# Exploiting Residual Channel for Implicit Wi-Fi Backscatter Networks

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

***Abstract*—The emerging deployment of IoT devices increasingly requires more energy-and-cost-efficient wireless links between devices. Nowadays backscatter networks, one of the most feasible technology to meet the requirement in IoT spaces, have evolved for better usability and wider coverage. The most likely consequence of the evolution is Wi-Fi backscatter networks that harmonize with widely deployed commercial devices. However recent Wi-Fi backscatter techniques are stuck in front of several hurdles. The backscatter techniques along with 802.11b devices impair the spectral efficiency of wireless channels and break backward compatibility. Meanwhile, the backscatter techniques along with the other types of 802.11 devices support only per-packet backscatter resulting poor performance. To tackle all these problems, we propose a flicker detector that achieves per-symbol in-band backscatter by exploiting residual channel of Wi-Fi packets. Our approach shows robust performance without any modification on the hardware and any side effect on wireless channels. Extensive experiments on a software-defined radio testbed demonstrate that our approach overcomes the hurdles of existing Wi-Fi backscatter networks.**

***Index Terms*—Backscatter, Wi-Fi, Internet of Things**

## I. Introduction

The basis of the IoT is a low power device consistently generating vast amounts of unstructured data sent to cloud or edge servers. This paradigm emphasizes the importance of energy efficient wireless networks. For now, there are several wireless technologies for connecting the IoT devices. However, manufacturers are reluctant to use them because there is no outstanding technology that dramatically reduces the energy consumption of data transmission compared to others. In this regard, backscatter has been attracted as a promising wireless technology to connect the devices.

A backscatter node does not generate a carrier signal, but borrows carrier signals from neighboring wireless devices, called as carrier emitters. More specifically, the backscatter node changes its load impedance to select whether absorbing or reflecting incident signals. When the backscatter node is in the reflection state, all incident signals coming through the receiving antenna are reflected, whereas no signal is reflected back when the backscatter node is in the absorption state. A backscatter receiver infers the state of the backscatter node from received signals and then decodes the transmitted bits. According to this scheme, a backscatter node consumes almost zero energy for data transmission.

Deploying carrier emitters and receivers is one of the major challenges in backscatter networks. Traditional backscatter systems, such as radio frequency identification (RFID), install a dedicated reader that serves as a carrier emitter and a receiver at the same time. However, this system model has two crucial drawbacks, short communication range and initial deployment costs. As a solution to the problem, [1] separates carrier emitters and receivers to improve backscatter communication range about 10 times, while the carrier emitters and receivers operate same as before. This approach sheds light on how to extend the coverage of backscatter networks. However, this approach still requires initial deployment costs.

Ambient backscatter is a promising solution for providing connectivity to backscatter nodes [2]. The ambient backscatter nodes modulate its bits through ambient RF carriers emitted by existing communication systems. Riding broadcast signals from TV towers or FM radio stations removes concerns about initial deployment costs in outdoor environments [3], [4]. For indoor scenarios, we can utilize commercial wireless devices already deployed around us. For example, a backscatter node can ride on an 802.11b packet or a Bluetooth packet to create another 802.11b packet [5], [6]. This approach clears up communication range and deployment costs issues. Unfortunately, however, this approach impairs spectral efficiency of wireless channels, since it exploits side-band backscatter requiring an additional channel for backscatter transmission. Moreover, this approach breaks backward compatibility. Side-band backscatter entails hardware modification on a backscatter node for much higher clock rate than the EPC Gen 2 Standard [7].

For these reasons, in-band Wi-Fi backscatter has attracted attention. In-band backscatter does not intrude other channels while providing backward compatibility. The theoretical performance of this approach is evaluated in [8] under the assumption of perfect channel knowledge. [9] is the first to show per-packet in-band Wi-Fi backscatter. Per-packet means that only a single backscatter symbol can be embedded in a Wi-Fi packet which takes at least 40 $\mu$s. Thus this approach entails short communication range and low throughput. [10] shows per-symbol in-band Wi-Fi backscatter with a specially designed hardware for self-interference cancellation. However, since this approach cannot separate a carrier emitter and a receiver, the drawbacks of traditional backscatter systems occur again.

978-1-5386-4128-6/18/$31.00 ©2018 IEEE

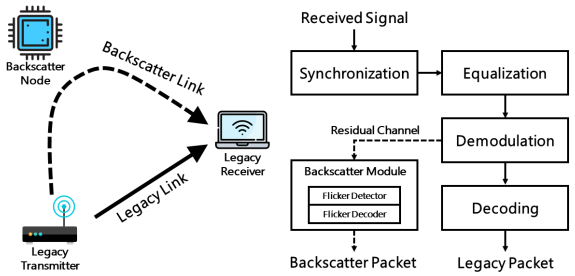



Fig. 1. Implicit Wi-Fi Backscatter systems consist of a legacy transmitter-receiver pair and a backscatter node. The legacy receiver accommodates the backscatter module that analyzes flickers of a residual channel.

In this paper, we introduce an implicit Wi-Fi backscatter scheme that exploits a residual channel to achieve per-symbol in-band backscattering without any hardware modifications for both Wi-Fi devices and backscatter nodes. We implement a backscatter module which draws out a residual channel from a Wi-Fi receiver similar to [11], [12]. A flicker detector picks sudden changes of a residual channel caused by a backscatter node, and then a flicker decoder translates the sequence of changes into a backscatter packet. The main contributions of this paper are summarized as follows

- We implement per-symbol in-band Wi-Fi backscatter without any hardware modifications
- We propose a flicker detector and a flicker decoder that logically transform Wi-Fi backscatter systems into traditional backscatter systems
- We validate the feasibility of implicit Wi-Fi backscatter networks based on the software-defined radio platform

## II. System Model

In this section, we introduce implicit Wi-Fi backscatter systems that deliver backscatter packets through Wi-Fi devices. Our design basically follows the IEEE Standard 802.11-2016, especially for SISO OFDM systems [13]–[15]. But, it should be noted that our design also can be applied to other OFDM systems such as LTE, since a residual channel is always present in OFDM systems.

### A. Legacy Receiver Architecture

Fig. 1 shows an architecture of implicit Wi-Fi backscatter systems. The legacy transmitter-receiver pair operates same as before. The pair establishes a legacy link to convey OFDM packets. Meanwhile, a backscatter node gets on the legacy link to modulate its bits. We call the influence of the backscatter node as a backscatter link. From the perspective of the legacy receiver, the backscatter link seems like a weird channel continuously blinking. The additional role of the legacy receiver in implicit Wi-Fi backscatter systems is diagnosing the fluctuation of the channel. Before discussing how to diagnose the fluctuation, we inspect the architecture of the legacy receiver consisting of several procedures.

In Wi-Fi, a special signal called as preamble is inserted ahead of each packet. The preamble contains the short training sequence (STS) and the long training sequence (LTS) for the synchronization and the equalization procedure. In the synchronization procedure, a legacy receiver detects the arrival of a legacy packet by using the STS [16]. Then carrier frequency offset correction and timing synchronization are performed. After the synchronization procedure, the legacy receiver performs the Fast Fourier Transform (FFT) to handle legacy packets in the frequency domain. In the equalization procedure, the legacy receiver estimates distortion of the legacy packet by comparing it with the LTS. The distortion is described in channel state information (CSI). After the estimation, the legacy receiver utilizes CSI to revert the distortion. Lastly, the legacy receiver infers the most probable data symbols in the demodulation procedure, and then the symbols are decoded into bits in the decoding procedure.

The effect of backscatter is observed in a channel of a legacy link. More specifically, a legacy receiver experiences the effect of backscatter as follows.

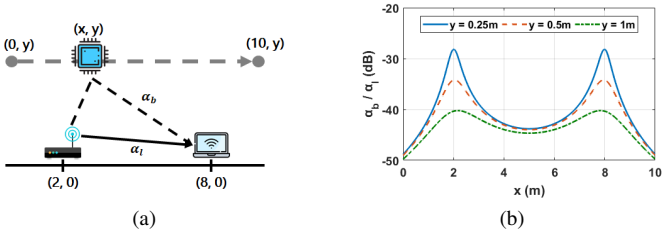
$$Y_k(n) = (H_{k,l} + H_{k,b}b(n))\, P_k(n)\, X_k(n) \tag{1}$$

where $Y_k(n)$ is the $n$-th received symbol at the subcarrier $k$ after taking the FFT. $H_{k,l}$ and $H_{k,b}$ represent the CSI of the legacy and backscatter links, respectively. Since most OFDM systems assume that channels are coherent during packet reception, $H_{k,l}$ and $H_{k,b}$ are independent to the symbol index $n$. Phase rotation due to the frequency mismatch in transmitter and receiver oscillators is $P_k(n)$. In wireless communication systems, the phase rotation is inevitable unless a transmitter-receiver pair shares a same oscillator for perfect clock synchronization. $b(n)$ indicates the state of the backscatter node where zero means absorption and one means reflection. $X_k(n)$ denotes the transmitted data symbol of the legacy link that should be detected in the demodulation procedure.

One design goal of a legacy receiver is canceling unintended distortions so that clear data symbols are transferred to the decoding procedure. Under the assumption that a backscatter node is in the absorption state at a preamble of a legacy packet, a legacy receiver correctly estimates CSI of the legacy packet. The legacy receiver then gets equalized symbols after reverting the effect of signal distortion described in the CSI.

$$\begin{aligned}\tilde{Y}_k(n) &= Y_k(n)/H_{k,l} \\ &= \left(1 + \frac{H_{k,b}}{H_{k,l}} b(n)\right) P_k(n)\, X_k(n) \\ &= R_k(n)\, X_k(n)\end{aligned} \tag{2}$$

where $R_k(n)$ denotes a residual channel representing signal distortion due to phase rotation as well as the effect of backscatter that cannot be canceled in the equalization procedure. In common wireless communication systems, only phase rotation $P_k(n)$ is shown in the residual channel. However, when a backscatter link exists along with a legacy link, the residual channel varies according to the state of the backscatter node $b(n)$.




(a) (b)

Fig. 2. Comparison of received signal strength between legacy and backscatter links depending on distance between devices.

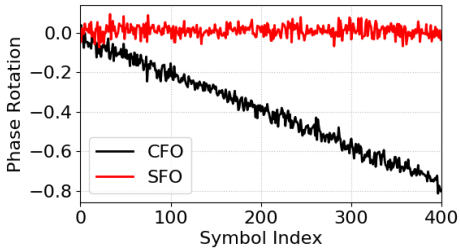



Fig. 3. Phase rotation caused by CFO and SFO across the symbol index.

### B. Residual Channel of the Legacy Link

An ideal legacy receiver should deduce a data symbol $X_k(n)$ from an equalized symbol $\tilde{Y}_k(n)$. However, as described in Eq. 2, an equalized symbol is a multiplication of a data symbol $X_k(n)$ and an unknown residual channel $R_k(n)$. Thus a legacy receiver should estimate the residual channel and compensate it from the equalized symbol for successful packet reception.

In OFDM systems, a legacy transmitter inserts pilot tones, pre-defined data symbol, into the certain subcarriers before packet transmission to facilitate residual channel estimation at a legacy receiver. Since a legacy receiver knows the data symbols $X_k(n)$ for the pilot subcarriers, the legacy receiver can estimate residual channels from the equalized symbols over the pilot subcarriers. Although the estimation results only describe residual channels of the pilot subcarriers, the legacy receiver can stretch the residual channels for all subcarriers by using linear interpolation.

Before discussing the residual channel estimation, we assess how much a backscatter node affects a residual channel. In order to look into the influence of a backscatter node, we compare the signal strengths of legacy and backscatter links as depicted in Fig. 2a. We use the Friis transmission equation for calculating the signal strengths [17]. Fig. 2b shows the signal strength ratio between the two links. The result shows that the influence of a backscatter node takes an extremely small portion of a residual channel, $1 \gg H_{k,b}/H_{k,l}$. Therefore, a legacy receiver can ignore the effect of backscatter, $R_k(n) \approx P_k$, during residual channel compensation.

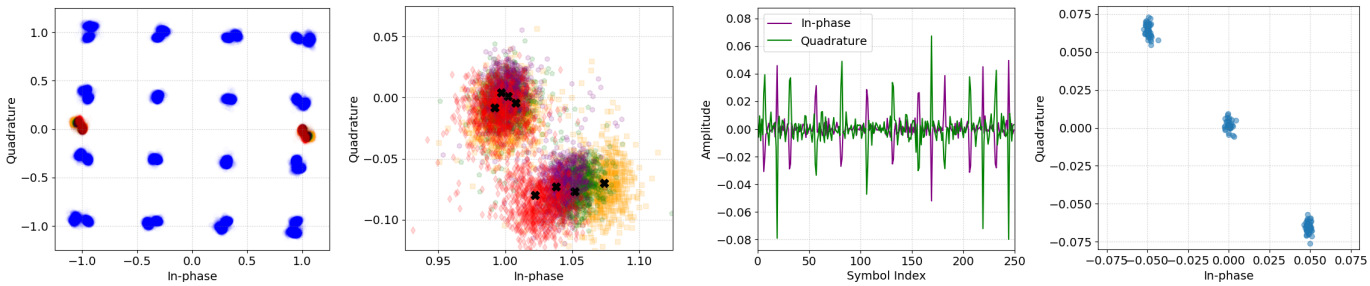
In wireless communication systems, the mismatch of the clock rates between a transmitter-receiver pair makes carrier frequency offset (CFO) and sampling frequency offset (SFO). The frequency offset incurs phase rotation and inter-carrier interference that mess up the entire receiving procedures unless a legacy receiver does not correct them [14]. In this paper, we focus on phase rotation rather than inter-carrier interference which has little effect in general. A legacy receiver corrects CFO twice by using the STS and the LTS before the demodulation procedure. However, even if the legacy receiver tries to remove the effect of CFO from received symbols, residual CFO still exists due to estimation error. Moreover, CFO and SFO are time-varying in the real world. Therefore, we should track the frequency offsets for successful correction.

To understand how CFO and SFO affect received symbols, we measure the effects of the frequency offsets with two USRP N210 software-defined radios as an OFDM transmitter-receiver pair. Fig. 3 shows phase rotation estimated by pilot tones, whose subcarrier indexes are -21, -7, 7 and 21 as in the IEEE Standard 802.11-2016 [13]. This result shows that phase rotation caused by CFO increases proportionally with the symbol index $n$. Although we cannot see the influence of SFO in this experiment, the phase rotation created by SFO also increases proportionally with the symbol index $n$ in theory [14]. Similar to this experiment, a legacy receiver estimates the frequency offsets from pilot tones to compensates the phase rotation in the same way.

## III. Implicit Wi-Fi Backscatter Networks

Existing backscatter systems do not concern about self-interference since they use a single-tone continuous wave for a carrier signal. In contrast, implicit Wi-Fi backscatter uses OFDM signals to carry backscatter packets. As addressed in [10], canceling OFDM signals while preserving effects of backscatter node in the time domain requires complex signal processing and a specialized hardware module. In terms of the frequency domain, [9] tries to figure the effect of backscatter from CSI, but their investigation does not come up with a well-designed backscatter detection method.

In this section, we introduce a flicker detector that transforms Wi-Fi backscatter systems into traditional backscatter systems. At first, the backscatter module draws out a residual channel from the demodulation procedure and passes it to the flicker detector. The flicker detector flattens the residual channel to clarify a backscatter link and converts the effects of backscatter into a series of peaks. Then, the flicker decoder translates the series of peaks into a backscatter packet. All the procedures are software-defined, and thus any hardware modifications are not required to implement our method. Also, thanks to the characteristic of the flicker detector, a backscatter node has the same RF frontend architecture as RFID tags for uplink transmission. Since implicit Wi-Fi backscatter provides backward compatibility, traditional backscatter nodes also can transmit their packets via the backscatter links. We validate our claims through experiments consisting of two USRP N210 and a WISP 5.0, a well-known prototype of a traditional backscatter node [18].




(a) (b) (c) (d)

Fig. 4. The flicker detector consists of several processing stages. (a) a legacy receiver extracts a residual channel from equalized symbols. (b) magnified pilot constellation shows the two disjoint clusters. (c) comparing two adjacent residual channels emphasizes flickers of a backscatter packet. (d) the decimated flickers show the three disjoint clusters.

### A. *How can we get backscatter packets from residual channel?*

The flicker detector extracts a state of a backscatter node $b(n)$ from a residual channel, that is a multiplication of phase rotation and effects of a backscatter link as described in Eq. 2. If a legacy receiver exactly knows effects of phase rotation, then the flicker detector can directly deduce $b(n)$ from the residual channel. However, a legacy receiver does not know the exact value of phase rotation. On the other hand, a legacy receiver exploits pilot tones to estimate phase rotation for each data symbol regardless of effects of a backscatter link as mentioned in Section II.B. Thus the estimation results of phase rotation include not only CFO and SFO but also effects of a backscatter link. It makes hard to separate phase rotation and effects of a backscatter link from a residual channel.

As a solution to the problem, the flicker detector focuses on an instantaneous change of a residual channel created by a backscatter node. When a backscatter node switches its state from absorption to reflection or vice versa, the residual channel suddenly jumps to another value. This feature enables the flicker detector to capture the instantaneous changes while correcting the phase rotation.

$$F_k(n) = \frac{R_k(n)}{R_k(n-1)} - 1 \tag{3}$$

where $F_k(n)$ denotes a flicker of a residual channel at the $n$-th data symbol. Since we calculate a ratio between two adjacent residual channels, the phase rotation terms are canceled out each other. As shown in Fig. 3, phase rotation is proportional to the symbol index $n$. It means that $P_k(n)$ divided by $P_k(n-1)$ is constant regardless of the symbol index $n$. Although the flicker entails a constant term due to phase rotation, the constant term does not affect the operation of the backscatter module. In this paper, we assume that the change of phase rotation according to the symbol index is negligible so that the constant term becomes one. This assumption is reasonable because CFO is corrected twice in the synchronization and demodulation procedure and thus only a small portion of CFO remains in the residual channel. If we want to perform perfect flicker detection, we can meet the requirement by subtracting the constant term from $R_k(n)/R_k(n-1)$.

One major advantage of the flicker detector is that existing backscatter nodes can be integrated with implicit Wi-Fi backscatter systems without any modifications. Implicit Wi-Fi backscatter accommodates every backscatter node that modulates its bits with the two states $b(n) = 0$ and $b(n) = 1$ and on-off keying (OOK) modulation. The case by case analysis explains the reason why implicit Wi-Fi backscatter provides backward compatibility.

$$F_k(n) = \begin{cases} \frac{H_{k,b}}{H_{k,l}} & \text{if } b(n-1) = 0, b(n) = 1 \\ -\frac{H_{k,b}}{H_{k,b}+H_{k,l}} & \text{if } b(n-1) = 1, b(n) = 0 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Considering $1 \gg H_{k,b}/H_{k,l}$, we can summarize the result of the second case as $-H_{k,b}/H_{k,l}$, which is opposite to the result of the first case. Thus flickers have three types of values: a positive flicker, a negative flicker, and a halt. The three types are in the same format as edges in LF-Backscatter, which introduces the edge detection method to separate collided packets in traditional backscatter systems [19]. Therefore, it proves two things: 1) a legacy receiver is able to decode a backscatter packet from flickers, and 2) the flicker detector enables a legacy receiver to read a backscatter packet transmitted from a traditional backscatter node.

To inspect the procedures of the flicker detector, we conduct the following experiment. We place a WISP 5.0 transmitting PRBS-7 sequences next to a USRP N210. In this experiment, we use a single USRP N210 for both a legacy transmitter and a receiver to be free from phase rotation created by the frequency mismatch of the local oscillators. Fig. 4a shows the equalized symbols and pilot tones for a legacy packet. We observe that the symbols are slightly separated into two clusters. The two clusters indicate whether the backscatter node is reflecting or absorbing. In order to observe the effect of backscatter on the legacy link more clearly, we magnify the constellation of the pilot tones as shown in Fig. 4b. When the backscatter node is absorbing incident signals, the pilot tones stay at $(1, 0)$ or $(-1, 0)$. However, when the backscatter node is reflecting the legacy signals, the pilot tones are shifted to another point. In this example, the bottom right clusters represent the shifted pilot tones.

The flicker detector demodulates backscatter signals without knowing a channel of a backscatter link. The only thing a legacy receiver needs to do is peak detection. Fig. 4c represents the flickers of the residual channel. As described in Eq. 4, the peaks in the flickers indicate a state change at the backscatter node while an opposite peak means the reverse of the state change. Therefore, the legacy receiver only focuses on the presence of peaks in the flickers and whether the peak corresponds to a positive flicker or a negative flicker.

### B. Is it enough to detect backscatter signals from flickers?

In Wi-Fi, a single data symbol consists of 56 subcarriers, 4 subcarriers for pilot tones and other 52 subcarriers for data transfer. It means that there are 56 residual channels in a single data symbol although Fig. 4c only shows the trace of residual channels for the 4 pilot subcarriers. Flicker detection only with pilot tones is also allowable, but this approach does not give sufficient evidence to detect backscatter signals because residual channels from the 4 pilot subcarriers are fragile to frequency selective fading and noise. As described before, backscatter signals are really weak compared to legacy signals in general. Therefore, in order to facilitate implicit Wi-Fi backscatter communications, a legacy receiver has to squeeze residual channels as much as it can. Our solution to the problem is utilizing demodulated symbols $X_k(n)$ to estimate residual channels for all subcarriers rather than only with the pilot subcarriers. As mentioned in Section II, since the effect of backscatter has little impact on legacy links, the demodulated symbols have no relation with backscatter links. Therefore, a legacy receiver can draw out residual channels from $\tilde{Y}_k(n)/X_k(n)$ for the data subcarriers as well as the pilot subcarriers. Flickers may have diverse directions according to a subcarrier index $k$. If a propagation delay of a backscatter link is much larger than a legacy link, phase distinction between subcarriers becomes evident. However, in indoor scenarios, the flickers are pointing the almost same direction usually. For these reasons, we utilize combined flickers $\sum_k F_k(n)$ as a result of the flicker detector.

Fig. 4c shows the peaks in the flickers, which indicate a state change at a backscatter node. This information may be useful when we resolve collided backscatter packets as in [19]. In contrast, our focus is to find a single backscatter packet rather than multiple collided packets, and hence there is a room for enhancement. The duration of a backscatter symbol is not always the same as the duration of a legacy symbol, 4 $\mu$s in Wi-Fi. In other words, a backscatter symbol consists of $M$ legacy symbols whereas flickers in Eq. 3 represent a ratio between only two adjacent legacy symbols. In order to perform ideal backscatter demodulation, a legacy receiver should compare $M$ legacy symbols with other adjacent $M$ legacy symbols, since a single backscatter symbol corresponds to $M$ legacy symbols.

$$F(n) = \sum_{l=0}^{M-1} \sum_{k} \left( \frac{R_k(n-l)}{R_k(n-l-M)} - 1 \right) \tag{5}$$

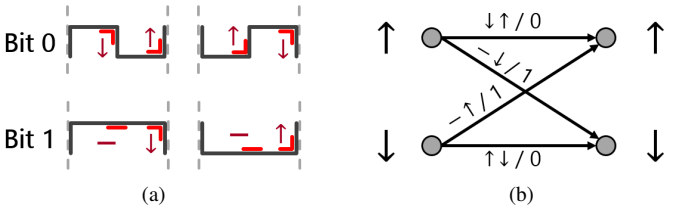



Fig. 5. A backscatter node encodes data bits before transmission. (a) FM0 encoding differentiates or holds the first and the second symbols to represent a data bit. (b) the flicker decoder using the Viterbi algorithm restores the flickers into a data bit.

By accumulating the flickers, SNR of the flicker is improved $M$ times than before. Fig. 4d shows the combined and accumulated flickers whose decimation ratio is $M$.

### C. How can we cope with noise and interference?

Every device in ISM band can barge in on a channel that is being used by legacy devices. The system model of implicit Wi-Fi backscatter assumes that there are only two types of devices, backscatter nodes and legacy devices. However other types of devices may intrude into the networks and then propagate unpredictable interference signals. From the legacy receiver's point of view, the interference signals are classified as fluctuation of residual channels. Unfortunately, the interference signals are much stronger than backscatter signals in common cases. Thus, if an external device is propagating wireless signals, the interference signals dominate the residual channel and blur out the effect of backscatter. Moreover, as a channel becomes wider, the probability of interference grows higher. Wi-Fi takes at least a 20 MHz bandwidth, which corresponds to 20% of 2.45 GHz ISM band.

We cannot predict or nullify interference signals, and thus we skip some of the subcarriers when we combine flickers. More specifically, a legacy receiver selects the top-$k$ strongest flickers in magnitude among all subcarriers. The selected flickers are excluded when the legacy receiver accumulates the flickers as in Eq. 5. We do not know whether the selected flickers encompass interference signals. If there is no interference at a received symbol while excluding the top-$k$ strongest flickers, we undergo a small loss of SNR. However, when the selected flickers include interference signals, we bypass the effect of interference signals by ignoring the selected flickers that mess up all procedures of a backscatter module.

In existing backscatter systems, a single bit consists of one or more backscatter symbols because they are using an encoding scheme to decrease the bit error rate of backscatter packets [7]. In this paper, we assume that a backscatter node uses FM0 encoding as illustrated in Fig. 5a. The up and down symbols in FM0 encoding indicate the absorption and reflection state on a backscatter node or vice versa. When the first symbol is opposite to the second symbol, the backscatter node is transmitting a bit 0. Otherwise, when the first symbol is identical to the second symbol, the backscatter node is transmitting a bit 1. In this way, the receiver translates two demodulated symbols into a single data bit.

In implicit Wi-Fi backscatter systems, the flicker detector produces a positive flicker, a negative flicker, and a halt rather than up and down symbols. Fig. 5a depicts how the flicker detector interprets an FM0 encoded backscatter symbol where $\uparrow$, $\downarrow$ and $-$ correspond to a positive flicker, a negative flicker, and a halt, respectively. Hence we design the flicker decoder using the Viterbi algorithm to parse the demodulated symbols in accordance with the relation between flickers and a data bit as shown in Fig. 5b. Each gray dot denotes a state of the backscatter decoder while each arrow means the state transition. If the backscatter node is transmitting a bit 0, the first and the second symbols show flickers pointing opposite directions. Similarly, when the backscatter node is transmitting a bit 1, the first symbol goes to a halt while the second symbol shows a flicker. For example, $\downarrow\uparrow$ /0 means that when the flicker decoder receives a negative flicker and a positive flicker in sequence, the two flickers are translated into a bit 0. We implement the soft-decision decoding algorithm for the flicker decoder.

## IV. Performance Evaluation

We implement our implicit Wi-Fi backscatter system using two USRP N210 for a legacy transmitter-receiver pair and a WISP 5.0 for a backscatter node. In order to ensure backward compatibility, the legacy transmitter and receiver operate at 915 MHz, optimized for WISP 5.0. Although our experiments do not use the standard frequency band, the legacy transmitter and receiver comply with all other requirements of the IEEE standard 802.11-2016 [13]. The legacy link uses the QPSK modulation by default and occupies a 20 MHz channel with 800 ns guard interval. The legacy transmitter-receiver pair does data communication rather than delivering pre-known dummy packets. The bit error rate of the legacy link affects the performance of the backscatter link because we draw out residual channels from both the pilot subcarriers and the data subcarriers. The backscatter node transmits eight bytes payload backscatter packets containing PRBS-7 sequences. In this experiment, we measure the packet error rate of the backscatter link. And then we calculate the throughput of the backscatter link from the packet error rate.

We observe the throughput of the backscatter link across the distance between the backscatter node and the legacy receiver. The distance varies from 0.5 m to 5.0 m while the backscatter transmitter is 0.5 m away from the backscatter node. We equip 2 dBi omni-directional antennas for the legacy transmitter and receiver. We attach a 10 dB attenuator to the legacy transmitter to set the transmission power as -5 dBm. The backscatter node continuously transmits backscatter packets at three different bit rates, 10 Kbps, 20 Kbps, and 40 Kbps with FM0 encoding. For the 40 Kbps backscatter link, we set the number of legacy symbols per a backscatter symbol $M$ as 3. Although $M$ is not perfectly matched to the bit rate of the backscatter link, the legacy receiver decodes backscatter packets well because it performs timing recovery during flicker decimation. Similarly, we set $M$ as 6 and 12 for the 20 Kbps and 10 Kbps bit rates, respectively.

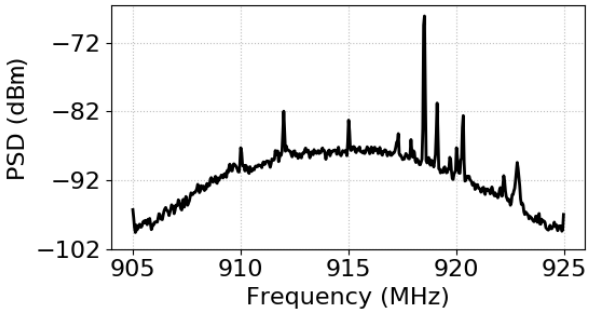



Fig. 6. The power spectral density of interference signals.

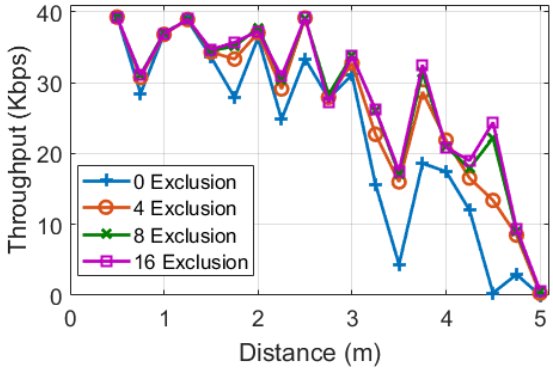



Fig. 7. The throughput of the backscatter link according to the number of excluded subcarriers. 8 exclusion means that the flicker detector combines 48 flickers after excluding the top-8 strongest flickers among 56 subcarriers.

### A. Resilience to Interference

Fig. 6 shows the power spectral density of interference signals measured at the legacy receiver while there is no transmission at the legacy transmitter. The power spectral density shows the evident interference signals around 920 MHz. But the interference signals cannot be eliminated since every wireless device can intrude the ISM band anytime. Therefore, the legacy receiver should withstand the interference signals for successful packet reception in this experiment. If backscatter signals are stronger than the interference signals, the legacy receiver successfully decodes backscatter packets. Otherwise, the legacy receiver suffers from the interference signals during the flicker detection.

The flicker detector excludes the top-$k$ strongest flickers to bypass interference signals. We observe robust performance against interference when choosing the appropriate $k$ to omit some subcarriers including interference signals. Fig. 7 shows the backscatter throughput for four different $k$ across distance. We set the bit rate of the backscatter node as 40 Kbps for this experiment. The fluctuation of the backscatter throughput is originated from the multipath effect since we are using omni-directional antennas. There is no significant performance improvement over $k$ when the distance is less than 3 m. However, when the distance is greater than 3 m, we can observe improved resilience against interference due to top-$k$

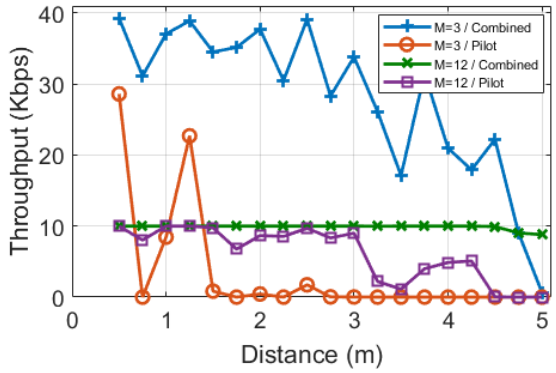



Fig. 8. The throughput of the backscatter link versus the number of combined subcarriers. Bringing residual channels from the data subcarriers reinforces the SNR of the backscatter link.

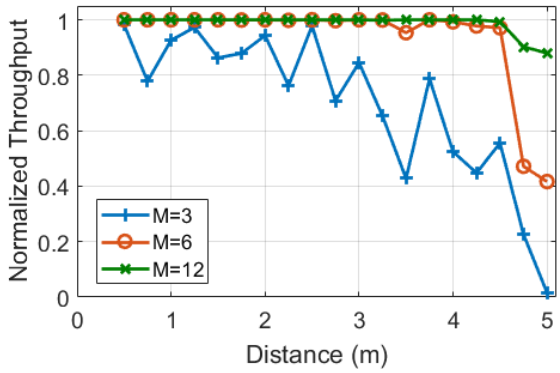



Fig. 9. The normalized throughput versus the number of legacy symbols per a backscatter symbol $M$. The backscatter links become more stable as $M$ increases.

exclusion. This is because the signal strength of the backscatter link decreases as the distance increases while the signal strength of the interference signals remains unchanged.

Interference signals represent different patterns in different environments. So an appropriate $k$ for interference exclusion varies with surrounding environments. We may choose a sufficiently large $k$ for perfect interference exclusion. But, a large $k$ results in a loss of SNR of the backscatter link because we may abandon undamaged flickers. In subsequent experiments, the flicker detector excludes 8 subcarriers for each legacy symbol.

### B. Impact of the Number of Combined Subcarriers

We draw out residual channels from not only the pilot subcarriers but also the data subcarriers. The main objective of this approach is SNR improvement of backscatter links. The flicker consisting of 56 subcarriers describes backscatter signals more clearly compared to that only with the pilot subcarriers. The combined flicker is also more stable against the multipath effect. If the backscatter link experiences frequency selective fading and some pilot tones have much weaker strength than other subcarriers, residual channels from the pilot subcarriers cannot be used. Fig. 8 describes the advantage of combining flickers. In terms of the throughput, the combined flicker always performs better. For the 40 Kbps backscatter link, the throughput of the pilot subcarriers goes to zero after 1.5 m, whereas the combined flicker fails at 5 m. On the other hand, the deep fading at 0.75 m causes significant throughput degradation. The backscatter link with pilot subcarriers fails to communicate, whereas the backscatter link with the combined flicker still works because of undamaged subcarriers. The 10 Kbps backscatter link shows a similar pattern. The combined flicker guarantees stable backscatter packet delivery. However, a flicker consisting of pilot subcarriers does not give enough SNR to decode backscatter packets. It is also vulnerable to frequency selective fading frequently occurring in wireless communication systems.

### C. Impact of the Bit Rate of a Backscatter Link

We run our experiments with three different bit rates for the backscatter node, 10 Kbps, 20 Kbps and 40 Kbps. Fig. 9 shows the normalized throughput for each bit rate. Decreasing bit rate of a backscatter link extends a transmission range of a backscatter node. The 10 Kbps backscatter link gathers 12 legacy symbols to form a single backscatter symbol, whereas the 40 Kbps backscatter link gathers only 3 legacy symbols. Hence the 10 Kbps backscatter link delivers much stronger backscatter signals than others. Likewise, decreasing bit rate of a backscatter link improves robustness against interference.

For these reasons, we can apply a rate adaptation algorithm to implicit Wi-Fi backscatter networks to fully utilize the potential of the backscatter link. For example, if a backscatter node has an ability to estimate RSSI of an incoming legacy packet, it can also predict the SNR of the corresponding backscatter link. RSSI of an incoming legacy packet implies the distance between the legacy device and the backscatter node. Thus the backscatter node learns its relative location after receiving uplink and downlink legacy packets. With the estimated location, the backscatter node guesses which bit rate provides the optimal throughput for the corresponding backscatter link.

We exploit residual channel to achieve per-symbol in-band backscatter. In Wi-Fi, the symbol duration is 4 $\mu$s when we use 800 ns guard interval. Hence the maximum bit rate of implicit Wi-Fi backscatter with FM0 encoding is 125 Kbps. By contrast, the maximum bit rate of per-packet in-band backscatter is 12.5 Kbps while a legacy link consistently delivers 40 $\mu$s dummy packets, whereas implicit Wi-Fi backscatter does data communication [9]. The performance gap between the two approaches becomes even more evident in throughput measurements. In implicit Wi-Fi backscatter, a backscatter node, 50 cm away from a legacy transmitter, achieves about 30 Kbps transmission at 3m away from a legacy receiver. However, in per-packet backscatter systems, even if a backscatter node is placed 5 cm away from a legacy transmitter, the backscatter link seldom exceeds 1 Kbps.

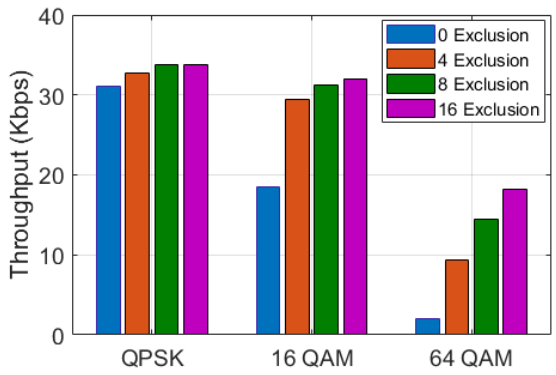



Fig. 10. The throughput of the backscatter link according to the modulation scheme of the legacy link. Top-$k$ exclusion mitigates throughput reduction due to demodulation errors.

### D. Impact of Legacy Data Rate

A backscatter node gets on a legacy link to transmit backscatter packets. That is, if an error occurs in the legacy link, the error propagates to the backscatter link. More specifically, the legacy receiver estimates residual channels with demodulated symbols $X_k(n)$. If the demodulated symbols are correct, then the estimated residual channels are also correct. But, if some of the demodulated symbols are wrong, then the errors affect to residual channels. Considering the signal strength of the backscatter link, the demodulation error significantly drops the throughput of the backscatter link.

Fig. 10 shows the effect of demodulation errors where a backscatter node is placed 3 m away from a legacy receiver. A legacy link with a 64 QAM modulation supports a higher bit rate than a QPSK modulation but also increases the bit error rate. So the throughput of the backscatter link is reduced along the complexity of modulation scheme. Meanwhile, we can see that top-$k$ exclusion mitigates throughput reduction due to the demodulation errors. In general, a faulty subcarrier produces a stronger flicker than a correct subcarrier. There is a high possibility that a flicker from a faulty subcarrier is selected as the top-$k$ strongest flicker and then is excluded from the flicker detector.

In this experiment, we use a -5 dBm legacy transmitter based on the software-defined radio platform. In contrast, the transmission power of commercial Wi-Fi devices is typically 20 dBm. In addition, the software-defined radio platform is used for experiments in general, and performance is always lower than that of commercial devices. Therefore, a bit error rate of a legacy link becomes much lower than this experiment when we implement the backscatter module within a commercial Wi-Fi device.

## V. Discussion

**Self-interference and dynamic range:** In-band backscatter cannot be free from self-interference [5], [10]. An RF frontend of a legacy receiver contains an automatic gain control (AGC) and an analog-to-digital converter (ADC). For example, a USRP N210 equips a 14-bit ADC that converts received analog signals into 14 bits complex digital signals. The digital signals have limited resolution because they can only describe discrete data while an analog signal represents continuous data. Thus, if a received signal is too weak to be described by an ADC, a quantization error occurs during the analog-to-digital conversion. This is why received signals pass through an AGC before the conversion. The AGC amplifies the received signals to make it fit in the interest of the ADC. Nonetheless, a backscatter signal may disappear during the conversion if the signal strength of the backscatter link is not within the dynamic range of the ADC, which is the ratio between the largest and smallest values described by the ADC. In this regard, communication range of in-band backscatter is limited, but it is still enough to connect IoT devices in indoor environments.

**MAC protocol for backscatter networks:** In this paper, we describe implicit Wi-Fi backscatter systems with a single backscatter node and a legacy transmitter-receiver pair. But when we imagine implicit Wi-Fi backscatter systems consisting of multiple devices, our approach outperforms side-band backscatter in terms of network utilization. Our approach does not require an additional channel, whereas legacy devices need to be synchronized with each other in order to simultaneously occupy two disjoint Wi-Fi channels in side-band backscatter. So our approach can support more flexible resource management compared to side-band backscatter.

Our approach also facilitates MAC protocol design for backscatter networks. In implicit Wi-Fi backscatter systems, legacy signals are always stronger than backscatter signals, created by reflection at a backscatter node. In other words, backscatter signals never leak outside the coverage of legacy transmission. Therefore, legacy transmission guarantees carrier sensing for backscatter nodes whereas side-band backscatter is hard to implement carrier sensing for backscatter transmission. Although side-band backscatter outperforms our approach for a single link communication, we expect that our approach provides much better performance when backscatter systems begin to accommodate multiple backscatter nodes and legacy receivers thanks to the ease of network management.

**Downlink communication:** Implicit Wi-Fi backscatter networks should support downlink communications from a legacy transmitter to a backscatter node. Since a backscatter node usually demodulates received signals with an envelope detector, a legacy transmitter should make amplitude modulation signals from OFDM symbols. Fortunately [6] describes how to create downlink packets using OFDM symbols. A time-domain OFDM symbol created from random bits looks like a continuous wave, while a symbol created from constant bits becomes empty except for the head of the symbol. But this method works only when there is no signal across the 2.45 GHz ISM band. A backscatter node cannot select a channel because there is no local oscillator or bandpass filter used for channel selection. It means that an envelope detector of a backscatter node responds to all incident signals regardless of their frequency. Thus we should study to solve this problem.

## VI. Related Work

Evolution of backscatter systems originates from UHF RFID researches. In order to serve rapid RFID tag identification, several amendments related to identification protocol have been proposed [20], [21]. However, even if they try to reach optimal performance by exploiting cache or physical layer information to remove scheduling overhead, the application space of traditional backscatter systems is too limited due to the structural limitations, short communication range and initial deployment costs.

Ambient backscatter facilitates more unrestricted deployment of backscatter systems compared to the traditional scheme. For example, TV signals are used for node-to-node communication [2]. Also, an FM radio station can serve as a carrier emitter [3]. Meanwhile [8] introduces ambient OFDM backscatter systems, which enable OFDM systems to deliver backscatter packets under the assumption that a receiver has complete knowledge of all channels. Ultra wideband backscatter combines the several ambient backscatter techniques into a single receiver to improve the signal to noise ratio [4]. But these approaches are only applicable to outdoor environments, not our focus.

Side-band backscatter is an attractive approach because it enables 802.11b devices to receive backscatter packets. Passive Wi-Fi demonstrates for the first time how to generate 802.11b backscatter packets using a single-tone carrier emitter [22]. Bluetooth devices or 802.11b devices can also serve as carrier emitters to construct backscatter networks. [6] demonstrates how to create 802.11b packets from Bluetooth packets at a backscatter node. Similarly, a backscatter node can create an 802.11b packet from another 802.11b packet at an adjacent channel [5]. However, the main drawback of side-band backscatter is spectral efficiency. Since it uses frequency shift keying for backscatter communications, it requires an additional channel for a backscatter link. This requirement is not desirable in terms of channel utilization. In case of [5], a 20 MHz channel is reserved for a backscatter link while a legacy link occupies another 20 MHz channel. Considering poor spectral efficiency of backscatter communications, we should use in-band backscatter rather than side-band backscatter to be in harmony with other wireless networks sharing the same frequency band.

## VII. Conclusion

We demonstrate a per-symbol in-band backscatter scheme for the first time that harmonizes with existing Wi-Fi devices. A backscatter node modulates its bits through a residual channel without affecting the communication link, while providing sufficient data rates to connect indoor IoT devices. Our scheme also ensures backward compatibility of backscatter nodes and does not require any hardware modifications. We shed new light on the potential of in-band backscatter from the network's point of view.

## Acknowledgment

This research was partly supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) 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. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 1091–1104, March 2014.
[2] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," in *Proc. of ACM SIGCOMM*, 2013.
[3] A. Wang, V. Iyer, V. Talla, J. R. Smith, and S. Gollakota, "FM backscatter: Enabling connected cities and smart fabrics," in *Proc. of USENIX NSDI*, 2017.
[4] C. Yang, J. Gummeson, and A. Sample, "Riding the airways: Ultra-wideband ambient backscatter via commercial broadcast systems," in *Proc. of IEEE INFOCOM*, 2017.
[5] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "HitchHike: Practical backscatter using commodity WiFi," in *Proc. of ACM SenSys*, 2016.
[6] 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.
[7] EPC UHF Gen2 Air Interface Protocol, Available at: https://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/2-0-1.
[8] 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.
[9] 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.
[10] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High throughput WiFi backscatter," in *Proc. of ACM SIGCOMM*, 2015.
[11] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, pp. 53–53, Jan 2011.
[12] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity WiFi," in *Proc. of ACM MobiCom*, 2015.
[13] IEEE 802.11-2016, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Available at: http://standards.ieee.org/about/get/802/802.11.html.
[14] M. Speth, S. A. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using OFDM," *IEEE Transactions on Communications*, vol. 47, no. 11, pp. 1668–1677, Nov 1999.
[15] M. Speth, S. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for OFDM-based broadband transmission," *IEEE Transactions on Communications*, vol. 49, no. 4, pp. 571–578, Apr 2001.
[16] 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.
[17] A. F. Molisch, *Wireless Communications*, 2nd ed. Wiley, 2011.
[18] WISP 5.0, Available at: https://wisp5.wikispaces.com.
[19] P. Hu, P. Zhang, and D. Ganesan, "Laissez-Faire: Fully asymmetric backscatter communication," in *Proc. of ACM SIGCOMM*, 2015.
[20] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tag-splitting: Adaptive collision arbitration protocols for RFID tag identification," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 6, pp. 763–775, June 2007.
[21] H. Wu, Y. Zeng, J. Feng, and Y. Gu, "Binary tree slotted aloha for passive RFID tag anticollision," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 19–31, Jan 2013.
[22] 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.