OFDMA-Enabled Wi-Fi Backscatter

Renjie Zhao
Shanghai Jiao Tong University
rjzhao@sjtu.edu.cn

Fengyuan Zhu
Shanghai Jiao Tong University
jsqdzhufengyuan@sjtu.edu.cn

Yuda Feng
Shanghai Jiao Tong University
fydsjtu15@sjtu.edu.cn

Siyuan Peng
Shanghai Jiao Tong University
pengsi_yuan@sjtu.edu.cn

Xiaohua Tian
Shanghai Jiao Tong University
xtian@sjtu.edu.cn

Hui Yu
Shanghai Jiao Tong University
yuhui@sjtu.edu.cn

Xinbing Wang
Shanghai Jiao Tong University
xwang8@sjtu.edu.cn

ABSTRACT

In this paper, we for the first time demonstrate how to enable OFDMA in Wi-Fi backscatter for capacity and concurrency enhancement. With our approach, the excitation signal is reflected, modulated and shifted to lie in the frequency band of the OFDM subcarrier by the tag; OFDMA is realized by coordinating tags to convey information to the receiver with orthogonal subcarriers concurrently through backscatter. The crux of the design is to achieve strict synchronization among communication components, which is more challenging than in regular OFDMA systems due to the more prominent hardware diversity and uncertainty for backscattering. We reveal how the subtle asychnronization scenarios particularly for backscattering can incur system offsets, and present a series of novel designs for the excitation signal transmitter, tag, and receiver to address the issue. We build a prototype in 802.11g OFDM framework to validate our design. Experimental results show that our system can achieve 5.2-16$Mbps$ aggregate throughput by allowing 48 tags to transmit concurrently, which is 1.45-5× capacity and 48× concurrency compared with the existing design respectively. We also design an OFDMA tag IC, and the simulation and numerical analysis results show that the tag's power consumption is in tens of μW.

MobiCom'19, October 21–25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6169-9/19/10…$15.00
https://doi.org/10.1145/3300061.3300121

CCS CONCEPTS

• **Networks → Wireless local area networks**.

KEYWORDS

OFDMA, backscatter, Wi-Fi

ACM Reference Format:
Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. 2019. OFDMA-Enabled Wi-Fi Backscatter. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom'19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3300061.3300121

1 INTRODUCTION

Recent years have witnessed extensive exploration of Wi-Fi backscatter, which provides wireless connectivity to Internet-of-Things (IoT) devices on tiny energy budget [1–5]. While promising in addressing the power consumption challenge, the existing Wi-Fi backscatter design still remains low network capacity for the following two reasons: First, concurrent transmissions from multiple backscatter devices (tags) incur collisions, for which tags must transmit sequentially [1, 2, 4, 5]; second, the spectrum efficiency is low under the single-carrier modulation scheme, where the transmitting tag exclusively occupies the spectrum resource [3].

The strength of the existing backscatter design is that the peak speed of the single connected tag is high (up to 11Mbps) [3]; however, with the rapid rise of connectivity needs from pervasive IoT applications, the Wi-Fi system itself is moving away from further improving the peak speed with a single device connected, but targets at increasing the rate of data exchange by all users [16–19], where it is more important to support a large number of connected IoT devices featured by short bursts of data [16, 17]. To this end, the next-generation Wi-Fi 802.11ax performs a ground-up reworking of the core multiple access mechanism to realize orthogonal frequency division multiple access (OFDMA).

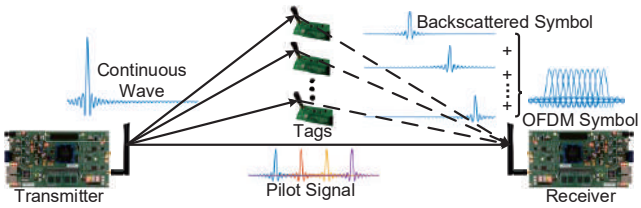

Figure 1: OFDMA backscatter system.

OFDMA is based on the orthogonal frequency division multiplexing (OFDM), which is a *multi-carrier modulation mechanism* adopted by 802.11a/g/n/ac. In contrast to the single-carrier counterpart in 802.11b, OFDM delivers a device's data with multiple orthogonal subcarriers. Due to the orthogonality, the subcarriers' frequency bands can partially overlap thus the overall spectrum efficiency (bit rate per Hz) is higher than that in 11b. With occupying the same Wi-Fi channel, the peak data rate of 11a/g/n/ac is therefore higher than that of 11b. OFDMA however is a *multiple access mechanism*, which enables assigning OFDM subcarriers to different devices at the same time; therefore, the OFDMA system allows many devices to transmit concurrently, and the network capacity (maximum aggregate throughput) is higher than that in systems based on single-carrier modulation.

The adoption of OFDMA in next-generation Wi-Fi indicates that fewer Wi-Fi devices with single-carrier modulation in the core will be used in the future, moreover, almost all of the modern Wi-Fi devices use 802.11g/n based on OFDM [5]; therefore, there is a strong necessity to investigate how to enhance the capacity of the Wi-Fi backscatter system accommodating the multi-carrier modulation mechanism.

In this paper, we for the first time demonstrate how to enable OFDMA in Wi-Fi backscatter. Our design maintains the μW level power consumption on tags, and meanwhile improves the system capacity and transmission concurrency. Specifically, we enable tags to generate backscattered symbols at orthogonal subcarriers' frequencies, which are then synthesized into an OFDM symbol at the receiver, as illustrated in Fig. 1. The OFDMA is realized because the excitation signal transmitter can coordinate the frequency shift in tags, which is equivalent to assigning different subcarriers to different tags.

The crux of any OFDMA system is the effective synchronization mechanism, which is supposed to overcome the time and frequency offsets caused by hardware diversity among communication entities [25, 26]. However, due to the resource indigence of the tag, materializing the concept of OFDMA backscatter as shown in Fig. 1 is confronted with new conundrums. In particular, the excitation signal generator needs to transmit not only the continuous wave (CW), but also other waveforms carrying the OFDM burst preamble and the control information; the tag needs efficient synchronization mechanisms to counteract subtle phase offsets incurred by generating the backscattered symbol; the receiver must be able to decode the synthesized OFDM symbol from the excitation signal transmitter and tags rather than from the single regular OFDM transmitter, which is hindered by asynchronization errors and the inconsistency with the standard OFDM receiver processing.

In addressing the challenges above, we make the following **technical contributions**:

- We present design of the excitation signal transmitter and the receiver to enable OFDMA of tags for Wi-Fi backscatter; we also show how to combine multiple regular OFDMA tags into an enhanced one that can provide higher-rate connectivity (§4).
- We reveal the phase offset issues particularly in the OFDMA backscatter system and provide corresponding calibration techniques as countermeasures (§5).
- We build a hardware prototype of the proposed OFDMA backscatter system in the WARP's 802.11g framework [29]; we also design an OFDMA tag IC for estimating the power consumption (§6).

Comprehensive experiments (§7) are conducted with our prototype and the results show that:

- (Capacity and concurrency) The system can support 48 concurrently transmitting tags with occupying only 1 of the Wi-Fi channels; the aggregate throughput is $5.2Mbps$ with BPSK and 1/2 coding rate, and can achieve up to $16Mbps$ with QPSK and 3/4 coding rate. This is 1.45-5× capacity and 48× concurrency compared with the Wi-Fi backscatter system based on single-carrier modulation [3].
- (Communication range) The transmission range of the regular OFDMA tag in our system can achieve more than $100m$ in the line-of-sight (LOS) setting, with $110Kbps$ data rate using BPSK and 1/2 coding rate. This is 2-3× the maximum range reported in existing designs [3, 4]. The transmission range of the enhanced 4-in-1 OFDMA tag is up to $35m$ at $440Kbps$.
- (Power consumption) The overall power consumption of the OFDMA tag is conservatively estimated to be 18.31-60.06μW, which is in the same order of the existing design [3].

We summarize and answer some FAQs of our work in a report, and we also present a brief demonstration of our system in a video, which are available at [42].

2 PRELIMINARIES

2.1 OFDM in 802.11g

We design and implement the OFDMA backscatter system in the OFDM framework of 802.11g, thus we first highlight the OFDM design in 11g, so that the following discussions in the paper can be understood. The PHY layer of 802.11g allocates the spectrum resource (20MHz bandwidth) of 2.4GHz band to 64 orthogonal subcarriers, where the frequency spacing between any two neighboring subcarriers is $0.3125MHz$. In

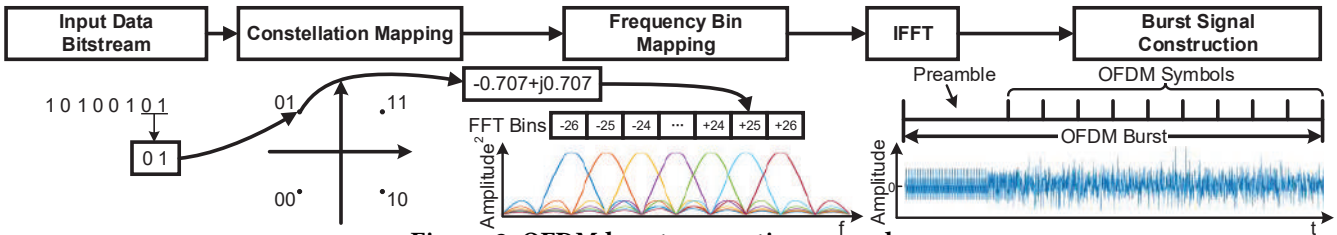

Figure 2: OFDM burst generation procedure.

particular, subcarriers with index ranges [-26:-22 -20:-8 -6:-1 1:6 8:20 22:26] are for data transmission, #-21, #-7, #7, #21 are pilot subcarriers for system calibration, #0 is DC subcarrier not used and the rest 11 are null subcarriers to reduce adjacent channel interference [24].

Suppose there are 48 bits of information to be transmitted by those 48 data subcarriers, if we let each of the subcarriers at different frequencies transmit 1 bit of the information using phase-shift keying (PSK) in a period of T in parallel, then combining those subcarriers in T can generate a time-domain *OFDM symbol* in an analog manner. The 802.11g system uses the similar principle to generate OFDM symbols but in a digital manner leveraging IFFT as shown in Fig. 2.

The input data bitstream after regular processing such as scrambling, coding and interleaving is first divided into groups of n bits, where $n = 1, 2, 4$ and 6 for BPSK, QPSK, 16QAM and 64QAM respectively corresponding to different data rate settings. Consider the QPSK case as shown in Fig. 2, each group of 2 bits is converted into a point in the constellation diagram, which is essentially a complex number in the form of $(I + jQ)$. Such complex numbers are mapped into subcarriers in the frequency domain termed as *FFT bins*.

The FFT blocks are then converted to time domain with IFFT, which become a set of complex time-domain samples representing the sum of those modulated subcarriers. There are 64 such samples from the IFFT output; If we replicate the last $\frac{1}{4}$ of those samples and put the replicated part in the front, then we obtain an 802.11g OFDM symbol, with the replicated 16 samples termed as the *cyclic prefix (CP)*. The obtained signal is clocked at $20Msps$, which yields a $4\mu s$ duration OFDM waveform with the CP duration $0.8\mu s$. The purpose of the CP design in the regular OFDM mechanism is to address the inter-symbol interference (ISI) and the inter-carrier interference (ICI), which are incurred by hardware clock offset and multipath effect; however, we find that the OFDM CP design also provides opportunities to realize OFDMA backscatter, which will be explained in Section 3.

The OFDM symbol generation procedure is repeated to produce symbols from the remaining bits groups in the stream. To complete the OFDM frame structure, those symbols are concatenated and added to a $16\mu s$ preamble, and the obtained signal is termed as an *OFDM burst* ready for transmission, as shown in Fig. 2.

2.2 Challenges

To realize OFDMA backscatter system as conceived in Fig. 1 by utilizing the OFDM framework described above, we have to address the following three particular challenges.

Challenge 1: Calibrating clock offsets. The crux of any OFMDA system is to realize strict synchronization. In the concrete case of OFDMA backscatter, the key is to calibrate clock offsets on the excitation signal transmitter, tags and the receiver, so that those components can agree on the starting point and duration of the OFDM symbol, moreover, maintain the frequency orthogonality of backscattered symbols. In the regular OFDM system without tags, the synchronization can be realized simply using the burst preamble from the transmitter to the receiver. In the OFDMA backscatter system as conceived in Fig. 1, the OFDM symbol at the receiver is factually a combination of backscattered symbols from tags, which naturally contains the tags' clock offsets that are not considered in the regular OFDM framework. Moreover, the on-tag frequency shift operation during backscattering incurs frequency offsets of subcarriers, which potentially impacts the frequency orthogonality.

Challenge 2: Customizing excitation signal. In contrast to existing Wi-Fi backscatter design with the excitation signal contains CW only, the excitation signal for OFDMA backscatter must contain the regular OFDM burst preamble and waveform of control information also.

The burst preamble is to realize tx-rx synchronization regulated in 11g; it is more complex than its counterpart in the single-carrier modulation system such as 11b, because the preamble contains multiple subcarriers' frequency ingredients. It is more practical to preserve the inherent burst preamble of 11g generated by the transmitter, instead of offloading the burden to resource-indigent tags as is done in [3]. Moreover, the excitation signal must be able to convey control messages to tags efficiently, in order to inform the tag the amount of frequency shift and realize tx-tag synchronization. The existing approach with AM modulating the excitation signal as in [3, 7] for control message delivery is infeasible, due to the lack of synchronization design and the low reliability and efficiency.

Further, even if we could somehow enable a regular 11g transmitter to generate the waveform as described above, we still have to appropriately configure the strength of the

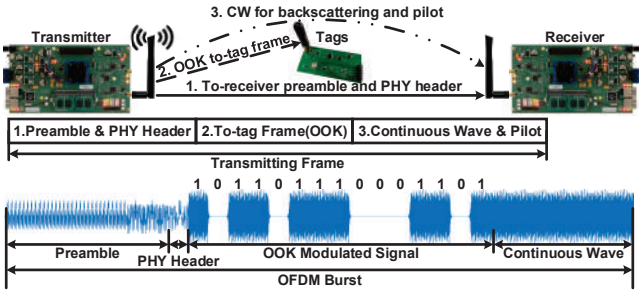

Figure 3: System model.

waveform to accommodate the 11g receiver's automatic gain control (AGC) scheme. In particular, we need to make amplitudes of the preamble and those backscattered symbols comparable, in order to let the 11g receiver process the OFDM burst as it were from the regular OFDM transmitter; however, since amplitudes of the backscattered symbols can not be controlled, we have to configure the amplitude of the CW to influence that of the backscattered symbols.

Challenge 3: Calibrating phase offsets. The tag-rx synchronization mechanism is unavailable in the regular 11g framework. This can incur three kinds of phase offsets in the received signal according to our experimental results, which make the receiver's constellation diagram deformed: 1) The static phase offset is caused by the aggregated backscatter delay and FFT window offset in receiving the OFDM symbol, for which it can be observed that the constellation diagram rotates a fixed degree compared with the ideal one. 2) The continuous dynamic phase offset is incurred by the residual frequency offset, for which we can observe the constellation diagram gradually form a circle. 3) The discrete phase offset is resulted from the square wave phase offset during the on-tag modulation process, for which it can be observed that the constellation diagram rotates several discrete degrees.

3 SYNCHRONIZATION FOR OFDMA BACKSCATTER

Based on the analysis above, we can see that the major challenge for realizing OFDMA backscatter is to synchronize the entire system. In this section, we first present the OFDMA backscatter system model, and then reveal why it is possible to implement the model in the 11g OFDM framework, where we particularly point out the opportunities to realize time and frequency synchronization for OFDMA backscatter.

System model. The OFDMA backscatter system model is shown in Fig. 3. The excitation signal transmitter first reserves the Wi-Fi channel by using request-to-send (RTS) and clear-to-send (CTS) frames as in [3]. After that the transmitter sends a customized frame. The first part of the frame contains the 802.11g preamble for tx-rx synchronization and PHY header; the second part is produced by modulating the CW with OOK, which contains necessary preamble allowing the tx-tag symbol clock synchronization, and control information destined to tags (further discussed in [42]); in the third part, the CW is to be broadcast and backscattered by tags, and the pilot subcarrier is for the receiver to calibrate phase and residual frequency offset with the transmitter. The backscattered symbols from tags are concatenated with the burst preamble and PHY header from the excitation signal transmitter to form a complete OFDM burst at the receiver.

Time synchronization. The CP design in the 11g OFDM framework provides the opportunity to realize time synchronization for OFDMA backscatter. In the regular OFDM system, it may also happen that subcarriers arrive at the receiver in slightly different time points, which potentially incurs ISI and ICI; the CP is to enable the system to tolerate such situation. In the perspective of the receiver, there will be no problem as long as the arrival time points of those subcarriers are within the duration of the CP, no matter if the subcarriers are from the single transmitter or backscattering tags. The CP in 11g is $0.8\mu s$, which is enough to tolerate the time asynchronization caused by backscattering. This will be verified by our experimental results to be shown in Section 7.1.

The excitation signal transmitter sends OOK modulated signal to the tag as shown in Fig. 3, which provides the opportunity to synchronize tx and tags' local clocks. In particular, those clocks can be configured to count the duration of the OFDM symbol equally with the help of tx-to-tag preamble, which will be described in Section 4.2. With the inherent CP design of the 11g OFDM framework and our design of the tx-to-tag synchronization preamble, we could resolve **Challenge 1**, and producing the tx-to-tag preamble is a part of **Challenge 2**.

Frequency synchronization. The model design also provides the opportunity to realize frequency synchronization, which is to deal with the possible frequency offset of the subcarrier incurred when performing frequency shift in the tag. The regular 11g transmitter's RF oscillator works at 2.4GHz, thus the resulted frequency offset could be up to hundreds of kHz even if precision of the oscillator is in tens of *ppm*. This is also the main problem of regular OFDMA system. The frequency offset in the same order still exists between the excitation signal and receiver in OFDMA backscatter, but can be solved by the tx-rx synchronization mechanism. Meanwhile, since the on-tag oscillator works at very low frequency (MHz) compared with the regular OFDM transmitter's RF oscillator, the corresponding frequency offset incurred by frequency shift will not be very high and could be tolerated by 11g's inherent scheme. This will be verified by our experimental results to be shown in Section 7.1.

The missing piece of the puzzle now is the tag-rx synchronization mechanism as described in **Challenge 3**, which will be addressed in Section 5.

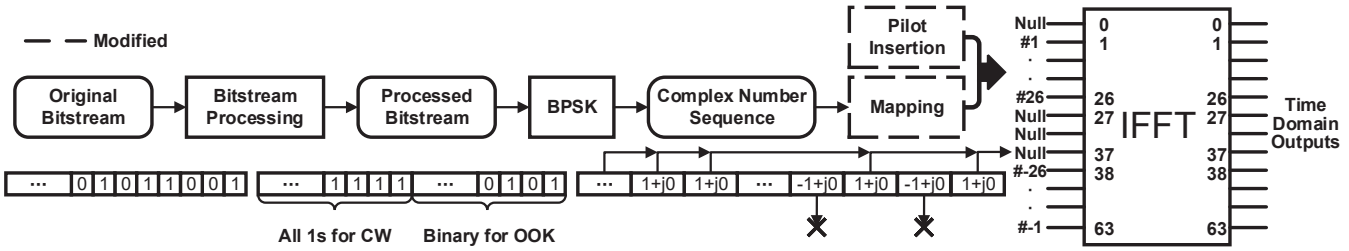

Figure 4: Excitation signal transmitter design.

4 DESIGN

This section presents detailed system design based on the proposed model as shown in Fig. 3. We will make some design decisions based on experimental results, thus we here preannounce the default experiments setup. Experiments are conducted using CHANNEL 1 of the Wi-Fi band in the LOS setting. The transmitter operates at 20dBm, and the tx-tag and the tag-rx distance are 1m and 5m, respectively. The tag is installed with a 2dBi omni-directional antenna. The tag is continuously transmitting $5M$-bit information with fixed length (500 OFDM symbols) with subcarrier #-12 every $10\mu s$. We purposely abandon channel coding and evaluate raw throughput when conducting experiments, in order to make the experiments phenomena more obvious.

4.1 Transmitter Design

We now show how to streamline the regular OFDM transmitter so that the waveform of the excitation signal as shown in Fig. 3 can be generated. In the waveform, the preamble and PHY header can be automatically composed with regular operations of the 802.11g transmitter; therefore, we mainly describe how the CW and the OOK signal are generated, and how the AGC issue can be addressed, where BPSK case is used for convenience of demonstration.

Produce OOK signal and CW. The main procedure of the transmitter is illustrated in Fig. 4, where the dashed-line modules are modified for our purpose. The input bitstream first goes through the bitstream processing module, which includes three kinds of processing in sequence: scrambling, convolutional encoding and interleaving. Our purpose is to compose an appropriate bitstream so that the result after those processing is the target stream for the control signal and CW. We here adopt the smart approach provided by interscatter system to obtain the target stream by appropriately setting the initial state of the scrambler [7].

However, the double-symbol modulation method in [7] is unreliable due to the false peak and glitch effect, which is reluctant to meet the strict synchronization requirement in our system. Therefore, we propose a new approach to customize the excitation waveform by modifying the mapping strategy before IFFT in the 802.11g transmitter, where CW can be generated, and the to-tag frame and control information can be conveyed by modulating the CW with OOK, as illustrated in Fig. 4.

The target bitstream includes the to-tag frame for OOK and all 1-bits for CW, which is transformed into a sequence of complex numbers after BPSK. The bit 1 and 0 in the target stream is transformed into complex numbers $1+j0$ and $-1+j0$, respectively. We then have $1 + j0$ and $-1 + j0$ mapped to subcarrier #-27 with values $1 + j0$ and $0 + j0$ respectively, which realizes OOK modulation. Pilot subcarriers are mapped following regular rules of 802.11g. The rest of subcarriers not being mapped are assigned values 0. In this manner, the target waveform as shown in Fig. 3 can be roughly produced.

How to choose a subcarrier to generate CW? We could use null subcarriers to produce the CW because they convey no payload data. The problem is how to choose the most appropriate one from multiple possible choices. In particular, null subcarriers [-32:-27 27:31] all are candidates. Due to the symmetric distribution of the two sets of null subcarriers in the frequency domain, we just use subcarriers [-32:-27] as an example to demonstrate the phenomena that can be observed when using different subcarriers to produce the CW, based on which we can make the design choice.

We use a WARP v3 board to continuously generate CW with each candidate subcarrier, and an Aglient N9320B spectrum analyzer that is connected to the board with a $1m$ SMA cable to analyze the corresponding spectrum. The spectra of #-31, #-30 and #-27 are illustrated in the first three subfigures of Fig. 5, and that of the subcarriers #-32, #-29 and #-28 are similar thus omitted due to limitation of the space.

It can be seen that there are three peaks in Fig. 5 (a), where peak 1 represents subcarrier #-31 itself, peak 2 is the DC subcarrier leakage, which is caused by DC offset of ADC and local oscillator (LO) leakage, and peak 3 is the replication of peak 1 created by IFFT, where the power is suppressed by the band-pass filter. In Fig. 5 (b), we can see that there are many other spectrum components associated with subcarrier #-30 except for the three peaks, which is caused by symbol phase discontinuity of the CW. In particular, the length of the OFDM symbol ($4\mu s$ in 802.11g) is not always equal to an integer multiple of the subcarrier's period, thus the initial phase of each symbol generated by the subcarrier varies.

Figure 5 (c) is for subcarrier #-27, which looks like Fig. 5 (a); the difference is that the power of peak 3 is lower than that for #-31, which are -10dBm and 15 dBm respectively. This is because peak 3 of #-27 is nearer to the stop-band

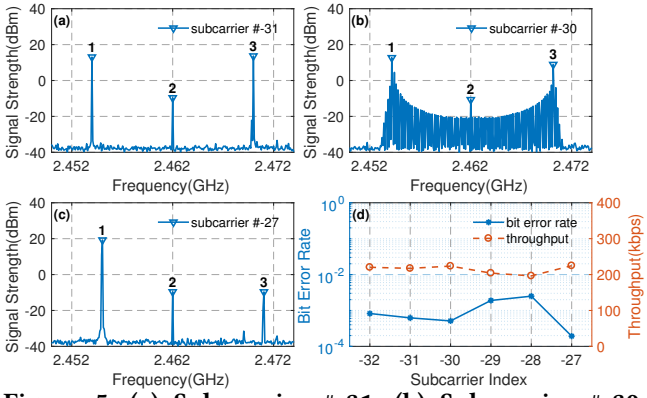

Figure 5: (a) Sub-carrier #-31; (b) Sub-carrier #-30; (c) Sub-carrier #-27; (d) Performance of 2.5MHz frequency shifting tag communication with different subcarriers as the CW.

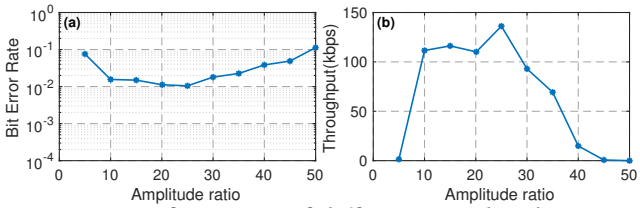

Figure 6: Performance of different amplitude ratios.

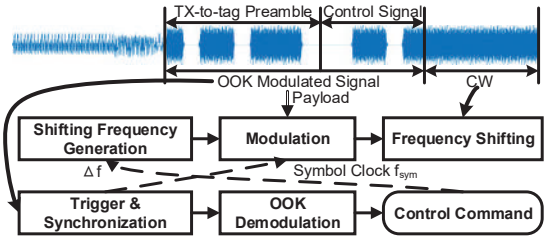

Figure 7: Tag processing.

and suppressed by the transmitter's band-pass filter, which makes #-27 an outstanding candidate for producing the CW. Specifically, the replication of the subcarrier will also be backscattered; if the power of the replication is high, then the backscattered signal could incur potential interference with devices operating on adjacent channels. Although Fig. 5 (b) seems to be a mess in the frequency domain, such structure factually does not impact performance of the backscatter system itself. Figure 5 (d) shows the performance when using different null subcarriers to produce the CW, which indicates that the resulted BER and the throughput do not vary significantly.

In summary, any null subcarrier can be used to produce the CW, but the one with frequency-domain replications created by the IFFT close to the stop-band of the transmitter's band-pass filter can mitigate potential interference caused by backscatter; although the phase discontinuity of subcarriers could incur the seemingly messy spectrum structure, it will not impact the performance of the backscatter system itself.

Configuring amplitude of the waveform. Recall the waveform design as shown in Fig. 3, we purposely set the amplitude of OOK modulated signal and CW to be higher than that of the regular preamble. This is to both increase the backscatter communication range and accommodate the AGC of the receiver: the signal strength of the backscattered symbol will be less than that of the CW; moreover, the AGC will set the receiver's amplifier gain according to the preamble's signal strength, so we need to have higher CW amplitude than the preamble to make the backscattered symbol's amplitude comparable to that of the preamble, or it will result in high BER due to the noise interference.

The amplitude of the signal is configured using the IFFT *scaling* value. For example, a 64-point IFFT processing with radix-4 decimation contains 3 stages of computation, the scaling value is usually set to be 4 for each stage to avoid overflow, which makes the output signal strength to be $\frac{1}{4^3}$ of the non-scaled amplitude. Similarly, if we change the scaling values to 1, 2, 2 for the 3 stages respectively, it will make the output signal strength equal to $\frac{1}{1\times2\times2}$ of the non-scaled amplitude, which is 16 times of that in the previous setting. The number of times is termed as the *amplitude ratio*. Consequently, we can maintain the regular scaling value when IFFTing the preamble and the PHY header, and change the scaling value when IFFTing OOK signals and the CW to configure the amplitude in the excitation signal. Meanwhile, the pilot insertion value should also be changed to maintain the amplitude of the pilot subcarrier correspondingly.

Note that the amplitude ratio impacts performance of the backscatter communication. Figure 6 shows experimental results where the tx-tag and tag-rx distance are 1m and 30m, respectively. The results indicate that the amplitude ratio should not be too high, or the amplitude of the preamble and pilot is suppressed, which makes synchronization and sampling frequency offset estimation at the receiver inaccurate. We choose 16 as the amplitude ratio in our design.

With accomplishment of the excitation signal transmitter design, we resolve **Challenge 2**. Based on the design, we are able to configure the tx-to-tag preamble for partially resolving **Challenge 1**.

4.2 Tag Design

Working procedure. As shown in Fig. 7, the tag is triggered by the OOK modulated signal. The tag will execute the correlation algorithm to check the tx-to-tag preamble in the OOK signal; noting that the tag is unlikely to be falsely triggered by existing Wi-Fi signals, which normally use phase modulation. We borrow the demodulation module design in [4, 5], where there is a passive energy detector and a comparator to obtain the on-off state. Besides awakening the tag, the tx-to-tag preamble is also used for synchronizing the tx and tag symbol clocks.

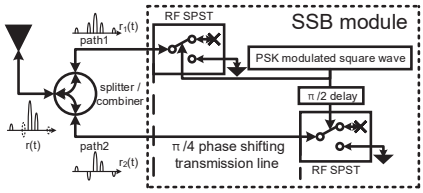

Figure 8: The single side-band backscatter circuit.

The on-tag receiver adopts a hard-decision decoding algorithm to detect the OOK code, where the performance can be influenced by the length of the code. In particular, a shorter code design may incur false triggering, while the longer one could lead to inefficiency. Moreover, although a longer code design benefits overcoming the noise and interference, the low energy budget of the tag dominantly restrains the tx-tag range. Based on our empirical studies, we choose to use 11-bit barker code for realizing synchronization at a reasonable overhead.

After processing the tx-to-tag preamble, the tag starts to demodulate the OOK signal for the control information, which specifies the subcarrier allocation to the tag by informing the tag subcarrier index. The tag then generates a square signal with frequency Δf according to the index; the square wave signal is then modulated with phase shifting keying (PSK) to encode the local payload data. The modulated square wave signal is multiplied with the CW, producing a backscattered symbol flying to the receiver. We also realize convolutional coding in the tag to reduce BER. With successful processing of the tx-to-tag preamble, we could resolve **Challenge 1**; moreover, we propose the following two new designs to the tag.

Single sideband backscatter. The signal obtained after the frequency shifting operation is factually a double sideband one, which not only wastes the spectrum resource but also incurs potential interference to other bands. The issue can be resolved by introducing a phase-shifted signal as mentioned in HitchHike [4]. We here present our new transmission delay line design to realize the single sideband signal generation as shown in Fig. 8. The double sideband signal first goes through the splitter and propagates along path 1 and path 2. We make the transmission line of path 2 longer than that of path 1, where the extra part produces exact $\frac{\pi}{4}$ phase shift of $r_2(t)$. Then the backscattered $r_2(t)$ and $r_1(t)$ are combined to form the single sideband signal $r(t)$. Our transmission delay line design can be realized in PCB of the tag, which needs no active phase-shifting device.

Enhanced tag supporting higher data rate. Another new design proposed in this paper is that we can combine multiple SSB modules to produce an enhanced OFDMA tag supporting higher data rate in our proposed architecture. The enhanced OFDMA backscatter tag design can be implemented in the similar manner as the analog OFDM, which separates the centralized clocks to sub-modules. The CW is

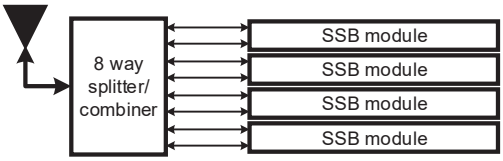

Figure 9: Enhanced backscatter circuit.

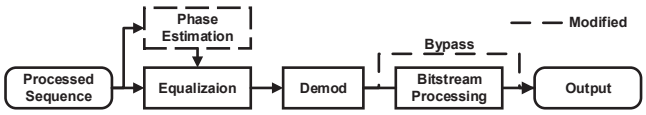

Figure 10: Processing in the receiver.

first split into 8 paths, with every two-path as a group for the SSB modulation, as shown in Fig. 9. In this way, the enhanced tag can be assigned 4 subcarriers thus theoretically providing 4× data rate compared with the regular one, which can be applied to more bandwidth demanding devices in practice [23]. With the flexible spectrum allocation of the OFDMA backscatter system, heterogeneous connectivity needs in practical IoT applications can be satisfied.

It is worth mentioning that the enhanced tag technique also helps resolving the frequency selective fading issue by conveying the information with multiple subcarriers; for the regular tag generating the single subcarrier, the frequency selective fading could be resolved by reassigning subcarriers using the upper layer protocol described in [42]. Theoretically, it is possible to enhance the tag with the capability of reflecting many even all the subcarriers, which however will incur high power consumption and big-size tag thus in conflict with our motivation.

4.3 Receiver Design

The preamble sent from the transmitter and the backscattered symbols from tags arrive at the receiver in sequence, which form a complete OFDM burst. The synthesized burst is then processed by the receiver as shown in Fig. 10. The I/Q stream from the ADC is processed by regular modules sequentially, including packet detection, LTS correlation, synchronization, frequency correlation, CP removal, FFT and demapping, after which a complex number sequence is obtained. Additional processing is enhanced into the original phase estimation module as shown in Fig. 10, in order to address the phase offset incurred by backscattering. This part will be elaborated in Section 5, where we describe how each kind of the phase offsets particularly for OFDMA backscatter is incurred and addressed systematically.

Another streamlining in the receiver is to bypass the bitstream processing module as shown in the right part of Fig. 10. The module includes functionalities of deinterleaving, Viterbi decoding, and descrambling. The Viterbi decoding is a reverse operation corresponding to the convolutional coding process in the transmitter. Note that the input of the bitstream processing module on the transmitter side is the

bitstream for producing the excitation signal; however, the input stream on the receiver side is payload data backscattered from tags. The inconsistency makes the Viterbi decoding module believe that the received bitstream is corrupted, so it will perform corrections on the stream, which pollutes the payload data and results in communication failure. Consequently, we need to bypass this module at the receiver.

5 PHASE OFFSET CALIBRATION

If we run the OFDMA backscatter system as described above, we can observe that the obtained constellation diagram at the receiver contains at least one of the phenomena as shown in Fig. 11. It is obvious that the diagrams are not the same as the ideal BPSK constellation diagram. The lack of tag-rx synchronization incurs such subtle phase offset patterns that have been unknown before. This section reveals the root cause of each phase offset effect and presents corresponding calibration techniques.

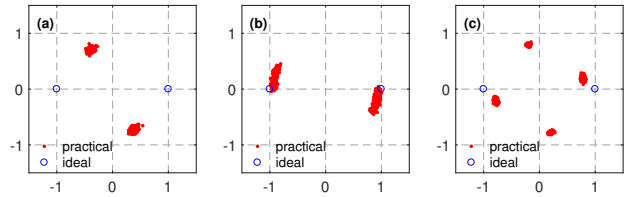

Figure 11: (a) Static phase offset; (b) Continuous dynamic phase offset; (c) Discrete dynamic phase offset.

5.1 Static Phase Offset

The consequence of the static phase offset is: the obtained constellation diagram rotates certain degree compared with the ideal one, where Fig. 11 (a) shows a snapshot of the phenomenon. Specifically, we find that the degree of the rotation varies among different tags; for a given tag, the rotation degree remains constant within a burst, but varies among different bursts.

We reveal that this is incurred by the delay in backscatter as shown in Fig. 12. In particular, the OFDM burst obtained by the receiver consists of the preamble from the excitation signal transmitter and backscattered symbols from tags. Due to the tag circuit delay, tx-to-tag preamble processing delay and the longer propagation delay, we can observe an aggregated delay between the starting point of the backscattered symbol and the corresponding OFDM symbol that would have been sent from the transmitter directly, as shown in Fig. 12.

In the receiver, the FFT window is responsible for separating each OFDM symbol from the burst; the FFT window can cover 64 out of the 80 samples in each OFDM symbol. Thus the starting point of the window does not necessarily align with the starting point of a symbol, and the difference between the two starting points is termed as *FFT offset* as shown in Fig. 12.

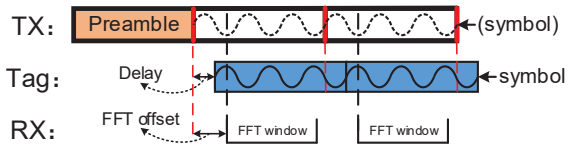

Figure 12: Root cause of static phase offset.

Since the starting point of the FFT window is determined by the OFDM burst preamble, the FFT offset is fixed for a given subcarrier (tag) in a given burst. In the burst, the arriving time of the tags' backscattered signals varies, and the frequencies of those signals differ from each other; therefore, although the FFT offset is constant, the corresponding phase offsets for subcarriers are different. For a different burst, the delay and FFT offset could change, thus the corresponding phase offset for a given subcarrier can be different from that in the previous burst.

We calibrate the static phase offset with the *tag-to-rx preamble*, which is inserted into the tag's local payload. Recall the tag's working procedure as shown in Fig. 7, we let the tag insert 8 bits before the real payload bits and derive the static phase offset of the subcarrier for those 8 bits at the receiver. We realize the calibrate scheme in the phase estimation module of the receiver as shown in Fig. 10. Based on the derived phase offset value from those 8 bits, we can calibrate the static phase offset for the real payload bits.

Although the preamble and the backscattered symbols are not seamlessly concatenated, the CP design in the OFDM mechanism still enables the receiver to decode the burst, which in fact provides the opportunity to realize OFDMA backscatter. The CP is essentially the partial replication of the symbol itself, which is redundant information dealing with ISI and ICI. The 802.11g CP is $0.8\mu s$; therefore, if the backscattered symbols' arrival time points fall in the duration of $0.8\mu s$ at the receiver, then the inherent synchronization scheme of 11g will automatically calibrate the time offsets. The aggregate backscatter delay and CP length factually determine the feasibility and robustness of the OFDMA backscatter system, which is to be examined in Section 7.1.

5.2 Continuous Dynamic Phase Offset

The effect of the continuous dynamic phase offset is: the points on the constellation diagram keep moving along the unit circle in the same direction and finally form a circle, as shown in Fig. 11 (b). Note that the sampled OFDM signal at the receiver can be represented by $r[n] = h[n] * s[n] \cdot e^{-j2\pi n\Delta f \Delta T}$, where Δf is the residual frequency offset and ΔT is the sampling period of $\frac{1}{20MHz}$ [25, 26]. The phase angle $\varphi = 2\pi n\Delta f \Delta T$ increases with the index of samples n. Since φ is very small in practice, the phase offset in each sampling operation increases non-dramatically, which is why we use the term "continuous".

Such an issue also occurs in the regular OFDM based system, which normally is resolved using the pilot signal.

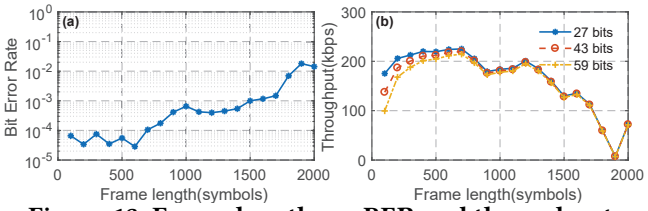

Figure 13: Frame lengths vs BER and throughput.

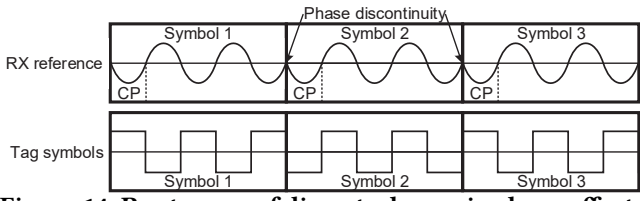

Figure 14: Root cause of discrete dynamic phase offset.

In particular, the pilot signal is transmitted along with the OFDM symbol, and the receiver can estimate the corresponding phase offset by decoding the fixed information conveyed by the pilot signal, based on which the offset can be calibrated. However, in OFDMA backscatter, the pilot signal in the backscatter system is transmitted by the excitation signal transmitter, but the OFDM symbol is synthesized with backscattered signals, which makes the phase offset estimated through decoding pilot signal unable to represent that of the synthesized OFDM symbol; therefore, we need to resolve the issue by other means.

We can see that the expression of φ indicates that the more sampling operations are carried out, the more phase offset can occur. The number of sampling operations required at the receiver is dependent on the number of symbols in the burst; therefore, constraining the frame length can effectively mitigate the dynamic phase offset. However, we need to strike a balance for choosing the frame length, because the proportion of the control bits is high if the frame length is too short, which could impact throughput; the space in the burst for the control signal could have been used for payload. We conduct experiments to find out an appropriate frame length, where the results are shown in Fig. 13. It shows that the BER and throughput achieve balance when the frame length is 500: the longer frame incurs higher BER, while the shorter one incurs throughput degradation.

Another possible method to resolve the issue is to utilize pilot symbol assisted modulation as in [27]: tags periodically send certain symbols with pilot subcarriers, so that the receiver can derive the reference amplitude and phase, which however will sacrifice some data rate for periodical calibration.

5.3 Discrete Dynamic Phase Offset

The effect of the discrete dynamic phase offset is: the points move along the unit circle but with a notable angular step size, as shown in Fig. 11 (c). The root cause of the phenomenon could be explained with Fig. 14. The upper part of the figure illustrates 3 standard OFDM symbols from a single subcarrier. Note that the 3 symbols are with the same initial phase, thus they could be regarded as conveying the same information, say bit 1. Such waveform acts as a reference for the receiver to decode information conveyed by OFDM symbols synthesized by tags' backscatter signals. In particular, if we use φ_r and φ_t to denote the initial phase of the reference signal and the tag's backscattered signal respectively, and the system uses BPSK, then the backscattered information is 1 and 0, when $\varphi_r - \varphi_t = 0$ and $\varphi_r - \varphi_t = \pi$, respectively. This is the ideal decoding process in the receiver, and the results are just like the ideal situation as shown in Fig. 11 (c).

However, the problem is that extra phase offset is incurred by the modulation process in the tag, which makes the difference between φ_r and φ_t not necessarily equal to 0 or π. Recall the modulation process as described in Section 4.2, the information is modulated on the *continuous square waveform* at shifting frequency Δf. The lower part of Fig. 14 shows an example. Suppose that the tag happens to transmit 3 symbols all representing bit 1, then the tag just chooses the square waveform with initial phase 0 to perform modulation as shown in the figure; however, we can see that the initial phase of symbol 2 are different from the other ones, because the duration of the symbol is not necessarily equal to the integer multiple of the square wave's period. This results in that the tag is actually transmitting 1, 0, 1 instead of 1, 1, 1.

We now calculate the exact difference between φ_r and φ_t introduced in backscatter. Calculating the value of φ_r as shown in the upper part of Fig. 14, we have to take CP into account. If we use $r[n] = e^{-j2\pi N\Delta F \cdot n\Delta T}$ to denote the reference signal waveform after sampling, since CP is the last $\frac{1}{4}$ of the sampled waveform itself (totally contains 64 samples), then $\varphi_r = 2\pi N\Delta F \cdot 48\Delta T$, where ΔF is the frequency spacing of OFDM subcarriers ($0.3125MHz$ in 802.11g), ΔT is the sampling period ($\frac{1}{20MHz}$ in 802.11g as the sampling frequency is $20MHz$), and N is the subcarrier's IFFT index (0-63) as shown in Fig. 4. We finally have $\varphi_r = 2\pi \cdot \frac{3N}{4}$.

The value of φ_t varies in different symbols as shown in Fig. 14. For the square wave, the initial phase of the m-th symbol is $\varphi_t = 2\pi N_t \Delta F \cdot \frac{1}{f_{sym}} m$, where $f_{sym} = 250KHz$ denotes the symbol frequency in 802.11g, and N_t is the index gap between the subcarrier for generating CW and the subcarrier allocated to the tag; therefore, we finally have $\varphi_t = 2\pi \cdot \frac{5N_t}{4} m$. If we try every possible combination of N_t and N in a given design, then we can find that the possible values of $\varphi_r - \varphi_t$ are 0, $\frac{\pi}{2}m$, πm, $\frac{3\pi}{2}m$ respectively. Those are extra phase offsets between φ_r and φ_t excluding the phase offset conveying information, which corroborates the phenomenon as shown in Fig. 11 (c).

In practice, the tag has the information of N_t, N and m, thus it can compensate the extra phase offset and then the decoding is normal.

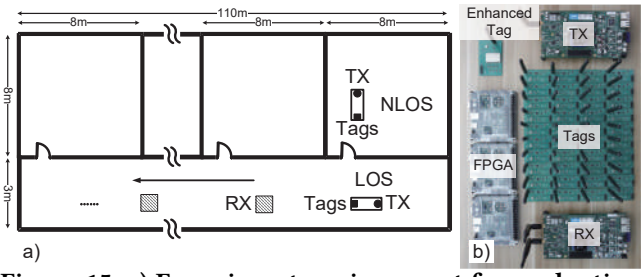

Figure 15: a) Experiment environment for evaluating capacity, concurrency and range. b) Pototype

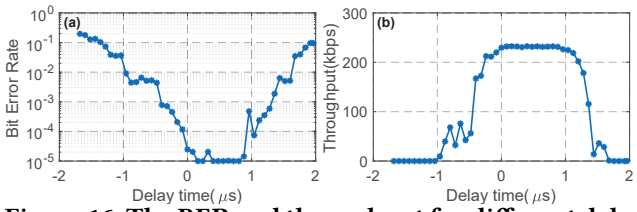

Figure 16: The BER and throughput for different delay evaluation.

6 IMPLEMENTATION

We implement a prototype as shown in Fig. 15. We use WARP v3 boards [29] to implement the transmitter and the receiver functionalities described in previous sections; the SSB module of the tag is implemented with COTS components in the similar way with the HitchHike tag [4]. We implement an enhanced tag by combining 4 SSB modules of regular tags, where we use an 8-way power spliter/combiner SEPS-8-272+ to separate the CW to 8 ways.

All baseband processing functions including synchronization, demodulating and responding to the control message, BPSK/QPSK modulation and frequency shifting clock choosing are written in VHDL, which are realized on a DIGILENT NEXYS4 FPGA development board [34]. The digital pins of the FPGA are connected to the tag to have access to the received signal and output control signals to the state switch.

7 EXPERIMENTAL RESULTS

7.1 Synchronization Robustness

The tag subsystem is the main source of time and frequency offsets in OFDMA backscatter as described in previous sections. We here investigate to what extent our prototype can tolerate tags' uncertainties that can essentially impact the system operation. The experimental results also verify that the inherent CP design of the 11g OFDM framework and our model design indeed make it possible to realize synchronization for OFDMA backscatter as analyzed in Section 3.

Impact of delay. The tag subsystem incurs 3 kinds of delays: the circuit delay, tx-to-tag preamble processing delay and the propagation delay, which can make the backscattered symbol arrive at the receiver at different time points, and cause the static phase offset as described in Section 5.1. We here verify if the CP ($0.8\mu s$) in the OFDMA backscatter system can neutralize such delay effect. We create an equivalent aggregate delay by adjusting the starting point of the symbol clock on the tag with a delta ranging from $-2\mu s$ to $2\mu s$, and observe the consequent BER and raw throughput. It can be seen from Fig. 16 that the delay tolerance of the system is up to $1\mu s$ in practice, which is close to the theoretical value.

In particular, consider the delay between the preamble and the backscattered symbol as shown in Fig. 12, which contains the 3 kinds of delays as mentioned above. In practice, the propagation delay is determined by the relative positions of the tx, tag and rx. That is, the tx-rx distance (d_1) determines the time point at which the preamble ends; the tx-tag (d_2) and tag-rx (d_3) distances partially determine when the backscattered symbol starts. In the worst case, tx is in between the two tags and rx is on the left/right side of the leftmost/rightmost tag, which creates the greatest propagation delay $\frac{2d_2}{c} = 26.6ns$ (c is the speed of light).

The circuit delay and tx-to-tag preamble processing delay are the other two factors influencing when the backscattered symbol starts. Note that the symbol rate of the OOK signal is only $250kps$, which is much lower than the sampling clock frequency of the FPGA (tens of MHz) thus incurring ns delay. We randomly select two tags and place them in the same position, and connect tags with an oscilloscope to examine the starting time point the tag is triggered. Such experiments are repeated until all the tags have been examined, and the results show that one tag can be triggered at most $20ns$ after the other one. This verifies that these two kinds of delay in aggregation are in the order of tens of ns. In summary, the 3 kinds of delays in aggregation are tens of ns, which is much less than the CP duration $0.8\mu s$; therefore, the time synchronization can be definitely guaranteed.

Impact of symbol clock synchronization. The symbol clock in the excitation signal transmitter and that in the tag should be synchronized, which in our system is realized by the tx-to-tag preamble as shown in Fig. 7. Such synchronization is important in realizing OFDMA backscatter, because it allows the transmitter and tags to agree on the starting point and duration of the OFDM symbol. We here examine performance of our synchronization mechanism. In the experiment, we change the tag's symbol clock by changing the value of the fraction counting clock. The results are shown in Fig. 17, we can see that if the clock offsets are within -2% to 2%, the performance is not significantly impacted. This validates the feasibility of our synchronization design, because the clock design implemented with the COTS electronic components can easily provide much higher accuracy.

Impact of subcarrier frequency offset. The subcarrier frequency offset is incurred by the on-tag clock when performing frequency shifting, which potentially impacts the subcarriers' orthogonality. In this experiment, we assign subcarriers #23, #24 and #25 to three different tags, where we

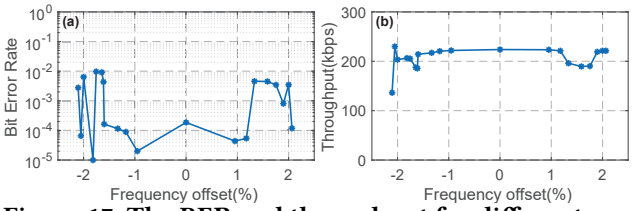

Figure 17: The BER and throughput for different symbol clock offset evaluation.

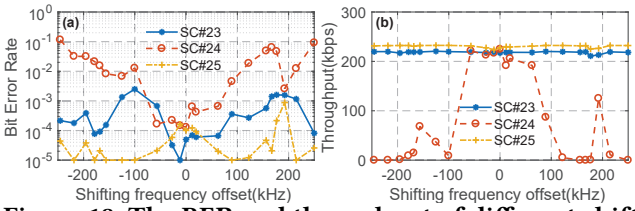

Figure 18: The BER and throughput of different shifting frequency offset evaluation.

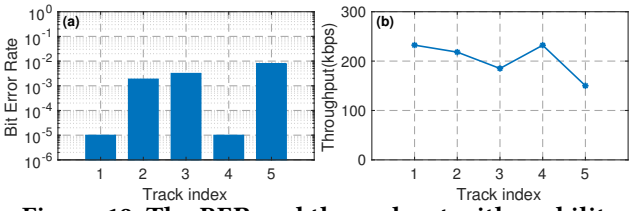

Figure 19: The BER and throughput with mobility.

purposely change the frequency of subcarrier #24 by a delta ranging from -250kHz to 250kHz. The consequent BER and raw throughput of the three tags are shown in Fig. 18. It can be seen that the subcarrier frequency offset's interference to nearby subcarriers #23 and #25 is quite limited compared with that to subcarrier #24 itself. We also conduct such experiments to other three sequential subcarriers and the results are similar. The tolerance to the subcarrier frequency offset is related to the subcarriers' frequency spacing in the OFDM mechanism. The results indicate that if the frequency shift operation in the tag yields a subcarrier within around 1% frequency drift, the performance of the backscattered subcarriers will not be impacted. This can be easily satisfied by the COTS electronic components.

Impact of mobility. We here test the possible impact of tag mobility, which is important for applications such as wearable devices. We put the tag $0.5m$ away from the transmitter and make the tag move along 5 tracks. Track 1 means static, track 2 is to move in the left half-plane of the line segment formed by the transmitter and the tag, track 3 is to move in the right half-plane, track 4 is to move in the 3D space, and track 5 is to move forward and backward to the transmitter. The results are shown in Fig. 19, where it shows that although the mobility could potentially incur the sub-carrier phase offset, the actually impact is very limited.

7.2 Performance of OFDMA Backscatter

After verifying the feasibility, we now comprehensively examine performance of the OFDMA backscatter system in the environment as shown in Fig. 15. We utilize channel coding when conducting communication experiments in order to explore the best the system can achieve.

Power consumption. We design an integrated circuit for the tag's digital processing module and perform simulations to measure the tag's power consumption. In our design, the frequency synthesizer is realized by All-Digital PLL, which uses time-to-digital converter (TDC) combined with 8-phase (4 stages) differential ring oscillator (DRO) as the digitally-controlled oscillator [28]. DRO based design provides 8 outputs at the same frequency with required phase offset ($0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{5\pi}{4}, \frac{3\pi}{2} and \frac{7\pi}{4}$) which benefits the PSK modulation. The TDC design makes flexible subcarrier allocation of OFDMA attainable. The power consumption of the frequency synthesizer is $0.47\mu W/MHz$.

In our system, the clock frequency is the shifting frequency Δf. The frequency is integer multiples of the subcarriers' frequency spacing, which means that $\Delta f = N_t \Delta F = N_t \times 0.3125MHz$ where N_t={1:5 7:19 21: 26 28:33 35:47 49:53} is the number of intervals between CW subcarrier and the tags' allocated subcarrier. Consequently, the power consumption of on-tag clock is $P_C = 0.47 \times N_t \times 0.3125\mu W$, ranging from $0.15\mu W$ to $7.78\mu W$. The processor takes the payload bits as input and performs the baseband processing procedure as is done in the FPGA. We use VHDL code verified in the FPGA implementation, the Synopsis Design Complier and IC Complier with 40 nm LP CMOS node by TSMC to generate the transistor level implementation. The simulated power consumption of the digital part is $P_D = 17.5\mu W$. For the SSB module of the tag, the power consumption is only caused by the two RF switches. The calculation is the same as in [6]. The power consumption of one SSB module is linearly related to the switching frequency, which means that $P_{SSB} = 2{\times}21\mu W{\times}\frac{1}{20MHz}{\times}N_t{\times}\Delta F$, ranging from $0.66\mu W$ to $34.78\mu W$. In summary, the overall transmitting power consumption of the OFDMA tag implementation is conservatively estimated to be $18.31\text{-}60.06\mu W$.

The power consumption of the enhanced tag can be computed in the similar way. The enhanced tag implemented in this work consists of 4 SSB modules and corresponding clock and processing core; therefore, the power consumption is the sum of P_C, P_{SSB} with 4 different $N_t = \{8\ 12\ 16\ 22\}$ and 4 times the core power consumption P_D. That is, $P_t = P_{C-8} + P_{C-12} + P_{C-16} + P_{C-22} + P_{SSB-8} + P_{SSB-12} + P_{SSB-16} + P_{SSB-22} + 4 \times P_D = 116.58\mu W$.

Capacity and concurrency. We conduct experiments to show that our OFDMA backscatter system can support

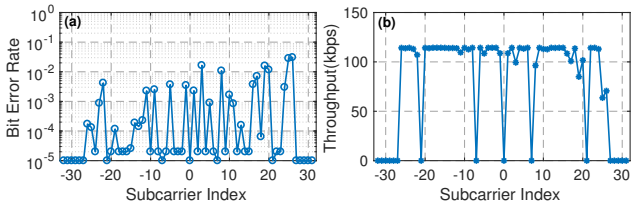

Figure 20: Capacity and concurrency with BPSK.

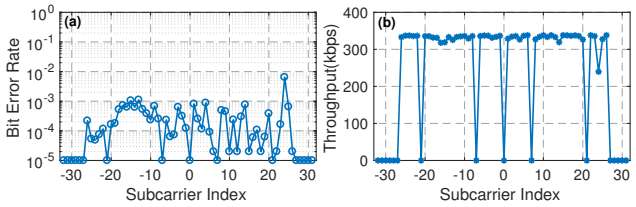

Figure 21: Capacity and concurrency with QPSK.

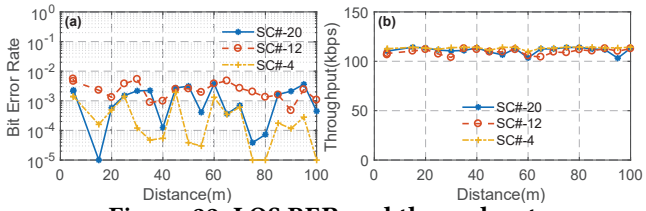

Figure 22: LOS BER and throughput.

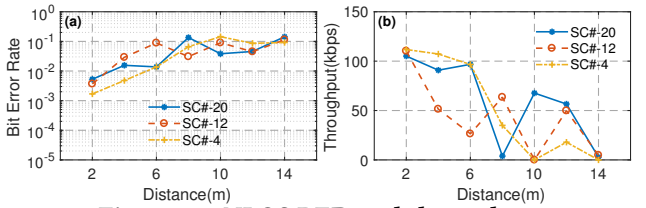

Figure 23: NLOS BER and throughput.

48 tags' concurrent transmissions. Those 48 tags are randomly placed in $4m$ neighborhood of the transmitter and the receiver is $10m$ away from the transmitter. The 48 data subcarriers in 802.11g are assigned to those tags respectively; tags cyclically transmit $5M$ data upon receiving the excitation signal, which are in the form of frames and stored in the connected FPGA. We have a video to demonstrate this experiment [42].

Figure 20 illustrates the experimental results with BPSK and $\frac{1}{2}$ coding rate. The vertical axis of BER subfigure is in logarithm, and we purposely set those 0-valued BER to be 2×10^{-5} for convenience of demonstration as there is no definition of $log_{10}0$. The pilot and null subcarriers are not used to transmit data, thus the corresponding throughput and BER readings are set to be 0 and 1×10^{-5} respectively also for convenience of demonstration. We can see that the BERs of those tags vary from the level of 10^{-5} to 10^{-2}, and the corresponding throughputs range from $114.3kbps$ to $63.6kbps$. The throughput is the number of bits in all correctly received frames per second. For the total $5M$ data transmitted by a tag, the lowest BER is in the level of 10^{-5}; when the BER is in the level of 10^{-2}, it is reasonable that the corresponding throughput reduction is about $50kbps$ as shown Fig. 20. We can see that a number of BERs are in the level of 10^{-3}, thus the corresponding throughput reductions of the tags are around 5-$10kbps$, because it may happen that a number of bit errors occurring in the same data frame, which also influences the throughput calculation. The network capacity (maximum aggregate throughput) of the system is $5.2Mbps$. Figure 21 shows the experimental results with QPSK and $\frac{3}{4}$ coding rate, where the capacity of the network can achieve $16Mbps$ with 48 tags transmit concurrently.

LOS range. We select 3 subcarriers from the previous experiments to examine the communication range. In particular, we set the tx-tag distance to be $1m$ as in [3, 4, 7] to make a fair comparison. We change the tag-rx distance to observe the obtained BER and throughput, with BPSK and coding rate of 1/2. Figure 22 shows the results, which indicates that the communication range of OFDMA backscatter system is at least $100m$ in our system. The backscatter signal is a narrow-band one, which yields a higher SNR compared with the wide-band counterpart as in previous works [3, 7]. This makes the signal receiving module in the tag able to detect the backscattered signal in a longer distance. Meanwhile, we can see that each tag can maintain the throughput of $110{+}Kbps$, which can meet connectivity needs of most IoT applications featured by short bursts of data.

Note that the SNR is expected to drop as the tag-rx distance increases, but we can see from Fig. 22 that the BER and throughput do not change dramatically. This is because the data sending rate of the tag is less than the tag-rx channel capacity; moreover, the multipath effect and the on-site interference from other Wi-Fi APs make the rx SNR inconsistent with that in the ideal free path loss situation. This also explains phenomena indicated by Fig. 23.

NLOS range. In the NLOS scenario, we locate the transmitter and tags in a room, and the receiver outside of the room in the corridor. The corresponding performance of three tags is evaluated also with changing tag-rx distance. Figure 23 shows that the maximum communication range is $12m$ in the NLOS case. It is difficult to make a relative fair comparison with the existing design in the NLOS scenario, as the building materials and floor plans are different. In fact, the NLOS issue also occurs in regular Wi-Fi systems, for which the extenders/boosters are used. Such solutions also can be applied to Wi-Fi backscatter systems.

Enhanced OFDMA tag. The enhanced tag is allocated 4 subcarriers with indices [#-25 #-24 #-23 #-22] using BPSK, which performs backscatter with other 44 tags concurrently. The introduction of the enhanced tag does not impact the system capacity, and the enhanced tag itself can achieve $430Kbps$ in the range of $35m$, which is almost 4× of the

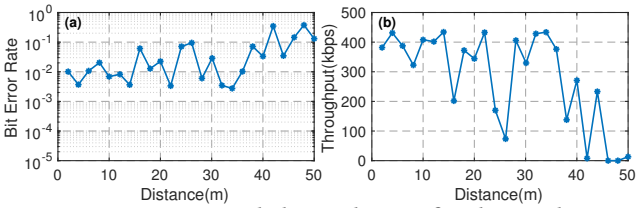

Figure 24: BER and throughput of enhanced tag.

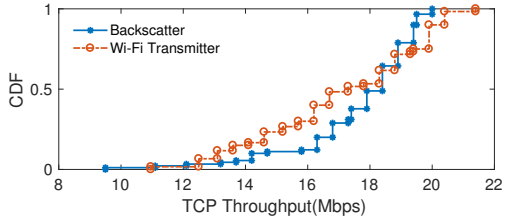

Figure 25: Impacts on existing Wi-Fi systems.

regular tag's data rate. Figure 24 shows the performance of the enhanced tag with different distances from the receiver. We can see that the maximum communication distance is 45m, which is shorter than that of the regular tags. This is because the power of CW is divided into 4 parts to generate 4 subcarriers.

Coexistence with other Wi-Fi systems. OFDMA backscatter system coordinates channels with other Wi-Fi systems using RTS and CTS messages as in [3]. In the experiment, we use a laptop with Intel(R) Dual Band Wireless-AC 3165 Wi-Fi chipset and a NETGEAR Nighthawk AC1900 wireless router to act as the transmitter and receiver of a Wi-Fi system, and use iPerf3 [41] to record the corresponding TCP throughputs as experimental results. The devices are transmitting at the highest data rate of 802.11g in CHANNEL 1 of 2.4G frequency band. We compare the performance of the Wi-Fi system in the presence of two devices: 1) another Wi-Fi router transmits every 10ms, and 2) the OFDMA backscatter system turned on every 10ms. Figure 25 plots the TCP throughput and shows that our system has a similar impact on the Wi-Fi transmission as the regular Wi-Fi transmitter.

8 DISCUSSIONS

Tx-tag range. The limitation that existing Wi-Fi backscatter systems [3–5] including ours have in common is the short tx-tag range, which is affected by the sensitivity of the on-tag receiver. In particular, higher sensitivity of the tag's receiver could allow longer range but incur considerable more power consumption, and lower sensitivity can save much power but results in short tx-tag range [3]. However, the high concurrency of our backscatter system still could be utilized in the scenario where IoT devices are super-densely deployed, such as the wireless avionics intra-communications (WAIC) [37, 38]. The purpose of WAIC is to replace the data-carrying wires in the widebody passenger jet with wireless links, which could save about 1.8 tons of the aircraft's weight and reduce the corresponding wiring complexity and uncertainty [38]. For example, there are more than 68-250 sensors in every single meter of the Airbus A380 [39, 40], and the wingspan and the body length of the aircraft are 79.75m and 72.75m respectively; therefore, the current tx-tag range of our approach is still usable for the scenario.

Enhance capacity and concurrency further. Our design in the paper utilizes 1 of the 11 channels regulated by Wi-Fi in 2.4GHz band. In fact, there are totally 3 non-overlapping channels in the band, which could improve the concurrency to be $3 \times 48 = 144$. In particular, we need to install 3 independent excitation signal transmitters, with each working in a non-overlapping channel; moreover, we must prevent the tag from performing frequency shift and backscatter to the other 2 excitation signals, which is factually to prevent assigning 3 subcarriers in the 3 channels to a single tag for interference avoidance.

The challenge could be finding an appropriate bidirectional passive RF filter with the passband approximately equal to the bandwidth of a single Wi-Fi channel. We have utilized the LC RF filter [36] to verify the feasibility of the preliminary idea; however, the filter's passband is much wider than the bandwidth of a single Wi-Fi channel, which hinders scaling up the system. We still do not find such an appropriate RF filter as of writing of this paper.

Moreover, we note that the OFDM mechanism of 802.11n and 11ax [16] are very similar with that of 11g in structure; there are only some differences in parameter values such as the frequency spacing and CP length. If the feasibility and robustness can be verified with experiments as described in Section 7.1, then it is possible to realize our OFDMA backscatter design also in 11n/ax, which possibly can support 108-1000 tags to transmit concurrently. The potential challenge is that the frequency-shift operation across 80MHz requires higher frequency and more accurate clock in the tag, which could incur more power consumption.

COTS deployment. To realize the proposed mechanism in COTS Wi-Fi APs, the IFFT mapping strategies, AGC, phase estimation and Viterbi decoding modules need to be modified. Wi-Fi chips normally contain several IFFT mapping schemes so that it can switch among different standards such as 802.11g/n/ac/ax; therefore, it may be possible to add the mapping scheme for OFDMA backscatter as another one. The bypassing could be implemented by leveraging the chip's debugging pins. To reduce modifications to accommodate the COTS device, an option is to transmit OOK signal before preamble, which enables tags to generate the LTS of the preamble; however, the problem is that an LTS synthesized by the tags will impact the LTS-based fine synchronization, such as timing and CFO correlation between transmitter and receiver, which will crush the whole system. How practical deployment of OFDMA backscatter can be realized is highly

dependent on implementation details of COTS Wi-Fi chips, which however are usually undisclosed information to the best of our knowledge.

9 RELATED WORK

Early Wi-Fi backscatter systems leverage the Wi-Fi signal in the air as the excitation signal, which results in limited data rate and backscatter range, since the excitation signal and the backscattered signal at the same frequency incur self-interference [1, 2]. Recent designs present novel ideas to deal with the issue: Frequency shift based systems such as Passive Wi-Fi make the tag to shift the CW from the excitation signal generator to another non-overlapping frequency band the receiver is listening [3, 6, 7, 20]; Codeword translation based systems such as FreeRider make the tag to transform the codeword presented in the excitation signal into another valid codeword in the same codebook to convey information to the receiver, which can be accommodated by commodity Wi-Fi devices [4, 5].

However, the existing Wi-Fi backscatter systems mentioned above basically coordinate transmissions among tags in sequence [5]. Such an approach can be equivalent to the multiple access scheme in commodity RFID systems based on the frame slotted aloha and tree-based arbitration [5, 14], where the inefficiency has long been acknowledged [11, 12, 14]. In fact, TDMA/FDMA/SDMA/CDMA based approaches have all been investigated in the past decade but found incurring high coordination overhead or co-location interference for backscatter systems [8–15]. Recent works improve backscatter communication efficiency by decoding collided transmissions based on tags' features in the IQ and time domain [11, 13–15], which achieves $4Mbps$ aggregate throughput theoretically [12, 14, 15]. The OFDMA scheme is still not realized in any backscatter system to the best of our knowledge.

Our work in this paper adopts the frequency shift method to avoid self-interference [3, 6, 7], but differs from the prior work in the following critical ways: 1) Prior works are based on single-carrier modulation, while our backscatter system is based on the multi-carrier modulation technique. 2) Prior systems control the tag backscattering only in the time domain, where shifting frequency is fixed in each tag, while our system enables controlling in both time and the frequency domain, which provides high concurrency.

Interscatter and FreeRide system can realize backscatter communication with OFDM signals from commodity devices as excitation signals [5, 7]. In particular, Interscatter transforms 802.11g Wi-Fi device into the AM modulator to encode bits with OFDM symbols, FreeRider backscattering device performs codeword translation to OFDM signals to convey bits to the receiver. The reflecting device in our system however encodes bits with the OFDM subcarrier locally generated from the CW. Moreover, Interscatter and FreeRide are unable to support concurrent transmissions from multiple tags, where tags must transmit in sequence. It is worth mentioning that the way we utilize OFDM in this paper is similar with the Distributed OFDM (D-OFDM) mechanism in SNOW [21], where the spectra components from an aggregate OFDM signal are extracted and allocated to different sensors; however, SNOW is realized over TV white spaces without supporting backscattering.

The recently proposed NetScatter system [22] can support 256 concurrent backscatter transmissions, which utilizes a combination of chirp spread spectrum (CSS) modulation and ON-OFF keying. Given the bandwidth, the number of concurrent transmissions can be supported by NetScatter is determined by the spacing of initial frequencies of upchirps allocated to tags, while ours by the spacing of orthogonal subcarriers' frequencies, which both require the upchirps (subcarriers) to be orthogonal to each other; therefore, the spectrum efficiency of the two systems are the same according to information theory. Our proposed mechanism targets at supporting Wi-Fi systems, thus the concurrency is constrained by the OFDM framework regulated by Wi-Fi standards. More concurrency can be supported in the new OFDM framework where more subcarriers can be provided as discussed in Section 8.

10 CONCLUSION

We have demonstrated how to enable OFDMA in Wi-Fi backscatter for capacity and concurrency enhancement. With our approach, OFDMA is realized by coordinating tags to generate orthogonal subcarriers concurrently through backscatter. The crux is to achieve strict synchronization among communication components. We have revealed how the subtle asychnronization scenarios particularly for backscattering can incur system offsets, and presented a series of novel designs for the excitation signal transmitter, tag, and receiver to address the issue. We have built a prototype in 802.11g OFDM framework to validate our design. Experimental results show that our system can achieve 5.2-16$Mbps$ aggregate throughput by allowing 48 tags to transmit concurrently, while constraining the tag's power consumption in tens of μW. This is 1.45-5× of capacity and 48× of concurrency compared with the existing design respectively.

ACKNOWLEDGMENTS

We would like to thank the shepherd Prof. Dinesh Bharadia and the anonymous reviewers for their valuable comments and suggestions. The work in this paper is supported by the National Key Research and Development Program of China 2017YFB1003000, and the National Natural Science Foundation of China (NSFC) 61872233, 61572319, 61829201, 61532012, 61325012, 61428205.

REFERENCES

[1] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith and D. Wetherall, "Wi-Fi backscatter: Internet connectivity for rf-powered devices," in *Proc. ACM SIGCOMM*, 2014.

[2] D. Bharadia, K. Joshi, M. Kotaru and S. Katti, "BackFi: High throughput WiFi backscatter," in *Proc. ACM SIGCOMM*, 2015.

[3] B. Kellogg, V. Talla, S. Gollakota and J. R. Smith, "Passive Wi-Fi: Bringing low power to Wi-Fi transmissions," in *Proc. Usenix NSDI*, 2016.

[4] P. Zhang, D. Bharadia, K. Joshi, S. Katti1, "HitchHike: Practical backscatter using commodity WiFi," in *Proc. ACM SenSys*, 2016.

[5] P. Zhang, C. Josephson, D. Bharadia and S. Katti, "FreeRider: Backscatter communication using commodity radios," in *Proc. ACM CoNEXT*, 2017.

[6] P. Zhang, M. Rostami, P. Hu and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proc. ACM SIGCOMM*, 2016.

[7] V. Iyer, V. Talla, B. Kellogg, S. Gollakota and J. R. Smith, "Inter-technology backscatter: Towards Internet connectivity for implanted devices," in *Proc. ACM SIGCOMM*, 2016.

[8] C. Mutti and C. Floerkemeier, "CDMA-based RFID systems in dense scenarios: Concepts and challenges," in *Proc. IEEE RFID*, 2008.

[9] J. Wang, H. Hassanieh, D. Katabi and P. Indyk, "Efficient and reliable low-power backscatter networks," in *Proc. ACM SIGCOMM*, 2012.

[10] L. Kong, L. He, Y. Gu, M. Wu and T. He, "A parallel identification protocol for RFID systems," in *Proc. IEEE INFOCOM*, 2012.

[11] P. Hu, P. Zhang, D. Ganesan, "Leveraging interleaved signal edges for concurrent backscatter," in *Proc. ACM HotWireless*, 2014

[12] P. Hu, P. Zhang, D. Ganesan, "Laissez-faire : Fully asymmetric backscatter communication," in *Proc. ACM SIGCOMM*, 2015.

[13] O. Abari, D. Vasisht, D. Katabi and A. Chandrakasan, "Caraoke: An E-toll transponder network for smart cities," in *Proc. ACM SIGCOMM*, 2015.

[14] J. Ou, M. Li, and Y. Zheng, "Come and be served: Parallel decoding for COTS RFID tags," in *Proc. ACM MobiCom*, 2015.

[15] M. Jin, Y. He, X. Meng, Y. Zheng, D. Fang and X. Chen, "FlipTracer: Practical parallel decoding for backscatter communication," in *Proc. ACM MobiCom*, 2017.

[16] 802.11ax - Standard for Information Technology - Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN, Available Online: http://standards.ieee.org/develop/wg/WG802.11.html.

[17] 802.11ax: Transforming Wi-Fi to bring unprecedented capacity and efficiency, Qualcomm Technologies, Available Online: https://www.qualcomm.com/solutions/networking/features/80211ax.

[18] 802.11ax: Next generation Wi-Fi for the Gigabit home, Broadcom white paper, Available Online: https://www.mobileworldlive.com/broadcom-whitepaper-802-11ax-next-generation-wi-fi-for-the-gigabit-home/.

[19] Introduction to 802.11ax, National Instruments white paper, Available Online: http://www.ni.com/80211ax/.

[20] A. Wang, V. Iyer, V. Talla, J. R. Smith and S. Gollakota, "FM backscatter: Enabling connected cities and smart fabrics," in *Proc. NSDI*, 2017.

[21] A. Saifullah, M. Rahman, D. Ismail, C. Lu, R. Chandra and J. Liu, "SNOW: Sensor network over white spaces," in *Proc. ACM SenSys*, 2016.

[22] M. Hessar, A. Najafi and S. Gollakota, "NetScatter: Enabling large-scale backscatter networks," in *Proc. NSDI*, 2019.

[23] V. Talla, B. Kellogg, S. Gollakota and J. R. Smith, "Battry-free cellphone," in *Proc. ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, article 25, Jun. 2017.

[24] IEEE Std 802.11-2016, "802.11-2016 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", Available Online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7786995.

[25] T. Hwang, C. Yang, G. Wu, S. Li and G. Y. Li, "OFDM and its wireless applications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1673–1694, Aug. 2008.

[26] S. Rathinakumar, B. Radunovic and M. K. Marina, "CPRecycle: Recycling cyclic prefix for versatile interference mitigation in OFDM based wireless systems," *ACM CoNext*, Dec. 2016, pp. 67–80.

[27] Cavers, J. K., "An analysis of pilot symbol assisted modulation for Rayleigh fading channels (mobile radio)." *IEEE Transactions on Vehicular Technology*, vol. 40, no. 4, pp. 686-693, 2002.

[28] Y. Hiraku, I. Hayashi, H. Chung, T. Kuroda, H. Ishikuro, "A 0.5 V 10MHz-to-100MHz 0.47 μz power scalable AD-PLL in 40nm CMOS," *Solid State Circuits Conference, 2012 IEEE Asian*, pp. 33–36, 2012.

[29] WARP Project, Available Online: http://warpproject.org

[30] SPDT RF switch, HMC190BMS8E by ADI, http://www.analog.com/media/en/technical-documentation/data-sheets/hmc190b.pdf

[31] Power splitter/combiner, BP2U+ by Mini-Circuits, https://www.minicircuits.com/pdfs/BP2U+.pdf

[32] Transmission line calculator, TX-LINE by NI, Available Online: http://www.awrcorp.com/products/additional-products/tx-line-transmission-line-calculator

[33] SPST reflective switch, ADG902 by ADI, http://www.analog.com/media/en/technical-documentation/data-sheets/ADG901_902.pdf

[34] FPGA development board, NEXYS4 by DIGILENT, https://reference.digilentinc.com/_media/reference/programmable-logic/nexys-4-ddr/nexys4ddr_rm.pdf

[35] 8-way Power Splitter/Combiner, SEPS-8-272+ by Mini-Circuits, https://www.minicircuits.com/pdfs/SEPS-8-272+.pdf

[36] RF filter, LFB2H2G45SG7A159 by Murata, https://www.murata.com/en-eu/api/pdfdownloadapi?cate=&partno=LFB2H2G45SG7A159

[37] Wireless avionics intra-communications project, Aerospace Vehicle Systems Institute, http://waic.avsi.aero/

[38] H. Canaday, "War on wiring," Aerospace America, https://aerospaceamerica.aiaa.org/features/war-on-wiring/

[39] B. Marr, " That's Data Science: Airbus Puts 10,000 Sensors in Every Single Wing," https://www.datasciencecentral.com/profiles/blogs/that-s-data-science-airbus-puts-10-000-sensors-in-every-single

[40] D. Shah, "Millions of data points flying in tight formation," http://www.aerospacemanufacturinganddesign.com/article/millions-of-data-points-flying-part1/

[41] Speed test tool, iPerf3 Available Online: https://iperf.fr/

[42] FAQs and video demonstration, Available Online: https://www.dropbox.com/sh/mdft6dndanbx28l/AACupb5fRpCFAR2VF5SpyCE-a?dl=0