminaries. Differently, our system in Fig. 2 takes ambient ZigBee transmissions to enable single-frequency tones, which is more preferred to work in a native ZigBee network.

ZigBee generation shown in (1) indicates that a specified chip sequence has the possibility of generating a single-tone. When we specify branch I with "101010..." (i.e., $I(t) = cos(2\pi ft)$) and branch Q with "101010" (i.e., $Q(t) = sin(2\pi ft)$), their combination produces a positive single-tone: $s(t) = I(t) + jQ(t) = cos(2\pi ft) + jsin(2\pi ft) = e^{j2\pi ft}$. Also, branch I specified with "101010..." (i.e. $I(t) = cos(2\pi ft)$) and branch Q with "01010..." (i.e. $Q(t) =$

$-sin(2\pi ft)$) produce a negative single-tone: $s(t) = I(t) + jQ(t) = cos(2\pi ft) - jsin(2\pi ft) = e^{-j2\pi ft}$. Unfortunately, ZigBee radios adhere to IEEE 802.15.4 [16] generally take DSSS to spread every four bits into one of the 32-chip PN sequences, whose spreading factor is 8. It specifies chip sequences constantly and none of them satisfy our needs.

We are pursuing ZigBee radios that do not strictly adhere to the IEEE 802.15.4, but are capable of transmitting single-tone. Our survey shows that Microchip Technology produces ZigBee radios (e.g., ATMEGA256RF2, AT86RF233, AT86RF231, etc.) that support various spreading factors for data rate control. As shown in Fig. 8, ZigBee packets comprise a synchronization header (SHR, which does synchronization for packets), a PHY header (PHR, which defines the number of data bits in PSDU), and a PHY service data unit (PSDU, which carries the data bits). The spreading factors of SHR and PHR are determined with 8, whereas PSDU supports multiple spreading factors (1,2,4,8). When the spreading factor is set to 1, one bit is spread into one chip unit. It indicates that we are capable of producing chip sequences arbitrarily. Further, our investigations show that when the scrambling register (SOFT_MODE) in the low spreading factor modes is disabled, a bit "0" represents a negative frequency deviation (-500 kHz), and a bit "1" represents a positive frequency deviation ($+500$ kHz). PSDU filled with a constant "0" or "1" produces a single-tone working at ± 500 kHz from the central frequency.

In conclusion, we use commodity radios to transmit ZigBee carriers consisting of a non-single-tone header (SHR+PHR) and a single-tone payload. Our tag is expected to adhere to IEEE 802.15.4 packets, which is the PHY layer of all ZigBee radios. It is notable that the single-tone transmitter can also be replaced by other single-tone transmitters (e.g., BLE), which doesn't affect the FPS modulation. The carrier has an IEEE 802.15.4 compliant header whereas the payload is eight times lower than that of IEEE 802.15.4. Transmitting packets with the same PHR, the IEEE 802.15.4 has a payload length of $8t_0$ while the carrier is t_0. An intuitive idea, simply modulating the single-tone carrier, is popular with advanced systems (RBLE [15], Interscatter [1]). The idea is easy to deploy whereas causes a waste on the non-single-tone carrier. Directly reusing the carrier PHR randomizes the demodulation for the remaining $7t_0$.

C. Codeword Translation

To maximize carrier utilization, a sub-symbol codeword translation on the non-single-tone carrier is attractive to deploy on our tag. It recycles the carrier header by re-customizing it into another. The carrier header information is pre-communicated to our tag through ON-OFF keying.

Codeword translation As shown in Fig. 9, the RF carrier ($E(t) = e^{j(2\pi f_e t + \phi_e)}$) follows the expression shown in (2), where $f_e = f_c \pm f_i$ and $\phi_c \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. f_c is the carrier central frequency. To transmit symbols ($B(t) = e^{j(2\pi f_B t + \phi_B)}$) on channel $f_c + f_{shift}$, our tag implements a sub-symbol (i.e., chip) level codeword translation without damaging the symbol

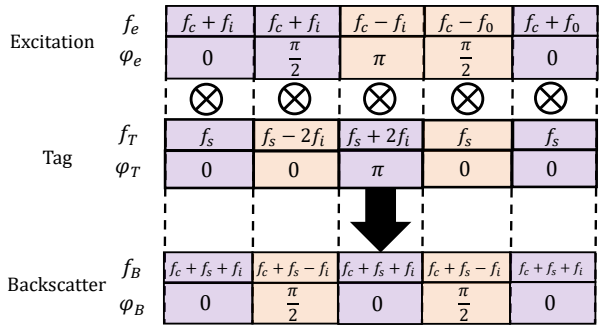


Fig. 9. Codeword translation for non-single-tones.

structure. Specifically, a toggling signal ($T(t) = e^{j(2\pi f_T t + \phi_T)}$) is determined by the difference in frequencies and phases between the carrier and backscatter chip units, i.e., $T(t) = B(t) * E^{'}(t) = e^{j(2\pi(f_B - f_e)t + (\phi_B - \phi_e))}$. To translate one chip $e^{j(2\pi f_e t + \phi_e)}$ into $e^{j(2\pi f_B t + \phi_B)}$, the toggling signal is parameterized with $f_T = f_B - f_e$ and $\phi_T = \phi_B - \phi_e$. Since each ZigBee symbol consists of a sequence of chips, our design works for carrier utilization improvement.

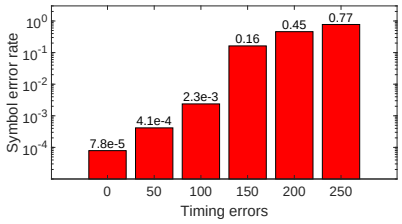


Fig. 10. Timing error analysis.

Synchronization The sub-symbol level codeword translation requires a toggling signal to synchronize with an RF carrier. We first simulate the backscatter operations on the tag to investigate the synchronization requirements. We use USRP N210 working at 20 MSPS to get active ZigBee radios I/Q samples. Then, we impose frequencies and phase shifts on the I/Q samples to emulate the codeword translation, which follows the principle discussed before. Further, an incremental synchronization error from -250 ns to 250 ns is introduced to the digital I/Q samples. The processed samples are retransmitted through the antenna. Commodity ZigBee receivers (CC2650) assess symbol error ratio (SER). As shown in Fig. 10, synchronization errors of up to $\pm$ 100 ns will not lead to significant BER degradation. Envelope detectors are popular in estimating the excitation signal' s arrival, which set a threshold on the amplitude for signal detection. We take AD8313 in our prototype, whose response time is 40 ns in theory. In our implementation, we evaluate that over 50% synchronization errors are limited to 100 ns, which is acceptable for our synchronization requirements.

Backscatter tag receiver design We adopt ON-OFF keying to decode the carrier instructions, which follows the design shown in [8]. Specifically, a high amplitude at a length of L_1 is decoded as a bit "1" and a low amplitude at a length of L_0 is decoded as a bit "0". We design a packet structure, consisting of a synchronization header, a PHY header, and PHY service data unit (follows the structure in IEEE 802.15.4), to modulate the carrier instructions.

IV. IMPLEMENTATION

ZigBee transceiver We adopt an ATMEGA256RF2 radio [22] for carrier transmission and an off-the-shelf TI CC2650 for ZigBee reception. The transmitter sets the spreading factor to be 1 and fills the payload with a constant "0"s to generate a negative single tone, whose frequency is -500 kHz from the central frequency. Its PHR is filled with 127 and supports a $127(bytes) * 8(bits) * 0.5(\mu s) = 508\mu s$ single-tone. The transmission power is set to 4 dBm and the packet rate is 100 packets/s. For simplicity, the transmitter works on ZigBee channel 12 (i.e., 2410 MHz) constantly in our evaluations. The backscatter tag produces IEEE 802.15.4 packets, which is the PHY layer of all ZigBee radios. Our receiver can use commodity ZigBee devices without any software or hardware alternation. Fig. 11(a) shows a real picture of the ZigBee transmitter (in the left), ZigBee receiver (in the right), and backscatter tag (in the middle).

Backscatter tag Our tag prototype consists of an RF front-end circuit and an FPGA, which follows the mainstream backscatter tag design [8] [23] [11] [1]. The RF front-end circuit includes an envelope detector and an RF switch. The envelope detector is AD8313 [24]. Its output is connected to a comparator, which functions to eliminate noise and sets a threshold for downlink instructions decoding. The RF switch is composed of ADG902 [25]. It has different impedance and can be controlled by an FPGA output for backscatter signals generation. We take XILINX ZYNQ 7000 for baseband processing and modulate the signal on ZigBee channel 14 (i.e., 2420 MHz), where the frequency shift (f_{shift}) is set to 10 MHz.

Deployment cost The RF switch consumes 1.8 mW and the detector is 78 mW. The prototype FPGA for different modulations has a resource utilization in TABLE I. IPS requires four square waves with a constant frequency and four phases for the RF switch toggling. FPS requires eight square waves split into two groups. Each group has a constant frequency and four phases. FPS consumes more hardware resources than IPS. Further, the FPGA power simulation is shown in TABLE II. FPS improves spectrum utilization and power consumption at the same time. In contrast, Interscatter [1] builds an IC prototype, which consumes 8.51 μW for the baseband signal generation, 9.79 μW for the backscatter modulator, and 28 μW in total. It benefits from the miniaturization following Moore's law. Our prototype consists of off-the-shelf components. It is built to validate the system's effectiveness.

Experiment setup Our experiment setup is shown in Fig. 11(b). Our tag works in line-of-sight (LOS) scenarios and non-line-of-sight (NLOS) scenarios. The distance between the carrier transmitter and the backscatter tag is fixed at 5 cm. We move a commodity ZigBee receiver gradually away from our tag and evaluate the system performance.

TABLE I
RESOURCE UTILIZATION

	Slice LUTs	Slice Registers	BUFGCTRL	MMCME2_ADV
FPS	171	57	9	1
IPS	168	54	5	1

TABLE II
POWER ANALYSIS

	Signals	Clocks	Logic	MMCM	Total
FPS	$1mW$	$1mW$	$1mW$	$121mW$	$124mW$
IPS	$1mW$	$1mW$	$1mW$	$106mW$	$109mW$

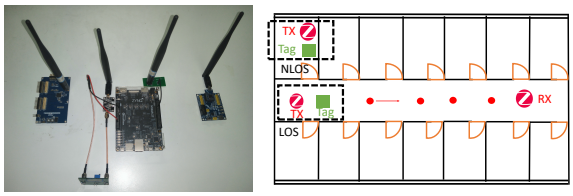
V. EVALUATION

A. Single tone generation

We first evaluate the single-tone carrier transmitted by a commodity ZigBee radio (ATMEGA256RF2). Its exposed antenna is first connected to a PXIe-5663 RF Vector Signal Analyzer (VSA), which shows the carrier spectrum. The carrier packet is filled with a constant "0"s or "1"s. Fig. 12(a) and (b) show that their frequency deviation is $\pm$500 kHz from the central frequency, which follows the expression in (1).

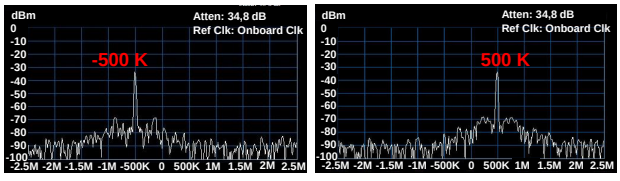
B. Spectrum efficiency

We evaluate the bandwidth of different modulations. A PXIe-5663 RF Vector Signal Analyzer is used to measure the occupied bandwidth containing over 99% RF energy. A commodity ZigBee radio (ATMEGA256RF2) transmits IEEE 802.15.4 packets continuously. Our tag takes single-tone carriers to transmit packets with IPS and FPS. Fig. 13 shows their occupied bandwidth. A commodity ZigBee radio has a bandwidth of 2.38 MHz. IPS has a bandwidth of 8.41 MHz,



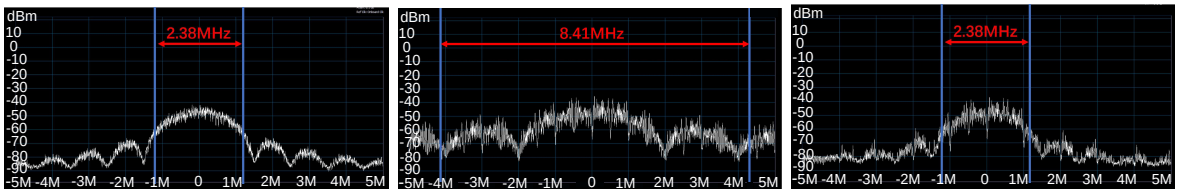
(a) System prototype. (b) LOS and NLOS deployment.

Fig. 11. Experiment setup.



(a) PSDU="000..." (b) PSDU="111..."

Fig. 12. The spectrum of single-tone carriers.



(a) Commodity ZigBee radio (b) IPS modulation (c) FPS modulation

Fig. 13. Frequency spectrum of commodity ZigBee radios, IPS, and FPS modulation.

which is 3.5x greater than the active radio. FPS occupies a bandwidth of 2.38 MHz, which is the same as active radios. Bandwidth efficiency is $\eta_B = R/BW$, where R denotes the chip rate. Since the ZigBee chip rate of 2 Mchip/s, the bandwidth efficiency of IPS and FPS are calculated as 0.23 bps/Hz and 0.84 bps/Hz, respectively. FPS has a bandwidth efficiency improvement of 3.5x over IPS.

C. Communication performance

We evaluate the system performance in both LOS and NLOS scenarios. Fig. 14 and 15 show the Goodput (calculates the throughput of packets with correct CRC checksum), Bit Error Ratio (BER), and Received Signal Strength Indicator (RSSI), respectively.

We also evaluate Interscatter design, whose basic idea is to generate a BLE advertising single-tone carrier. However, a normal BLE advertising packet can only build a $31(bytes) * 8(bits) * 1(\mu s) = 248\mu s$ single-tone, which is unable to support a complete ZigBee packet with a minimum length of 288 μs (SHR+PHR+Payload (1 byte) +CRC). Instead, we use the BLE advertising extension packets transmitted by Nordic nRF52840 to produce a maximum length of $60(bytes)*8(bits)*1(\mu s) = 480\mu s$ single-tone carrier. Its non-single-tone is calculated as $20(bytes)*8(bits)*1(\mu s) = 160\mu s$ and supports 75 % ($\frac{480}{160+480}$) carrier utilization in theory. The BLE transmitter is set to 8 dBm and working at 2410 MHz constantly.

1) LOS: As shown in Fig. 14(a), the uplink distance of our tag can be extended over 17 meters and the maximum goodput achieves 16.6 kbps. The carrier has a non-single-tone header of 192 μs and a single-tone PSDU of 508 μs, whose channel capacity is calculated as 16.8 kbps and represented as red lines in the figure. The goodput of our tag has utilization of over 98% on the carrier. Without codeword translation on the non-single-tone header, the tag has a maximum carrier utilization of 72% in theory. Further, the BLE carrier (non-single-tone header + single-tone payload) provides Interscatter with a channel capacity of 7.8 kbps. Its maximum goodput achieves 5.76 kbps. Fig. 14(b) and (c) evaluate the BER and PER for our system. The BER doesn't exceed 10^{-2} till 14 meters and gradually increases to 1.3% when the uplink distance is 17 meters. The RSSI decreases from -60 dBm to -70 dBm. In contrast, Interscatter seems to have worse performance, which may contribute to the reduced signal strength.

2) NLOS: Fig. 15 shows the performance of our tag working on the NLOS scenarios. The carrier transmitter and our tag are put in a separate room. There is no direct path to propagate wireless signals such that the signal quality decreases. Fig. 15(a) evaluates the system goodput. The uplink distance can be extended to 14 meters and its goodput achieves 3.3 kbps. It can be observed that the goodput of FPS decreases to 0.8 kbps till 12 meters. Fig. 15(b) shows that the BER doesn't exceed 10% within 14 meters. Fig. 15 (c) shows the RSSI variance when the uplink distance increases. In contrast, the performance of Interscatter working on the BLE single-tone is similar to our tag.

D. IPS vs FPS

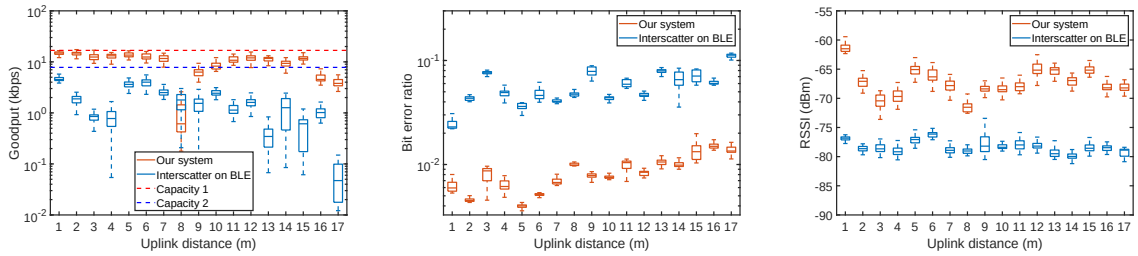
We use IPS and FPS to modulate ZigBee single-tone. Fig. 16 show the performance of different modulations. When their signal strength is similar to each other, the system has a similar performance. Fig. 16 (a) shows the BER performance and Fig. 16 (b) shows the RSSI performance. In the evaluation, we show that the BER of different modulations is similar to each other.

E. Signal strength

Our tag takes a single-tone carrier for signal excitation and adopts two modulation technologies (i.e., IPS and FPS) for the backscatter packet generation. The tag is placed at different locations and its distance from the excitation source is gradually increased from 1 meter up to 20 meters. Fig. 17 shows their signal strength distribution, respectively. It demonstrates that the backscatter signal strength can be over -60 dBm for practice. Half of the signal strength distribution can be over -70 dBm.

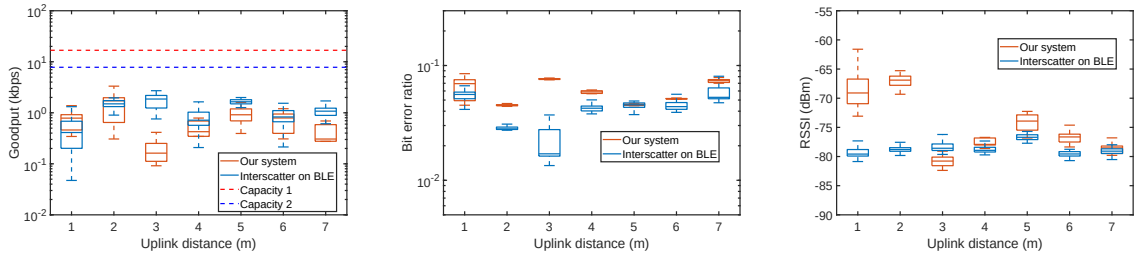
F. Interference on neighbor devices

Interference on BLE Bluetooth Low Energy (BLE) [26] operates in the 2.4 GHz band over 40 channels with a bandwidth of 2 MHz. One pair of BLE connections is used to investigate the effect of different modulation technologies (IPS and FPS modulation) on neighbor BLE devices. A BLE transmitter (CC2650) is working at 0 dBm and the transmission rate is 16 packets/s. Our tag has been put neighbor to the BLE receiver (CC2650) and their distance is fixed at 0.5 meters. Then, the communication distance between the pair of BLE transceivers is gradually increased in a straight line along the hallway. IPS modulation occupies a bandwidth of 8.41 MHz. It affects neighbor four BLE channels which are symmetrical around the central frequency of the IPS-enabled ZigBee channel. FPS modulation concentrates its energy at



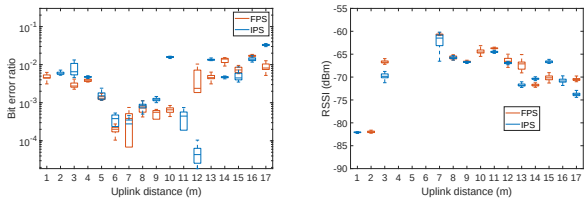
(a) Goodput (b) BER (c) RSSI

Fig. 14. Backscatter Goodput, BER, and RSSI in the LOS deployment.



(a) Goodput (b) BER (c) RSSI

Fig. 15. Backscatter throughput, BER, and PER in the NLOS deployment



(a) BER (b) RSSI

Fig. 16. The performance comparison of IPS and FPS.

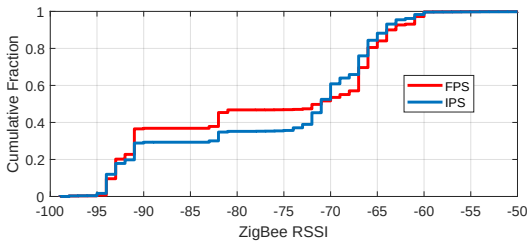


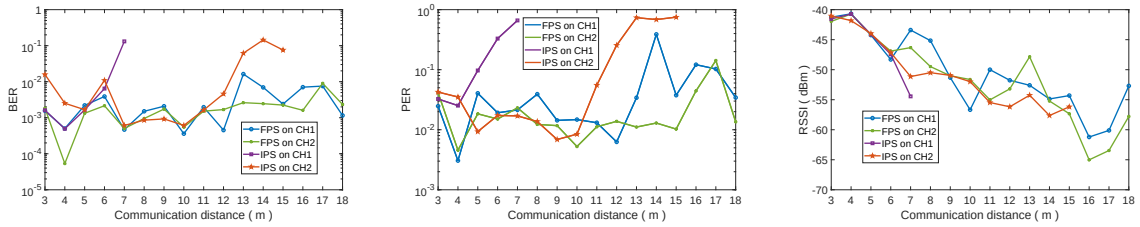
Fig. 17. CDF of backscatter signal RSSI.

2.38 MHz. When our tag backscattering packets on ZigBee channel 2420 MHz, BLE transceivers are set to work on neighbor two BLE channels for evaluation, where we denote 2422 MHz as channel 1 (CH1) and 2424 MHz as channel 2 (CH2).

Fig. 18(a) shows the BER comparison for neighbor BLE devices. It shows that BLE devices working on CH1 greatly suffer from IPS poor spectral efficiency. Its BER exceeds 10% at a communication distance of 7 meters. Besides, BLE devices working on CH2 have a communication distance limitation of 15 meters. Its BER exceeds 10% when the distance exceeds 14 meters. Further, BLE devices working on CH1 and CH2 have a BER of no more than 1% when the communication distance reaches 18 meters. Our analysis demonstrates that IPS modulation affects the performance of neighbor BLE devices even if they are working on other BLE channels. Fig. 18(b) shows the Packet Error Ratio (PER) comparison for neighbor BLE devices. Fig. 18(c) shows their RSSI degradation with the communication distance increasing.

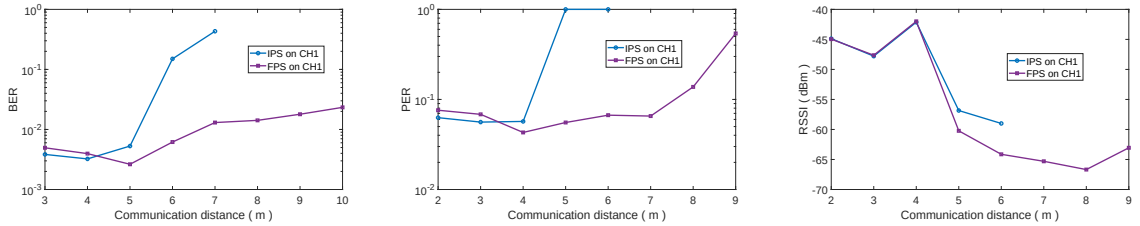
Interference on ZigBee ZigBee has a channel bandwidth of 5 MHz. We investigate the effect of different modulation technologies on the neighbor ZigBee connections. Our tag is set to backscatter ZigBee packets on 2420 MHz. One pair of ZigBee transceivers is set to communicate on the neighbor ZigBee channel (2425 MHz, denoted as CH1). The distance between the backscatter tag and the ZigBee receiver (CC2650) is fixed at 0.5 meters. The ZigBee transmitter (CC2650) is working at 0 dBm and the transmission rate is set to be 9 packets/s. We gradually move the transmitter away from the ZigBee receiver.

Fig. 19(a) shows the BER comparison of neighbor ZigBee devices suffering from different modulation technologies. When the tag transmitting packets with IPS modulation, ZigBee devices working on CH1 have a communication distance of 7 meters. Their BER exceeds 10% at a distance of 6 meters. It indicates that ZigBee connections suffer from IPS spectrum inefficiency greatly. In comparison, ZigBee devices working with FPS-enabled transmissions have a communication distance of over 10 meters. Further, their BER will not exceed 1% till 6 meters.



(a) BER (b) PER (c) RSSI

Fig. 18. BER, PER, and RSSI of neighbor BLE devices



(a) BER (b) PER (c) RSSI

Fig. 19. BER, PER, and RSSI of neighbor ZigBee devices

Fig. 19(b) shows the PER comparison of neighbor ZigBee devices. When the tag transmits packets with FPS modulation, the throughput stays at 250 kbps till 15 meters. However, when the tag adopts IPS mode, the communication distance is limited to 10 meters. Fig. 19(c) shows their RSSI with an increasing communication distance. Our analysis above demonstrates that IPS introduces a great effect on neighbor ZigBee devices while FPS enables a novel way to co-exist in a crowded spectrum.

VI. Discussion

Carrier transmission Backscatter tags leverage various RF signals ([27], [15], [28], [17], [29], [30], [31], [32], [33], [11]) for excitation carrier. RBLE [15] takes ubiquitous BLE radios for excitation carriers and builds a reliable BLE connection, whose communication distance can be extended to 56 meters in an outdoor environment. LScatter [27] leverages continuous LTE ambient traffic to modulate information, and the throughput achieves 13.63 Mbps. FreeRider [11] leverages ambient 802.11g/n Wi-Fi, ZigBee and Bluetooth for excitation carrier.

Modulation technologies The state-of-art (SoA) backscatter systems adopt various modulation technologies to transmit bit stream ([10], [11], [34], [35], [32], [36], [37], [38], [39], [40], [41]). FM backscatter [10] takes 2-FSK to modulate ambient FM signals at a rate of 100 bps. Specifically, two different frequencies are used to represent bits “0” and “1”. It also uses a combination of 4-FSK and frequency division multiplexing to enable a higher data rate (1.6 kbps and 3.2 kbps). IBLE [35] takes GFSK to modulate information, whose Packet Error Ratio (PER) achieves 0.04% at the uplink distance of 2 meters. It takes RF switch control to emulate the GFSK phase shift and shows a bandwidth of 0.678 MHz. By controlling the switching of the finite state RF switch, we can change the bandwidth of each harmonic of the backscattered signal, but we cannot eliminate other harmonics besides the primary harmonic. These harmonics, although lower in energy than the primary harmonics, may interfere with other channels. pulseShaping [41] redesigned the RF front-end to eliminate as many harmonics as possible by continuously changing the backscatter wash. In addition, JUDO [40] proposes a low-power RF transmitter mode. It uses a tunnel emitter locally to generate analog baseband signals and RF signals to achieve local mixing in a low-power way, thereby eliminating multiple harmonics with a total system power consumption of 100 microwatts.

Downlink improvement People are concerning the limitation of the transmitter-to-tag distance. There are many possible solutions: Multiscatter [17] improves the carrier signal strength. Passive DSSS [42] transmit carrier with a 20 dB processing gain. Its distance can be extended to 4 meters. All of them can be candidate solutions for the limitation. SyncScatter [43] deploys an RF amplifier on the tag to improve the downlink distance. It reaches a distance of 30+ meters.

VII. Conclusion

In this paper, we propose FPS modulation, which enables backscatter communications with high spectrum efficiency. We also build a novel ZigBee backscatter system to validate the modulation effectiveness. The system uses ZigBee single-tone for RF carrier. Further, a sub-symbol codeword translation is applied to maximize carrier utilization.

VIII. Acknowledgments

We thank the shepherd Jorg Liebeherr and the ICNP reviewers for their helpful comments. This work was supported by NSFC Grant No. 61932017 and 61971390.

REFERENCES

[1] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *Proc. of ACM SIGCOMM*, 2016.

[2] Yi Sun, Jie Liu, Keping Yu, Mamoun Alazab, and Kaixiang Lin. Pmrss: privacy-preserving medical record searching scheme for intelligent diagnosis in iot healthcare. *IEEE Transactions on Industrial Informatics*, 18(3):1981–1990, 2021.

[3] Aditya Gaur, Bryan Scotney, Gerard Parr, and Sally McClean. Smart city architecture and its applications based on iot. *Procedia computer science*, 52:1089–1094, 2015.

[4] Mahanth Gowda, Ashutosh Dhekne, Sheng Shen, Romit Roy Choudhury, Lei Yang, Suresh Golwalkar, and Alexander Essanian. Bringing {IoT} to sports analytics. In *Proc. USENIX NSDI*, 2017.

[5] Joshua F. Ensworth and Matthew S. Reynolds. Every smart phone is a backscatter reader: Modulated backscatter compatibility with bluetooth 4.0 low energy (ble) devices. In *Proc. IEEE RFID*, 2015.

[6] A. Zolfaghari and B. Razavi. A low-power 2.4-ghz transmitter/receiver cmos ic. *IEEE Journal of Solid-State Circuits*, 38(2):176–183, 2003.

[7] Marc Tiebout, Hans-Dieter Wohlmuth, Herbert Knapp, Raffaele Salerno, Michael Druml, Mirjana Rest, Johann Kaeferboeck, Johann Wuertele, Sherif Sayed Ahmed, Andreas Schiessl, Ralf Juenemann, and Anna Zielska. Low power wideband receiver and transmitter chipset for mm-wave imaging in sige bipolar technology. *IEEE Journal of Solid-State Circuits*, 47(5):1175–1184, 2012.

[8] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. Passive wi-fi: Bringing low power to wi-fi transmissions. In *Proc. of USENIX NSDI*, 2016.

[9] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proc. ACM IMWUT*, 2017.

[10] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R. Smith, and Shyamnath Gollakota. FM backscatter: Enabling connected cities and smart fabrics. In *Proc. of USENIX NSDI*, 2017.

[11] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. Freerider: Backscatter communication using commodity radios. In *Proc. of ACM CONEXT*, 2017.

[12] Yifan Yang and Wei Gong. Universal space-time stream backscatter with ambient wifi. In *Proc. IEEE PerCom*, 2022.

[13] Lonzhi Yuan, Can Xiong, Si Chen, and Wei Gong. Embracing self-powered wireless wearables for smart healthcare. In *Proc. IEEE PerCom*, 2021.

[14] Qiwei Wang, Si Chen, Jia Zhao, and Wei Gong. Rapidrider: Efficient wifi backscatter with uncontrolled ambient signals. In *Proc. IEEE INFOCOM*, 2021.

[15] Maolin Zhang, Jia Zhao, Si Chen, and Wei Gong. Reliable backscatter with commodity ble. In *Proc. IEEE INFOCOM*, 2020.

[16] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pages 1–320, 2006.

[17] Wei Gong, Longzhi Yuan, Qiwei Wang, and Jia Zhao. Multiprotocol backscatter for personal iot sensors. In *Proc. ACM CoNEXT*, 2020.

[18] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. In *Proc. of ACM IMWUT*, 2017.

[19] Cc2650 datasheet. https://www.ti.com/product/CC2650.

[20] T. Aulin, N. Rydbeck, and C.-E. Sundberg. Continuous phase modulation - part ii: Partial response signaling. *IEEE Transactions on Communications*, 29(3):210–225, 1981.

[21] J. Oetting. A comparison of modulation techniques for digital radio. *IEEE Transactions on Communications*, 27(12):1752–1762, 1979.

[22] Atmega256rf2 datasheet. http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8393-MCU_Wireless-ATmega256RFR2-ATmega128RFR2-ATmega64RFR2_Datasheet.pdf.

[23] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proc. of ACM SenSys*, 2016.

[24] Ad8313 datasheet. https://www.analog.com/cn/products/ad8313.html.

[25] Adg902 datasheet. https://www.analog.com/en/products/adg902.html.

[26] Bluetooth core specifcation, 2019. https://www.bluetooth.com/specifcations/bluetooth-core-specifcations.

[27] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. Leveraging ambient lte traffic for ubiquitous passive communication. In *Proc. ACM SIGCOMM*, 2020.

[28] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: Wireless communication out of thin air. In *Proc. of ACM SIGCOMM*, 2013.

[29] Jia Zhao, Wei Gong, and Jiangchuan Liu. Microphone array backscatter: An application-driven design for lightweight spatial sound recording over the air. In *Proc. ACM MobiCom*, 2021.

[30] Mohammad Hossein Mazaheri, Alex Chen, and Omid Abari. Mmtag: A millimeter wave backscatter network. In *Proc. ACM SIGCOMM*, 2021.

[31] Jia Zhao, Wei Gong, and Jiangchuan Liu. Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In *Proc. ACM MobiSys*, 2020.

[32] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. Aloba: Rethinking on-off keying modulation for ambient lora backscatter. In *Proc. ACM SenSys*, 2020.

[33] Jia Zhao, Wei Gong, and Jiangchuan Liu. X-tandem: Towards multi-hop backscatter communication with commodity wifi. In *Proc. ACM MobiCom*, 2018.

[34] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. Verification and redesign of OFDM backscatter. In *Proc. of USENIX NSDI*, 2021.

[35] Maolin Zhang, Si Chen, Jia Zhao, and Wei Gong. Commodity-level ble backscatter. In *Proc. ACM MobiSys*, 2021.

[36] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. Ofdma-enabled wi-fi backscatter. In *Proc. ACM MobiCom*, 2019.

[37] Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. NetScatter: Enabling Large-Scale backscatter networks. In *Proc. NSENIX NSDI*, 2019.

[38] Zhanxiang Huang and Wei Gong. Eascatter: Excitor-aware bluetooth backscatter. In *Proc. IEEE IWQoS*, 2022.

[39] Yifan Yang, Longzhi Yuan, Jia Zhao, and Wei Gong. Content-agnostic backscatter from thin air. In *Proc. ACM MobiSys*.

[40] Ambuj Varshney, Wenqing Yan, and Prabal Dutta. Judo: Addressing the energy asymmetry of wireless embedded systems through tunnel diode based wireless transmitters. In *Proc. ACM MobiSys*, 2022.

[41] John Kimionis and Manos M. Tentzeris. Pulse shaping: The missing piece of backscatter radio and rfid. *IEEE Transactions on Microwave Theory and Techniques*, 64(12):4774–4788, 2016.

[42] Songfan Li, Hui Zheng, Chong Zhang, Yihang Song, Shen Yang, Minghua Chen, Li Lu, and Mo Li. Passive DSSS: Empowering the downlink communication for backscatter systems. In *Proc. USENIX NSDI*, 2022.

[43] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. Syncscatter: Enabling wifi like synchronization and range for wifi backscatter communication. In *Proc. USENIX NSDI*, 2021.