Pushing the Throughput Limit of OFDM-based Wi-Fi Backscatter Communication

Qihui Qin[†‡*], Kai Chen[†¶*], Yaxiong Xie[♯], Heng Luo[†♮]
Dingyi Fang[†‡§¶], Xiaojiang Chen[†‡♮⋄]

[†] Northwest University, China, [♯] University at Buffalo SUNY, New York, USA
[‡] Shaanxi International Joint Research Centre for the Battery-Free Internet of Things, China
[§] Xi'an Key Laboratory of Advanced Computing and System Security, China
[¶] Internet of Things Research Center, Northwest University, China
[♮] Xi'an Advanced Battery-Free Sensing and Computing Technology International Science and Technology Cooperation Base, China
{qihui,ck,luoheng}@stumail.nwu.edu.cn,yaxiongx@buffalo.edu,{dyf,xjchen}@nwu.edu.cn

ABSTRACT

The majority of existing Wi-Fi backscatter systems transmit tag data at rates lower than 250 kbps, as the tag data is modulated at OFDM symbol level, allowing for demodulation using commercial Wi-Fi receivers. However, it is necessary to modulate tag data at OFDM sample level to satisfy the requirements for higher throughput. A comprehensive theoretical analysis and experimental investigation conducted in this paper demonstrates that demodulating sample-level modulated tag data using commercial Wi-Fi receivers is unattainable due to excessive computational overhead and demodulation errors. This is because the significant tag information dispersion, loss, and shuffling are caused by Wi-Fi physical layer operations. We conclude that the optimal position for demodulation is the time-domain IQ samples, which do not undergo any Wi-Fi physical layer operations and preserve the intact, ordered, and undispersed information of tag-modulated data, thereby minimizing complexity and maximizing accuracy.

We devise a demodulation algorithm using time domain IQ samples and implement on two types of demodulator: a dual radio chain demodulator and a single radio chain demodulator. Experiments show that our demodulation algorithm not only decrease the BER by at least three orders of magnitude, but also reduces the time complexity from exponential to linear. It achieves a tag data rate of up to 10 Mbps with QPSK modulation and a BER at 10^{-4} for the dual radio chain demodulator, and a tag data rate of up to 1 Mbps with BPSK and a BER at 10^{-4} for the single radio demodulator. We believe our results pave the way for designing Wi-Fi backscatter system with extremely high throughput.

CCS CONCEPTS

• **Hardware → Printed circuit boards**; **Communication hardware, interfaces and storage**; • **Human-centered computing → Ubiquitous and mobile computing**.

KEYWORDS

IoT, Wi-Fi Backscatter, High Throughput Backscatter, Wireless Communication System

ACM Reference Format:
Qihui Qin[†‡*], Kai Chen[†¶*], Yaxiong Xie[♯], Heng Luo[†♮], Dingyi Fang[†‡§¶], Xiaojiang Chen[†‡♮⋄]. 2024. Pushing the Throughput Limit of OFDM-based Wi-Fi Backscatter Communication. In *International Conference On Mobile Computing And Networking (ACM MobiCom '24), November 18–22, 2024, Washington D.C., DC, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3636534.3690672

1 INTRODUCTION

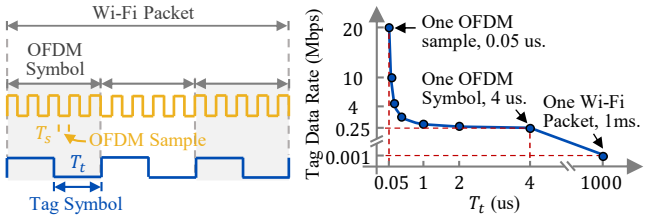
Wi-Fi backscatter technology has emerged as a frontrunner for passive Internet of Things (IoT) applications due to its ability to operate with minimal power and leverage existing Wi-Fi infrastructure. This approach hinges on the ability to seamlessly embed tag data onto ambient Wi-Fi signals, backscatter it for reception, and accurately recover the embedded information through demodulation techniques.

The Wi-Fi backscatter tag modulates its data by subtly altering a characteristic of the Wi-Fi signal, such as phase,

∗ Co-primary authors, both authors contributed equally to this research.
⋄ Corresponding author.

ACM MobiCom '24, November 18–22, 2024, Washington D.C., DC, USA

ACM ISBN 979-8-4007-0489-5/24/09
https://doi.org/10.1145/3636534.3690672



(a) T_t is a multiple of that of the OFDM sample duration. **(b)** The relationship between the tag data rate and its symbol duration T_t.

Figure 1: The tag data rate directly depends on the tag symbol duration T_t in backscatter communication.

amplitude, or frequency. Among these options, phase modulation is the most widely adopted due to its effectiveness and compatibility with existing Wi-Fi infrastructure [29, 61]. A critical factor influencing the backscatter communication's throughput is the tag symbol duration, denoted as T_t, as depicted in Figure 1a. This parameter essentially dictates the speed at which the tag transmits its data. Intuitively, shorter tag symbol durations T_t allow for higher tag data rates, as shown in Figure 1b.

Research efforts have been persistently pushing the throughput limit of Wi-Fi backscatter by continuously reducing the tag symbol duration. In the pioneering works on Wi-Fi backscatter [11, 29, 40], the tag symbol duration spanned an entire Wi-Fi packet. These works employed on-off keying (OOK) to modulate a single bit within each packet, achieving a data rate of around 1 kbps [29]. To keep pushing the limit, researchers explored OFDM symbol-level modulation techniques. These techniques modulate data by altering the phase of the entire OFDM symbol [63, 64]. Assuming BPSK, such methods can achieve a maximum data rate of 250 kbps, as shown in Figure 1b, representing a significant 250× improvement compared to packet-level modulation.

OFDM symbol-level modulation offers a distinct advantage: demodulation can be implemented on commercial Wi-Fi devices. In other words, we can demodulate the tag data using packet bits reported by standard Wi-Fi network cards. The fundamental reason lies in how Wi-Fi operates. Most physical layer operations in Wi-Fi occur at the individual OFDM symbol level. This confines the impact of tag modulation to the packet bits transmitted within that specific OFDM symbol. Consequently, by comparing the decoded packet bits with and without tag modulation, we can isolate the impact of the tag modulation.

Research efforts aimed at enhancing Wi-Fi backscatter throughput have encountered a bottleneck at the OFDM-symbol level. The challenge does not stem from modulating data at finer granularities (IQ sample level), but rather from demodulating such signals. While programming the backscatter tag to modulate data at the IQ sample level and achieving a higher tag data rate is feasible even with current backscatter tag hardware, the complexity of the tag demodulation algorithm experiences a significant surge when transitioning into the sample-level realm.

To investigate the reason behind the surge in demodulation complexity when transitioning from the OFDM symbol level to IQ sample modulation, we conducted a first-of-its-kind comprehensive study through theoretical analysis and experimental investigation. Our aim is to understand the impact of various operations within the Wi-Fi physical layer on tag-modulated data. From our study, we discovered that the Wi-Fi physical layer operations introduce three types of distortion to the tag-modulated data:

- **Information Dispersion:** the tag-modulated information within each tag symbol gets spread across multiple frequency domain IQ samples or bits.
- **Information Loss:** the tag-modulated information gets lost after undergoing physical operations.
- **Information Shuffling:** the tag-modulated inforamtion gets reordered.

Both information dispersion and shuffling contribute to increased demodulation complexity. Information loss leads to significant demodulation errors. Importantly, the more operations the tag-modulated data undergoes, the higher the demodulation complexity and the larger the demodulation error introduced.

Our study has both theoretically and experimentally demonstrated that the most significant advantage of OFDM-symbol level tag modulation—capable of demodulating tag data using packet bits reported by commercial Wi-Fi devices—is unattainable due to the excessive computational overhead and demodulation errors incurred after undergoing all physical layer operations. Furthermore, our study highlights a simple yet crucial observation: without undergoing any Wi-Fi physical layer operations, the time domain IQ sample contains intact, ordered, and undispersed information of the tag-modulated data. Consequently, demodulating tag data using time domain IQ samples minimizes complexity and simultaneously maximizes accuracy.

Based on our study, to push the limit throughput of OFDM-based Wi-Fi backscatter systems, we reduce the tag symbol duration to the sample level and propose corresponding demodulation solutions that take the time domain IQ samples as input. Specifically, we introduce two types of tag-data demodulators: a dual radio solution and a single radio solution. In both solutions, the tag operates similarly by shifting the Wi-Fi transmission to a new frequency and modulating on the new channel.

For the dual radio solution, we utilize one radio chain to capture the IQ of the tag-free Wi-Fi transmission in the original channel and another radio chain to listen to the

tag-modulated Wi-Fi signal on the frequency-shifted channel. Bycomparing the captured time domain IQ samples, we are able to extract the modulated data. Assuming BPSK modulation, our backscatter system using two radio chains theoretically achieves a throughput of 20 Mbps.

In the single radio solution, we only listen to the tag-modulated signal on the frequency-shifted channel. Our key insight is that the *cyclic prefix* (CP) is actually a sequence of repeated IQ samples of a subset of data samples inside one OFDM symbol. Therefore, we instruct the tag to only modulate data on the CP and compare the tag-modulated CP with the corresponding data samples inside the same OFDM symbol to extract the tag data. Assuming BPSK modulation, our backscatter system using a single radio chain theoretically achieves a throughput of 4 Mbps.

We have implemented a prototype of the proposed sample level tag modulation and demodulation system. Extensive experimental results demonstrate that we can actually achieve a tag data rate up to 10 Mbps and 1 Mbps with the demodulation BER remaining at 10^{-4} in the dual and single radio chain demodulator, respectively.

2 IMPACTS OF WI-FI PHYSICAL LAYER OPERATIONS ON DEMODULATION

In this section, we first introduce the major operations inside the Wi-Fi physical layer followed by a combination of theoretical analysis and experimental investigation to analyze the impact of these operations on tag data demodulation.

2.1 Primer On Wi-Fi Physical Layer

Figure 2 illustrates the main operations of the Wi-Fi physical layer. Specifically, the time domain IQ samples of Wi-Fi signal are segmented into OFDM symbols. The cyclic prefix of each OFDM symbol is removed since it is redundant information primarily used for mitigating inter-symbol interference. CP-removed OFDM symbols undergo FFT, yielding frequency domain IQ. These IQs correspond to four subcarrier types: data, DC, guard-band, and pilot subcarriers. Only data subcarriers transmit Wi-Fi data, hence only they are fed to the demodulator, with the rest discarded. Data subcarrier IQs are demodulated into binary bits (coded bits). Coded bits are subjected to deinterleaving and then decoded into packet bits before reaching the Wi-Fi MAC layer.

2.2 Theoretical Analysis

In this section, we theoretically analyze the impact of Wi-Fi physical layer operations on sample-level tag data demodulation. Specifically, we have observed three types of disturbance on the tag-modulated information: the *information dispersion*, the *information loss*, and the *information shuffling*,

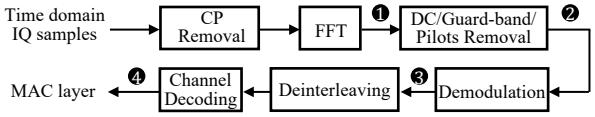


Figure 2: The main operations of Wi-Fi physical layer.

resulting in a significant increase in the BER and complexity of tag data demodulation.

2.2.1 Information Dispersion. Two Wi-Fi physical layer operations, namely the FFT and the channel decoding, spreads the information the tag modulated inside one OFDM sample or coded bit across a broader range of IQ samples or bits, resulting in information dispersion.

Fast Fourier Transform (FFT). The FFT converts time domain OFDM samples into the frequency domain. Figure 3a illustrates an example of FFT transformation. It is observed that the information encapsulated within each time domain sample disperses across all frequency domain samples, as depicted by the *blue arrows* in Figure 3a. Consequently, each frequency domain sample incorporates information from all time domain samples pre-transformation, as illustrated by the *red arrows* in Figure 3a.

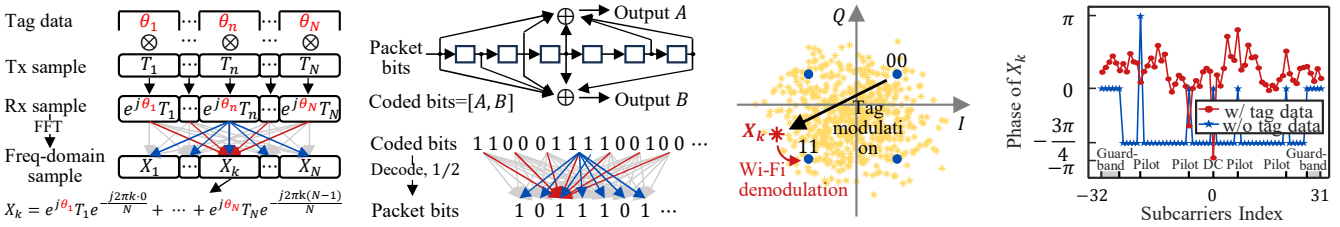
It is important to note that the tag information is modulated onto the time domain sample before FFT, which is also diffused across the frequency domain samples. Specifically, if we denote the tag modulated information on n^{th} domain sample T_n as θ_n, then the k^{th} frequency domain sample X_k after FFT is given as:

$$X_k = \sum_{n=1}^{N} e^{j\boldsymbol{\theta_n}} T_n e^{-j\frac{2\pi k(n-1)}{N}}. \quad (1)$$

According to Eqn. 1, it is evident that the tag-modulated information on each time domain sample gets spread across all frequency samples after FFT.

Channel Decoding. Channel decoding also leads to the dispersion of information. For instance, in the case of binary convolutional codes commonly employed in Wi-Fi, the encoder generates coded bits by employing generating polynomials on a group of seven consecutive packet bits. This process is depicted in Figure 3b *upper*. As a result, after decoding, the information contained within each data bit becomes distributed across a sequence of seven consecutive decoded packet bits, as demonstrated by the *blue arrow* in Figure 3b *lower*. Furthermore, each decoded packet bit encompasses information from fourteen consecutive coded bits, given the coding rate of 1/2, as illustrated by the *red arrow*.

2.2.2 Information Loss. Due to the information dispersion, every frequency domain IQ sample or bits demodulated from the IQ sample contains tag-modulated information. Therefore, dropping any IQ samples or bits results in the loss of



(a) Impact of FFT. **(b)** Impact of channel decoding. **(c)** Impact of demod. **(d)** Impact of subcarrier removal.

Figure 3: The impact of Wi-Fi physical layer operations on the tag-modulated data. FFT operation causes information disperation **(a)**; channel decoding introduces both information dispersion and information loss **(b)**; both demodulation and subcarrier removal, including both guard band carriers and DC subcarriers, cause tag information loss **(c)** and **(d)**.

the tag-modulated information. The demodulation from IQ samples to bits also results in information loss. All the operations that result in tag information loss are detailed in the rest of the section.

CP Removal. The CP is redundant information added before the OFDM symbol to mitigate inter-symbol interference caused by multipath during Wi-Fi signal propagation. It is subsequently removed at the receiver. As a result, the tag data carried on the CP is lost.

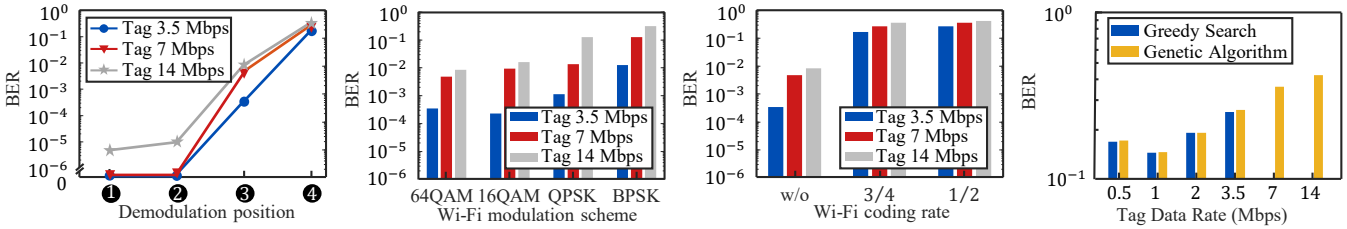
Demodulation. The demodulation of bits from frequency domain samples inherently entails information loss. In theory, the received frequency domain IQ, assuming an ideal channel devoid of any distortion, should precisely align with the transmitted IQ on the constellation map. For instance, in the case of QPSK, the received IQ should align with the four constellation points, as illustrated in Figure 3c. However, as depicted in Figure 3a and governed by Eqn. 1, the frequency domain IQ sample contains tag information modulated across all time domain IQ values, resulting in its location deviating from the four constellation points, independent of any wireless channel influence. For instance, the *yellow dots* in the constellation map signify potential locations of the received frequency domain IQ sample, modulated from "00" when various random θ values are applied to each time domain sample. We note that, although the precise location of the frequency domain IQ after FFT contains valuable tag information, the demodulation process selects the nearest constellation point as the output, thereby leading to a significant loss of tag information, just as shown in Figure 3c.

DC and Guard-band Subcarriers Removal. Wi-Fi transmits no data on the DC and guard-band subcarriers, so the IQ samples demodulated from those subcarriers convey no information and thus are discarded. Due to information dispersion, the tag-modulated data spreads within these DC and guard-band subcarriers, despite not carrying Wi-Fi data. To illustrate this phenomenon, we refer to the example depicted in Figure 3(d). Figure 3(d) showcases the phase of the IQ demodulated from all Wi-Fi subcarriers, where Wi-Fi transmits identical data "11" on all data subcarriers using QPSK, both with and without tag modulation. Without tag modulation, the phase of the demodulated IQ is $-\frac{3}{4}\pi$ and 0 on data subcarriers and other subcarriers, respectively. However, when the tag modulates its data on the time domain IQ, the modulated information disperses, altering the phase of all subcarriers, especially the DC and guard-band subcarriers. Consequently, discarding the IQ demodulated from those DC and guard-band subcarriers also results in significant information loss.

Channel Decoding. The channel decoding process also introduces information loss as it eliminates the redundancy of the coded bits to generate the packet bits. For instance, with a coding rate of 1/2, one packet bit is decoded from two coded bits. Additionally, due to forward error correction, different coded bits may be decoded into the same packet bits, as shown in Figure 3b.

2.2.3 Information Shuffling. The interleaving process within the Wi-Fi physical layer alters the sequence of demodulated bits. In theory, if the data undergoes both interleaving at the sender and deinterleaving at the receiver, the final bit order should remain unchanged. However, it's important to note that the tag directly modulates its data on time-domain IQ samples during wireless transmission, thus only experiencing the deinterleaving operation. Consequently, the tag-modulated information undergoes shuffling due to the deinterleaving process.

2.2.4 Impact on Tag Data Demodulation. The perturbations induced by Wi-Fi physical layer operations, including information dispersion, loss, and stuffing, impact two key facets of tag data demodulation: demodulation complexity and demodulation accuracy. Firstly, information dispersion and shuffling significantly complicate the correlation between the tag-modulated data and the metadata within or output by the Wi-Fi physical layer. This complexity poses challenges in reversing the mapping process to derive the original data



(a) Impact of positions. **(b)** Impact of Wi-Fi modulation. **(c)** Impact of Wi-Fi coding rate. **(d)** Impact of tag data rate.

Figure 4: The accuracy of tag-data demodulation using GA algorithm. The impact of the position that the data recorded inside the physical layer is shown in **(a)**. The impact of Wi-Fi modulation scheme and coding rate is shown in **(b)** and **(c)**. The impact of tag data rate is shown in **(d)**.

modulated by the tag. Secondly, information loss renders accurate demodulation of the tag data unattainable unless intentional redundancy is added within the tag data, albeit at the expense of reduced throughput. More importantly, as the tag data undergoes more Wi-Fi operations, higher computational overhead and increased demodulation bit error rate (BER) are anticipated.

2.3 Experimental Verification

In this section, we conduct the simulation to validate and quantify the impact of Wi-Fi physical operations on the demodulation complexity and accuracy.

2.3.1 Tag Data Demodulation Algorithm. We introduce the tag data demodulation algorithm we implemented in our simulation. Our algorithm decodes the tag data from either the meta-data inside the physical layer, *e.g*, the frequency domain IQ and coded bits, or the packet bits output by the physical layer. Specifically, we implement a maximum-likelihood demodulator:

$$\Theta = \arg\min_{\Theta} \|\mathbf{M}^* - \mathbf{M}(\Theta)\| \tag{2}$$

where $\Theta = [\theta_1, \theta_2, \dots \theta_N]^T$ represents a vector of size N containing the tag-modulated data (*e.g.*, phase shifts) applied to the Wi-Fi time-domain IQ samples. The $\mathbf{M}^*$ represents the received metadata or the packet bits; and the $\mathbf{M}(\Theta)$ represents the theoretical metadata or packet bits, given the tag modulated data Θ. Essentially, our demodulation algorithm searches for the possible tag data Θ that minimizes the distance between the theoretical data and the received data. To solve such an optimization problem, we implement a greedy search (GS) and a genetic algorithm (GA) similar to the algorithm implemented in the TScatter [35].

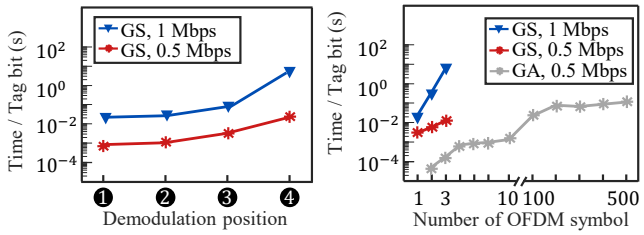
2.3.2 Experimental Setup. We employ the MATLAB WLAN Toolbox [1] for our simulations. This toolbox offers a comprehensive implementation of the IEEE 802.11n physical layer [2]. We leverage the 802.11n sender to generate time-domain IQ samples, followed by incorporating the tag-modulated data (denoted by Θ). Finally, these tag-modulated IQ samples are fed into the 802.11n receiver for processing, whose structure is depicted in Figure 2.

We evaluate the demodulation complexity and accuracy using metadata recorded at four key points within the physical layer, denoted as ❶ ❷ ❸ ❹ in Figure 2. It's important to note that our simulations assume a *perfect wireless channel with infinitely large SNR* for controlled evaluation. The simulations were conducted on a desktop equipped with an Intel Xeon E5-2650 CPU. We systematically varied the tag symbol duration T_t, which represents the number of IQ samples per tag bit, to investigate the impact of tag data rates (ranging from 0.5 Mbps to 14 Mbps). Additionally, we explored the influence of different Wi-Fi modulation and coding schemes.

2.3.3 Experimental Results. We present the simulated demodulation accuracy and complexity in this section.

Demodulation Accuracy. We configure the Wi-Fi to transmit using 64QAM and a coding rate of 3/4. The backscatter tag then modulated its data bits at three different rates. We calculate the Bit Error Rate (BER) of the tag data demodulated from the recorded metadata at positions ❶ ❷ ❸ ❹. The results are plotted in Figure 4a. It is evident that more physical layer operations the tag-modulated data goes through, more information loss it experiences and thus higher the BER after demodulation. Specifically, the BER reaches 33% when we demodulate using the packet bits that go through all physical layer operations.

We also observe a sharp increase of the BER between positions ❷ and ❸, which is attributed to significant tag information loss caused by Wi-Fi demodulation, The extent of this information loss depends on Wi-Fi modulation schemes. To quantify that, we vary the modulation scheme and plot the BER of the tag-data demodulation using data recorded at position ❸ in Figure 4c. We see that lower modulation has fewer points on the constellation map and thus causes larger



(a) Average demodulation time per tag symbol at the positions. **(b)** Impact of tag data rate and number of OFDM symbol.

Figure 5: Demodulation complexity.

quantization error during demodulation, which in turn results in more information loss and higher BER. At last, we note that lower Wi-Fi coding rates lead to more tag information loss and result in higher BER. For instance, the BER at 1/2 coding rate is higher than that at 3/4 coding rate, as illustrated in Figure 4c.

We also compare the demodulation performance of the GS and GA algorithm using packet bits at position ❹ and plot the BER of two algorithms in Figure 4d [1]. These two algorithms exhibit no significant difference in their BER, demonstrating the correctness of the implementation of our GA algorithm. Figure 4d also demonstrates that, even under perfect channel with infinite SNR, the demodulation BER of using packet bits output by the Wi-Fi physical layer exceeds 10^{-1}, even at the minimum tag data rate of 0.5 Mbps ($T_t = 28T_s$). Therefore, it is impossible to demodulate the sample-level tag-modulated data using commercial Wi-Fi NIC that only provides the decoded packet bits at position ❹.

Demodulation Complexity. We investigate the demodulation complexity by calculating the average demodulation time using data recorded at positions ❶ ❷ ❸ ❹. In this experiment, we test Wi-Fi packets containing only three OFDM symbols, with the tag data rate set to 0.5 Mbps and 1 Mbps. We configure the Wi-Fi to transmit using 64QAM and a coding rate of 3/4. The results are plotted in Figure 5a, revealing that demodulation complexity increases exponentially with the number of physical layer operations the data undergoes. Specifically, the decoding time reaches 0.02 and 7.48 seconds per tag bit when decoding data at position ❹ at data rates of 0.5 Mbps and 1 Mbps, respectively, a duration that is prohibitive for real-world implementation.

Furthermore, we explore the impact of packet length on decoding complexity. We extend the packet size from one to 500 OFDM symbols, modulating tag data on each symbol with tag data rate of 0.5 Mbps and 1 Mbps. Demodulation of tag data occurs at position ❹, and the decoding time is depicted in Figure 5b. The results indicate an exponential

[1]It is computationally infeasible to decode tag date using greedy search (GS), when its data rate exceeds 3.5 Mbps ($T_t < 0.2\mu s$, 4 OFDM samples).

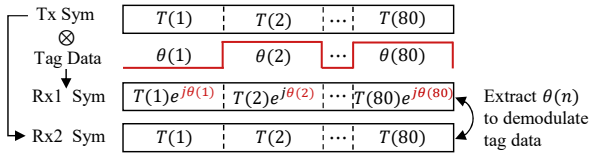


Figure 6: An overview of demodulation scheme.

increase in decoding time, with the GS algorithm quickly becoming incapable of demodulating the data. While the GA algorithm manages to decode data even with a packet of 500 OFDM symbols, its computational overhead remains unacceptable. For instance, modulating tag data at a rate of 0.5 Mbps across 2 to 500 symbols yields an average demodulation time ranging from 4.9×10^{-5} to 0.1 seconds. This analysis underscores the significant gap between demodulation speed and data transmission rate.

Takeaways. Based on the analysis above, both demodulation error and complexity exhibit exponential growth as the number of physical layer operations that the tag data experienced increases. This observation yields two important insights. Firstly, it becomes impractical to demodulate tag data modulated at the sample level using data received from commercial Wi-Fi NIC, specifically, the packet bits recorded at position ❹. Second, the time domain IQ samples experience zero information dispersion, loss, and shuffling. Therefore, a tag-data demodulator using time domain IQ samples achieves the highest level of time efficiency and accuracy.

3 DESIGN OF TAG-DATA DEMODULATOR

In this section, we introduce our demodulator design tailored for tag data modulated at the OFDM sample level. Specifically, leveraging insights from Section 2, our demodulator processes the time-domain IQ samples as input.

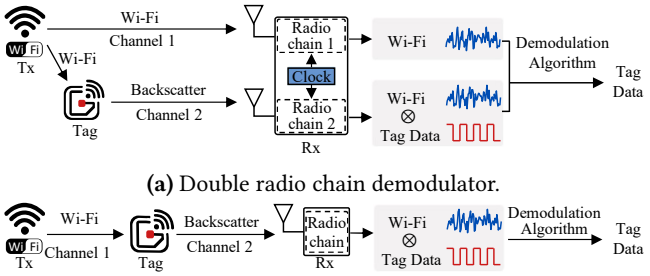
3.1 Overview of Demodulation Scheme

Signal Model. The backscatter tag modulates its data by altering the phase of the Wi-Fi signal at time domain IQ samples, so the backscatter signal is represented as:

$$R_1(n) = T(n) \cdot e^{j\theta(n)}. \tag{3}$$

where $T(n)$ represents the n-th OFDM sample and $\theta(n)$ is the tag modulated data (phase variation) on the n-th OFDM sample, just as shown in Figure 6. Therefore, the task of our demodulator is to derive the tag-modulated data from the received time domain sample $T(n)$.

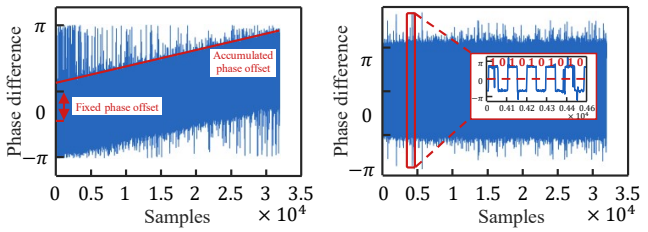
Reference Signal: Key for Demodulation. The cornerstone of the time-domain demodulator lies in identifying the appropriate reference signal. For instance, when we receive a duplicate of the transmitted signal without tag modulation alongside the tag-modulated signal, as depicted in Figure 6,



(a) Double radio chain demodulator.

(b) Single radio chain demodulator.

Figure 7: A comparison of the double radio chain demodulator and the single radio chain demodulator.



(a) Phase offsets caused by non-ideal oscillators at Tx, tag and Rx.

(b) Eliminating phase offset by differential operation.

Figure 8: Phase offset in the dual radio demodulator.

we can demodulate the tag data by directly comparing the phase of each corresponding OFDM sample within both versions of the received signal.

Two Types of Demodulator. Depending on the source of the reference signal, we propose two demodulator types: the dual radio chain demodulator and the single radio chain demodulator, as illustrated in Figure 7. For the dual radio chain demodulator, we utilize one radio chain to capture the tag-free Wi-Fi transmission in the original Wi-Fi channel and a separate radio chain to capture the tag-modulated Wi-Fi transmission in a different channel, as the tag shifts the Wi-Fi signal to a separate channel. In contrast, the single radio chain demodulator only listens and records the tag-modulated Wi-Fi transmission, where we have access to both the reference signal and the tag-modulated signal.

3.2 Double Radio Chain Demodulator

Tag Modulation. The tag is able to modulate its data on every time domain OFDM samples, *i.e.*, 80 in total, just as shown in Figure 6, achieving a tag data rate up to 20 Mbps with BPSK modulation and 40 Mbps with QPSK modulation.

3.2.1 Demodulator. To accurately decode the tag-modulated data, the two received signal copies must be perfectly aligned in time, which requires two tightly synchronized radio chains. Therefore, we implement the two radio chains using two daughter boards on one USRP which share a common clock source, as shown in Figure 7a. We set the frequency of one radio daughter board to receive the original Wi-Fi signal and the other to receive the backscatter signal. This ensures that both signals are sampled simultaneously, aligning their corresponding samples in time.

3.2.2 Phase Offsets. We address phase offsets in this section.

Source of Phase Offsets. The phase offsets are mainly caused by non-ideal oscillators at the Tx, tag and Rx. Since the Wi-Fi signal is backscattered and frequency-shifted by the tag, it should be down-converted to the baseband at the receiver. Ideally, the local carrier frequency for down-conversion should be the sum of the transmitted Wi-Fi carrier and the tag's shifting frequency, with a phase of zero. However, non-ideal oscillators at the Tx, tag and Rx, can disrupt this, causing the local carrier frequency to deviate from this sum and the phase to be non-zero, resulting in residual frequency and fixed phase offsets. This affects both radio chains receiving the original Wi-Fi and backscatter signals. We denote the frequency offsets as Δf_1 and Δf_2, and the fixed phase offsets as $\Delta\phi_1$ and $\Delta\phi_2$. Therefore, the received Wi-Fi signal at the first radio is:

$$R_1(n) = T(n) \cdot e^{j(2n\pi\Delta f_1 + \Delta\phi_1)}. \tag{4}$$

the received backscatter signal at the second radio chain is:

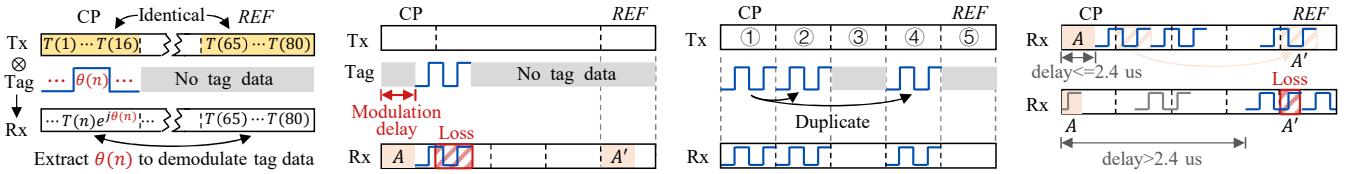
$$R_2(n) = T(n) \cdot e^{j\theta(n)} \cdot e^{j(2n\pi\Delta f_2 + \Delta\phi_2)}. \tag{5}$$

Therefore, the phase difference between the two signals incorporates the tag-modulated phase, an accumulated phase offset caused by frequency offset $\Delta f_1 - \Delta f_2$, and a fixed phase offset $\Delta\phi_1 - \Delta\phi_2$, as illustrated in Eqn. 6:

$$\frac{R_2(n)}{R_1(n)} = e^{j\theta(n)} \cdot e^{j(2n\pi(\Delta f_1 - \Delta f_2) + (\Delta\phi_1 - \Delta\phi_2))}. \tag{6}$$

To further understand this phenomenon, we modulate tag data onto Wi-Fi signal using BPSK and receive both the Wi-Fi and backscatter signals simultaneously. The phase difference between corresponding OFDM samples of the two signals is plotted in Figure 8a. The phase difference increases gradually with the samples, causing phase errors at the receiver and leading to tag-data demodulation errors.

Solution. A typical Wi-Fi receiver calibrates frequency offset in the frequency domain using CSI and pilots. However, as explained in section 2, sample-level modulated tag data is associated with all frequency-domain subcarriers, causing standard calibration methods to lose tag information. In this paper, we address this by performing a differential operation on the phase difference between samples of two adjacent tag symbols and demodulating the tag data based on the phase variation. We then estimate the fixed phase offset using the first known tag data. As illustrated in Figure 8b,



(a) The *REF* is serve as reference to demodulate tag data on the CP. **(b)** Modulation delay leads to tag data that outside the CP loss. **(c)** Repeatedly modulate tag data three times within a symbol. **(d)** The repeated modulation can tolerate up to 2.4 μs delay.

Figure 9: Modulation and demodulation scheme of the single radio chain demodulator. The basic idea of modulation and demodulation is shown in **(a)**. **(b)** shows the tag data outside the CP is unable to demodulated due to lack of reference samples. **(c)** and **(d)** show our repetition modulation scheme to address tag modulation delay.

the phase difference no longer accumulates across OFDM samples, enabling accurate phase difference decisions and successful tag data demodulation.

3.2.3 Tag Modulation Delay. Since the Wi-Fi preamble must remain unchanged for the receiver to identify backscatter signal, the tag data should be modulated onto the Wi-Fi payload. Tags utilize the detection method in Section 4 to detect the Wi-Fi signal and determine the payload position before modulating data. However, due to inherent processing delay of the detection circuit, the detected payload position may lag behind the true, resulting in tag modulation delay.

To estimate this delay and locate the tag data within the backscatter signal, a synchronization sequence (1010) is added before the tag data. Upon receiving the backscatter signal, the receiver first searches for this synchronization sequence, and its end marks the start of the tag data.

3.3 Single Radio Chain Demodulator

Key Observation. The key observation we have is that, inside each OFDM symbol, the cyclic prefix and the last quarter of the OFDM symbol are identical, just as shown in Figure 9a. Therefore, we can effectively use the last quarter of the OFDM symbol (referred to as *REF*) as a reference for calculating the tag's phase modulation and, consequently, demodulating the tag data.

3.3.1 Tag Data Modulation and Demodulation. In this section, we detail the tag modulation and demodulation process.

Modulation. Taking 802.11n Wi-Fi signals with 20 MHz bandwidth as an example, both the CP and the *REF* contain 16 OFDM samples, allowing for a maximum of 16 tag symbols modulated inside each OFDM symbol, as illustrated in Figure 9a, which achieves a theoretical maximum tag data rate of 4 Mbps and 8 Mbps, if the tag modulates data using BPSK and QPSK, respectively. It's worth noting that, while the theoretical maximum tag data rate of our single radio chain solution is slightly lower than that of the dual radio chain solution, we, however, significantly reduce hardware costs and complexity.

Just as shown in Figure 9a, the received tag-modulated signal can be represented as:

$$R_c(n) = T_c(n) \cdot e^{j\theta(n)}. \tag{7}$$

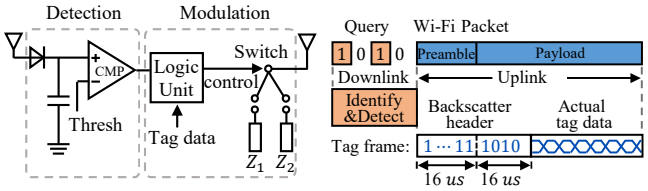
Here, $T_c(n)$ and $R_c(n)$ represent the n^{th} sample of the CP in the Tx symbol and Rx symbol, respectively. $\theta(n)$ is the tag modulated phase change on n^{th} sample. It's important to note that only the CP is modulated with tag data, while the *REF* remains unchanged.

Demodulation. At the receiver, we separate the samples inside each received OFDM symbol that belongs to the CP, and that belongs to the *REF*, denoted as $R_e(n)$. Since the tag modulates no data on *REF* and the samples in *REF* is identical to that in the CP within the transmitted OFDM symbol, so we have $R_e(n) = T_e(n) = T_c(n)$. Consequently, the tag data can be demodulated by directly comparing the phase differences between the corresponding samples in the CP and *REF* of the received OFDM symbol.

3.3.2 Tag Modulation Delay. The modulation delay induced by the detection circuit described in Section 4 results in some tag data being modulated outside the CP and unable to be demodulated due to the lack of reference samples, as illustrated in Figure 9b.

We have an observation from Figure 9b, the portion A within the CP and the portion $A^{'}$ within the *REF* are identical, with neither portion modulated by tag data. This inspires us to artificially delay the tag data modulated outside the CP to align with $A^{'}$, and serve the portion A as reference to demodulate this tag data. We achieve this by repeatedly modulating tag data three times on the segment ① ② ④ within an OFDM symbol, each with the same duration as the CP, as illustrated in Figure 9c.

Figure 9d illustrates that the repetition modulation makes the tag data modulated outside the CP appears at $A^{'}$ within the *REF*. While the corresponding samples at A remain unchanged. Consequently, the samples from A can serve as a



(a) Tag hardware. **(b)** Tag data frame.

Figure 10: Tag Design: **(a)** detection and modulation are the two main modules of the tag. Tag data frame and MAC layer protocol to support multiple tags is shown in **(b)**.

reference to demodulate tag data in $A^{'}$, enabling the demodulation of tag data outside the CP. However, if the modulation delay exceeds 2.4 μs, the portion A within the CP is modulated by other tag data, rendering it unable to serve as a reference for demodulation. Consequently, the tag data outside the CP cannot be demodulated in this case, indicating that our repetition modulation scheme can tolerate a modulation delay within 2.4 μs.

3.3.3 Phase Offset. Similar to the dual radio chain demodulator, non-ideal oscillators on the Tx, tag and Rx also induce phase offsets to the received OFDM symbols in the single radio chain demodulator. Since the CP and *REF* are within one OFDM symbol, they experience the same frequency offset (denoted as Δf) and fixed phase offset. However, the accumulated phase offset caused by frequency offset on the *REF* is greater than that on the CP, as the REF is at the end of the OFDM symbol and the CP is at the beginning. We denote the number of OFDM samples between the CP and *REF* as m. Therefore, the phase difference of the corresponding samples in the CP and *REF* will be $2m\pi\Delta f + \theta(n)$. Similar to dual radio chain demodulator, we perform differential operation on this phase difference between samples corresponding to two adjacent tag symbols and then demodulate tag data based on the phase variation.

4 TAG DESIGN

In this section, we introduce the tag designed in this paper, including tag hardware, CP detection and tag data frame.

4.1 Tag Hardware

We have demonstrated that the complexity of high-throughput backscatter lies in the demodulation scheme, not in the tag's modulation. Therefore, our tag shares a similar hardware implementation with FreeRider [63]. It consists of a *detection module* and a *modulation module*.

Detection Module. The detection module serves two purposes: detecting Wi-Fi signal to ensure tag data is modulated onto the Wi-Fi signal rather than others, and determining the starting position of the Wi-Fi payload for tag modulation. Standard Wi-Fi detection methods are not suitable for backscatter tags due to low power constrains. We detect Wi-Fi signals based on amplitudes levels, as it typically has higher power compared to noise. This is achieved by a low-power envelope detector followed by a comparator, as illustrated in Figure 10a. The comparator outputs a high level if the envelope's amplitude exceeds threshold, indicating Wi-Fi signal detection. The payload's starting position is then determined after the Wi-Fi preamble duration, and the modulation module is activated to begin modulating data.

Modulation Module. The modulation module performs two key tasks: altering the phase of the Wi-Fi signal based on the tag data and frequency-shifting the backscatter signal to a separate channel to avoid interference with the original Wi-Fi signal. Our low-power approach uses a *switching mixer*, where an RF switch connected to the backscatter antenna toggles between two impedances, Z_1 and Z_2, as shown in Figure 10a. When connects to Z_1, the Wi-Fi signal is totally reflected, while it is totally absorbed when connects to Z_2. This toggling essentially multiplies the Wi-Fi signal by a square wave at the toggling rate, resulting in a frequency shift. The toggling rate is controlled by a clock generated by the PLL within FPGA on the tag. This clock also alters the Wi-Fi signal phase for tag data modulation, For instance, BPSK modulation requires two clocks with different phases, while QPSK modulation requires four.

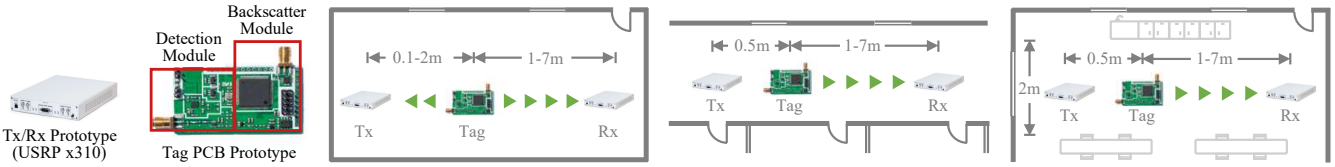
4.2 Detecting CP Position

For our single radio chain demodulator, tag data should ideally be modulated on the CP. Therefore, detecting the CP before modulating is necessary. We detect the CP position by identifying the start of the Wi-Fi payload, as OFDM symbols within the payload have a fixed structure that begins with the CP, using detection circuit described in Section 4.1.

There is a delay between the detected and actual CP positions, resulting in modulation delay. The delay mainly depends on the performance of components in the detection circuit. Specifically, in both FreeRider [63] and our paper, the NCS2200 [41] comparator has a propagation delay up to 1.1 μs, and the LT5534 [4] envelope detector has a full-scale settling time of 0.038 μs. Theoretically, the delay does not exceed 1.138 μs. Therefore, this detection circuit is theoretically sufficient for our single radio chain demodulator, which can tolerate a modulation delay (detection delay) up to 2.4 μs. To better justify the accuracy and robust of this detection circuit, we conduct experiments in Section 5.5.

4.3 Tag Data Frame

The tag data frame comprises two fields: a backscatter header field and an actual tag data filed, as illustrated in Figure 10b.



(a) Tx/Rx and Tag prototype. **(b)** Empty room. **(c)** Corridor. **(d)** Office.

Figure 11: Testbed and diagram of the experimental environments. (a) Tx, Rx and tag prototype. (b) An empty room without multipath. (c) A corridor with few multipath. (d) An office with rich multipath.

The backscatter header consists of two segments. The first is a 16μs sequence of all ones, reflecting the Wi-Fi preamble to the receiver without alteration. The second segment is a fixed sequence of 1010 with a duration of 16μs, assisting the receiver in locating the actual tag data. The actual tag data field contains the effective tag data, with its rate determined by the modulation scheme and the tag symbol duration.

To support multiple tags, the Tx can transmit a unique query sequence followed by excitation Wi-Fi signal to each tag, similar to FreeRider [63]. Upon identifying the sequence intended for itself, the tag activates the detection module to detect the subsequent excitation Wi-Fi signal, and determine the Wi-Fi payload or the CP for modulation. As illustrated in Figure 10b *upper*, the query sequence is a binary sequence achieved by the presence or absence of Wi-Fi short packets.

5 EVALUATION

In this section, we first introduce the implementation of the evaluation system and then present the evaluated performance of our tag-data demodulation algorithm in both dual radio chain demodulator and single radio chain demodulator.

5.1 Implementation

Our evaluation system comprises a Wi-Fi transmitter (Tx), a tag and a receiver (Rx). Details as follows:

Tx and Rx prototype. Both the Tx and Rx prototype are implemented on USRP x310 [14] equipped with UBX-160 daughterboards, as shown in Figure 11a. The Tx is configured to operate at 2.412 GHz, transmitting 802.11n Wi-Fi signals with a power of 26 dBm. For the dual-radio chain demodulator, the two Rx channels are set to operate at 2.412 GHz and 2.442 GHz to receive the excitation Wi-Fi signal and backscatter signal, respectively. For the single-radio chain demodulator, the Rx channel is set to operate at 2.412 GHz to receive the backscatter signal.

Tag prototype. Our tag shares a similar hardware with FreeRider [63]. It is implemented on an open-source backscatter platform [55], consisting of an LT5534 [4] envelope detector followed by an NCS2200 [41] comparator for the detection module, an ADG902 RF switch [5] controlled by an AGLN250 FPGA [39] for the modulation module, and a 20 MHz oscillator. The tag data is modulated using both BPSK and QPSK, and the backscatter signal is reflected with a 30 MHz frequency shift. The difference from FreeRider [63] is that our tag data is modulated at the OFDM sample level, while FreeRider modulates at the OFDM symbol level.

Testing environment. To extensively evaluate the demodulation and detection performance, we conduct experiments in three scenarios, as demonstrated in Figure 11: an empty room has almost no multipath (Figure 11b), a corridor with few multipath (Figure 11c), and an office with very rich multipath (Figure 11d).

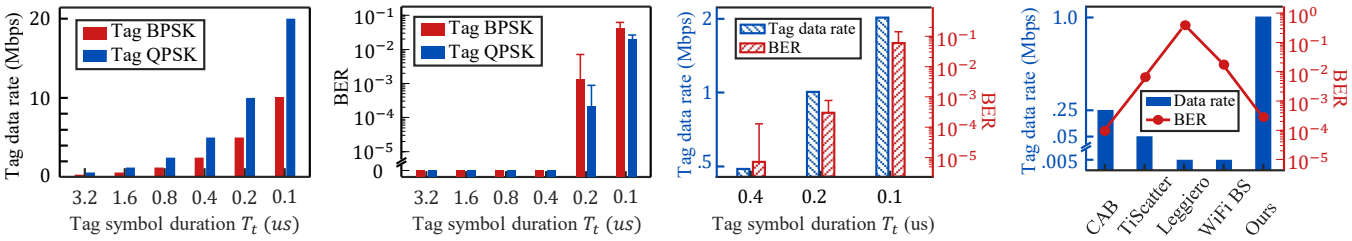
5.2 Tag Power Consumption.

The power consumption of tag consists of two parts: detection module and modulation module. The LT5534 [4] envelope detector and NCS2200 [41] comparator in the detection module consumes 21 mW and 0.03 mW, respectively. The power consumption of modulation module implemented on the AGLN250 FPGA [39] consists of static and dynamic components. The static power consumption, which occurrs when the tag is powered but not transmitting, is 0.026 mW. The dynamic power consumption, which occurs when the tag is transmitting, is up to 2.503 mW. Therefore, the total power consumption of the tag PCB prototype is up to 23.559 mW. Notably, the envelope detector can be implemented using passive analog components, such as capacitors and diodes, requiring no power. And the IC simulation using a 45 nm power analysis tool in HitchHike [61] demonstrates that the modulator's power can be reduced to μW-level. Therefore, a potential IC prototype of the tag can be provided by an energy harvesting system, such as solar panels.

5.3 Evaluate Demodulation Performance

We evaluate the performance of our dual radio chain and single radio chain demodulator, and then investigate the impact of Wi-Fi modulation scheme, Tx-to-tag distance, tag-to-Rx distance, multipath, and tag modulation delay.

5.3.1 Demodulation Accuracy. In this section, we conduct experiments in the empty room. Figure 12a and Figure 12b



(a) The tag data rate of varying T_t in dual radio demodulator.

(b) The BER of varying T_t in dual radio chain demodulator.

(c) Rate and BER in single radio chain demodulator.

(d) Compare with exising single radio chain demodulator.

Figure 12: Demodulation accuracy of the dual and single radio chain demodulator. **(a)** and **(b)** show that we can achieve a tag data rate up to 10 Mbps in the dual radio chain demodulator. **(c)** show that we can achieve a tag data rate up to 1 Mbps in the dual radio chain demodulator. **(d)** shows that our single radio chain demodulator achieves higher tag data rate and lower BER.

illustrate the corresponding data rate and demodulation BER for varying tag symbol duration, ranging from 3.2 μs to 0.1 μs, in the dual radio chain demodulator. It is evident that both the tag data rate and BER rise as the tag symbol duration decrease. For instance, the BER remains 0 when $T_t \geq 0.4\mu s$, while it increases over 10^{-2} when $T_t \leq 0.1\mu s$. This is because shorter tag symbols have lower signal-to-noise ratio (SNR) that in increased channel distortion and thus higher BER. Therefore, we can achieve a tag data rate up to 10 Mbps ($T_t = 0.2\mu s$) with QPSK modulation to achieve a BER of at 10^{-4} in the double radio chain demodulator.

Figure 12c shows that it achieves a tag data rate up to 1 Mbps ($T_t = 0.2\mu s$) with BER at 10^{-4} in the single radio chain demodulator. Figure 12d compares existing OFDM-based single radio chain demodulators (CAB [57], TiScatter [11], Leggiero [40], and Wi-Fi BS [29]) with ours. It is evident our algorithm achieves higher tag data rate and lower BER.

5.3.2 Robust to Wi-Fi Modulation Schemes. We conduct an experiment embedding tag data at 5 Mbps and 10 Mbps using QPSK modulation onto Wi-Fi signals with different modulation schemes ranging from BPSK to 64 QAM, and demodulating using the dual radio chain demodulator. Figure 13 shows consistent demodulation accuracy across various Wi-Fi modulation schemes, indicating the robustness of our algorithm. This robustness is due to the use of time domain IQ samples that does not experience any Wi-Fi physical layer operations. Therefore, various in Wi-Fi characteristics (such as modulation scheme) naturally do not impact its performance. The same applies to the single radio chain demodulator, which operates on the same principle.

5.3.3 Impact of Tx-to-tag and tag-to-Rx Distance. To evaluate the impact of Tx-to-tag distance, we conduct an experiment in the empty room, with a fixed tag-to-Rx distance of 1 m and varying Tx-to-tag distance from 0.1 m to 2 m. Tag data is modulated at rates of 5 Mbps and 10 Mbps using QPSK and demodulated with the dual radio chain demodulator.

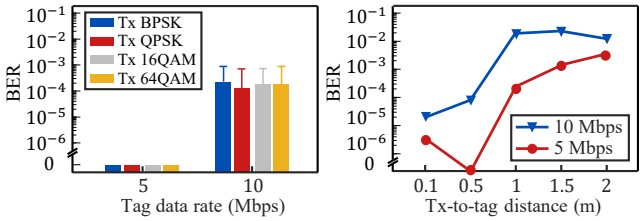


Figure 13: Robust to Wi-Fi modulation scheme.

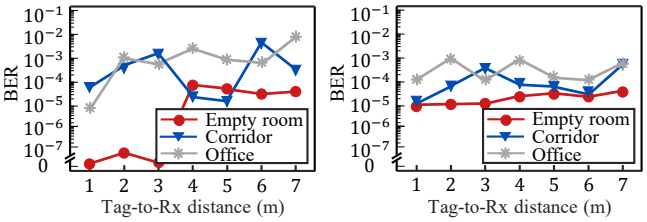
Figure 14: Impact of Tx-to-tag distance.

Figure 14 illustrates that the BER generally increases with Tx-to-tag distance. For instance, the BER remains at 10^{-4} for Tx-to-tag distance up to 0.5 m, but exceeds 10^{-2} beyond 1 m.

To evaluate the impact of tag-to-Rx distance, we fix the Tx-to-tag distance at 0.5 m and vary the tag-to-Rx distance from 1 m to 7 m. Using BPSK modulation with a tag symbol duration T_t of 0.4μs. The *red line* in Figure 15a and 15b illustrate that the BER increases with tag-to-Rx distance increase, indicating that the increased BER is primarily due to reduced backscatter signal power as the tag-to-Rx distance increases.

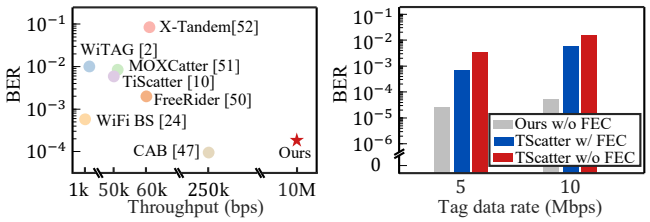
5.3.4 Impact of Multipath. In a standard Wi-Fi system, the CP at the beginning of the OFDM symbol mitigates inter-symbol interference (ISI) caused by multipath. However, in our single radio chain demodulator, the CP is altered by tag data, compromising this function. Multipath signals arriving later than direct signals cause interference between tag symbols, whose durations span several OFDM samples. This overlap results in tag symbol distortion and increases the demodulation BER.

To assess the impact of this distortion on tag data demodulation, we conduct experiments in three environments with different multipath characteristics, and plot results in Figure 15. Using BPSK modulation with a T_t of 0.4 μs and both dual and single radio chain demodulators, we observe that the severity of multipath impact on demodulation performance depends on its richness. For instance, an office with



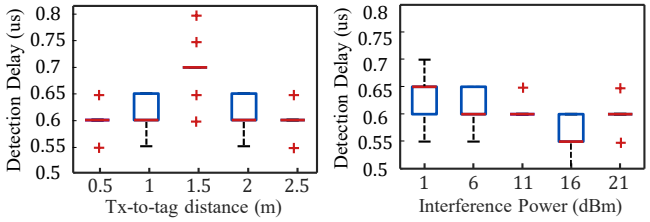
(a) Dual radio demodulator. **(b)** Single radio demodulator.

Figure 15: Impact of tag-to-Rx distance and multipath.



(a) **(b)**

Figure 16: Compare with state of the art. (a) Compare with packet-level [29] and symbol-level [3, 11, 57, 63–65] modulation. (b) Compare with sample-level modulation [35].



(a) Detection delay under different Tx-to-tag distance. **(b)** Detection delay with interference.

Figure 17: Evaluate detection circuit.

multiple desks and cabinets exhibits richer multipath, resulting in greater backscatter signal distortion and higher BER, exceeding 10^{-3}. Moreover, in corridor and office environments, the multipath signal's superposition varies with different tag-to-Rx distances, so BER does not monotonically increase with increasing distance.

5.4 Comparing with state of the art

5.4.1 Compare with Modulation at the Wi-Fi Packet level and OFDM Symbol level. The main difference between our approach and packet-level or symbol-level methods is that we modulate at the OFDM sample level. This enables shorter tag symbol durations and significantly higher throughput. As illustrated in Figure 16a, our method achieves up to 10 Mbps, compared to approximately 1 kbps for packet-level and 0.25 Mbps for symbol-level approaches in existing OFDM Wi-Fi backscatter systems. Moreover, we compare the lowest achievable BER of our approach with those of packet-level and symbol-level approaches corresponding to the aforementioned throughputs. Figure 16a demonstrates that our approach achieves a BER of 10^{-4} — comparable to the symbol-level approach [57]— but with a data rate at least 40 times higher. Overall, our approach offers higher throughput while maintaining a low BER.

5.4.2 Compare with Modulation at the OFDM Sample level. We compare our work with existing high-throughput Wi-Fi backscatter research, such as BackFi [7] and TScatter [35].

Difference with BackFi [7]. It requires a full-duplex Wi-Fi transceiver, which is extremely complicated to implement.

Difference with TScatter [35]. We would like to emphasize that the BER presented in TScatter is obtained using convolutional code-protected tag bit (2/3 coding rate). In contrast, our BER is reported without any protection on the tag bits. Even with FEC on tag bits, TScatter's BER is approximately two orders of magnitude higher than ours. For instance, as show in Figure 16b, at a tag rate of 5 Mbps, TScatter's BER is close to 10^{-3}, whereas ours is 1.7×10^{-5}. At 10 Mbps, TScatter's BER is 5×10^{-3}, while ours is 5×10^{-5}. Without FEC, TScatter's BER exceeds 10^{-2}. This is because TScatter uses packet bits output by the Wi-Fi physical layer, while we use time-domain IQ samples, for demodulation. As analyzed in Section 2, Wi-Fi physical layer operations lead to tag information distortion, resulting in higher BER. Moreover, Section 2.3.3 shows that the TScatter method encounters an extremely high computational complexity, which increases exponentially with data rates and OFDM symbol numbers.

Overall, it is unattainable to demodulate sample-level modulated tag data using commercial Wi-Fi receivers due to the excessive computational overhead and demodulation error.

5.5 Evaluate Detection Performance

To better justify the accuracy and robust of the detection circuit, we conduct two experiments in the empty room.

In the first experiment, we fix the transmitted Wi-Fi signal power at 26 dBm and evaluate the detection delay across a range of Tx-to-tag distance from 0.5 m to 2.5 m. The results, shown in Figure 17a, indicate that the maximum detection delay does not exceed 0.8 μ s, which is consistent with our theoretical analysis in Section 4.2 and satisfies the requirement of not exceeding 2.4 μ s for our single radio chain demodulator. It is known that the detection delay primarily depends on the comparator's propagation delay, which is influenced by the input overdrive [41] — the difference between the input signal and the comparator's threshold. A larger input overdrive results in a shorter delay. As the Tx-to-tag distance increases, the Wi-Fi signal power at the

tag decreases, reducing the input overdrive and slightly increasing the delay.

In the second experiment, we fix the Tx-to-tag distance at 1 m and introduce continuous sine wave interference to evaluate its impact on the detection performance. The interference power ranges from 1 dBm to 26 dBm in 5 dB steps. We preliminarily assess detection performance by measuring the packet reception rate (PRR), defined as the ratio of Wi-Fi packets received by the Rx to those transmitted by the Tx. If interference prevents the tag from detecting the Wi-Fi signal, the signal won't be reflected to the receiver, resulting in a PRR below 1. Our experiments show that the PRR remains 1 when the interference signal is below 26 dBm, indicating that the tag can still detect the Wi-Fi signal. However, when the interference power reaches 26 dBm (equal to the Wi-Fi signal strength), the PRR drops to 0, indicating the Wi-Fi signal is overwhelmed by interference and undetectable by the tag. Therefore, Figure 17b only presents results for interference power below 26 dBm. As long as the interference power is less than the Wi-Fi signal power, the tag can detect the Wi-Fi signal and maintain a detection delay within 0.8 µs, demonstrating the robustness of the detection circuit.

6 RELATED WORK

Backscatter is an innovative communication technology that utilizes existing ambient signals such as light [8, 17, 51–53, 56], acoustics[16, 24], and electromagnetic signals [3, 6, 7, 9, 10, 12, 13, 15, 19–23, 25–28, 30–34, 37, 38, 42–50, 54, 58, 60, 62, 66] as carriers to transmit tag data, resulting in a substantial reduction in tag power consumption. Among these, the Wi-Fi backscatter has attracted significant attention due to the widespread presence of Wi-Fi signals in daily life. We investigate Wi-Fi backscatter communication from two perspectives: modulation granularity and the number of receiving radio chains.

Modulation Granularity. Pioneering work Wi-Fi backscatter [29] modulating tag data at the Wi-Fi packet level, *i.e.*, embedding 1-bit tag data per packet, achieving a rate of 1 kbps. TiScatter [11] improves this by utilizing time intervals between Wi-Fi symbols in consecutive packets to transmit multiple tag data, but the maximum rate is still limited to 100 kbps. To achieve higher rates, HitchHike [61] proposes a symbol-level modulation scheme, known as *codeword translation*, raising the rate up to 1 Mbps with 802.11b signals. FreeRider [63] extends this to OFDM-based Wi-Fi backscatter, achieving a rate up to 60 kbps. Subsequent research, such as MOXcatter[64], VMScatter [36], X-Tandem [65], and CAB [57], achieves rates from 50 to 500 kbps using this scheme. To further increase data rates, TScatter [35] proposes a sample-level modulation scheme, embedding multiple tag data within a single OFDM symbol to achieve up to 10 Mbps. However, it suffers from high demodulation BER and complexity due to significant tag information distortion and intricate mapping between tag data and Wi-Fi metadata (such as packet bits) caused by Wi-Fi physical operations.

Number of Receiving Radio Chains. Since backscatter tags modulate data by altering Wi-Fi signal characteristics, two receivers are required: one for receiving backscatter signal and the other for receiving original Wi-Fi signal, which serves as a reference for demodulation [35, 61, 63–65]. Other Wi-Fi backscatter systems such as Wi-Fi backscatter [29], CAB [57], TiScatter [11], Leggiero [40], and Chameleon [59], propose single-receiver solutions to further reduce system cost but achieve limited rates ranging from 1 to 250 kbps. Other single-radio chain systems, such as RF-Transformer[18], SD-PHY [67], and passive Wi-Fi[52], require dedicated sinusoidal signal generators, increasing system cost.

7 CONCLUSION

We push Wi-Fi backscatter throughput by modulating tag data at the OFDM sample level. Our theoretical and experimental analysis highlights that it is unattainable to demodulate sample-level modulated tag data using commercial Wi-Fi receivers due to the excessive computational overhead and demodulation error. We conclude that using time-domain IQ samples for demodulation minimizes complexity and simultaneously maximizes accuracy. We devise dual and single radio chain demodulators implementing on USRPs and achieving tag data rates of 10 Mbps and 1 Mbps, respectively, and reducing BER by at least three orders of magnitude.

To the best of our knowledge, no commercial Wi-Fi card allows direct access to raw data, including IQ samples and metadata within physical layer, further making sample-level tag data demodulation using commercial Wi-Fi receivers impractical. We believe our results pave the way for designing Wi-Fi backscatter system with extremely high throughput.

ACKNOWLEDGEMENTS

We thank our reviewers and shepherd for their insightful feedback which helped improve this paper. This work was supported by the National Natural Science Foundation of China under grant number 62372374, 62172332 and 62372372, the Shaanxi International Science and Technology Cooperation Program 2024GH-ZDXM-49, 2024GH-YBXM-07 and 2024GH-ZDXM-46.

REFERENCES

[1] [n. d.]. *WLAN Toolbox*. https://www.mathworks.com/products/wlan.html

[2] 2009. IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)* (2009), 1–565. https://doi.org/10.1109/IEEESTD.2009.5307322

[3] Ali Abedi, Farzan Dehbashi, Mohammad Hossein Mazaheri, Omid Abari, and Tim Brecht. 2020. Witag: Seamless wifi backscatter communication. In *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. 240–252.

[4] ADI. 2022. 50MHz to 3GHz RF Power Detector LT5534. https://www.analog.com/media/en/technical-documentation/data-sheets/5534fc.pdf.

[5] ADI. 2022. RF SPST Switches ADG902. https://www.analog.com/media/en/technical-documentation/data-sheets/ADG901_902.pdf.

[6] Kang Min Bae, Namjo Ahn, Yoon Chae, Parth Pathak, Sung-Min Sohn, and Song Min Kim. 2022. OmniScatter: extreme sensitivity mmWave backscattering using commodity FMCW radar. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 316–329.

[7] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. 2015. Backfi: High throughput wifi backscatter. *ACM SIGCOMM Computer Communication Review* 45, 4 (2015), 283–296.

[8] Rens Bloom, Marco Zúñiga Zamalloa, and Chaitra Pai. 2019. LuxLink: creating a wireless link from ambient light. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*. 166–178.

[9] Baicheng Chen, Huining Li, Zhengxiong Li, Xingyu Chen, Chenhan Xu, and Wenyao Xu. 2020. Thermowave: a new paradigm of wireless passive temperature monitoring via mmwave sensing. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.

[10] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. 2020. Leveraging ambient lte traffic for ubiquitous passive communication. In *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. 172–185.

[11] Caihui Du, Jiahao Liu, Shuai Wang, Rongrong Zhang, Wei Gong, and Jihong Yu. 2023. Timespan-based Backscatter Using a Single COTS Receiver. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. 450–461.

[12] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. 2021. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter Communication. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. 923–937.

[13] Rashad Eletreby, Diana Zhang, Swarun Kumar, and Osman Yağan. 2017. Empowering low-power wide area networks in urban settings. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*. 309–321.

[14] Etuss. [n. d.]. USRP X310. https://www.ettus.com/all-products/x310-kit/

[15] Chuhan Gao, Yilong Li, and Xinyu Zhang. 2018. LiveTag: Sensing Human-Object Interaction through Passive Chipless WiFi Tags. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*. 533–546.

[16] Reza Ghaffarivardavagh, Sayed Saad Afzal, Osvy Rodriguez, and Fadel Adib. 2020. Ultra-wideband underwater backscatter via piezoelectric metamaterials. In *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. 722–734.

[17] Seyed Keyarash Ghiasi, Marco A Zúñiga Zamalloa, and Koen Langendoen. 2021. A principled design for passive light communication. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 121–133.

[18] Xiuzhen Guo, Yuan He, Zihao Yu, Jiacheng Zhang, Yunhao Liu, and Longfei Shangguan. 2022. RF-transformer: a unified backscatter radio hardware abstraction. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*. 446–458.

[19] Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. 2022. Saiyan: Design and implementation of a low-power demodulator for {LoRa} backscatter systems. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. 437–451.

[20] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. 2020. Aloba: rethinking ON-OFF keying modulation for ambient LoRa backscatter. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 192–204.

[21] Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. 2019. {NetScatter}: Enabling {Large-Scale} Backscatter Networks. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 271–284.

[22] Pan Hu, Pengyu Zhang, and Deepak Ganesan. 2015. Laissez-faire: Fully asymmetric backscatter communication. *ACM SIGCOMM computer communication review* 45, 4 (2015), 255–267.

[23] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. 2016. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *Proceedings of the 2016 ACM SIGCOMM Conference*. 356–369.

[24] Junsu Jang and Fadel Adib. 2019. Underwater backscatter networking. In *Proceedings of the ACM Special Interest Group on Data Communication*. 187–199.

[25] Jinyan Jiang, Zhenqiang Xu, Fan Dang, and Jiliang Wang. 2021. Long-range ambient LoRa backscatter with parallel decoding. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 684–696.

[26] Meng Jin, Yuan He, Xin Meng, Yilun Zheng, Dingyi Fang, and Xiaojiang Chen. 2019. Fliptracer: Practical parallel decoding for backscatter communication. *IEEE/ACM Transactions on Networking* 27, 1 (2019), 330–343.

[27] Mohamad Katanbaf, Vivek Jain, and Joshua R Smith. 2020. Relacks: Reliable backscatter communication in indoor environments. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 2 (2020), 1–24.

[28] Mohamad Katanbaf, Anthony Weinand, and Vamsi Talla. 2021. Simplifying Backscatter Deployment:{Full-Duplex}{LoRa} Backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. 955–972.

[29] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. 2014. Wi-Fi backscatter: Internet connectivity for RF-powered devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*. 607–618.

[30] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. 2016. Passive {Wi-Fi}: Bringing Low Power to {Wi-Fi} Transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. 151–164.

[31] Atsutse Kludze and Yasaman Ghasempour. 2023. Leakyscatter: A frequency-agile directional backscatter network above 100 GHz. In *Proc. 20th USENIX Symp. Networked Syst. Design Implementation*.

[32] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. 2018. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In *Proceedings of the 16th ACM conference on embedded networked sensor systems*. 159–171.

[33] Zhengxiong Li, Baicheng Chen, Zhuolin Yang, Huining Li, Chenhan Xu, Xingyu Chen, Kun Wang, and Wenyao Xu. 2019. Ferrotag: A paper-based mmwave-scannable tagging infrastructure. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*. 324–337.

[34] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. 2013. Ambient backscatter: Wireless communication out of thin air. *ACM SIGCOMM computer communication review* 43, 4 (2013), 39–50.

[35] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. 2021. Verification and Redesign of {OFDM} Backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. 939–953.

[36] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, and Ting Zhu. 2020. VMscatter: A Versatile MIMO Backscatter. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 895–909.

[37] Yunfei Ma, Xiaonan Hui, and Edwin C Kan. 2016. 3D real-time indoor localization via broadband nonlinear backscatter in passive devices with centimeter precision. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. 216–229.

[38] Mohammad Hossein Mazaheri, Alex Chen, and Omid Abari. 2021. Mmtag: A millimeter wave backscatter network. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 463–474.

[39] MicroChip. 2019. IGLOO Low Power Flash FPGAs AGLN250. https://ww1.microchip.com/downloads/aemDocuments/documents/FPGA/ProductDocuments/DataSheets/microsemi_ds0110_igloo_nano_low_power_flash_fpgas_ds.pdf.

[40] Xin Na, Xiuzhen Guo, Zihao Yu, Jia Zhang, Yuan He, and Yunhao Liu. 2023. Leggiero: Analog WiFi Backscatter with Payload Transparency. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. 436–449.

[41] onsemi. [n. d.]. NCS2200. https://www.onsemi.com/download/data-sheet/pdf/ncs2200-d.pdf.

[42] Aaron N Parks, Angli Liu, Shyamnath Gollakota, and Joshua R Smith. 2014. Turbocharging ambient backscatter communication. *ACM SIGCOMM Computer Communication Review* 44, 4 (2014), 619–630.

[43] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. 2018. PLoRa: A passive long-range data network from ambient LoRa transmissions. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. 147–160.

[44] Swadhin Pradhan and Lili Qiu. 2020. Rtsense: passive rfid based temperature sensing. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 42–55.

[45] Mohammad Rostami, Karthik Sundaresan, Eugene Chai, Sampath Rangarajan, and Deepak Ganesan. 2020. Redefining passive in backscattering with commodity devices. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–13.

[46] Yihang Song, Li Lu, Jiliang Wang, Chong Zhang, Hui Zheng, Shen Yang, Jinsong Han, and Jian Li. 2023. {μMote}: enabling passive chirp de-spreading and {μW-level}{Long-Range} downlink for backscatter devices. In *20th USENIX symposium on networked systems design and implementation (NSDI 23)*. 1751–1766.

[47] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. 2017. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 1, 3 (2017), 1–24.

[48] Ambuj Varshney, Oliver Harms, Carlos Pérez-Penichet, Christian Rohner, Frederik Hermans, and Thiemo Voigt. 2017. Lorea: A backscatter architecture that achieves a long communication range. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. 1–14.

[49] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. 2017. FM backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*. 243–258.

[50] Ju Wang, Omid Abari, and Srinivasan Keshav. 2018. Challenge: RFID hacking for fun and profit. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. 461–470.

[51] Purui Wang, Lilei Feng, Guojun Chen, Chenren Xu, Yue Wu, Kenuo Xu, Guobin Shen, Kuntai Du, Gang Huang, and Xuanzhe Liu. 2020. Renovating road signs for infrastructure-to-vehicle networking: a visible light backscatter communication and networking approach. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–13.

[52] Qing Wang, Marco Zuniga, and Domenico Giustiniano. 2016. Passive communication with ambient light. In *Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies*. 97–104.

[53] Yue Wu, Purui Wang, Kenuo Xu, Lilei Feng, and Chenren Xu. 2020. Turboboosting visible light backscatter communication. In *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*. 186–197.

[54] Binbin Xie, Jie Xiong, Xiaojiang Chen, Eugene Chai, Liyao Li, Zhanyong Tang, and Dingyi Fang. 2019. Tagtag: material sensing with commodity RFID. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*. 338–350.

[55] Chenren Xu and Pengyu Zhang. 2019. Open-source software and hardware platforms for building backscatter systems. *GetMobile: Mobile Computing and Communications* 23, 1 (2019), 16–20.

[56] Xieyang Xu, Yang Shen, Junrui Yang, Chenren Xu, Guobin Shen, Guojun Chen, and Yunzhe Ni. 2017. Passivevlc: Enabling practical visible light backscatter communication for battery-free iot applications. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. 180–192.

[57] Yifan Yang, Longzhi Yuan, Jia Zhao, and Wei Gong. 2022. Content-agnostic backscatter from thin air. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 343–356.

[58] Zhice Yang, Qianyi Huang, and Qian Zhang. 2017. Nicscatter: Backscatter as a covert channel in mobile devices. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. 356–367.

[59] Longzhi Yuan and Wei Gong. 2023. Enabling Native WiFi Connectivity for Ambient Backscatter. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. 423–435.

[60] Maolin Zhang, Si Chen, Jia Zhao, and Wei Gong. 2021. Commodity-level BLE backscatter. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 402–414.

[61] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. 259–271.

[62] Pengyu Zhang and Deepak Ganesan. 2014. Enabling {Bit-by-Bit} Backscatter Communication in Severe Energy Harvesting Environments. In *11th USENIX symposium on networked systems design and implementation (NSDI 14)*. 345–357.

[63] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. Freerider: Backscatter communication using commodity radios. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. 389–401.

[64] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2018. Spatial stream backscatter using commodity wifi. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. 191–203.

[65] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2018. X-tandem: Towards multi-hop backscatter communication with commodity wifi. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. 497–511.

[66] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. 2019. OFDMA-enabled Wi-Fi backscatter. In *The 25th Annual International Conference on Mobile Computing and Networking*. 1–15.

[67] Fengyuan Zhu, Mingwei Ouyang, Luwei Feng, Yaoyu Liu, Xiaohua Tian, Meng Jin, Dongyao Chen, and Xinbing Wang. 2022. Enabling software-defined PHY for backscatter networks. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 330–342.