October 2021

SCALING DOWN THE ENERGY COST OF CONNECTING EVERYDAY OBJECTS TO THE INTERNET

Mohammad Rostami
University of Massachusetts Amherst

SCALING DOWN THE ENERGY COST OF CONNECTING EVERYDAY OBJECTS TO THE INTERNET

A Dissertation Presented

by

MOHAMMAD ROSTAMI

Submitted to the Graduate School of the
University of Massachusetts Amherst in fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

September 2021

College of Information and Computer Sciences

SCALING DOWN THE ENERGY COST OF CONNECTING EVERYDAY OBJECTS TO THE INTERNET

A Dissertation Presented

by

MOHAMMAD ROSTAMI

Approved as to style and content by:

_____

Deepak Ganesan, Chair

_____

Ivan Lee, Member

_____

Jie Xiong, Member

_____

Jeremy Gummeson, Member

_____

Karthik Sundaresan, Member

_____

James Allan, Department Head

College of Information and Computer Sciences

ABSTRACT

SCALING DOWN THE ENERGY COST OF CONNECTING EVERYDAY OBJECTS TO THE INTERNET

SEPTEMBER 2021

MOHAMMAD ROSTAMI

B.Sc., SHARIF UNIVERSITY OF TECHNOLOGY

M.Sc., UNIVERSITY OF MASSACHUSETTS AMHERST

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Deepak Ganesan

The Internet of Things (IoT) promises new opportunities for better monitoring and control of thousands of objects and sensors in households and industrial applications. The viability of large-scale IoT is, however, still a challenge given that the most widely known options for connecting everyday objects, i.e. duty-cycled active radios such as WiFi, Bluetooth and Zigbee, are power-hungry and increase the cost of deployment and maintenance of the connected devices.

The main argument of this thesis is that passive radios that use backscatter communication, which has been used primarily for RFIDs, can fill this gap as an ultra-low power

replacement for active radios to enable truly large-scale IoT deployments. However, passive radios offer insufficient performance today in terms of bandwidth and range that makes them unattractive for integration in IoT applications.

The main contributions of this thesis are: (1) xShift, enabling battery-free backscatter tags that can directly communicate with commodity radios without any additional infrastructure. (2) MIXIQ, a new ultra low power receiver design that leverages the available devices nearby for converting a simple envelope detector to a high-range, high-throughput receiver. (3) Polymorphic Radio (Morpho), a novel approach for ultra low power radio design based on combining active and passive radios, in order to enable robust and pervasive streaming and cloud offloading. The proposed contributions have all been successfully prototyped using off-the-shelf components and show promising performance.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

Chapter 1

Introduction

The Internet of Things (IoT) has emerged as an exciting new technology and promises to have tremendous impact due to the ability to connect every object, big or small, to the Internet. With the advent of ultra-low cost microcontrollers and ubiquitous wireless connectivity, IoT is entering a new era, *massive IoT*, which promises better real-time analytics and control using a combination of technologies such as cloud computing, artificial intelligence (AI), virtual reality (VR) and others. Qualcomm, one of the leading players in this space, predicts that IoT will grow to $3.3 trillion in market and create more than 22 million jobs by 2035 [94].

1.1 Problem Statement

While the newest generations of wireless networks (e.g. 5G) deliver excellent performance along several axes including good network quality, up to several Gbps throughput and $<$ 1ms latency , the viability of a massive IoT deployment is also determined by the efficiency of these radios. The most widely used solutions so far, i.e. commodity radios such Bluetooth, WiFi, and ZigBee remain too inefficient for providing connectivity and data transfer to everyday objects to enable massive-scale IoT deployments. Figure 1.1 shows a simple

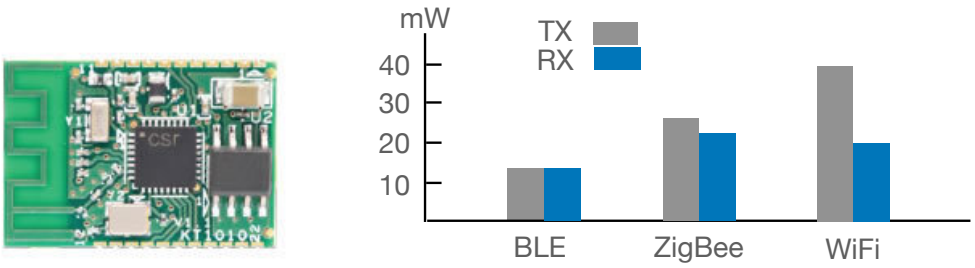


Figure 1.1: Left: A Bluetooth Low Energy (BLE) module — Right: Power consumption of commodity embedded radios.

BLE module and the power consumed by state-of-art IoT radios during transmission and reception. We see that these radios consume milliwatts of power during transmission and reception which introduces a number of serious practical challenges:

Cost of deployment: In many applications that are going to be empowered by massive IoT, numerous (tens to thousands) of sensors, items, and products need to be connected to the network. However, the cost of every single commodity radio such as Bluetooth low energy is around $10, which makes the total cost of deployment very high. This is especially true in supply chains and warehouses where it is essential to monitor and track every single item and product, not just the largest or most expensive packages but even the smallest and cheapest ones.

Pervasiveness: The other challenge is that since these radios consume mWs of power, they need a big enough battery to operate. This in turn significantly increases their form factor which makes them unsuitable for many applications. For example, some applications need to put the sensor on a very small object or surface. Additionally, for wearables and on-body sensors it becomes very tough to wear them all the time if they have a huge battery on them. On the other hand, reducing the form-factor using a tiny battery is possible only if these radios are heavily duty-cycled. That, however, reduces the average data rate to very low levels (e.g. a few Kbps) which limits their applicability to applications that need to send sporadic messages, such as temperature sensors.

Maintenance: Finally, unless these radios are heavily duty-cycled, they drain

their battery so quickly. For example, a Bluetooth Low Energy (BLE) radio that sends data at average throughput of 100Kbps (i.e. at %10 duty-cycling) will drain a medium coin cell battery (with 100mAh capacity) in less than a week. Therefore, to enable continuous connectivity for applications that need real-time tracking or sensing at high data rates, one needs to replace the batteries frequently which is both impractical and expensive.

1.1.1 Technological Energy Gap

The aforementioned problems that emerge when using commercial commodity radios such as Bluetooth and WiFi result from the fact that they use active components for data transmission and reception. These radios are referred to as *active radios* because they need to actively generate a local RF carrier signal at ultra high frequencies (e.g. 2.4GHz) with which they modulate the data signal (during transmission, before sending over the air through the antenna) or demodulate the received signal (during reception, after receiving at the antenna). To perform successful modulation/demodulation, the locally generated RF carrier signal needs to have adequately precise amplitude, phase, and frequency. Generating such a precise carrier at ultra high frequencies draws mWs of power, which can drain even a medium size coin cell (100mAh) battery so quickly (i.e. in a few hours) if they are continuously ON.

Therefore, these radios need to be heavily duty-cycled to effectively optimize their average power consumption. For example, Bluetooth Low Energy (BLE) is the heavily duty-cycled version of the classic Bluetooth protocol where the radio goes to deep sleep mode for a long time and wakes up for a very small window only to send a small sized message. Duty cycling is a very simple and mostly effective scheme but its main drawback is that the average throughput will be reduced a lot. For example, to achieve two months of battery life on a 100mAh coin cell battery, the BLE radio needs to be %0.2 duty-cycled which in turn reduces average throughput to about 2Kbps. Thus, it can only be suitable for applications where a small amount of data is transmitted infrequently (e.g. smart thermostat or smart water level sensor). In contrast, applications that need to send data more frequently or use richer and higher data-rate sensors or actuators cannot benefit from such a radio.

1.2 Key Idea: Leveraging Passive Radios for Filling the Energy Gap

In this work, we ask: *Can we replace the existing commercial embedded radios with novel RF transmitter/receiver designs that operate at much lower energy footprints without having to heavily duty-cycle them?* We show that the answer to this following question is YES if we rely on *passive* radio technology as an ultra low power alternative to active radios such as Bluetooth and WiFi to enable massive IoT deployments.

Passive radio and backscatter communication (see §2) have been known for decades and have been used in RFID tags for wireless identification. But research over the last two decades has shown that this technology has significantly broader utility beyond RFIDs – indeed, this technology can be a viable solution that can enable significantly lower power communication than today's active radios for energy-limited devices and connected objects in IoT applications.

The key enabler of broader applicability of backscatter is recent research that has shown the feasibility of *high-performance* backscatter systems that can directly communicate with existing wireless infrastructure and consumer devices by being compatible with standard radios such as WiFi [52, 17, 53]. Even though the progress of the proposed systems in this field of study, aka *backscatter computing*, has been substantial, there remains several practical challenges and performance gaps that have not been fully addressed yet. The main goal of this thesis is to demonstrate the capabilities of the *backscatter computing* as a practical ultra low power wireless solution, and propose solutions to address the most crucial open challenges and performance gaps with existing systems.

Overall, we believe that the contributions of this thesis can bring us closer to a *complete* backscatter solution that can offer a complete and significantly more energy-efficient alternative to active radios and thereby make massive IoT deployments practical.

Chapter 2

Backscatter: Background, Recent Enhancements and Open Challenges

2.1 Why passive radios?

As we discussed in Chapter 1, today's active radios such as Bluetooth and WiFi are not always a practical solution to enable pervasive connectivity for everyday objects, particularly when the radio needs to be very low cost, operate at extremely small energy budgets, and have small form factor. While CMOS technology has continuously scaled down the size and power consumption of digital logic systems, analog RF components that are necessary for wireless communication have not seen a similar trend. As a result, active radios such as WiFi and Bluetooth radios on sensors and mobile devices still consume tens to hundreds of milliwatts of power [53, 65, 60, 74].

However, there is another category of radios, called *passive radios*, that operate at much lower power regimes, i.e. μWs, which is 2–3 orders of magnitude lower than active radios such as Bluetooth and WiFi. The reason for this extremely low power requirement is that passive radios do not actively generate a local RF signal. Instead, they rely on an external RF carrier signal that is generated by another device and comes over-the-air through

the antenna.

Therefore, passive radios are very simple in their structure and have very low energy footprint since they do not contain the sophisticated and power-hungry RF elements of radios like WiFi and Bluetooth. As a result, they can be built in a very small silicon area, which makes them very low price (a few cents a piece). In addition, they require a very tiny amount of energy to transmit and receive data packets which enables them to operate without any battery attached to them. Overall, these make passive radio technology a compelling alternative to active radios in the massive IoT scenarios since it does not suffer from the drawbacks of active radios.

2.2 Traditional RFID: Dominant use of passive radios

Radio Frequency Identification (RFID) is the most prevalent technology that is based on passive radios. Traditional UHF RFID has come a long way from its first application of identifying airplanes as friend or foe in World War II [2]. Over the last few decades, tagging items with battery-free RFID tags (figure 2.1) has transformed supply chain and inventory management by enabling industries to pervasively and uniquely identify and track thousands of inventory and assets at very low deployment cost. EPCGen2, the best known standard RFID platform in the market, defines the necessary protocols for reading the identity of the tags, aka electronic product code (EPC).

Let us now take a look at how a traditional UHF RFID system works based on passive radios. As shown in figure 2.2, a traditional RFID system consists of central device called *RFID reader* that is power-hungry and usually needs to be plugged to AC power. A UHF RFID system leverages this asymmetry to enable an energy-rich RFID reader to assist EPCGen2 tags in the environment to send their EPC IDs without requiring a battery.

In order to do so, the reader device emits a strong *carrier* signal at 900MHz ISM band, which fulfills two important tasks: (1) it illuminates the tags as an excitation signal

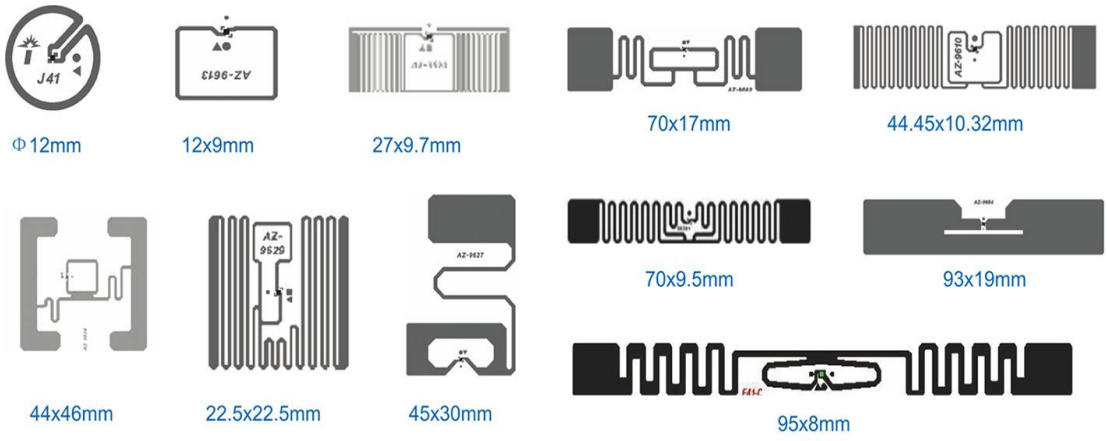


Figure 2.1: Standard UHF RFID (EPC Gen2) tags in the market.

through RF energy harvesting. (2) it provides the necessary external RF carrier for the tags to perform bit transmission to the reader (uplink) and bit reception from the reader (downlink) with passive elements at extremely μW levels (§2.1), after storing sufficient energy through energy harvesting.

2.2.1 RF Energy harvesting

One of the most compelling advantages of RFID tags is their ability to completely rely on *RF energy harvesting* as their energy source by absorbing energy from the reader's carrier signal. The benefit of using the RF carrier transmitted by the RFID reader as the tags' energy source is that as long as the reader device is working, it provides sufficient energy to power up tags within a radius of several meters. Moreover, RFID tags can use the same antenna that they use for data communication for energy harvesting as well, hence this method has no impact on their form factor.

Figure 2.3 shows the building blocks of the RF energy harvesting circuit used in the standard UHF RFID tags. A passive voltage multiplier, consisting of RF diodes converts the RF carrier signal at the antenna to DC power, which charges a sufficiently big energy storage capacitor. An impedance matching circuit consisting of inductors and capacitors is placed between the antenna and the voltage multiplier, and their values are finely tuned to

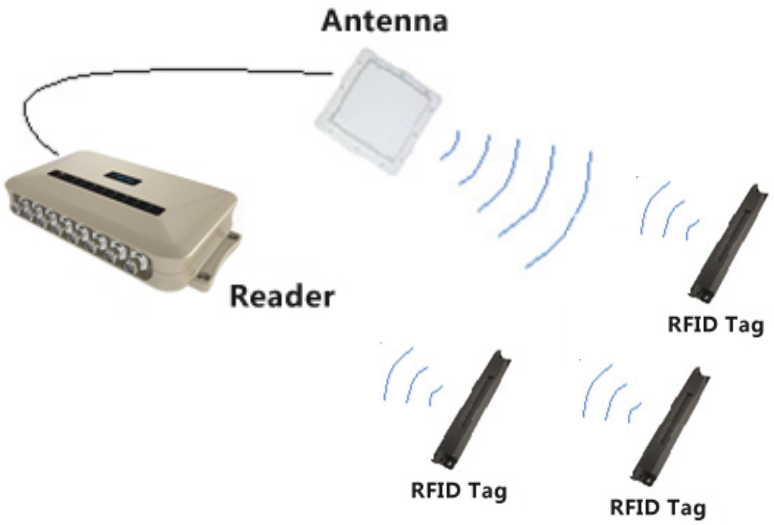


Figure 2.2: Standard UHF RFID system.

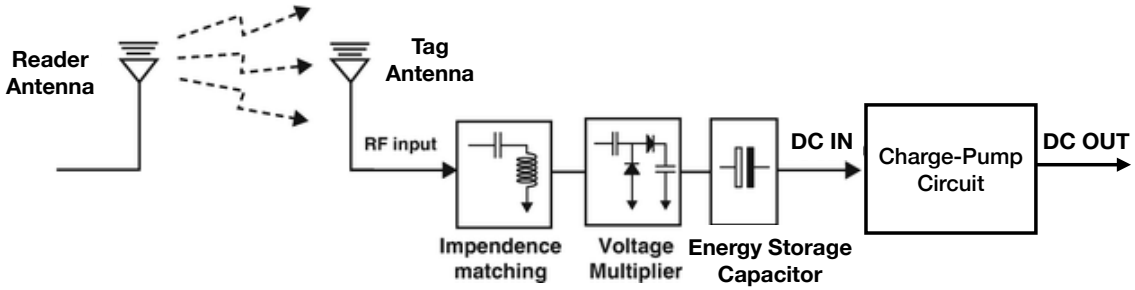


Figure 2.3: Block diagram of the RF energy harvesting circuit used in RFID tags.

maximize the DC power that is extracted from the RF carrier signal. Note that the output of the voltage multiplier also contains an RF signal term but this disappears because of low pass filtering by the energy storage capacitor. Finally, a self-startup charge-pump circuit starts to activate the tag when the voltage at the energy-storage capacitor reaches a certain voltage threshold or equivalently a certain amount of stored energy ($E \propto CV^2$).

The size of the energy capacitor is selected carefully in the design of the RFID tags. It should not be very small so that when the charge-pump circuit starts working, the amount of stored energy is sufficient for accomplishing tag's data transmission reception tasks. On the other hand, a very large capacitor increases the silicon area consumed by the RFID chip and makes the tag unnecessarily slow to respond to incoming RF energy.

2.2.2 Passive Radio-Based Uplnik/Downlink

In this section, we introduce the principles for transmission and reception of data bits through passive radios in traditional RFID systems. Since the focus of this work is to investigate possible ways for employing these primitives as a practical ultra low power radio solution, we skip over other mechanisms in the EPCGen2 protocol that are designed to orchestrate the querying of the tags and multiple access methods. We refer the readers to reference books about RFID [34] for an in-depth discussion about those mechanisms.

Backscatter-based uplink: The uplink, i.e. tag-to-reader, data bit transmission in RFID systems is based on backscatter communication (Figure 2.4). Backscattering is the process of reflecting the carrier signal with an amplitude and phase that is determined by the antenna load. The resulting signal is called the *backscatter* signal. The tag modulates its data bits on top of the backscatter signal using an ultra low power RF switch that toggles between different antenna loads, based on whether it is driven by '1' or '0' at the baseband of the tag. Therefore, the resulting backscatter signal has time-varying amplitude and phase corresponding to the tag's information bits.

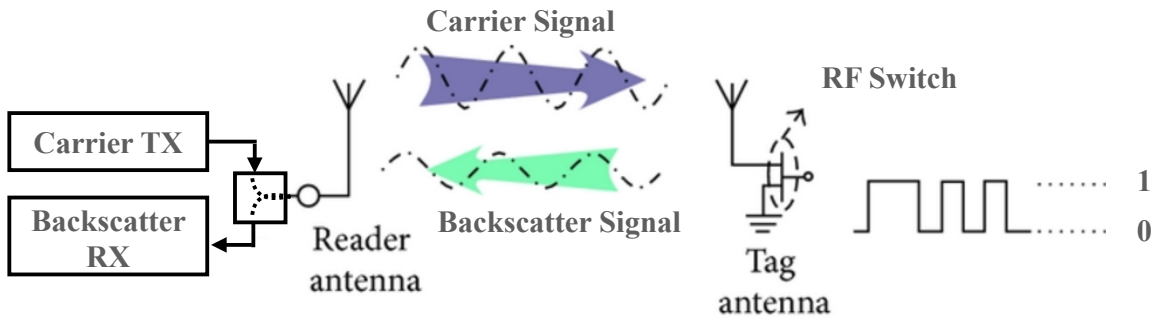


Figure 2.4: Backscatter uplink in traditional RFID systems.

The reader device uses the same antenna to receive the backscatter signal as well. This configuration, where both carrier TX and backscatter RX are located within the same device and share a single antenna, is called a *mono-static* reader deployment. Also, the reader device is a *full-duplex* radio, meaning that it transmits the carrier signal and receives the backscatter signal from the tag simultaneously.

It can be observed that the backscatter signal traverses two channels: the forward channel (h_f) from the reader antenna to the tag antenna, and the backward channel (h_b) in the opposite direction. It is also impacted by the modulation factor, M of the tag. Thus, it experiences one extra round of channel attenuation and its signal strength at the reader is much lower than the original carrier. The goal of reader is to detect the time-varying phase[1], $\theta(t)$, of this weak backscatter signal accurately in the presence of a significantly strong version of the carrier signal, called *self-interference*, that leaks from TX path to the RX path due to the shared TX/RX front-end and antenna.

This vast difference between signal strength of the backscattered and the self-interference terms can easily become more than the dynamic range of the reader's receiver chain, especially when the tag is not in the close proximity of reader's antenna. This would end up overwhelming the backscatter receiver circuit. But since the carrier signal is a single tone ($e^{j2\pi f_c t}$), *self-interference cancellation* becomes very simple. This is because the self-interference cancellation after being down-converted with the local carrier signal will translate to a DC term, which can then be cancelled using a simple analog high-pass filter.

Envelope detector-based downlink: For sending the information bits in downlink direction, i.e. from the reader to the tag, the reader turns the carrier signal On/Off. This creates an Amplitude Shift Keying (ASK) signal at the input of the antenna, figure 2.5.

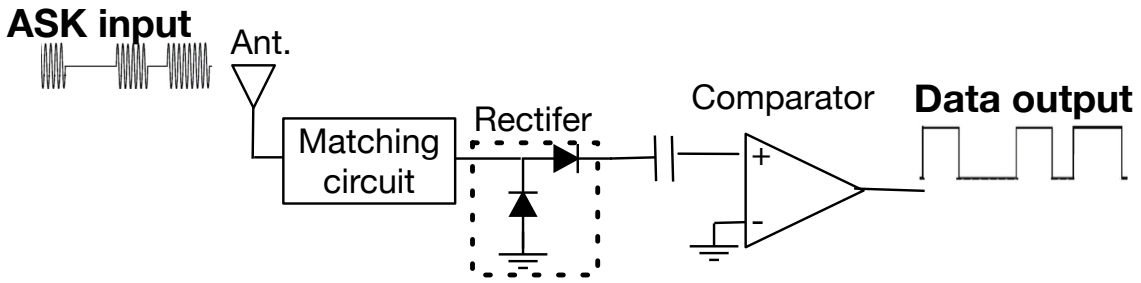


Figure 2.5: Downlink of the traditional RFID systems.

The reader then translates the '0' and '1' bits to the the amplitude pulse width. The

[1]Note that in general, in a backscatter signal both phase and amplitude can be time-varying. But in the case of EPCGen2 tags, only phase modulation is performed.

tag detects these changes in the amplitude using a passive envelope detector. The envelope detector is a circuit that converts the input RF signal to a baseband signal whose amplitude is proportional to the amplitude of the RF input signal. The output of the envelope detector is then processed by a voltage comparator to produce 'high' and 'low' which is then processed at the baseband of the tag for decoding the information bits.

2.3 Computational RFID Tags

Standard RFID tags, despite all their benefits in terms of cost, energy, and form factor, can only send a hard-coded set of bits, i.e. their EPC numbers, which limits their application to only identification purposes. On the other hand, we need to enable many other applications that want to send actual (e.g. sensor) data and evaluate the performance of passive radios in these applications. This requires access to tag hardware platforms that allow for sending arbitrary data bits besides their EPC.

To bridge this gap, computational RFID (CRFID) tag prototypes have been proposed [115]. CRFID tags augment traditional RFID tags with sensing and computational capabilities and can operate while relying on RF energy harvesting. Over the years, these have been used to enable many applications such as localization [105], image sensing [77], autonomous robotics [49], smart dust [104], human-computer interfaces (HCIs) [107], and wearables [112]. Let us now introduce one of the most successful CRFID prototypes.

WISP Tag: The WISP is a wireless identification and sensing hardware platform that supports sensing and computing. It was developed by Intel Research Seattle, and later by the Sensor Systems Laboratory at the University of Washington [3]. Like a passive RFID tag, the WISP is powered and read by a standard off-the-shelf RFID reader. It can also power up using the harvested energy from the reader's carrier signal. To an RFID reader, a WISP is just a normal EPC gen1 or gen2 tag; but inside the WISP, the harvested energy operates a 16-bit general purpose ultra low power micro-controller (MSP430). The WISP also supports a myriad of sensors (light, temperature, accelerometer, etc.) that can be read

by the micro-controller at very low energy footprints. The WISP also uses the EPCGen2 radio protocol for sending the sensor data bits to the RFID reader.

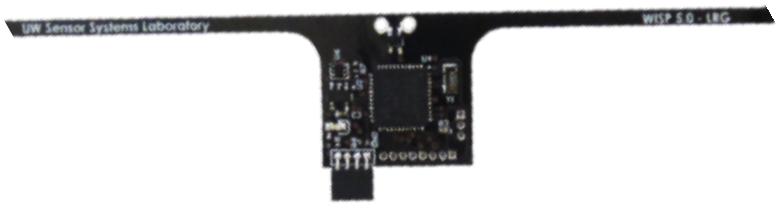


Figure 2.6: WISP PCB prototype.

2.3.1 Understanding the potentials and challenges with traditional RFID systems

Open source CRFID platforms like the WISP have enabled large body of research on passive radios and applications where they can be employed. At the highest level, these works focus on these aspects:

- Investigating the viability as well as the performance of new types of data streaming, more importantly samples from various types of sensors [77, 105], based on the capabilities of RFID backscatter communication.
- Optimizing or modifying parts of the EPCGen2 protocol e.g. MAC layer [37], as well as the firmware on the tag [147] in order to improve energy efficiency, throughput, and other performance metrics.

Platforms like the WISP have allowed the research community to understand the challenges in leveraging the EPC Gen 2 protocol and backscatter communication for IoT devices. Some of these include:

1. Very limited performance: The performance of the backscatter uplink/downlink is severely limited by the EPCGen2 standard as well as the architecture of the reader. The

tag, for instance, has to send its data at a maximum of 100kbps, which is a serious problem given that the tag can only send at a very small fraction of channel time according to the standard. In addition, the overall bandwidth available to the reader at 900MHz ISM band is 26MHz which is insufficient especially in cases where several tags in the environment want to stream richer types of data.

Additionally, the communication range and thus the coverage is very limited due to the mono-static architecture of the reader. Since the self-interference signal is not perfectly cancelled, the residual term impacts the backscatter receive sensitivity, -70 to -80 dBm whereas today's receivers can easily have as low as -100 dBm sensitivity when they are not interfered by such leakage. As a result, the communication range is limited to $<$10m even at ideal situations when the reader radiates at its maximum power and the tag is in the direct line-of-sight of the reader's antenna.

2. Need for dedicated infrastructure: RFID readers operate in a completely different band (ISM 900MHz) than other commercial wireless solutions such as WiFi. This makes their deployment very complicated especially in consumer spaces where we want them to coexist with other networks such as WiFi and send their collected information to the internet. Additionally, every single reader device is able to cover only a small area which means that full coverage of an area (e.g. whole house coverage) needs a dense deployment of readers that are in coordination with each other, thereby making the deployment excessively difficult and expensive.

2.4 Backscatter Computing

To address the shortcomings of traditional RFID systems, research on passive radios has departed from simply modifying the baseband of the RFID tags to send arbitrary packets. Instead, researchers over the last decade have been investigating new ways of backscattering that do not rely on commercial RFID systems. This new area of research, *backscatter computing*, aims to shift the way of thinking about backscatter from a single-purposes

limited radio technology to a practical, available solution for a wide range of applications in IoT, wearables, and on-body sensors.

The primary goal of backscatter computing research is to leverage the existing signals in the environment for backscattering rather than relying on the continuous tone that comes from a dedicated reader. Consequently, backscatter tags are designed in a way that their signal can be decodable by commodity infrastructure and devices such as WiFi and Bluetooth. This makes backscatter a very attractive option for consumers since ubiquitous sensing and tracking can be enabled simply by using already deployed WiFi APs and mobile phones without requiring additional reader infrastructure.

While early efforts in backscattering with ambient signals and commodity radios [133, 144, 52, 17] focused on showing the feasibility of backscatter computing, more recent efforts have focused on innovations to improve performance metrics such as throughput, range, and robustness of the backscatter links so that they can serve a broader variety of applications. Figure 2.7 shows this trend over the last decade. We see that throughput has continuously from from 1Kbps in the early efforts to 11Mbps in most recent systems; range has also increased from 0.7 meters to more than 100 meters .

This continuous improvement in practicality as well as performance has resulted from a number of architectural modifications and technical innovations in the design of backscatter systems. Here, we want to talk about a few of these innovation that have had the most impact in the field and are relevant to this thesis.

Leveraging ambient signals: Ambient RF signal from sources such as TV, FM radios, cellular communications, WiFi networks, Bluetooth nodes, and others is widely available in urban areas (day and night, indoors and outdoors) at different frequency bands. This means that many options are available for backscatter carrier generation as well as RF energy harvesting. Additionally, this makes backscatter a ubiquitous communication paradigm at many different indoor/outdoor environments. This method of designing backscatter communication links to leverage ambient carriers is referred to as *ambient backscatter*.

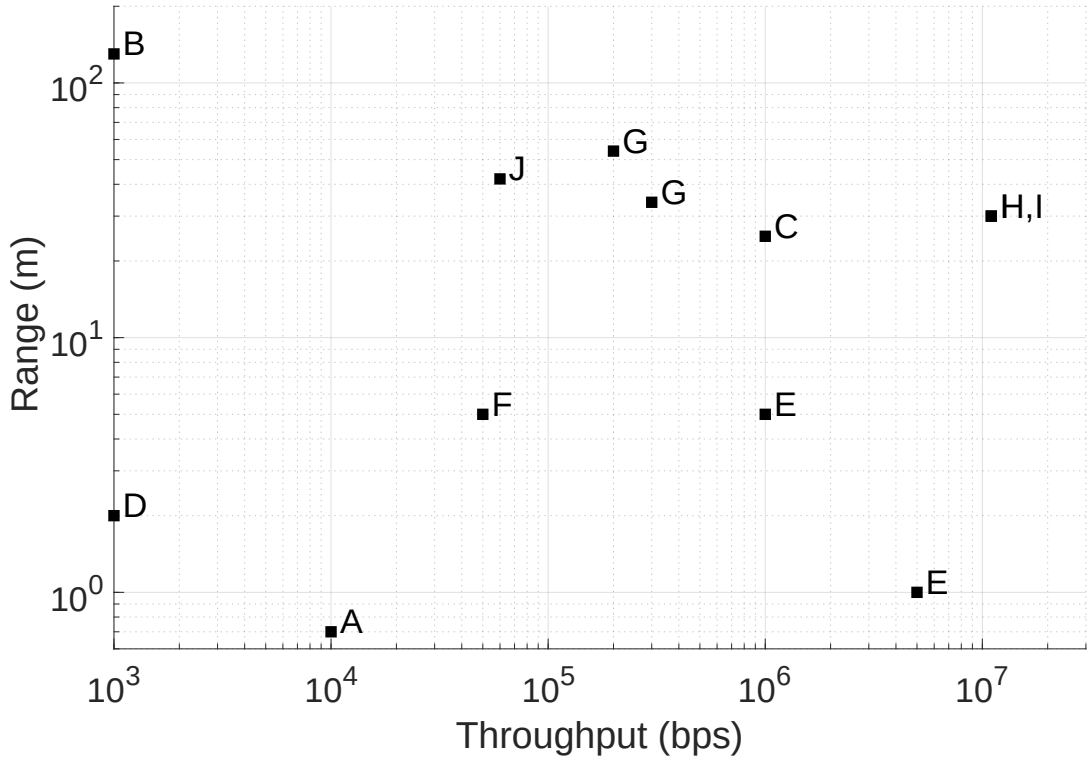


Figure 2.7: Performance of the state-of-the-art backscatter computing systems. A: [133], B: [55], C: [84], D: [52], E: [17], F: [149], G: [146], H: [53], I: [48], J: [148],

Bi-static deployment: Traditional RFID readers are called *mono-static* because both the transmitter and the receiver are integrated in the same device which is capable of sending and receiving RF signals simultaneously. Thus, RFID readers are *full-duplex* radios; in contrast, commodity radios are *half-duplex*, meaning that they can transmit and receive RF signals but not at the same time. Therefore, a *bi-static* deployment consists of one device as carrier transmitter and another one as backscatter receiver, as shown in figure 2.8.

In addition to making backscatter viable with half-duplex commodity radios, bi-static deployments improves the range significantly compared to mono-static readers. The tag uses the carriers that comes from a nearby TX device which makes the forward channel (i.e. the channel from TX device to the tag) very low loss. As a result, the backward channel (i.e. from the tag to the receiver) can tolerate more loss which means boosted communication range. All of the systems in figure 2.7 that achieve 10s – 100s meters of range ([53, 117, 86])

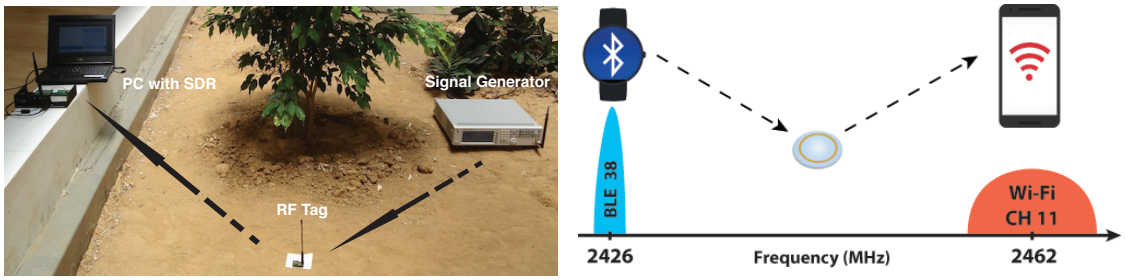


Figure 2.8: Left:An outdoor bi-static deployment setup [55]. Right: A bi-static setup consisting of commodity TX/RX [48].

are based on this idea.

Leveraging commodity radios as backscatter receiver: The first efforts for backscattering with WiFi devices [17, 52] simply use the signal within the WiFi packets as carrier signal. The tag reflects the WiFi packet with different antenna loads which results in a backscatter signal with time-varying phase. A separate standard WiFi RX captures the WiFi packet transmitted over the air and tries to decode the backscatter signal by analyzing the signal variations within the packet.

Similar to the standard RFID, the backscatter signal is in the same frequency as the original WiFi packet (aka *in-band backscatter*) and therefore is strongly interfered by it. But the key differences here are: (1) the carrier signal is no longer a single tone, and (2) the commercial WiFi receivers, unlike RFID readers, are not equipped with a self-interference cancellation circuit. The solution that these works propose is to send backscatter signal at very slow rates and use the entire channel bandwidth (20 – 40MHz) to scan the tiny signal variations. As a result, both range and throughput are very limited in these early efforts (figure 2.7).

Frequency-shifted backscatter: While a dedicated RFID transceiver is full-duplex and incorporates self-interference cancellation between the transmitted and backscaterred signals, commodity devices are inherently half-duplex. Existing works [146, 53, 48, 148, 144] 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. 3.1. 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) [62, 131]; or (ii) *explicitly*: low power oscillators on the tag directly generate the Δf signal, which drives a RF switch [53, 146, 48, 145].

Explicit-FS backscatter has been given more attention, 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 [13, 20].

Synthesizing Standard Radio Packets: The most naive approach for backscattering with commodity radios is to simply reflect the entire packet sent by TX device for sending '1' and absorb it for sending '0'. This method is called *packet-level* decoding which results in very low throughput, since every packet's presence/absence translates to one single backscatter *bit*. In contrast, in more advanced backscatter systems with commodity radios ([144, 53, 48]), the passive backscatter tag perform digital baseband operations like coding and modulation in order to synthesize a packet from scratch. This method is called *bit-level decoding*, since every bit of the backscatter packet contains information from the tag and thus the backscatter receiver should decode every single bit to capture the full backscatter data. This scheme dramatically increases the throughput compared to packet-level decoding, since instead of carrying one bit of data per packet, tens to hundreds of bits are transmitted. The systems that achieve the highest throughputs (several Mbps) in figure 2.7, all follow the bit-level decoding scheme.

2.5 Efforts at Addressing Backscatter Performance Gaps

Despite these substantial advancements in the field of backscatter computing, there are still practical issues that have not been fully addressed yet.

Robustness: Backscatter is a two-part channel (forward, and backward) which makes the backscatter signal doubly attenuated. In addition, there is always considerable signal loss that is introduced by imperfections in the tag circuit. As a result, even state-of-the-art backscatter with WiFi approaches that frequency-shift the backscatter signal to leverage WiFi receivers only achieve limited range of less than 10 meters. Greater distances of a few 10s of meters from RX device can only be achieved when there is a TX device is in the vicinity of the tag (i.e., 1–2 meters away from the tag) [53], which is not the case in many scenarios.

In addition, the range numbers are achieved only in line-of-sight scenarios where the tag is fully exposed to the TX and RX devices without any blocking object nearby as well as the tag and TX/RX devices antennas have the same orientation. In practice, many IoT applications target environments with a lot of multi-path reflections and human body effects which deteriorate the quality of the backscatter signal excessively. As a result, backscatter remains limited to very short distances in those environments.

1. Using reflection amplifiers to boost backscatter signal strength: One possible approach for boosting the backscatter robustness is to amplify the backscatter signal at the tag by adding semi-active components as the antenna load. One of these elements that has been studied in recent efforts is tunnel diode [9, 130]. When a tunnel is reverse-biased, it behaves like a negative resistance ($R < 0$), which is due to an effect known as tunneling effect in quantum physics. Thus, when a reverse-biased tunnel diode is used as the antenna load, the reflection coefficient of the antenna, $\Gamma = \frac{R-Z0}{R+Z0}$, would have a magnitude > 1 since $R < 0$. This means that the power of the backscatter signal is boosted (backscatter signal strength $\propto |\Gamma|^2$).

Boosting the backscatter signal strength in this way potentially contributes to more robustness. However, these efforts only fit well in long-range scenarios. The reason is that the aforementioned reflection gain delivered by tunnel diode based circuits is highly dependent on the input power to be very low ($< -50dBm$); which is the case in *outdoor* long-range scenarios. In most applications targeted by backscatter research, the main focus is on shorter-range *indoor* environments. In these scenarios, the input power to the tag's antenna is -20dBm to -30dBm in the worst case scenarios, a regime where tunnel diodes do not work well.

2. Leveraging Chirp spread spectrum modulation to boost receive sensitivity: Another line or work has proposed backscatter solutions that rely on the LoRa technology [117, 86]. LoRa employs *chirp spread spectrum* (CSS) modulation, which encodes data using a frequency *chirp*, which is a single tone whose frequency changes linearly over time. To modulate '0's and '1', increasing and decreasing chirps are used as the carrier over the symbol time. To demodulate the CSS signal, the receiver produces a local chirp and mixes it with incoming signal, and then performs an FFT on the output of the mixer and decides whether 0 or 1 has been sent based on the location of the peak that appears in the FFT output.

LoRa-based backscatter fits applications that require robustness and long ranges because CSS is able to achieve a very high sensitivity because of its ability to utilize an excessively large bandwidth. This allows for decoding the transmit signals below noise level . For example, SX1276 Lora chip has a receive sensitivity of -149dBm [111]. The downside is that the throughput is sacrificed a lot (<1 Kbps – a few Kbps) which makes LoRa unsuitable for many applications including streaming or many types of sensors (e.g. accelerometers) that require higher data rates.

Improving throughput by leveraging OFDM: Orthogonal frequency-division multiplexing (OFDM) is a widely used signaling technique in the different standards of WiFi (e.f. 802.11n/ac). It is capable of achieving tens of Mbps by splitting the WiFi channel into several sub-carrier and streaming bits of data in every individual sub-carrier using

high-order modulations (e.g. 256-QAM). Several works have been proposed so far that implement backscatter tags that are capable of performing OFDM modulations over the air [141, 150, 78]. Thereby, these systems achieve significantly high throughput that allows them to stream high-fidelity multimedia using backscatter. The range, however, is more limited than vanilla backscatter as the sensitivity of the receiver is sacrificed for higher throughput.

2.6 Gaps that we address in this thesis

Leveraging commodity radios: WiFi Backscatter has high potentials in terms of bandwidth and coverage; but current solutions that we discussed are incomplete yet and introduce serious challenges. Two major challenges are:

1. Huge energy overhead of backscatter frequency-shifting: Most of the work 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[144], [146], [53], and [48]. 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 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, which is needed converging to zero phase/frequency error.

From an energy perspective, the oscillator circuit draws a certain amount of current from the power supply during this transient phase. The total amount of energy consumed by the oscillator during the transient phase ranges from 7.5μJ to 210μJ [113, 4, 68], which is substantial. If the tag has a large battery, the oscillator can remain in the steady-state mode for a significantly long time. Tags with tiny batteries or battery-free tags, in contrast, 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 in battery-free tag that relies

on RF energy harvesting, can run the oscillator for only a few seconds. This means that the oscillator must go On and Off and every time it wants to turn On, it incurs the overhead of the transient phase which drains a significant part of the energy stored during the time when the oscillator is turned Off.

As a consequence, the performance of the tag is heavily degraded. When relying on small capacitors, charging is fast but since the stored energy is not sufficient to meet the needs of the oscillator transient phase, it would never enter the operational mode and thus the throughput is absolutely zero. On the other hand, bigger capacitors can allow the oscillator to get past 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 waking up the oscillator, resulting in a practically non-usable bandwidth (<1%) and throughput (<2 bps/μJ) efficiency.

2. Asymmetry between uplink/downlink performance: While the focus of the majority of work in passive wireless radios has been on backscatter communication (i.e. uplink from tag to reader), developments in backscatter communication over the last decade have shifted the communication bottleneck from uplink to downlink (infrastructure to tag).

The vast majority of passive receivers in the proposed backscatter systems with commodity radios use the same simple envelope detector as used in RFID tags, which comprise of an RF rectifier (typically an RF diode) followed by an ultra low power comparator (figure 4.1). But passive envelope detectors have poor sensitivity due to the specifications of its components that limits how well it can convert the received signal to a voltage output that triggers a comparator for decoding.

We wish to design a complete WiFi backscatter solution that addresses these limitations. In Chapter 3, we propose the design of our xShift system, a first-of-its-kind system that accomplishes backscatter to commodity devices without relying on oscillators in the tag to enable true passive operation. xShift moves the central role of frequency shifting signal generation away from the tag to commodity device, thereby eliminating the need for oscillators altogether. In Chapter 4, we propose MIXIQ, a novel, ultra low power WiFi

receiver design that can receive data at high speeds and large distances from commercial WiFi devices. MIXIQ can benefit downlink-focused applications such as audio streaming to Hearables.

Improving performance: Passive radios are improving but still far from the performance of active radios. In addition, they are not robust since they operate at sensitivity edge of the receivers and thereby decoding errors can be very frequent especially in scenarios that involve mobility and human body blockage.

In Chapter 5, we argue that there is significant room to optimize low-power radios if we can take advantage of channel dynamics, particularly in short-range settings. To achieve this, we face two challenges: first, we need to adapt to highly dynamic channels resulting from body movements and second, we need radios that can efficiently operate between μW and mW power consumption to take advantage of channel variations. To achieve this, we propose a new design paradigm, radio polymorphism, which tightly integrates passive and active components with fast switching across them, allowing us to turn high channel dynamics from being a disability to a strength. We leverage passive modes in myriad ways within the network stack, from minimizing data transfer and control overheads to improving rate selection and enabling channel-aware opportunistic transmission. We instantiate our design in a full hardware-software prototype, Morpho , and demonstrate an order of improvement in efficiency across diverse scenarios and applications.

Chapter 3

Redefining Passive WiFi Tags

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.

3.1 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[146, 53, 48, 148] 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. 3.1.

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) [62, 131]; or (ii) *explicitly*: low power oscillators on the tag directly generate the Δf signal, which drives a RF switch [53, 146, 48, 145] . 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 [13, 20].

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),

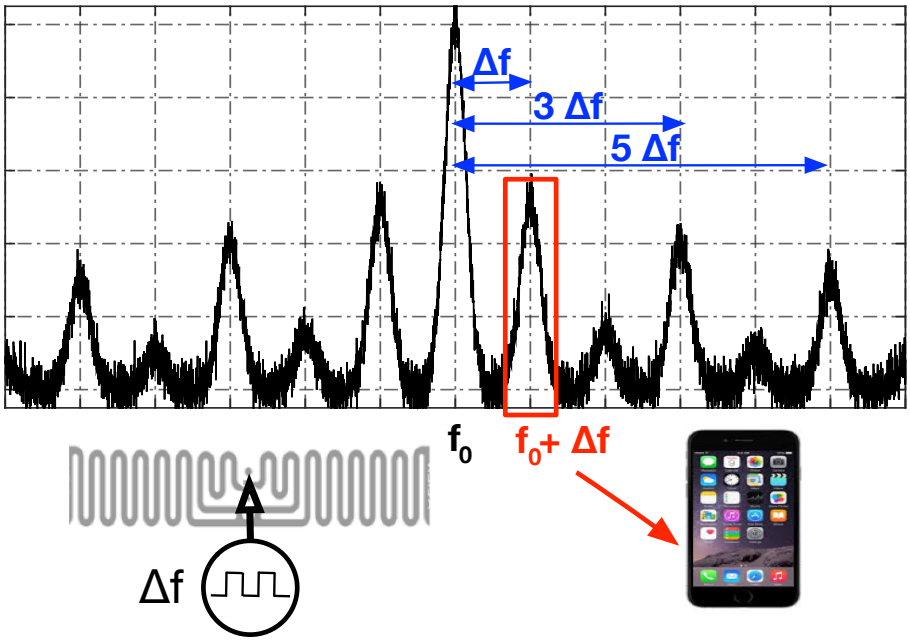


Figure 3.1: Frequency-shifted backscatter

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 [113], 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 [30] , 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.

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. 3.2). 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

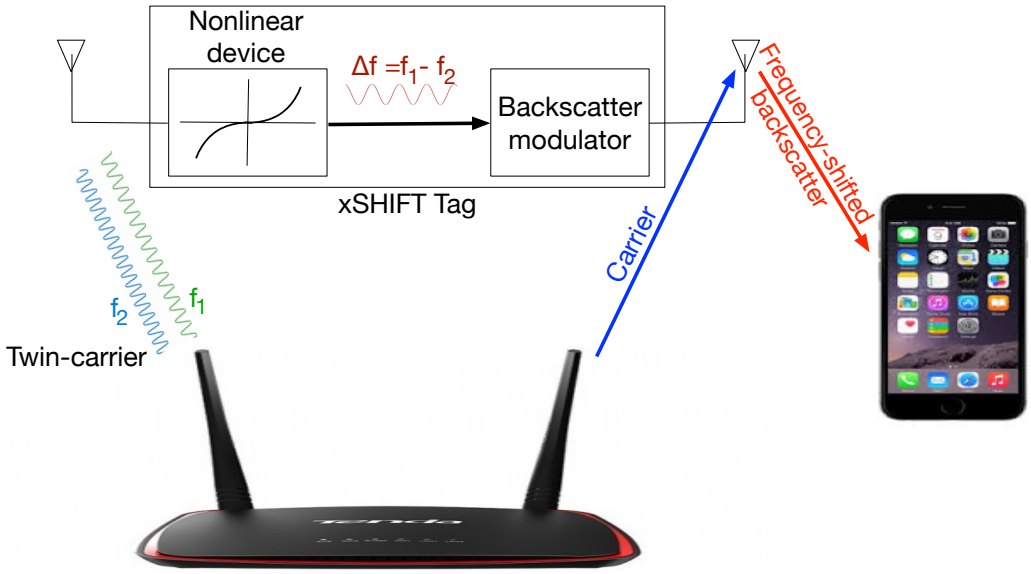


Figure 3.2: xShift backscatter system.

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. 3.12). 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.

3.2 Limitations of Oscillator driven Frequency Shifting

3.2.1 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, 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 [146, 144, 53, 48] 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 3.3), thereby eliminating the impact of self-interference.

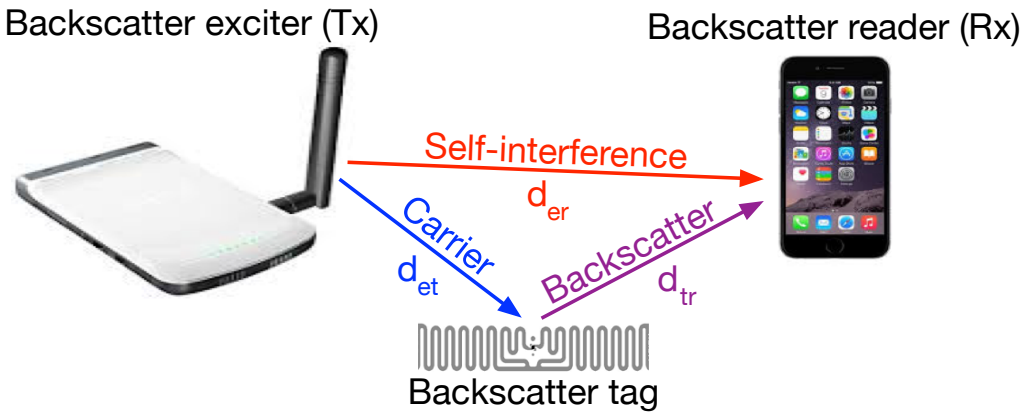


Figure 3.3: Commodity backscatter setup.

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 3.1. 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,

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

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,

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

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 3.1. As a result, the receiver can successfully obtain $X(t)$, which is a standard signal after demodulation.

3.2.2 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 [144], [146], [53], and [48] 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.

3.2.2.1 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 [113, 4, 68], which is substantial. The lower range points to a very novel design based on MEMS technology, SiT1576, released in early 2018[113]. A few recent works (e.g. [30]) 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.

3.2.2.2 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[27]), then the SiT1576 oscillator can stay On 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 3.4. 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

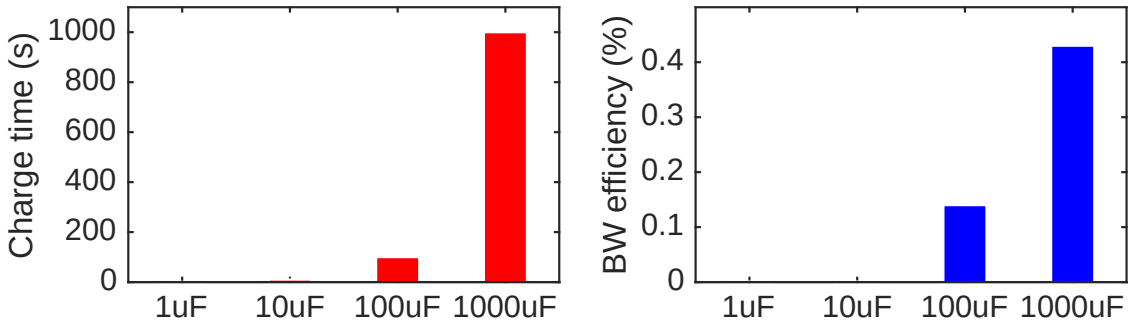


Figure 3.4: Osc.-based tag charge time and BW efficiency.

in a practically non-usable bandwidth (<1%) and throughput (<2 bps/μJ, Section 3.7.1.1) 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.

3.3 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.

3.3.1 xSHIFT backscatter

Figure 3.2 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 F) with each other, resulting in,

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

where the coefficients α_{mn} are specified by the function F. Hence, if we can filter out all the unwanted terms in (3.3.1) 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 [30], 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 [35, 131] 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 Chapter **??**). More importantly, xShift 's goal is to realize this construct with commodity devices, a significant hurdle that has not been addressed before.

3.3.2 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 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 3.5. 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.

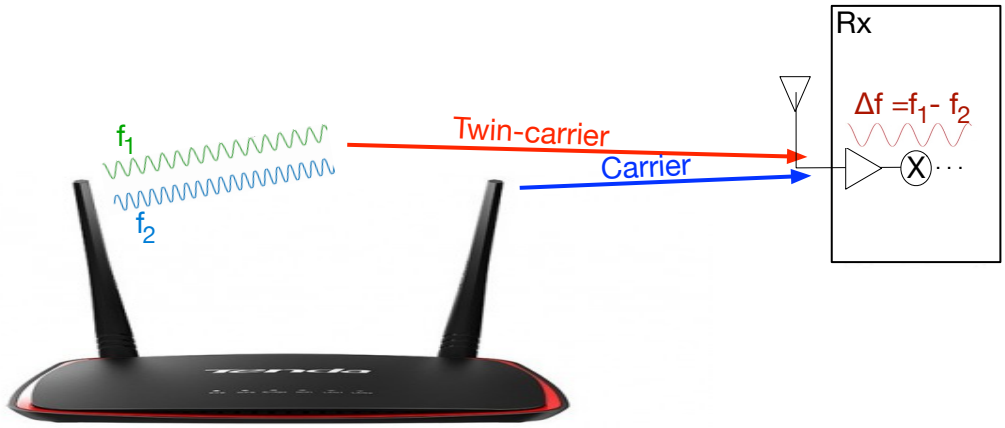


Figure 3.5: Internal interference in the receiver.

3.4 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.

3.4.1 Tag Design

Figure 3.6 shows the block diagram of our proposed tag design for creating the desired delta signal from a twin-carrier signal input.

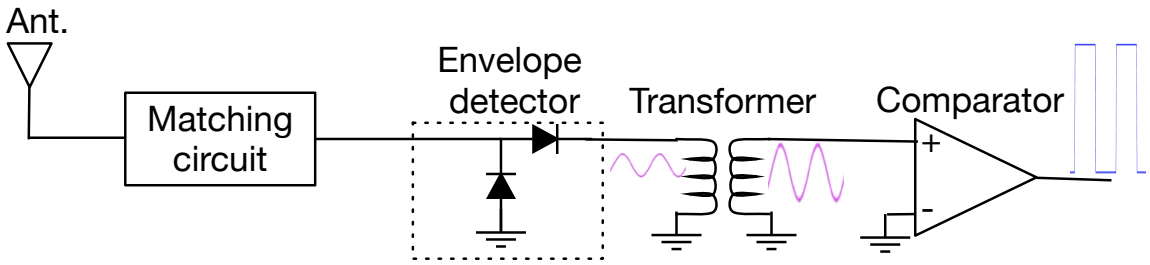


Figure 3.6: Block diagram of xShift 's delta generator.

3.4.1.1 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 3.7 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+[71]), (2) passive mixer followed by a 1:5 impedance transformer (Mini-Circuits TT25-1-X65[70]), (3) Schottky envelope detector (SkyWorks SMSA7630-061[114]), and (4) Schottky envelope detector followed by a 1:5 impedance transformer.

The results of figure 3.7 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 (§3.4.2). 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.

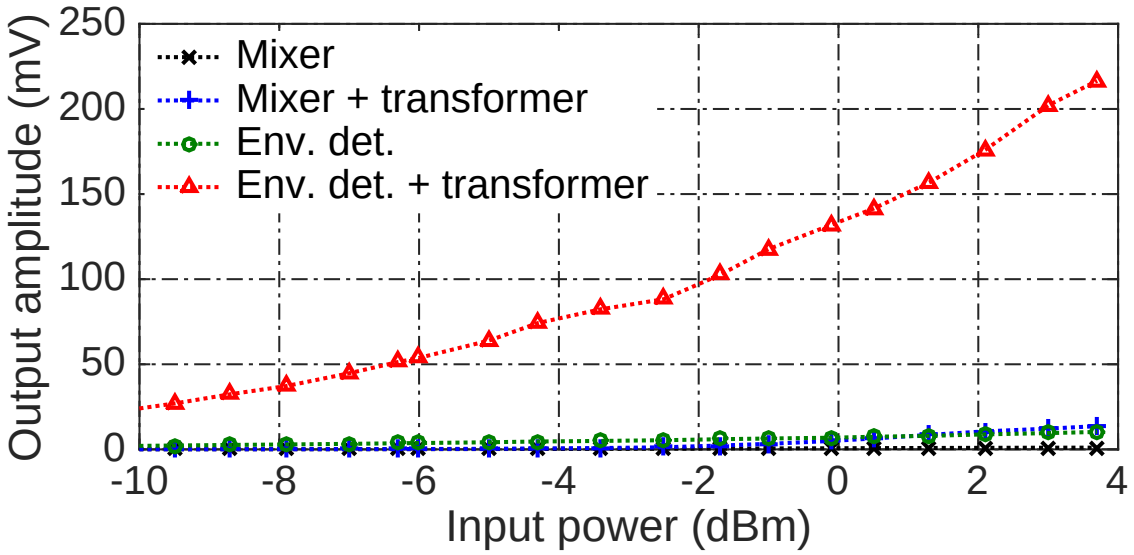


Figure 3.7: Performance of various delta gen. designs.

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[121]) 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.

3.4.1.2 Delta Signal Manipulation

As mentioned earlier in 3.3.2, the twin-carrier signal induces another delta signal with frequency 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. 3.10. The D-input of the flip-flop is connected to its inverted Q-output ($\bar{Q}$) 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 3.4.2, $\frac{\Delta f}{2}$ 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.

3.4.2 Twin-carrier Embedding

3.4.2.1 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) $\times$ 78.125kHz = 1.09375MHz (78.125kHz is the bandwidth of every single sub-channel in 802.11ax); this specifies the value of Δf, for which the delta generator part of the tag hardware should be designed and optimized.

3.4.2.2 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 3.8. 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.

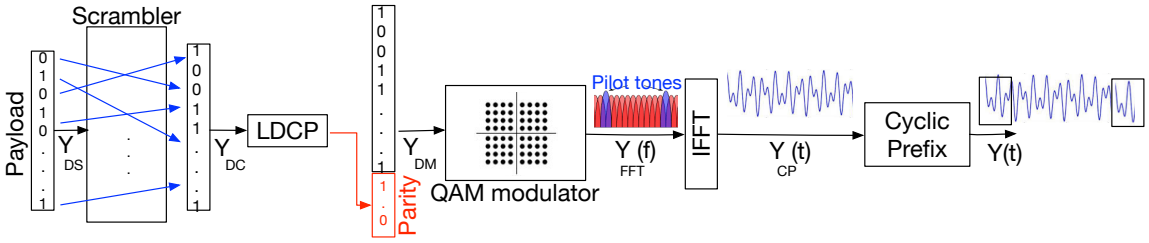


Figure 3.8: Payload-to-waveform pipeline in a 802.11ax WiFi transmitter.

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 3.8. 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 $C_1 = 0.03829 + 0.03829\,j$, $C_2 = 0.03829 - 0.03829\,j$, $C_3 = -0.03829 - 0.03829\,j$, and $C_4 = -0.03829 + 0.03829\,j$. 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[54] 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 3.8) Y_{DC} is related to Y_{DM} by:

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

where $H_{12000\times14400}$ 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.

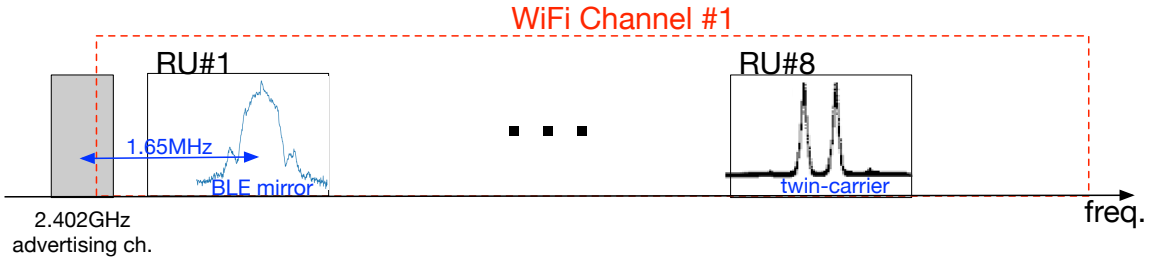
De-scramble: Finally, we perform de-scrambling, i.e. the inverse of the scrambling at the beginning of the pipeline to find Y_{DS}. This is straight-forward given that the Scrambler in 802.11ax is a linear-feedback shift register (LFSR), with the initial state of the LFSR being an integer number from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

3.4.3 Main Carrier (BLE) Embedding

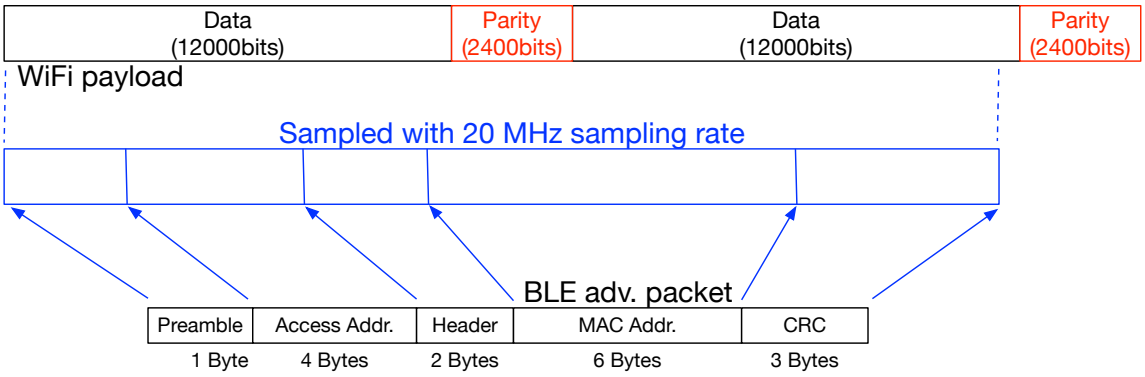
3.4.3.1 Placing the Main Carrier Signal

Recalling our discussion on internal interference from Section 3.3.2, 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 3.9(a). We refer to this signal as *BLE mirror*, $M_{BLE}(t)$. Note that as shown in [48], 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.

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 §3.4.2) for placement in RU 1.



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



(b) Embedding BLE in 802.11ax payload.

Figure 3.9: 802.11ax embedding

3.4.3.2 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 §3.4.2 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 $X_2'(t)$ in the exact same procedure as in §3.4.2. 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 $X_2(t)$.

3.4.4 Tag hardware

Aside from the delta generator, which forms the novel aspect of our design, the tag requires other hardware primitives for operation (figure 3.10) that we now describe.

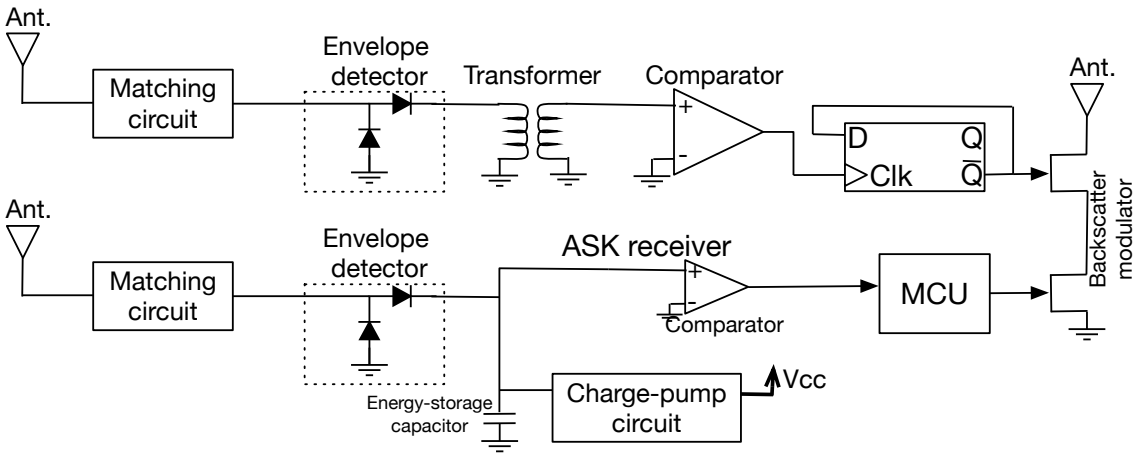


Figure 3.10: Block diagram of tag hardware.

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 $CV^2 = 2\mu\text{F} \times (0.3\text{V})^2 = 0.18\mu\text{J}$ energy available for the tag hardware to consume.

3.5 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. 3.11. 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

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

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.

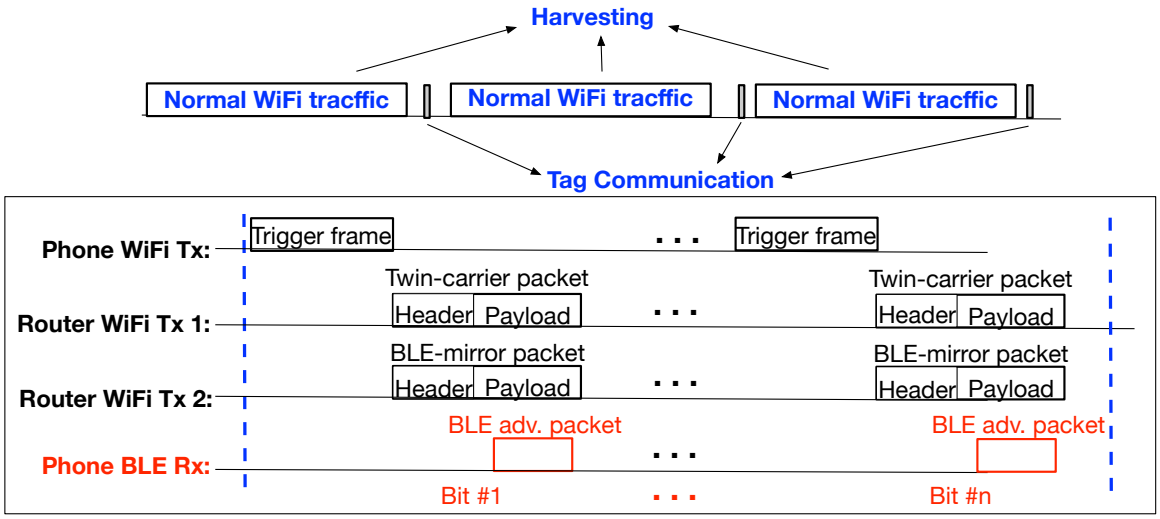


Figure 3.11: Timing diagram of xShift 's operation.

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 [54]). 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 [144]. 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.

3.6 Implementation

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

Tag prototype: Figure 3.12 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[75], one each for backscattering, delta generation, and harvesting/ASK reception. For backscatter modulation, we have used Analog Devices ADG902 RF switches[10]. The components used in the delta generator are the ones mentioned in §3.4.1. Also, we use the ultra low power SN74LVC1G80 D-type flip flop[120] for halving Δf.

The MCU that controls the Tx/Rx baseband is a MSP430FR5969 low power MCU[119] which is used also in other low power tag prototypes such as Intel WISP5.0[3].

Figure 3.12: xShift prototype vs. commercial RFID tag.

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[110] 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 (§3.4.1). The output of the envelope detector goes through a low power TLV7031 comparator[122] 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[32] 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 gener-

ated 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[125] evaluation board, along with the PER TEST firmware.

3.7 Evaluation

3.7.1 Tag hardware benchmarks

3.7.1.1 Efficiency

To understand the impact of individual components, we compare xShift with state-of-the-art oscillator-based designs (MEMS oscillator [113]) 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).

Power consumption: Table 3.1 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 3.1, 3.2, 3.3 has the same hardware as xShift 's prototype tag, except that the delta generation circuit (figure 3.6) is replaced by a MEMS oscillator [113].

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

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 3.1: Power consumption of tag components.

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 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[113]. Now, Table 3.2 shows xShift 's prototype and IC energy efficiency is two to three orders magnitude 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

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 3.2: xShift vs. osc. design (bits/μJ)

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 3.3, which are three to four orders of magnitude lower compared to xShift prototype tag and IC.

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 3.3: xShift vs. osc.design [min,max] (bps/μJ).

3.7.1.2 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, 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 3.13 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.

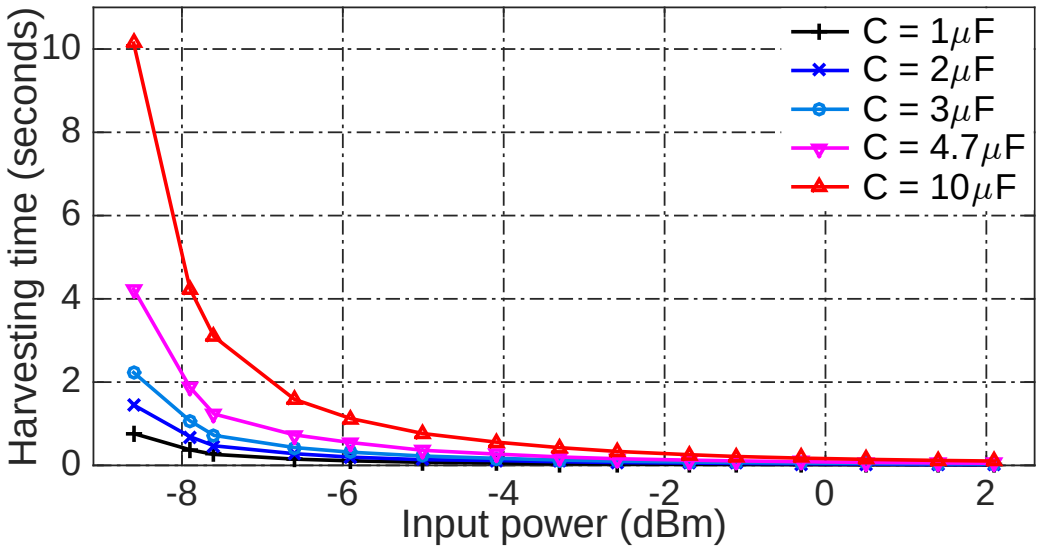


Figure 3.13: Charge time vs. RF power vs. capacitor size.

Delta generator: Fig. 3.14 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. 3.14) 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.

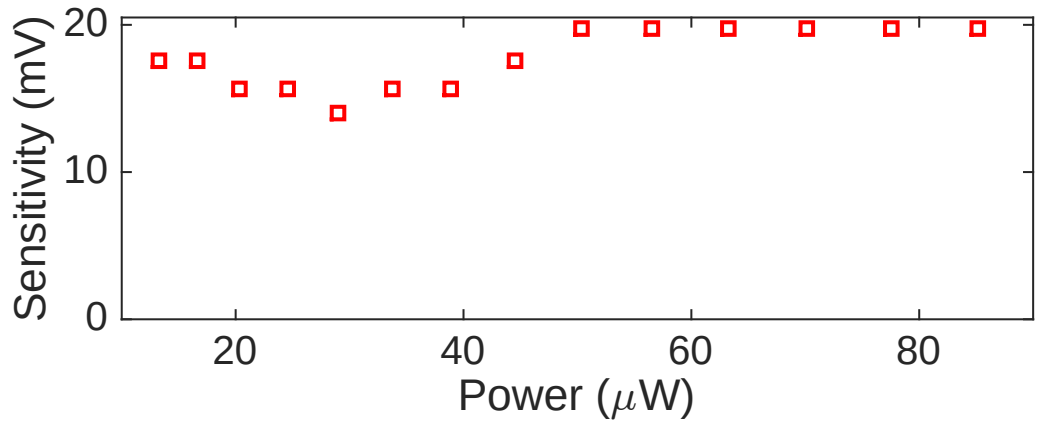


Figure 3.14: sensitivity vs. power drop of TLV7011.

3.7.2 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 3.15 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.

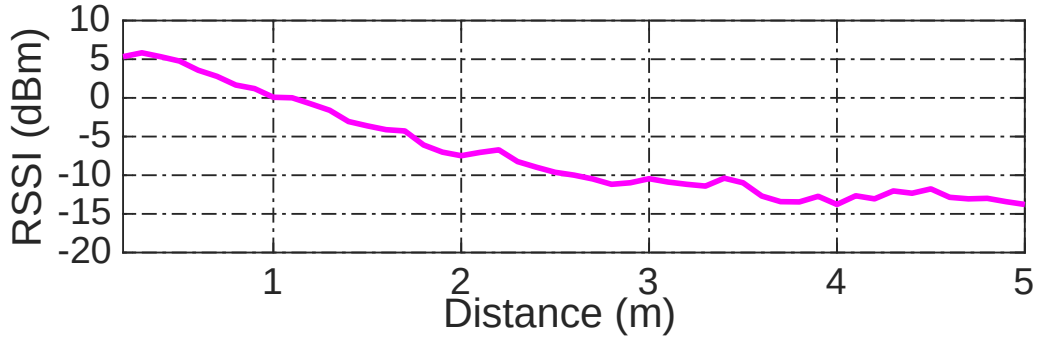


Figure 3.15: RSS vs. distance in line-of-sight.

From figure 3.15, 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 3.16 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 3.17 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.

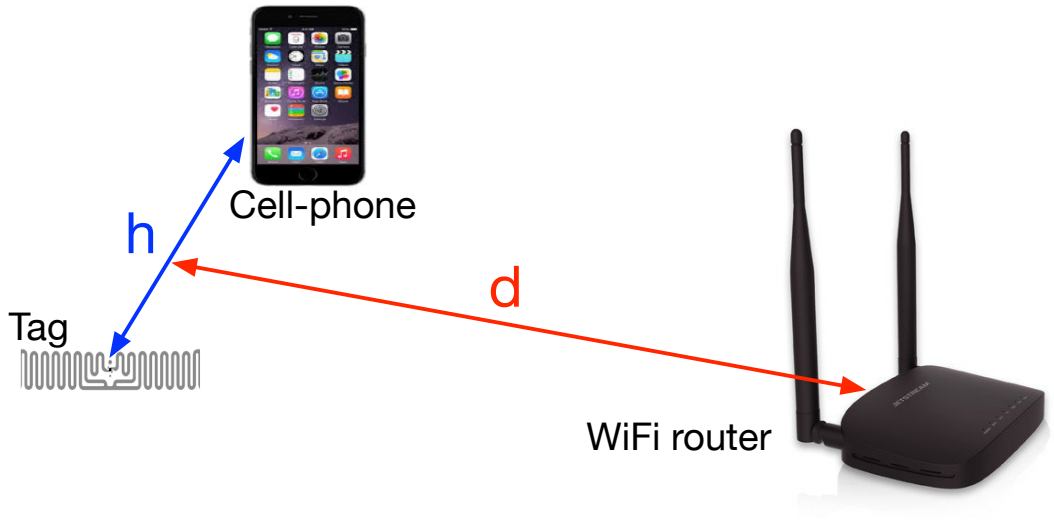


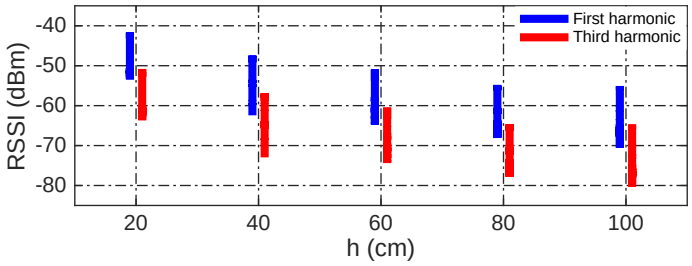
Figure 3.16: xShif experimental setup.

Figure 3.17 validates two key design choices in xShift for handling interference. First, comparing figures 3.17(a) and 3.17(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.

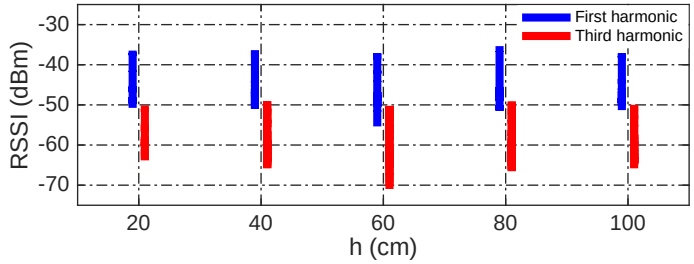
Second, comparing figures 3.17(a) and 3.17(c), the first harmonic of the backscatter is highly interfered by the BLE mirror signal due to their proximity (0.55 MHz), while the third harmonic of the backscatter signal is well above the interference level from the mirror signal. Hence, xShift 's choice for using the third harmonic of the backscatter signal, which is sufficiently shifted ($\frac{3}{2}\Delta f = 1.65$ MHz) from the mirror signal, is indeed appropriate.

3.7.3 Macro-level Benchmarks

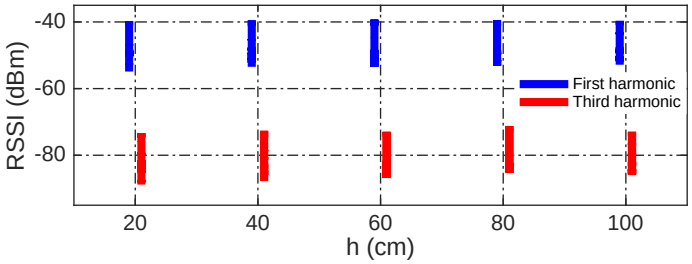
We study xShift 's performance in both static and mobile scenarios using two popular macro-level metrics, namely bit error rate (corresponds to packet error rate, PER with packet-level decoding) and throughput.



(a) Backscatter



(b) Internal interference



(c) Mirror interference

Figure 3.17: RSS of the backscatter and interfering signals at different values of h and d.

3.7.3.1 Static Scenarios

The measurement setup for static experiments is exactly as shown in figure3.16. 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 3.18 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.

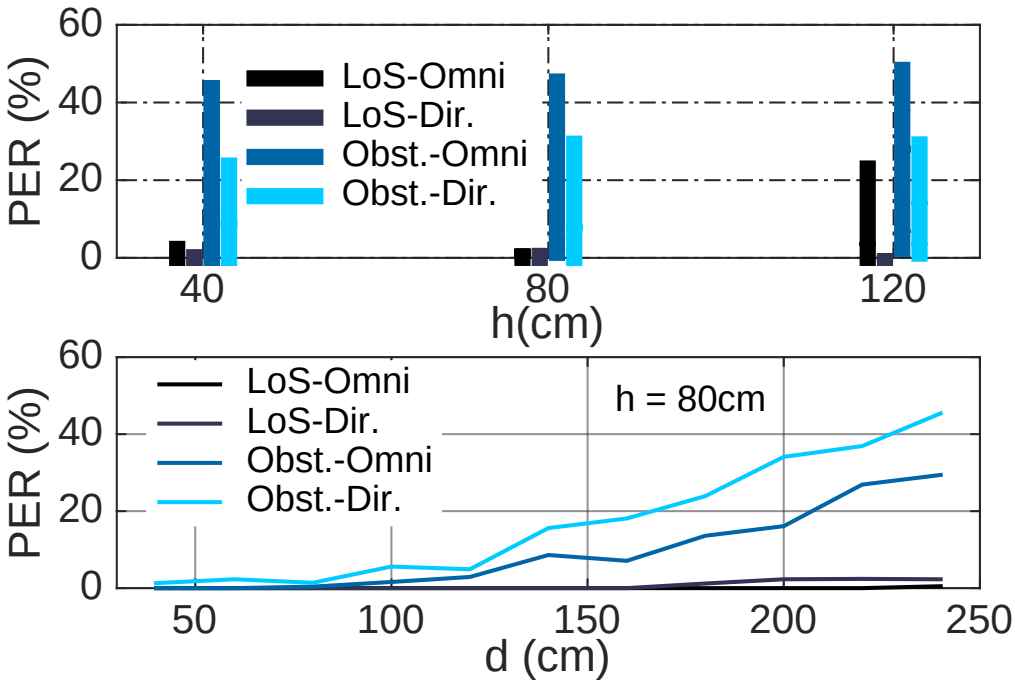


Figure 3.18: PER of various static configurations.

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 3.19 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.

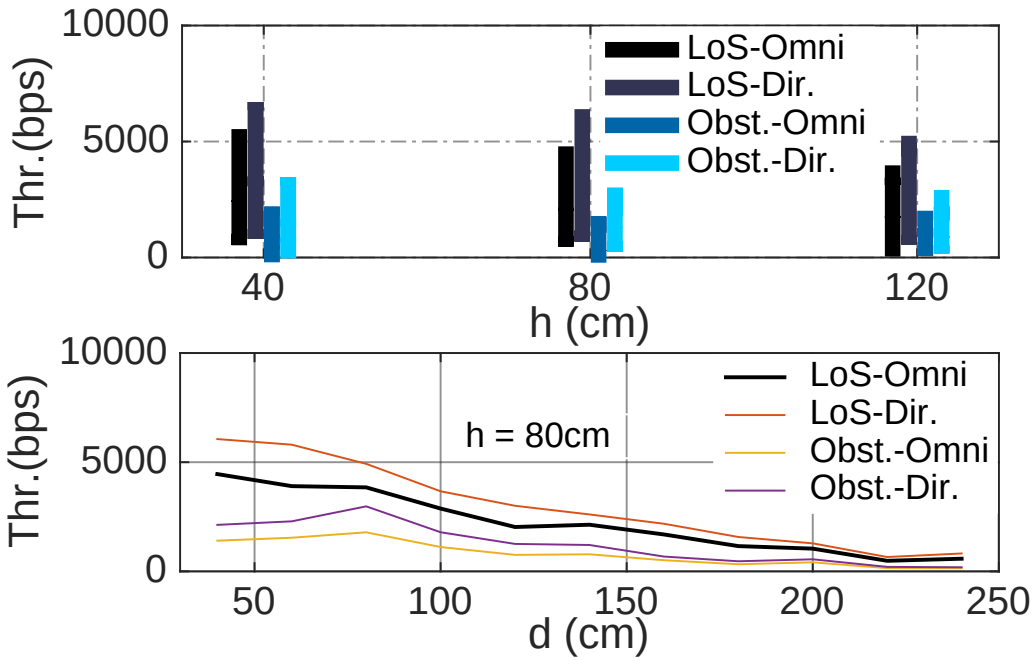


Figure 3.19: Throughput of static configurations.

3.7.3.2 Mobile Scenarios

The set-up for the mobility experiment is captured in Figure 3.23. 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 3.21 and 3.22 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.

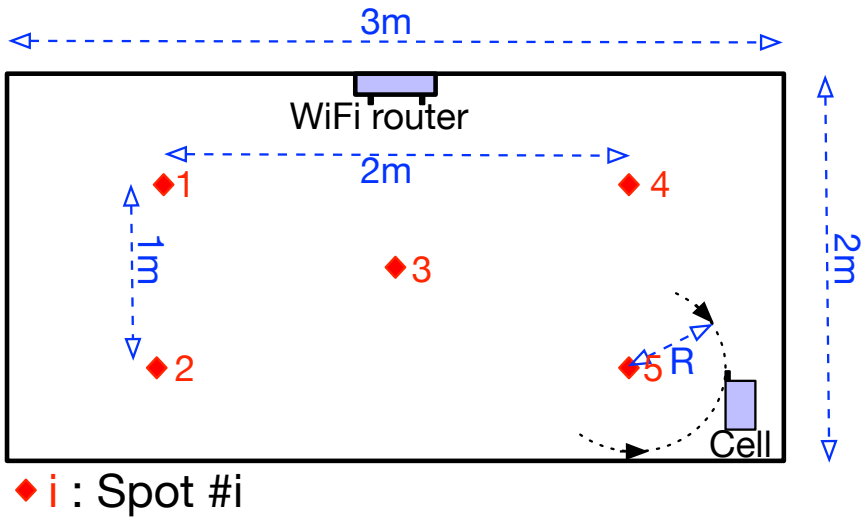


Figure 3.20: Mobility experiment setup.

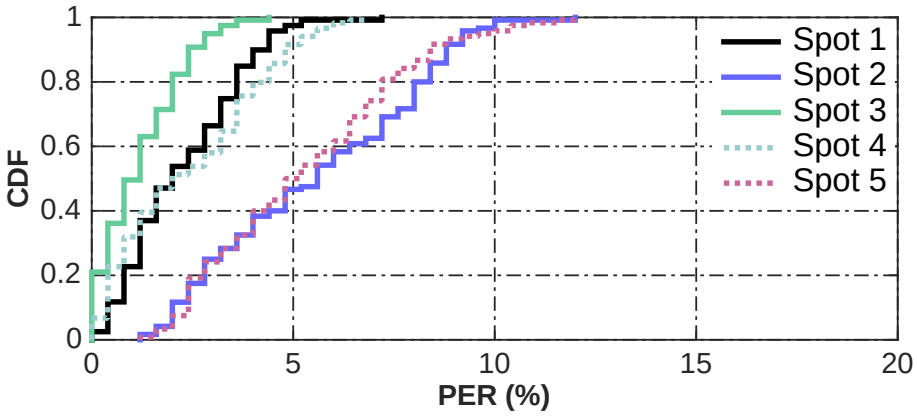


Figure 3.21: CDF of PER in the mobility scenario.

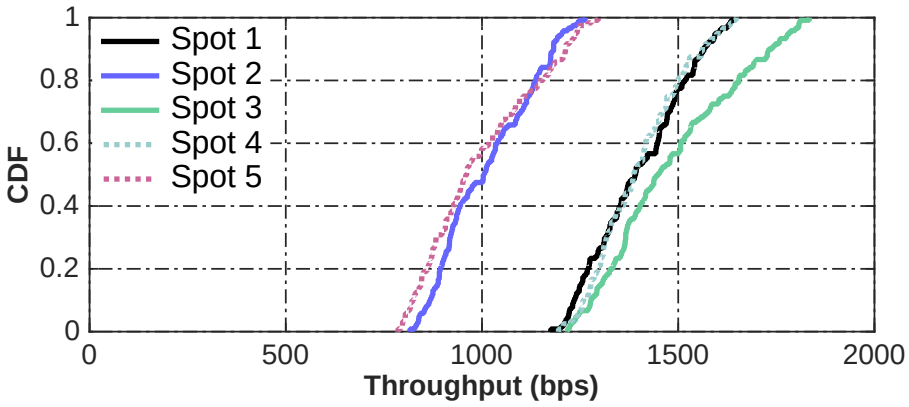


Figure 3.22: CDF of throughput in the mobility scenario.

3.8 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. 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. 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.

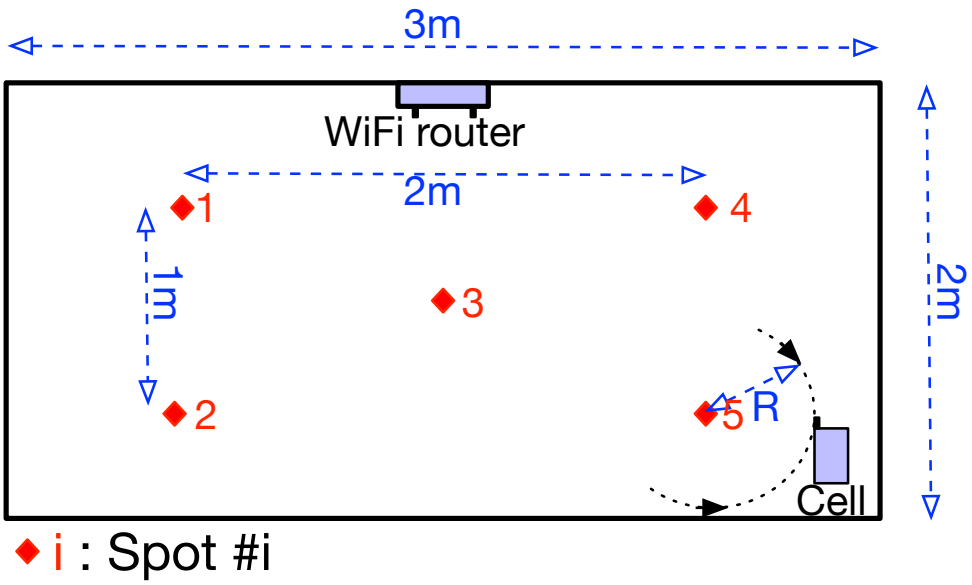


Figure 3.23: Mobility experiment setup.

3.9 Related Work

Commodity backscatter: One of the early works, BackFi[17], 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 [53], 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, [145] 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 [146] takes a different approach, where the tag XoR's its bits with that of the original WiFi packet and shifts it to an adjacent channel for reception by another WiFi device. Similarly, [48] 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[117], PLoRa[86]), by leveraging the superior sensitivity of LoRa receivers (-150dBm) and their chirp spread spectrum (CSS) modulation.

Ambient backscatter: A closely related set of works [133, 134, 141, 41], 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 [23, 24, 35, 95, 62, 131] have leveraged non-linear devices on the tag to backscatter the signal at harmonic frequencies. In particular, [35, 131] 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 [59, 19, 151, 21] 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 [59], WiFi signals are embedded into LTE frames in [19]. 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.

Chapter 4

Novel Ultra Low Power Receiver with Enhanced Capabilities

A long-standing challenge in radios for wearables is to design ultra-low power, yet high performance receivers with good sensitivity and spectral efficiency while being compatible with WiFi. Envelope detectors (EDs) are the most popular receivers on backscatter tags since they are passive but suffer from poor sensitivity and cannot decode complex modulations, which makes them a poor choice for directly decoding data from WiFi packets. Several custom ASIC-based designs have been explored to bridge this gap but these are usually difficult to prototype and deploy in practice.

In this chapter, we present our design of an easy-to-prototype ultra-low power receiver called MIXIQ that operates at μWs of power while providing improved sensitivity and decode-ability of complex high-rate signals. MIXIQ uses the signaling capabilities of the newest standard of WiFi, 802.11ax, to turn a standard WiFi packet into a helper + data signal. The same ED circuit driven by this twin signal now behaves like a *passive mixer* i.e. it down-converts the RF carrier data to the sub-MHz range without adding any energy overhead. MIXIQ then uses an ultra low-power largely digital baseband pipeline to (i) significantly boost sensitivity using ultra low power components; (ii) enable the

demodulation of complex signals for substantial boost in spectral efficiency. We show that MIXIQ improves upon a passive envelope detector by 25dB in sensitivity and 89× in bandwidth efficiency, while consuming 0.3mW for a PCB-based implementation and 40μW for an ASIC-based implementation. We also demonstrate a Hearable system that leverages MIXIQ to improve VOIP reception range by 10× compared to envelope detectors.

4.1 Introduction

A significant body of research in wireless communication in recent years has focused on the development of ultra-low power backscatter radios that can operate on extremely tiny power budgets while being compatible with commodity radios such as WiFi, LoRa, BLE and Zigbee [53, 48, 144, 17, 58, 86, 117]. Of these, WiFi compatibility is perhaps the most important given the widespread coverage offered by WiFi. An efficient and reliable WiFi backscatter system can be a key cog on how we design IoT and wearables, particularly when high data rates are needed.

The majority of these efforts, however, focus on enhancing upstream communication from the tag to the application device with few, if any, hardware-level enhancements to the tag-side receiver for downstream communication. For example, while the WiFi backscatter uplink has evolved over the years to achieve impressive bitrates of $>$10 Mbps (e.g. [150]), downlink performance has largely remained stagnant. Most WiFi Backscatter efforts use the same simple envelope detector circuit that is used in standard UHF RFID as the RF receiver (figure 4.1), and reverse-engineer the WiFi packet to mimic an OOK signal that is decodable by the detector. However, this OOK emulation is inefficient and has poor spectral efficiency with throughput in the low 100s of Kbps [48].

The reason for this gap between uplink and downlink performance is not due to the lack of advances in ultra-low power receivers but due to the difficulty in prototyping these designs. There have been many recent efforts that seek to enhance the sensitivity of envelope detectors and some of these have reported impressive sensitivities of -70dBm to -90dBm

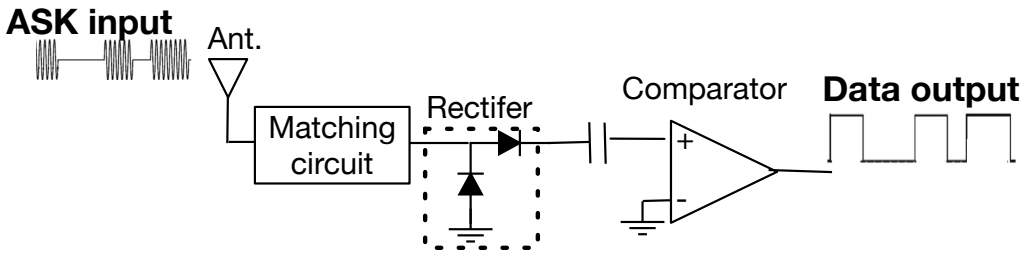


Figure 4.1: Simple envelope detector.

[89, 83, 108, 103, 44, 8, 43, 137]. The downside of these solutions, however, is that they are not easy to prototype unlike the uplink solutions. The upstream communication advances in backscatter have relied on easy-to-prototype elements like RF switches, transistors, and simple circuits, whereas the ultra-low power receivers are all IC-level designs that are not commercially available. As a result much of the recent systems activity in backscatter has focused on the upstream communication with limited enhancements to the receiver.

This gap has skewed exploration of new research and application ideas within backscatter communication. While several efforts have focused on leveraging the growing uplink bandwidth of WiFi backscatter to transmit richer sensor data to the base station, for example, streaming video and audio in real-time, there has been essentially no work on applications like Hearables that are dominated by downlink data transfer [139, 22, 38, 15]. Similarly, work on Backscatter MAC and upper layers have been skewed by the fact that the downlink is highly inefficient.

To fill this gap, we introduce MIXIQ, a novel ultra low power receiver design that (1) greatly outperforms the simple envelope detector used in the existing backscatter tags, (2) can be easily prototyped with off-the-shelf components, and (3) is compatible with WiFi for easy deployment and to enable a high throughput downlink that leverages OFDMA. MIXIQ adopts two strategies to fulfill these goals:

(1) Sub-carrier based WiFi packet emulation: The key contribution of our work is an OFDMA-compatible sub-carrier based (rather than symbol based) WiFi packet emulation technique that retains the benefits of using an envelope detector while (a) allowing the transmitter

to use its full dynamic range of power and (b) allowing the use of bits of data encoded in individual subcarriers. This technique is based on the fact that when an envelope detector receives two carriers, a data-carrying signal intertwined with a "helper" signal without data, at separate frequencies, it will behave like a frequency mixer and output a signal delta between the pair of transmitted signals which has the same phase and amplitude as the input data signal. Thus, the MIXIQ receiver can down-convert the data signal from UHF frequencies (e.g. 2.4GHz) to a LF (few 100 KHz) delta signal, all while preserving the complex phase and amplitude of the high data-rate data signal without any additional energy cost.

Our ideas extend those that have been proposed in prior work; for example, several backscatter systems leverage envelope detector non-linearity for creating an external helper tone [131, 62] and some work has looked at creating two identical tones from an OFDMA transmitter [102]. We combine these building blocks in the context of a receiver design, but also enhance them by showing that we can leverage the fine-grained frequency resolution offered by OFDMA versions (802.11ax, WiFi 6) to transmit two different signals from a WiFi transmitter (helper and data). This allows MIXIQ to be deployed with commodity WiFi radios that support 802.11ax.

(2) Digital-heavy demodulation pipeline: In addition to optimizing RF down-conversion, we also need to avoid the use of power-hungry RF/analog components in the demodulation pipeline to operate at the desired μW power regime while being able to decode complex, high data-rate signals.

To address this, MIXIQ employs an extremely power efficient, largely digital implementation of the entire demodulation pipeline. While such a digital-heavy approach is typically less power-efficient compared to analog, MIXIQ leverages the fact that the externally-assisted down-conversion results in very low frequencies (LF) of 100s of KHz. This in turn, paves the way for several optimizations: (i) *high-impedance voltage amplification* that substantially improves sensitivity with minimal additional energy cost (unlike power amplification) since MIXIQ can take advantage of the LF signal to leverage high impedance

components at both the input and output (power $\propto V^2/Z$); (ii) *high resolution ADC* that preserves information of high data rate signals while consuming very little power owing to the low sampling rate (1 MSPS) for the LF signal; and (iii) *full-digital IQ demodulation* by correlating with sampled sine and cosine signals entirely with digital circuits, thereby completely eliminating the need for analog filtering and its associated degradation in analog demodulators, while requiring significantly lower power. This also provides robustness to interference by considering the latter as noise in the digital domain.

Performance: We have implemented all different parts of MIXIQ using commercial off-the-shelf devices and components. On the WiFi TX side, we use a commercial WiFi 6 device (Qualcomm IPQ6010 [93]) and a version of openWRT driver on top of it to implement the sub-carrier based emulation. In addition, we prototyped MIXIQ's receiver on PCBs and have comprehensively characterized its performance and power consumption under various conditions.

Our evaluations reveal that MIXIQ delivers a sensitivity of -55dBm and a spectral efficiency of 0.51 bps/Hz (1.125 Mbps over 2.2 MHz bandwidth), which substantially improves upon existing envelope detector designs by 25dB and 89×, respectively. Further, our case study with a Hearable system built with MIXIQ as its receiver, reveals that it can receive high-rate VOIP data from a WiFi device with good signal quality and 10× the operational range of envelope detectors. We believe MIXIQ's contributions can open the door for higher performance ultra-low power receivers to be integrated with backscatter transmitters in several new and compelling applications in body area networks.

4.2 Case for a New Easy-to-Prototype Passive WiFi Rx

In this section, we discuss in more depth why much of the recent experimental on backscatter communication still rely on a simple envelope detector circuit as their receiver despite the fact that it delivers very poor performance.

Limitation of Envelope Detector as WiFi receiver: An envelope detector consists of an RF rectifier circuit (typically based a Schottky diode) followed by an ultra low power voltage comparator, figure 4.1. When an OOK signal arrives at the antenna, the rectifier converts the RF signal to an amplitude-varying LF signal. The comparator then generates 0s and 1s based on whether the amplitude is below or above the threshold. Such a circuit is very energy efficient and also easy to assemble using one of the many RF Schottky diodes and ultra low power comparators available in the market.

The vanilla Envelope Detector is also simple to interface with WiFi by manipulating the payload of a packet to mimic an OOK signal (e.g. [48]). This makes it possible for a simple envelope detector on a tag to directly decode the conveyed data bits. We refer to this mode of using an Envelope Detector with WiFi via emulated OOK as *WiFi-ED* .

The downside of the WiFi-ED, however, is that sensitivity is only around -20dBm to -30dBm, regardless of the bit rate. This makes it impractical for many interesting application scenarios for ultra-low power backscatter communication. For example, on-body links (e.g. from wrist to head) can easily introduce up to 60dB attenuation to the transmit signal at practical distances [109, 143]. Hence, if the transmitting device (say, a smartwatch) operates at 10dBm, the RSSI can be as low as -50dBm, which is far below the sensitivity of the detector.

Performance of the WiFi-ED is further diminished for three reasons. First, the TX power of WiFi TX is at least 10 dB lower than the radiated power of an RFID reader which means that range is severely limited. Second, the dynamic range of the emulated OOK signal via manipulating WiFi packets (i.e. the difference between low an high power levels) is also several dBs lower compared to the genuine OOK signal that is output by RFID TX antenna. Third, WiFi operates at 2.4GHz rather than 900MHz which suffers from more channel attenuation. As a result, the simplicity of the WiFi-ED also comes with significant downsides.

Limitations of Advanced Envelope Detector Designs: So far, we have looked only at the vanilla Envelope Detector, but can we take advantage of more advanced designs that have

been proposed in literature [136, 42, 81, 103, 100]? The issue is that these designs appear in the form of a transistor-level circuit diagrams that are simulated, tested, optimized in an Integrated Circuit (IC) environment. While achieving excellent performance, there are two important problems that make it difficult to prototype these designs. First, their performance improvement comes from optimizations and design techniques that are applicable only in an IC environment where parameters (e.g. Q factors of the components) and parasitic values are highly controlled. This is not the case when working with a PCB prototype with discrete parts inter-connected via PCB tracks. Second, these designs are not available in the market and they are fabricated in very small numbers just for the purposes of testing and proof-of-concept research. As a result, there still is no packaged, ready-to-use *enhanced Envelope Detector chip* that can be mounted on a PCB hardware prototype.

4.3 Overview of MIXIQ

We present MIXIQ – an easy-to-prototype ultra low power receiver design that transforms the passive envelope detector to behave like an advanced receiver with high sensitivity and ability to decode complex, high data rate signals, while also keeping its energy footprint in the μW regime. MIXIQ is built on two techniques, as shown in figure 4.2.

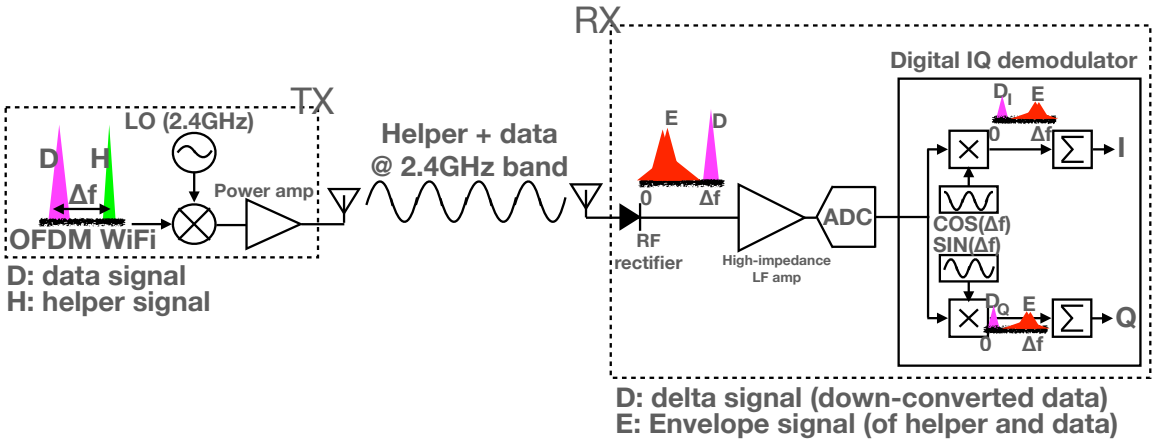


Figure 4.2: Overview of MIXIQ .

1. Transforming the RF rectifier into an externally triggered passive mixer: The first

contribution in MIXIQ is a technique to enable a "helper tone" signal to be provided *externally* by the transmitting WiFi device, allowing us to offload its energy requirement from the receiver to the transmitter. The helper tone signal is needed as input to a mixer which multiplies (or mixes) with the incoming data RF signal – the output has an intermediate frequency (Δf) of $f_{data} - f_{helper}$ which is a down-conversion of the incoming RF frequency.

To reduce the power consumption of the mixer, MIXIQ generates a helper signal by employing a new signaling approach whereby the data-carrying signal is accompanied by a "helper" signal (without any data) at a slightly different frequency as shown in figure 4.2.

The helper signal is intelligently designed such that it can be seamlessly embedded alongside the data signal into existing WiFi signal waveforms, making MIXIQ compatible with commodity WiFi devices. When such a *helper+data* signal passes through an envelope detector, the latter's non-linearity allows for the conversion of the incoming data signal to a much lower frequency that is the difference of the two carrier frequencies (called *delta* signal). Thus, the information (phase and amplitude) from the incoming UHF data signal (e.g. 2.4 GHz) is transferred onto the delta signal at just a few hundred KHz, without any additional energy cost. If we denote the incoming UHF data and helper signals by $X_d(t) = A_d(t)\cos(2\pi f_d t + \phi_d(t))$ and $X_h(t) = A_h\cos(2\pi f_h t)$, then the rectifier's output is:

$$V_{rect.} = A_d^2(t) + A_h^2 + 2A_h A_d(t)\cos(2\pi\Delta f t + \phi_d(t)) \tag{4.1}$$

The last term is the resulting delta signal at Δf that preserves the amplitude and phase of the incoming UHF data signal.

We note that prior work has also used a helper tone [64] to turn an envelope detector into an externally-triggered passive mixer but the difference is that this effort used a separate "helper" device that emits a pure tone helper signal whereas MIXIQ uses the capabilities of OFDMA WiFi to embed the helper signal within the same device that is sending the data signal. Thus, our approach is more practical in terms of deployability.

2. An ultra low power digital-heavy demodulation pipeline: The delta signal (with frequency Δf) at the output of the mixer, is accompanied by some inter-modulation terms

that arise due to the re-purposed rectifier not being an ideal mixer. In other words, it outputs the envelopes of the data and helper signals, which can interfere with the down-converted delta signal. MIXIQ leverages the very low frequency nature of the delta signal to design a highly power-efficient demodulation pipeline that not only gets rid of the undesired inter-modulation signals, but also increases (a) sensitivity through voltage amplification that leverages high impedance analog components at micro-power, and (b) spectral efficiency through a fully-digital micro-power IQ demodulation (Figure 4.2) that eliminates the degradation faced by the analog demodulators.

4.3.1 Practical Challenges

Realizing MIXIQ 's architecture in practice necessitates addressing several technical challenges.

Challenge 1: Embedding data + helper signal in WiFi packets: The helper signal needs to be generated in the same commodity device that is sending the data signal since a separate device for helper signal generation makes the system less practical. Further, the helper and data signals should be sufficiently separated in the frequency domain, with the spectrum between them being unused so that the delta signal is created at the envelope detector.

Challenge 2: Tradeoff between bandwidth and sensitivity: Increasing the channel bandwidth contributes to larger data rates but results in a severe degradation of receive sensitivity. Higher bandwidth requires a higher Δf; however, increasing Δf has two detrimental effects on sensitivity: (1) the downconversion ratio i.e. the ratio between the amplitude of the downconverted signal at the output of the rectifier and RF input power, rapidly decreases with higher Δf as shown in Figure 4.3 for two different RF rectifiers (BAT63-02V [46], and HSMS-285C [14]), indicating the generality of the problem; (2) gains achieved by micro-power amplifiers at higher Δf are lower. For example, for a bandwidth of 1 MHz, we need a Δf of several MHz (e.g. 8MHz in [87]), to be able to filter out the unwanted low-frequency terms as well as perform IQ demodulation successfully. However, as shown

in Figure 4.3, the down-conversion ratio is less than 0.3mV/μW, which contributes to around 15dB worse sensitivity, compared to when the bandwidth is as low as 100 KHz. Further, the state of the art designs do not achieve more than 30dB voltage gain with micro-power amplifiers at these frequencies, compared to the 60dB voltage gain possible at sub-MHz frequencies, thereby leading to another 15 dB difference in sensitivity. Thus, migrating from sub-MHz to several MHz for obtaining higher bandwidth can compromise the sensitivity by as much as 30dB.

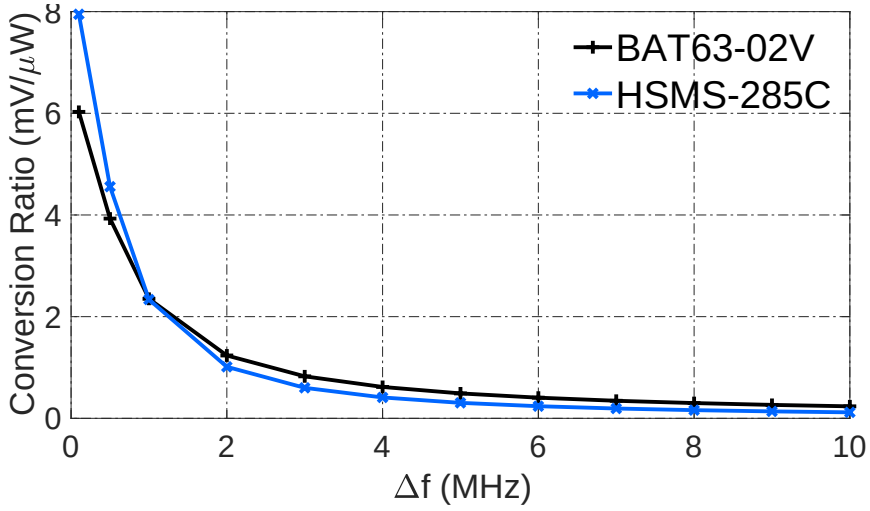


Figure 4.3: Conversion ratio of RF rectifiers vs. Δf.

Challenge 3: Preserving the amplitude and phase information accurately: Demodulation of complex waveforms requires us to track the abrupt changes in the amplitude and phase of the down-converted data signal without introducing any distortion. However, achieving this goal with passive and low power components is challenging. Consider a passive RLC filter that is used to eliminate the unwanted low frequency components at the output of the rectifier. If it has a wide passband, it cannot completely filter out the unwanted terms that are very close in frequency to the down-converted data signal. On the other hand, a narrow passband makes the filter simple but unable to track the rapid changes in amplitude and phase, rendering it not useful for IQ demodulation. In essence, designing a base-band for our receiver is highly non-trivial.

Challenge 4: The impact of interference: Even though MIXIQ's design behaves like an

active radio in many aspects, it is still frequency non-selective like an envelope detector, i.e. it is unable to distinguish the frequency of the RF signal received at the antenna. Hence, if there exists another signal at frequency f_i, $X_i(t) = A_i(t)\cos(2\pi f_i t + \phi_i(t))$in Equation4.1, it will also be detected by the rectifier, with the corresponding low frequency term A_i^2 appearing at the output. Also, other terms such as $2A_hA_i(t)\cos(2\pi(f_i - f_h)t + \phi_i(t))$ and $2A_d(t)A_i(t)\cos(2\pi(f_i - f_d)t + \phi_i(t) - \phi_d(t))$ might also appear close or even overlap with the *delta* signal in the frequency domain. These terms interfere with the down-converted data signal, affecting its demodulation. We also wish to avoid deactivating other transmitters in the network during MIXIQ's reception since this will hurt spectral efficiency as only a small fraction of the entire band (e.g. only hundreds of kHz of the total 80MHz of the 2.4GHz ISM band) will be used.

We now present MIXIQ's design components that tackle these challenges.

4.4 External down-conversion with Commodity Radios

MIXIQ enables commercial WiFi 6 devices to transmit a *helper + data signal* with no hardware modifications and also no change in the format of standard 802.11ax packets.

4.4.1 Leveraging Spectrum Channelization

To account for the tradeoff between larger bandwidths (hence larger Δf) and lower sensitivity, MIXIQ leverages 802.11ax's OFDMA to operate commodity transmissions on much smaller bandwidths (2.2MHz). This allows it to design the LO signal with a much smaller Δf and has three key benefits. The first is increased sensitivity from improved down-conversion ratio and ultra low power amplifier gains (discussed in Section 4.3.1). The second is increased data rates from sampling the down-converted signal at a higher resolution, allowing for a fully digital IQ demodulation of complex, high-rate modulations at ultra low power consumption (discussed in Section 4.5.3). The third is increased spectral efficiency from not

only increased data rates on individual transmissions but the ability to multiplex multiple such transmissions from different users on orthogonal spectral chunks (called resource units, RUs). A resource unit can be as small as 2.2MHz (i.e. $\frac{1}{10}\times$ 22 MHz channel bandwidth). Hence, the LO signal would occupy only 2.2MHz of the WiFi channel, while the rest of the RUs can be allocated to other WiFi (either MIXIQ or legacy) transmissions. Note that such a multiplexing is not possible with existing passive receiver designs, where the energy on the entire bandwidth (WiFi transmission) is used to decode low-rate information.

4.4.2 Placement of the LO Signal

OFDMA allows for splitting a given bandwidth into several smaller sub-channels (RUs), each consisting of a set of sub-carriers that can be individually modulated. MIXIQ leverages this feature to embed the data and helper signals within a single RU, where each of the signals occupy one or more sub-carriers and are separated by several sub-carriers in between, as shown in Figure 4.4.

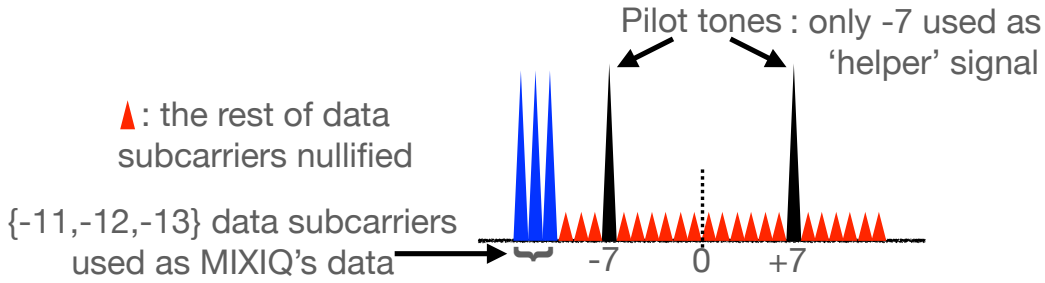


Figure 4.4: MIXIQ 's signaling within a 802.11ax RU.

Selecting Δf: In order to successfully demodulate the down-converted IQ data signal, the symbol rate must be sufficiently smaller than the carrier frequency. The output of the IQ demodulator contains the original I and Q values along with some residual terms – a larger magnitude of the latter leads to demodulation errors. If we denote the delta signal as: $r(t) = i\cos(2\pi\Delta ft) + q\cos(2\pi\Delta ft)$, where i and q are called the in-phase and quadrature parts of the signal, the obtained I and Q values in digital domain can be written as: $\hat{I} = \frac{1}{k}\sum_1^k r(nT).\cos(2\pi\Delta fnT)$ and $\hat{Q} = \frac{1}{k}\sum_1^k r(nT).\sin(2\pi\Delta fnT)$. ($T$ is the sampling

period). The ratio between the magnitude of the residual terms, (i.e. the difference between $\hat{I}$, $\hat{Q}$ with the original i and q) and the magnitude of the constellation points reduces as Δf $\times T_S$ (where $T_S = k.T$ is the symbol time) increases. Numerical analysis on the residual terms show that when Δf $\times T_S \leq 3$, the value of $\hat{I} + j\hat{Q}$ falls into other constellation points, resulting in demodulation error. Therefore, Δf $\times T_S > 3$ is necessary for enabling high order modulations that need a larger ratio (e.g. 25dB for QAM-64).

Selecting helper and data signals: MIXIQ leverages the smallest RU of 2.2 MHz, which consists of two pilot tones (sub-carriers). Given that the pilot tones cannot be suppressed, MIXIQ employs one of the pilot tones (-7) as its helper signal, as shown in Figure 4.4. With the chosen Δf > 234kHz, the sub-carriers used for carrying the data signal in our transmitter should be at least 4 sub-carriers away from the helper signal. There are 18 such data subcarriers in our 2.2MHz RU (all of them except {-10,-9,-8,-6,-5,-4}).

MIXIQ uses only the three sub-carriers on the left side of the {-7} pilot tone, i.e. {-13,-12,-11}. The reason is that the rest of the subcarriers located on the right side of the {-7} pilot tone, i.e. {-3,-2,...,+12,+13} either overlap in frequency with {-13,-12,-11} after the passive mixer, or are too far from the {-7} helper tone which in turn degrades sensitivity. Δf does not exceed 468.75kHz for any of the chosen data sub-carriers, and remains in the efficient region of sub-MHz, wherein both the down-conversion ratio of the rectifier and the gains of the micro-power voltage amplifiers are high. This enhances sensitivity of our receiver.

Choosing Δf to be less than 468.75kHz also ensures that the bandwidth of the data signal after down-conversion does not exceed 500kHz; hence, its information will be fully preserved when being sampled at 1MSPS (1MSPS > 2 $\times$ 500kHz ; Nyquist theorem). This allows MIXIQ to leverage extremely low power, very high resolution (e.g. 12-bit) ADCs at the desired 1MSPS sampling rate, which are available both off-the-shelf [124] and as ASIC [128]. Thus, the data signal can be transferred to the digital domain, where demodulation can be accomplished using ultra low power logic elements without compromising accuracy, which reduces power consumption.

Nullifying unwanted data sub-carriers: Sub-carriers not used for the data and helper signals need to be nullified to prevent corruption of the LO signal that is needed for accurate down-conversion. While one cannot completely nullify a sub-carrier, MIXIQ leverages higher-order modulations to “almost" nullify un-wanted sub-carriers – the farthest constellation points in higher-order modulations (e.g. QAM-256) from the origin can have more than 15$\times$ greater amplitude than the closest ones. Thus, data and helper sub-carriers are assigned constellation points with the largest magnitude, while others are nullified by assigning those with the smallest amplitude.

Minimizing the residual terms that appear as transmitter noise: The fact that unwanted sub-carriers do not become completely nullified does, however, impact noise. Although the unwanted sub-carriers get the constellation points with the lowest power to resemble nullified sub-carriers, these small values can add up and appear as a significant *transmitter noise* term. The noise power is at its peak when the *low amplitude* constellation points assigned to the nullified sub-carriers have all the same phase resulting in a constructive total sum.

To address this problem, we search for the combination of the phases for the unwanted sub-carriers (through exhaustive search) that minimizes their impact. This is a one-time effort and after 162 iterations of the search, MIXIQ is able to reduce the power of these residual terms after demodulation to be 35dB below at the power of the data for every down-converted data sub-carrier. This ratio is well above the ratio required for successful demodulation of QAM-64 signals (25dB).

Compliance with 802.11ax standard: Our signaling method also complies with the packet structure defined in 802.11ax standard. When the WiFi TX device is sending the “data+helper” signal as we have proposed, it is actually sending packets in its normal mode of operation. As a result, our approach does not impact any aspect of the performance, including the power consumption, of the WiFi TX device. Additionally, the WiFi TX device operates as a normal WiFi 802.11ax-compatible client of a 802.11ax WiFi network: it takes a portion of the channel that is assigned by the WiFi AP, called resource unit (RU), to transmit

the data + helper signal. Since RUs are separated in frequency domain, it will not interfere with other WiFi clients that take different RUs for transmitting their packets to the AP.

4.4.3 Encoding the Data Signal

Once the data subcarriers in the RU are selected, MIXIQ optimizes their modulation and coding to ensure a robust delivery of high-rate modulations.

Modulation scheme selection: While the highest modulation order available in 802.11ax is QAM-1024, which translates to 10 bits per subcarrier per symbol time, MIXIQ employs QAM-64 that has six bits per subcarrier per symbol time. Modulations higher than QAM-64 are less robust to the residual terms of the IQ demodulation, and fail to work with the closest data sub-carriers (and hence Δf) chosen. On the other hand, incorporating an additional data subcarrier or increasing Δf to accommodate even higher modulations, impacts the power consumption and sensitivity of the receiver. Hence, MIXIQ settles for QAM-64 to maintain the optimal design choice of the data-subcarriers. MIXIQ 's design choices result in a raw throughput of: 3 subcarriers $\times$ 6 $\frac{\text{bit}}{\text{subcarrier}}$ $\times$ $\frac{1}{16\mu s}$ = 1.125Mbps over the 2.2 MHz RU.

LDPC for coding: MIXIQ leverages the option of LDPC (low density parity check) codes in 802.11ax (compared to convolutional codes in prior standards). Being a type of block codes, LDPC allows for better control of the data in different RUs, since the data bits are separated from the parity bits, unlike convolutional codes, where they are interleaved. Also, the scrambler before the LDPC can be easily reverse engineered given its known pattern.

4.4.4 Reverse-engineering 802.11ax

Finally, we need to reverse-engineer the 802.11ax pipeline to determine the appropriate payload bits that will generate the desired data and helper waveform $Y(t)$. We borrow the 802.11ax reverse engineering technique introduced in [102], but with two main differences. First, [102] nullifies all the data sub-carriers in the 26-tone resource unit and only keeps

the two pilot tones as the twin-carrier signal; whereas, we want to use data sub-carriers {-13,-12,-11} for data transmission. Second, the twin carrier signal emulated in [102] is sensitive cyclic prefix wherein a small chunk of the initial samples that is added to the tail of the 256-element vector of IQ samples. Therefore, their choice is limited to 8-th resource unit. However, MIXIQ receiver can completely ignore the cyclic prefix part and focus on the main 256-element vector when demodulating and thus the cyclic prefix step of the reverse engineering can be skipped. As a result, MIXIQ can leverage any 26-tone RU within the channel which is beneficial when co-existing with other devices in the WiFi network.

Therefore, we take the following steps for reverse engineering the payload of the standard 802.11ax packets in uplink trigger mode when the client is sending on a 26-tone resource unit.

FFT: The OFDMA modulator of 802.11ax takes a 26-element complex vector, $Y_{FFT}(f)$ as input and performs inverse fast fourier transform (IFFT) to obtain the transmit signal in time domain. Each element of $Y_{FFT}(f)$ corresponds to the phase and amplitude of one of the 26 subcarriers (24 data subcarrier and two pilot tones) within the resource unit. The output of IFFT, $Y_T(t)$ is a 256-element complex vector that determines the I and Q values. Note that in OFDMA all the sub-carriers outside the selected resource unit are null. Since FFT and IFFT are inverse mathematical functions, we can calculate $Y_{FFT}(f)$ by taking the FFT of $Y_T(t)$ as,

$$Y_{FFT}(f_m) = \sum_{n=1}^{256} Y_T(n)\, e^{-j2\pi f_m n}, \tag{4.2}$$

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

QAM-64 constellation de-map: In our configuration of the 802.11ax device, every element of Y_{FFT} is assigned to a QAM-64 constellation point. Since our goal is to nullify all of the data subcarriers except {-13,-12,-11}, we select the constellation points with the lowest energy, or closest ones to the origin, for those subcarriers. Note that the two pilot tones cannot be reverse engineered and they toggle between +1+0j and -1+0j per OFDM symbol according to the pattern specified in 802.11ax standard. In QAM-64, the closest points to the origin are $C_1 = 0.17 + 0.17j$, $C_2 = 0.17 - 0.17j$, $C_3 = -0.17 - 0.17j$,

and $C_4 = -0.17 + 0.17j$. Thus, every 6-bit chunk of Y_{DM} for data sub-carriers {-10,-9,-8,-6...,+6,+8,+12,+13} maps to a complex number from the set $\{C_1, C_2, C_3, C_4\}$.

LDPC decode: Next, we need to find the data bits that result in the desired constellation points. The 802.11ax standard is equipped with an LDPC encoder that converts the input bit-vector Y_{DC} consisting of the bits of the data to the encoded bit-vector Y_{DM} and then every 6-bit sector of Y_{DM} is converted to a QAM-64 constellation point. Y_{DM} is obtained by attaching parity bits to chucks of Y_{DC}, which can be shown as $Y_{DM}^{(i)} = Y_{DC}^{(i)}.H$ where H is the matrix of the code [54]. The size of the data chunks followed by parity blocks is determined by LDPC code rate. We choose the highest rate = $\frac{5}{6}$ to maximize the throughput since it minimizes the size of parity blocks that cannot be reverse engineered. In this case, the 802.11ax LDPC encoder takes every 12000-bit chunk of data bits, $Y_{DC}^{(i)}$ and attaches a 2400-bit chunk of parity bits to obtain $Y_{DM}^{(i)}$.

De-scramble: Finally, we perform the inverse of the scrambling that is done on the input data bits before they are LDPC encoded. This is straightforward since the 802.11ax scrambler consists of a linear-feedback shift register (LFSR) and the initial state of the LFSR is known from the standard. Therefore, we can reverse the steps from the desired data bits to the initial bits of the LFSR to find the input data bits.

4.5 Receiver Architecture

We now describe MIXIQ 's receiver baseband pipeline that is employed at the output of the rectifier. Our goal is to achieve the desired sensitivity and spectral efficiency at μW by leveraging MIXIQ 's choice of subcarriers which results in a small Δf (described in 4.4.2).

4.5.1 High-impedance voltage amplification

At UHF radio frequencies such as 2.4GHz, it is important to keep input and output impedance of the amplifiers at 50Ω to avoid reflection loss caused by impedance mismatch. In contrast, at sub-MHz frequencies, one can have stable voltage amplifiers with input and output impedance much greater than 50Ω (e.g. tens of kΩ), while providing up to 60dB voltage gain. Being high-impedance at the input and output reduces the power dissipation of these amplifiers to μW levels. Hence, SNR can be dramatically increased, which improves the sensitivity even for high-order modulations that need high SNR (e.g. 25dB for QAM-64) for successful demodulation.

4.5.1.1 Two-stage common-emitter based amplification:

MIXIQ employs a voltage amplifier design, consisting of a few common-emitter (in BJT implementation, or common-sources in our CMOS simulations which we discuss later) stages that can significantly amplify the output of the rectifier at μW power consumption, with a minimal distortion to amplitude and phase of the down-converted data signal. Figure 4.5 shows an implementation of a micro-power amplifier with NPN bipolar junction transistors (BJT). It consists of two stages for generating a higher voltage gain. The NPN transistor used at each stage is an On Semiconductor 2N3904 [82], which is biased using these values: $R_{B_1} = R_{B_2} = 10k\Omega$, $R_C = 9.1k\Omega$, $R_E = 2.2k\Omega$, and $C_B = C_E = C_C = 100nF$ ($V_{cc} = 1.8$v).

Voltage gain: Each stage of our implemented BJT amplifier has 33.0dB small signal (SS) gain. However, this happens only when it is not impacted by the input and output load impedances. In practice, the voltage at the output of the first and second stages get compromised by about 3dB each because of the loading effect at their input and output. Thus, the overall gain of MIXIQ's two-stage amplifier is about 57dB when the amplifier is placed between the rectifier and the next stage in the pipeline.

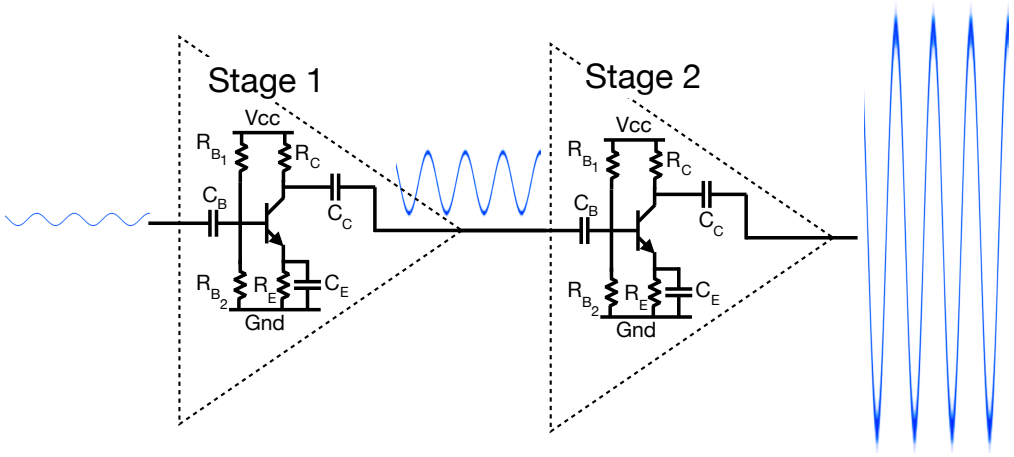


Figure 4.5: Two-stage common-emitter amplifier.

4.5.1.2 Distortion control:

Employing high impedance pushes the bias point of the transistors very close to the saturation region of the transistor. Hence, if the output of the rectifier, is greater in amplitude, the transistors can saturate, severely distorting the amplitude and phase of the down-converted data signal. To overcome this issue, MIXIQ employs a gain control unit that measures the received signal strength (RSS), based on which it decides to turn off the amplifier either fully or partially if necessary to prevent distortion of the down-converted data signal.

MIXIQ allocates the first two symbols of the WiFi packet are for RSSI measurements based on which the receiver decides how many stages to be used for the rest of the packet that contains actual data bits. Therefore, MIXIQ performs the distortion control with no additional components. Note that this reduces the overall throughput but if the channel variations are not so fast it can be reduced to one channel control per ten packets thereby minimizing its overhead.

4.5.2 Low-power ADC

The output of the rectifier is just a few hundreds of kHz, which allows MIXIQ to acquire the whole delta waveform with just a sampling rate of 1MSPS (1 Mega samples per second).

Thus, a reasonably high-resolution (12-bit) ADC can be employed to convert the signal to the digital domain at very low power, thereby paving the way for full-digital IQ demodulation. Note that MIXIQ provisions a buffer (common-collector in BJT, or common-drain in CMOS) stage between the output of the amplifier's second stage and ADC's input to minimize the impact of ADC's low input impedance (2.5kΩ). Therefore, the overall gain is compromised by only 6.1dB; as opposed to 16.9dB if there were no buffer between amplifiers and ADC.

4.5.3 Fully-digital IQ demodulation

Demodulation of complex signals such as QAM-64 requires an IQ demodulator that does not influence the amplitude and phase of the delta signal. Briefly, an IQ demodulator calculates the correlation of the incoming modulated signal with the cosine and sine wave-forms to obtain the in-phase (I) and quadrature (Q) component values, respectively. Then, the closest constellation point to the calculated I+jQ value (after scaling the amplitude) is determined so as to decode the data bits.

Challenges with analog implementation: One challenge is that analog components used to implement the correlation (e.g. analog multipliers), are non-ideal and produce unwanted terms such as the square terms of the inputs. Thus, if the low frequency terms, i.e. the envelopes of the data and helper, are not filtered out, the comparator will produce their inter-modulation, which will interfere with the output of the correlator. Hence, there needs to be an analog filter between the rectifier and the analog IQ demodulator. However, using analog filters leads to a degradation in sensitivity and/or throughput, as discussed in §4.3.1.

Full-digital design: Figure 4.2 shows the building blocks of MIXIQ's IQ demodulator, which consists of all the tasks, including the multiplications, being implemented arithmetically with digital circuits. This in turn, prevents the inter-modulations, thereby allowing it to completely bypass the bandpass filter in its design.

In essence, MIXIQ digitally multiples the samples of the delta signal with the locally stored cosine and sine waveforms. The different values of the cosine and sine

waveforms at different timestamps are stored in permanent memory for instantaneous access at the same sampling rate at which the delta signal is acquired.

The digital multiplication is implemented with in a parallel way and therefore the clock frequency of the demodulator logic circuit does not have to be several times higher than ADC sampling rate. In addition, we use an ultra low power CPLD (complex programmable logic device) for implementing the logic. CPLDs are very similar in nature to FPGAs – both programmable logic – but can be found at lower energy footprints than FPGAs since they have less complex logic blocks and resources than FPGAs. Therefore, a CPLD that works at low clock frequency substantially reduces the power consumed during demodulation.

Robustness Against Interference: Since the rectifier cannot distinguish the frequency of the incoming RF signal at its antenna, signals from other simultaneous transmissions can also be rectified and potentially interfere with the down-converted data signal. However, MIXIQ is highly robust to such interference caused by other WiFi transmitters. This is because the transmit power of the interfering devices is not concentrated on the three data subcarriers, but rather distributed among the 24 subcarriers and two pilot tones (in case of the smallest size RU that has 26 subcarriers, while for larger RUs, the power is even further distributed). Hence, the interference power at the three target data subcarriers becomes much lower.

Even if the interference on the down-converted data subcarriers exceeds the threshold that can be tolerated by MIXIQ's QAM-64 demodulator, the data can be protected by compromising on the bit rate and adapting it based on the interference. This is accomplished by selecting a *subset* (instead of all) of the QAM-64 constellation points as the alphabet, thereby increasing the minimum distance between any two constellation points. This in turn increases $\frac{E_s}{N_0+I}$ to more than 25dB, where I is the power of the interference on the data subcarriers. Our evaluations in Section 4.8.4 reveal MIXIQ's higher degree of robustness to varying levels of interference.

4.6 System Configuration

We now describe how MIXIQ is able to co-exist with a standard 802.11ax WiFi network by only occupying 10% of a single channel bandwidth (22 MHz during operation).

802.11ax uplink trigger mode: In 802.11ax, there is a multi-user mode of operation defined for uplink OFDMA (i.e. from the clients to the AP), which allows a single WiFi channel to be split among several clients. Therefore, clients can concurrently send their data in a particular portion of the channel, called resource unit(s) (RU) allocated to them. MIXIQ configures the uplink of the network to work in trigger mode and its transmitter is chosen to be one of the clients, which is assigned a RU that has the smallest size possible, i.e. consisting of 26 sub-carriers (24 data and two pilot tones), each 78.125 KHz wide, making the whole RU to be 2.2MHz.

Packet structure: MIXIQ adapts the encoding and the decoding of data to 802.11ax's structure of the packet payload. The packet's payload consists of blocks of data bits, each followed by a set of parity bits. Note that we can only control the data bits, while the parity bits are automatically determined by the LDPC encoding matrix based on the data bits. Hence, MIXIQ embeds the data + helper (LO) signals in the OFDM symbols that correspond to the data bits and simply bypass the symbols that correspond to the parity bits. We set the LDPC code rate to 5/6, which is the highest code rate in 802.11ax for QAM-64, to minimize the throughput loss due to the inactivity during the parity bits.

Preamble insertion: MIXIQ uses the first two symbols in the data payload to create a custom preamble. MIXIQ modulates each of the three subcarriers (that is used for data) with constellation point C_1 = 1+j (has the most distance from the origin in QAM-64) in the first symbol time and $C_2 = -C_1$ in the second symbol time. MIXIQ's receiver uses this preamble for (1) detecting the beginning of a packet, (2) finding the reference amplitude and phase values to perform IQ demodulation successfully, and (3) doing distortion control as described in §4.5.1.2.

Cyclic prefix: In 802.11ax, like other OFDM WiFi signals, the 12.8μs OFDM symbol interval is followed by a guard interval, called cyclic prefix with a specific length that can be as short as 3.2μs. This cyclic prefix is exactly taken from the beginning of the OFDM symbol. MIXIQ's receiver does not use this cyclic prefix for demodulation and the 12.8μs symbol is directly correlated with the Cosine and Sine waveforms. Hence, we set the length of the cyclic prefix to its minimum of 3.2μs to minimize the throughput loss from cyclic prefix overhead. In this case, 3 (number of subcarriers) $\times$ 8 (number of bits per QAM-64 symbol) = 24 bits are sent per 16μs (OFDM symbol time + cyclic prefix).

Pilot tone phase variation: Even though the amplitude of the pilot tones remains constant within the entire packet, their phases take different values, from $\{0,\pi\}$ per symbol according to the pattern defined by the standard. As a result, the phase of the QAM-64 symbols on the down-converted data subcarriers have π offset from the true value at some of the symbol times. But since the pattern is known, the receiver can simply reverse the phase at these symbol times to compensate for the phase offset.

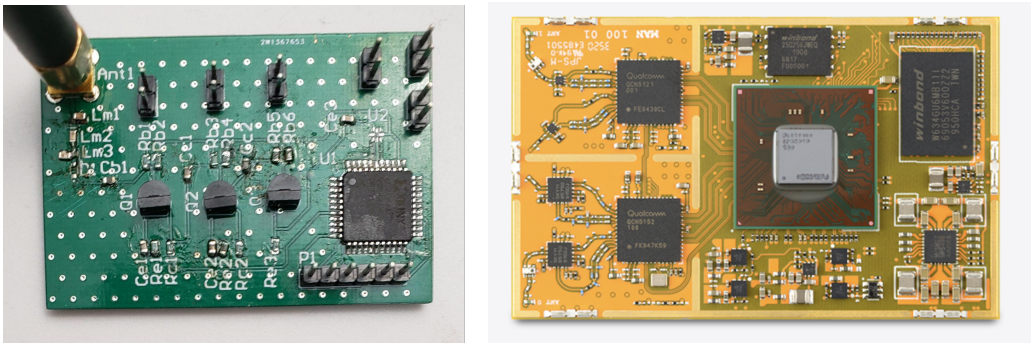
4.7 Implementation

4.7.1 Tag hardware

Figure 4.6(a) shows a PCB prototype of our MIXIQ's receiver. The components employed are as follows.

Antenna + rectifier: A W24-SSMA-M 2.4GHz small whip antenna with 2dBi gain. Also, Infineon BAT63-02V RF Schottky diode [46] serves as the RF rectifier with a π matching network between it and the antenna, resulting in the conversion ratio plotted in Figure 4.3.

High-impedance sub-MHz Amplifiers and ADC buffers: ON-Semi 2N3904 general-purpose bipolar transistors [82] are used to implement the two-stage common-emitter amplifier(§4.5.1) as well as the common-collector impedance buffer between the amplifier



(a) MIXIQ Prototype. (b) IPQ6010 module.

Figure 4.6: MIXIQ 's TX and RX hardware.

and ADC (§4.5.2).

ADC: Texas Instruments ADS7042 serves as the ADC. It draws 122.9μA from a 1.5v DC power supply during analog-to-digital conversion at 1MSPS with a 12-bit resolution.

Baseband logic: A Xilinx XC2C64A-7VQGC CoolRunnerII CPLD [140], which is compatible with a 1.5v logic level is used to implement the tasks of digital IQ demodulation, preamble detection, and pilot tone phase adaptation. Even though this CPLD is highly optimized for power efficiency, it provides enough resources to do all the arithmetic required for these tasks. In addition, MIXIQ is able to store the values of sine and cosine waveforms required for IQ demodulation in the memory blocks of the CPLD. In total, 43 of the total 64 macro-cells (67%) of XC2C64 are used to implement the full functionality of the digital parts of the receiver.

ADC and logic clock oscillator: Two SiTime SiT1576 [113] (a micro-power MEMS oscillator) are used to produce the 1MHz ADC clock and the 2MHz CPLD clock.

CMOS Simulation: We also conduct a CMOS simulation of the analog/digital pipeline after the rectifier using Cadence Virtuoso IC Design software. This allows us to test the functionality and estimate the power consumption of MIXIQ's building blocks in TSMC 130nm technology. For the ADC, we employ the design proposed in [128] which is a 10-bit charge-redistribution analog-to-digital converter consuming only 1.9μA from a 1V DC voltage source. Hence, we set the overall gain of the amplifier+buffer stages to 63dB

(6dB higher than the gain of the BJT amplifiers) to appropriately compensate for the lower resolution of the ADC compared with the off-the-shelf one used in our prototype (ADS7042).

4.7.2 802.11ax TX

We implement MIXIQ on both a commercially-available WiFi 6 chipset (the IPQ6010 [93]) as well as in MATLAB's WLAN 802.11ax PHY-MAC stack. The MATLAB emulation allows us to evaluate the effect of hardware imperfections and to ensure that the results can generalize to any 802.11ax implementation.

Our implementation is based on a version of openWRT (an open-source, linux-based driver that supports a myriad of commercial Wireless routers) developed for 8-devices Mango-I [127] (Figure 4.6(b)) which is an IPQ6010 daughterboard that is connected to Mango DVK board [126]. This version of openWRT provides APIs for configuring IPQ6010 to operate as a client in the uplink trigger mode while using one 26-tone resource unit to send its packet to the AP with QAM-64 and $\frac{5}{6}$-rate LDPC as modulation and coding schemes, respectively. We choose the first RU of the first 802.11ax WiFi channel (i.e. the RU that starts at 2402.59MHz and end at 2404.61MHz).

In addition, the 8-devices openWRT allows us to send raw payloads over 802.11ax WiFi packets, i.e. no protocol such a IPV4 and TCP on top of it. That allows us to send our reverse engineered payloads that result in the data+helper structure that we discuss in §4.4.2. Throughout our experiments, we configure the transmit power of the Mango-I board to 17dBm, to mimic a cellphone device.

Our emulation uses MATLAB's WLAN toolbox (for 802.11ax PHY-MAC stack) for embedding the data+helper signal within the payload of 802.11ax packets. It allows us to do the required reverse engineering on the payload of the packet such that the desired subcarriers {-13,-12,-11} are made to contain data while the rest of the sub-carriers are nullified by assigning lowest constellation points to them. In addition, later during the evaluation of an audio application in §4.8.5, we use MATLAB to encode 128 Kbps audio

streams to data bits that are used to modulate MIXIQ's data transmission.

4.8 Evaluation

We characterize MIXIQ 's overall performance, followed by a validation of the benefits of its key design components. We then present a case study of MIXIQ 's potential through a hearable application that we prototyped.

4.8.1 MIXIQ's Overall Performance

MIXIQ Sensitivity: Figure 4.7 compares the bit error rate (BER) of MIXIQ against WiFi-ED (§4.2). The WiFi-ED is implemented with the same RF rectifier, BAT63-02, and Texas Instruments TLV7011 micro-power comparator). We also plot the measurement results with MATLAB+SDR to show that we achieve the similar gains regardless of what WiFi device we use as TX.

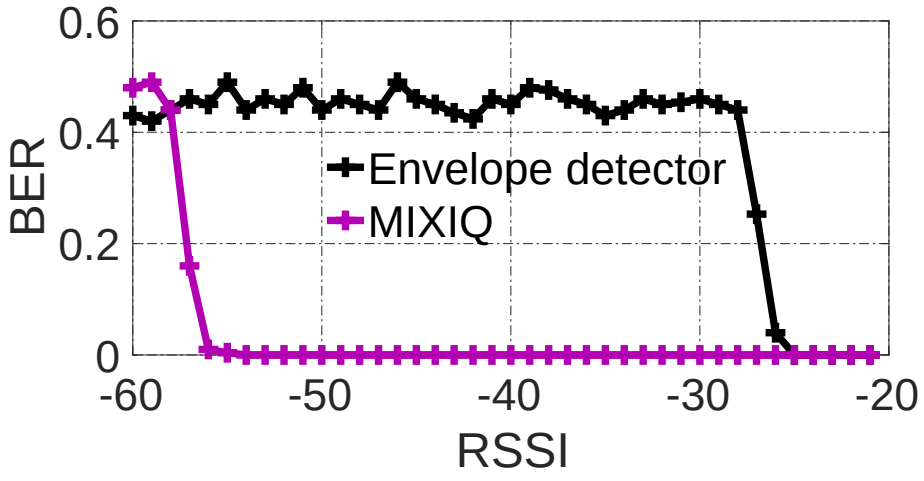


Figure 4.7: Sensitivity of MIXIQ vs. WiFi-ED.

In order to measure the MIXIQ 's BER, we modulate a total of 100,000 random bits on its three data subcarriers {-13,-12,-11} and compare the output of its IQ demodulator with the original bits to calculate BER, and repeat this for various RSSI of the 802.11ax

WiFi packet, ranging from -60dBm to -20dBm. Similarly, for obtaining the BER of the WiFi-ED, we modulate 100,0000 bits on 802.11ax symbols according to the OOK method proposed in [48] (even though the method in [48] is for 802.11ac, the same technique for emulating OOK using OFDM symbols is applicable to 802.11ax as well). It can be seen that to achieve near zero (<0.0001) BER, WiFi-ED needs an RSS $>$ -26dBm, whereas MIXIQ can work at RSS as low as -52dBm. In other words, *MIXIQ improves the receive sensitivity by $>$ 25 dB over that of WiFi-ED*.

We also see that the 802.11ax emulation with MATLAB and SDR and experimental results on IPQ6010 are very similar which shows that our results should generalize to any 802.11ax implementation. The performance of the WiFi-ED is identical in emulation and experimentation. The performance of the MIXIQ receiver in emulation and experimentation are only 3dB apart (possibly due to small hardware imperfections which introduce additional interfering terms to the data+helper signal).

MIXIQ Spectral Efficiency: Table 4.1 shows MIXIQ 's performance in terms of throughput and spectral efficiency and compares these against the WiFi-ED's performance. *MIXIQ not only has 9$\times$ better throughput; it also occupies 10$\times$ less bandwidth than the WiFi-ED (2.2MHz compared to 22MHz).* As a result, MIXIQ 's spectral efficiency is significantly better (90$\times$) than that of the WiFi-ED. The throughput increase from Kbps to Mbps also offers a substantial spectral efficiency gain of 9$\times$, even if the rest of the 22MHz channel is not utilized by any other WiFi devices to avoid interference.

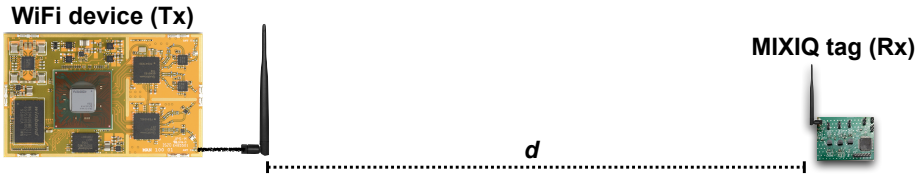
Metric	MIXIQ	WiFi-ED
Throughput (Kbps)	1125	125
Spectral Eff. (bps/Hz)	0.51	0.0057

Table 4.1: MIXIQ vs. WiFi-ED

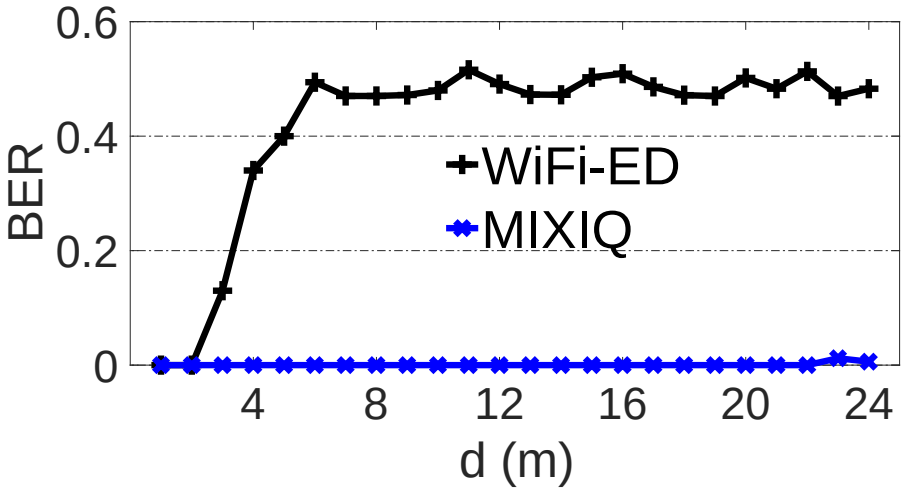
Range: Figure 4.8(a) shows the experimental setup for our range experiment. It consists of a standard WiFi 6 TX device (Mango-I IPQ6010 evaluation board) and MIXIQ PCB tag being in the Line of Sight (LoS) of each other. At one end of this LoS link, the WiFi TX devices transmits the reverse engineered *data+helper* packets at 17dBm via a 5dBi

2.4GHz whip antenna. At the other end of the link, the tag demodulates the data bits within the packets at d meters away from the WiFi TX device.

To determine the range, i.e. the maximum distance at which the tag is able to decode data with extremely low BER, we locate the tag at different distances , d, from the WiFi TX device in 1 meter steps. The nodes were placed in a long 24 meter hallway. At each location, we measure the BER the same way as we did in the Sensitivity experiment. Note that the same setup and measurement procedure can be done for the WiFi-ED receiver, too.



(a) Experimental Setup.



(b) BER vs distance.

Figure 4.8: MIXIQ 's range vs. WiFi-ED.

Figure 4.8(b) shows the experimental results. We see that in the LoS scenario, WiFi-ED can successfully decode at only 2–3 meters away from the WiFi TX device whereas MIXIQ is able to decode the data bits with zero or near-zero BER across all the distances (1–24 meters). Thus, Figure 4.8(b) shows that MIXIQ has at least 10× higher range than WiFi-ED although this may be even larger since MIXIQ 's BER is still low at the end of the

hallway.

4.8.2 MIXIQ Power Benchmarks

Table 4.2 shows the breakdown of power consumption of various parts of MIXIQ 's PCB prototype and also provides, as reference, expected numbers if such a system were to be implemented in ASIC.

Component	PCB prototype	ASIC
Amplifiers	132.9μW	29.6μW
ADC	184.3μW	1.9μW
IQ demodulator	47.4μW	9.3μW
Total	**364.6μW**	**40.8μW**

Table 4.2: MIXIQ's power consumption: (PCB vs. ASIC).

While the values in Table 4.2 shows power consumption when the receiver is in data modulation mode without performing any other task, we note that the CPLD used in the digital demodulator design has enough resources remaining for also doing gain control, power management, and other tasks. Unlike data reception, these other tasks do not happen very frequently and also require only a few μA from the power supply of the CPLD. Therefore, their overall contribution to the average power consumption is negligible.

We see that the overall consumption of our PCB-based implementation is 364.6μW and the power consumed by the ASIC version is 40.8μW. Rhe achievable bitrate is 1.125Mbps which translates to 3248 bits/μJ and 27,573 bits/μJ for MIXIQ 's PCB prototype and ASIC designs, respectively.

For the ASIC design, the power consumption of all blocks reduces with respect to their PCB counterparts; but the most significant reduction happens to the ADC; ADC's power consumption reduces by 100$\times$ compared to the discrete part mounted on the PCB. This results from an ADC power optimization technique called *charge distribution* that

we borrow from recent work on ultra low power ADC [128] which allows us to design a high-resolution yet ultra low power ADC.

Thus, we see that MIXIQ provides much improved performance while sacrificing a small amount of energy efficiency in the process. While 0.3mW power consumption is greater than what may be acceptable to an RFID tag, it is acceptable for an ultra-low power receiver on an active backscatter-based system.

4.8.2.1 How does MIXIQ compare to state-of-the-art IC-based envelope detector designs?

Table 4.3 lists the performance of prominent state-of-art enhanced ED IC designs that can directly receive data from standard WiFi devices. As expected, these designs mostly outperform MIXIQ in terms of receive sensitivity — they achieve better than -70dBm sensitivity while MIXIQ provides -52dBm (the -52dBm sensitivity is still a $>$ 25dB improvement of a PCB prototyped WiFi-ED). However, our proposed design has two important benefits over other efforts. First, it boosts spectral efficiency by $5\times - 50\times$ compared to other designs which can result in better bandwidth usage. Second, as we have described, our design can be easily prototyped using off-the-shelf components. Thus, MIXIQ bridges the gaps between uplink and downlink performance of an easy-to-prototype backscaatter tag.

4.8.3 Impact of MIXIQ's Design Choices

Now, we validate the effect of MIXIQ's design choices and their contribution to its overall performance.

Comparison between 0,1,2 - stage amplifiers. Figure 4.9 compares the sensitivity for different modulation schemes (and consequently different bitrates) when we choose different amplifier pipelines. The result is obtained by repeating the sensitivity experiment of Section 8.1. for 0, 1, and 2 amplifiers and WiFi TX. We see two interesting observations. First, using

Work	WiFi standard	Modulation	Sensitivity (dBm)	Spectral Eff. (bps/kHz)	Energy Eff. (bits/μJ)	PCB prototype
[43] (2017)	802.11a (5.8GHz)	FSK	-67, -70	11, 1.4	746, 93	No
[8] (2018)	802.11g/n (2.4GHz)	OOK	-72	2.8	659	No
[44] (2019)	802.11ba (5.8GHz)	OOK	-83	2.8	285	No
[137] (2020)	802.11b (2.4GHz)	OOK	-42.5	0.3	2286	No
MIXIQ (2021)	802.11ax (2.4GHz)	64-QAM	-52	51	3248(PCB), 27573(IC)	Yes

Table 4.3: Comparison of MIXIQ against state-of-the-art IC-based Envelope Detector designs.

a two-stage amplifier (as in MIXIQ) significantly improves the sensitivity and thus we can achieve a sensitivity of -52dBm for 64-QAM. Second, there is not a significant sensitivity difference between 1-stage and 2-stage for low order modulations, especially BPSK. The reason is that when the RSS < -55dBm, the passive rectifier is operating close to its physical limits and stops converting the signal; hence, irrespective of the amount of amplification (1 or 2 stages), we are unable to improve sensitivity to below -55dBm. Consequently, *the sensitivity for different modulations are approximately the same when using a two-stage amplifier*.

Effect of number of subcarriers Figure 4.11 shows the energy efficiency (bit/μJ) versus the number of subcarriers when we use the same architecture of MIXIQ but at different sampling rates to demodulate the sub-carriers. *We see that three sub-carriers results in the highest efficiency of around 3000 bits/*μJ; performance rapidly degrades thereafter due to the higher sampling rates needed to perform IQ demodulation. Note that the power consumption of the amplifier remains the same as we are still in sub-MHz regime and leverage the benefits

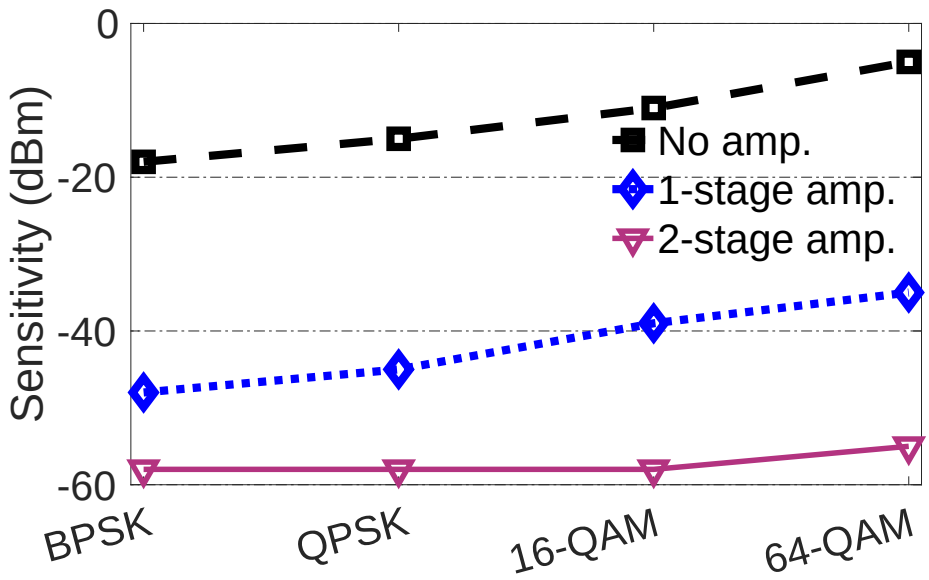
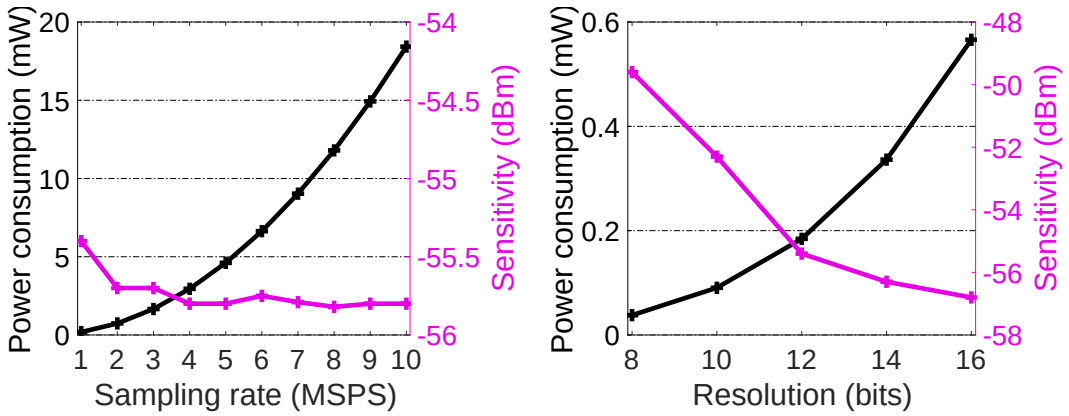


Figure 4.9: Sensitivity of different amplifier pipelines.

of the μW amplifiers (§4.5.1). Hence, the sensitivity remains the same across the number of subcarriers in Figure 4.11.

Rationale for choice of subcarriers. To understand which data sub-carriers provide best performance, we look at the extent of inter-modulation and residual terms that exist at different data sub-carriers in Figure 4.12. We generate random data bits at the sub-carriers and measure the signal to inter-modulation interference ratio (SIR, Fig. 4.12(a)) and signal to residual terms ratio (SRR, Fig. 4.12(b)) at the output of MIXIQ 's demodulator. This experiment is done by placing the WiFi Tx and MIXIQ antennas 1 meters away from each other, and with the WiFi TX device transmitting WiFi packets at 17dBm. It can be observed that for subcarriers -13,-12,-11 both SIR and SRR are sufficiently above 25dB allowing for 64-QAM modulations. Subcarrier -10 has a very good SIR as it is far from the inter-modulation terms; however, it suffers from residual terms are still large and therefore the overall ratio between the signal and the unwanted terms (inter-modulation and residual terms) is <25dB. Thus, *the three sub-carriers -13, -12, and -11 offer good robustness against both inter-modulation and residual impacts and form the rationale behind MIXIQ 's choice of data sub-carriers.* For brevity, we do not include results for different distances between TX and RX. MIXIQ shows the same behavior across different distances except when the tag

is very close (<20cm) to the TX device in which case non-linear distortions at the output of the rectifier overwhelm the modulator.



(a) Sampling rate (b) Resolution

Figure 4.10: Sensitivity/power vs. ADC specs.

Effect of ADC sampling rate and resolution: Figure 4.10 captures ADC's performance and sensitivity as a function of its resolution and sampling rate. Increasing the sampling rate as well as the resolution of the ADC, boosts decoding sensitivity, but is also accompanied by a rapid increase in power consumption and whereas slight improvement in sensitivity. *MIXIQ strikes a balance between the sensitivity and power consumption to operate the ADC at 12-bit resolution and 1 MSPS.*

4.8.4 Co-existence with other WiFi devices

We now capture MIXIQ's robustness to other WiFi clients that transmit in other resource units of the 802.11ax WiFi channel in parallel. Figure 4.13 shows our experimental setup. We used two IPQ6010-based devices, one as MIXIQ's (original) TX and one as the interfering TX (another WiFi client), at distances d_1 and d_2 from MIXIQ's RX, respectively. We conducted this experiment in a 6m$\times$6m space in our hardware lab. The original TX transmits based on MIXIQ's signaling (wherein only three data sub-carriers are used and the rest are null), while the interfering TX transmits over the entire resource unit it is using, both with the same transmit power of 17dBm. Now, at different d_1 and d_2, we capture the output of the

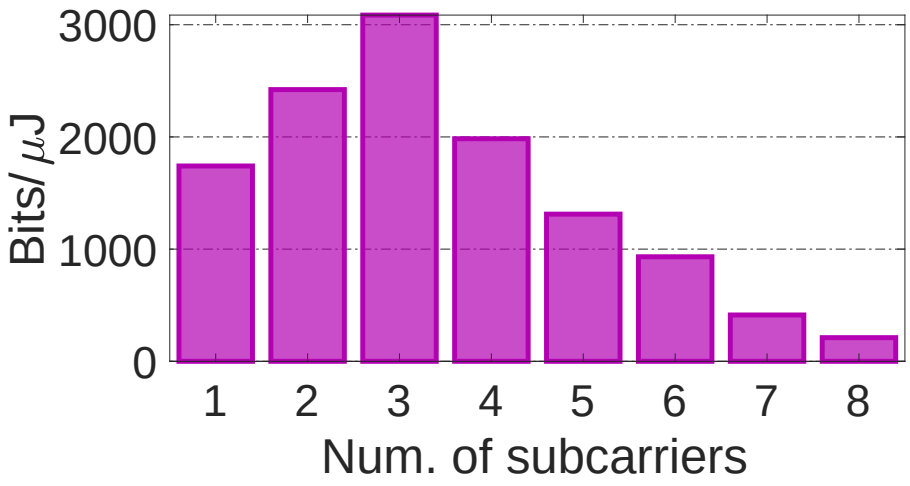
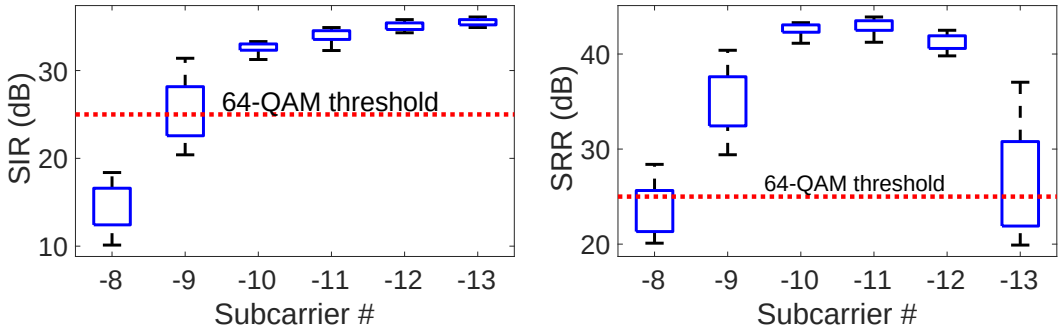


Figure 4.11: Bits/μJ vs. number of subcarriers.



(a) SIR

(b) SRR

Figure 4.12: SIR and SRR across data subcarriers.

digital IQ demodulator at the three data subcarriers and calculate the minimum SINR among these three subcarriers. Figure 4.13 shows the heat-map of the SINR for different distances. It is observed that when the interfering TX is 3m or more away from RX, the SINR is >25dB (original TX is 3m or closer to RX), thereby allowing for 64-QAM demodulation; while lower order modulations such as 16-QAM should be possible at farther distances. *MIXIQ's potential for co-existence, opens the door for improved (aggregate) network throughputs in the future.*

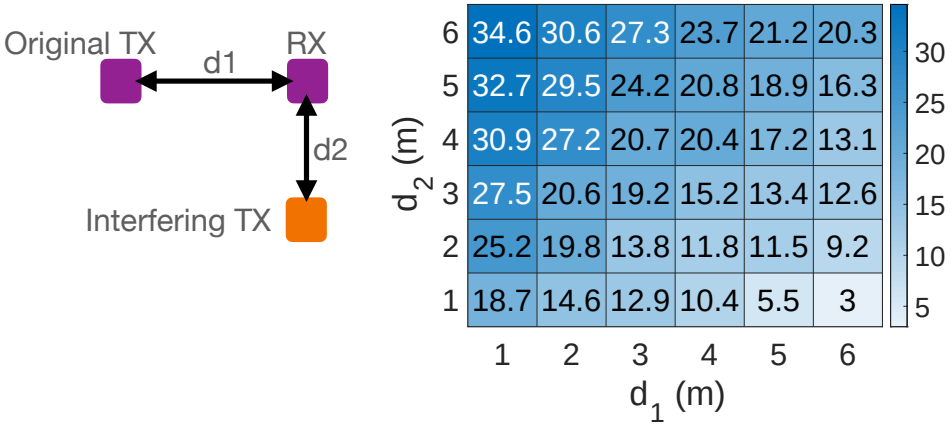


Figure 4.13: SINR at different locations.

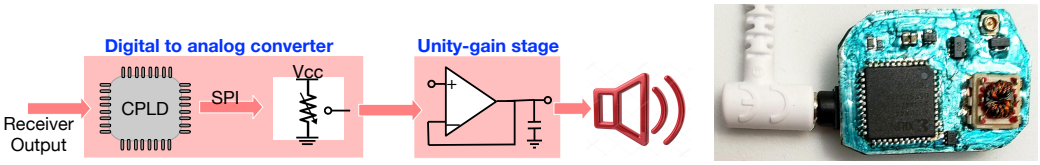
4.8.5 Ultra-low Power Audio Streaming

An enhanced ultra-low power receiver can benefit any IoT or wearable application where downlink overhead is non-trivial. We evaluate the use of MIXIQ in one such application, audio streaming to a Hearable device like an earphone.

We show the benefits of a better receiver using a novel WiFi-based VoIP or audio streaming prototype that uses MIXIQ achieve better performance. We consider a WiFi TX device (IPQ6010 evaluation board) that is transmitting the VoIP signal (or a music stream) with an audio quality of 128 Kbps at 17dBm. Our goal is to investigate the quality of the audio received with MIXIQ's receiver and compare it with that of WiFi-ED.

Digital audio player (DAP): Figure 4.14 shows the design of our low power digital audio player (connected via a 3.5mm jack connector to the radio) that mimics a simple version of a hearable. While the audio front-end is not our innovation, a full system prototype allows us to holistically evaluate performance. It consists of a TPL0501-100DCNR[123] ultra low power digital potentiometer for converting the received 8-bit audio samples to analog values. The logic resources of the CPLD of the receiver are also used to communicate with the digital potentiometer through SPI protocol. Since the analog output of the potentiometer varies between 0 and V_p (Figure 4.14), the magnitude of the signal and hence the volume

of the voice being played depends on how big V_p is. To isolate the high impedance of the digital potentiometer (100kΩ) and the low impedance of speaker (64 Ω), we use a unity gain stage consisting of a LPV511MG[118] ultra low power op-amp.



(a) Block diagram (b) Prototype

Figure 4.14: Ultra low power digital audio player.

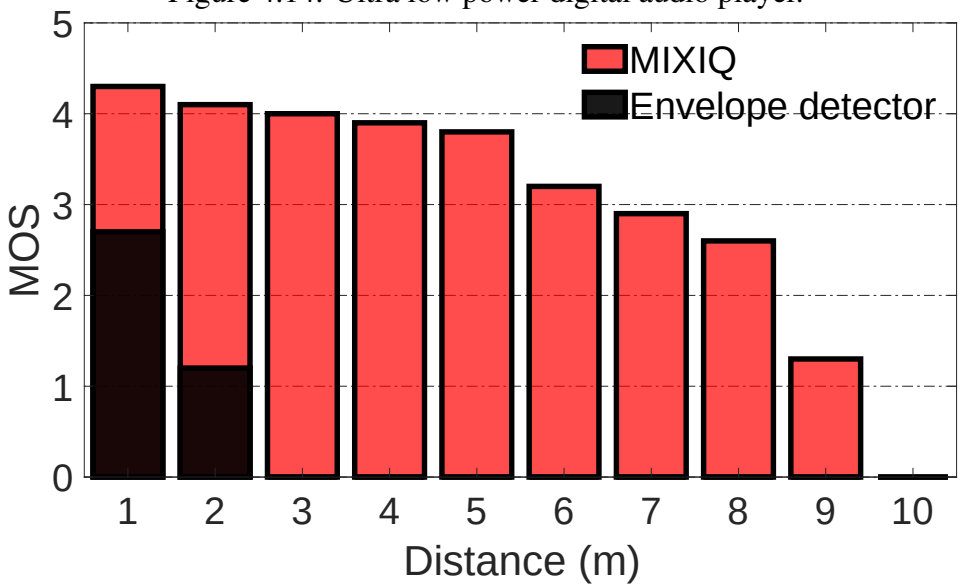


Figure 4.15: MOS vs. distance.

Performance: Figure 4.15 shows the results when the WiFi TX (IPQ6010 evaluation baord) transmits bits of audio on top of 802.11ax according to MIXIQ's signaling (data+helper) with an 17dBm transmit power. The WiFi TX device is at different distances from the wireless earphone (i.e. our DAP) worn by a person who is doing body movements according to a known pattern for 5 minutes at each point of the hallway next to the lab where the receiver is placed (same experimental setup as §4.8.1), except that the tag is worn by a person rather than being static in the Line of Sight).

We see that MIXIQ has good MOS scores (> 3) when the IPQ6010 evaluation board is < 7m since signal strength of the data is fairly good, but slightly degrades to a little

below 3 MOS scores when the IPQ6010 evaluation board is 6–10 meters. Finally, the quality drops quite a bit at 10-11 meters until MOS can no longer be measured at 12m, as there is a lot of noise in the audio. On the other hand, the WiFi-ED fails to deliver good quality audio even at 1 meter and MOS cannot be measured even at >2m, when it delivers just noise. *This 10× increase in operational range can be attributed to MIXIQ 's improved sensitivity even at higher data rates.* Note that the results of this experiment show lower operational range than the range experiment done in §4.8.1 despite having the same experimental setup. This is due to human body effects that introduce additional signal loss and thus limit the range.

4.9 Discussions and Limitations

In this paper, we tackle the long-standing problem of designing better ultra low power receivers. We present a new architecture, MIXIQ , that builds on the idea of an external oscillator-based mixer and synergistically complements it with a novel hybrid baseband pipeline. That enables dramatic improvements in both sensitivity and spectral efficiency, while operating in the μW power regime. MIXIQ is compatible with WiFi radios via a novel signaling method that leverages OFDMA for generating the external oscillator signal. Our results show that very interesting on-body applications can be made possible by having an ultra low power radio that can deliver a superior energy-efficient downlink performance.

Our work can be improved in a number of ways that we are continuing to explore. MIXIQ 's bit rate is currently limited to 1.1Mbps, which can be low in scenarios where multiple nodes want to receive high-rate data simultaneously without occupying the WiFi network traffic too much. Our current design is also limited in its ability to work in the presence of multiple concurrent WiFi devices which will interfere with the downlink transmissions. Finally, we show that we can support a limited level of concurrency (three nodes) but this can be improved to support more tags. In future work, we are looking at new signaling and multiplexing techniques that can build on MIXIQ to tackle these problems.

4.10 Related Work

Ultra low power receivers: There has been considerable work on improving the performance of envelope detectors and ultra low power receivers. An important category is wake-up radios with boosted sensitivity (better than -70 dBm) at ultra low power consumption (<100 μW). The focus of wake up radios is primarily on sensitivity and low power and not spectral efficiency. Hence they are typically designed for very low bit rates (a few kbps or less), which makes them suitable primarily for wake-up applications [136, 42, 81, 103, 100]. However, newer efforts in the field of RF IC design achieve up to tens of Kbps at a higher sensitivity of -70dBm to -97dBm. While some of these designs need specialized transmitter and carriers [89, 83, 108, 103], there are also several recent ultra low power radio designs that can directly receive OOK, FSK, or QPSK signals emulated on standard WiFi packets [44, 8, 43, 137], which makes them compliant with commodity WiFi networks while achieving up to -80dBm and 62.5kbps bitrate at μW regime. A key distinction between these and our work is that ours is easier to prototype and does not rely on a specialized ASIC to achieve our gains.

Backscatter research: There has been a large volume of work focused on frequency-shifted backscatter with commodity devices. Among these, some use analog elements like tunnel diodes [130, 9] and impedance transformers [102] to generate and/or amplify the backscattered signal. Our work is significantly different in that we leverage such analog elements in the receiver design rather than in the transmitter.

The use of a helper signal for backscatter transmission is quite common (and referred to as bi-static backscatter). These are often used to enable a backscatter transmitter to talk to a commodity radio such as WiFi AP or Bluetooth radio [146, 145, 144, 53, 48, 148, 86, 141, 117, 134]. Their focus is on the transmitter whereas we bring to bear the ideas in the context of an ultra-low power receiver that can receive from a commodity WiFi radio.

External-helper tone receivers: Our work is related to recent receiver designs

that use an external helper tone to convert envelope detectors to mixers [87, 28]. However, these works focus primarily on enabling IQ detection, without improving sensitivity, spectral efficiency, or power consumption. In addition, these methods require a separate device to generate the external helper tone whereas we can leverage 802.11ax to achieve this goal. MIXIQ provides a complete design that significantly improves all aspects of the energy-performance tradeoff, while working with commodity WiFi devices.

Chapter 5

Radio Polymorphism

Duty-cycling has emerged as the predominant method for optimizing power consumption of low-power radios, particularly for sensors that transmit sporadically in small bursts. But duty-cycling is a poor fit for applications involving high-rate sensor data from wearable sensors such as IMUs, microphones, and imagers that need to stream data to the cloud to execute sophisticated machine learning models.

We argue that there is significant room to optimize low-power radios if we can take advantage of channel dynamics in short-range settings. However, we face challenges in designing radios that are both efficient at power levels between μWs and mWs to take advantage of periods of good signal strength and nimble to deal with highly dynamic channels resulting from body movements. To achieve this, we propose radio polymorphism, a radio architecture with tightly integrated passive and active components that allows us to turn high channel dynamics to our advantage. We leverage passive modes in myriad ways within the network stack, from minimizing data transfer and control overheads to improving rate selection and enabling channel-aware opportunistic transmission. We instantiate our design in a full hardware-software prototype, Morpho , and demonstrate up to an order of improvement in efficiency across diverse scenarios and applications.

5.1 Introduction

Duty-cycling has emerged as the predominant method for optimizing power consumption of low-power radios. For example, Bluetooth LE is an optimization of the Bluetooth standard that enables rapid connection establishment, transmission of a short burst of information, and rapid disconnection. This rapid transition time makes it possible to mask the power consumed during active operation of the radio, which is milliwatts compared to microwatts in sleep mode. As a result, duty-cycled radios like Bluetooth LE and Zigbee have become the preferred choice for sensors that transmit sporadically in small bursts, for example, home temperature monitoring, location beacons, security alarms, humidity sensors, and other similar IoT devices.

But duty-cycling is insufficient for applications involving high-rate sensor data from IMUs, ECG, microphones, and imagers, that are used in wearable and tactile computing applications. The signals from these devices are noisy and complex which makes data interpretation a significant challenge [97]. To address this problem, we often need sophisticated machine learning techniques that are more complex than what we can execute locally and require computational resources in the cloud. The end result is a growing need for low-power radios that can support continuous streaming rather than transfer in short, intermittent bursts.

This trend has significant consequences from a power perspective. Normally, we would expect high-rate sensors to be the bottleneck in terms of power consumption but this has changed in recent years. For example, state-of-art low-power microphones, cameras, IMUs and ECG chips in the market consume between tens of microwatts and a few milliwatts for continuous sampling [132, 39, 18, 66]. But streaming communication has not kept pace with sensor developments — active mode power consumption of low-power radios is around ten milliwatts, which is an order of magnitude higher than the sensors. Continuous streaming of sensor data for real-time applications means that the radio needs to wake up frequently and cannot batch data before transmission. In these regimes, the

prevailing wisdom of using duty-cycling to judiciously use the radio is ineffective.

We argue that there is significant room to optimize low-power radios if we can take advantage of channel dynamics, particularly in short-range settings. To achieve this, we face two challenges: first, we need to adapt to highly dynamic channels resulting from body movements and second, we need radios that can efficiently operate between μW and mW power consumption to take advantage of channel variations. To achieve this, we propose a new design paradigm, radio polymorphism, which tightly integrates passive and active components with fast switching across them, allowing us to turn high channel dynamics from being a disability to a strength. We leverage passive modes in myriad ways within the network stack, from minimizing data transfer and control overheads to improving rate selection and enabling channel-aware opportunistic transmission. We instantiate our design in a full hardware-software prototype, Morpho , and demonstrate an order of improvement in efficiency across diverse scenarios and applications.

Radio polymorphism: In this paper, we argue that there is significant room for optimization in the form of large gaps between received signal strength and receiver sensitivity. But these gaps often occur at extremely low power levels, and existing radio-level methods like transmit power control are too inefficient in these regimes. The problem is exacerbated by the highly dynamic nature of wireless channels from wearable peripherals due to body blockage and mobility. Thus, an ideal radio needs to be opportunistic and take advantage of gaps between signal strength and receive sensitivity while also being nimble and reacting quickly to channel degradation.

We argue for a new architectural paradigm for low-power radios, radio polymorphism, that tightly integrates active radio components like oscillators and active amplifiers with passive radio components like backscatter reflectors and envelope detectors. The key advantage of passive components is that they use extremely simple circuit components thereby allowing them to scale down power consumption to the microwatt regime. But compared to their active counterparts, passive radios suffer from lower signal strength, higher signal dynamics, and lower receive sensitivity. In other words, active radios are

robust but inefficient whereas passive radios are efficient but fickle. The central challenge that we face is integrating active and passive radio components to accentuate their positives and mask their negatives.

To address this challenge, we take a step back and look holistically at integrating active and passive components while balancing energy-efficiency and robustness. Surprisingly, we find that there are several ways to approach the problem — passive components can be used for minimizing data transfer and control overheads, improving active bitrate selection, and enabling channel-aware transmissions, each leading to different ways of optimizing the overall system.

We put these ideas together in our instantiation of a polymorphic radio, Morpho , and extensively evaluate the benefits of the radio using benchmarks and trace-driven simulations. We also demonstrate the benefits of Morpho in two compelling application case studies: a) Morpho -enabled wearable eye tracking where we combine the radio with the iShadow eye tracker [67] to optimize gaze tracking performance without increasing the overall power budget, and b) Morpho -enabled audio streaming to optimize energy-efficiency without sacrificing audio quality.

Our work is distinct from a long line of work in multi-radio wireless communication. Most existing work does not specifically target the ultra-low power radio regime and generally looks at integrating WiFi, Bluetooth, LTE and other commercial radios at the MAC and transport layers. A small body of work has explored the integration of passive components in active radios but for specialized purposes like wakeup radios and power offload [99, 40]. There have been only preliminary efforts to design radios that truly integrate active and passive components [98, 47], and none that attempt to design the entire stack from hardware to application layers. Our work is a deep dive into this topic and unifies active and passive components across all layers of a wireless network stack.

In summary, our work has several contributions:

The work that is closest to ours is a recent effort to integrate an active BLE

transceiver and a passive WISP tag [47]. While the high-level idea is similar, we show that BLE-WISP integration is simply not nimble enough to allow us to take advantage of the multitude of possibilities with active-passive integration. We take a deeper dive in this paper, and re-think hardware, MAC and application layers to take advantage of active-passive radios.

- We present Morpho , a clean-slate re-design of ultra-low power radios that integrates active and passive components such that the modules operate in unison. Such a design combined with the ability to switch between modes in tens of microseconds allows us to optimize data transfer and control efficiency even under highly dynamic channel conditions.
- We show that Morpho provides 3.8× to 9× improvement in energy efficiency over active radios without compromising reliability under high channel dynamics that is typical in mobile and wearable scenarios.
- We show that Morpho can improve application-layer performance with two examples, a video-based wearable eye tracker where accuracy improves by 3× to 5× for a fixed energy budget, and an audio streaming application where energy efficiency improves by 5.8× – 10× while minimally sacrificing audio quality.

5.2 Case for Morpho

The primary opportunity to save power in low-power radios stems from the fact that communication is often short range i.e. within a few meters, whereas low-power radios are often provisioned to operate at ranges of a few tens of meters. This leads to a significant gap between received signal strength and receiver sensitivity that can be leveraged to save power.

Figure 5.1 illustrates this gap. The blue line corresponds to the RSS when a wrist-worn sensor is communicating with a proximate base-station via Bluetooth while a user is performing various gestures. The red dotted line shows the sensitivity of a typical Bluetooth receiver i.e. the lowest power level at which the receiver can detect an RF

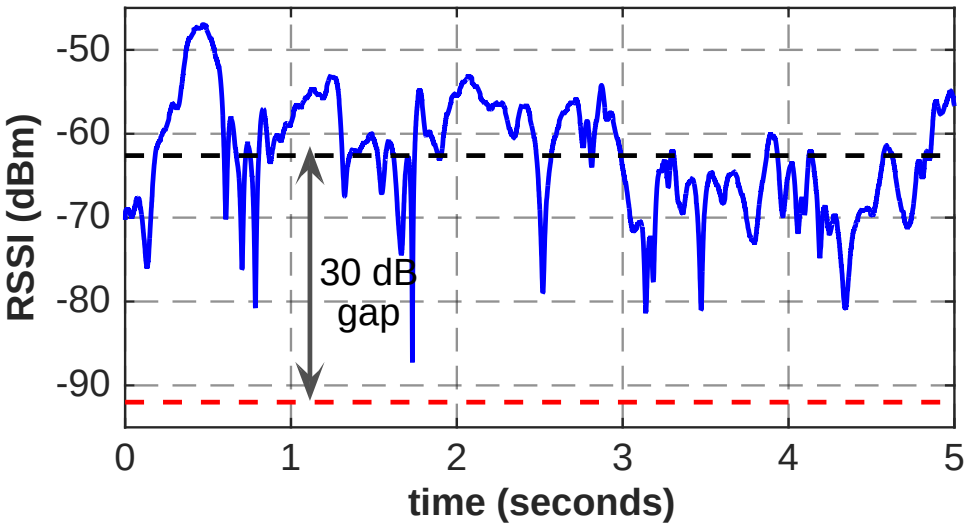


Figure 5.1: Gap between RSS and Rx sensitivity during short-range communication between a smartwatch and access point via Bluetooth @ 0dBm output power.

signal and demodulate data. In general, the receive sensitivity depends on thermal noise given the channel bandwidth, the noise added by receiver electronics, and the required signal to noise ratio for the modulation scheme being used. In the case of Bluetooth, the thermal noise is -114 dBm for a 1 MHz channel [91] and the receive sensitivity is around -96 dBm at 1 Mbps [79]. As a result, in short range settings, the signal strength is often about 35 dB higher than receive sensitivity.

5.2.1 Leveraging the RSS-Sensitivity Gap

Thus, we often have a dramatic 30-40 dB gap between the received signal and the receiver sensitivity, but can we convert the opportunity into comparable power savings? There are two potential designs that can leverage this gap — transmit power adaptation and radio duty-cycling.

Transmit softly: Transmit power adaptation essentially involves reducing power consumption by dropping the output power of the transmitter so that the RSS becomes closer to the noise floor of the receiver. However, this does not lead to proportional power savings since the baseline operation of a low-power radio is already at a very

low power level. For example, when a typical low-power radio transmits at 0dBm (i.e. output power of 1mW), the RF analog circuit consumes only around 5-10mW. If we wanted to reduce the output power from 0dBm to -30dBm (i.e. 1mW to 1μW) to take advantage of the gap, then we would need the RF analog circuit to operate at 10μW to achieve proportional power savings. But this is not possible due to the constant overheads of the active elements in a radio. In fact, the oscillator alone in a low-power radio consumes a few hundred microwatts, so power efficiency would be less than 1% when the output power is 1 μW [31]. Any other active elements like active mixers would only add to this overhead. Some of this inefficiency is apparent when we measure commercial low-power radios. For example, the Nordic nRF52840 BLE chip [79] draws 4.8mA when the transmit power level is 0 dBm and 2.3 mA at -40 dBm i.e. a 50% reduction in current draw for a four orders of magnitude reduction in transmit power. Thus, the fixed costs of a low-power radio swamp any gains that can be achieved by reducing transmit power.

Transmit rapidly: Radio duty-cycling involves transmitting at as high a bitrate as possible and saving energy by sleeping for longer. A higher speed PHY achieves lower power consumption (given that the same amount of data is transferred) since the radio-on time is reduced without changing transmit power. This is the approach used by virtually all low-power IoT radios. For example, BLE is typically configured to operate at either 1 Mbps or 2 Mbps to reduce power consumption.

But duty-cycling has two side-effects. The first is that the radio has no visibility into channel variations during radio-off periods. This means that mechanisms like rate adaptation are less effective in a duty-cycled radio since the channel may have changed since the last radio-on period. As a result, bitrates are often set to a fixed value in duty-cycled radios. The second is that constant overheads are significant for each wakeup. For example, a typical BLE radio goes through several stages during each wakeup cycle including MCU wakeup and shutdown, BLE protocol stack preparations and processing, and the radio on-off transitions [51]. The actual data transmission consumes only a fraction of the overall energy during each wakeup. These constant overheads can be masked if the messages are infrequent as is the case with BLE or

when we can batch data to amortize the overheads. But they cannot be masked when streaming sensor data to the edge cloud. For example, real-time streaming of data from a microphone to an edge cloud (8 kHz sampling rate @ 16 bits/sample) via a 2 MHz Bluetooth radio would involve thousands of wakeups per second.

5.2.2 The Morpho Approach

We propose a new design paradigm that combines active radio architectures (i.e. RF oscillators, I/Q receivers, active mixers, power amplifiers, and low-noise amplifiers) with passive radio architectures (i.e. backscatter transmitters and envelope detectors). Such a design allows us to tackle the above issues in two ways. First, the constant overheads are a non-issue for passive radio architectures which do not have active components. Second, passive transmitters and receivers can operate in always-on mode and do not have to be duty-cycled since there is virtually no energy cost to using them. These advantages open up new possibilities in terms of how we can design low-power streaming radios.

But passive radios present a number of challenges that make it non-trivial to design an integrated active-passive architecture. In the case of a passive transmitter (i.e. backscatter), the main issue is substantially higher path-loss. Since the backscatter signal has to traverse the forward path and the reverse path, the attenuation is exponentially greater than an active radio where the signal only needs to traverse the forward path. In effect, this is a double-whammy since the signal average is considerably lower than an active radio, and the signal dynamics is a considerably exaggerated version as that for an active radio. The challenge is not limited to the transmitter — a passive receiver (envelope detector) also presents problems since its sensitivity is often considerably lower than an active receiver. Thus, when we integrate these two vastly different radio architectures, we need to carefully consider how we accentuate their positives and mask their idiosyncrasies in-order to improve performance.

Morpho presents a unification of active and passive modules into a single radio that transparently switches across these modules to optimize energy-efficiency without los-

ing robustness. The application is agnostic to the manner in which Morpho switches between modules even when it includes rapid transitions needed to handle highly dynamic channels that are typical in mobile situations. Our vision is to enable a deep stack integration, where the physical layer, protocol layer, and application layer are all re-architected to squeeze the most out of opportunities to use passive radio modes without sacrificing the intrinsic robustness of low-power active radios.

5.3 Design Rationale & Key Insights

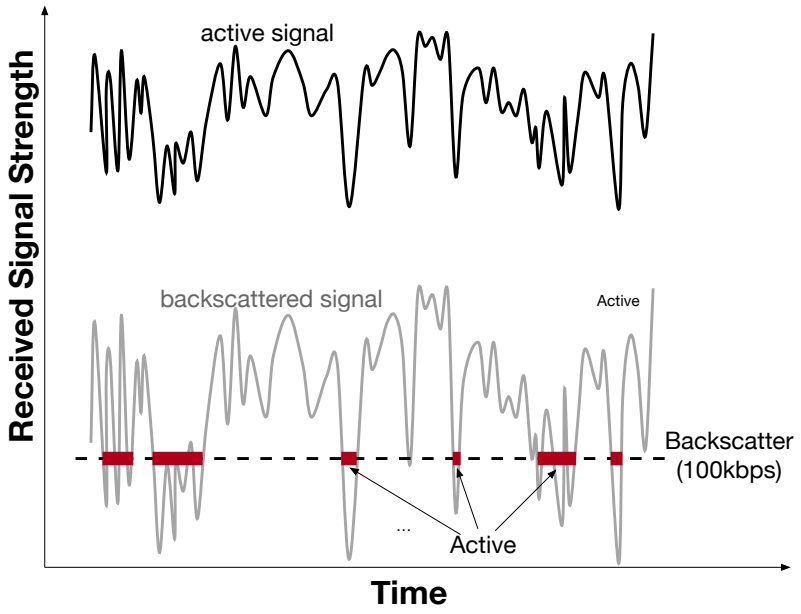
How should we combine active and passive modes to design a unified radio? When considering the answer to this question, we found that there are two distinct approaches to unify the two modes. We describe these approaches in this section.

5.3.1 Active-Assisted Passive

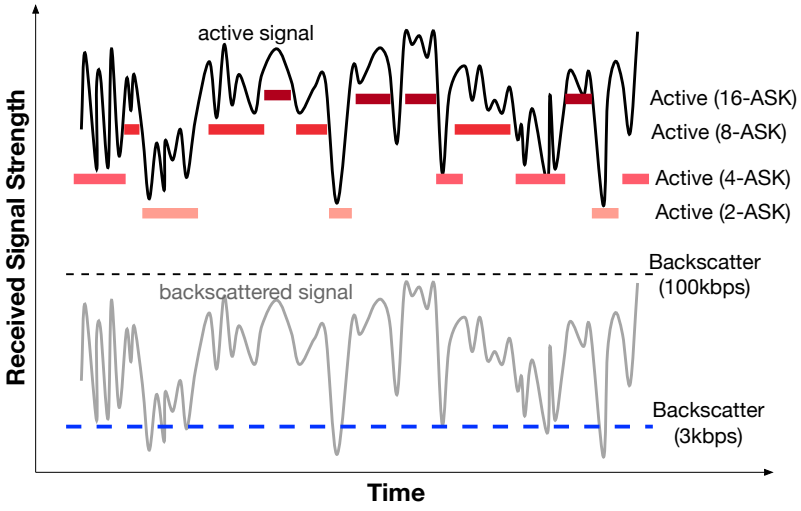
The first method for combining active and passive modes is somewhat evident — use the passive mode whenever available for data transfer since it has better energy-efficiency and use the active mode to smooth out periods when the passive mode is flaky. We refer to this mode as *active-assisted passive* since passive is the preferred data transfer mode and active is backing it up by filling connectivity gaps.

Let us first consider the case of a peripheral (e.g. IoT sensor) transmitting to a central station (e.g. access point) via a polymorphic radio. Here, the choice is between transmitting via a (passive) backscatter transmitter or via an (active) I/Q transmitter. This scenario is shown in Figure 5.2(a) — the bold line is the active signal strength and the grey line is the backscatter version of the same signal. The dotted horizontal line represents the receive sensitivity at a desired data rate, 100kbps in this example. The backscatter signal has lower RSS and higher signal variation compared to the active signal, but despite this the signal is mostly above the receiver sensitivity and can be decoded. In this case, backscatter can be used for data transmission most of the time with active being used as backup whenever the backscatter signal strength

goes below the receive sensitivity.



(a) Active-assisted Backscatter



(b) Backscatter-assisted Active

Figure 5.2: Morpho 's modes of operation.

We note that there are several parameters that can be tuned to change the operating region shown in the figure. The first is the carrier signal power from the central station. The second is the acceptable bitrate — the receive sensitivity line in Figure 5.2(a) can be lowered if the acceptable bitrate for the passive mode is less than the stated 100 kbps figure.

This approach is equally applicable to the case of a peripheral receiving data from the central station. Here, the peripheral has to decide whether to use the (passive) envelope detector or to use an (active) I/Q detector. In an active-assisted passive approach, the peripheral uses the passive mode whenever the received signal is strong enough to use the passive envelope detector as the primary receiver, and the active mode kicks in when the signal falls below the sensitivity of the passive receiver (at the desired bitrate).

5.3.2 Passive-assisted Active

While active-assisted passive is ideal under conditions where the passive modes offer sufficient throughput, there are often conditions where bitrate offered by the passive mode is too low. For example, when active RSS is -65 dBm, the corresponding active bitrate for 16-QAM modulation is 4 Mbps whereas the corresponding backscatter bitrate would be $\sim$5 kbps. Thus, there are often scenarios where the difference in throughput between active and passive mode is too high for active-assisted passive to be practical. The question we ask is whether we can still leverage the passive modes to improve performance in these situations.

Our main insight is that even though backscatter may be impractical for supporting data transfer, it can still be useful for *channel measurement* at extremely low bitrates. Let us again consider the case of a peripheral transmitting to a central station via a polymorphic radio. In order to measure the channel, a short training sequence of a few bits can be transmitted, and the RSS estimated by obtaining the correlation between the received signal and the training sequence. Since the training sequence can be as short as a few bits, the backscatter bitrate can be as low as a few kilobits/second which can allow it to operate at longer distances (e.g. 75 m @ 2.9 kbps [129]). Figure 5.2(b) illustrates this idea — the grey line corresponding to backscatter RSS is below the receive sensitivity when operating at 100 kbps but mostly higher than the sensitivity when transmitting at 3 kbps.

The central benefit of being able to use backscatter for channel measurement is

enhanced visibility into the channel at near-zero power consumption. The additional visibility allows us to be more judicious about use of the active radio in two ways: a) we can select the best bitrate for the active radio even after a long sleep gap, and b) we can select the best times to wakeup the active radio by choosing times when the RSS is strongest. The figure shows these advantages — by leveraging backscatter for channel visibility, we can choose the best active bitrates (the line-segments) and the best times for active transmission (the peaks).

We note that this approach does not directly translate to the scenario where the peripheral is receiving data from the central station. This is because an envelope detector does not provide signal strength information, so cannot be used for channel measurement. Therefore, we use passive-assisted active solely for uplink transmission from the peripheral to the central station.

5.4 Morpho PHY Layer

The main challenge at the PHY layer is how to seamlessly integrate passive and active radio components so that they can transparently switch between various modes without the application perceiving the switching behavior. To accomplish this, we design the Morpho hardware to enable rapid and seamless switching.

To illustrate the need for a new design, we start with a strawman solution for an active-passive radio that simply connects an active radio like BLE together with a passive radio (e.g. WISP), and switches between these two as needed (similar to BLISP [47]).

Such a design is inefficient due to the lack of configurability. Virtually all radio ICs have the TX and RX components tied together, and do not provide us the freedom to mix-and-match different possibilities. For example, low-power active radios like BLE turn on both the TX and RX components when they switch on from sleep mode since they assume that active-mode ACKs will follow the data packet. In addition, most commercial radios incur setup delays upon receiving a command, which makes it difficult to rapidly switch between the different modes. In contrast, our goal is to

have the freedom to rapidly switch between all four combinations of passive rx/tx and active rx/tx.

5.4.1 Morpho Sensor Architecture

Morpho is designed for one-hop asymmetric settings where the peripheral (e.g. IoT sensor or mobile accessory) is resource-constrained whereas the central station (e.g. access point or edge cloud) is resource-rich. We first describe the radio architecture on the peripheral shown in Figure 5.3 (upper block).

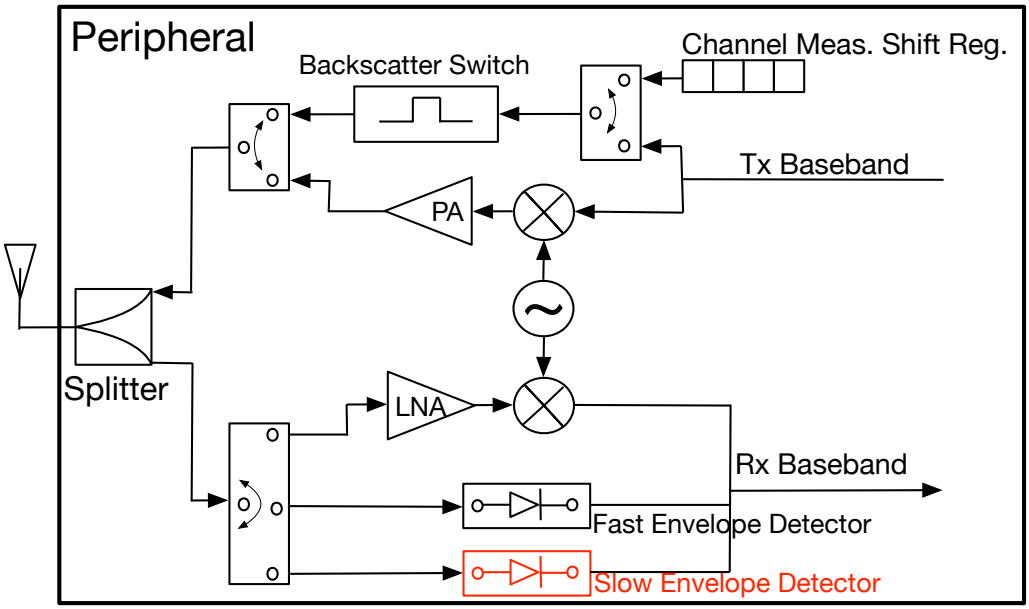


Figure 5.3: The building blocks of Morpho hardware.

Morpho TX: The Morpho transmitter is equipped with an ultra-low power RF oscillator that shares the antenna path with a backscatter transmitter allowing us to turn on the oscillator and send data in an on-demand manner without incurring additional overheads.

The figure also shows the channel measurement circuit for the backscatter-assisted active mode. Channel measurement using low-rate backscatter can be implemented as a simple shift register in hardware since a fixed set of bits are backscattered each time to measure the channel. This makes it extremely low power (similar to an RFID tag)

since it avoids the overhead of waking up the MCU.

Morpho RX: On the receiver end, the radio has a switch between an envelope detector receiver and an active ASK receiver (which shares the oscillator used by active transmitter). One notable design issue that we encountered was that the envelope detector receiver needs to be tuned to specific bitrates (and consequently operating ranges) — high bitrates need low RC constants and long ranges need high RC constants. This is different from a backscatter transmitter which can transmit at different rates simply by toggling the RF transistor at different speeds. Thus, we were presented with a tradeoff between bitrate and range.

We therefore used two envelope detectors — one specifically tuned for data transfer and the second tuned for longer range and lower rate operation. This is shown in Figure 5.3, where a second envelope detector (in red) is tailored for low rate control messages where range is more important than rate. A significant sensitivity gap can be expected between these two detectors — for example, a state-of-art detector for rates of 100 kbps has a receive sensitivity of -50 dBm whereas a detector for low rates of a few kbps has a receive sensitivity of -68 dBm [135].

5.4.2 Morpho Central Station Architecture

The Morpho central station (or base station) is a more power-hungry system since it needs to generate the carrier whenever the peripheral is operating in backscatter mode. The architecture of the central station resembles that of a typical backscatter reader but with the difference that it can switch between being generating a carrier when needed to support backscatter at the peripheral and operating as a standard active receiver when the peripheral is transmitting in active mode. The central station needs methods to deal with self-interference when generating the carrier for backscattering from the peripheral since the carrier can overwhelm the weak backscattered response from the peripheral. There are many approaches to perform carrier cancellation [40]; Figure 5.3 (lower block) shows an approach that relies on a circulator [91].

5.5 Morpho MAC Layer

We now have a radio that can rapidly switch between active and passive modules but we now need to orchestrate these components to optimize robustness and energy-efficiency. Morpho is a master – slave system where the central station controls the operation of the peripheral and makes decisions regarding the TX and RX modes of the peripheral. Thus, the MAC layer is based on a simple TDMA protocol that is driven by the central station similar to other backscatter-based protocols.

We first describe the decision engine is responsible for tracking channel dynamics and deciding between the various passive and active modes and then the MAC layer protocol that provides the rubric for switching between the modes.

5.5.1 Decision Engine

The decision engine is responsible for tracking channel dynamics and deciding between the various passive and active modes. The decision engine has two key components as shown in Figure 5.4.

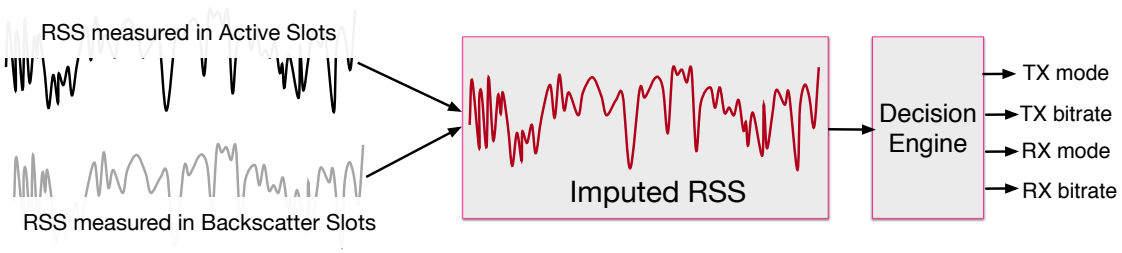


Figure 5.4: Prediction model for deciding whether to use active or passive mode.

Imputation of active and backscatter RSS: A unique feature of the Morpho decision engine is that it has visibility into the channel even when the active radio is not being used. However, since the active and backscatter radios are interleaved, we have RSS for only one of these radio modes for each slot and have to impute the missing data. The imputation function leverages the fact that Active Tx incurs only one-way pathloss whereas Backscatter Tx incurs two-way pathloss. There are also

several constant offsets due to carrier self-interference and transmit power level but these are known a priori and can be accounted for.

To deal with noise, we impute not only using the RSS in a particular slot but also the RSS of previous N-1 slots. In slots for which we have no information i.e. when backscatter or active fails entirely, we use a pre-defined RSS that is below the detection threshold of the receiver. The output of the imputation is the smoothed active and backscatter RSS for the past N slots.

Figure 5.5 shows the relationship between Backscatter and Active RSS for communication between a smartwatch to base-station during normal movements. We can see that the relationship is generally quite linear (in dB) since links are symmetric at short ranges and the forward and reverse path are typically the same. However, there is more measurement error when we are near the receive sensitivity of our measurement infrastructure since the noise levels are higher.

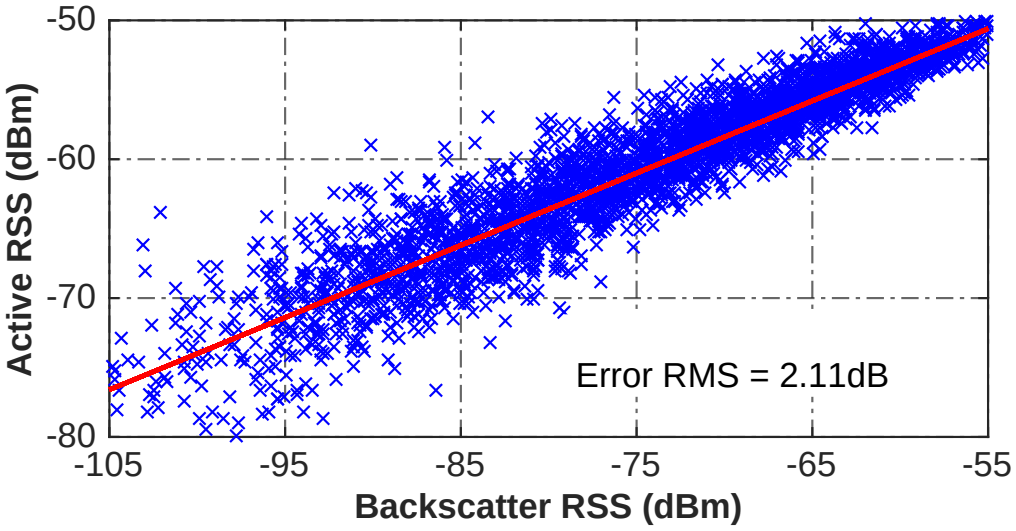


Figure 5.5: A linear relationship is observed between the backscatter RSS and active RSS.

Prediction engine: Given the imputed signal, the prediction engine makes the following decisions: a) for data messages, it needs to decide between backscatter data, active data, and no data (i.e. just measure channel via backscatter), and b) for control messages, it needs to decide between passive high-rate receiver, passive long-range receiver, and active receiver.

The prediction engine first looks at the most recent backscatter RSS measurement and if it is above the threshold for transmitting data via backscatter at the desired bitrate, then it decides to send immediately via backscatter. Since backscatter has very low cost, there is nothing to be gained by waiting for a better RSS. If backscatter for data is not a viable option, it needs to decide whether to send immediately with one of the active modes or wait for a better RSS (within an application-defined latency window). In order to do so, the prediction engine needs to look at the trends in RSS variations by using all measured RSS samples within the several past time windows. Let us define T to be the time (in slots) from the current slot until a better RSS will appear for the first time. We compute the probability distribution of T, given two parameters: the current RSS, and the current RSS slope. We define segments in the 2-D space of RSS values and slopes and obtain the distribution of T for every cell. Given the distribution, our goal is basically to determine whether at the current slot there is a high probability of having a better RSS before the window ends. We define t to be the number of slots until the window ends. Therefore, we must look at:

$$P \;=\; \text{Prob.}\{T \;\leq\; t \mid \text{current RSS}\;,\; \text{current slope}\}\;,$$

and if it is below a threshold (80% in our implementation), the decision is to send via active at the bitrate determined by the imputation process, and if not, the decision is to wait. Note that waiting is the same as measuring the channel via low-rate backscatter, so we continue to have visibility into the channel.

5.5.2 MAC Layer Protocol

At the protocol level, we design an integrated MAC layer that is able to switch between four modes — Active TX, Active RX, Backscatter TX and Passive RX — as and when needed based on the results of the decision engine.

Since Morpho is a master – slave system, the central node needs to inform the peripheral regarding which mode to use. To enable this, every slot is partitioned to a small control sub-slot during which the central node sends the control commands to the peripheral, and a bigger data sub-slot for sending or receiving data bits.

Figure 5.6 shows a sequence of slots in the case of uplink data transfer from the peripheral to the central station. During the control sub-slot, the central station sends a command to the peripheral which provides information about: a) the uplink mode and bitrate, and b) the downlink mode and bitrate, and c) an ACK for the data transfer that occurred in the previous slot. Each of these is only a few bits, so the overhead is small. The figure shows cases where the peripheral transmits uplink data using backscatter (top), performs a backscatter channel measurement using shift register (middle), and transmits uplink data using active mode (bottom).

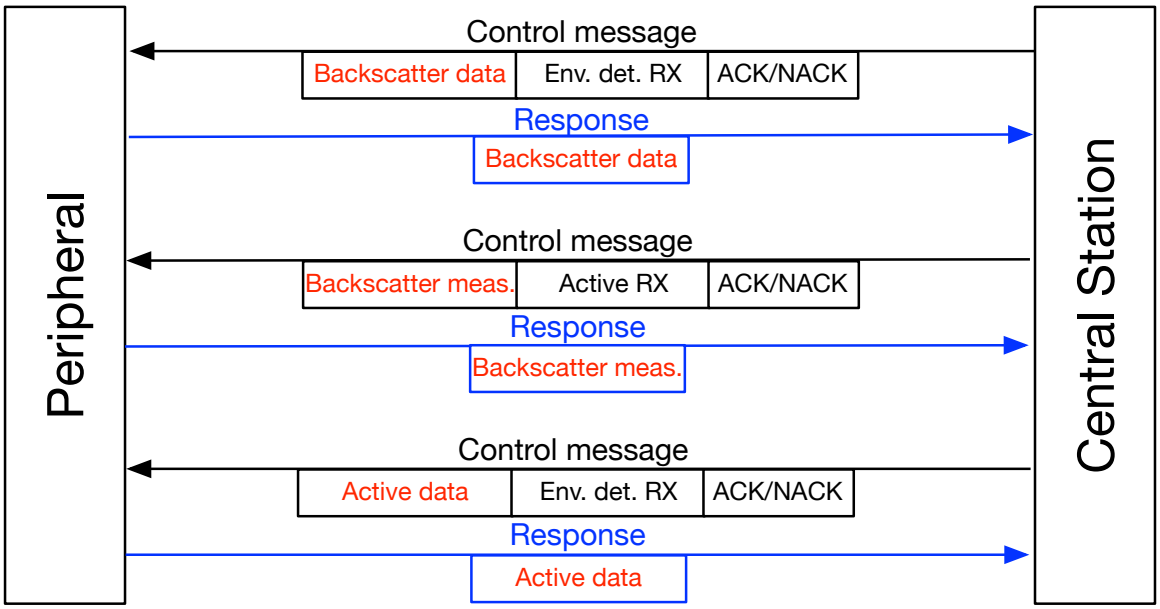


Figure 5.6: The Morpho MAC layer.

To ensure robustness, we fallback to the active modes when failures occur in the passive modes. In particular, the control channel needs to be as reliable as possible since it drives the behavior of the system. Therefore, whenever the passive receiver fails in the control sub-slot, the peripheral switches to the active receiver in the subsequent control sub-slot. Since the control sub-slot is generally much smaller than the data sub-slot, overall power efficiency is not significantly compromised by using an active receiver for control. If backscatter transmission in the data sub-slot fails, then the decision of whether to retransmit or switch to active mode is provided by the central station in the next control sub-slot.

5.6 Re-thinking Application Design

Unlike typical low-power radios which offer some limited capability to tune power consumption, Morpho is unique in that its power consumption can vary by three orders of magnitude depending on whether active or passive modes are being used. We now describe two ways in which applications can leverage this power gap to improve performance.

Quality-Power tradeoffs in audio streaming: The most straightforward way in which an application can use Morpho is to use the passive radio whenever it provides sufficient bandwidth. Morpho then uses the passive mode whenever RSS is high enough to support the required throughput, and if that is not possible, it tries to use the passive mode for channel measurement. If the passive mode does not work at all, it exclusively uses the active radio as a traditional low-power radio. To illustrate this approach, we consider audio streaming using an application like Skype or Pandora which can leverage Morpho to tradeoff application performance for significant gains in power consumption. Audio streaming typically operates at low rates of 32–64kbps for speech and 128kbps for audio, and such bandwidth is frequently achievable using passive communication at short range. This gives Morpho the opportunity to leverage passive communication aggressively and tradeoff a small reduction in audio perception quality for substantial power gains.

Eye tracking with adaptive sampling: Morpho can also be used in concert with the application — as the radio adapts to dynamics and adjusts its operating point along the active–passive spectrum, the application layer can also adjust its computation and sensing decisions to leverage the ultra-low power operation in passive modes. This adds a new dimension to how we opportunistically use cloud and local resources to improve application performance.

We illustrate these advantages with a case study involving a wearable eye tracker [67] that uses sparse sampling to sample pixels from an imager, and uses a neural network to compute gaze parameters as shown in Figure 5.7. In this example, a

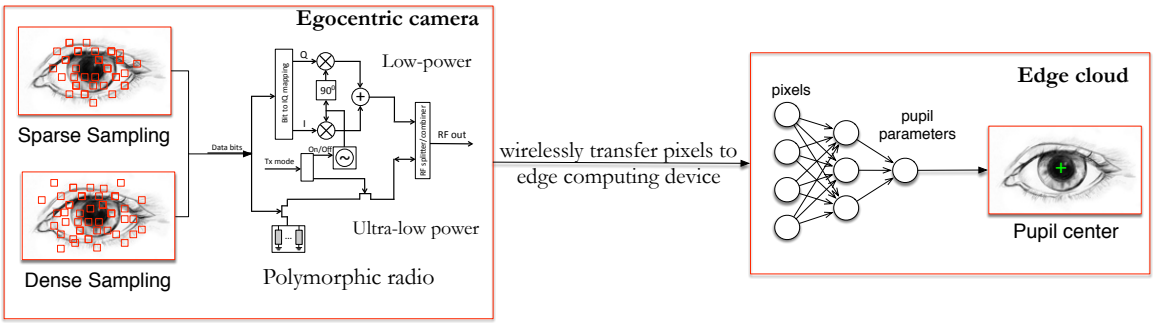


Figure 5.7: Eye tracking with cloud offload.

polymorphic radio can be used to adapt the amount of energy used for sensing vs communication. If more energy is expended for communication via an active radio, then the eye tracker can reduce the pixels sampled and transmit fewer pixels to reduce the overhead of using the the active radio. If less energy is consumed for communication via backscatter, then the camera can be sampled more densely, and these pixels transmitted cheaply to an edge cloud for processing. Thus, by working in concert with the radio, the application layer can improve its accuracy.

5.7 Implementation

The main challenge that we faced in implementing Morpho is the complexity of building a radio and its protocol stack from the ground up. Our design has many non-traditional requirements including: a) power adaptation from microwatts to milliwatts, b) configurability to enable arbitrary combinations of active and passive modes with tiny switching overheads, and c) multiple backscatter transmission subsystems and multiple envelope detectors tuned for different purposes. The combination of these meant that the use of off-the-shelf components and transceivers were essentially off the table.

5.7.1 Morpho prototype

One issue we encountered was that ultra-low power RF oscillators with tight sleep-active transition times were not available as stand-alone components for PCB-level integration. Hence, we custom-designed a Collpitt LC oscillator and integrated it with the backscatter radio (RF oscillator block in Figure 5.3). The oscillator was first designed in ADS simulation environment in order to tune its LC components as well as the lengths of micro-strip tracks to the right frequency and output power, then implemented on a PCB with an NXP BFU690F NPN RF transistor [80]. The Collpitt oscillator that we designed has an output power of +1.1 dBm and wakeup time of 25-35 μs, and generates a 910MHz carrier.

For completeness, we also mention other components of the design. We use an ADG902 SPST RF switch [10] is used as backscatter switch, and HSMS-285C Schottky diodes [14] are used in the envelope detectors. An ADEX-10L+ passive mixer [72] is used for implementing higher order ASK modulations to change the active bitrate as needed. Also, ADG919 SPDT RF switches [11] are used in order to multiplex between the [Tx/Rx $\rightleftarrows$ antenna] paths and to switch between active and passive modes. Finally, an ADP-2-10+ RF power splitter [73] is used to split the Tx and Rx paths to the antenna, and we use a W1910 1dBi small whip antenna [92] as our antenna for Morpho prototype.

On the digital side, the packetizer, MAC layer controller, and the low bit rate sequence generator used for measurement is implemented externally on a AGLN250 low power FPGA development board [69], which connects to the prototype via the connectors shown in Figure 5.8.

5.7.2 Base station implementation

Our base-station is built based on a X300 USRP [32] operating at +30 dBm carrier. Since the base-station must be able to work in both backscatter and active modes, we use an ADG902 evaluation board [10] to turn on and off the carrier. The entire decision engine and data decoding stack is implemented inside a Mac mini computer

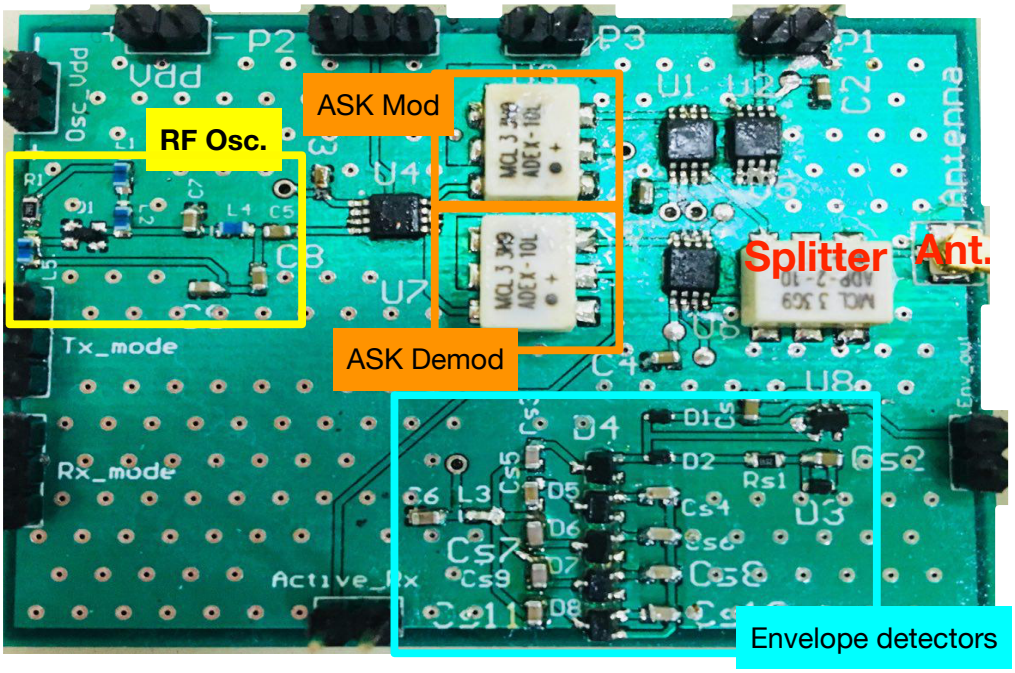


Figure 5.8: Morpho prototype

that is connected to the USRP and to the ADG902 switch. The UBX-40 daughter board has -100 dBm noise level for 1 MHz bandwidth.

On the software side, we run our switching and control tasks in MATLAB, and transfer raw IQ samples from USRP to the MATLAB environment using a TCP socket. There is a 200 μs-300 μs latency in the connection, which has a small effect on overall performance. Within MATLAB, we implemented several software modules including backscatter RSSI measurement, active RSSI measurement, ASK demodulation, data imputation, and prediction engine.

5.8 Evaluation

Our evaluation uses a combination of trace-driven evaluation and real experiments. Since we need to compare many different communication strategies on the same underlying channel dynamics, our benchmark and comparison results are evaluated on traces where we simultaneously collected data from the active and passive radios. The application studies are based on a live implementation.

5.8.1 Hardware micro-benchmarks

We start with hardware micro-benchmarks before showing overall performance results. Table 5.1 benchmarks the performance of Morpho at the hardware level. The most important optimization is the ability to switch within tens of microseconds between passive and active modes allowing us to respond swiftly to channel dynamics. The result also shows that we operate at extremely low power levels while measuring the channel via backscatter. We also see that our Colpitt oscillator performs efficiently at output power levels typically used by low-power radios.

Component	**Performance**
Mode Switching - Latency	30 μs
Mode Switching - Power	5.2 mW
Active mode	5.2 mW @ 1.1 dBm
Backscatter TX (data)	50 μW
Backscatter TX (measurement)	10 μW
Passive RX (env. detector)	10 μW
— Env. Detector 1	$<$ 32kbps, -28dBm sens.
— Env. Detector 2	32–128kbps, -20dBm sens.

Table 5.1: Morpho micro-benchmarks showing low-power operation and tight switching latency.

The table also shows the benefits of using both a high-rate but short-range detector and a long-range but low-rate detector. The fast detector supports good bitrates of 32 kbps to 128 kbps but can only operate at high RSS levels of roughly -20 dBm whereas the slow detector operates down to -28 dBm but only supports bitrates of up to 32 kbps. The combined detector covers the superset of the two receivers.

5.8.2 Morpho vs. active and passive radios

In this section, we validate our claim is that Morpho provides the robustness of active radios and the efficiency of passive radios. To do so, we compare Morpho against a

duty-cycled fully active radio and against a fully passive radio.

Data traces: In-order to perform a fair comparison between the three schemes under the same channel conditions, we obtain four traces corresponding to exemplar applications that involve high rate communication from or to wearable device (as shown in Table 5.2). Of these, the first three are upload-intensive and increase in data rate from T_1 to T_3 and the last one (T_4) is download-intensive. For each of these traces, we collect simultaneous channel information in both passive and active modes, allowing us to compare strategies.

Trace	**Description**
$\mathbf{T}_1$: Wrist IMU	Streaming data from a Smartwatch Inertial Measurement Unit (IMU) to central station for gesture recognition. Streaming 100 samples/second from a nine-axis IMU. Medium average throughput of 10 kbps.
$\mathbf{T}_2$: Lapel Audio	Streaming audio from a lapel sensor for dialog-based applications. Streaming audio at 4 kHz. High average throughput of 32 kbps.
$\mathbf{T}_3$: Eyeglass camera	Streaming video from low power camera on an eyeglass for first-person vision applications. Streaming video at 30 (sub)frames per second - every (sub)frame consists of 800 pixels. Average throughput of 240 kbps.
$\mathbf{T}_4$: Audio download	Same scenario as $\mathbf{T}_2$ but audio is streamed from the central device to peripheral (e.g. music).

Table 5.2: Description of experimental traces. In all cases, we assume that the data is streamed roughly sample-by-sample with a low latency of 30ms. In each case, we collect simultaneous channel information in both passive and active modes, allowing us to compare strategies.

We use a scripted procedure to collect these traces. We first divided the whole experimental area which is a large 7m $\times$ 6m room to three sub-regions based on the distance to the reader: Short-distance ($\sim$ two meters), Medium-distance ($\sim$ four meters), and Long-distance ($\sim$ six to seven meters). Then, we designated 10 locations in each sub-region in order to cover the space of distances between the Morpho node and the base station. For each trace, we placed Morpho at the appropriate spot on

the body and walked between the pre-defined locations while spending 30 seconds at each location. We also scripted a set of natural gestures to be performed at each location including natural movements of the hand while picking up an object, moving the head and hands normally while speaking, and turning the body.

In-order to evaluate the three methods over these traces, we implemented the complete Morpho MAC layer in MATLAB with parameters obtained from hardware micro-benchmarks. To avoid differences across hardware platforms, we assume that active and passive are executing over the Morpho hardware prototype. We assume a 1 ms TDMA slot size (roughly the size of an EPC Gen 2 slot [138]).

Overall performance: Figure 5.9 shows the packet loss rate vs. power consumption of the three methods. Duty-cycled Active and Morpho methods have very low loss rates (0.1%- %1.5), whereas Fully Passive has 25% – 50% loss rate. Note that Morpho has marginally higher loss rate than active because of occasional decision engine errors such as choosing passive rather than active, or too high a bitrate for active communication. In terms of energy-efficiency, Morpho is between 2.5× — 5× more efficient than duty-cycled active radios depending on the specific trace. These results validate that Morpho provides a balance of robustness and efficiency by intelligently using the two radio modes.

We now breakdown the above results in several ways to better understand the contribution of various building blocks of Morpho to the overall performance.

Results by distance: Morpho works best at shorter distances where passive modes can be heavily relied upon for transmission and reception of data. Figure 5.10 illustrates this effect in the instance of the Wrist IMU scenario (T_2). We see that largest gains for Morpho come at short distances where backscatter can be heavily used for data transfer. At this distance, Morpho is about 9.1× more efficient than an active-only approach. At larger distances, the benefits are roughly equal for active-assisted backscatter and backscatter-assisted active and the improvement is about 3.3× — 5.6×. Since T_2 primarily involves data upload from the peripheral to the central station, the contribution of the active-passive receiver is low.

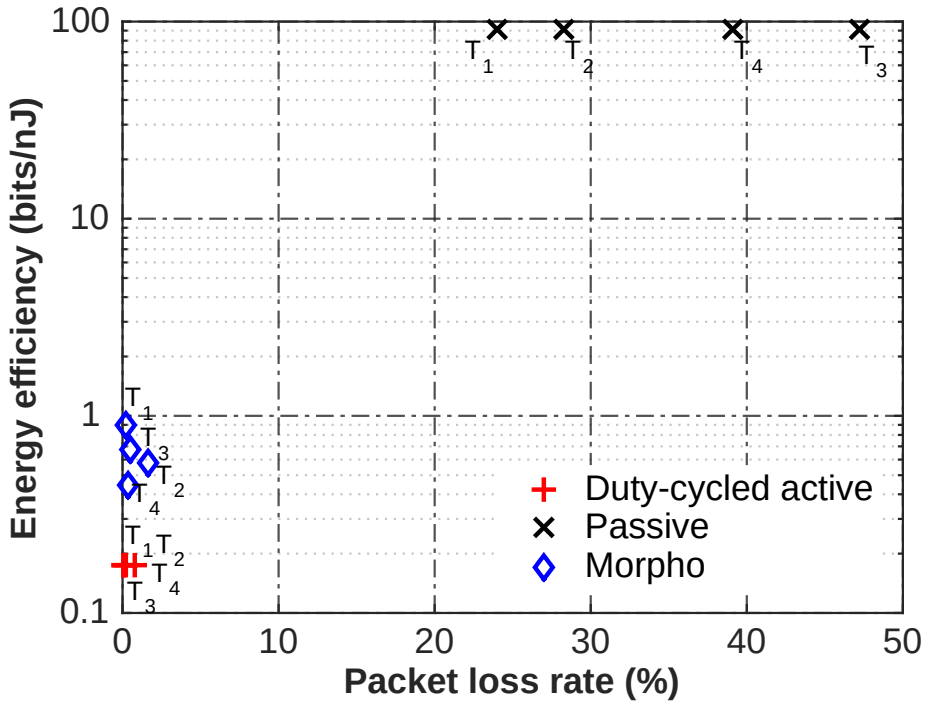


Figure 5.9: Energy Efficiency v.s. Packet loss rate of Passive, Active, and Morpho for all traces.

Breaking down the benefits: We now look at how the building blocks of Morpho contribute to the overall performance. Figure 5.11 compares the contribution of the different building blocks of Morpho normalized against the power consumption of duty-cycled active for that specific trace. We zoom into the short-range part of all traces since all the building blocks of Morpho work together in this regime. The figure shows the contribution of the three main innovations in Morpho — active-assisted backscatter (i.e. using backscatter for data), backscatter-assisted active (i.e. using backscatter for measurement), and use of active-passive receivers for control. For reference, we also show an omniscient version of our decision engine that can predict the perfect policy.

The contribution of different building blocks varies across the traces. Let us first look at the upload-intensive traces T_1 — T_3. Backscatter-assisted Active provides a steady benefit of roughly 2.5× across these traces. In contrast, the benefit from Active-assisted Backscatter is roughly 6× for T_1 and T_2 whereas it is only 1.6× for T_3. This

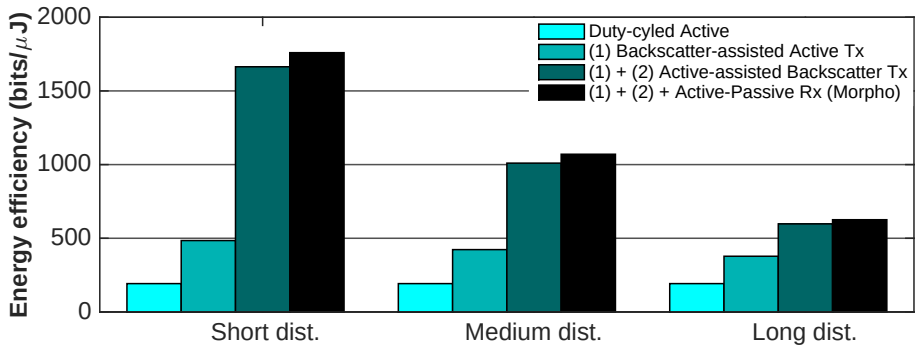


Figure 5.10: The effect of distance on the contribution of each building block towards overall energy efficiency (for Wrist IMU trace, T_1).

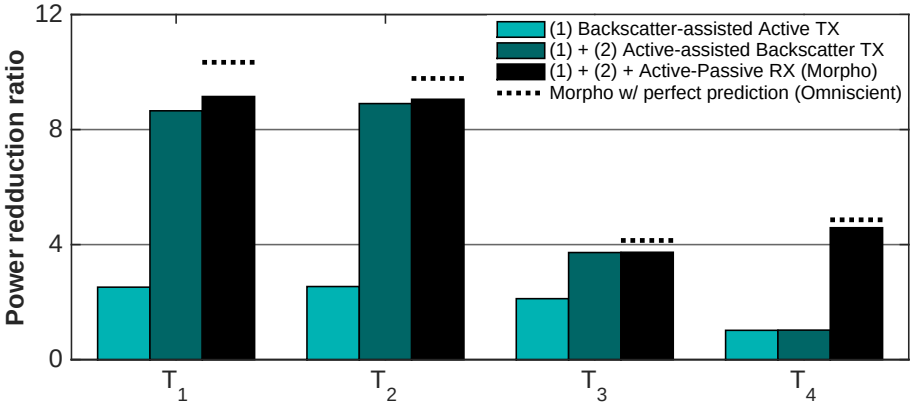


Figure 5.11: Gains due to each of the building blocks of Morpho for short-range communication. Gains are computed relative to Duty-cycled Active on that particular trace.

is because the data rate is lower for T_1 and T_2, hence there is more time to wait until channel conditions improve such that the passive mode can be used. Let us now look at the download-intensive trace T_4. Here, almost all of the 4.5× improvement comes from active-passive receiver rather than from transmitter optimizations. We also see that Morpho performs close to the omniscient scheme that has perfect knowledge of channel conditions.

Impact of rapid switching: One of the advantages that Morpho provides is the ability to switch rapidly in a manner transparent to upper layers. We now look at the benefits of rapid switching for the different traces.

Table 5.3 shows the rate and fraction of switching between different modes for the

Trace		T_1	T_2	T_3	T_4
Data Slot	Active	33%	44%	64%	53%
	Passive	67%	56%	36%	47%
Control Slot	Active	25%	36%	47%	34%
	Passive	75%	64%	53%	46%
Switch rate (per second)		11.1	15.4	19.3	21.4

Table 5.3: Percentage of time spent in active and passive modes in data/control slots, and aggregate switching rate in each trace)

traces. We see that switches between the two modes are frequent and occur roughly 10–20 times per second. This validates the need for a radio that can rapidly transition between modes to adapt to a dynamic channel in-order to minimize energy overheads while providing a unified abstraction of a single radio to upper layers.

To further illustrate the benefits of fast switching, we contrast Morpho against BLISP [47], which combines a BLE active radio with a WISP passive radio [106]. BLISP relies on an algorithm similar to active-assisted backscatter i.e. it uses backscatter mode when available and active mode when backscatter fails. Since BLISP relies on commodity radios, it has high switching latency and incurs more overhead for transition between modes. We empirically measured the switching latency and power from deep sleep to active mode for BLE (560μs & 11.3mW respectively), and use these parameters for the BLISP comparison.

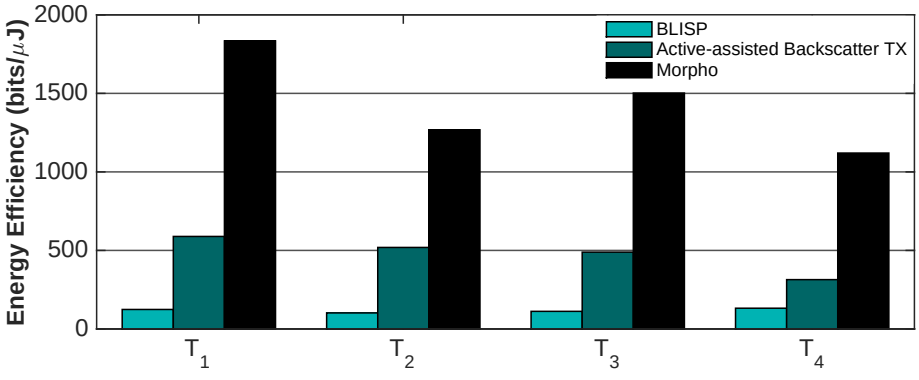


Figure 5.12: Comparison of Morpho against BLISP [47].

Figure 5.12 shows that Morpho is 8.5× to 14.8× more efficient than BLISP across the traces, and even the active-assisted backscatter component within Morpho is, by itself, between 2.4× – 5.1× more efficient. This is because Morpho is far more nimble than BLISP with tight switching capability, but also because it has several additional design elements including backscatter-assisted active and active-passive control optimization.

Benefits of predicting active channel: We now look at the benefit of our prediction scheme against a baseline method that assumes that the RSS for the current slot is the same as the RSS for the previous slot. Table 5.4 shows that our prediction method improves energy efficiency of Morpho by roughly two times over the naïve prediction method which cannot deal with a dynamic channel.

Method	Energy Efficiency (bits/μJ)			
	T_1	T_2	T_3	T_4
Baseline (use prev. slot RSSI)	685	545	321	244
Morpho Prediction	1092	968	535	556

Table 5.4: Benefits of prediction.

5.8.3 Application-layer Performance

We now consider two applications that leverage Morpho and evaluate how the radio can improve their performance. The results in this section are based on a full hardware-software integration to enable live experimentation.

Eye tracking: Here, we illustrate the benefits of Morpho for an eye tracker whose sampling decisions are varied based on the current power consumed by the radio. We integrated Morpho with an eye tracker as shown in Figure 5.13.

While a complete description of the eye tracking mechanism and hardware can be found in [67], we describe salient details to understand the results. Briefly, the eye tracker is able to sample the imager at different resolutions and extract user gaze location by running neural network models trained for different sampling patterns.

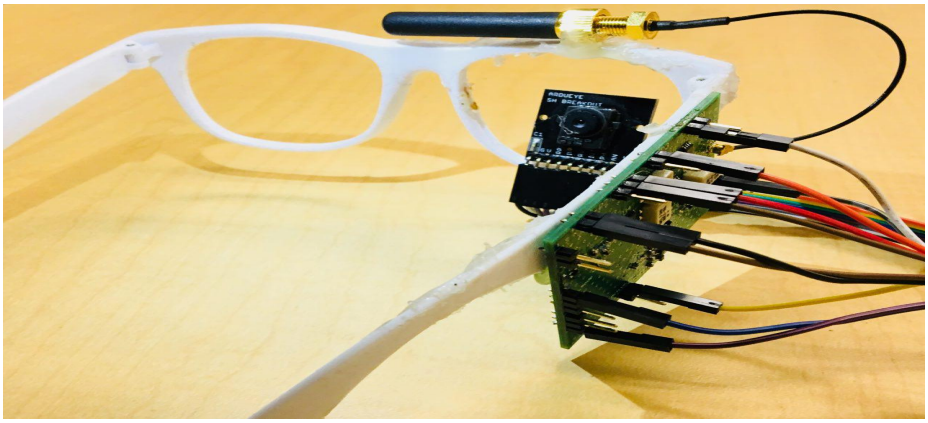


Figure 5.13: Prototype of eye tracker with Morpho

Clearly, accuracy depends on the sampling resolution and varies from a gaze error of 10—15 pixels at 77 pixels/frame to 0—3 pixels at 1984 pixels/frame, where error is the euclidean distance between actual and predicted gaze location.

For this evaluation, we assume that the eye tracker device has a fixed power budget of 100μW for every gaze location update (at 30Hz frame rate). The tracker adjusts the sampling rate depending on available budget — when communication costs more, it samples less and vice-versa. We follow the same procedure that we used to collect the traces in Table 5.2 i.e. we move around a room in a scripted manner with the main difference being that we were running a live version of the eye tracker.

Table 5.5 shows that Morpho reduces gaze error by about 3$\times$ over an active-only approach and 4–5$\times$ over a backscatter-only approach (both at short distance and across all distances). The improvements occur because Morpho is able to use energy saved in communication on sensing, thereby transmitting more samples and improving accuracy.

Method	Gaze Err (all dist.)	Gaze Err (short dist.)
Active	9.1 $\pm$ 5.7	8.8 $\pm$ 6.0
Backscatter	17.8 $\pm$ 8.6	10.6 $\pm$ 7.4
Morpho	3.6 $\pm$ 3.4	2.7 $\pm$ 2.7

Table 5.5: Optimizing eye tracking with Morpho .

Voice audio streaming: We now look at streaming voice audio over Morpho (upload from peripheral to central station). For this experiment, we attached Morpho to a shirt (convenient location for microphone) and transmitted a stored audio stream via the different modes. We use typical audio streaming parameters (40kbps rate, 125 byte audio packets, and 30ms latency). We followed the same procedure as the eye tracking example in terms of moving across different locations in the room while the data was being transmitted. We then computed the Mean Opinion Score (MOS) of the audio stream [96].

Method	Short distance		All distance	
	MOS	bits/nJ	MOS	bits/nJ
Active	4.4	0.17	4.3	0.17
Backscatter	2.85	100	2.51	100
Morpho	4.1	1.74	4.0	0.98

Table 5.6: Audio voice quality over Morpho versus duty-cycled active and backscatter-only.

Table 5.6 shows that MOS score is marginally lower than for the active radio (primarily because of bit rate changes when switching between active and passive modes) but energy efficiency is four times higher across all distances and an order of magnitude higher at short distance. Backscatter has considerably lower MOS score but it has very high energy-efficiency. Thus, Morpho is able to take advantage of the channel to improve energy efficiency without significant impact on application-level performance.

5.9 Discussion and Limitations

We briefly discuss some additional issues that we did not cover in the rest of this paper.

RF tuning and hardware optimization: We expect that the performance of Morpho can be increased substantially with better RF optimization. Other work has reported tens of meters backscatter range and higher sensitivity passive detectors

[129, 76, 45, 135]. Such improvements can extend our techniques to larger sized areas (e.g. multiple rooms or a home), and also allow us to reduce carrier transmit power levels such that battery-powered mobile devices like smartphones can take the role of the central station.

Multi-node evaluation: Our evaluation focuses on the single sensor to base-station case. This is because we found that the multi-node scenario does not provide insights specific to Morpho and is only an evaluation of TDMA performance. As one would expect, if there are more nodes in the network, each individual node has few transmission slots, so there are fewer opportunities to measure the channel. However, since Morpho can switch efficiently, it can work with small slots and therefore the frequency of transmission/measurement opportunities can be kept high.

Frequency-hopping in Morpho: The main issue to consider when extending our architecture to frequency-hopping spread spectrum radios is the fact that passive radios are not frequency selective. Frequency hopping can be enabled on the passive transmitter side (i.e. backscatter), by leveraging frequency shifting and recent advances in single-sideband backscattering [48]. These methods only add a small amount of complexity and power to our design. One area that needs more research to complete this design is the question of how to endow the passive receiver with similar frequency hopping capabilities.

One way to circumvent this issue is to use a dedicated channel for passive communication, and allow active communication to proceed with frequency hopping. The advantage of such decoupling is that we can use passive components like a SAW filter tuned to the specific channel before the passive receiver to make it frequency selective [40]. But this method restricts us to a single channel for passive communication which might be scalable to large networks.

Design options between active and backscatter: Along the way to designing our final version of Morpho , we explored several failed directions. One of these was the addition of a reflection amplifier, which have been proposed as providing an intermediate point between active and passive radios [56]. We prototyped this

architecture, but our empirical studies revealed that this technique only works in a narrow range of SNR, and causes feedback when operating outside this range. This makes it too unstable to be used in a general-purpose radio.

Bit-level switching: While we assume that the entire data frame is transmitted in either backscatter or active mode, the tight integration between modes also makes it possible to switch *at the bit level*. For example, data bits may be transmitted in active whereas the CRC for a packet may be transmitted in active mode for more reliability. Other coding options such as unequal error protection is also possible with Morpho . These are areas for further exploration.

How much of the baseband processing can be shared between active and backscatter? The low bitrate modulations of active and backscatter may be shared (e.g. BPSK). Higher bitrate modulation methods may be active-only but not shared with backscatter. Backscatter for measurement can use a very low bitrate + long range method that may not be useful for active, maybe even something like CSS. (Bluetooth uses GPSK, DPSK, 8DPSK modulation, so maybe we can bring this in).

Can the active radio be frequency-hopping or narrowband? The active radio can be frequency hopping but making the passive modes perform in a frequency hopping scenario is not viable. Main reason is that passive methods are not frequency selective and either absorb or reflect all energy that is captured by the antenna. This is particularly true for the envelope detector front-end which is not frequency selective. The backscatter transmitter can potentially be made frequency selective by mixing with an appropriate signal although this increases the complexity and power consumption. The simplest method is to use passive methods in a single band with SAW filter, and for the active to do whatever it pleases. When there are multiple readers, the control slot can be in active mode to ensure reliability. The data slot can use reservations in backscatter mode i.e. the reader can reserve the channel using a NAV before asking the tag to transmit data or measure channel in backscatter mode.

5.10 Related Work

We briefly review relevant related work that we have not highlighted in previous sections.

Multi-radio wireless networks: There has been much work on the general idea of multi-radio wireless radios. This work has explored many combinations including Bluetooth + WiFi [6, 88, 12], WiFi + LTE [25, 63, 16], and WiFi + 60 GHz [116]. This work has leveraged multi-radio combinations for energy-efficiency [6, 61, 50, 36, 57], traffic management [33], mobility management [90], and routing management [26, 7]. While there is similarity between these efforts and ours at a high level, the crucial difference is that we are designing an multi-radio system that operates at ultra-low power regimes between 1 μW to 1 mW, and can switch at micro-second granularity to react to highly dynamic channels. This is a completely different design space and necessitates re-thinking all layers of the stack.

Active-Passive radios: There has been some recent work that explores integration of active and passive components, albeit in restricted ways. In terms of receiver side integration, recent work on wakeup radios integrate passive envelope detectors with active receivers to enable extremely low power remote wakeup [101, 99]. In terms of transmitter side integration, a recent short paper looks at reusing hardware elements between 10 Mbps BPSK Backscatter and 1Mbps Bluetooth [98]. A couple of approaches have explored integration at higher layers of the stack as well. One is BLISP [47], which we have previously discussed. Another is Braidio [40], which leverages active and passive components for power offload by shifting carrier generation between end-points. Our work shows how such active-passive radio components can be leveraged in every aspect of communication including data transfer, measurement, and control messages.

Backscatter communication: There has been significant activity in backscatter communication in recent years. A significant fraction of this work has focused on repurposing ambient carriers such as Bluetooth [29, 48, 148], WiFi [85, 142, 144, 17,

146, 53, 148], Zigbee [48, 148], FM [134], and LoRA [117] to enable backscatter communication. Recent work has also shown that it is possible to use backscatter for applications like low-power HD video streaming [76]. However, the issue of how to deal with the inherent flakiness of passive radios under channel dynamics has received very little attention. Morpho bridges this gap.

Chapter 6

Conclusions

This thesis addresses key gaps in the energy efficiency of wireless connectivity for next-generation massive IoT deployments. We expand on the recent line of research on backscatter as a plausible, μW alternative to active radios, and address a number of non-trivial performance gaps between the performance state-of-the-art backscatter tags and the bandwidth and robustness requirements of IoT applications.

We propose 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 present 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 that need battery-free tags to directly communicate with commodity off-the-shelf devices.

We propose MIXIQ, a new design paradigm for boosting the performance of passive envelope detectors with the help of commercial WiFi transmitters. Properly orchestrating the signaling in the WiFi packets, the envelope detector behaves like a passive mixer which allows for IQ detection as well as boosted through and communication range using a novel, highly energy efficient baseband. As opposed to envelope detectors which are very finicky even in the close of proximity of WiFi transmitters, MIXIQ can reliably receive high rate streams of data in downlink direction at up to several meters from commodity WiFi devices, which makes it ideal for several applications

such as ultra-low power hearables.

Lastly, we propose Radio Polymorphism which is a new architecture for low-power radios that leverages passive and active components in a tightly intertwined manner to improve performance. In contrast to duty-cycling based radios that aim to maximize sleep times to save power, polymorphic radios leverage passive modes to save power. This is a new paradigm that is particularly useful for low-power radios that are used in streaming mode to transmit data from or to wearable, IoT, and mobile devices. We instantiate our ideas in a full hardware-software stack that we call Morpho, and show that we can get up to an order of magnitude improvements in energy-efficiency while still being robust to channel fluctuations. Our exploration paves the way for low-power radios that are designed for continuous streaming from embedded sensing devices to the cloud.

BIBLIOGRAPHY

[1] *Bluetooth Core Specification Version 4.2*.

[2] The history of rfid technology over the past 80 years. `https://medium.com/micro-tracking-macro-insights/the-history-of-rfid-technology-over-the-past-80-years-1f7f69dc0ccb`. Accessed: 2019-03-28.

[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 4×4, 4-stream, 802.11ax Access Point with Integrated Antennas*, 2018.

[6] Y. Agarwal, T. Pering, R. Want, and R. Gupta. Switchr: Reducing system power consumption in a multi-client, multi-radio environment. In *Wearable Computers, 2008. ISWC 2008. 12th IEEE International Symposium on*, pages 99–102. IEEE, 2008.

[7] M. Alicherry, R. Bhatia, and L. E. Li. Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks. In *Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 58–72. ACM, 2005.

[8] E. Alpman, A. Khairi, R. Dorrance, M. Park, V. S. Somayazulu, J. R. Foerster, A. Ravi, J. Paramesh, and S. Pellerano. 802.11g/n compliant fully integrated wake-up receiver with -72 dbm sensitivity in 14-nm finfet cmos. *IEEE Journal of Solid-State Circuits*, 53(5):1411–1422, 2018.

[9] F. Amato, C. W. Peterson, B. P. Degnan, and G. D. Durgin. Tunneling rfid tags for long-range and low-power microwave applications. *IEEE Journal of Radio Frequency Identification*, 2(2):93–103, 2018.

[10] 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.

[11] Analog Devices. *Wideband 4 GHz, 43 dB Isolation at 1 GHz, CMOS 1.65 V to 2.75 V, 2:1 Mux/SPDT*. Rev. E.

[12] G. Ananthanarayanan and I. Stoica. Blue-fi: enhancing wi-fi performance using bluetooth signals. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 249–262. ACM, 2009.

[13] 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.

[14] Avago Technologies. *Surface Mount Zero Bias Schottky Detector Diodes*, 5 2009.

[15] J. E. Bardram. The cams esense framework: Enabling earable computing for mhealth apps and digital phenotyping. In *Proceedings of the 1st International Workshop on Earable Computing*, EarComp'19, page 3–7, New York, NY, USA, 2019. Association for Computing Machinery.

[16] M. Bennis, M. Simsek, A. Czylwik, W. Saad, S. Valentin, and M. Debbah. When cellular meets wifi in wireless small cell networks. *IEEE communications magazine*, 51(6):44–50, 2013.

[17] 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.

[18] Bosch. *BMI160: Ultra Low Power Inertial Measurement Unit*.

[19] 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.

[20] 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.

[21] 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.

[22] R. R. Choudhury. Earable computing: A new area to think about. In *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*, HotMobile '21, page 147–153, New York, NY, USA, 2021. Association for Computing Machinery.

[23] 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.

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

[25] S. Deng, R. Netravali, A. Sivaraman, and H. Balakrishnan. Wifi, lte, or both?: Measuring multi-homed wireless internet performance. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 181–194. ACM, 2014.

[26] R. Draves, J. Padhye, and B. Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128. ACM, 2004.

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

[28] J. F. Ensworth, A. T. Hoang, and M. S. Reynolds. A low power 2.4 ghz superheterodyne receiver architecture with external lo for wirelessly powered backscatter tags and sensors. In *2017 IEEE International Conference on RFID (RFID)*, pages 149–154, May 2017.

[29] J. F. Ensworth and M. S. Reynolds. Every smart phone is a backscatter reader: Modulated backscatter compatibility with bluetooth 4.0 low energy (ble) devices. In *RFID (RFID), 2015 IEEE International Conference on*, pages 78–85. IEEE, 2015.

[30] 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.

[31] M. et al. *Ultra-Low-Power Short-Range Radios*. Springer, 2015.

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

[33] S. Ferlin, T. Dreibholz, and Ö. Alay. Multi-path transport over heterogeneous wireless networks: Does it really pay off? In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 4807–4813. IEEE, 2014.

[34] K. Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. Wiley Publishing, 2nd edition, 2003.

[35] 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.

[36] J. Gummeson, D. Ganesan, M. D. Corner, and P. Shenoy. An adaptive link layer for heterogeneous multi-radio mobile sensor networks. *IEEE Journal on Selected Areas in Communications*, 28(7), 2010.

[37] J. Gummeson, P. Zhang, and D. Ganesan. Flit: A bulk transmission protocol for rfid-scale sensors. 06 2012.

[38] G. Haas, E. Stemasov, M. Rietzler, and E. Rukzio. *Interactive Auditory Mediated Reality: Towards User-Defined Personal Soundscapes*, page 2035–2050. Association for Computing Machinery, New York, NY, USA, 2020.

[39] Himax. *HM01B0: Ultra Low Power Image Sensor*.

[40] P. Hu, P. Zhang, M. Rostami, and D. Ganesan. Braidio: An integrated active-passive radio for mobile devices with asymmetric energy budgets. In *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*, pages 384–397. ACM, 2016.

[41] 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.

[42] X. Huang, S. Rampu, X. Wang, G. Dolmans, and H. de Groot. A 2.4ghz/915mhz 51μw wake up receiver with offset and noise suppression. In *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, pages 222–223, Feb 2010.

[43] J. Im, H. Kim, and D. D. Wentzloff. A 335μw -72dbm receiver for fsk back-channel embedded in 5.8ghz wi-fi ofdm packets. In *2017 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 176–179, 2017.

[44] J. Im, H. Kim, and D. D. Wentzloff. A 220μ w -83 dbm 5.8 ghz third-harmonic passive mixer-first lp-wur for ieee 802.11ba. *IEEE Transactions on Microwave Theory and Techniques*, 67(7):2537–2545, 2019.

[45] Impinj. *Impinj XArray RAIN RFID Gateway*.

[46] Infineon. *BAT6302-V Silicon Schottky Diode*.

[47] I. in't Veen, Q. Liu, P. Pawelczak, A. Parks, and J. R. Smith. Blisp: Enhancing backscatter radio with active radio for computational rfids. In *RFID (RFID), 2016 IEEE International Conference on*, pages 1–4. IEEE, 2016.

[48] 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.

[49] B. Jiang, A. Sample, R. Wistort, and A. Mamishev. Autonomous robotic monitoring of underground cable systems. In *ICAR '05. Proceedings., 12th International Conference on Advanced Robotics, 2005.*, pages 673–679, 2005.

[50] T. Jin, G. Noubir, and B. Sheng. Wizi-cloud: Application-transparent dual zigbee-wifi radios for low power internet access. In *INFOCOM, 2011 Proceedings IEEE*, pages 1593–1601. IEEE, 2011.

[51] S. Kamath and J. Lindh. Measuring bluetooth low energy power consumption. *Texas instruments application note AN092, Dallas*, 2010.

[52] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. *SIGCOMM Comput. Commun. Rev.*, 44(4):607–618, Aug. 2014.

[53] 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.

[54] 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.

[55] J. Kimionis, A. Bletsas, and J. Sahalos. Bistatic backscatter radio for tag read-range extension. 11 2012.

[56] J. Kimionis, A. Georgiadis, A. Collado, and M. M. Tentzeris. Enhancement of rf tag backscatter efficiency with low-power reflection amplifiers. *IEEE Transactions on Microwave Theory and Techniques*, 62(12):3562–3571, 2014.

[57] B. Kusy, C. Richter, W. Hu, M. Afanasyev, R. Jurdak, M. Brünig, D. Abbott, C. Huynh, and D. Ostry. Radio diversity for reliable communication in wsns. In *Information Processing in Sensor Networks (IPSN), 2011 10th International Conference on*, pages 270–281. IEEE, 2011.

[58] Y. Li, Z. Chi, X. Liu, and T. Zhu. 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*, SenSys '18, page 159–171, New York, NY, USA, 2018. Association for Computing Machinery.

[59] 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.

[60] F. Lu, G. Voelker, and A. Snoeren. Slomo: downclockingwifi communication. pages 255–268, 04 2013.

[61] D. Lymberopoulos, N. B. Priyantha, M. Goraczko, and F. Zhao. Towards energy efficient design of multi-radio platforms for wireless sensor networks. In *Proceedings of the 7th international conference on Information processing in sensor networks*, pages 257–268. IEEE Computer Society, 2008.

[62] 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.

[63] R. Mahindra, H. Viswanathan, K. Sundaresan, M. Y. Arslan, and S. Rangarajan. A practical traffic management system for integrated lte-wifi networks. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 189–200. ACM, 2014.

[64] V. Mangal and P. R. Kinget. A wake-up receiver with a multi-stage self-mixer and with enhanced sensitivity when using an interferer as local oscillator. *IEEE Journal of Solid-State Circuits*, 54(3):808–820, 2019.

[65] J. Manweiler and R. Choudhury. Avoiding the rush hours: Wifi energy management via traffic isolation. *Mobile Computing, IEEE Transactions on*, 11:739–752, 05 2012.

[66] Maxim Integrated. *Ultra-Low Power, Single-Channel Integrated Biopotential (ECG, R to R Detection) AFE*.

[67] A. Mayberry, P. Hu, B. Marlin, C. Salthouse, and D. Ganesan. ishadow: design of a wearable, real-time mobile gaze tracker. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 82–94. ACM, 2014.

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

[69] MicroSemi. *IGLOO nano Low Power Flash FPGAs*, 9 2015. Rev. 19.

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

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

[72] Mini-Circuits. *Frequency Mixer, Level 4 (LO Power +4 dBm) 10 to 1000 MHz*. Rev. E.

[73] Mini-Circuits. *Power Splitter/Combiner 2 Way 50ω 5 to 1000 MHz*. Rev. F.

[74] R. Mittal, A. Kansal, and R. Chandra. Empowering developers to estimate app energy consumption. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Mobicom '12, page 317–328, New York, NY, USA, 2012. Association for Computing Machinery.

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

[76] S. Naderiparizi, M. Hessar, V. Talla, S. Gollakota, and J. R. Smith. Low-power HD video streaming. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, 2018.

[77] S. Naderiparizi, Y. Zhao, J. Youngquist, A. P. Sample, and J. R. Smith. Self-localizing battery-free cameras. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '15, page 445–449, New York, NY, USA, 2015. Association for Computing Machinery.

[78] M. Nemati, M. Soltani, J. Ding, and J. Choi. Subcarrier-wise backscatter communications over ambient ofdm for low power iot, 07 2020.

[79] Nordic Semiconductor. *nRF52840: Ultra-low power 2.4GHz wireless system on chip (SoC)*.

[80] NXP Semiconductors. *NPN wideband silicon RF transistor*, 3 2014. Rev. 2.

[81] S. Oh, N. E. Roberts, and D. D. Wentzloff. A 116nw multi-band wake-up receiver with 31-bit correlator and interference rejection. In *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference*, pages 1–4, Sep. 2013.

[82] On Semiconductor. *General Purpose Transistors*.

[83] J. N. Pandey, J. Shi, and B. P. Otis. A 120μw mics/ism-band fsk receiver with a 44μw low-power mode based on injection-locking and 9x frequency multiplication. *2011 IEEE International Solid-State Circuits Conference*, pages 460–462, 2011.

[84] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith. Turbocharging ambient backscatter communication. *SIGCOMM Comput. Commun. Rev.*, 44(4):619–630, Aug. 2014.

[85] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith. Turbocharging ambient backscatter communication. *ACM SIGCOMM Computer Communication Review*, 44(4):619–630, 2015.

[86] 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.

[87] C. Pérez-Penichet, C. Noda, A. Varshney, and T. Voigt. Battery-free 802.15.4 receiver. In *Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks*, IPSN '18, pages 164–175, Piscataway, NJ, USA, 2018. IEEE Press.

[88] T. Pering, Y. Agarwal, R. Gupta, and R. Want. Coolspots: reducing the power consumption of wireless mobile devices with multiple radio interfaces. In *Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 220–232. ACM, 2006.

[89] N. Pletcher, S. Gambini, and J. Rabaey. A 52 μw wake-up receiver with-72 dbm sensitivity using an uncertain-if architecture. *Solid-State Circuits, IEEE Journal of*, 44:269 – 280, 02 2009.

[90] C. Pluntke, L. Eggert, and N. Kiukkonen. Saving mobile device energy with multipath tcp. In *Proceedings of the sixth international workshop on MobiArch*, pages 1–6. ACM, 2011.

[91] D. M. Pozar. *Microwave engineering*. John Wiley & Sons, 2009.

[92] PulseLarsen Antennas. *Penta Band Stubby Antenna*, 2 2010. Rev. 1.

[93] Qualcomm. *Qualcomm Networking Pro 400 Platform*.

[94] Qualcomm. How will 5g transform industrial iot?, 2019.

[95] 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.

[96] I. Recommendation. Vocabulary for performance and quality of service, 2006.

[97] J. M. Rehg, S. A. Murphy, and S. Kumar. *Mobile Health: Sensors, Analytic Methods, and Applications*. Springer, 2017.

[98] M. S. Reynolds. A 2.4-ghz, hybrid 10-mb/s bpsk backscatter and 1-mb/s fsk bluetooth tx with hardware reuse. *IEEE Microwave and Wireless Components Letters*, 27(12):1155–1157, 2017.

[99] N. E. Roberts, K. Craig, A. Shrivastava, S. N. Wooters, Y. Shakhsheer, B. H. Calhoun, and D. D. Wentzloff. 26.8 a 236nw- 56.5 dbm-sensitivity bluetooth low-energy wakeup receiver with energy harvesting in 65nm cmos. In *Solid-State Circuits Conference (ISSCC), 2016 IEEE International*, pages 450–451. IEEE, 2016.

[100] N. E. Roberts, K. Craig, A. Shrivastava, S. N. Wooters, Y. Shakhsheer, B. H. Calhoun, and D. D. Wentzloff. 8 a 236 nw-56 . 5 dbm-sensitivity bluetooth low-energy wakeup receiver with energy harvesting in 65 nm cmos. 2017.

[101] N. E. Roberts and D. D. Wentzloff. Ultra-low power wake-up radios. In *Ultra-Low-Power Short-Range Radios*, pages 137–162. Springer, 2015.

[102] M. Rostami, K. Sundaresan, E. Chai, S. Rangarajan, and D. Ganesan. Redefining passive in backscattering with commodity devices. In *The 26th Annual International Conference on Mobile Computing and Networking*, 2020.

[103] C. Salazar, A. Cathelin, A. Kaiser, and J. Rabaey. A 2.4 ghz interferer-resilient wake-up receiver using a dual-if multi-stage n-path architecture. *IEEE Journal of Solid-State Circuits*, 51(9):2091–2105, Sep. 2016.

[104] A. Sample, M. Buettner, B. Greenstein, A. Sample, J. Smith, and D. Wetherall. Revisiting smart dust with rfid sensor networks. 10 2008.

[105] A. Sample, C. Macomber, L.-T. Jiang, and J. Smith. Optical localization of passive uhf rfid tags with integrated leds. pages 116–123, 04 2012.

[106] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R. Smith. Design of an rfid-based battery-free programmable sensing platform. *IEEE transactions on instrumentation and measurement*, 57(11):2608–2615, 2008.

[107] A. P. Sample, D. J. Yeager, and J. R. Smith. A capacitive touch interface for passive rfid tags. In *2009 IEEE International Conference on RFID*, pages 103–109, 2009.

[108] N. Saputra and J. R. Long. A fully integrated wideband fm transceiver for low data rate autonomous systems. *IEEE Journal of Solid-State Circuits*, 50(5):1165–1175, 2015.

[109] T. S. P. See, C. W. Kim, T. M. Chiam, Y. Ge, A. A. P. Wai, and Z. N. Chen. Study of dynamic on-body link reliability for wban systems. In *2012 IEEE Asia-Pacific Conference on Antennas and Propagation*, pages 112–113, 2012.

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

[111] SEMTECH. *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*, 8 2016.

[112] R. L. Shinmoto Torres, D. C. Ranasinghe, Q. Shi, and A. P. Sample. Sensor enabled wearable rfid technology for mitigating the risk of falls near beds. In *2013 IEEE International Conference on RFID (RFID)*, pages 191–198, 2013.

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

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

[115] J. Smith, A. Sample, P. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. volume 4206, pages 495–506, 09 2006.

[116] S. Sur, I. Pefkianakis, X. Zhang, and K.-H. Kim. Wifi-assisted 60 ghz wireless networks. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 28–41. ACM, 2017.

[117] 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.

[118] Texas Instruments. *LPV511 Micropower, Rail-to-Rail Input and Output Operational Amplifier*. Rev. D.

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

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

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

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

[123] Texas Instruments. *TPL0501 256-Taps, Single-Channel, Digital Potentiometer With SPI Interface*. Rev. C.

[124] Texas Instruments. *Ultra-Low Power, Ultra-Small Size, 12-Bit, 1-MSPS, SAR ADC*. Rev. A.

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

[126] `https://shop.8devices.com/MANGO-DVK`. Mango DVK.

[127] `https://shop.8devices.com/MANGO-I`. Mango-I Wi-Fi 6 module.

[128] M. van Elzakker, E. van Tuijl, P. Geraedts, D. Schinkel, E. Klumperink, and B. Nauta. A 1.9µw 4.4fj/conversion-step 10b 1ms/s charge-redistribution adc. In *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 244–610, 2008.

[129] A. Varshney, O. Harms, C.-P. Penichet, C. Rohner, F. Hermans, and T. Voigt. Lorea: A backscatter architecture that achieves a long communication range. In *ACM SenSys 2017*. ACM Digital Library, 2017.

[130] A. Varshney, A. Soleiman, and T. Voigt. Tunnelscatter: Low power communication for sensor tags using tunnel diodes. In *The 25th Annual International Conference on Mobile Computing and Networking*, pages 1–17, 2019.

[131] 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.

[132] Vesper. *VM1010: Wake-on-Sound Piezoelectric MEMS Microphone*.

[133] e. a. Vincent Liu. Ambient backscatter: Wireless communication out of thin air. *SIGCOMM Comput. Commun. Rev.*, 2013.

[134] 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.

[135] P. H. P. Wang, H. Jiang, L. Gao, P. Sen, Y. H. Kim, G. M. Rebeiz, P. P. Mercier, and D. A. Hall. A 400 mhz 4.5 nw -63.8 dbm sensitivity wake-up receiver employing an active pseudo-balun envelope detector. In *ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference*, pages 35–38, Sept 2017.

[136] P. P. Wang, H. Jiang, L. Gao, P. Sen, Y. Kim, G. M. Rebeiz, P. P. Mercier, and D. A. Hall. A near zero power wake up receiver achieving -69 dbm sensitivity. *IEEE Journal of Solid-State Circuits*, 53(6):1640–1652, June 2018.

[137] P. P. Wang, C. Zhang, H. Yang, D. Bharadia, and P. P. Mercier. 20.1 a 28μw iot tag that can communicate with commodity wifi transceivers via a single-side-band qpsk backscatter communication technique. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 312–314, 2020.

[138] R. Want. Rfid explained: A primer on radio frequency identification technologies. *Synthesis Lectures on Mobile and Pervasive Computing*, 1(1):1–94, 2006.

[139] H. Watanabe and T. Terada. Manipulatable auditory perception in wearable computing. In *Proceedings of the Augmented Humans International Conference*, AHs '20, New York, NY, USA, 2020. Association for Computing Machinery.

[140] Xilinx Inc. *XC2C64A CoolRunner-II CPLD*. Version 2.3.

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

[142] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei. Modulation in the air: Backscatter communication over ambient ofdm carrier. *arXiv preprint arXiv:1704.02245*, 2017.

[143] Yu Ge, Jeng Wai Kwan, J. S. Pathmasuntharam, Zhengye Di, T. S. P. See, Wei Ni, Chee Wee Kim, Tat Meng Chiam, and Maode Ma. Performance benchmarking for wireless body area

networks at 2.4 ghz. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 2249–2253, 2011.

[144] 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.

[145] 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.

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

[147] P. Zhang, D. Ganesan, and B. Lu. Quarkos: pushing the operating limits of micro-powered sensors. pages 7–7, 05 2013.

[148] 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.

[149] 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.

[150] R. Zhao, F. Zhu, Y. Feng, S. Peng, X. Tian, H. Yu, and X. Wang. Ofdma-enabled wi-fi backscatter. In *The 25th Annual International Conference on Mobile Computing and Networking*, MobiCom '19, New York, NY, USA, 2019. Association for Computing Machinery.

[151] 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.