Channel Independent Wi-Fi Backscatter Networks

Taekyung Kim and Wonjun Lee
Network and Security Research Lab.
School of Information Security
Korea University, Seoul, Republic of Korea
{tkkim92, wlee}@korea.ac.kr

***Abstract*—Wi-Fi backscatter is an emerging technique that enables ultra-low power wireless communications thanks to the simplicity of a backscatter tag. This simplicity drastically reduces communication power. However, this simplicity also removes channel selectivity of the backscatter tag. In this regard, we introduce two issues, violation of the wireless regulations and the waste of resources, in Wi-Fi backscatter networks. To solve these problems, we introduce channel independent packet detection and error vector demodulation. We first design a backscatter receiver accepting Wi-Fi frames on the listening channel as well as adjacent channels, because the backscatter tag responds to all incoming signals regardless of their frequencies. We then investigate how the error vectors of each subcarrier are changed in Wi-Fi backscatter systems. Based on the analysis, we propose a method that translates the error vectors into a backscatter frame. We implement and evaluate our design with commodity 802.11n access points as carrier sources, a software-defined radio as a receiver, and a 2.4 GHz backscatter tag. The results show that channel independent Wi-Fi backscatter is always better than channel dependent approaches.**

I. Introduction

Backscatter techniques have attracted attention from low power wireless communications as well as localization, gesture recognition, and material identification applications [1, 2]. In backscatter systems, a carrier source propagates a continuous wave so that a backscatter tag can utilize it. The tag then inserts data bits into the carrier signal by changing its reflection coefficient. In this way, the tag can transmit various data frames such as an identifier, a voice, or a video [3, 4]. A backscatter receiver decodes the backscatter frame by detecting sudden changes in the received signal.

In Wi-Fi backscatter systems, the tag uses a Wi-Fi frame as a carrier signal [5]. Since the tag reflects every signal received from the antenna, Wi-Fi frames are also reflected by the tag. The main advantage of Wi-Fi backscatter in contrast to other schemes such as radio frequency identification (RFID) is that Wi-Fi devices already deployed around us can serve as carrier sources. This approach eliminates the need for initial installation of dedicated devices such as RFID readers. Another advantage of this approach is backscatter network coverage extension. Reducing the distance from a carrier source to a tag increases the backscatter signal strength [6]. From the perspective of Wi-Fi backscatter, we already deployed carrier sources such as smartphones, laptops, or Wi-Fi access points.

The key challenges of Wi-Fi backscatter are a signal reflection method at the tag and a backscatter demodulation method at the receiver. There are two approaches to solve the challenges. The first approach is in-band Wi-Fi backscatter. In this approach, backscatter frames share the same channel with Wi-Fi frames. The tag changes its reflection coefficient to insert abnormal distortion patterns into the Wi-Fi frame. The receiver then inspects the received data symbols for backscatter demodulation. The second approach is side-band Wi-Fi backscatter. This approach requires an additional oscillator at the tag to generate a high-frequency clock. The tag utilizes the oscillator to create a copy of a received Wi-Fi frame on the side channel. In this process, the tag manipulates the copied frame to insert backscatter data bits. The receiver listens to the side channel and then compares the copied frame with the transmitted frame. The difference between the two frames indicates the backscatter data bits of the tag. The underlying assumption of this technique is a prior knowledge of the transmitted frame. The transmitter may send a dummy frame. Alternatively, we can synchronize two receivers that listen to the transmitted and the side channels.

Both approaches have developed in recent years, but the implementation results reveal their drawbacks. In-band Wi-Fi backscatter has a short communication range. Since a Wi-Fi signal is much stronger than a backscatter signal, it is difficult for the receiver to focus on a backscatter frame. The receiver requires a high-resolution analog-to-digital converter to find a backscatter frame inside a Wi-Fi frame. Side-band Wi-Fi backscatter is free from the power imbalance. The tag creates a frame on the side channel that is separated from the channel of the Wi-Fi devices. However, this design doubles channel occupancy. The tag occupies an additional 20 MHz channel to transmit a backscatter frame. Wireless devices in the side channel experience throughput degradation due to interference created by the tag. To make matters worse, the tag lacks channel selectivity. The tag responds to all incoming signals and copies the signals to the side channels. Not only wireless signals in the Wi-Fi channels but also Bluetooth and ZigBee signals are copied by the tag. The tag also intrudes the licensed spectrum such as the LTE band 7. Most of Wi-Fi antennas receive all wireless signals around 2.45 GHz similar to [2]. In addition, the tag has no ability to distinguish the frequencies of the received signals.

As a solution to the drawbacks, we introduce channel independent Wi-Fi backscatter. Our design is based on in-band backscatter. The tag that we are using has the same architecture as passive RFID tags except for the operating frequency. Although the tag still responds to licensed band signals, the

effect is negligible compared to the communication signals. In contrast, a side-band tag near a transmitter creates interference signals at adjacent frequencies that may overwhelm other communication signals. From the receiver perspective, our design removes channel dependency to be harmonized with more Wi-Fi devices. Wi-Fi frames transmitted near the tag provide backscatter transmission opportunities regardless of their frequencies. However, most of the opportunities has been wasted because an in-band receiver only accepts Wi-Fi frames whose center frequency is the same as the center frequency of the receiver. By contrast, our design utilizes as many transmission opportunities as possible. We implement channel independent packet detection and error vector demodulation on a Wi-Fi receiver with some modifications. The two methods enable the receiver to decode backscatter frames from Wi-Fi frames on the listening channel as well as adjacent channels. The tag utilizes more Wi-Fi devices as carrier sources than before. The additional transmission opportunities created by adjacent channel Wi-Fi devices improve the effective throughput of the tag. Also, an adjacent channel Wi-Fi device, closer to the tag than listening channel Wi-Fi devices, extends the backscatter communication range by reducing the distance from the carrier source to the tag.

In summary, channel independent Wi-Fi backscatter has the following contributions.

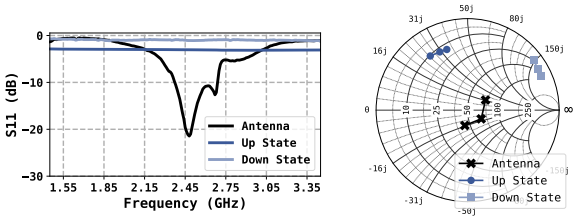
- Expose violation of the wireless regulations and the waste of resources in current Wi-Fi backscatter designs
- Design channel independent packet detection and error vector modulation for better effective throughput and farther communication range
- Implement and validate our design with 802.11n access points and software-defined radios

II. Motivation and Observation

In this section, we investigate side-band and in-band Wi-Fi backscatter in terms of wireless channel. Our interest is a single stream 802.11n frame which consists of 52 data subcarriers and 4 pilot subcarriers as follows:

$$S_n(t) = \frac{1}{K} \sum_k X_{n,k} e^{j2\pi(f_c + k\Delta f)t}, \quad 0 \le t < T \qquad (1)$$

where $S_n(t)$ represents the OFDM symbol n. According to the IEEE 802.11 Standard [7], the symbol duration T, the number of subcarriers K, and the subcarrier spacing Δf are 4 μs, 64, and 312.5 KHz respectively by default. f_c is the center frequency of the frame related to Wi-Fi channels. For example, the center frequency 2462 MHz corresponds to the Wi-Fi channel 11. $X_{n,k}$ denotes the n-th data symbol at the subcarrier k. A backscatter tag receives a Wi-Fi frame $S_n(t)$, and then reflects it after doing some manipulations. The difference between the in-band and side-band Wi-Fi backscatter design is how to represent backscatter bits by using the Wi-Fi frame.



(a) S11 parameter (b) Smith chart

Fig. 1. RF characteristics of a 2.45 GHz 3 dBi omni-directional antenna and the RF front-end of a HitchHike tag.

A. Why Side-band Wi-Fi Backscatter Violates the Regulations?

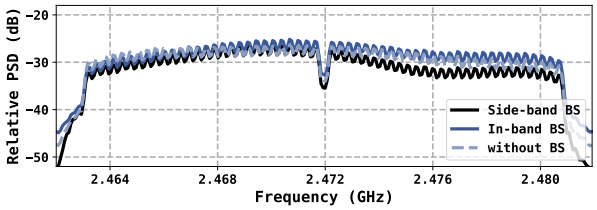
A side-band backscatter tag creates a copy on the adjacent frequencies located f_b away from a received Wi-Fi frame. In detail, the tag feeds a square wave of frequency f_b to an RF switch which decides the reflection coefficient of the tag. Then, the Wi-Fi frame multiplied by the square wave is reflected back from the tag. The square wave is conceptually a periodic repetition of 1 and -1 in the time domain. On the other hand, the square wave is a summation of sine waves in the frequency domain. Suppose $S_n(t)B_n(t)$ is the backscatter signal reflected from the tag. Then, $B_n(t)$ can be written as,

$$B_n(t) = A_n \sum_{m=1,3,5,\ldots} \frac{4}{m\pi} \sin(2\pi m f_b t) \qquad (2)$$

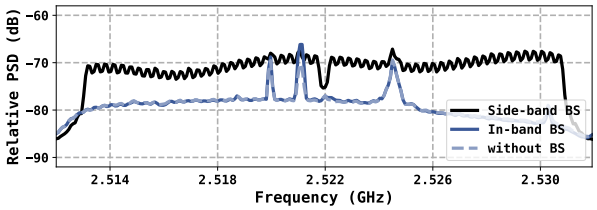
where A_n represents a backscatter symbol, 1 or -1 in general. Since $\sin(2\pi m f_b t)$ can be decomposed into $e^{j2\pi m f_b t}$ and $e^{-j2\pi m f_b t}$, the backscatter signal $S_n(t)B_n(t)$ is at $\pm m f_b$ away from the Wi-Fi frame $S_n(t)$. To eliminate negative frequency components in the square wave, [8, 9] introduce single side-band backscatter. The tag feeds a signal repeating $1+j$, $1-j$, $-1+j$, and $-1-j$ instead of 1 and -1. In addition, [10] introduces the harmonic cancellation technique to suppress undesired harmonics at $3f_b, 5f_b, \ldots$ so that only frequency components of f_b exists.

However, side-band backscatter tags do not abide by the wireless regulation. Assume that we deploy a 50 MHz side-band backscatter tag. The tag creates a channel 11 (2462 MHz) backscatter frame from a channel 1 (2412 MHz) Wi-Fi frame. During this process, the tag inserts backscatter bits into the copied frame by switching A_n in Eq. 2. However, in practice, the tag not only reflects the channel 1 Wi-Fi frame but also reflects all other incoming signals. If there is a Bluetooth device near the tag, then a Bluetooth signal of the advertising channel 39 (2480 MHz) is copied to 2530 MHz. In other instances, if there is a Wi-Fi device using the channel 13 (2472 MHz) near the tag, the tag creates a copied frame at 2522 MHz. Both unintended backscatter signals are outside the ISM band. To make matter worse, the LTE Band 7 uses 2500 $\sim$ 2570 MHz for uplink and 2620 $\sim$ 2690 MHz for downlink.

In contrast to general wireless devices, a backscatter tag omits several circuits such as a down converter and a low-pass filter, since backscatter design aims for ultra-low power



(a) Power spectral density from 2462 MHz to 2482 MHz



(b) Power spectral density from 2512 MHz to 2532 MHz

Fig. 2. Power spectral density measured on a USRP X310 with 50 MHz side-band and 62.5 Kbps in-band backscatter tags while continuously transmitting channel 13 (2472 MHz) Wi-Fi frames.

consumption. Hence, the tag has no way of guessing the frequency of the incoming signal. The tag cannot select signals within a specific frequency range for the same reason. To investigate this problem in detail, we measure the RF characteristics of an antenna and a HitchHike tag [8] with the Keysight N9914A Network Analyzer. First, we measure the $S11$ parameter from 1.45 GHz to 3.45 GHz as shown in Fig. 1(a). The $S11$ parameter means the ratio of the reflected voltage divided by the input voltage. The result shows that the antenna accepts 99% of 2.45 GHz signals and 90% of 2.65 GHz signals. The antenna is optimized at 2.45 GHz as we intended, but it does not mean that the antenna accepts 2.45 GHz ISM band signals only. [2] is an example of this characteristic for a 915 MHz backscatter tag. The up and down states in Fig. 1 denote the two different backscatter symbols of the HitchHike tag. Since the tag controls its reflection coefficient using the Analog Devices ADG902, a reflective RF switch from DC to 4.5 GHz, the $S11$ parameters are -1 dB and -3 dB within the frequency range. Therefore, the tag reflects all incoming signals through the antenna receiving 2.45GHz as well as adjacent frequencies. For further analysis, we measure the reflection coefficient from 2.4 GHz to 2.5 GHz. Fig. 1(b) shows the Smith chart of the antenna and the HitchHike tag. We observe the phase difference of $\pi/2$ between the up and down states, so A_n of our tag can be written as 1 and j.

In order to show that a side-band backscatter tag invades the licensed band, we conduct an experiment about spectral occupancy. In this experiment, a Wi-Fi access point beside the tag transmits channel 13 Wi-Fi frames. We then place a USRP X310 to monitor the channels. The USRP only gives relative received signal strength rather than accurate values, but the implication of our experiment does not change since our interest is whether the tag interferes the licensed band or not. The first daughterboard of the USRP listens to the channel

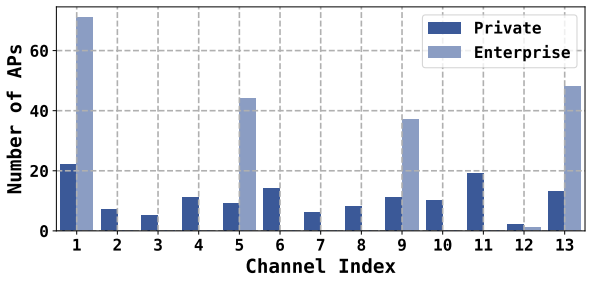


Fig. 3. Wi-Fi channel statistics collected from the campus.

13 and the second daughterboard listens to 2522 MHz with 20 MHz bandwidth. Fig. 2 shows the relative power spectral density for the two channels. From the viewpoint of signal strength, the tag does not make any change on the channel 13. However, we observe the distinct difference between in-band and side-band backscatter from Fig. 2b. The presence of the in-band backscatter tag does not change the result. However, the side-band backscatter tag creates interference signals strong enough to overwhelm existing signals. This situation also occurs around 2.3 GHz in our testbed. The device makes 2390 MHz signals from 2340 MHz licensed band signals. The observation results indicate that the side-band backscatter design violates the wireless regulations and cannot be deployed in the real world.

B. Why In-band Wi-Fi Backscatter Wastes Resources?

We also need to consider the lack of channel selectivity of a backscatter tag for in-band Wi-Fi backscatter receiver design. Wi-Fi signals outside the listening channel have been ignored so far in in-band backscatter designs [5]. From the viewpoint of a Wi-Fi receiver, it is natural to ignore received signals not in the listening channel, because the receiver cannot decode whole subcarriers. On the contrary, the backscatter receiver is not in the same position. The tag reflects all incident signals regardless of their frequencies as shown in Fig. 1. Thus, the receiver should inspect all received Wi-Fi frames no matter what channel it uses. However, there was no in-band Wi-Fi backscatter considering this aspect. Fig. 3 shows the Wi-Fi channel statistics of our university campus. We scan access points at 6 locations. Access points deployed by our university and ISPs are classified as enterprise access points. The rest are private access points. The enterprise access points use the channels 1, 5, 9, and 13 that are the best practice of channel planning in the most of world. In North America, enterprise access points use the channels 1, 6, and 11, because using the channels 12 and 13 is not allowed. The private access points do not follow the best practice. Considering the channel statistics, the channel dependency of the backscatter receiver causes a large amount of resource waste. The tag responds to all channels, but the receiver listens to a single channel.

The channel dependency of the backscatter receiver causes negative effects on the throughput and the communication range. According to the principle of Wi-Fi backscatter, Wi-

Fi devices already deployed around us can serve as carrier emitters. This design improves the communication range of a backscatter tag thanks to the dense deployment of carrier emitters as described in [6]. Communication range extension is equivalent to improvement of backscatter signal strength, which enables high data rate backscatter transmission. The more Wi-Fi devices are placed around the tag, the more opportunities the tag can transmit frames farther and faster with an appropriate rate adaptation algorithm. However, unfortunately, current Wi-Fi backscatter schemes do not come up to the expectation, because they can utilize a part of Wi-Fi devices in the same channel with the backscatter receiver. If there is a way to take advantage of Wi-Fi devices outside the receiver's channel, tags will experience better communication performance than before. This is the reason why we design channel independent Wi-Fi backscatter.

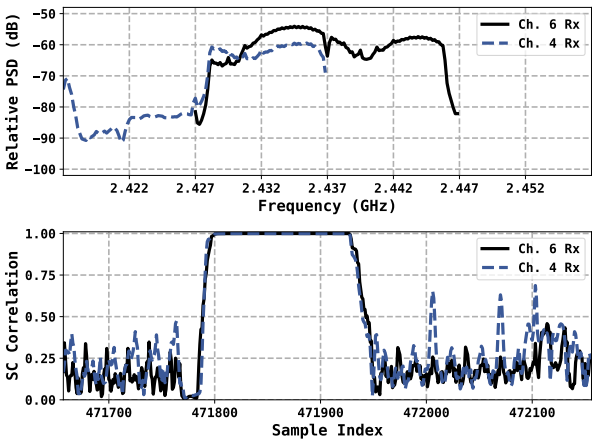
III. Channel Independent Wi-Fi Backscatter

In this section, we introduce channel independent Wi-Fi packet detection and error vector demodulation. We first show that a Wi-Fi receiver can detect frames on both the listening and adjacent channels after some modifications. Then, we introduce error vector demodulation that finds backscatter symbols inside the Wi-Fi frame regardless of the channel. With these efforts, our receiver monitors multiple channels simultaneously so that the tag interacts with as many Wi-Fi devices as possible. We omit backscatter tag design in this paper, because we use a simple on-off keying backscatter tag like an RFID tag.

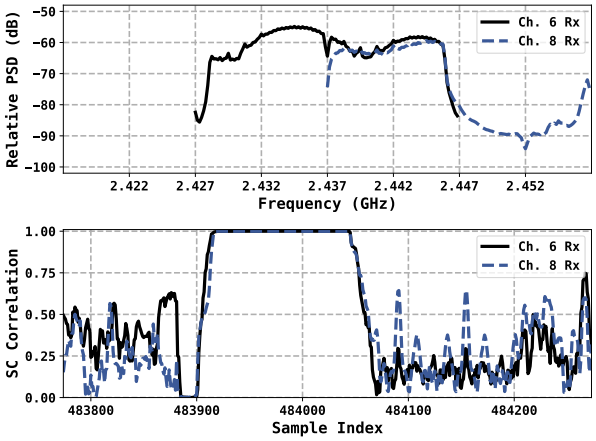
A. Channel Independent Wi-Fi Packet Detection

A Wi-Fi receiver consists of multiple processing blocks such as equalizer, demodulator, and decoder. Among these blocks, our interest is a packet detector. A Wi-Fi transmitter adds a preamble before sending a data frame. The preamble begins with the short training field that repeats the short training sequence 10 times. The role of the packet detector is finding the short training field. The most common detection method is the Schmidl-Cox algorithm [11, 12]. This algorithm finds the periodic signal repetition instead of correlating a received signal with the short training sequence. Wireless signals experience unpredictable attenuation and distortion throughout signal propagation, so the received preamble is far different from the short training sequences. Nevertheless, the received preamble evenly experiences the attenuation and the distortion, so similarity between the 10 repeating sequences is the same as before. The packet detector calculates the correlation between the received signal and the delayed signal to find the short training field. When the receiver detects a correlation plateau having a length similar to the short training field, the receiver initiates the next procedure.

One interesting feature of the Schmidl-Cox algorithm is that it does not care about the channel of the received frame. The receiver cannot explain the reason why the frame is distorted. The preamble may be distorted during wireless propagation. Otherwise, the preamble may look different from



(a) Listening to the channel 4 and 6 simultaneously

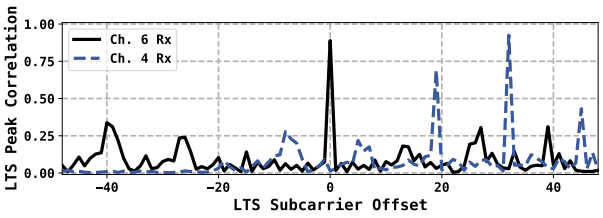


(b) Listening to the channel 6 and 8 simultaneously

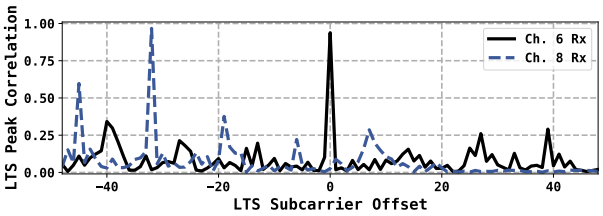
Fig. 4. Schmidl-Cox correlation and power spectral density measured on two different daughterboards of a USRP X310 while continuously transmitting channel 6 Wi-Fi frames.

the short training sequences, because the preamble is not in the listening channel. Even if the frame is not on the same channel as the receiver, the packet detector observes a valid correlation plateau, because the interest of the packet detector is the periodic signal repetition. The short training field in the adjacent channel frame also shows periodic repetition of the short training sequences of the adjacent channel. Therefore, Wi-Fi frames detected by the Schmidl-Cox algorithm are not related with the Wi-Fi channel.

To validate that the Schmidl-Cox algorithm accepts not only listening channel frames but also adjacent channel frames, we conduct an experiment. There are an access point and a client using the channel 6. We run *iperf3* on the Wi-Fi devices to generate data frames. We then place a USRP X310 listening to two different channels simultaneously. The first daughterboard of the USRP listens to the channel 6 (2437 MHz). The second daughterboard listens to the channel 4 (2427 MHz) once and the channel 8 (2447 MHz) once. Fig. 4 shows the relative power spectral density of the received



(a) LTS correlation measured on the channel 4 and 6



(b) LTS correlation measured on the channel 6 and 8

Fig. 5. Long training sequence peak correlation of a channel 6 Wi-Fi frame while varying the subcarrier offsets.

signals and the correlation plateau of the Wi-Fi frame in each channel. The relative power spectral density shows that the second daughterboard receives a half of the subcarriers, but we observe almost same correlation plateaus for the two different daughterboards. Although a center frequency of a received Wi-Fi frame is not same as the center frequency of the receiver, the receiver concludes that it is receiving a valid Wi-Fi frame and then initiates the next procedure.

The next receiving procedure after the Schmidl-Cox packet detection is timing synchronization using the long training field. The long training filed is transmitted just after the short training field. The long training field contains the two long training sequences and one cyclic prefix. The synchronizer finds an accurate boundary of the long training sequences so that the equalizer can correct frequency offsets and estimate channel state information before taking FFT. The synchronizer calculates a correlation between a received signal and the long training sequence. The ideal correlation result shows the two sharp peaks that are 64 samples distant from each other. The positions of the two peaks correspond to the boundaries of the long training sequences. If the distance between the two peaks is far from 64 samples, then the receiving procedure is suspended until a new valid correlation plateau is detected. Hence, adjacent channel Wi-Fi frames accepted by the Schmidl-Cox packet detector are discarded by the synchronizer due to incorrect correlation results of the long training sequence.

Discarding adjacent channel Wi-Fi frames is not desirable in Wi-Fi backscatter networks. The frames may deliver backscatter frames, so a backscatter receiver should accept as many Wi-Fi frames as possible. In addition, the receiver should identify the channel of the received frame to determine which subcarriers should be inspected. To achieve these goals, we modify the synchronizer. The receiver emulates frequency shifted long training sequences for adjacent channels. In the frequency domain, a 20 MHz Wi-Fi symbol consists of 64 subcarriers. This feature can be explained in a different way. The channel offset C is the same as the subcarrier offset $16C$. Suppose that a channel 4 receiver gets a channel 6 Wi-Fi frame. The channel 6 frame contains the long training sequence consisting of subcarriers located from -26 to 26 (-28 to 28 for the HT-LTS). From the viewpoint of the channel 4 receiver, the subcarriers of the channel 6 frame are located from 6 to 31. The receiver observes a shifted OFDM frame and the subcarriers outside the bandwidth are discarded. Fig. 5 shows the long training sequence correlation peak for a channel 6 Wi-Fi frame while varying the subcarrier offset. The USRP listens to the channels 4, 6, and 8 respectively the same as before. The long training sequence without subcarrier offset is suitable for the channel 6 receiver. From the channel 4 receiver's perspective, the long training sequence is shifted to the right, resulting in the best correlation at the subcarrier offset 32. Similarly, the channel 8 receiver observes the best correlation at the subcarrier offset -32. In this way, our scheme finds the best subcarrier offset among -32, -16, 0, 16, and 32 to estimate the channel index of the received frame. Because the receiver cannot decode the L-SIG field for adjacent channel frames, the receiver concludes that the frame reaches the end of the frame when a symbol power is 8 times weaker than the long training sequence power.

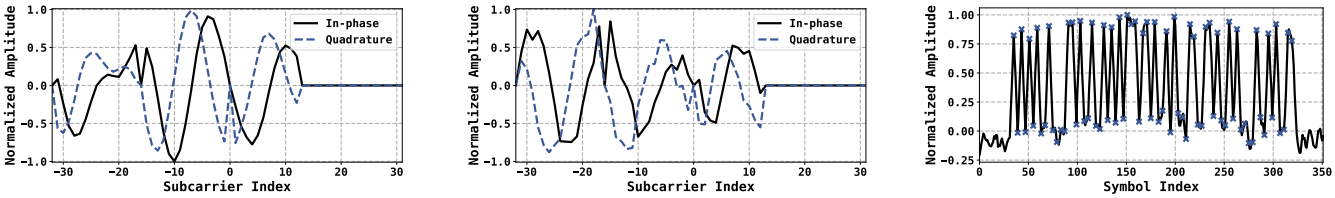
B. Error Vector Demodulation

We analyze error vectors of received symbols for backscatter signal demodulation. The error vector is the difference between the data symbol and the received symbol. In common wireless communication systems, a noise is the major cause of the error vector. By contrast, in backscatter communication systems, the error vector is another representation of a backscatter signal.

$$Y_k[n] = e^{jn(\phi_c + k\phi_s)} \left(H_k + H_k^{'} B[n] \right) X_k[n] \qquad (3)$$

This equation represents the n-th received symbol at the subcarrier k. The received symbol consists of a data symbol $X_k[n]$, a channel H_k, and phase shifts, ϕ_c and ϕ_s, caused by carrier frequency and timing offsets. The received symbol also contains a backscatter signal $H_k^{'} B[n]$, where $H_k^{'}$ is a channel of a backscatter link and $B[n]$ is a backscatter data bit of 0 or 1. When $B[n]$ becomes one, the error vector contains a noise signal as well as a backscatter signal. Detecting this change is the principle of error vector demodulation.

Backscatter signal is negligible compared to Wi-Fi signals in general. Additional error vector created by a backscatter tag seldom affects Wi-Fi frame decoding results. Thus, the receiver proceeds the equalization and demodulation procedures the same as before. The receiver estimates H_k, ϕ_c, and ϕ_s based on the long training field and the pilot tones. For adjacent channel frames, the receiver estimates the modulation scheme of the frame by analyzing the first four data symbols. The correct modulation scheme produces the smallest error



(a) CSI of the adjacent channel Wi-Fi frame (b) CSI of the backscatter frame (c) Error vectors after equalization and summation

Fig. 6. Error vector demodulation procedures to extract the backscatter frame from the adjacent channel Wi-Fi frame.

vector compared to other modulation schemes. With the estimation results, the receiver reverts the signal distortion to infer the data symbol $X_k[n]$. Additionally, the backscatter receiver reverts the data symbol once again to get the error vector as follows.

$$\bar{Y}_k[n] = \frac{Y_k[n]}{H_k X_k[n]} = e^{jn(\phi_c + k\phi_s)} \left(1 + \bar{H}_k B[n]\right) \quad (4)$$

The receiver does not utilize ϕ_c and ϕ_s estimated during the Wi-Fi receiving procedures, because the receiver does not separate phase shifts and a backscatter signal at that stage. Instead, the receiver analyzes the first part of the error vectors where $B[n] = 0$, and then it reverts the phase shifts for the rest of the error vectors. Eventually, the error vector becomes $1 + \bar{H}_k B[n]$ in which only a backscatter signal remains.

To get the backscatter data bit $B[n]$, we estimate the residual channel $\bar{H}_k = H_k^{'}/H_k$ using the preamble of the backscatter frame. The backscatter frame starts with a preamble bits 10101010 in this work. Similar to Wi-Fi equalization, the receiver estimates the residual channel $\bar{H}_k$ from the first eight bits for all valid subcarriers. The receiver removes the constant component from the error vector and converts the result into the backscatter data bit by dividing the residual channel $\bar{H}_k$. Fig. 6 illustrates the error vector demodulation procedures for a 5 MHz adjacent 802.11n frame. Since the 802.11n frame uses subcarriers from -28 to 28, the received subcarriers are located from -32 to 12 as shown in Fig. 6(a). The receiver utilizes the emulated long training sequence, shifted to the left by 16 subcarriers, to estimate the channel state information of the frame. The subcarrier 0 and -16 are the DC components of the transmitter and receiver. Fig. 6(b) shows the residual channel state information. Previous in-band backscatter schemes [5, 13] add up the error vectors like $\sum \bar{H}_k B[n]$ to get backscatter symbols. However, adding up the error vectors without proper processing is not desirable, since the error vectors may cancel each other. For example, the residual channels of the subcarrier -30 and -24 are canceled. This is the reason why we estimate and equalize the residual channel once again before adding up the error vectors. In the end, the receiver gets a backscatter symbol as shown in Fig. 6(c). The data rate of the tag is 62.5 Kbps in this example. The tag uses 4 Wi-Fi symbols (16 μs) to transmit a single data bit. We can observe that the backscatter symbols after equalization and summation are separated into two clusters like RFID signals.

IV. Evaluation

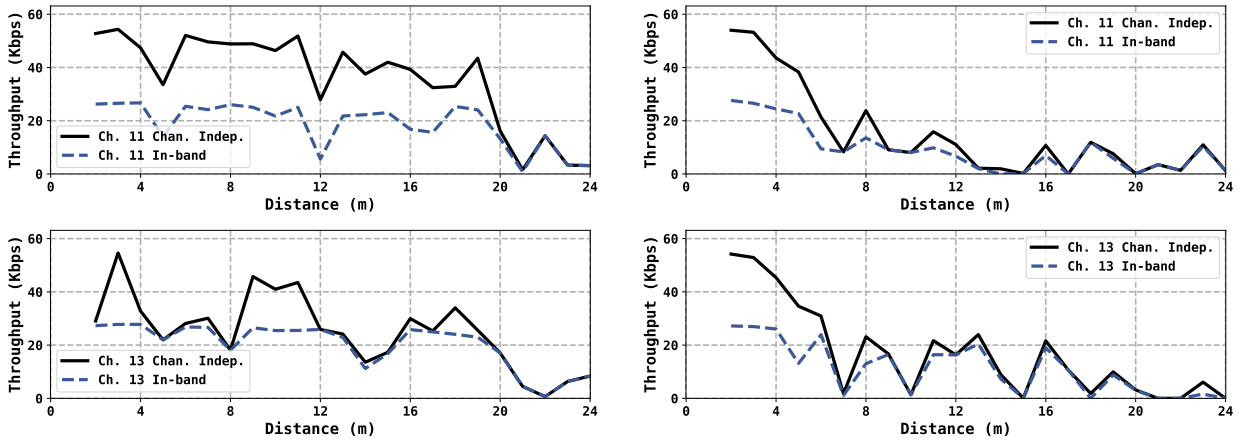
In this section, we describe how we implement and evaluate channel independent Wi-Fi backscatter. We measure throughput and communication range of a backscatter link in both line-of-sight and non-line-of-sight environments. We then discuss the evaluation results in terms of adjacent channels. Finally, we evaluate the side effects caused by the tag with respect to Wi-Fi networking performance.

A. Experimental Setup

Our experimental setup consists of 802.11n devices, a software-defined radio, and a backscatter tag. The backscatter tag is based on the HitchHike platform [8]. We use the same hardware schematic, but we modify the software stack to transmit a backscatter frame with simple on-off keying. The tag starts transmission when it receives a wireless signal stronger than a certain threshold longer than 160 μs. The backscatter frame is composed with an 8 bits preamble and an 8 bytes payload. The data rate of the tag is 62.5 Kbps. We use an AR9380 802.11a/b/g/n chip on a TP-Link Archer C7 as a carrier source. The access point sends an 802.11n frame to a client at a chip's maximum transmission power 13 dBm. A software-defined radio platform USRP X310 with two SBX-120 daughterboards serves as a backscatter receiver. Since there is no automatic gain control in the receiver, we fix the receiver gain to 30 dB for all measurements. We use 2.45 GHz omni-directional antennas for all devices.

B. Backscatter Throughput

We conduct an experiment on throughput and communication range measurement for channel independent Wi-Fi backscatter. We deploy two pairs of an 802.11n access point and a client. The first pair uses the channel 11 and the second pair uses the channel 13. We run *iperf3* on the access points for traffic generation with MCS 0. Note that our approach does not utilize any prior knowledge about packet payloads compared to the recent Wi-Fi backscatter designs [8, 9, 14, 15]. The error vectors can be measured no matter what payload is transmitted. In this experiments, the tag is 1 m away from the access points. The distance between the tag and the receiver varies from 2 m to 24 m. In the LoS scenario, all devices are placed along the corridor. In the NLoS scenario, the access point and the tag are placed behind the corner while the receiver moves along the corridor.



(a) Line-of-sight environment

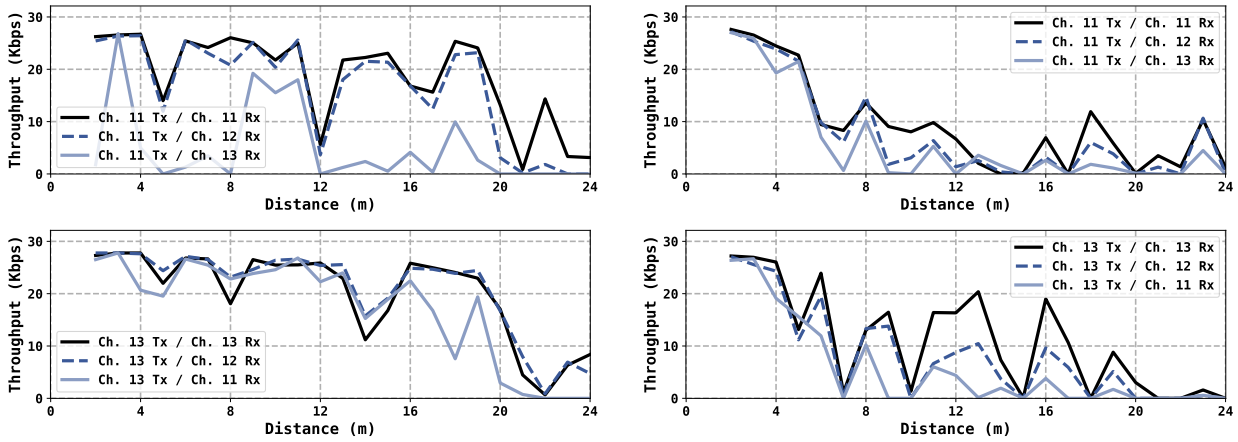
(b) Non-line-of-sight environment

Fig. 7. Backscatter throughput for the channel independent and in-band band designs.

In this evaluation, we get comparable results to the side-band backscatter scheme [14] and much better results than the in-band backscatter scheme [13]. We can say that channel independent Wi-Fi backscatter outperforms the in-band backscatter scheme because we implement and evaluate it. However, we cannot say that our approach, not the result, shows comparable performance to the side-band backscatter in terms of throughput. First, a USRP X310 is designed for various wireless experiments rather than 2.45 GHz OFDM communications. It has a 14-bit ADC capable of high-resolution inspection of error vectors, but does not have an automatic gain control and well-optimized signal processing components compared to commodity Wi-Fi devices. Secondly, the phase difference of the up and down states is $\pi/2$ in our tag as shown in Fig. 1(b), whereas the best phase difference is π. For these reasons, we try to implement single side-band Wi-Fi backscatter like [8, 14] to compare the communication performance with our approach. However, a single HitchHike tag can reproduce double side-band backscatter only. Two HitchHike tags, an RF splitter, and a $\pi/4$ transmission line are required to implement single side-band backscatter. There are interference signals from Wi-Fi to LTE in addition to interference signals from LTE to Wi-Fi as shown in Fig. 2 with a double side-band backscatter tag. Also, harmonics in Eq. 2 (m = 3, 5, 7, ...) make interference problem worse. Therefore, the throughput comparison between channel independent and single side-band Wi-Fi backscatter is the focus of future work.

We first measure the backscatter throughput in both line-of-sight and non-line-of-sight environments. Fig. 7(a) shows the throughput in the line-of-sight environment. We evaluate both channel independent and in-band Wi-Fi backscatter. The in-band backscatter receiver only accepts frames in the listening channel, whereas the channel independent backscatter receiver accepts listening channel frames as well as adjacent channel frames. For this reason, the channel independent backscatter receiver gets about two times more communication opportunities than the other. However, it does not mean that the backscatter throughput is doubled. A backscatter signal is spread out over 56 subcarriers of a Wi-Fi frame. For example, when the channel 11 receiver gets a channel 11 Wi-Fi frame, it decodes the frame using the 56 subcarriers. In contrast, the channel 11 receiver utilizes 28 subcarriers for a channel 13 Wi-Fi frame. The backscatter throughput is doubled if a backscatter signal in an adjacent channel frame is strong enough, but the throughput gain drops sharply as the tag moves away from the receiver. We observe the throughput gain clearly with the line-of-sight channel 11 receiver. The line-of-sight channel 13 receiver shows unstable throughput gain compared to the channel 11 receiver. We guess that subcarriers from 2462 MHz to 2472 MHz are nullified during propagation. This selective fading of a Wi-Fi backscatter signal was observed in previous studies [5, 16]. Fig. 7(b) shows the throughput in the non-line-of-sight environment. The throughput decreases faster than the line-of-sight environment since the receiver gets weak signals. For the same reason, the throughput gain from adjacent channel frames almost disappears when the receiver is farther than 8 m.

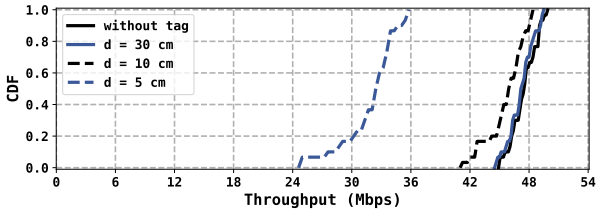
To investigate the effects of the channel offset, we measure the backscatter throughput on the channels 11, 12, and 13. In other words, the measurements show the performance degradation with the subcarrier offset of -32, -16, 0, 16, and 32. We first decode backscatter frames on the three different channels in the line-of-sight environment as shown in Fig. 8(a). We observe the best throughput when the receiver performs error vector demodulation on the listening channel. The throughput decreases as the channel offset increases since the receiver has fewer subcarriers to inspect. The results from the non-line-of-sight environment show the similar pattern as shown in Fig. 8(b). For both line-of-sight and non-line-of-sight environments, the channel independent receiver decodes backscatter frames in the listening channel as well as the adjacent channels. We demonstrate our design on the channels



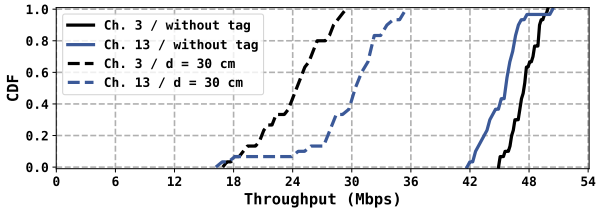
(a) Line-of-sight environment

(b) Non-line-of-sight environment

Fig. 8. Backscatter throughput versus the channel offset between the transmitted and listening channels.



(a) Wi-Fi throughput with the 62.5 Kbps in-band backscatter tag



(b) Wi-Fi throughput with the 50 MHz side-band backscatter tag

Fig. 9. Throughput measured on the access points with and without in-band and side-band backscatter tag.

11, 12, and 13 in this experiment, but other channels also can be used. For example, a channel independent receiver listening to the channel 7 inspects Wi-Fi frames of the channels 5, 6, and 9 that are the frequently used channels by commodity access points as shown in Fig. 3.

C. Side Effects on Wi-Fi Networks

To evaluate the side effects of a backscatter tag on Wi-Fi networks, we conduct experiments on Wi-Fi throughput. We place two pairs of 802.11n devices. The access points and the clients are 3 m distant from each other. The distance between the access points is 0.6 m. The first pair uses the channel 3 and the second pair uses the channel 13. The devices adjust their MCS from 0 to 7 based on the minstrel algorithm. We run *iperf3* on the devices to measure the Wi-Fi throughput with and without the tag while varying the distance d between the tag and the access point.

We first measure the side effect of a 62.5 Kbps in-band backscatter tag on the channel 3. Because channel Wi-Fi independent backscatter is based on the same tag as in-band backscatter, the measurement result also describes the side effect of channel independent Wi-Fi backscatter. As described in Eq. 3, the tag creates additional error vectors inside the data symbols. The Wi-Fi throughput is reduced if the error vectors are strong enough to cause demodulation errors. Fig. 9(a) shows the throughput with and without the in-band backscatter tag. We observe a little throughput degradation for the tag 10 cm away from the access point. The side effect becomes evident when the tag is located 5 cm away from the access point.

Side-band backscatter affects Wi-Fi networks in different ways. In this experiment, we use a 50 MHz double side-band backscatter tag. The tag creates a channel 3 frame by using a channel 13 Wi-Fi frame and vice versa. In other words, Wi-Fi devices share the channel through the tag. To investigate the effect of the tag, we place the tag at the center of the access points. Fig. 9(b) shows the side effect caused by the tag. The result shows that there is evident throughput reduction due to the tag. Because the tag connects the channel 3 and 13, the access points contend each other to take a transmission opportunity. Therefore, the access points show almost half throughput. If we use a single side-band backscatter tag, there is no throughput degradation on the channel 3. However, the tag interferes with the channel 13 aggressively more than before. With a double side-band backscatter tag, Wi-Fi devices perform clear channel assessment on the shared channel before transmission. In contrast, with a single side-band backscatter tag, channel 3 Wi-Fi devices transmit frames regardless of the channel 13 occupancy. The tag copies every channel 3 frame to the channel 13. From the viewpoint of channel 13 Wi-Fi devices, the tag is an unpredictable interference source.

V. Related Work

Backscatter systems based on Wi-Fi devices have evolved rapidly in recent years. Wi-Fi backscatter [5] demonstrates this approach for the first time. It shows that a Wi-Fi receiver can decode backscatter frames by analyzing the sequence of channel state information. Since the tag requires one or more Wi-Fi frames to represent a single backscatter bit in this approach, the data rate of the tag is limited to a few Kbps.

To overcome the poor communication performance, Passive Wi-Fi [17] introduces a side-band backscatter design. A tag generates a square wave to create 802.11b frames by using a single tone transmitter. Interscatter [9] has taken this approach one step further. Instead of the single tone transmitter, it utilizes a Bluetooth device transmitting a special dummy frame for single tone signal emulation. In other words, a tag creates 802.11b frames from a special Bluetooth frame. Similarly, HitchHike [8] introduces Wi-Fi backscatter systems consisting of 802.11b devices. A tag copies 802.11b frames to the side channel. The transmitter and receiver are replaced with 802.11g/n devices in FreeRider [14]. This design also introduces a tag creating Bluetooth and ZigBee frames in the same principle. MOXcatter [15] extends the scope of Wi-Fi backscatter. It shows that 802.11n MIMO frames also can be used for backscatter communications. However, side-band backscatter schemes have achieved these goals while violating the wireless regulations. We should design side-band backscatter systems in which tags do not invade the licensed band.

There are several attempts to improve Wi-Fi backscatter systems in other ways. [18] provides a generalized backscatter communication performance analysis model for OFDM carrier signals. [19] introduces another method to decode backscatter frames inside OFDM symbols. It compares the latter part of the symbol with the cyclic prefix to detect whether the tag changes its reflection coefficient within the symbol. In contrast, [13] proposes a flicker detection method that focuses on the change of residual channel across a Wi-Fi frame. These approaches are classified as channel dependent in-band backscatter. The receiver only accepts listening channel Wi-Fi frames, whereas other frames in adjacent channels are also conveying backscatter frames. [20] introduces a universal backscatter receiver that combines ambient signals from FM, TV, and cellular towers. It also points out the channel dependency problem, but it solves the problem by combining multiple receivers. In contrast, we introduce the backscatter demodulation scheme with a single receiver.

VI. Conclusion

In this paper, we introduce why a backscatter tag lacks channel selectivity and why the tag causes problems in Wi-Fi backscatter networks. To solve the problems, we design the channel independent Wi-Fi backscatter receiver. The receiver accepts Wi-Fi frames not only in the listening channel but also in the adjacent channels. The receiver then inspects the error vectors of the frame to extract backscatter symbols. According to our experiments, the receiver is able to decode backscatter frames in the listening channel as well as the adjacent channels and is always superior to the channel dependent backscatter receiver. We believe that our design provides a novel solution to the channel selectivity problem of a backscatter tag.

Acknowledgment

This research was partly sponsored by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science and ICT (No. 2017R1A2B2004811), and Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (No. 2017M3C4A7083676). Wonjun Lee is the corresponding author.

References

[1] J. Wang, J. Xiong, X. Chen, H. Jiang, R. K. Balan, and D. Fang, "Tagscan: Simultaneous target imaging and material identification with commodity rfid devices," in *Proc. of ACM MobiCom*, 2017.

[2] Y. Ma, N. Selby, and F. Adib, "Minding the billions: Ultra-wideband localization for deployed rfid tags," in *Proc. of ACM MobiCom*, 2017.

[3] V. Talla, B. Kellogg, S. Gollakota, and J. R. Smith, "Battery-free cellphone," *Proc. of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, pp. 25:1–25:20, June 2017.

[4] S. Naderiparizi, M. Hessar, V. Talla, S. Gollakota, and J. R. Smith, "Towards battery-free HD video streaming," in *Proc. of USENIX NSDI*, 2018.

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

[6] P. N. Alevizos, K. Tountas, and A. Bletsas, "Multistatic scatter radio sensor networks for extended coverage," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4522–4535, July 2018.

[7] *IEEE Std 802.11-2016, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Dec 2016.

[8] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "Hitchhike: Practical backscatter using commodity wifi," in *Proc. of ACM SenSys*, 2016.

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

[10] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, "Lora backscatter: Enabling the vision of ubiquitous connectivity," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 3, pp. 105:1–105:24, Sep 2017.

[11] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, Dec 1997.

[12] R. Bhardwaj, K. Chintalapudi, and R. Ramjee, "Skip-correlation for multi-power wireless carrier sensing," in *Proc. of USENIX NSDI*, 2017.

[13] T. Kim and W. Lee, "Exploiting residual channel for implicit wi-fi backscatter networks," in *Proc. of IEEE INFOCOM*, 2018.

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

[15] J. Zhao, W. Gong, and J. Liu, "Spatial stream backscatter using commodity wifi," in *Proc. of ACM MobiSys*, 2018.

[16] Z. Yang, Q. Huang, and Q. Zhang, "Nicscatter: Backscatter as a covert channel in mobile devices," in *Proc. of ACM MobiCom*, 2017.

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

[18] D. Darsena, G. Gelli, and F. Verde, "Modeling and performance analysis of wireless networks with ambient backscatter devices," *IEEE Transactions on Communications*, vol. 65, no. 4, pp. 1797–1814, April 2017.

[19] G. Yang, Y. C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient ofdm carrier," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1219–1233, March 2018.

[20] C. Yang, J. Gummeson, and A. Sample, "Riding the airways: Ultra-wideband ambient backscatter via commercial broadcast systems," in *Proc. of IEEE INFOCOM*, 2017.