Redefining Passive in Backscattering with Commodity Devices

Mohammad Rostami[1,2], Karthik Sundaresan[1], Eugene Chai[1], Sampath Rangarajan[1], and Deepak Ganesan[2]
[1]NEC Labs of America
[2]University of Massachusetts Amherst

ABSTRACT

The recent innovation of frequency-shifted (FS) backscatter allows for backscattering with commodity devices, which are inherently half-duplex. However, their reliance on oscillators for generating the frequency-shifting signal on the tag, forces them to incur the transient phase of the oscillator before steady-state operation. We show how the oscillator's transient phase can pose a fundamental limitation for battery-less tags, resulting in significantly low bandwidth efficiencies, thereby limiting their practical usage.

To this end, we propose a novel approach to FS-backscatter called xSHIFT that shifts the core functionality of FS away from the tag and onto the commodity device, thereby eliminating the need for on-tag oscillators altogether. The key innovation in xSHIFT lies in addressing the formidable challenges that arise in making this vision a reality. Specifically, xSHIFT's design is built on the construct of beating twin carrier tones through a non-linear device to generate the desired FS signal – while the twin RF carriers are generated externally through a careful embedding into the resource units of commodity WiFi transmissions, the beating is achieved through a carefully-designed passive tag circuitry. We prototype xSHIFT's tag, which is the same form factor as RFID Gen 2 tags, and characterize its promising real-world performance. We believe xSHIFT demonstrates one of the first, *truly* passive tag designs that has the potential to bring commodity backscatter to consumer spaces.

CCS CONCEPTS

• **Networks → Home networks**; • **Hardware → Wireless devices**.

1 INTRODUCTION

Backscatter is the process of reflecting and modulating impinging wireless signals using simple tags, of which RFIDs (radio frequency IDs) are a quintessential example. Due to their versatility, portability and low-cost, RFIDs are growing in popularity for backend inventory management, supply chain logistics. etc. However, the need for a separate RFID transceiver/infrastructure has posed a significant impediment for their adoption in consumer spaces, especially homes. Making them viable in consumer spaces has the potential to unlock a whole new paradigm of physical analytics.

Role of frequency-shifted backscatter: Given such potential, research has focused on bringing backscatter to commodity devices. While a dedicated RFID transceiver is full-duplex and incorporates self-interference cancellation between the transmitted and backscaterred signal, commodity devices are inherently half-duplex in nature. Existing works[20, 21, 47, 48] have used separate commodity interfaces/radios tuned to different frequencies f_0 and f_s to transmit (Tx) and receive (Rx) the backscattered signal respectively. Their innovation lies in how the Tx signal at f_0 is *frequency shifted* by Δf on the tag to allow the Rx to capture the backscaterred signal in a different channel $f_s = f_0 + \Delta f$ as shown in Fig. 1.

Such frequency shifting can be accomplished either (i) *implicitly*: non-linear devices (e.g. diodes) on the tag backscatter the signal at harmonic frequencies of the input signal(s) [24, 41]; or (ii) *explicitly*: low power oscillators on the tag directly generate the Δf signal, which drives a RF switch [20, 21, 45, 47, 49]. Explicit-FS backscatter forms our focus, as it offers a fundamental advantage translating to better operational ranges (20-30 dB gain over implicit-FS) – the tags can direct most of the harvested power to the backscattered signal, unlike those in implicit-FS, where it depends on the non-linear device characteristics and cannot be controlled [7, 10].

Limitations of oscillator-driven designs: We demonstrate that by only considering the steady state oscillator operation energy (without accounting for its start-up/transient energy), current designs targeting explicit-FS are unable to capture the energy footprint of the tag in its entirety. This in turn has significant implications for the practical operation and utility of the tag itself. The oscillator's start-up phase does not have a significant impact for battery-assisted tags, which use the available battery to keep the tag operating in steady state most of the time. However, this is not the case for truly passive (battery-less) tags. The latter have to harvest energy from the Tx, store it in capacitors when the tag is OFF and use it for backscattering when it is ON, thereby going through a start-up phase every time the tag switches ON for operation. Further, a large capacitor (e.g. 1000 μF) is needed to store sufficient energy so as to activate the start-up phase of the oscillator. Indeed, we show that a few seconds of tag operation requires a charging time lasting several minutes even with the best state-of-the-art low-power MEMS oscillators [32], resulting in significantly low bandwidth (<1%) and throughput (<2 bps/μJ) efficiencies. Thus, existing oscillator-based FS tag designs apply well to battery-assisted tags, but face a significant limitation in accommodating RF harvesting for battery-less tags. While the oscillator designs for low-power applications continue to improve [15, 18], the objective of this work is to bring the benefits of explicit frequency-shifting to battery-less tags without any reliance on oscillators, thereby bringing backscatter with commodity devices much closer to consumer adoption.

MobiCom '20, September 21–25, 2020, London, United Kingdom
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7085-1/20/09…$15.00
https://doi.org/10.1145/3372224.3380880

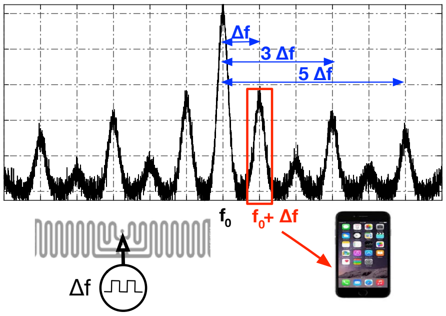


Figure 1: Frequency-shifted backscatter

Case for external frequency shifting: To this end, we propose the design of our xSHIFT system, a first-of-its-kind system that accomplishes explicit-FS backscatter without relying on oscillators in the tag to enable true passive operation. xSHIFT moves the central role of delta signal generation away from the tag to the commodity device, thereby eliminating the need for oscillators altogether. The key mathematical construct underpinning xSHIFT's design is the simple notion of beating two carrier tones (called twin carriers) through a non-linear device on the tag to generate the desired delta signal for backscattering (shown in Fig. 2). While a simple approach at the outset, realizing this primitive with commodity radios faces several formidable challenges along the way: (i) given the rigid transmission format (e.g. pilot signals) of commodity OFDM transceivers, how to generate the desired twin carriers (in addition to main carrier) responsible for the FS within commodity devices; (ii) even if we are successful in embedding the twin carriers, how can we ensure the generation of the delta signal with appropriate power on the tag to be useful for backscattering; and (iii) finally, the price to pay for frequency-shifting externally arises in the form of self-interference in the shifted frequency f_s, where the twin carriers also interact with the non-linearities in the commodity receiver to correspondingly shift the self-interference as well.

xSHIFT's Design: xSHIFT's innovation lies in addressing these critical challenges to make our vision of external frequency shifting with commodity devices a reality. Its design incorporates three key elements: (i) a novel tag design that involves a combination of Schottky envelope detector and transformer along with a tuned impedance matching circuit to provide efficient conversion of the twin carriers to the desired delta signal of sufficient amplitude for backscattering; (ii) leverages the opportunity of flexible multi-user transmissions (OFDMA) in the recently introduced 802.11ax (products already available [5]) to reverse-engineer and orchestrate desired payload transmissions from commodity devices. This enables embedding of both the desired carrier signal (e.g. bluetooth, BLE) as well as the twin carriers (leveraging the appropriate pilot signals) in specific resource units of the OFDMA frame, thereby allowing for realization with commodity devices; and (iii) the tag design incorporates a novel fractional frequency shifting (halving) that allows the backscattered signal to be isolated and received on a different channel (delta signal at harmonics of $\frac{\Delta f}{2}$), compared to the self-interference from the twin carriers, which exists at harmonics of Δf.

Deploying xSHIFT: xSHIFT leverages 802.11ax's uplink trigger mode to allow two WiFi radios on a commodity device (e.g. smart router, voice-activated device, etc.) to serve as clients – one transmitting the embedded BLE signal in its allocated RU, while the other transmitting the twin carriers in its allocated RU. The uplink transmission is orchestrated by another commodity device (e.g. smartphone) that serves as the virtual AP. While xSHIFT currently enables BLE backscattering by embedding it within 802.11ax WiFi radios, the limitation to BLE arises from the restricted rules for RU usage in the current standard, which if relaxed could also enable WiFi backscattering in the future. We build a PCB-based prototype of xSHIFT's tag, whose form factor is the same size as an RFID Gen 2 tag (shown in Fig. 12). Our real-world evaluations highlight that xSHIFT can enable FS-backscatter at promising throughput efficiencies of 6 Kbps/μJ with battery-less tags at distances of 2m from the WiFi device. We also discuss xSHIFT's potential in physical analytics applications as well as its limitations and plans for future extensions. The contributions of this work are as follows.

(1) We highlight a significant limitation of existing approaches to FS backscatter that result in very low throughput efficiencies, when deployed in battery-less tags.

(2) We present a novel approach to FS backscatter with commodity devices, xSHIFT that moves the core FS functionality away from the tag and onto the commodity device, resulting in truly passive tag designs.

(3) We prototype a truly passive FS backscatter tag and characterize its real-world performance.

Potential applications for xSHIFT: xSHIFT opens the door to a host of applications in physical analytics, including but not limited to,

Inventory and asset management: xSHIFT's tags can be attached to everyday products in the kitchen to aid in inventory tracking. An Amazon Echo, Google Home, etc. device sitting on the kitchen counter, serves as the WiFi transceiver illuminating the tags. An app (integrated with Amazon Alexa, Google Home, etc.) running on the user's phone is responsible for automatically reading and tracking products in the kitchen shelves, pantry, etc. as and when the user moves around the kitchen, without his/her explicit intervention. Beyond convenience to the user, such product consumption information is highly valuable for retailers in optimizing and enhancing the omni-channel shopping experience for their users. An analogous application can be envisioned for asset management in warehouses, where retailers can leverage their existing WiFi infrastructure to track assets as workers move around the warehouse with phones.

Product localization: Another interesting application, is tracking the location of often-misplaced objects in homes and enterprises. Whenever a user moves in close proximity (1-2m) of the tagged object, he/she can be notified of the object's presence through an app on the phone.

2 LIMITATIONS OF OSCILLATOR DRIVEN FREQUENCY SHIFTING

2.1 FS for Commodity Backscatter

Backscatter is the process of reflecting and modulating impinging wireless signals using simple, often inexpensive and passive tags. RFIDs are a popular example of this process, where a RFID reader is responsible for both sending the interrogation signal to the tags,

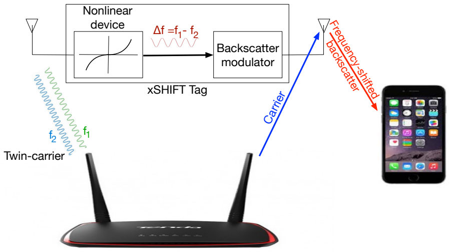


Figure 2: xSHIFT backscatter system.

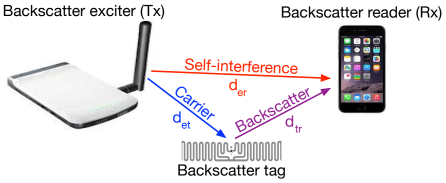


Figure 3: Commodity backscatter setup.

as well as receiving the tag's backscattered response in the same frequency/channel. RFID readers are full-duplex in nature and employ self-interference cancellation to resolve the backscatter signal that is often buried within the exciting (main carrier) signal.

Commodity backscatter [20, 21, 46, 47] aims to eliminate the need for a dedicated reader by bringing backscatter to commodity devices such as WiFi and BLE. However, since these devices are inherently half-duplex in nature, their inability to address self-interference significantly limits their backscattering capability to just a few cms. Hence, the key innovation of commodity backscatter has been to enable "frequency-shifting" of the backscattered signal, such that it can be received by a separate device on a channel different from that used by the transmitting device (Figure 3), thereby eliminating the impact of self-interference.

While different approaches have been taken to generate a standard signal ($X(t)$ being WiFi or BLE) from the tag that can be decoded by a commodity radio, the approach to frequency-shifting the backscatter signal from the main carrier, has been the same in principle.

This is accomplished with a modification to the tag hardware by incorporating a local oscillator in the backscatter modulator, as shown in figure 1. The output of the local oscillator, $S(t)$, is typically a square wave with frequency Δf which can be re-written as a series of cosine waves that are the odd harmonics (first, third, fifth, ...) of the cosine wave with frequency Δf and amplitudes in accordance with the Fourier series coefficients of a square wave. Mathematically speaking,

$$S(t) = \sum_{n=1,3,5,...} \frac{4}{n\pi} \cos(2\pi n \Delta f t)$$

If the main carrier signal is a data signal $X(t)$ modulated on top of an RF tone with frequency f_0, i.e. $C(t) = X(t)\, cos(2\pi f_0 t)$ (more precisely, $C(t) = I(t)\, cos(2\pi f_0 t) + Q(t)\, sin(2\pi f_0 t)$; but we only consider the cosine term for brevity), then the resulting backscatter signal, $B(t)$, which is the product of $C(t)$ and $S(t)$ with some modulation factor m can be written as,

$$\begin{aligned} B(t) = m \times S(t) \times C(t) &= \sum_{n=1,3,5,...} \frac{4m}{n\pi} X(t)\, \cos(2\pi f_0 t)\, \cos(2\pi n \Delta f t) \\ &= \sum_{n=1,3,5,...} \frac{2m}{n\pi} X(t) \left[\cos(2\pi(f_0 + n\Delta f)t) + \cos(2\pi(f_0 - n\Delta f)t)\right] \end{aligned}$$

The receiver can tune to the channel with frequency $f_0 + \Delta f$ while it is de-tuned for the rest of the frequencies, as displayed in figure 1. As a result, the receiver can successfully obtain $X(t)$, which is a standard signal after demodulation.

2.2 Missing Piece in Energy Efficiency

Most of the works in commodity and ambient backscatter systems have proposed oscillators (in simulation or implementation) that consume only tens of μWs, while generating the required frequency shifts with adequately low amounts of frequency/phase error. For example, in [46], [47], [21], and [20] the frequency synthesizer consumes 20.8μW, 5.6μW, 4μW, and 9.69μW, and the amounts of frequency shift being 20MHz, 1&11MHz, 11MHz, and 30MHz, respectively.

2.2.1 Steady-state vs. transient phase. However, these above numbers only capture the steady-state operation mode of the oscillator, i.e. when the oscillator has successfully initialized and produces the output with frequency Δf and very low amount of phase/frequency error. However, every oscillator circuit in reality needs to pass a start-up/transient phase after waking up from sleep mode before it can generate the desired output. This transient phase is indeed required for the electronic circuit to iteratively correct the amplitude and frequency of the output, e.g. with a phase-locked loop (PLL) mechanism, until the error in the output converges to zero, which is called the steady-state mode.

From an energy perspective, the oscillator circuit draws a certain amount of current from the power supply during this transient phase. Our study on the existing state-of-the-art low power oscillator designs shows that for the frequencies of our interest (i.e. several hundreds of kHz up to several MHz), the total amount of energy consumed by the oscillator during the transient phase ranges from 7.5μJ to 210μJ [4, 25, 32], which is substantial. The lower range points to a very novel design based on MEMS technology, SiT1576, released in early 2018[32]. A few recent works (e.g. [15, 18]) have shown ultra low-power oscillator designs (at a few MHz frequency) that achieve a low transient time and transient energy of tens of nJ. However, these come at the expense of relying on a precisely-timed signal that needs to be injected to the oscillator circuit, and does not account for the generation of such a precise signal. Thus, while a spectrum of oscillator designs exist that operate at varying levels of transient energy costs, the ones that can be leveraged for low-cost, battery-less tag designs, have a large transient energy footprint.

2.2.2 Battery-assisted tag vs. battery-free tag. Whether or not this amount of energy drained by the oscillator during the transient phase can cause a problem, depends on whether the tag is battery-assisted or battery-free.

If the tag is battery-assisted, the oscillator can remain in the steady-state mode for a significantly long time. For instance, if the tag is equipped with a small coin-cell battery with 25mAh capacity (e.g. CR1216[14]), then the SiT1576 oscillator can stay On

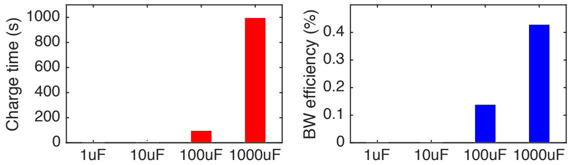


Figure 4: Osc.-based tag charge time and BW efficiency.

in steady state mode for more than three months. This means that the transient mode is not triggered often and its effect would be negligible.

Battery-free tags, in contrast, are dependent on a very limited energy budget (from an energy-storage capacitor) which cannot keep the oscillator in steady mode for long. For example, even a 1000μF capacitor which is considered as huge and takes significantly long to fully charge, can run the SiT1576 oscillator for only five seconds! This means that the oscillator must go On and Off and every time it wants to turn On it should pass the transient phase which drains a big part of the energy stored during Off time.

The performance of the tag would be heavily degraded as depicted in figure 4. The plots correspond to when the RF power arriving at the tag antenna is -10dBm (we will explain the rationale behind the choice -10dBm in the design). It is observed that for small capacitor sizes the charging is fast. However, since the stored energy is not sufficient to accomplish the oscillator transient phase, it would never enter the operational mode and thus the bandwidth efficiency is absolutely zero.

On the other hand, bigger capacitors can allow the oscillator to pass the transient mode and enter the operational mode; however, they take a very long time (several hundreds of seconds) to charge the capacitor, most of which is spent on loading the capacitor, resulting in a practically non-usable bandwidth (<1%) and throughput (<2 bps/μJ, Section 7.1.1) efficiency.

Thus, the design paradigm of using an internal oscillator for frequency-shifting faces a significant limitation of energy harvesting in battery-less tags. Hence, a structural change that removes the dependence on oscillators for frequency shifting, can be highly beneficial in enabling commodity backscatter with battery-less tags.

3 KEY IDEAS AND CHALLENGES

To this end, we propose a novel paradigm for frequency-shifting (FS) the backscatter signal from the main carrier. The key idea is to trigger the generation of the explicit-FS signal *externally* to the tag. This is accomplished by projecting an RF signal with a specially-constructed format towards the tag, so that the latter can generate the *desired* delta signal with frequency Δf without relying on a local oscillator, thereby eliminating the associated energy limitations. We name our system xSHIFT to capture the notion of external generation/trigger of the FS signal.

3.1 xSHIFT backscatter

Figure 2 captures how xSHIFT works at a high level. The exciter device (depicted as a router in the figure) is responsible for generating two signals: one that is the summation of two sine waves with frequencies f_1 and f_2 – we call this signal **twin-carrier** ($Y(t)$); and another that is the main carrier signal at f_0 ($X(t)$). The tag converts the twin-carrier signal to the desired delta signal using a simple, passive non-linear device, and employs the resulting delta signal for FS-backscattering of the carrier signal sent by the same exciter device. The receiver (pictured as a cellphone) listens to the frequency-shifted backscatter signal from the tag at $f_0 + \Delta f$. The simple mathematical construct behind xSHIFT's operation is: if two RF tone carriers with frequencies f_1, f_2 are simultaneously passed through a nonlinear device, they will end up beating (a non-linear function $\mathscr{F}$) with each other, resulting in,

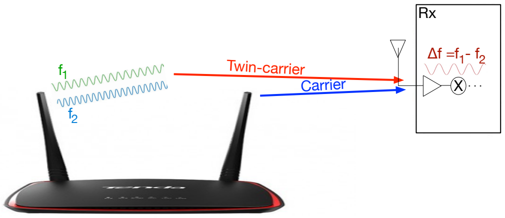


Figure 5: Internal interference in the receiver.

$$\mathscr{F}[\cos(2\pi f_1) + \cos(2\pi f_2)] = \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} \alpha_{mn} \cos(2\pi(mf_1 + nf_2)),$$

where the coefficients α_{mn} are specified by the function $\mathscr{F}$. Hence, if we can filter out all the unwanted terms in (3.1) and retain only the one with frequency $f_1 - f_2$, we would have successfully generated the desired delta signal. Hereafter, we refer to the described input and output signals as *twin-carrier* and *delta* signals, respectively. We refer to this design as *passive* in that no signal is actively generated within the tag, and whose hardware components merely translate externally generated signals to a usable form with minimal energy requirements that can be afforded by a battery-free tag. This is in contrast to the oscillator-based FS designs that need to internally generate the delta signal within the tag, thereby requiring a significant amount of energy. Thus, while oscillator designs may continue to improve in their energy footprint [15], xSHIFT's primitive provides a valuable alternative (without requiring oscillators) and an addition to the toolkit of practitioners employing FS-backscatter designs.

Remarks: Past works [17, 41] have also leveraged the interaction of two signals with a non-linear device on the tag, albeit to directly backscatter the signal at a harmonic frequency (i.e. implicit-FS). In contrast, xSHIFT leverages this notion of signal mixing to *explicitly* generate the *delta* signal (explicit-FS), which has the fundamental advantage of better energy transfer (hence operational range) for backscattering (see Section 8). More importantly, xSHIFT's goal is to realize this construct with commodity devices, a significant hurdle that has not been addressed before.

3.2 Practical Challenges

While a simple, elegant idea at the outset, realizing it with commodity devices faces several technical challenges.

Challenge 1 - Efficient RF-to-delta conversion: If we employ only passive elements for delta generation, this can result in a significantly poor performance, as it might not be able to produce a sufficiently powerful delta signal even with a fairly high-powered

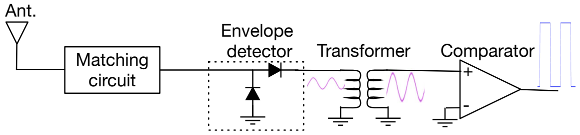


Figure 6: Block diagram of xSHIFT's delta generator.

twin-carrier signal. We verify this fact in our experiments. On the other hand, the use of active components may suffer from un-affordable power consumption or transient mode energy drain issues similar to those faced by the oscillator-based designs.

Challenge 2 - Twin-carrier embedding with commodity radios: The twin-carrier signal, being the most important trigger signal in xSHIFT, needs to be generated cleanly with a commodity transmitter. Specifically, we need to embed the twin-carrier within a standard packet without any corruption, which is quite challenging given the rigid packet structure (e.g. fixed pilot signal placement in WiFi).

Challenge 3 - Internal interference induced by the twin-carrier signal: While triggering the FS process external to the tag has its benefits, an un-desirable side-effect is that it also penetrates into the receiver circuit. Due to the non-linear elements in the receiver, another delta signal ($\Delta f'$) is generated inside the receiver, as shown in figure 5. This delta signal mixes with the carrier signal at f_0 and shifts it to the backscatter target channel $f_0 + \Delta f$, since the frequency of this delta signal is exactly the same as that generated within the tag (i.e. $\Delta f' = \Delta f$). This results in self-interference even after frequency shifting the backscatter signal.

4 DESIGN OF XSHIFT

There are two main components to xSHIFT's design: (1) process of embedding the twin-carrier ($Y(t)$) and data carrier ($X(t)$) signals into the commodity radio transmitter; and (2) design of the tag itself that (a) leverages the twin-carrier signal to generate a desired delta signal of sufficient amplitude, and (b) manipulates the delta signal to backscatter the data carrier onto a channel that does not incur interference from the twin-carrier signal at the commodity receiver. For ease of exposition, we explain the tag-specific components first, followed by the embedding process.

4.1 Tag Design

Figure 6 shows the block diagram of our proposed tag design for creating the desired delta signal from a twin-carrier signal input.

4.1.1 Delta Signal Generation. **Matching circuit:** We employ a matching circuit first to increase the tag's receive sensitivity; i.e. its ability to efficiently receive signal or harvest energy at lower power. Our matching circuit consists of a series inductor followed by a shunt capacitor tuned for 2410 MHz (frequency of signal illuminating the tag). This allows us to boost its sensitivity from -5.3 dBm to -9.7 dBm, a 4.4 dB improvement, which is significant. The tuning values for the inductor and capacitor are 2.2 nH and 1.8 pF respectively.

Non-linear device: The key step in the delta generation process is conversion of the twin-carrier signal to a sine wave with frequency Δf. Figure 7 shows the amplitude of the delta signal across different power levels ranging from -9.7dBm (the sensitivity of the energy harvester as we show in the evaluation, below which the tag is unable to operate) to 3.6dBm (very close to the signal source antenna) for 4 different choices used to convert the twin-carrier to a sine wave. These choices are created using two simple passive, non-linear devices, namely mixer and Schottky envelope detector: (1) passive mixer (Mini-Circuits ZX05-43-S+[27]), (2) passive mixer followed by a 1:5 impedance transformer (Mini-Circuits TT25-1-X65[26]), (3) Schottky envelope detector (SkyWorks SMSA7630-061[33]), and (4) Schottky envelope detector followed by a 1:5 impedance transformer. The results of figure 7 are shown for Δf = 1.1MHz (one carrier at 2.4120GHz and another one at 2.4131GHz); this value is determined by the device embedding the twin-carrier, namely a WiFi router in our case (§4.2). It is clear that the fourth design option (i.e. Schottky envelope detector followed by a 1:5 impedance transformer) has a strictly better performance than the other three, and is hence adopted in our design. This arises from the envelope detector having a much better performance than the mixer – while the use of the impedance transformer magnifies the amplitude by a factor of 5, the mixer is designed to perform well, when one of the two input signals (LO) is at least as strong as several dBm.

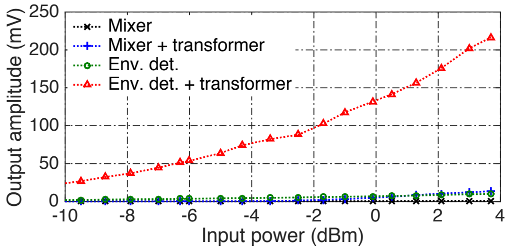


Figure 7: Performance of various delta gen. designs.

The transformer after the Schottky envelope detector, which is a band-pass element around frequency Δf, not only helps magnify the amplitude of the produced sine wave, but also rules out the unwanted terms produced by the envelope detector - the most important one being the persistent DC (zero-frequency) component that would otherwise simply overwhelm the signal components in the subsequent stages.

Magnifier: The resulting sine wave might still not be strong enough (several mV amplitude at most) to directly drive the backscatter RF switch. Thus, we convert it to a full-swing square wave with frequency Δf by means of a micro-power comparator. The micro-power comparator (Texas Instrument TLV7011[38]) is the only active component of our proposed delta generator circuit. It consumes only 16.7μW during sine-to-square conversion at 1.1MHz (the choice of this frequency is explained later). One might wonder if the use of this active component jeopardizes our vision for a passive design. We note that unlike the oscillators, this comparator does not drain energy for initialization; as long as its supply voltage is available, it is ready to operate. Hence, we are still able to build a functional battery-less tag.

4.1.2 Delta Signal Manipulation. As mentioned earlier in 3.2, the twin-carrier signal induces another delta signal with frequency

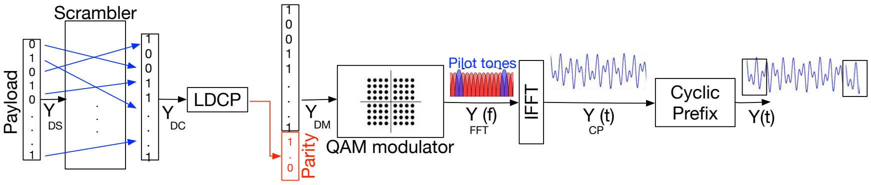


Figure 8: Payload-to-waveform pipeline in a 802.11ax WiFi transmitter.

exactly equal to Δf at the receiver. This delta signal in turn produces an interfering signal at a frequency that is Δf away from the frequency of the carrier signal. To bypass this frequency-shifted interference signal, xSHIFT halves the frequency of the delta signal generated inside the tag, i.e. generates a square wave with a frequency equal to $\frac{\Delta f}{2}$). This is accomplished using a low-power D-type flip-flop as shown in Fig. 10. The D-input of the flip-flop is connected to its inverted Q-output ($\bar{\text{Q}}$) and the square wave output of the delta generator is made to serve as its clock. This results in dividing the frequency of the clock by two.

Dividing the frequency by two creates backscatter signals at $\frac{\Delta f}{2}$, $\frac{3\Delta f}{2}$, $\frac{5\Delta f}{2}$, ... (referred to as fractional frequency shifts) away from the carrier signal, thereby allowing the receiver to bypass the internal interference by tuning into any of these channels. For a strong received signal, the preference is to tune the receiver to $\frac{\Delta f}{2}$ away from the carrier signal. However, as we explain in section 4.2, $\frac{\Delta f}{2}$ is only 0.55MHz away from the carrier signal and thus the backscatter signal would be highly masked by the carrier signal from the commodity transmitter. For this reason, xSHIFT opts to tune the receiver to the third harmonic of the backscatter, which is $\frac{3}{2}\Delta f$ away from the carrier signal (1.65MHz in our design, which is sufficiently far from the carrier signal) even though the third harmonic is about 10dB weaker than the first harmonic.

4.2 Twin-carrier Embedding

4.2.1 Leveraging WiFi's Evolution to OFDMA. To illuminate the tag with the twin-carrier signal, xSHIFT creates a signal within the payload of a standard WiFi packet that resembles a twin-carrier signal. WiFi standards in use today (802.11b/g/n/ac) are based on OFDM and employ *more than two* pilot tones in each channel (e.g. 4 pilot tones in a 20MHz 802.11ac channel). Given these pilots cannot be suppressed, this significantly restricts our capability in generating a clean twin carrier signal. However, xSHIFT is able to leverage the latest opportunity presented by WiFi's evolution to OFDMA (orthogonal frequency division multiple access), namely 802.11ax (whose first commercial router release in March 2019) for high-efficiency (HE) WLANs [5]. 802.11ax's OFDMA allows multiple users to share a single channel concurrently by dedicating different portions of the entire channel, called resource units (RUs), to them. The smallest size RU, which is a 26-tone 2.2MHz sized RU, only has two pilot tones spaced about 1.1MHz from each other. So, if we can somehow shut down the rest (24) of the sub-carriers, i.e. the data sub-carriers, then the resulting signal can be made to look like a twin-carrier.

802.11ax ground rules: Note that *the two pilot tones always exist at the 7-th and the 21-st sub-carriers of every 26-tone resource unit.* This implies two things: first, we need to enforce low power symbols on all the sub-carriers other than the pilots (i.e. the data sub-carriers) so that the outcome can resemble a twin-carrier (represented by the two pilot tones). If we denote the target signal (twin-carrier) by $Y(t)$, then

$$Y(t) = \alpha[\cos(2\pi f_1 t) + \cos(2\pi f_2 t)],$$

where f_1 and f_2 correspond to the locations of the two pilot tones within the resource unit of interest. Second, $\Delta f = f_1 - f_2$ is not in our control and is specified by the frequency difference between the pilot tones, which is fixed at (21-7) × 78.125kHz = 1.09375MHz (78.125kHz is the bandwidth of every single subchannel in 802.11ax); this specifies the value of Δf, for which the delta generator part of the tag hardware should be designed and optimized.

4.2.2 Reverse-engineering 802.11ax. We now describe how xSHIFT reverse-engineers 802.11ax's pipeline to determine the appropriate payload bits that will generate the desired twin carrier waveform $Y(t)$.

Cyclic prefix inverse: The first step is to reverse engineer the cyclic prefix block, i.e. obtaining $Y_{CP}(t)$ (256 element vector) from $Y(t)$ (272-element vector of IQ samples), as shown in figure 8. The function of the cyclic prefix module is to provide robustness against multipath by taking the first 16 samples (depending on the configuration it can also be set to 32 or 64) of $Y_{CP}(t)$ and appending to its end.

We observe that the 8-th resource unit in channel 1 (2.402GHz-2.422GHz) is robust against the addition of cyclic-prefix. In other words, if $Y_{CP}(t) = \alpha[\cos(2\pi f_1 t) + \cos(2\pi f_2 t)]$, then $Y(t) \approx \alpha[\cos(2\pi f_1 t) + \cos(2\pi f_2 t)]$ as well. The reason is that the values (periods) of f_1 and f_2 in the 8-th RU are in harmony with the number of samples before and after the addition of cyclic prefix, so as to not introduce any significant discontinuity to $Y_{CP}(t)$. Hence, xSHIFT selects the 8-th RU for the twin carrier signal transmission and $Y_{CP}(t) = \alpha[\cos(2\pi f_1 t)\ +\ \cos(2\pi f_2 t)]$.

FFT: Next, we try to obtain Y_{FFT}, the input of the IFFT block in figure 8. Note that $Y_{CP}(t) = \text{IFFT}\{Y_{FFT}(f)\}$, i.e. the IFFT block generates a 256-element time-domain I/Q vector $Y_{CP}(t)$ from a 26-element FFT-vector $Y_{FFT}(f)$ corresponding to the 8-th RU (24 for data sub-carriers and 2 for pilot sub-carriers) by assuming other sub-carriers to be null. Since FFT and IFFT are inverse mathematical functions, we can calculate $Y_{FFT}(f)$ by taking the FFT of $Y_{CP}(t)$ as,

$$Y_{FFT}(f_m) = \sum_{n=1}^{256} Y_{CP}(n)\, e^{-j2\pi f_m n},$$

where f_m is the frequency of a sub-carrier in the 8-th RU.

QAM-1024 constellation de-map: Every data sub-carrier in 802.11ax is assigned a QAM constellation point. To reverse engineer Y_{DM} that results in the desired $Y_{FFT}(f)$, we should select the constellation points with the lowest energy for the data-subcarriers, while the two pilot tones toggle between +1+0j and -1+0j per OFDM symbol according to the pattern specified in 802.11ax standard. We choose QAM-1024, the heaviest modulation scheme in 802.11ax, to maximize the power ratio between the pilot tones, which take points with maximum energy (i.e. either +1+0j or -1+0j values), and the data sub-carriers, which take points with least energy, i.e. closest to the Origin=0+0j. In QAM-1024, the latter points are $C_1 = 0.03829 + 0.03829j$, $C_2 = 0.03829 - 0.03829j$, $C_3 = -0.03829 - 0.03829j$, and $C_4 = -0.03829 + 0.03829j$. Thus, every 10-bit chunk of Y_{DM} translates to a word from the $\{C_1, C_2, C_3, C_4\}$ alphabet.

LDPC decode: Next, we need to reverse engineer Y_{DC}, the bit-vector at the input of the LDPC encoder that generates a Y_{DM} with the aforementioned property. The LDPC encoder keeps the original chunk of input bits and attaches parity bits to them. The LDPC matrix of 802.11ax[22] has a code rate of $\frac{5}{6}$; it takes 12000 bits of data and attaches a 2400-bit chunk of parity bits (the red set of bits in figure 8) Y_{DC} is related to Y_{DM} by:

$$Y_{DM} = Y_{DC}.H,$$

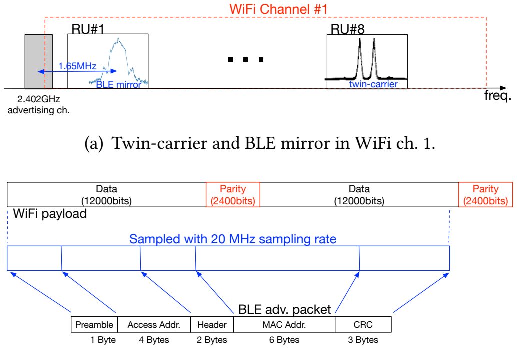
where $H_{12000\times 14400}$ is the binary encoding matrix of 802.11ax LDPC. However, directly finding the inverse of H is not straight-forward. Our strategy for resolving this issue is to first note that the desired Y_{DM} is not unique and it has the required property as long as each element of Y_{DM} belongs to the alphabet $\{C_1, C_2, C_3, C_4\}$.

Reverse-engineering LDPC can now be seen as the problem of finding a Y_{DC}, whose every element belongs to $\{C_1, C_2, C_3, C_4\}$ that produces a Y_{DM}, whose every element also belongs to $\{C_1, C_2, C_3, C_4\}$. xSHIFT conducts a randomized search in the space of all possible Y_{DC} vectors. However, after less than just 1000 (specifically 861) trials, an acceptable set of 12000 bits was found. Further, this is a one-time effort.

De-scramble: Finally, we perform de-scrambling, i.e. the inverse of the scrambling at the beginning of the pipeline to find Y_{DS}. This is straight-forward given that the Scrambler in 802.11ax is a linear-feedback shift register (LFSR), with the initial state of the LFSR being an integer number from 1 to 127 for each packet.

4.3 Main Carrier (BLE) Embedding

4.3.1 Placing the Main Carrier Signal. Recalling our discussion on internal interference from Section 3.2, with the space between the tone carriers in 802.11ax being approximately 1.1MHz, the backscatter signal needs to be shifted 1.65MHz (= $\frac{3}{2}\times$ 1.1MHz) from the carrier signal. However, there are no two standard WiFi channels that are 1.65MHz away from each other, preventing us from backscattering a WiFi packet. On the other hand, if we set the backscatter reader to be a Bluetooth low energy (BLE) receiver standing at the 2.402GHz advertising channel, we can embed a signal resembling the waveform of a BLE advertising packet within the first resource unit that is 1.65MHz shifted from the advertising channel, as shown in figure 9(a). We refer to this signal as *BLE mirror*, $M_{BLE}(t)$. Note that as shown in [20], the backscatter modulator can be modified slightly to produce a single side-band backscatter signal, i.e. there is no signal at the right side of the BLE mirror signal. Hence, there would be no interference from the backscatter signal to the other WiFi resource units.



(a) Twin-carrier and BLE mirror in WiFi ch. 1.

(b) Embedding BLE in 802.11ax payload.

Figure 9: 802.11ax embedding

We first generate the baseband waveform of the BLE advertising packet by passing its bits through a 1Mbps Gaussian Frequency Shift Keying (GFSK) modulator, as specified by Bluetooth Low Energy PHY layer[1]. Then, we shift the frequency of the generated baseband signal so as to center it at 2.40365GHz (=2.402GHz + 1.65MHz). This gives us $M_{BLE}(t)$, which is then sampled at the sampling rate of the 20MHz WiFi channel to obtain $X(t)$. This now forms the data signal, whose corresponding payload bits will be reverse-engineered (similar to §4.2) for placement in RU 1.

4.3.2 Reverse-engineering the BLE Signal. The key challenge compared to twin-carrier embedding is that a whole BLE packet (not just two tones) needs to be embedded. At the WiFi sampling rate, the BLE signal now spans 25,600 bits, resulting in its partial overlap with the parity bits of the WiFi packet (even for the largest WiFi payload). With the parity bits being a function of the preceding data, these cannot be flexibly manipulated, causing the CRC check to fail, and hence the backscattered BLE packet to be discarded at the BLE receiver.

Towards addressing this challenge, we note that only the first 1120 samples of $M_{BLE}(t)$ (i.e. first 7 bytes) of the BLE advertising packet ({preamble|access address|header}) are specified by the standard, and need to be perfectly reconstructed. For the rest of the samples, only the CRC checksum of the ultimate backscattered BLE advertising packet needs to pass at the BLE Rx. Hence, we take the first 1120 samples of $X(t)$ as $X_1(t)$ and perform the exact same reverse engineering of §4.2 on $X_1(t)$. The resulting reconstructed signal, $X_1'(t)$ now contains additional samples corresponding to the parity bits introduced in the pipeline.

After passing $X_1'(t)$ through the GFSK de-modulator, we get back the first seven bytes of the BLE advertising packet followed by the first part of the BLE MAC address. We take this part of the MAC address (less than 2 bytes) that is generated by the parity bits of the WiFi packet (i.e. cannot be changed), and add to it the rest of the MAC address bits, which can be arbitrarily chosen. Then, we add 24 bits of the CRC, pass it through the GFSK modulator and sample it with the WiFi channel's sampling rate to obtain $X_2(t)$. Finally, we reverse engineer the payload bits corresponding to $X_2(t)$ as $X_2'(t)$

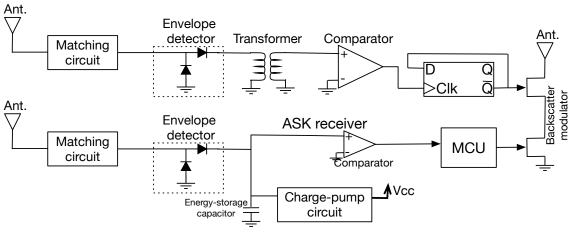


Figure 10: Block diagram of tag hardware.

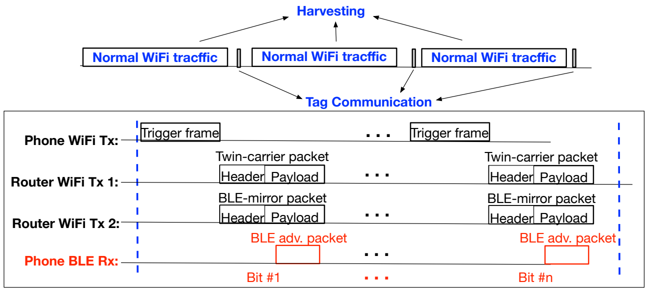


Figure 11: Timing diagram of xSHIFT's operation.

in the exact same procedure as in §4.2. The overall reconstructed signal would be $X'(t) = [X'_1(t), X'_2(t)]$. Note that, we can generate BLE advertising packets with various MAC addresses by choosing appropriate values for the MAC address in $X_2(t)$.

4.4 Tag hardware

Aside from the delta generator, which forms the novel aspect of our design, the tag requires other hardware primitives for operation (figure 10) that we now describe.

Backscatter modulator: This consists of two cascaded RF switches between the backscatter antenna and the ground. The upside switch is fed by the output of the frequency divider for frequency shifting, while the downside switch is fed by the MCU for modulating bits of data on top of the FS-backscattered signal.

ASK receiver: This is used for receiving downlink (reader-to-tag) messages. It uses a Schottky envelope detector followed by a very low power comparator to create the receiver.

RF energy harvester: The same Schottky envelope detector used by the ASK receiver is also used to charge a 2μF energy-storage capacitor that triggers the input of a charge-pump circuit. The input voltage threshold of the charge-pump circuit is 0.3v, which means that every time the energy-storage capacitor is full, there is CV^2 = 2μF × (0.3V)^2 = 0.18μJ energy available for the tag hardware to consume.

5 DEPLOYMENT SETUP

We now describe how xSHIFT is deployed and operated in a practical environment. The deployment consists of a WiFi router with two 802.11ax compatible WiFi cards[1] (serving as interrogator), a phone that is equipped with a 802.11ax chip as well as a BLE chip (serving as receiver), and one or more xSHIFT tags, which can be attached to objects and products. This is easily foreseeable – our smartphones already support 802.11ac and will soon upgrade to 802.11ax, while smart routers/hubs and voice-activated devices come standard with multiple radios already.

Operation Sequence: The timing diagram of the operation is shown in Fig. 11. The WiFi router serves its traffic as a conventional AP most of the time. When the application on the phone is ready to read its neighborhood tags on its BLE interface, it sets its 802.11ax chip in the virtual AP mode, and its BLE chip in the scan mode on 2402MHz advertising channel (channel-37). In addition, it coordinates with the router to operate its two WiFi cards as client nodes. Then, the virtual AP run by the phone allocates the 26-tone resource units 8 and 1 in channel 1 to the two client cards responsible for generating the twin-carrier and BLE mirror signals, respectively. This is accomplished by allowing the client nodes (i.e. WiFi router) to operate in the uplink **trigger** mode. While the conventional WiFi traffic is not served by the router during the scanning of the tags, this happens only when the phone's scanning application is activated by the user. Further, even when active, a less than 2-3% of channel occupancy by the scanning application (i.e. 20-30 ms per second), is sufficient to read tens of tags in the neighborhood of the phone, given the 1 Mbps data rate offered by BLE. Once triggered, the scanning operation consists of two phases: harvesting and communication, where the harvesting phase happens asynchronously (non-concurrent) from the communication.

Harvesting: Either of the WiFi cards can be used to transmit WiFi packets back-to-back so that the tag(s) in the vicinity can harvest RF energy through its antenna. However, given that harvesting can be asynchronous and agnostic to data payloads, bulk of the tag's energy can be harvested during the router's operation in its conventional AP mode. xSHIFT uses a 2μF capacitor as the energy-storage capacitor. Based on our evaluation results, 2500 back-to-back packets are sufficient for the tag to harvest up to a distance of 2 meters.

Communication: First, the phone sends a trigger frame to the two client WiFi cards, which then begin their packet transmissions (embedded twin-carrier and BLE mirror signals) immediately. This leverages the OFDMA MAC approach (instead of conventional random access) introduced in 802.11ax, where the trigger mode is used by the AP to handle the very tight synchronization required between the concurrent client transmissions in the uplink (for further details, see [22]). Each WiFi card concurrently sends its structured packet with one payload containing twin carrier and the other containing the BLE mirror signal. Communication cycle occurs multiple times and during each cycle the tag can decide whether or not to frequency shift and backscatter the BLE mirror, depending on whether it wants to send a zero or one, which is then captured by the phone. This approach, wherein a single bit is modulated on top of a BLE packet is called packet-level decoding [46]. Note that the WiFi interface on the phone triggers the other two WiFi interfaces on the router before the scanning starts. Hence, it will not be operating in tandem with the BLE receiver on the phone, and hence will not generate any interference to the latter.

[1] WiFi routers with multiple WiFi interfaces/radios are common today with the growing popularity of WiFi mesh networks [2].

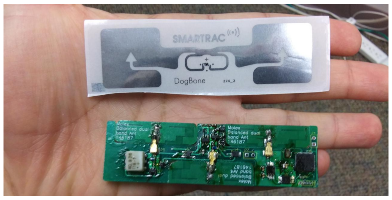


Figure 12: xSHIFT prototype vs. commercial RFID tag.

6 IMPLEMENTATION

We now present the pending implementation details of our xSHIFT backscatter system.

Tag prototype: Figure 12 shows a prototype of the xSHIFT tag fabricated that has the same form-factor as a commercial RFID tag. It consists of three WM16990-ND 2.4GHz PCB antennas[28], one each for backscattering, delta generation, and harvesting/ASK reception. For backscatter modulation, we have used Analog Devices ADG902 RF switches[6]. The components used in the delta generator are the ones mentioned in §4.1. Also, we use the ultra low power SN74LVC1G80 D-type flip flop[37] for halving Δf.

The MCU that controls the Tx/Rx baseband is a MSP430FR5969 low power MCU[36] which is used also in other low power tag prototypes such as Intel WISP5.0[3]. Note that the MCU uses its internal RC oscillator to produce a 32kHz clock for its operation. While the amount of energy for MCU wake-up in this clock frequency is less than 200nJ, we plan to replace it with a simple, ultra low-power logic circuit, whose clock is fed from the output of the delta generator circuit. The harvesting unit uses the S-882Z24-M5T1G charge-pump IC[31] to generate a regulated 2.4v DC output out of DC inputs of greater than 0.3V after the 2μF energy-storage capacitor becomes full – i.e. its voltage reaches 2.4V. Finally, the ASK receiver and the energy harvester share the same Schottky envelope detector that is also used in the delta generator (§4.1). The output of the envelope detector goes through a low power TLV7031 comparator[39] in the ASK de-modulator.

802.11ax router: Since we did not have access to commercial 802.11ax WiFi cards when developing our system (first commercial 802.11ax product released in Jan 2019), we implemented the key tasks of 802.11ax router using a USRP X300[16] as the radio front-end and MATLAB 2018a WLAN toolbox as the bit-to-waveform generator. Note that MATLAB provides the necessary TX/RX toolchains for 802.11ax, most particularly, the standardized PHY layer features (e.g. OFDMA) – this allows us to verify xSHIFT's design in practice with an actual 802.11ax stack.

BLE receiver: For verifying the integrity of the BLE advertisement packet generated by our MATLAB+USRP based 802.11ax router, we use an iPhone BLE Scanner app. Also, for evaluating more fine-grained metrics like RSSI, bit-error-rate, and throughput, we employ the CC2650[40] evaluation board, along with the PER TEST firmware.

7 EVALUATION

7.1 Tag hardware benchmarks

7.1.1 Efficiency. To understand the impact of individual components, we compare xSHIFT with state-of-the-art oscillator-based designs (MEMS oscillator [32]) along three metrics: power consumption (μW; w/o oscillator transient phase), energy efficiency (bits/μJ; w/ transient phase), and throughput efficiency (bps/μJ; w/ RF harvesting and transient phases).

Component	Prototype	IC
Backscatter modulator	3.4μW	1.3μW
Baseband Tx & Rx	18.2 & 11.3μW	1.4 & 1.1μW
Delta gen + freq. divider	26.5μW	2.9μW
ASK receiver	1.3μW	0.8μW
Transmitter (total)	**48.1μW**	**6.8μW**
Receiver (total)	**12.6μW**	**1.9μW**

Table 1: Power consumption of tag components.

Bits per message	xSHIFT	xSHIFT IC	osc.-based
10	162.4bits/μJ	1148.2bits/μJ	1.4bits/μJ
100	162.4bits/μJ	1148.2bits/μJ	14.1bits/μJ

Table 2: xSHIFT vs. osc. design (bits/μJ)

Power consumption: Table 1 lists the power consumption of the various primitives in the tag hardware. In transmit (Tx) mode, the delta generator consumes 16.7μW, largely owing to the comparator (TLV7011). Including that of the frequency divider, i.e. 9.8μW, the overall consumption for xSHIFT's tag is 26.5μW. This is only slightly worse than a few of the existing designs in the range of 4μW–9.69μW. The oscillator design in tables 1, 2, 3 has the same hardware as xSHIFT's prototype tag, except that the delta generation circuit (figure 6) is replaced by a MEMS oscillator [32].

However, note that our design does not suffer from the energy-hungry transient phase incurred by the oscillator designs that is not captured in these numbers. Besides, the 4μW–9.69μW numbers are obtained through simulation results with a 90nm and smaller integrated-circuit technologies that are optimized for their particular purpose. In contrast, our design employs concrete general-purpose components without any assumed optimizations on them. The rest of the Tx mode entities that are common to most designs (e.g. backscatter modulator, MCU), contribute to 21.6μW. This results in a total of 48.1μW power consumption during transmission for xSHIFT. In addition, the envelope detector-based ASK receiver consumes 1.3μW at 10kbps bit rate. Further, we simulated our design in HSPICE [34] with 180nm technology and the resulting power analysis shows that the Tx and Rx power consumption can be reduced to 6.8μW and 1.9μW, respectively.

Energy efficiency: If we denote n as the number of message bits transmitted by the tag during every active cycle, T_b as the amount of time the tag needs to modulate a single bit, and P_t as the overall power consumed by the tag during backscatter modulation, then the amount of energy required by the tag in sending the message would be $E = [n{\times}T_b{\times}P_t]$ for xSHIFT tag, while it would be $E = [E_{\text{transient}} + n{\times}T_b{\times}P_t]$ for the MEMS osc-based tag. Here, $E_{\text{transient}}$ is the amount of energy drained by the oscillator during wake up, which is eliminated by xSHIFT. In xSHIFT's packet-level decoding scheme, a single bit is conveyed (independent of message size) during the length of a BLE advertising packet, $T_b = 128\mu s$. Further, P_t is 48.1μW, 6.8μW and 38.7μW for the xSHIFT prototype, xSHIFT IC, and and osc.-based tags, respectively; while $E_{\text{transient}}$ is 7.2μJ for SiT1576 MEMS oscillator[32]. Now, Table 2 shows xSHIFT's prototype and IC energy efficiency is two to three orders magnitude

Bits per message	xSHIFT	xSHIFT IC	osc.-based
10	[60,600]bps/μJ	[424.2,4242]bps/μJ	[0.02,0.2]bps/μJ
100	[600,6000]bps/μJ	[4242,42420]bps/μJ	[0.2,2]bps/μJ

Table 3: xSHIFT vs. osc.design [min,max] (bps/μJ).

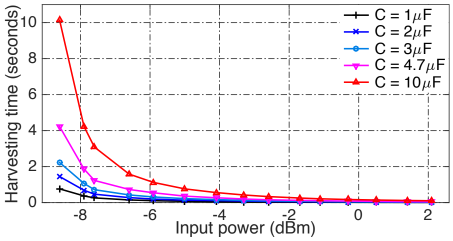


Figure 13: Charge time vs. RF power vs. capacitor size.

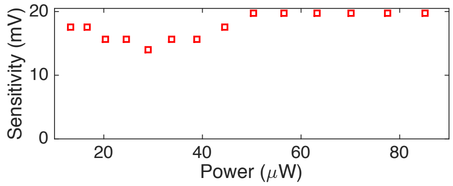


Figure 14: sensitivity vs. power drop of TLV7011.

better than osc-based designs, which we expect to further increase when xSHIFT is able to support bit-level decoding.

Throughput efficiency: Finally, we are interested in understanding how fast we can transmit for a given amount of energy. This is obtained by dividing the energy efficiency of sending n bits with the corresponding time taken, which includes both the transmission as well as harvesting duration. For a harvesting range of 2m, xSHIFT's prototype tag employs a 2μF capacitor that can be charged within 0.4-2s, and xSHIFT's IC will require a 330nF capacitor that can be charged within 0.06-0.28s for sending the same message. In contrast, oscillator-based designs require a much larger capacitor (100-1000μF) to start-up the oscillator, thereby incurring a harvesting time spanning several hundreds of seconds. This harvesting bottleneck results in non-functional throughput efficiencies of osc-based designs in Table 3, which are three to four orders of magnitude lower compared to xSHIFT prototype tag and IC.

7.1.2 Micro Benchmarks. **RF energy harvester:** While xSHIFT's matching circuit plays a critical role in boosting the tag's harvesting sensitivity by 4.4 dB (Section 4.4, the size of its energy-storage capacitor (varied between {1, 2, 3, 4.7, 5.7, 6.9, 9.4}μF) has little to no effect. In contrast, it does have an effect on the harvesting time. Figure 13 plots the harvesting time (in seconds) versus the RF input power level (in dBm–values chosen are above sensitivity with impedance matching, i.e. -9.7dBm) for different energy-storage capacitor sizes. xSHIFT's choice of 2μF takes less than 2 seconds to fully charge in the worst case, which suffices for sending the full tag message. Larger capacitors are unnecessary and increase the worst-case harvesting times to several seconds.

Delta generator: Fig. 14 captures the sensitivity of xSHIFT's low-power comparator TLV7011 as a function of input power. It has the best sensitivity (minimum input amplitude for operation) of 15mV, to deliver which, xSHIFT's choice of Schottky envelope detector with transformer (delivers a minimum output of 27 mV, Fig. 14) is essential – other choices for the non-linear device are unable to drive the comparator. Further, given that increasing the supply voltage does not appreciably impact the comparator's sensitivity, xSHIFT operates it at the lowest voltage (power) possible.

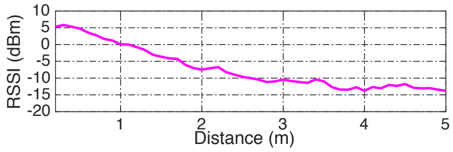


Figure 15: RSS vs. distance in line-of-sight.

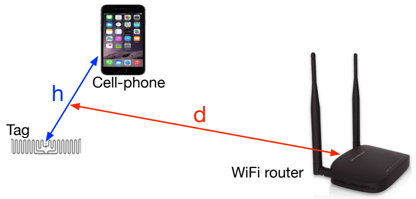


Figure 16: xSHIFT experimental setup.

7.2 Validating xSHIFT's Design Choices

Operational Range: First, we neeed to understand how the sensitivity values for harvesting and delta generation map to physical operational distances. Figure 15 shows the received signal strength versus distance between tag and the router antenna in a line-of-sight scenario, when the router is equipped with an omni-directional antenna transmitting at max. power of 30 dBm.

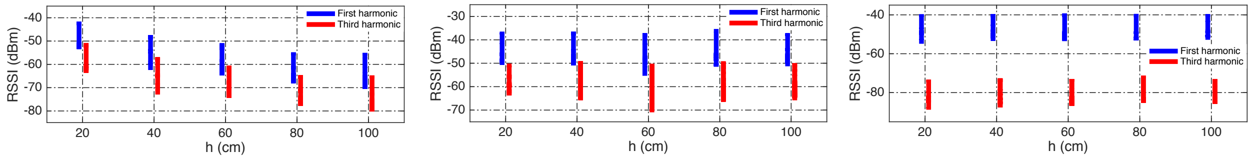
From figure 15, the -9.7dBm harvesting sensitivity translates to ≈2.4m harvesting range. xSHIFT is able to generate its delta signal from a farther 3.6m. However, with the harvesting range being the bottleneck, we consider 2.4m as the practical, **combined harvesting/delta generation range** for xSHIFT's tag.

Impact of interference: To characterize the backscatter channel, we measure the signal strength of the desired backscatter signal along with that of two un-desired interfering signals: the internal interference generated by the delta signal within the receiver on its Rx channel, and the inter-channel interference between the transmit carrier signal and the backscatter signal.

Figure 16 shows our experimental setup for measuring the received strength of these three signals. The router cards are d m away from the middle of the line between the tag and the cellphone, which in turn are spaced apart by h m. Figure 17 presents the measurements. For every value of h, the blue(red)-colored bar shows the RSS of the first (third) harmonic of each signal, measured at various d values ranging from 0.2m to 2.4m in steps of 0.1m.

Figure 17 validates two key design choices in xSHIFT for handling interference. First, comparing figures 17(a) and 17(b), the RSS of the internal interference significantly overwhelms that of the backscatter signal irrespective of the values of h and d and the strength of the harmonic. This justifies xSHIFT's decision for leveraging fractional (and not integral) harmonics of Δf.

Second, comparing figures 17(a) and 17(c), the first harmonic of the backscatter is highly interfered by the BLE mirror signal due to their proximity (0.55 MHz), while the third harmonic of the backscatter signal is well above the interference level from the mirror signal. Hence, xSHIFT's choice for using the third harmonic



(a) Backscatter (b) Internal interference (c) Mirror interference

Figure 17: RSS of the backscatter and interfering signals at different values of *h* and *d*.

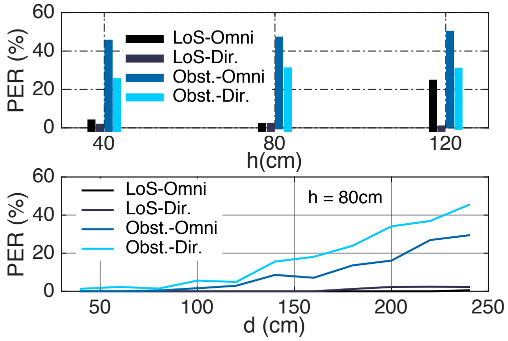


Figure 18: PER of various static configurations.

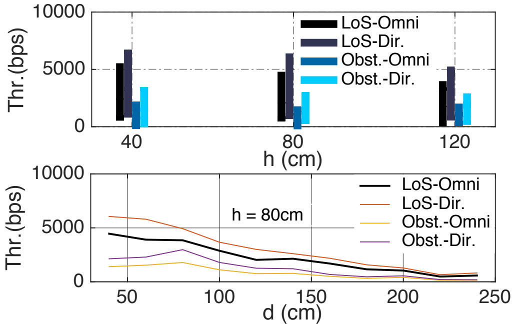


Figure 19: Throughput of static configurations.

of the backscatter signal, which is sufficiently shifted ($\frac{3}{2}\Delta f = 1.65$ MHz) from the mirror signal, is indeed appropriate.

7.3 Macro-level Benchmarks

We study xSHIFT's performance in both static and mobile scenarios using two popular macro-level metrics, namely bit error rate (corresponds to packet error rate, PER with packet-level decoding) and throughput.

7.3.1 Static Scenarios. The measurement setup for static experiments is exactly as shown in figure16. We repeat the same experiment with four different configurations, varying the nature of antenna (omni vs. directional 6 gBi gain) at the router as well as channel between router and tag-cellphone (line-of-sight vs. non-LOS) : (1) omni-antenna router with LOS channel; (2) directional-antenna router with LOS channel; (3) omni-antenna router with NLOS channel (a copper sheet obstacle between the router and tag-cellphone channel); (4) directional-antenna router with NLOS channel.

Packet error rate: The results in figure 18 show that in the LoS scenario, the PER is small except when the omni-directional antenna is more than 2 meters away from the tag-cellphone pair, which in turn are 1.2m away from each other. In addition, the PER is low for NLOS scenarios as well for short distances (upto 0.5m for omni-directional and upto 1m for directional antenna), while farther distances are a challenge in NLOS.

Throughput: We examine xSHIFT's throughput from its packet-level decoding system, where BLE advertisement packets are sent every 128μs. Our throughput measurements also account for the time taken for the tag to harvest energy as well as its bit error rate. The results in figure 19 show that in LOS, the throughput is >2Kbps and can be as high as 6Kbps at short distances, but reduces to hundreds of bps at farther distances. Also in the NLOS cases with the obstacle, the throughput is able to scale to 3Kbps for shorter distances.

While there is room for a lot of improvement in range and throughput (e.g. with bit-level decoding), we believe xSHIFT's real-world performance shows promise and viability for its external approach to frequency-shifting with battery-less tags.

7.3.2 Mobile Scenarios. The set-up for the mobility experiment is captured in Figure 20. Five spots are chosen within a 2m×3m room with a WiFi router located at the middle of one of the 3 meter wide walls. At each spot, we place the tag steady and the cellphone starts to move around the tag in a circle with radius *R* at a constant speed. For every spot and radius ranging from 0.2m to 1m in steps of 0.2m, we capture one minute of data and calculate the bit error rate and throughput. Figures 21 and 22 show the CDF of PER and throughput for each spot, respectively. The results highlight the ability of our xSHIFT tags to function in practical environments, where *mobile* consumers can leverage their cellphones as receivers for reading them.

8 RELATED WORK

Commodity backscatter: One of the early works, BackFi[8], relied on just RSS changes to detect the backscatter signal in the same channel, leading to degraded performance and robustness. Subsequent works started leveraging oscillator-driven frequency-shifting. In [21], the tag synthesizes an 802.11b WiFi packet in baseband, and spreads the signal in frequency domain using its barker code generator for compatibility with 802.11b decoding. In contrast, [45, 49] modulate the raw backscatter bits by toggling on the standard WiFi and Bluetooth excitation signals, to enable decoding at either symbol-level (using amplitude variants) or packet-level. Hitchhike [47] takes a different approach, where the tag XoR's its

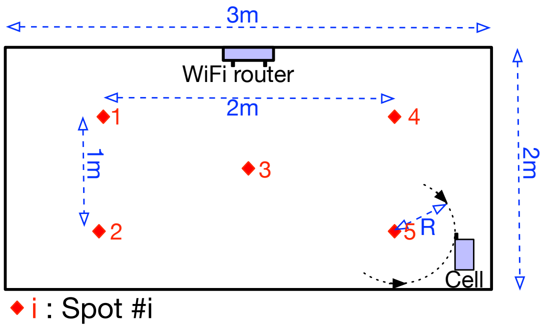


Figure 20: Mobility experiment setup.

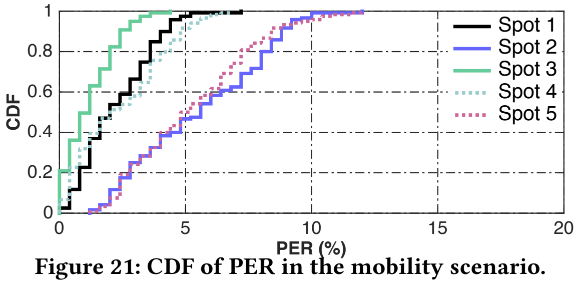


Figure 21: CDF of PER in the mobility scenario.

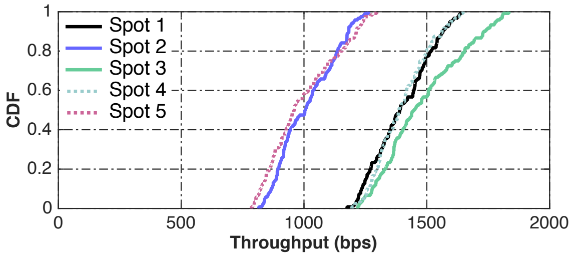


Figure 22: CDF of throughput in the mobility scenario.

bits with that of the original WiFi packet and shifts it to an adjacent channel for reception by another WiFi device. Similarly, [20] frequency-shifts and backscatters a standard Bluetooth signal to the channel of another WiFi radio. A recent work aims to significantly extend the backscattering range to hundreds of meters, albeit at the cost of very low bit rates (LoRa Backscatter[35], PLoRa[29]), by leveraging the superior sensitivity of LoRa receivers (-140dBm) and their chirp spread spectrum (CSS) modulation.

Ambient backscatter: A closely related set of works [19, 42–44], try to leverage the prevailing ambient signals in the environment such as WiFi, Cellular, TV, etc. for backscattering and inter-tag communication.

Harmonics from non-linearity: Past works [12, 13, 17, 24, 30, 41] have leveraged non-linear devices on the tag to backscatter the signal at harmonic frequencies. In particular, [17, 41] employ the mixing of two carriers to generate the harmonic backscatter signal directly at $2f_0, 3f_0$, etc., thereby alleviating reflections/interference from the environment at the main carrier frequency f_0. While such implicit-FS employs the non-linear device as the load of the antenna, xSHIFT uses the non-linear device to create the delta signal, which in turn is used in an explicit-FS architecture to produce the backscatter signal at $f_0 + \Delta f$. In addition to not being usable with commodity devices, such direct backscattering at harmonic frequencies (implicit-FS), prevents them from controlling the backscatter power, resulting in 20-30 dB degradation compared to explicit-FS (oscillator-based). xSHIFT shares this benefit of explicit-FS backscatter sans local oscillators, while working with commodity devices.

Packet emulation: Our work is also related to a few recent works [9, 11, 23, 50] that embed a packet from one standard into that of another for purposes of cross-technology communication and coexistence. While ZigBee packets are generated by reverse engineering 802.11ac WiFi packets in [23], WiFi signals are embedded into LTE frames in [9]. xSHIFT leverages the notion of such packet emulation but instruments it in the context of 802.11ax (OFDMA) for the purpose of twin carrier generation.

9 DISCUSSIONS AND LIMITATIONS

We plan to extend xSHIFT along the following dimensions,

Single WiFi interface: With the growing popularity of WiFi mesh networks, several commercial WiFi routers/APs come with at least two WiFi interfaces [2]. However, working with a single WiFi interface would increase xSHIFT's scope for adoption with existing WiFi infrastructure. We are working on executing a part of the BLE embedding, namely its base-band, within the tag, while keeping it ultra low power. This would then require a single WiFi interface for the generation of just the twin carriers, one of which can also serve as the main carrier for backscattering.

Bit-level decoding: Packet-level decoding currently limits xSHIFT's throughput to a few Kbps. By addressing the first limitation (moving to a single WiFi interface design), xSHIFT's tag will be able to synthesize arbitrary BLE packets, thereby enabling bandwidth efficient bit-level decoding, and boosting throughputs to tens of Kbps. This will automatically allow xSHIFT to scale and support the reading tens of tags in a single scanning round.

Multi-tag support: With the bit-level decoding providing the necessary data rates (max of 1 Mbps from BLE) needed for multiplexing multiple tags, we can implement a simpler version of the backoff-based random access MAC layer (employed in EPC Gen 2) to support their channel access. The tags harvest energy simultaneously from the router's normal (downlink) traffic, and respond (with tag-specific payload) based on their backoff process, when the scanning process is triggered by the phone.

Improved range: Lastly, xSHIFT's operation is currently limited (2 meters), largely due to the imperfect tuning between antenna and envelope detector. Albeit, a significant first step for external FS that enables some practical applications, we are working on tag optimizations through proper impedance matching to further boost its sensitivity for harvesting energy and delta signal generation, as well as its backscatter power.

10 CONCLUDING REMARKS

We proposed xSHIFT, a novel approach to frequency-shifting backscatter with commodity radios that eliminates the fundamental energy limitations of oscillator-designs by moving FS external to the tag. We presented the design and practical realization of xSHIFT with truly passive battery-less tags and commodity WiFi transceivers. xSHIFT opens the door to a myriad of applications in physical analytics that span both consumer and commercial spaces.

REFERENCES

[1] *Bluetooth Core Specification Version 4.2.*

[2] Wireless mesh network market 2019 global industry size, growth, segments, revenue, manufacturers and 2025 forecast research report. https://www.marketwatch.com. Accessed: 2019-05-21.

[3] S. N. P. Aaron Parks. Advanced rfid prototyping with the wisp 5.0. *http://www.github.com/wisp/wisp5.*

[4] Abracon. *POWER OPTIMIZED MEMS OSCILLATORS*, 8 2018.

[5] Aerohive Networks. *Enterprise-Grade 4x4, 4-stream, 802.11ax Access Point with Integrated Antennas*, 2018.

[6] Analog Devices. *0 Hz to 4.5 GHz, 40 dB Off Isolation at 1 GHz, 17 dBm P1dB at 1 GHz SPST Switches.* Rev. D.

[7] L. Antonio, V. Ramon, and G. David. A passive harmonic tag for humidity sensing. *http://dx.doi.org/10.1155/2014/670345*, (670345):11, 2014.

[8] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti. Backfi: High throughput wifi backscatter. *ACM SIGCOMM Computer Communication Review*, 45(4):283–296, 2015.

[9] E. Chai, K. Sundaresan, M. A. Khojastepour, and S. Rangarajan. Lte in unlicensed spectrum: Are we there yet? In *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, pages 135–148, New York, NY, USA, 2016. ACM.

[10] X. Chen, Y. Chen, H. Zhang, N. Yan, J. Wang, H. Min, and L. Zheng. Long read range class-3 uhf rfid system based on harmonic backscattering. *Electronics Letters*, 54(22):1262–1264, 2018.

[11] Y. Chen, Z. Li, and T. He. Twinbee: Reliable physical-layer cross-technology communication with symbol-level coding. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pages 153–161, April 2018.

[12] B. G. Colpitts and G. Boiteau. Harmonic radar transceiver design: miniature tags for insect tracking. *IEEE Transactions on Antennas and Propagation*, 52(11):2825–2832, Nov 2004.

[13] H. Cravo Gomes and N. Borges CARVALHO. Rfid for location proposes based on the intermodulation distortion. *Sens. Transducers Mag.*, 106:85–96, 07 2009.

[14] ENERGIZER. *Lithium Coin, 3.0 Volts, 25 mAh battery.*

[15] H. Esmaeelzadeh and S. Pamarti. A quick startup technique for high- q oscillators using precisely timed energy injection. *IEEE Journal of Solid-State Circuits*, 53(3):692–702, March 2018.

[16] Ettus Research. *USRP X300: High performance, Scalable, Software Designed Radio (SDR).*

[17] H. C. Gomes and N. B. Carvalho. The use of intermodulation distortion for the design of passive rfid. In *2007 European Radar Conference*, pages 377–380, Oct 2007.

[18] D. Griffith, J. Murdock, and P. T. RÃÿine. 5.9 a 24mhz crystal oscillator with robust fast start-up using dithered injection. In *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 104–105, Jan 2016.

[19] Q. Huang, Y. Mei, W. Wang, and Q. Zhang. Battery-free sensing platform for wearable devices: The synergy between two feet. In *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9, April 2016.

[20] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*, pages 356–369. ACM, 2016.

[21] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith. Passive wi-fi: Bringing low power to wi-fi transmissions. In *NSDI*, volume 16, pages 151–164, 2016.

[22] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi. A tutorial on ieee 802.11ax high efficiency wlans. *IEEE Communications Surveys Tutorials*, pages 1–1, 2018.

[23] Z. Li and T. He. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, MobiCom '17, pages 2–14, New York, NY, USA, 2017. ACM.

[24] Y. Ma, X. Hui, and E. C. Kan. 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*, MobiCom '16, pages 216–229, New York, NY, USA, 2016. ACM.

[25] Microchip Technology Inc. *Ultra-Small, Ultra-Low Power MEMS Oscillator with Spread Spectrum*, 9 2017. Rev. A.

[26] Mini-Circuits. *50Ω 0.02 to 30 MHz RF Transformer.*

[27] Mini-Circuits. *Coaxial wide-band, Level 7, 750 to 4200 MHz frequency mixer.*

[28] Molex. *RF ANT 2.4/5.5GHZ PCB TRACE MMCX.*

[29] Y. Peng, L. Shangguan, Y. Hu, Y. Qian, X. Lin, X. Chen, D. Fang, and K. Jamieson. 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*, SIGCOMM '18, pages 147–160, New York, NY, USA, 2018. ACM.

[30] K. Rasilainen, J. Ilvonen, A. Lehtovuori, J. Hannula, and V. Viikari. On design and evaluation of harmonic transponders. *IEEE Transactions on Antennas and Propagation*, 63(1):15–23, Jan 2015.

[31] Seiko Instruments Inc. *ULTRA-LOW VOLTAGE OPERATION CHARGE PUMP IC.* Rev.2.0-00.

[32] SiTime. *1.2mm^2 μPower, Low-Jitter, 1Hz – 2.5 MHz Super-TCXO*, 2018. Rev. 1.3.

[33] SkyWorks. *Surface Mount, 0201 Zero Bias Silicon Schottky Detector Diode.*

[34] Synopsys. *HSPICE: The Gold Standard for Accurate Circuit Simulation.*

[35] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *arXiv preprint arXiv:1705.05953*, 2017.

[36] Texas Instruments. *MSP430FR596x, MSP430FR594x Mixed-Signal Microcontrollers.*

[37] Texas Instruments. *Single Positive-Edge-Triggered D-Type Flip-Flop.* Rev. S.

[38] Texas Instruments. *Small-Size, Micro-Power, Low-Voltage Comparators.* Rev.C.

[39] Texas Instruments. *Small Size, nanoPower, Low-Voltage Comparators.* Rev.B.

[40] Texas Instruments. *SimpleLink^{TM} Multistandard Wireless MCU*, 7 2016.

[41] D. Vasisht, G. Zhang, O. Abari, H.-M. Lu, J. Flanz, and D. Katabi. In-body backscatter communication and localization. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, pages 132–146, New York, NY, USA, 2018. ACM.

[42] V. T. S. G. D. W. J. R. S. Vincent Liu, Aaron Parks. Ambient backscatter: Wireless communication out of thin air. *SIGCOMM Comput. Commun. Rev.*, 2013.

[43] A. Wang, V. Iyer, V. Talla, J. R. Smith, and S. Gollakota. Fm backscatter: Enabling connected cities and smart fabrics. In *NSDI*, pages 243–258, 2017.

[44] G. Yang and Y. Liang. Backscatter communications over ambient ofdm signals: Transceiver design and performance analysis. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, Dec 2016.

[45] P. ZHANG, D. Bharadia, K. Joshi, and S. Katti. Enabling backscatter communication among commodity wifi radios. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, pages 611–612, New York, NY, USA, 2016. ACM.

[46] P. Zhang, D. Bharadia, K. Joshi, and S. Katti. Enabling backscatter communication among commodity wifi radios. In *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*, pages 611–612. ACM, 2016.

[47] P. Zhang, D. Bharadia, K. R. Joshi, and S. Katti. Hitchhike: Practical backscatter using commodity wifi. In *SenSys*, pages 259–271, 2016.

[48] P. Zhang, C. Josephson, D. Bharadia, and S. Katti. Freerider: Backscatter communication using commodity radios. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '17, 2017.

[49] P. ZHANG, M. Rostami, P. Hu, and D. Ganesan. Enabling practical backscatter communication for on-body sensors. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, pages 370–383, New York, NY, USA, 2016. ACM.

[50] X. Zheng, Y. He, and X. Guo. Stripcomm: Interference-resilient cross-technology communication in coexisting environments. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pages 171–179, April 2018.