UNIVERSITY OF CALIFORNIA SAN DIEGO

Highly Reliable Communication and Sensing for Battery-free IoT

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Electrical Engineering (Communication Theory and Systems)

by

Renjie Zhao

Committee in charge:

Professor Xinyu Zhang, Chair
Professor Rajesh Gupta
Professor Wing Ching Vincent Leung
Professor Patrick Mercier
Professor Patrick Pannuto
Professor Bhaskar Rao

2023

The Dissertation of Renjie Zhao is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2023

DEDICATION

To my parents,

those whom I care

and those who care me.

EPIGRAPH

Thus we may have knowledge of the past but cannot control it;
we may control the future but have no knowledge of it.

Claude Elwood Shannon

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to all those who have supported and contributed to the completion of this Ph.D. dissertation. Their guidance, encouragement, and assistance have been invaluable throughout this 5 years research journey.

First and foremost, I am immensely grateful to my advisor, Professor Xinyu Zhang, for his unwavering support, insightful guidance, and continuous encouragement. His expertise, dedication, and mentorship have been instrumental in shaping my research work and academic development. I will never forget the days and nights that I worked with him on coming up with ideas and pushing the boundaries. I could not have hoped for a better advisor and I hope to be as good an advisor when nurturing my future students.

I extend my heartfelt thanks to the members of my Ph.D. committee: Professor Rajesh Gupta, Professor Wing Ching Vincent Leung, Professor Patrick Mercier, Professor Patrick Pannuto, and Professor Bhaskar Rao. I am deeply appreciative of their time, expertise, and valuable feedback throughout the evaluation process, including the qualifying exam, the yearly spring evaluations, and the final defense. Their constructive criticism and insightful suggestions have significantly enhanced the quality of this dissertation.

I would also like to acknowledge the invaluable support and guidance provided by my internship mentors: Pengyu Zhang, Yunfei Ma, and Krishna Chintalapudi. Their mentorship and collaboration during my internships were truly enriching experiences, and I am grateful for their expertise and encouragement. Specifically, the works advised by Pengyu Zhang and Yunfei Ma at Alibaba Group are the most important parts of this dissertation. I would also like to thank my managers Hongqiang Harry Liu and Ranveer Chandra who supported me during the internship and faculty job seeking.

I am indebted to my undergraduate advisors, Professor Xiaohua Tian and Xinbing Wang, for their guidance during my earlier academic journey. Their teachings and mentorship laid a solid foundation for my research pursuits and helped shape my scholarly interests.

I express my sincere gratitude to my collaborators, Tim Woodford, Kun Qian, Teng Wei,

Purui Wang, Bo Liang, Kejia Wang, and Kai Zheng, as well as others who have contributed to the papers associated with this dissertation. Their intellectual contributions and collaborative efforts have played a significant role in the development of my research work.

I would like to acknowledge my friends, Ke Sun, Song Wang, Jingqi Huang, Chen Chen, Yi Xu, and many others, for their unwavering support, camaraderie, and shared experiences during my Ph.D. journey. Their friendship and encouragement have made the challenging times more bearable and the successes more meaningful.

In closing, my heartfelt appreciation goes out to my parents, Jun Zhao and Suyuan Ren and other relatives for their unwavering love, support, and unwavering belief in me. Throughout my academic journey, their encouragement and sacrifices have been the bedrock of my success, particularly during the most challenging times of the pandemic. Their constant presence and reassurance have given me the strength and determination to persevere, and I am forever indebted to them for the opportunities they have provided me. Furthermore, I want to express my profound gratitude to my girlfriend, Zhiying Xu. She introduced me to the academic realm and remains the driving force behind my continued pursuit of this path. Her inspiration is a guiding light that propels me forward, and I am truly fortunate to have her by my side on this journey.

To everyone mentioned above, and to all those whose names may have inadvertently been omitted, please accept my sincerest thanks for your contributions and support. This dissertation would not have been possible without your unwavering assistance and encouragement.

Chapter 2 contains material from “SlimWiFi: Ultra-Low-Power IoT Radio Architecture Enabled by Asymmetric Communication”, by Renjie Zhao, Kejia Wang, Kai Zheng, Xinyu Zhang, and Leung Vincent, which appears in the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2023. The dissertation author was the primary investigator and author of this paper.

Chapter 3 contains material from “NFC+: Breaking NFC Networking Limits through Resonance Engineering”, by Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu and Ming Zhang, which appears in Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM), 2020. The dissertation author was the primary investigator and author of this paper.

Chapter 4 contains material from “RF-Chord: Towards Deployable RFID Localization System for Logistic Networks”, by Bo Liang, Purui Wang, Renjie Zhao, Pengyu Zhang, Xinyu Zhang, Hongqiang Harry Liu and Chenren Xu, which appears in the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2023. The dissertation author was the primary investigator and author of this paper.

VITA

2018	Bachelor of Engineering, Shanghai Jiao Tong University
2018–2020	Research Assistant, University of California San Diego
2020	Master of Science, University of California San Diego
2020–2023	Research Assistant, University of California San Diego
2023	Doctor of Philosophy, University of California San Diego

ABSTRACT OF THE DISSERTATION

Highly Reliable Communication and Sensing for Battery-free IoT

by

Renjie Zhao

Doctor of Philosophy in Electrical Engineering (Communication Theory and Systems)

University of California San Diego, 2023

Professor Xinyu Zhang, Chair

The Internet of Things (IoT) has experienced remarkable growth in recent years, with the number of IoT devices reaching 11.3 billion by 2020, surpassing even the global population as well as the combined market of smartphones, tablets, and PCs. However, this growth has been slower than the previous predictions of trillions of deployed IoT devices within the past decade. One of the primary reasons for this slower growth is the challenges posed by existing battery-supported architecture, including high device and maintenance costs, as well as environmental concerns, all of which hinder scalability. To overcome these obstacles, there is a proposal for battery-free IoT devices that can harvest energy from ambient sources. However, The conventional active radios used in IoT devices consume tens to hundreds of milliwatts of power, making them unsuitable for energy harvesting, which typically provides less than 10 µW of power. In response, researchers have been exploring new radio architectures for ultra-low-power (ULP) communication and sensing.

However, ULP communication and sensing techniques face reliability challenges that hinder their practical deployment. Two specific challenges are identified: Firstly, widely adopted backscatter communication systems are susceptible to double attenuation of the two-part channel, making them vulnerable to blockages and environmental changes. Secondly, ULP sensing systems typically have low bandwidth, making them susceptible to issues in indoor multipath-rich environments.

To address the reliability problem, this dissertation proposes the following contributions: Firstly, it introduces a novel system architecture that enables micro-watt-level active transmission, thereby improving communication reliability. Additionally, the system adopts an asymmetric communication scheme to reuse commodity devices, enhancing practicality and efficiency. Secondly, the dissertation presents a long-range magnetic RFID system that utilizes magnetic signals instead of electromagnetic signals. This innovative approach helps reduce the impact of blockages and environmental factors, ensuring more reliable and consistent performance. Finally, the dissertation introduces a multi-antenna wideband UHF RFID localization system that leverages the frequency-agnostic property of backscatter to collect wide bandwidth RFID signals. This system achieves more accurate and dependable localization results, particularly in challenging multipath-rich indoor environments.

Chapter 1

Introduction

Empowered by the advancements in mobile networks, today's Internet has successfully connected 5.1 billion people, accounting for approximately 64% of the global population [159]. This interconnectedness has given rise to an "internet of people" enabling a wide range of modern applications that have become an integral part of our daily lives, including video calling, video streaming, virtual reality (VR), augmented reality (AR), and more. However, it is worth noting that the growth in the number of connected individuals is gradually decelerating. In fact, the actual number of connected people since 2022 falls short by 200 million compared to earlier predictions [61], and this number is expected to be limited by the world's population itself.

Conversely, the number of the Internet of Things (IoT) has experienced remarkable growth, surpassing the global population and even the number of mobile devices, as illustrated in Fig. 1.1 [129]. This burgeoning field is only in its nascent stage but holds tremendous potential. We envision a future where billions, or even trillions, of IoT devices seamlessly connect wirelessly, bridging the gap between the physical and digital world. This interconnected network of objects, facilitated by computer management, will serve as the backbone for fully automating human life. It will usher in a new era of applications in environment and behavior sensing, asset tracking, and ambient human-computer interaction, transforming how we interact with and perceive the world around us.

However, it is essential to acknowledge that the concept of the Internet of Things (IoT) is

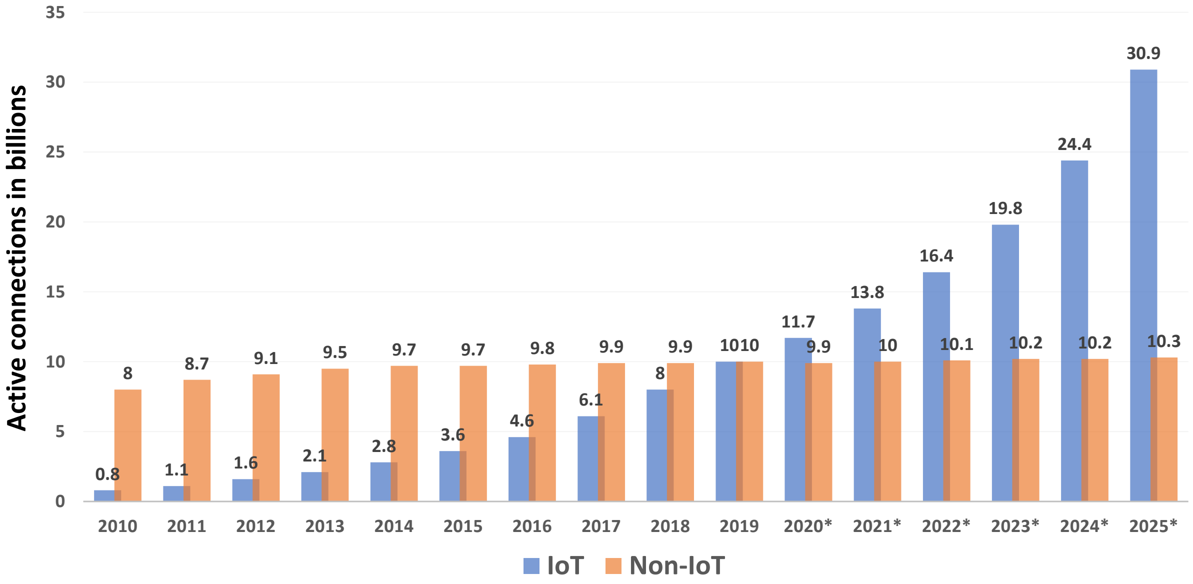


Figure 1.1. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. The data after 2020 are predictions.

not a recent development. As far back as the early 2000s, Kevin Ashton laid the foundation for what would eventually evolve into the IoT at MIT's AutoID lab [188]. Initially, there were lofty expectations surrounding IoT, with predictions suggesting that the number of IoT devices would reach an astounding one trillion by 2015 [150]. However, the reality proved to be more modest. In 2015, only 3.6 billion IoT devices were deployed, and by 2020, that number had increased to 11.3 billion [177]. This significant gap between expectations and actual figures raises questions about the reasons behind it and how we can achieve the deployment of one trillion IoT devices within the next decade.

1.1 Battery-powered v.s. Battery-free

The current battery-powered architecture employed in IoT poses significant challenges that impede its scalability. Although battery-powered systems have revolutionized the functionality of mobile devices like laptops, smartphones, tablets, and smartwatches, this same approach falls short in addressing the unique requirements of IoT devices, giving rise to several obstacles for massive IoT deployment:

- The cost of battery-supported IoT devices is prohibitively high. For instance, existing smart home sensors typically exceed $40 per device [82, 75]. Deploying tens or even hundreds of such devices within a home becomes financially burdensome for the majority of households.

- The limited battery life necessitates frequent recharging or replacement. Even if we assume a conservative three-year battery life for all one trillion IoT devices, the need to charge or replace close to one billion batteries each day would lead to exorbitant maintenance costs [76].

- Batteries introduce safety risks, such as the potential for combustion and severe environmental damage. For instance, improper handling or disposal of batteries can contribute to pollution and harm ecosystems [145].

On the other hand, battery-free IoT avoids these problems by replacing the battery with harvesting energy from ambient sources such as solar, radio waves, motion, etc. With the alternated power source, IoT devices can be battery-free, maintenance-free, and low cost, which makes widespread deployment feasible. The proliferation of trillions of battery-free IoT devices unlocks a vast array of new applications across various domains.

In the realm of consumer IoT, battery-free devices can revolutionize areas such as smart homes, wearable textiles, and biomedical or biological applications. By eliminating the need for batteries, these devices can seamlessly integrate into our daily lives, providing enhanced convenience and efficiency.

Furthermore, in industrial IoT, battery-free solutions have the potential to drive transformative changes in sectors such as logistics and manufacturing automation, as well as infrastructure monitoring. With the ability to operate without the limitations of batteries, these devices can enable more effective and scalable systems, optimizing processes and improving productivity.

The advent of battery-free IoT represents a promising future where energy-efficient, cost-effective, and widely deployed devices open up a multitude of possibilities for innovation and advancement across various industries and sectors.

1.2 Reliability Problems of Battery-free IoT

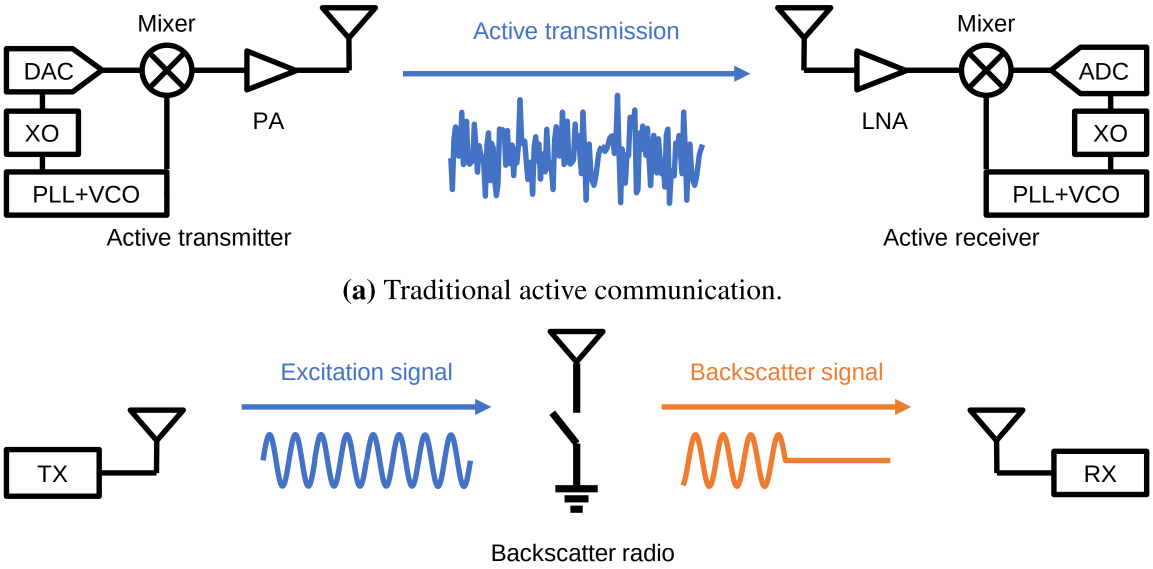
Despite the promising potential of battery-free IoT for large-scale applications, it is worth noting that these devices are often associated with reliability challenges. The power provided by energy harvesting sources is typically in the range of micro-watts, which is orders of magnitude lower than that of a traditional battery [191]. This limited power budget necessitates the development of novel ULP communication and sensing techniques that consume significantly less power than conventional methods. However, ULP communication and sensing methods are frequently plagued by unreliability, posing obstacles to the practical deployment of these systems. This unreliability may result in additional costs associated with fixing the inaccuracies in the system's output.

To thoroughly investigate the underlying causes of unreliability, this section will provide background information and discussions on typical ULP communication and sensing techniques. For more comprehensive details on related research, please refer to the subsequent chapters.

1.2.1 Ultra-Low-Power Communication

The conventional active communication radio architecture is widely recognized for its high power consumption due to the trade-offs made by the hardware between power consumption and competing requirements such as range, bit rate, and spectrum efficiency. Fig. 1.2a illustrates a typical active transmitting radio[1], which comprises three key components: a high-power and high-linearity power amplifier (PA) to ensure adequate transmit power and low distortion, a crystal oscillator (XO) reference and carrier generator consisting of a phase-locked loop (PLL)

[1] In the IoT application, there is usually more uplink traffic (from IoT to the host device) than downlink (from the host device to IoT). Therefore, we will mainly focus on the uplink communication technique. Downlink communication is studied by many works like [143, 201, 200, 199]



(a) Traditional active communication.

(b) Backscatter communication.

Figure 1.2. High power traditional active transmitter v.s. ultra-low-power backscatter communication.

and voltage-controlled oscillator (VCO) to maintain a stable carrier frequency, and a high-resolution digital-to-analog converter (DAC) to support complex modulation schemes. These power-intensive hardware components are primarily responsible for the high power consumption [42]. For instance, Wi-Fi transmitters typically consume around 300 milliwatts (mW) [92], BLE transmitters consume 10.2 mW [149], ZigBee transmitters consume 6.9 mW [148], and LoRa transmitters consume 32.4 mW [171].

To mitigate power consumption, researchers have proposed backscatter techniques, which offload power-consuming components from the IoT device to a helper device. As depicted in Fig. 1.2b, the helper device generates an excitation signal that assists the IoT device in eliminating the need for a power amplifier, clock generation components, and further replaces the high-resolution DAC by utilizing simple modulation. The IoT device then backscatters and modulates the excitation signal, which is received by another RX device. Consequently, the backscatter device only requires an RF switch and an antenna, consuming power in the micro-watt range, which is more than four orders of magnitude lower than traditional active radios.

However, backscatter communication suffers from a two-part channel (the forward one for the excitation signal and the backward one for the backscatter signal), resulting in double attenuation of the tag signal. Additionally, imperfections in the tag circuit introduce significant signal loss. As a result, existing UHF RFID systems and even state-of-the-art frequency-shift-based backscatter approaches achieve a limited range of less than 10 meters. Greater distances of a few tens of meters from the RX device can only be achieved when a TX device is in close proximity to the tag (i.e., 1–2 meters away), which is not always feasible in many scenarios [109, 211, 221].

Moreover, backscatter communication is more susceptible to the influence of blockages or environmental changes, as the effects are doubled in comparison to active communication. This makes backscatter communication less reliable and more vulnerable than active communication, especially considering that most typical IoT application scenarios operate close to the system's maximum operating range.

In this dissertation, I address the issue of unreliability by pursuing two approaches. Firstly, I propose a novel system architecture that enables micro-watt-level active transmission instead of relying on backscatter, thereby improving reliability. Secondly, I design a long-range magnetic RFID system that utilizes magnetic signals instead of electromagnetic signals, thereby reducing the impact of blockages and environmental factors.

1.2.2 Ultra-Low-Power Sensing

To enable the seamless integration of the physical and digital worlds, IoT devices must be capable of sensing their surrounding environment. One highly promising approach for obtaining sensing information is through the reuse of wireless signals. By leveraging the phase and timing information of these signals, it becomes possible to extract valuable location information from IoT devices.

However, existing ULP signals often fail to provide reliable sensing results. In order to minimize power consumption, current low-power wireless communication schemes generate signals with limited bandwidth. This limited bandwidth, denoted as B, leads to a restricted range resolution of c/B, where c is the speed of light. The range resolution determines the ability to distinguish between signals that traverse different path lengths. Consequently, in environments with multiple signal paths (multipath-rich), all signals with path length differences smaller than c/B become combined, resulting in ranging errors larger than c/B. For instance, consider the UHF RFID signals with a bandwidth on the order of 100 kHz. In this case, the ranging error can exceed 3000 meters. Consequently, the localization and sensing accuracy are severely compromised, leading to highly unreliable results.

To tackle this challenge, I developed a multi-antenna wideband UHF RFID localization system. This system capitalizes on the observation that backscatter modulation is frequency agnostic, enabling RFID tags to modulate all transmitted signals in the environment. By generating a wider bandwidth signal alongside the carrier signal of the RFID reader, we can achieve a broader signal bandwidth from the RFID tag. Consequently, more reliable localization results can be obtained due to the increased signal bandwidth, especially in the multipath-rich indoor environment.

1.3 Dissertation Contributions

This dissertation explores fundamental factors that limit the communication and sensing reliability of battery-free IoT applications. Based on a thorough understanding of the whole system, from the application down to the analog and digital circuits, we have employed a set of techniques, including hardware design, wireless communication, and operating systems, to significantly improve the reliability of battery-free IoT systems. The main contributions of this dissertation are:

- In Chapter 2, we first designed a system called SlimWiFi [218] that improve the reliability of battery-free IoT communication. We proposed a novel simplified active radio architecture that has a more robust performance compared to backscatter communication. To address the compatibility problem with the existing wireless infrastructure, we proposed a novel asymmetric communication scheme that enables COTS Wi-Fi devices to directly communicate the simplified active radio. Through a careful codesign of the signal modulation scheme and reverse processing of the Wi-Fi data, SlimWiFi enables existing Wi-Fi access points to modulate/demodulate on-off keying (OOK) waveform sent by an extremely low-power IoT tag. With this measure, SlimWiFi radically simplifies the IoT radio architecture, evading power-hungry components such as data converters and high-stability carrier generators. Through collaboration with RFIC experts, we taped out the integrated chip version of SlimWiFi radio and verified it can perform active data transmission at sub-100 µW power, 3 orders of magnitude lower than standard IoT radios! The final system can achieve a robust communication performance with around 100 kbps goodput up to a range of 50 m.

- We further explored the methods to improve the reliability of RFID reading in practical logistic network applications in Chapter 3. We found the root cause of the reliability issue lies in the UHF signal properties. The high carrier frequency electromagnetic signal will be inevitably blocked by RF-unfriendly items like water/metal containers (which leads to miss-reading) and will experience strong reflections in the indoor environment (which leads to cross-reading). Therefore, we designed a novel system called NFC+ [219] which uses the lower carrier frequency magnetic waves of near-field communication (NFC) systems. Traditional NFC systems work in a very short range, which has hampered their deployment in practice. In contrast, NFC+ is a new NFC reader hardware architecture, leveraging resonance engineering and MIMO techniques to reach commercial NFC tags at a long range. Compared to UHF RFID, NFC+ can reduce the miss-reading rate from 23% to 0.03%, and the cross-reading rate from 42% to 0, for randomly oriented objects within a range of 3 meters. NFC+ works even in RF-adverse settings, e.g., tracking water bottles and objects shielded by metal. NFC+ is in the process of being integrated into Alibaba's latest logistic network for online shopping, grocery delivery and local life services.

- Chapter 4 introduces a system that can localize battery-free UHF RFID tags with higher reliability. We found that the existing UHF RFID localization techniques are not reliable enough for industry settings, due to RFID's narrow bandwidth and hence coarse time/distance resolution. To address the high reliability requirements, we designed a system called RF-CHORD [119] which consists of COTS UHF RFID readers and our own UHF RFID sniffer hardware which can capture the tag signal across multiple antennas and wide bandwidth. We further incorporated FPGA and GPU acceleration to process the signal in real time. Combined with a multipath-suppression algorithm, RF-CHORD can determine whether the tag is in the range of interest with extremely high confidence. It can localize up to 180 tags 6 m away from a reader within 1 second and with a 99th long tail error of 0.786 m. RF-CHORD was demonstrated at Alibaba Apsara Conference 2021 and received lots of interest from the attendees in the supply chain industry.

Chapter 2

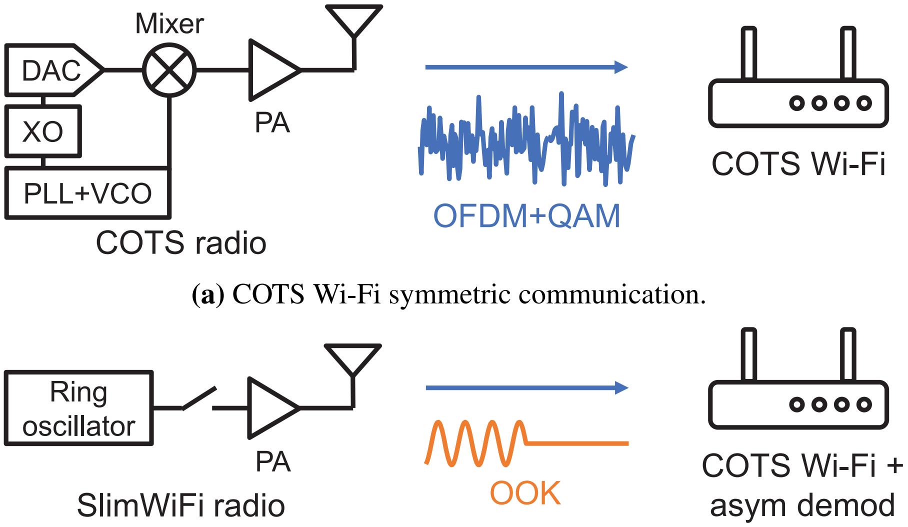
Asymmetric Communication for Ultra-Low-Power IoT

2.1 Introduction

The Internet of Things (IoT) is playing a key role in bridging the physical and digital worlds. IoT will act as the workhorse to fully automate human life, through a new wave of applications in environment/behavior sensing, asset tracking, ambient human-computer interaction, *etc.* As of 2021, the population of active IoT endpoints already reached 12.2 billion, and will surge towards 27 billion in 2025 [81]. Maintaining the connectivity between the IoT fabric and the existing Internet infrastructure entails non-trivial human efforts, and will ultimately be feasible only if the IoT devices can sustain themselves, *e.g.*, through RF energy harvesting.

In practice, RF energy harvesting can usually reach at most tens of µW [191] for IoT devices, so any self-sustainable communication paradigm has to adhere to this limit. RFID represents one such paradigm, which is truly battery-free and communicates by merely harvesting and remodulating the RF power from an interrogator (reader). Yet to date, RFID has witnessed limited adoption in consumer applications, due to its limited communication range, relatively high cost of the reader, and limited functionality (mostly restricted to reading preprogrammed information on passive tags).

Ideally, we would prefer to reuse the existing wireless infrastructures (*e.g.*, the pervasive Wi-Fi) as gateways to connect the ultra-low-power (ULP) IoT radios to the Internet. Unfortu-



(a) COTS Wi-Fi symmetric communication.

(b) SlimWiFi asymmetric communication.

Figure 2.1. Comparison between COTS Wi-Fi and SlimWiFi.

nately, mainstream wireless communication standards cannot support battery-free operations due to their high *peak power*. For example, the commercial off-the-shelf (COTS) Wi-Fi, BLE, ZigBee, NB-IoT, and LoRa devices all require tens to hundreds of mW of peak power [92, 149, 148, 171], orders of magnitude higher than that available from RF energy harvesting. Their self-sustained operations are feasible only under an extremely low duty cycle (a few dozen bytes per day) while supported by a bulky power source (*e.g.*, a solar panel).

We argue that the root cause of the high power consumption of such systems lies in the requirement of *symmetric communication*, *i.e.*, the IoT radios must adopt the same high-profile modulation/demodulation hardware as the existing wireless infrastructures. As illustrated in Fig. 2.1a, to be compatible with existing Wi-Fi access points (APs), an IoT radio needs to support OFDM and QAM, which entails stringent hardware requirements, such as accurate and stable carrier frequency, low phase noise, wideband and high-resolution ADC/DAC, and a high-gain high-linearity (but often low-efficiency) power amplifier, all of which translate into power hungry components. We thus pose an important question: *Is it possible to relax such requirements and make the communication hardware and modulation asymmetric?*

We explore the answers through a novel system design called *SlimWiFi*. SlimWiFi adopts a novel *asymmetric communication* scheme to realize Wi-Fi-compatible ULP radio. Specifically, the SlimWiFi ULP radio builds on a highly simplified architecture as shown in Fig. 2.1b, capable of only modulating/demodulating on-off keying (OOK) waveforms. But it can directly communicate with existing Wi-Fi APs that are designed to modulate/demodulate sophisticated OFDM waveforms. Essentially, SlimWiFi shifts the PHY layer complexity to the high-power infrastructure side, and by doing so, it can improve the energy efficiency of the IoT radio by orders of magnitude. Unlike the backscatter-based systems[109, 97, 211, 84] that rely on additional helper devices to generate external carrier signals, SlimWiFi is an active, stand-alone radio transceiver. To materialize the design principles behind SlimWiFi, we need to address two key challenges.

(a) How to enable direct communication between asymmetric hardware, i.e., the OFDM-based Wi-Fi device and the OOK based SlimWiFi device? The uplink communication, *i.e.*, demodulating the OOK signal with an unmodified Wi-Fi OFDM device, is very challenging due to the highly incompatible waveforms and demodulation hardware. Note, however, that any demodulation process is essentially sampling and mapping analog waveforms into a binary sequence. The SlimWiFi Wi-Fi receiver thus reverses its OFDM demodulation steps, as well as the Forward-Error-Correction (FEC) decoder, and descrambler, and then reconstruct the incoming OOK symbols merely based on the payload bits reported by the Wi-Fi driver. With this measure, an ordinary Wi-Fi AP can decode the OOK signals from the ULP SlimWiFi transmitter, *without any hardware modifications*. On the other hand, the downlink modulation is straightforward, as recent work [97, 211, 202] has well-explored ways of mapping a sequence of bits into a pseudo-OOK waveform using a WiFi transmitter. To achieve MAC layer compatibility, SlimWiFi delegates the carrier sensing task to the Wi-Fi AP, which uses the CTS-to-self packets to virtually reserve the channel, and then informs the SlimWiFi node to start its transmission.

(b) How to optimize the SlimWiFi radio hardware to minimize power consumption while maintaining Wi-Fi compatibility? In commensurate with the complicated modulation, the typical

hardware architecture of a COTS Wi-Fi radio necessarily consists of a power amplifier (PA) for a high transmit power, high precision and wideband digital-to-analog converter (DAC) for high-order modulation, and phase-locked loop (PLL) and voltage-controlled oscillator (VCO) for accurate carrier generation. The power consumption of these components is fundamentally governed by physical laws, and almost impossible to fall below several mW [137, 154, 41, 56]. SlimWiFi circumvents the fundamental limitation with a highly simplified radio architecture that leverages asymmetric communication. The SlimWiFi ULP radio eliminates the power hungry DAC/ADC and PLL and affords a more efficient PA owing to the lower power and linearity requirements. As for carrier generation, we adopt a free-running ring oscillator [216], which bears a low frequency stability, but suffices for SlimWiFi as its narrowband OOK signal can be asymmetrically demodulated as long as the carrier falls within the 2.4 GHz ISM band.

To verify the effectiveness of our design, we implement asymmetric communication with a COTS Wi-Fi device and a prototype SlimWiFi device. Our experiments demonstrate that the OOK based SlimWiFi signals can be decoded from the payload bits of the Wi-Fi device over a range of 60 m, with a goodput of around 100 kbps. We have also designed and taped out a SlimWiFi IC based on the aforementioned SlimWiFi radio architecture. Our measurement shows that the SlimWiFi only consumes around 90 µW of power, approximately 3 orders of magnitude lower compared with COTS WiFi radios.

To summarize, we make the following contributions through the SlimWiFi design and implementation.

- We propose SlimWiFi, a novel asymmetric communication paradigm that enables COTS Wi-Fi devices to decode OOK signals from ULP radios. The design enables such ULP radios to reuse the existing Wi-Fi as the IoT infrastructure, which can substantially reduce the deployment cost for attaining ubiquitous connectivity.

- We introduce a new SlimWiFi ULP radio architecture, which leverages the asymmetric communication to enable the first *active* Wi-Fi-compatible transmitter at a peak power of

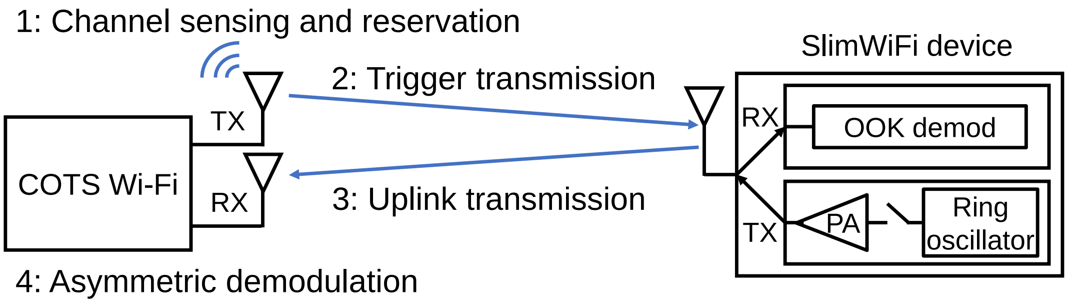


Figure 2.2. Workflow of a SlimWiFi uplink transmission.

tens of μW.

- We implement the asymmetric communication system through a PCB prototype and IC tape-out. Our experiments verify the potential of SlimWiFi in supporting self-sustained IoT communication.

2.2 System Workflow

The SlimWiFi design mainly focuses on the IoT uplink, consisting of the SlimWiFi device and the COTS Wi-Fi radio. The former transmits OOK modulated data, through a highly simplified ULP radio architecture. The latter acts as the demodulator and gateway to connect the SlimWiFi device to the Internet. As illustrated in Fig. 2.2, a typical uplink transmission attempt involves the following workflow.

(1) The Wi-Fi device first runs standard carrier sensing to acquire the channel and reserves access by transmitting the CTS-to-self frame.

(2) The Wi-Fi device emulates an OOK modulated trigger frame by manipulating the Wi-Fi bit sequence. The SlimWiFi device's ULP OOK receiver decodes the information and synchronizes with the trigger frame.

(3) Following step (2) immediately, the Wi-Fi device initiates the demodulation procedure of its receiver chain, and meanwhile, the SlimWiFi device sends an OOK modulated uplink signal to the Wi-Fi device.

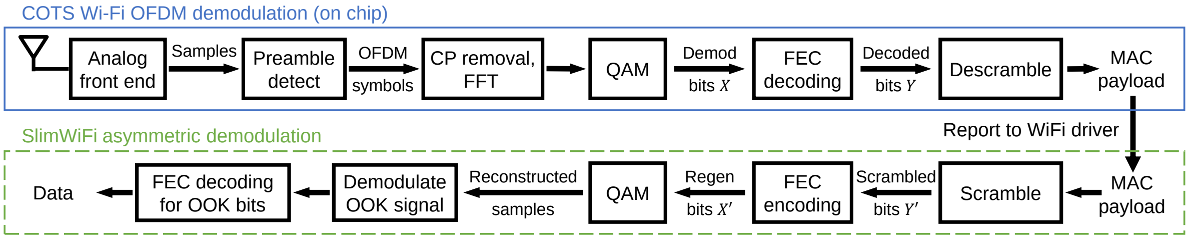


Figure 2.3. Receiving procedure of a SlimWiFi uplink receiver, *i.e.*, the COTS Wi-Fi device.

(4) The Wi-Fi device decodes the OOK modulated signal by applying asymmetric demodulation.

In what follows, we introduce the SlimWiFi asymmetric communication design (Sec. 2.3) and the SlimWiFi ULP radio hardware (Sec. 2.4). Our exposition mainly focuses on the novel uplink design (steps 3 and 4). The ULP downlink design (step 2) follows the same asymmetric modulation + simplified hardware principle. It builds on recent cross-technology communication (CTC) and backscatter techniques [97, 118, 167, 60, 202], and will be discussed briefly in Sec. 2.4.4.

2.3 Asymmetric Demodulation for SlimWiFi

In this section, we first provide a quick primer on the standard Wi-Fi receiver. Then we introduce the Wi-Fi compatible asymmetric communication in SlimWiFi.

2.3.1 A Primer on Standard Wi-Fi Receiver

Without loss of generality, we focus on 802.11n, a standard adopted by most modern COTS Wi-Fi devices, running on a 20 MHz channel and single antenna [113]. The upper part of Fig. 2.3 shows the 802.11n demodulation procedure, which is hard coded into the receiver's IC. The incoming analog signals are first captured by the RF front end and converted into baseband samples. The receiver searches across the samples to identify a standard 802.11 preamble–a predefined OFDM modulated training sequence. If no valid preamble is detected, the samples will be discarded. Otherwise, the receiver will proceed to additional demodulation steps.

The samples are first sliced into *OFDM symbols*, each consisting of 16 samples of cyclic prefix (CP) and 64 samples of data. The CP is redundant samples used to overcome inter-symbol interference due to the multi-path effect. The Wi-Fi demodulator needs to remove the CP and apply a 64-point FFT to convert the 64 data samples into frequency-domain, which essentially slices the entire 20 MHz band into 64 *subcarriers*. Only 52 of the subcarriers are extracted as valid data. The remaining are either null subcarriers to mitigate adjacent channel interference or pilots for calibrating the residual offsets of the channel estimation.

Afterwards, a QAM block demaps the complex sample on each subcarrier into one or more bits, depending on the baseband modulation method, *i.e.*, BPSK, QPSK, 16-QAM, and 64-QAM. The resulting bit sequence X contains redundant bits due to forward-error-control (FEC) and needs to be decoded into a sequence Y. The ratio between the length of Y and X is called *coding rate* and can be 1/2, 2/3, 3/4, or 5/6.

The decoded bits Y need to be further reordered to recover the original transmitted bits. This so-called *descrambling* is performed by an XOR operation with a repeatedly generated 127-bit sequence whose initial state is determined by a *scrambler seed*. The PHY layer processing ends here and the output bits will be reported to the upper layer as a MAC frame. We emphasize that *the entire PHY-layer demodulation is implemented in the Wi-Fi IC and thus cannot be bypassed without hardware modification*.

On the other hand, the MAC layer control, management, and frame processing are usually implemented in software (Soft MAC) or firmware (Full MAC) [86, 121]. The MAC frames will be passed to the Wi-Fi driver and can be post-processed in software.

2.3.2 Overview and Challenges in Asymmetric Demodulation

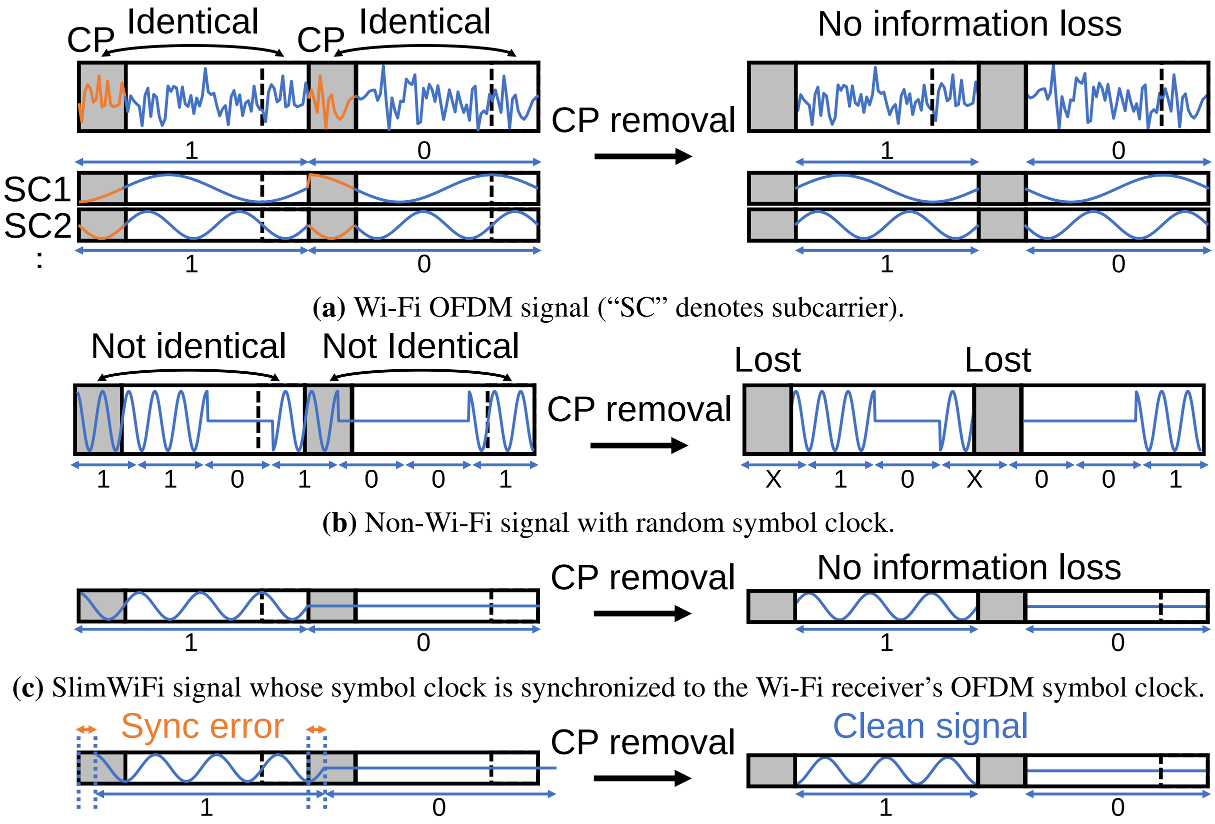
The asymmetric demodulation design is grounded on a key observation: *The Wi-Fi OFDM demodulation procedure is deterministic and at least partially reversible.* An OFDM receiver essentially converts the incoming time domain samples into frequency domain through FFT, and then “quantizes” the samples through QAM demapping. Theoretically, any signals within the 20 MHz bandwidth can be *reconstructed from the OFDM receiver's bit sequence output*, by reversing the Wi-Fi demodulation procedure. *The SlimWiFi asymmetric demodulator essentially performs such reconstruction in software at the Wi-Fi receiver to recover the incoming OOK waveforms and subsequently demodulate them*, as illustrated in the bottom part of Fig. 2.3.

Unfortunately, the standard Wi-Fi receiver blocks, such as CP removal, QAM, and FEC, inevitably induce information loss or ambiguities. As a result, SlimWiFi must address the following key challenges.

(1) How to design the OOK signal in order to avoid the impact of information loss while enabling asymmetric demodulation? The hard-coded OFDM demodulation procedure does eliminate certain incoming samples. For example, CP removal erases part of the signal in the time domain, and data subcarrier extraction removes all information in the non-data subcarriers (*i.e.*, null and pilot subcarriers). If the removed segments contain useful data symbols from the SlimWiFi device, it would be hard to reconstruct them. We thus need to carefully design the SlimWiFi OOK waveform to avoid the impact of information loss (Sec. 2.3.3).

(2) How to deal with the reconstruction errors introduced by the COTS receiver? Besides the information loss from the OFDM block, the QAM and FEC blocks also cause two types of reconstruction errors: *Quantization error*, *i.e.*, the difference between the SlimWiFi signal and the closest point in Wi-Fi's QAM constellation; and *coding error*, *i.e.* the mismatch between the Wi-Fi demodulated bit sequence X and the regenerated bit sequence X' after reversing the FEC, as shown in Fig. 2.3. SlimWiFi addresses the reconstruction errors by (i) judiciously configuring the receiver parameters and (ii) performing additional channel coding on top of the SlimWiFi signals, as to be described in Sec. 2.3.4.

(3) How to integrate SlimWiFi with standard Wi-Fi protocols? To make SlimWiFi fully compatible with standard Wi-Fi, several PHY/MAC layer primitives are needed, *e.g.*, generating PHY preamble, PHY/MAC headers, and triggering the Wi-Fi receiver to start demodulation. We address these practical challenges in Sec. 2.3.5.



(a) Wi-Fi OFDM signal ("SC" denotes subcarrier).

(b) Non-Wi-Fi signal with random symbol clock.

(c) SlimWiFi signal whose symbol clock is synchronized to the Wi-Fi receiver's OFDM symbol clock.

(d) SlimWiFi signal with synchronization error.

Figure 2.4. Symbol clock sync to counteract CP removal.

2.3.3 SlimWiFi Signal Design

Overcoming signal erasures on the COTS Wi-Fi demodulator

In this section, we introduce the transmission waveform of the SlimWiFi device which are designed to circumvent the signal erasures on the COTS Wi-Fi demodulator.

As shown in Fig. 2.4a, the standard Wi-Fi waveform inside a CP is a replica of the last 0.8 µs of the OFDM symbol (4 µs in total) hosting the CP. Therefore, removing the CP does not cause any information loss for the Wi-Fi demodulator. In contrast, for a non-Wi-Fi signal with an arbitrary symbol clock (Fig. 2.4b), this operation may inadvertently erase 20% of the original signal which makes the demodulation unreliable. To overcome this issue, we choose to synchronize the OOK symbol clock of the SlimWiFi device with the OFDM symbol clock of the Wi-Fi receiver, *i.e.*, 250 kHz for 802.11n. Fig. 2.4c shows that, with such symbol-level clock synchronization, the SlimWiFi signal acts the same as the signal of one Wi-Fi subcarrier (in Fig. 2.4a). Therefore, the signal erasure caused by CP removal can be avoided. To realize the symbol level clock synchronization, the SlimWiFi device simply generates a 250 kHz clock and aligns its transmission time to the aforementioned trigger frame (Sec. 2.2). Such synchronization relies on symbol energy detection and may not be precise. However, as shown in Fig. 2.4d, the redundant CP part can be utilized to tolerate the synchronization errors, which we will further verify in Sec. 2.6.2.

Recall that 12 out of the 64 subcarriers within the 20 MHz Wi-Fi channel are null or pilot subcarriers, eventually discarded by the Wi-Fi demodulator. Therefore, to prevent information loss, the SlimWiFi device should avoid modulating its OOK waveform at the same frequencies as the non-data subcarriers. This in turn imposes more constraints on its signal bandwidth and carrier frequency, which we address below.

Relaxing the hardware requirements on the SlimWiFi radio device

Range, TX power, and bandwidth. The communication range of the SlimWiFi uplink can be estimated based on the classical link budget equation [223]:

$$k_bT_aB + NF + SNR_o = P_{TX} + G_{TX} + G_{RX} - 20log_{10}(4\pi d f_c/c)$$

where k_b is the Boltzmann constant, and T_a is the equivalent noise temperature in [K]. B, NF, and SNR_o denote the signal bandwidth, RX noise figure, and SNR threshold for robust decoding, respectively. P_{TX}, G_{TX}, and G_{RX} are TX power, TX, and RX antenna gain, respectively. d is the operating range, f_c is the carrier frequency and c is the light speed.

To achieve a target range d while keeping the SlimWiFi device at ULP, we propose to reduce B, which can in turn lower the total transmit power P_{TX}. This design choice hinges on the observation that we can treat each subcarrier of the OFDM receiver as an individual narrow-band (312.5 kHz) channel. As long as the SlimWiFi signal falls within one of the subcarriers, it can be captured and demodulated by the OFDM receiver. Therefore, even if its P_{TX} is reduced by $10log_{10}(20000/312.5) = 18$ dB, the total power of a SlimWiFi symbol can still be equivalent to that of a Wi-Fi subcarrier, and SlimWiFi can still keep the same transmission range as a normal Wi-Fi! The operating range can be further traded off for even lower transmit power. In fact, with the 250 kHz OOK symbol rate the SlimWiFi signal bandwidth is 250 kHz which can already fit within one Wi-Fi subcarrier.

Carrier frequency requirement. Most existing communication standards require an accurate carrier frequency. In particular, a highly stable carrier is crucial for synchronizing OFDM TX and RX, and reducing leakage between subcarriers. However, this usually entails a high-profile carrier generator, consisting of a VCO and PLL which consumes several mW power [175, 128, 163]. The SlimWiFi asymmetric demodulation circumvents this requirement for the first time. As long as the OOK signal's carrier frequency f_C is located within the 20 MHz Wi-Fi band, it can be captured and recovered by demodulating the Wi-Fi receiver's subcarrier that covers f_C. However, two issues need to be solved to accommodate the inaccurate carrier frequency.

First, f_C might be in the non-data subcarriers which are discarded by the Wi-Fi receiver. We overcome this problem by making use of the partially overlapped Wi-Fi channel designated in the 2.4 GHz band, where the non-data subcarriers of one channel are the data subcarriers of an adjacent channel, as shown in Fig. 2.5. With this mechanism, the carrier frequency requirement can be further relaxed from 20 MHz (a single Wi-Fi channel) to 80 MHz (the entire 2.4 GHz ISM band covering 13 Wi-Fi channels). Note that, the Wi-Fi receiver can identify the subcarrier where the SlimWiFi signal is located by simply checking the subcarrier energy level. If the Wi-Fi receiver does not observe any uplink signal after the trigger frame (Sec. 2.2), then the signal may fall on a non-data subcarrier, and the receiver should switch to an adjacent channel instead.

The second issue is that the OOK carrier frequency f_C may not be aligned exactly with an OFDM subcarrier. Although OOK can be demodulated non-coherently, the carrier frequency offset (CFO) leads to non-orthogonality in the Wi-Fi receiver's FFT processing, which may in

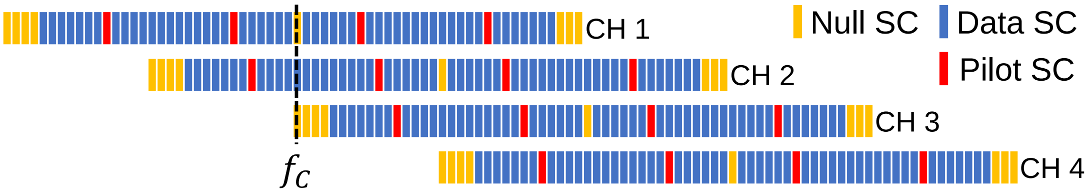


Figure 2.5. Subcarrier mapping between different channels of Wi-Fi on the 2.4 GHz band. Only 4 channels are illustrated.

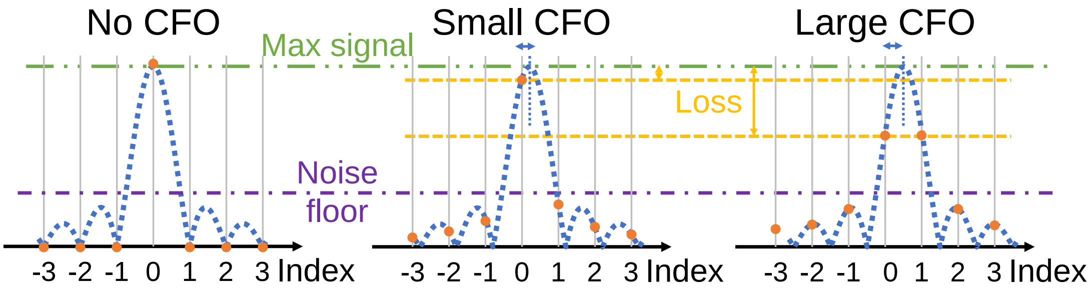


Figure 2.6. Amplitude of different subcarriers with or without the CFO, when receiving a single tone OOK signal.

turn affect the asymmetric demodulation. Fig. 2.6 illustrates a case where a single tone signal (OOK with ON state) spreads to multiple subcarriers due to CFO. Demodulating the OOK signal on a single subcarrier will result in a low SNR. Combining the signal energy across subcarriers does not necessarily help either because it increases the noise bandwidth. Nonetheless, the worst-case SNR loss due to CFO is only 3 dB (signal spreads evenly between two adjacent subcarriers), which will be verified in Sec. 2.6.2.

2.3.4 Resolving Quantization and Coding Errors

QAM and quantization error

The Wi-Fi receiver's QAM demapping block quantizes the phase and amplitude of the signal on each subcarrier. Fig. 2.7 illustrates the case when a SlimWiFi OOK signal is demapped on a 64-QAM constellation diagram. For the ON state of OOK, the signal sample will have a non-zero amplitude with an arbitrary phase, hence falling at the outer circle. For the OFF state, the sample will have a near-zero amplitude, falling at the origin point. For other subcarriers where no active signals are located, the demapped sample will be the same as the OFF state.

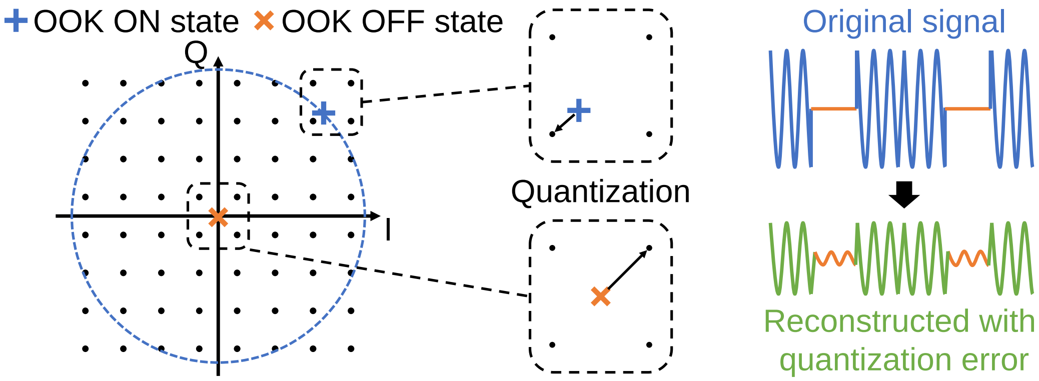


Figure 2.7. OOK modulated signal with QAM demodulation.

Essentially, the QAM demapping is performing quantization in the complex domain. Thus the original OOK signal on the active subcarrier can be easily reconstructed through the reverse operation, *i.e.*, QAM mapping which converts bits to a complex number. However, this process will introduce quantization errors, which compromises the SNR of the reconstructed signal. The quantization error depends on the precision of quantization which is determined by QAM modulation order. We thus configure the Wi-Fi receiver to the highest modulation order 64-QAM, leading to the lowest quantization error.

FEC and coding error

When receiving the non-OFDM SlimWiFi signal, the FEC block causes a mismatch between the demodulated bit sequence X and regenerated bit sequence X' shown in Fig. 2.3. The fundamental reasons are two-fold: (i) The demodulated bit sequence can be treated as an arbitrary bit sequence instead of a valid codeword of FEC; (ii) The standard Wi-Fi FEC decoding is a many-to-one mapping, whereas the reverse operation (*i.e.*, FEC encoding in Fig. 2.3) is a one-to-one mapping. So there is no guarantee that the reconstructed X' can match the original X by simply reversing the FEC.

Fortunately, we found that the number of mismatched bits is limited and can be mitigated with a careful design. The coding errors induced by the two standard FEC schemes in Wi-Fi, *i.e.*, binary convolutional coding (BCC) and low-density parity check (LDPC), are different. Here we

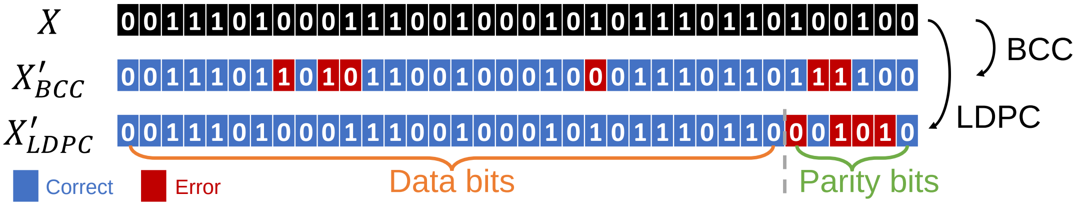


Figure 2.8. Distribution of coding errors (mismatch between X and X'), for BCC and LDPC, respectively.

only summarize their properties. The detailed proofs are in Appendix A.

(1) Both BCC and LDPC incur fewer coding errors at a higher coding rate. Therefore, we configure the Wi-Fi receiver to the highest available coding rate (*i.e.*, 5/6) when performing the asymmetric demodulation. With this measure, the fraction of FEC-induced errors can be reduced to around 1/6 and can be further reduced if we apply a separate FEC coding on the SlimWiFi OOK transmitter.

(2) When the Wi-Fi receiver runs the LDPC decoder, the locations of the FEC errors are known a priori on the time-frequency domain. Fig. 2.8 shows an example of the error distributions when using BCC and LDPC with 5/6 coding rate. X'_{BCC} and X'_{LDPC} are the regenerated bit sequence under BCC and LDPC, respectively. The mismatched bits of the BCC scheme are spread randomly all over the bit sequence X'_{BCC} due to the BCC decoding and interleaving. In contrast, the mismatched bits of the LDPC scheme is always located at the parity bits block (also proven in Appendix A.2).

Based on this observation, we configure the Wi-Fi receiver to LDPC mode in the asymmetric demodulation, which brings two advantages: (i) The error bits are distributed in a periodic way across the reconstructed sequence X' (more details in Sec. 2.3.6). Therefore, they can be easily corrected by applying a convolutional encoding on the data from SlimWiFi device and using a convolutional decoder on the asymmetric demodulator. (ii) The receiver knows which bits are parity bits (*i.e.*, where the coding errors are clustered). The convolutional decoder can adopt a soft decision decoder which sets those bits with a low log-likelihood ratio, thus improving the decoding performance.

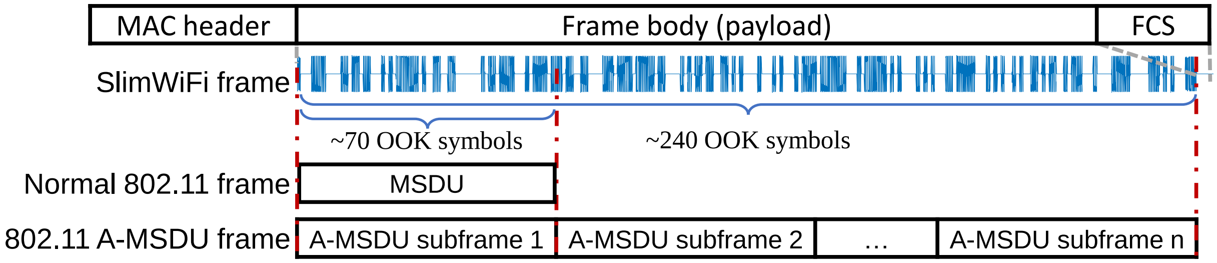


Figure 2.9. Mapping between the standard Wi-Fi MAC frame and SlimWiFi signal waveform.

2.3.5 Practical Challenges

MAC layer configuration

To ensure the MAC payload bits can be used to reconstruct the SlimWiFi signal, we need to resolve two issues: (i) incorrect frame check sequence (FCS), and (ii) limited MAC frame length.

Incorrect FCS. As shown in Fig. 2.9, the FCS, a 32-bit cyclic redundancy check (CRC) located at the end of the whole frame, is adopted for error protection. Since the received signal is an OOK modulated instead of a valid Wi-Fi signal, it is nearly impossible that the FCS is correct. But we need to capture the data frames through the Wi-Fi driver, even if they fail the FCS check. This is supported by many COTS Wi-Fi devices [64, 31]. A simple software/firmware update can enable the same capability on other Wi-Fi devices.

Data frame length. The length of the payload in a normal Wi-Fi frame is limited by the 2,304 bytes maximum size of the MAC Service Data Unit (MSDU). Recall that SlimWiFi needs to configure the Wi-Fi receiver to the highest data rate (64-QAM, 5/6 code rate, Sec. 2.3.4). Under this configuration, the maximum number of OFDM symbols is less than 70, corresponding to only 70 OOK symbols as illustrated in Fig. 2.9. To create a longer frame, we choose to use the aggregate MAC service data unit (A-MSDU) with a quality of service (QoS) data frame, whose maximum size is 7,935 bytes, which extends the frame length to about 240.

Scrambler seed

Since the descrambling is a one-to-one mapping operation on the Wi-Fi receiver, it can be easily reversed by applying a scrambling block with the same scrambler seed. Although the scrambler seed is not reported to the driver, it is set by the PHY header which triggers the receiver's demodulation process (Sec. 2.3.5). Therefore, we can just set a fixed scrambler seed, which can be used to reverse the descrambling block.

Initiating the receiving procedure on Wi-Fi

The final practical challenge lies in generating a valid Wi-Fi preamble and PHY/MAC header. The preamble is needed for triggering the Wi-Fi receiver to start the receiving procedure (packet detection), and is also used for auto gain control, synchronization, and channel estimation. The PHY/MAC header is needed for specifying demodulation parameters such as QAM order, coding rate, scrambling seed, and packet length. Unfortunately, the Wi-Fi preamble and PHY/MAC header are complex OFDM modulated signals, and cannot be directly generated by the SlimWiFi ULP transmitter.

Note that many Wi-Fi devices have separate but co-located transmitter and receiver modules. For example, many Wi-Fi APs [40, 39, 147] usually have multiple transceiver chips (to support concurrent multi-band and multi-antenna operation) which can be configured as co-located TX and RX modules. Therefore, we repurpose the co-located Wi-Fi TX module as an *initiator* to emit a self-initiation frame, comprised of the legitimate preamble and PHY/MAC header but without any payload. Such zero-payload frames are supported by Wi-Fi drivers such as Nexmon [169], or through Wi-Fi frame emulation methods [100]. Upon receiving the initiation frame, the receiver starts its Wi-Fi demodulation workflow followed by the asymmetric demodulation (Fig. 2.3). Notably, since the transmission of the initiation frame and the reception of OOK data occur consecutively, there is no self-interference between the co-located transmitter and receiver. Therefore, unlike backscatter communication systems, the link budget and receiving sensitivity is not affected by direct Tx leakage or near-far problems [104]. For those Wi-Fi

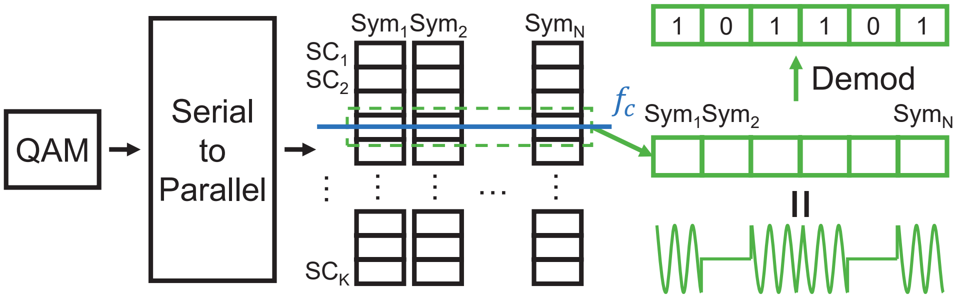


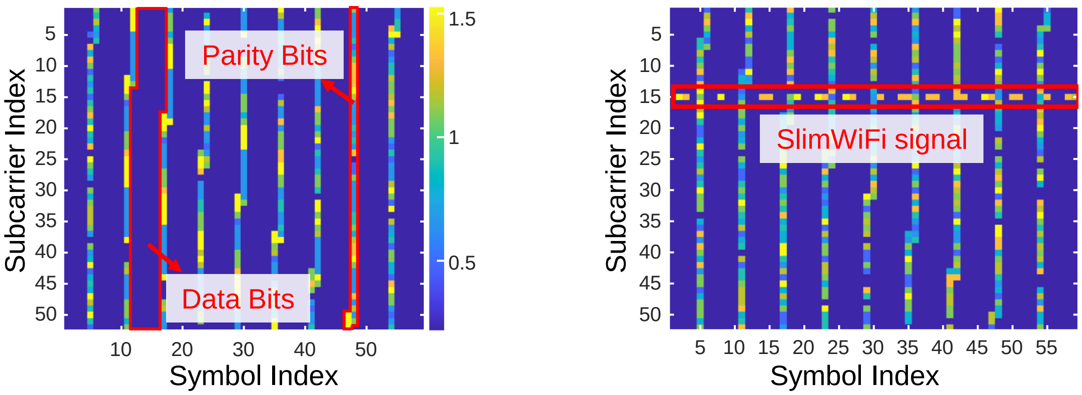
Figure 2.10. Demodulating the SlimWiFi OOK symbols directly in the frequency domain. The subcarrier with non-zero signal power contains the OOK symbols.

devices with integrated transceivers, a firmware update is needed to enable the receiver to start its demodulation workflow immediately after the transmitter sends out the trigger frame.

Optimizing receiver gain and sensitivity. A standard Wi-Fi receiver performs automatic gain control (AGC) based on the signal strength of the preamble from the transmitter. For SlimWiFi, since the preamble is from the co-located initiator instead of the actual transmitter, the AGC may be misconfigured. If the initiation frame is too strong, the receiver will set a low gain, leading to insufficient amplification of the incoming SlimWiFi signals. In this situation, the demodulation performance will be bottlenecked by the quantization error (Sec. 2.3.4). Therefore, to achieve the best receiver sensitivity, we would prefer to reduce the power of the initiation frame. This may risk forcing the receiver to tune to a high gain, resulting in the clipping of high amplitude signals. Fortunately, for OOK signals, the clipping effect will not impact demodulation, since clipped signals are recognized as “1” regardless of their amplitude. We will evaluate the effects of the receiver gain in Sec. 2.6.2.

2.3.6 Putting Everything Together

Overall, the Wi-Fi receiver follows the processing blocks shown in Fig. 2.3 to perform the asymmetric demodulation. At a high level, the incoming OOK samples go through the hard-coded normal Wi-Fi demodulation steps which result in a MAC frame. Our asymmetric demodulator reconstructs the complex samples from the MAC frame, by reversing the Wi-Fi demodulation steps, and then decodes the desired bit sequence from the reconstructed samples.



(a) Without active transmission.

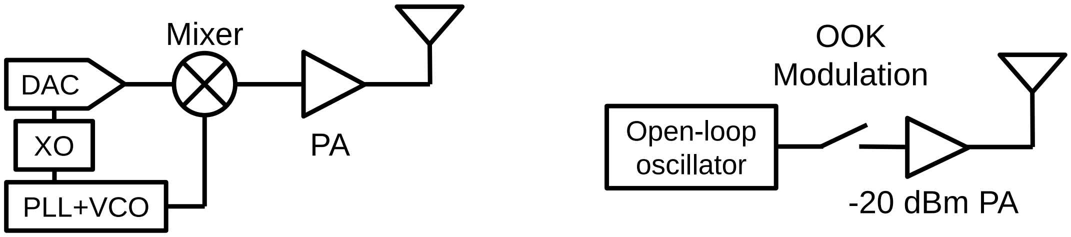
(b) With OOK signal.

Figure 2.11. Waterfall plots of reconstructed time-frequency domain samples.

Note that the reverse processing skips the IFFT. Since the OOK signal is narrowband and only occupies one subcarrier, we can directly process the complex samples on that subcarrier, without IFFT-converting them to the time domain, as shown in Fig. 2.10. The amplitude of the complex sample is used directly to decode the OOK modulated symbol.

To visualize the samples in the time-frequency domain, we collect an example trace with the following configurations: 802.11n with 20 MHz bandwidth, 64-QAM modulation, 5/6 coding rate, LDPC code, and frame length of 2,000 bytes. The waterfall plot in Fig. 2.11a shows the case without any active transmission. The *x* and *y* axis are the symbol index in the time domain, and the subcarrier index in the frequency domain, respectively. The color represents the amplitude of the samples. It can be seen that the samples corresponding to the data bits of the LDPC coded sequence always have a low amplitude (since no coding errors occur there), while the ones corresponding to the parity bits have uncertain results. If we pick the time domain symbols within one subcarrier, the symbols with coding errors (*i.e.* contain parity bits) appear once every 6 symbols. The result corroborates our observations in Sec. 2.3.4.

Fig. 2.11b shows the case when a SlimWiFi device is transmitting signals, causing a high amplitude to appear at subcarrier 15 of the Wi-Fi demodulator. The other subcarriers remain the same as the idle case. The OOK signals can thus be demodulated using the samples on subcarrier 15.



(a) Traditional active transmitter. **(b)** SlimWiFi active transmitter.

Figure 2.12. Transmitter radio hardware architecture.

2.4 SlimWiFi ULP Radio Hardware Design

In this section, we focus on the SlimWiFi transmitter hardware, which is designed for asymmetric demodulation. We also provide a brief discussion on the ULP OOK receiver which explains how SlimWiFi device interacts with the COTS Wi-Fi device on the downlink.

2.4.1 High Power Consumption in Traditional IoT Radios

Modern IoT radio designs need to make challenging trade-offs between power consumption and other competing requirements, including range, bit rate, spectrum efficiency, *etc.* Regardless of how they bias the trade-offs, the IoT radio architecture invariantly comprises 3 key components (Fig. 2.12a): a high power PA to ensure sufficiently high transmit power; a crystal oscillator (XO) reference and carrier generator consisting of a PLL and VCO, to ensure a stable carrier frequency; a high-resolution DAC to support complex modulation schemes. These high-profile hardware components are the main culprit behind the high power consumption [42].

For example, the industry's most power efficient Wi-Fi radio consumes around 300 mW for TX and 100 mW for RX [92]. BLE consumes 5.1 mW at -20 dBm transmit power and 8.1 mW for RX [149]. ZigBee chip consumes 6.9 mW for transmission and 6 mW receiving [148]. LoRa takes 32.4 mW and 14.8 mW for TX and RX, respectively [171]. Even the most advanced low power BLE IC [154] which adopts many aggressive optimizations consumes more than 3.9 mW. Tab. 2.1 shows a breakdown of the power consumption of each component. All in all, to achieve extremely low power and open the pathways for battery-free operations, a

Table 2.1. Power break down of IC implementation

	BLE [154]	SlimWiFi (Simulated)
Power amplifier	2.5 mW	43 µW
Carrier generation	0.7 mW	30 µW
Modulation	0.5 mW	∼0 µW
Rest	0.2 mW	N/A
Sum	3.9 mW	73 µW

fundamentally different architecture is needed that evades all the power hungry components.

2.4.2 SlimWiFi Transmitter Architecture

Owing to the asymmetric communication design (Sec. 2.3), the SlimWiFi device only needs to generate signals with low transmit power, low-accuracy carrier frequency, and simple OOK waveforms. Therefore, we propose the SlimWiFi active transmitter architecture shown in Fig. 2.12b. Compared to the traditional active transmitters, the SlimWiFi transmitter: (i) replaces the high-power PA with a low-power PA optimized for constant-amplitude signals at -20 dBm output power; (ii) replaces the closed-loop PLL+VCO with a simple open-loop oscillator; (iii) removes the DAC and uses an RF switch for OOK modulation. With such optimizations, SlimWiFi can bring the power consumption down to 73 µW in simulation. Tab. 2.1 provides the power breakdown of SlimWiFi in comparison with the aforementioned BLE IC. Now we explain how the extremely low power is achieved.

Transmit power

Existing IoT radio designs aim for long-range, high throughput, and robust communication, which in turn requires a high transmit power. For example, Wi-Fi devices usually transmit at more than 20 dBm (*i.e.*, 100 mW). BLE, ZigBee, or LoRa devices are at around 0 dBm (*i.e.*, 1 mW). The transmit power, and the associated PA hardware, dominates the power consumption of the entire transmitter.

For SlimWiFi, recall it can reduce the transmit power by 18 dB while keeping the same link budget, owing to the narrower bandwidth (250 kHz) (Sec. 2.3). This comes at the cost of a lower bit-rate, but is a much preferred trade-off for most IoT applications, especially considering the existing Wi-Fi infrastructure can be reused. Since the Wi-Fi preamble is generated by the initiator instead of the SlimWiFi device, the PA only needs to support a narrow bandwidth and can be optimized for high efficiency. Our actual on-chip PA is optimized for -20 dBm, whose power consumption can be as low as 43 µW with 24 % drain efficiency. This would be equivalent to a Wi-Fi transmitter at $18 - 20 = -2$ dBm, and comparable to the emission power of BLE, LoRa, and ZigBee radios.

However, reducing the transmit power alone cannot bring the peak power to tens of µW. For example, a BLE IC [149] still consumes 4.5 mW when transmitting at -40 dBm (1 μW), and [154] still consumes 1.4 mW even without a PA (Tab. 2.1). At an extremely low transmit power, the carrier generator and modulation blocks will become the bottleneck.

Open-loop carrier generation

Traditional closed-loop carrier generators are based on PLL, which can generate a highly accurate carrier frequency but consumes high power due to the requirement of phase detection. For example, typical analog PLLs for IoT consume power in the mW level [175, 128]. All digital PLLs can potentially bring down the power consumption to several hundred µW [123, 154, 41], but still around one order of magnitude higher than our target power consumption. The asymmetric demodulation design enables SlimWiFi to drastically relax the requirements of frequency stability. Instead of tolerating around 48 kHz (± 20 ppm) of carrier frequency offset as in COTS Wi-Fi devices [113], SlimWiFi works as long as its carrier falls within the 80 MHz range of the entire 2.4 GHz Wi-Fi band! Therefore, SlimWiFi can use an open-loop oscillator with low frequency accuracy as the carrier generator. More specifically, we chose an open-loop ring oscillator for the 2.4 GHz carrier generation which consumes only around 30 µW when implemented on an IC (more details in Sec. 2.4.3).

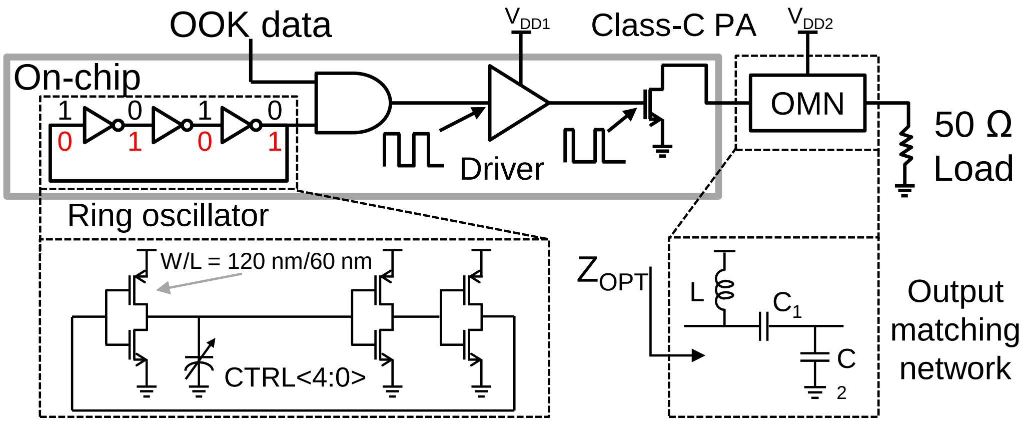


Figure 2.13. Circuit diagram of the SlimWiFi chip.

Low power modulation

To synchronize with the symbol clock of the Wi-Fi receiver (Sec. 2.3.3), the SlimWiFi transmitter uses an RF switch at 250 kHz switching rate to generate the OOK symbols. In fact, our IC implementation realizes OOK by simply powering on and off the PA, without the need of an additional RF switch. Since the open-loop ring oscillator's start-up time (ns level) is much shorter than the symbol period, it can also be power-cycled with the PA, which together can reduce the modulation power consumption to nearly zero.

2.4.3 IC design

Fig. 2.13 shows the circuit diagram of our SlimWiFi IC, consisting of an open-loop ring oscillator and a PA optimized for OOK signal at -20 dBm.

Ring oscillator

The ring oscillator consists of an odd number (3-stage in our design) of inverters cascaded into a ring, as illustrated in Fig. 2.13. The logic input is inverted after passing through the inverters, which causes oscillation between two voltage levels. The open-loop design circumvents the requirement of an external reference clock (*e.g.*, crystal oscillator), thus further reducing the radio cost and form-factor.

The zoom-in plot in Fig. 2.13 shows the detailed on-chip design of the ring oscillator. It is composed of minimum size transistors (W/ L = 120 nm/ 60 nm) for the minimum area and lowest power consumption. The ring oscillator's actual carrier frequency output is affected by the process, voltage and temperature (PVT) variations. We introduce a 5-bit binary weighted capacitor bank (CTRL$\langle 4:0 \rangle$) loading the first stage of the inverter to tune the propagation delay across different stages of the circuit. This in turn allows us to empirically adjust the oscillation frequency at design time, so it falls within the 2.4 GHz band under typical PVT conditions.

Class-C PA

The carrier is directly modulated by a 250 kHz data sequence and then fed to the inverter-based driver to drive a PA. We choose a Class-C PA for its easy implementation in terms of harmonic terminations and better efficiency at low output power [99]. This comes at the cost of low linearity but is acceptable for SlimWiFi since its OOK waveform is insensitive to clipping distortion (Sec 2.3.5). For a Class-C PA, the relationship between the output power P_{out}, optimal load impedance Z_{OPT} and supply voltage V_{DD} follows [99]:

$$P_{out} = V_{DD}^2/(2 \cdot Z_{OPT})$$

For the target of -20 dBm output power, the optimal load impedance can be 18 kΩ, which would be impractical to match to the standard 50 Ω. To alleviate this problem, a dual-supply voltage scheme [87] is applied for efficiency enhancement. Specifically, we use a 0.9 V V_{DD1} to supply the VCO and driver stage, and 0.3 V V_{DD2} to supply the final PA stage. Off-chip high-Q components [198] are utilized in the tapped-capacitor output matching network to achieve the impedance transformation.

Tab. 2.2 compares the simulated IC performance with and without the PCB parasitic S-parameter (SP) model (extracted using ADS Momentum). Both simulation results are obtained with chip post-layout parasitic extraction (LPE). The table shows that, when co-simulated with the PCB SP model, the output power and efficiency are degraded, indicating that the PCB parasites can have a detrimental effect on the IC performance. This problem can be solved by integrating the capacitors on-chip to ensure a good match and carefully modeling the inductor on PCB to co-optimize the performance.

Another potential solution is to replace the 50 Ω termination with a non-50 Ω antenna. For example, a patch antenna can have an input impedance of 100-400 Ω at resonance [43], which can effectively lower the impedance transformation ratio, thus reducing loss in the matching network.

Table 2.2. Simulated IC performance

	LPE	LPE +PCB SP
Frequency (MHz)	2451	2438
Pout (dBm)	-19.9	-21.3
Pdrain (µW)	42.9	43.4
Pvco+driver (µW)	29.2	29.3
Drain efficiency (%)	23.7	16.9
Global efficiency (%)	14.1	10.1

2.4.4 Downlink ULP Receiver

To enable downlink communication for SlimWiFi, the COTS Wi-Fi transmitter needs to emulate OOK waveforms using OFDM. Such emulation has been well explored in recent cross-technology communication and backscatter systems [97, 118, 167, 60], and can be directly adopted by SlimWiFi. The resulting OOK receiver does not need a carrier generator or PA, and thus consumes even less power than the transmitter.

Considering that the TX power of the COTS Wi-Fi device can be 30 dBm, 50 dB higher than the SlimWiFi device's transmit power, a similar uplink and downlink range can be achieved even if the downlink OOK receiver's sensitivity is 50 dB worse than the uplink Wi-Fi receiver. To achieve a 100 m target range, the required receiver sensitivity is 30 dBm + 6 dBi + 2 dBi - 80 dB (FSPL) = -42 dB, which has been achieved in many existing systems. For example, [202] achieves -42.6 dBm sensitivity at 2.8 µW power; [55] achieves -50 dBm sensitivity at 4.5 µW.

Much better sensitivity (smaller than -70 dBm) can be achieved with wake-up radio designs [32, 57, 85, 201, 143, 200, 199] at µW level power consumption.

Other than the 2.4 GHz carrier, the SlimWiFi device also requires a 250 kHz symbol clock. Such low frequency clock can be generated with a ULP oscillator (*e.g.*, 0.3 µW [54]) or extracted from the 2.4 GHz carrier through a ULP fraction counting clock as proposed in [221]. The symbol clock can also be calibrated based on the downlink trigger frame which has a 250 kHz OFDM symbol rate.

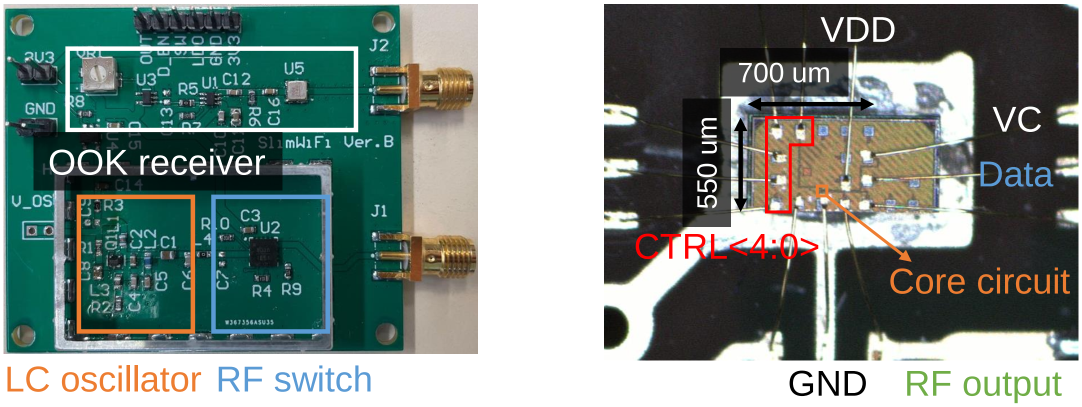
2.5 Implementation

2.5.1 SlimWiFi Device

We have implemented three versions of the SlimWiFi device for different evaluation purposes.

Emulation. To benchmark the performance of the asymmetric demodulation, we need to flexibly control SlimWiFi's signal transmission, such as carrier frequency, symbol time, transmit power, *etc.* Therefore, we use the WARP software radio [138] to emulate the SlimWiFi signals. To faithfully represent the performance of a real SlimWiFi device, we carefully tune the amplitude of the samples and the RF gain of the WARP board, so that the emulated signal has a calibrated transmission power of -20 dBm, consistent with other versions of implementation.

Discrete circuit prototype. The prototype version thoroughly implements both the SlimWiFi TX and RX on a PCB (Fig. 2.14a), and is used for end-to-end functional validation of the SlimWiFi design. Following the hardware architecture in Sec. 2.4.2, the TX device consists of an open-loop LC oscillator BFP720 [91] and an RF switch HMC8038 [35] for OOK modulation. The RLC components of the oscillator are carefully designed to tune the oscillation frequency to the 2.4 GHz ISM band. The OOK RX is implemented by a power detector LT5534 [36] and the sensitivity is tuned to -45 dBm. A Cmod A7 [70] FPGA evaluation board is used to process the trigger frame, synchronize the symbol clock, and generate TX data.



(a) Prototype version.

(b) IC version.

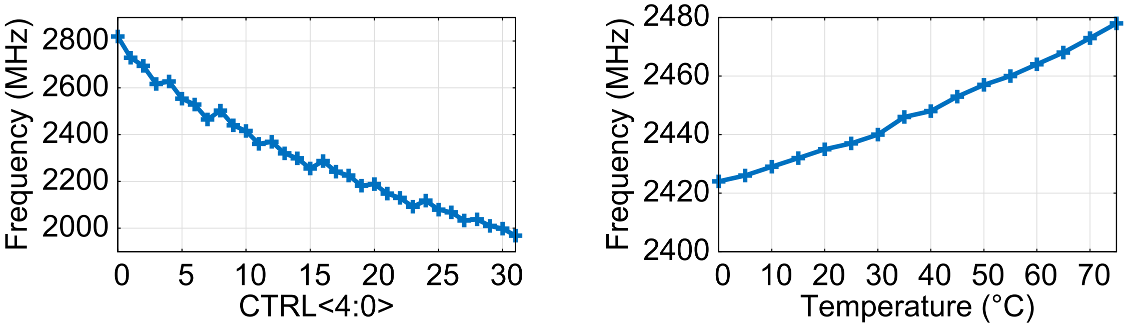
Figure 2.14. Two versions of the SlimWiFi device implementation.

IC fabrication. We also tape out a SlimWiFi transmitter following Sec. 2.4.3 in TSMC 65 nm RF LP process [187] to evaluate its functionality and power consumption. Die photo of the fabricated chip is shown in Fig. 2.14b, whose core size is 30×25 μm^2. The die is directly bonded to a PCB for testing. More advanced process nodes can be utilized to further scale down the chip size and power consumption.

2.5.2 COTS Wi-Fi Device

We use DWA-192 [64], a Wi-Fi dongle that supports LDPC code and A-MSDU, to communicate with the SlimWiFi device. To calibrate the antenna gain, we replace the original antennas of unknown gain with two 8 dBi antennas [33]. To implement the asymmetric demodulation on this Wi-Fi receiver, we capture the data frames with CommView [182] on the user space of the PC host and implement the signal processing workflow in Matlab. No additional software, firmware, or hardware modification is needed for receiving.

For the initiation procedure discussed in 2.3.5, the DWA-192 firmware does not support the generation of a zero-payload initiation frame. As a workaround, we verified that a COTS Nexus 5 smartphone with Nexmon Wi-Fi driver [139, 169] can be used as the initiator to send the CTS-to-self, trigger frame and initiation frame, thus triggering the demodulation procedure on DWA-192. However, the signal strength of the COTS devices cannot be well calibrated and



(a) Frequency v.s. CTRL$\langle 4:0 \rangle$.

(b) Frequency v.s. temperature.

Figure 2.15. SlimWiFi IC carrier frequency drift corresponding to CTRL$\langle 4:0 \rangle$ and temperature.

controlled which hinders us from benchmarking the impact of the power difference between the initiation frame and the SlimWiFi's signal. Therefore, we use the WARP software radio [138] to send the initiation frame for emulation-based evaluation (Sec. 2.6.2).

2.6 System Evaluation

Our evaluation mainly focuses on the SlimWiFi uplink, since the OFDM-to-OOK downlink has been studied in prior research (Sec. 2.4.4).

2.6.1 SlimWiFi Device Microbenchmark

We first benchmark the different implementations of the SlimWiFi device. Tab. 2.3 summarizes some important parameters of the SlimWiFi device.

Carrier frequency. We first profile the frequency stability of the SlimWiFi IC with the open-loop ring oscillator. Fig. 2.15a illustrates the measured carrier frequency when varying the CTRL$\langle 4:0 \rangle$ from 0 to 31 with 0.95 V supply voltage at room temperature (25 $^\circ C$). We see that the ring oscillator design achieves a wide tuning range (around 1 GHz) and fine steps (30 MHz) compared to the 80 MHz frequency tolerance. In addition, as shown in Fig. 2.15b, the frequency variance is within 54 MHz even when considering a very wide temperature range of 0 to 75 $^\circ C$. Therefore, it suffices to perform a one-time calibration to tune the oscillator to the center of the the 2.4 GHz band and let it run freely.

Table 2.3. SlimWiFi prototype and chip performance

	Frequency (Drift)	Power Consumption @ TX Power
Emulation	Tunable	N/A @ -20 dBm
Prototype	2460 (± 5) MHz	1 mW @ -20 dBm
Simulated IC	2438 (± 10) MHz	73 µW @ -21 dBm
Fabricated IC	2465 (± 10) MHz	90 µW @ -24 dBm

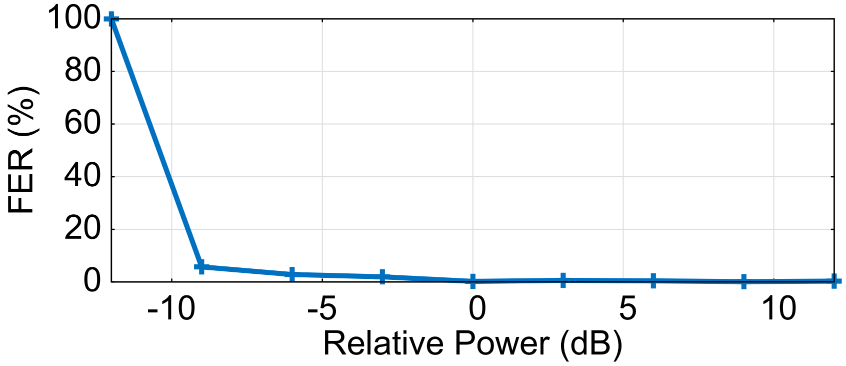


Figure 2.16. Frame error rate with different relative power between the SlimWiFi signal and the initiation signal.

We found that the emulated and prototype version of SlimWiFi show consistent behavior compared with the IC version. The prototype board also has an inaccurate carrier frequency, though a relatively lower drift (around 5 MHz). The WARP setup can emulate arbitrary carrier frequencies for evaluation purposes.

Power consumption and transmit power. The discrete prototype version of the SlimWiFi transmitter consumes around 1 mW power when transmitting at -20 dBm. This is already superior to state-of-the-art IoT ICs (Sec. 2.4). The chip version further cuts the power consumption by an order of magnitude owing to the highly optimized oscillator and PA. Sub-100 µW of power consumption is achieved, for both the simulated and fabricated SlimWiFi chips. The measured output power is -24 dBm, which is 3 dB lower than the simulated results. We suspect this is due to the tolerance of the inductor and capacitors used for the high-Q output matching and/or the PCB parasitics (*e.g.* bond wire inductance) not fully captured by the EM simulation. We expect much lower power consumption and a higher PA efficiency is feasible by

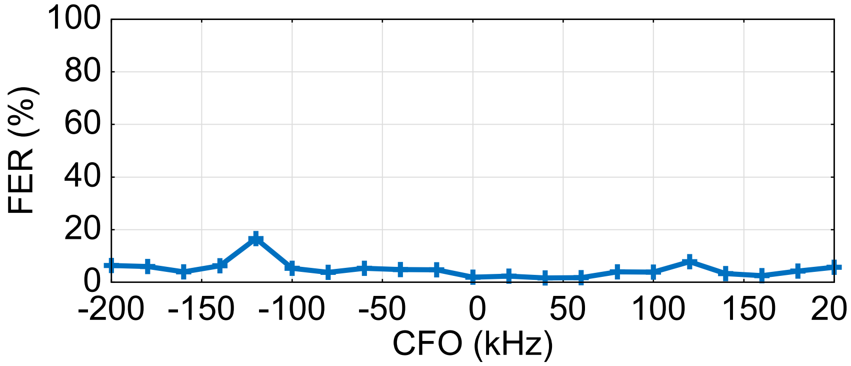


Figure 2.17. Frame error rate under different carrier frequency offset.

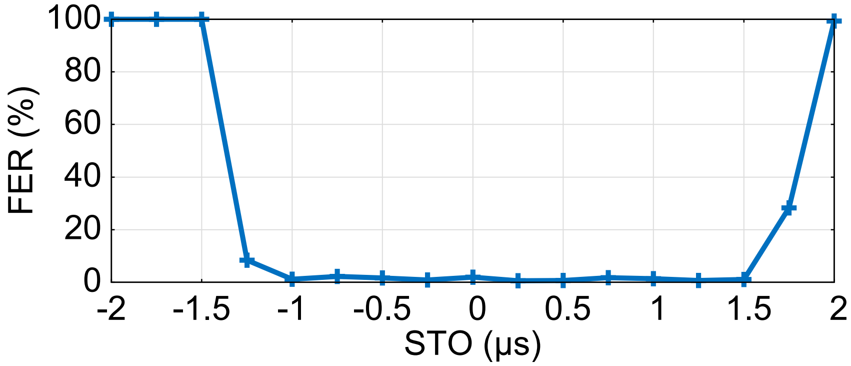


Figure 2.18. Frame error rate under different symbol time offset.

optimizing the PCB peripherals and by using advanced fabrication processes (lower than 65 nm).

2.6.2 Microbenchmark for Asymmetric Demodulation

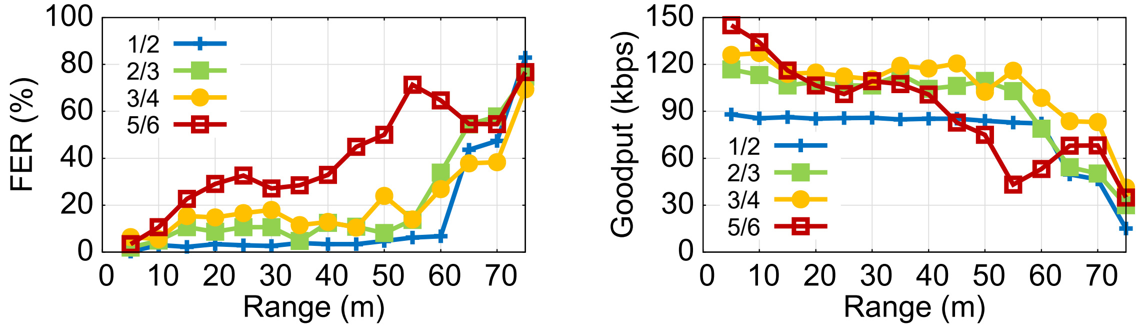
The demodulation performance depends on various parameters, including CFO, symbol time offset (STO), receiver gain, *etc.* Since SlimWiFi uses an open-loop carrier generator that keeps drifting, it is impossible to manually fix these parameters for controlled experiments. We thus calibrated the signal strength and used WARP to decouple and benchmark the impact of each parameter individually.

We conduct link-level experiments in an outdoor parking space, with the following default configurations of the Wi-Fi receiver: 20 MHz 802.11n OFDM, 64-QAM modulation, LDPC coding with 5/6 coding rate and 7935 bytes frame length. Meanwhile, we use WARP to emulate the SlimWiFi device transmitting OOK modulated signals with a frame length of 240 bits and 1/2 BCC coding rate. By default, the link distance is 20 m.

Impact of receiver gain. Recall that the mismatch of signal strength between the initiation signal and the SlimWiFi signal may mislead the Wi-Fi receiver towards a suboptimal gain setting (Sec. 2.3.5). To evaluate its impact, we use the WARP board to transmit the initiation frame along with the emulated signal, so that the strength difference can be intentionally controlled. We consider the relative power of the emulated SlimWiFi signal as 0 dB when the signal strength is the same as that of one subcarrier in the initiation frame. Fig. 2.16 shows that the receiver performance does not degrade significantly until the relative power is lower than -9 dB, when the receiver gain is too low for robust demodulation. This corroborates our explanation in Sec. 2.3.5. Therefore, instead of adjusting the power of the initiation frame which will lead to complicated management overhead, we can just transmit an initiation frame at a fixed low power. By default, our experiments control the relative power to -6 dB to prevent degrading the demodulation performance.

Impact of carrier frequency offset. Note that the 802.11n subcarrier spacing is 312.5 kHz, and asymmetric demodulation works as long as the SlimWiFi signals overlap with one of the subcarriers. We thus only evaluate the case when the SlimWiFi transmitter's carrier frequency deviates from a representative Wi-Fi subcarrier 15. To achieve higher SNR, we combine the samples of the two subcarriers that partially overlap with SlimWiFi's signals, only when the frequency offsets by 140 to 180 kHz (around half of the subcarrier width). Otherwise, the combination may induce more noise (Sec. 2.3.3). With this setting, the worst-case SNR loss is only 3 dB, *i.e.*, when nearly half of the signal power spills into an unusable adjacent subcarrier. To summarize, the asymmetric demodulator can tolerate arbitrary frequency offsets of the SlimWiFi signals in common cases.

Impact of synchronization. To evaluate how the symbol time offset (STO) influences the receiver performance, we manually introduced a delay between the emulated SlimWiFi signal and the initiation frame (both transmitted by the WARP board). The result in Fig. 2.18 shows that within an STO from -1 μs to 1.5 μs, the receiver performance is not affected in a noticeable



(a) Frame error rate.

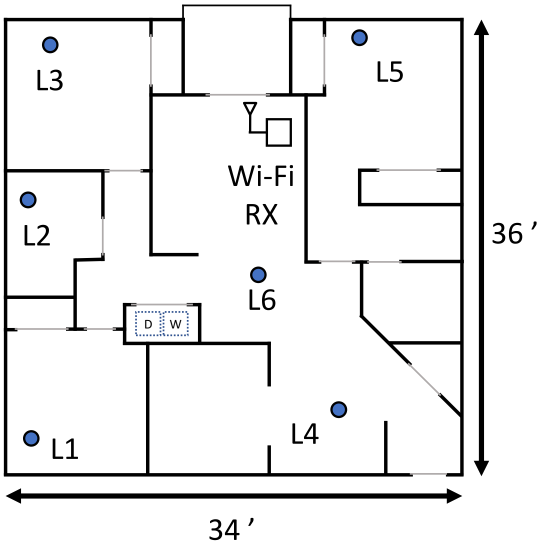
(b) Goodput.

Figure 2.19. Performance of the asymmetric demodulation receiver *w.r.t.* (a) frame error rate (FER) and (b) goodput at different range and coding rate.

manner. Therefore, the system performance should not be affected by the STO since a much better symbol level synchronization can be achieved by the OOK receiver [202, 211]. Notably, the performance is not symmetric around 0 offset (*i.e.*, there is around 0.5 µs more tolerance on positive STO), because of the 0.8 µs redundancy introduced by the CP.

Range and coding rate on SlimWiFi device. Fig. 2.19a and Fig. 2.19b show the frame error rate (FER) and goodput with different link distances and BCC coding rate (applied on the data from SlimWiFi device to combat with the coding error discussed in Sec. 2.3.4). The goodput is calculated by only counting the frames with no bit error and including the overhead of channel access, initiation, and trigger frame as discussed in Sec. 2.2. It can be seen that SlimWiFi maintains a low FER of below 5% even at 60 m of communication range. A goodput of around 100 kbps can be achieved within the range of 60 m. A higher coding rate leads to higher goodput, with some sacrifice on the FER.

Non-line-of-sight (NLoS). We finally evaluate SlimWiFi in an indoor NLoS environment with rich multipath. Fig. 2.20 shows the deployment setup. We place the Wi-Fi receiver in the living room of a 3B2B apartment, and vary the location of the SlimWiFi transmitter (emulated by WARP). It can be seen that a FER lower than 0.5% is achieved for all the locations except “L1”, despite the multipath and under NLoS. A FER of 1.3% can be achieved at “L1” even though the emulated transmitter is placed at the furthest end of the apartment with 2 concrete walls



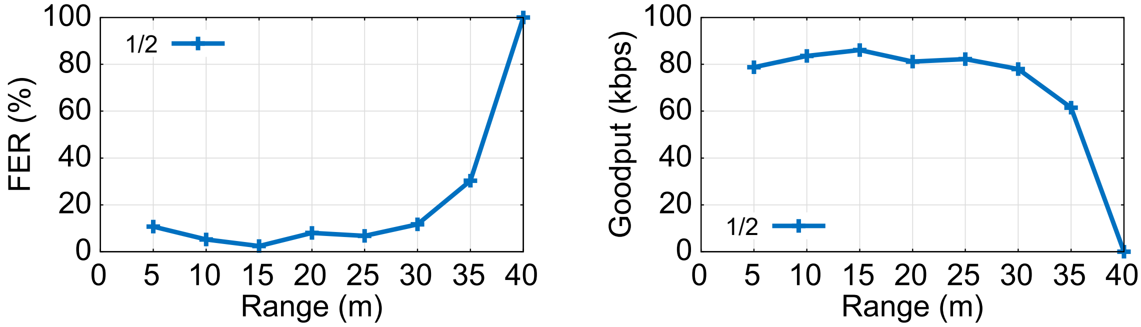
Location	FER
L1	1.382%
L2	0.311%
L3	0.340%
L4	0.218%
L5	0.411%
L6	0.043%

Figure 2.20. Experimental setup and result for NLoS deployment.

blocking the LoS. We note that the non-coherent demodulation of SlimWiFi is insensitive to the signals' phase variations and naturally resilient to the multipath effects. In addition, as discussed in Sec. 2.4.2, although SlimWiFi bears a low transmit power, it still keeps an ample link budget owing to the high sensitivity of asymmetric demodulation, thereby easily achieving whole-home coverage even with NLoS links.

2.6.3 System Level Evaluation

We now put the workflow in Fig. 2.2 together and evaluate the SlimWiFi system end-to-end. We use the prototype SlimWiFi device to transmit an OOK signal with a 1/2 coding rate. The initiator's output power is tuned for the highest receiving gain. The experiments are conducted in an outdoor parking lot. Fig. 2.21 shows that SlimWiFi can achieve a working range of around 30 m at a FER of 11% and goodput of 78.0 Kbps, and 35 m at a FER of 30% and goodput of 61.5 Kbps. Compared to the result in Fig. 2.19, the range is reduced by around 1/2. This is reasonable because the impacts of receiver gain, CFO, synchronization error, *etc.* are combined together. For example, unlike the emulated SlimWiFi device, the carrier frequency of the prototype device or IC is not strictly controlled. The resulting carrier frequency offset is



(a) Frame error rate.

(b) Goodput.

Figure 2.21. Performance of the SlimWiFi system *w.r.t.* (a) frame error rate (FER) and (b) goodput at different range.

unpredictable and will cause up to 3 db of SNR loss (Sec. 2.6.2) which translates into a range reduction. The result also indicates that the proposed symbol synchronization scheme based on a simple OOK receiver can satisfy the synchronization requirement.

2.7 Discussion

Other Wi-Fi standards. We use 802.11n Wi-Fi as the Internet gateway for SlimWiFi devices because the 802.11n standard is supported by mainstream Wi-Fi devices. Other OFDM-based Wi-Fi standards can also support asymmetric modulation, albeit with a few limitations: 802.11a/ac only resides in the 5 GHz band which is not ideal for ULP communication due to the larger path loss; 802.11g, the predecessor of 802.11n, does not support A-MSDU and hence can only accommodate 70 OOK symbols in one frame (Sec. 2.3.5); 802.11ax devices are still not widely deployed and the longer symbol period will lead to lower SlimWiFi throughput.

Initiating the Wi-Fi demodulation. The current SlimWiFi implementation requires an initiator as a workaround to trigger the standard Wi-Fi receiver's demodulation procedure (Sec. 2.3.5). We expect a firmware update to the receiver can enable its self-triggering of the demodulation following the CTS-to-self, as discussed in Sec. 2.3.5. An alternative way to circumvent the initiator is to use the spectral scan function of certain Wi-Fi cards (*e.g.*, the Atheros Wi-Fi [122]), which can continuously report the samples before the QAM block without

Table 2.4. Comparing SlimWiFi with representative state-of-the-art low-power communication

	Radio arch.	Power	Data rate	Interference	Range	Infrastructure
Wi-Fi [92]	Active	100s mW	High	Low	Long	COTS Wi-Fi
BLE [153]	Active	$\sim$ 5 mW	Medium	Low	Medium	COTS BLE
Wi-Fi backscatter [107]	Direct backscatter	1s µW	Low	Low	Short	COTS Wi-Fi
Braidio [84]	Direct backscatter	10s µW	Medium	Low	Short	Custom device
PassiveWiFi [109]	Freqshift backscatter	10s µW	Medium to high	High	Medium	Custom device
HitchHike [211]	Freqshift backscatter	10s µW	Medium	High	Medium	COTS Wi-Fi
SlimWiFi	Slim active	10s µW	Medium	Low	Long	COTS Wi-Fi

explicit triggering. We leave the implementation of these approaches for future work.

2.8 Related Work

Low-power communication hardware. ULP radio hardware design has been the holy grail of the IoT industry. Many RFIC techniques have been proposed for ULP radios, such as harmonic injection-locked carrier generator [156, 83, 120], crystal-free design [157, 52], power oscillator [142], *etc.* However, these radical radio designs are incompatible with existing IoT network infrastructures. In contrast, SlimWiFi demonstrates for the first time that signals from a ULP OOK radio can be demodulated by a COTS Wi-Fi device. The SlimWiFi ULP radio is extremely simple and can be easily mass-produced and embraced into the existing IoT ecosystem.

We note that most modern network standards have protocol-level power-saving mechanisms [29, 113, 69] based on sleep scheduling. These mechanisms cannot reduce the peak power consumption–a more essential metric for battery-free communication hardware. Nevertheless, they are complementary to the SlimWiFi design and can be used to further reduce its average power consumption.

Cross technology communication (CTC). The primary motivation behind CTC is to allow different communication standards to exchange messages, so as to reduce interference and enable sharing of data/control information. Recent work has explored both receiver-transparent CTC [118, 60, 58, 124, 117, 102] and transmitter-transparent CTC [101, 80, 125, 100]. However, CTC mainly sticks to the complex modulation adopted by the COTS IoT devices. In contrast, SlimWiFi aims to design the SlimWiFi signal so that it can be effectively decoded by high-profile OFDM demodulators while relaxing the hardware requirement of the transmitter. In addition, existing CTC systems can not be used in ULP settings due to two reasons. First, none of the existing CTC designs can reduce power consumption because they rely on standard transceivers such as Wi-Fi, BLE, ZigBee, and LoRa. Second, they have relatively low communication performance. For example, the recently proposed XFi [125] can only reach 10 m range at 3% FER. For such CTC systems, the majority of the energy is wasted to maintain an unreliable link between heterogeneous hardware, which is not desired in ULP IoT applications. In contrast, SlimWiFi is optimized to achieve a reasonable communication performance targeting IoT applications, with around 3 orders of magnitude lower power than standard transceivers.

Backscatter communication. Recent work has extended classical UHF RFID backscatter communication to realize ambient backscatter, which piggybacks on existing communication links to convey information. For example, Wi-Fi backscatter *et al.* [107, 44, 126, 84, 168] adopt direct backscatter where the tag data is directly modulated to the excitation signal. But due to the self-interference, they usually operate within a very short range and have a very low data rate. PassiveWiFi *et al.* [109, 214, 181, 192, 221] introduces frequency shifting backscattering to deal with the self-interference issues. A single-tone excitation signal is required as an RF carrier source for a low-power backscatter tag, and the tag can reflect and remodulate standard-compatible signals (Wi-Fi, BLE, LTE, ZigBee, *etc.*). HitchHike *et al.* [97, 211, 202, 74, 213, 59, 117, 127, 217] apply codeword translation, so that a COTS transmitter, instead of a dedicated single-tone generator, can be used as an excitation signal source.

Tab. 2.4 compares SlimWiFi with the representative communication schemes discussed above. Unlike these systems that backscatter signals from existing links, the SlimWiFi device is a *standalone active transmitter* and does not require an external RF carrier signal transmitter. Moreover, as verified in [68], Wi-Fi backscatter systems can cause interference to adjacent Wi-Fi channels, and may inadvertently remodulate and interfere with 5G NR links due to lack of frequency selectivity. Active transmitters like SlimWiFi do not have such out-of-band interference problems. On the other hand, the asymmetric demodulation design in SlimWiFi can also facilitate existing backscatter systems. Owing to the asymmetric demodulation design of SlimWiFi, the backscatter tag can generate a simple modulated signal instead of the sophisticated Wi-Fi compatible signal. Therefore, the tag can evade the need for an accurate and high frequency (tens of MHz) clock source for channel level frequency shifting, which can potentially cut its power consumption by multi-folds.

2.9 Conclusion

To our knowledge, SlimWiFi represents the first active OOK-modulated radio that can directly communicate with existing Wi-Fi infrastructures. Such asymmetric communication capabilities enable radical simplifications to the radio architecture, opening pathways towards standalone, battery-free Wi-Fi compatible IoT communication. Our SlimWiFi IC achieves a peak power consumption of 90 µW, but still leaves ample space for optimization, *e.g.*, through more advanced fabrication processes. The asymmetric communication paradigm can be similarly applied to other wireless standards, which we leave for future exploration.

2.10 Acknowledgements

This chapter contains material from “SlimWiFi: Ultra-Low-Power IoT Radio Architecture Enabled by Asymmetric Communication”, by Renjie Zhao, Kejia Wang, Kai Zheng, Xinyu Zhang, and Leung Vincent, which appears in the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2023. The dissertation author was the primary investigator and author of this paper.

Chapter 3

Long Range Magnetic RFID for Reliable Object Identification

3.1 Introduction

Today's major e-commerce companies need to operate the most sophisticated logistics networks that have ever existed. Companies like Alibaba, Amazon or Walmart need to handle a package volume that is over 87 billion per year [158]. UHF RFID has been widely acclaimed to be the vital enabler that could revolutionize the digital tracking, recording, sorting and verification at the core of logistics operations. However, after numerous trials in real-world deployments, UHF RFID today only finds its use in very specific application scenarios[1]. It is unable to cover wide-ranging media and objects including food, biological, electrical, chemical, mechanical and pharmaceutical products in sophisticated logistics systems that global e-commerce companies operate.

Based on the operating experience of Alibaba–one of the largest e-commerce companies in the world, we demystify the reason why today's UHF RFID system does not work at large scale. The answer is simple: today's UHF RFID is just unable to achieve the 99.9% accuracy[2]

[1] Today's major UHF RFID adopters are apparel retailers [88] such as Zara and Uniqlo whose products are most RF-friendly.

[2] On one hand, the accuracy needed by logistics network has to be extremely high. Since 87 billion packages are shipped every year [158]. With 99% accuracy, the logistics network will mis-deliver 870 million packages, which costs billions of dollars for handling mis-delivered packages. On the other hand, today's bar-code scanning achieves an accuracy of 99.9% and therefore, in order to replace bar-code at large-scale, an RFID solution with higher accuracy is desired.

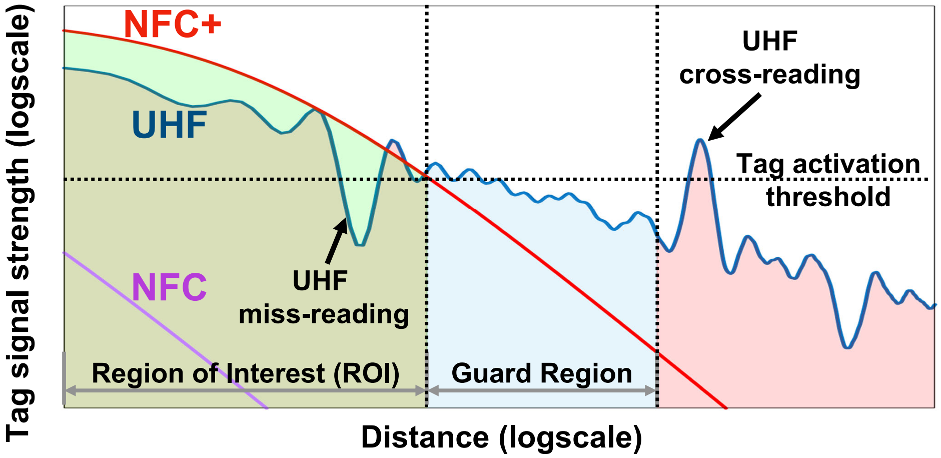


Figure 3.1. The propagation characteristics of the RF signal make UHF RFID unable to avoid miss-reading and cross-reading. In contrast, NFC+ leverages magnetic field to avoid miss-reading and cross-reading. Its operational range is significantly larger than NFC, which makes it suitable for logistics network applications.

needed by complex logistic networks. To have a 99.9% accuracy, an RFID system needs to achieve the following two goals at the same time: *i*) Read ALL (≥99.9%) the tags placed in the region of interests (ROI), and *ii*) Do NOT read any (≤0.1%) undesired tags that are beyond the guard region, shown in Fig. 3.1.

Unfortunately, current RFID systems cannot attain the two goals at the *same* time. To reliably read all the tags in ROI, an RFID system usually needs to add transmission power and improve its sensitivity, thus inevitably cross-reading undesired tags far away. To eliminate cross reading, it usually ends up missing the desired tags nearby. This fundamental dilemma roots in the propagation characteristics of the UHF RF signal as illustrated in Fig. 3.1. As many common objects including water and metal would reflect RF signals, multipath effect thereby induces unpredictable variation over path loss. We want to set a boundary about tag-reader distance (vertical line) as that of the ROI. Unfortunately, the read-or-not criterion essentially translates to a threshold of relative path loss (horizontal line). Thus the outliers along the path loss curve can cause miss- or cross-reading. Workarounds may include an extended guard zone, sometimes too large to be practical. Researchers have explored advanced near-field antennas [141], but such antennas as large as the ROI is bulky and costly. It is possible that the localization-based approach would replace the read-or-not criterion, but the localization algorithm itself is unreliable in practice under the fate of "garbage in, garbage out" [194].

In this paper, we introduce the design and implementation of NFC+, a magnetic RFID system that can address the issue of miss-reading and cross-reading. At a high level, NFC+ is made possible by rethinking how we can construct magnetic fields with multiple highly resonant coils. However, translating this high-level idea into a practical system entails multiple challenges. First, current magnetic RFID systems, such as NFC, can only operate at a short distance (typically $\leq$ 10 cm), which is not sufficient for logistic applications. Second, current magnetic RFID systems can only read a tag when it is placed with a specific orientation. NFC+ introduces the following innovations to overcome the above challenges.

First, NFC+ employs resonating magnetic coils with extremely high-quality factor (Q). We challenge the conventional wisdom that the quality factor Q should stay low (around 10) to prevent the resonance effect from distorting communication symbols [94, 90]. Instead, we choose to escalate the Q factor by orders of magnitude and re-architect the reader with separated TX and RX coils. The TX and RX coils resonate at different carrier frequencies to avoid symbol distortion. With ultra-high Q coils, much more energy can be delivered to the tag and received by the reader under the same transmit power budget, and in the meantime, the reader can also decode much weaker backscattered signals from the tag.

Second, NFC+ leverages a *passive self-interference cancellation* design to curtail the leakage from the TX chain to the RX chain that can severely impact the NFC+ reader's sensitivity and read range. In our TX/RX separating design, because the RX coil's resonant frequency deviates from that of TX coils, the high Q RX coil will cause sharp degradation to the leakage from TX. Then, by using 13.56 MHz crystal, we design a novel ultra-narrow-band notch filter at carrier frequency. By further combining with intermediate frequency filtering, the self-interference is minimized so that we can achieve optimized RX sensitivity and read range.

Third, we propose a novel *multi-coil magnetic beamforming* mechanism, which can fully utilize the diversity gain of multiple coils. By analyzing the vector field property and modeling the NFC+ in a far field way, we prove that the NFC+ reader can "steer" its magnetic field by using multiple coils with binary phase configurations (i.e., 0 and π). This simple scanning mechanism enables the reader to cover the maximum combination.

Finally, we design *passive magnetic repeaters* to further improve the reading range and reliability. These battery-free repeaters can be excited by the magnetic field from the TX coil. Then they regenerate a complementary field to diversify the total vector field's directions and enhance its strength.

We implement NFC+ based on a custom-built reader platform, which can directly read *standard NFC tags*. To verify its performance, we conduct microbenchmark experiments along with large-scale warehouse tests involving over 10,000 tags. The results show that:

- NFC+ can reach a maximum reading range of 3 m, whereas state-of-the-art NFC systems can only achieve 0.9 m even with the most favorable tag orientation.
- NFC+ achieves a low miss-reading rate of 0.03% when the tags are attached to various products with arbitrary orientation, in contrast to 40% and 23% of NFC and UHF RFID, respectively.
- NFC+ does not cross read any tag outside of the ROI, in comparison to a cross-reading rate of 42% in UHF RFID.

To our knowledge, NFC+ represents the first system to solve the cross-reading and miss-reading problem that has plagued RFID for decades in realistic deployment. We believe that NFC+ paves the way towards deploying RFID at scale in logistics networks. We also hope this work can bring magnetic communication back into researchers' sight because the physical property of magnetic field is extremely superior in many large-scale applications.

3.2 Motivation and background

3.2.1 Rethink RFID system design

The miss-reading and cross-reading problems are direct consequences of the intrinsic physical nature of UHF radio waves. In order to overcome this challenge, we argue that we should rethink the design of today's logistic RFID systems at a fundamental level. Specifically, instead of relying on electromagnetic radio waves, we propose NFC+ to harnesses magnetic signals and re-architect RFIDs in logistic networks. NFC+ embraces the magnetic nature of near field communication (NFC) and transforms these short-range battery-free NFC tags into long-range and reliable RFIDs. NFC+ exploits NFC for the following immediate advantages:

- NFC relies on 13.56MHz magnetic signal for communication, which can easily penetrate all kinds of media that would block or reflect RF signals including liquid and even metallic objects[3].

- Magnetic signal is non-radiative, and its "energy" degrades at $O(1/d^6)$ with distance d, much faster than $O(1/d^2)$ for UHF electromagnetic signal. In addition, a magnetic signal rarely experiences multipath reflection, which prevents cross-reading undesired tags beyond the operating range.

- NFC tags are battery-free and extremely low-cost. Similar to UHF RFID, NFC relies on energy harvesting and does not require a battery for operation. In addition, NFC tags have already been produced on a massive scale. The cost of an NFC tag has been made as low as 5 cents [152], comparable to UHF RFID tags[4].

- NFC is well supported by multiplexed protocols such as ISO 15693 and ISO 14443, which allow multiple tags to be read simultaneously. The read rate is more than 50 tags/s which is sufficient for logistic applications.

[3] Thin and non-ferromagnetic, *e.g.* aluminum foil.

[4] Note that due to application difference, today's NFC chips have more memory volume than UHF RFID. We expect the cost of the NFC tag to further shrink down if NFC tags are applied to logistics.

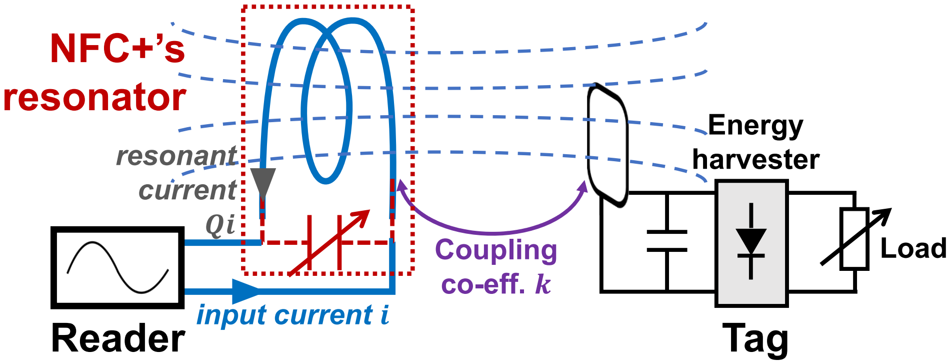


Figure 3.2. NFC reader-tag setup and close-loop magnetic coupling when tag is close to the reader. NFC+ leverages an additional high-Q resonator (simplified as the paralleled shunt capacitor and the coil inductor) which builds on top of NFC to boost the reading range.

3.2.2 Physics behind NFC and its limitations

Unfortunately, today's NFC systems are fundamentally crippled by its communication range. Current NFC systems are designed following the principles of inductive magnetic coupling [172]. As shown in Fig. 3.2, an NFC reader usually employs a loop antenna to elicit magnetic fields while NFC tags also employ small coils to pick up the produced magnetic fields. When the reader's fields traverse a tag's coil. The NFC reader and the tag are inductively coupled with each other via a magnetic field, so the antennas between the reader and the tag effectively form a transformer with a specific coupling coefficient k which is a function of the tag's location and orientation. The reader delivers power and commands to the tag through the transformer and detects the load changing when the tag is doing load modulation. However, in such an inductively coupled system, when a tag is placed slightly away from the reader or has a small degree of undesired orientation, the coupling coefficient k quickly diminishes. This will lead to loose coupling between the reader and the tag, which impedes the tag's energy harvesting and data communication. Therefore, NFC systems that are built based on inductive coupling typically only operate with a range of less than 10 centimeters [186].

3.2.3 Resonance effect and quality factor

To fundamentally overcome the limited communication range in the current NFC system, NFC+ builds on top of a physical phenomenon called *Resonance*, which is the amplification that occurs when a signal is applied at the natural frequency of a system. In order to leverage the resonance effect, a resonator is required as shown in the red block of Fig. 3.2. Because the size of the loop antenna is relatively small compared to the NFC carrier wavelength (22 m), the input current is evenly distributed on the loop [160]. Hence, the loop antenna itself can be regarded as a discrete inductor and resistor. To form a resonator, an additional capacitor is added across the loop antenna. The energy in a resonator is stored in two different ways: (1) the electrical energy as charges accumulate at the capacitor electrodes and (2) magnetic energy as currents flow through the inductor. There is a tendency of such two types of energy converting into one another, causing oscillation between the capacitor and the inductor. The natural frequency of such oscillation is decided by:

$$f_0 = \frac{1}{2\pi\sqrt{LC}} \tag{3.1}$$

By changing the value of the capacitor, we can tune the resonant frequency to 13.56 MHz in NFC. The strength of such oscillation is measured by an important physical parameter called quality factor (Q) [115], which is defined as the ratio of the peak energy stored in the resonator to the energy lost per radian in a cycle of oscillation. In an RLC parallel circuitry, Q can be calculated as:

$$Q = \frac{R}{2\pi f_0 L} \tag{3.2}$$

When an input current is fed into a resonator, the resonant current passing through its coil will be Q× of the input current, which means that magnetic field strength is amplified by Q× compared to a resistive load even though the input power stays the same. However, it is worth noting that there is also a trade-off between the frequency, bandwidth, and Q, which can be written as:

$$BW = \frac{f_0}{Q} \tag{3.3}$$

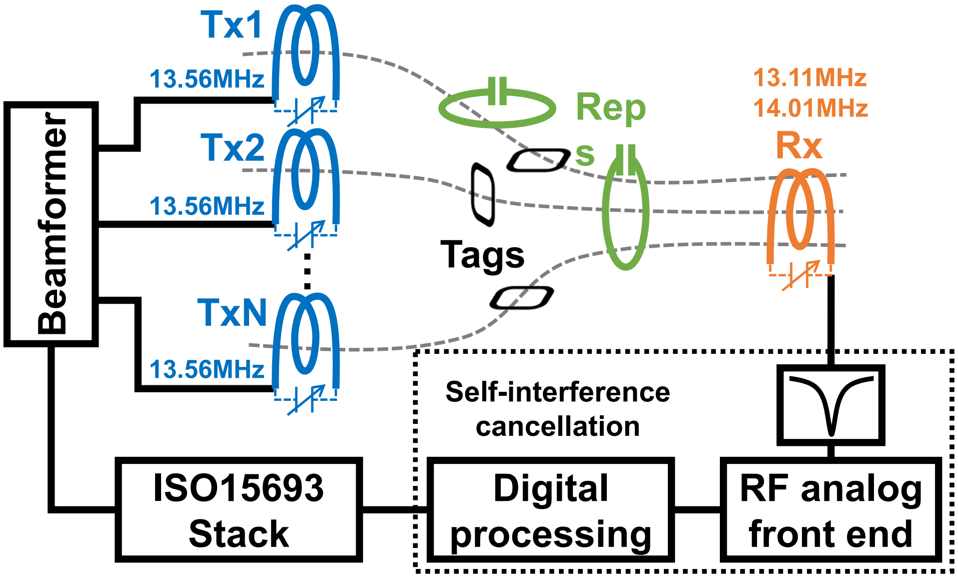
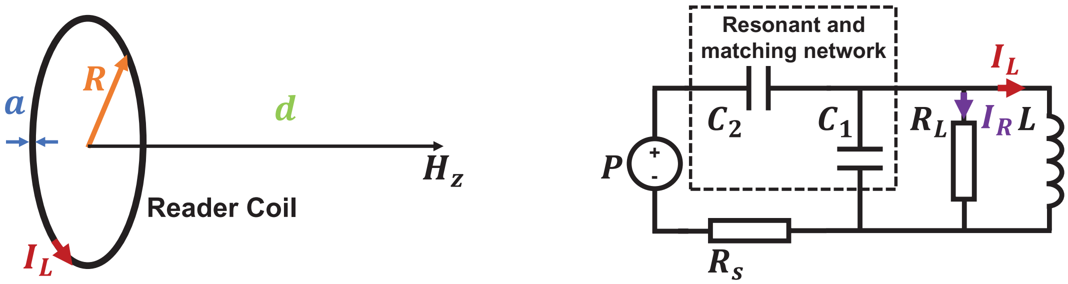


Figure 3.3. NFC+'s system overview

The above equation tells that the communication bandwidth is inversely proportional to the quality factor of the resonator. As a result, in communication, high Q is rarely employed due to the bandwidth constraint it imposes on sending and receiving data.

3.3 NFC+ system overview

Fig. 3.3 summarizes the key components in NFC+. To extend the range where a tag can operate, we physically separate transmission and reception coils and leverage high quality factor coils for both transmission and reception. However, TX coils are tuned to resonate around 13.56 MHz while the RX coil will resonate around 13.11 MHz or 14.01 MHz. In addition, we design passive self-interference cancellation circuit to enable the reader to receive and decode very weak backscattered signal when a tag is far away from the reader. Then, we leverage multiple TX coils to realize efficient magnetic beamforming to ensure tags with undesired orientations can also obtain sufficient power for its operation. Finally, we design passive (batteryless) repeater which is deployed at locations close to the tag and helps read tags far away from the TX coil or with undesired orientations. We will introduce the design of each component in the following sections.



(a) Reader current loop model.

(b) The equivalent circuit model.

Figure 3.4. The physical model and the equivalent circuit model of a reader coil.

3.4 Pushing range limits

In this section, we will describe how NFC+ leverages high Q coil, TX/RX separated transceiver design and self-interference cancellation techniques to significantly boost the operational range.

3.4.1 Why we need high quality factor coils?

We start by modeling the magnetic field generated from a reader coil. The goal is to identify the fundamental design knobs that determine the field strength. Without loss of generality, we model the coil as a circular loop carrying current I_L, as shown in Fig. 3.4a. The equations corresponding to different coil shapes are slightly different, but our conclusion still holds regardless. Since the coil size is much smaller than the signal wavelength, the current I_L can be considered as evenly distributed, and hence we can use a static magnetic model to analyze the system [43]. Following the Biot-Savart law [146], the field along the coil's central axis is:

$$H_z = \frac{R^2 I_L}{2(d^2 + R^2)^{\frac{3}{2}}} \tag{3.4}$$

where d is the distance between reader coil and tag and R is the radius of the coil.

Because the reader coil is a “small loop” compared to the 22 m wavelength, the reader coil can be treated as an inductor L shunted with a resister R_L. Then, taking a simple resonant and matching network which is used to form a resonator and match the coil impedance to the voltage source internal resistance R_s, the reader can be simplified as the circuit in Fig. 3.4b, the current I_L is related to the reader's output power P and the quality factor Q of the coil. The reader coil's inductance can be calculated as [185]:

$$L \propto R\left[\ln\left(\frac{8R}{a}\right)-2\right] \tag{3.5}$$

where a is the wire radius. The resistance R_L is made tunable to achieve different Q values with the same L. Given a specific Q, $R_L = \omega_c LQ$. If the matching is perfect, R_L is loaded with half of the available power from the signal source, which is P and the current through R_L is $I_R = \sqrt{\frac{P}{R_L}} = \sqrt{\frac{P}{\omega_c LQ}}$. Therefore, we have:

$$I_L = QI_R = \sqrt{\frac{PQ}{\omega_c L}} \tag{3.6}$$

Then, the magnetic field generated by a reader passing through the tag can be modeled as:

$$H \propto \sqrt{\frac{PQ}{R\left[\ln\left(\frac{8R}{a}\right)-2\right]}}\frac{R^2}{(d^2+R^2)^{\frac{3}{2}}} \tag{3.7}$$

The field strength H depends on the following factors: reader transmission power P, reader coil radius R, coil quality factor Q, coil wire radius a and distance d. *Obviously, to achieve longer distance d, we may increase P, R, a or Q.*

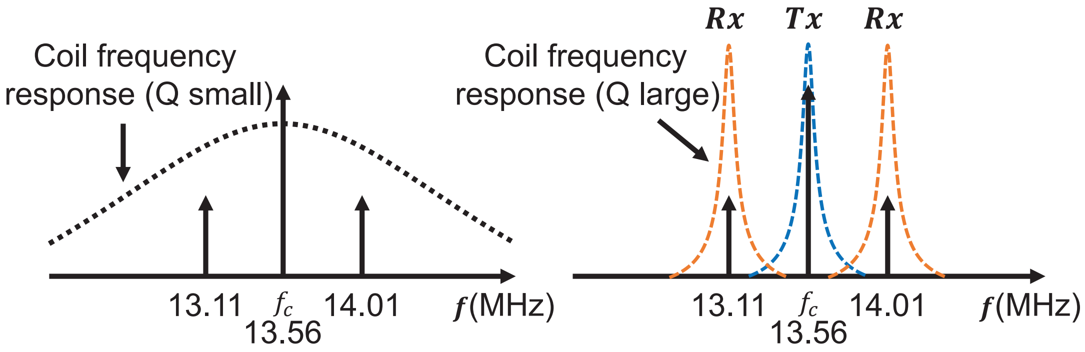
However, simply increasing the transmission power P will cause severe safety problems. The most powerful state-of-the-art commercial NFC reader [130] has 8 Watts output power and offers a maximum read distance up to 0.9 m. To extend the reading distance to 3 m, the reader's output power needs to reach an alarming level of $8 \times (\frac{3}{0.9})^6 = 11$ kW, which is hardly achievable by practical power source and dangerous for human operators [77]. The reason roots in the fact that P is proportional to d^6 as shown in Eq. 3.7. Similar to P, increasing the wire radius a is not a viable solution, either. To reach 3 m distance, wire radius needs to be increased by $e^{(\frac{3}{0.9})^6} = e^{1372}$

times, which is infeasible in practice.

Another idea is to play with the geometry R. An optimal R can be calculated by setting the derivative of Eq. 3.7 to zero, which leads to an R comparable to d. Unfortunately, abusing R is also infeasible for two reasons: (1) A large coil has a high self-inductance, which can only function under small resonating capacitance when the coil is tuned to 13.56 MHz as shown in Eq. 3.1. The small capacitance can be easily affected by parasitic capacitance which is induced from nearby environment. As a result, the coil would get detuned from the desired 13.56 MHz frequency even though it has been carefully calibrated. (2) To efficiently elicit magnetic fields from the source, the loop currents shall be evenly distributed along the coil to avoid spurious electromagnetic emission at far-field [73], which implies that the maximum circumference of the coil can only be a small fraction of the wavelength λ ($< 0.1\lambda$ as a rule of thumb [73]). As a result, in practice, R has to be limited to around 0.5 m.

The above analysis implies that the quality factor Q of a coil remains as the major factor that can be practically leveraged to extend the range. A Q value on the order of several hundred is feasible since the internal resistor of a coil can be made very small. This kind of high Q loop antenna has been well studied in amateur radio [73]. Unfortunately, a commercial NFC reader coil typically employs a very small Q factor of around 8 by adding an additional resistor [94]. Such a design was made to ensure that the same coil can be used simultaneously for wireless power transfer and reader-tag bidirectional data communication.

Fig. 3.5 shows how the quality factor of a coil impacts data communication. In the ISO 15693 NFC protocol, a tag talks to a reader through sideband modulation with a sub-carrier of 423.75 kHz or 484.25 kHz. To decode the tag's signal with 13.56 MHz carrier received by the same transmitting coil, the sampling bandwidth needed is around 484.25 kHz $\times 2 \approx 1$ MHz. Since bandwidth BW of a coil is inversely proportional to its quality factor $Q = f_c/BW$, the Q of the coil should be no more than 13.56 MHz$/1$ MHz $= 13.56$. A typical practice is to employ a $Q = 8$ so that it can also support ISO-14443 which has larger sub-carrier frequency. Using such a small Q, the frequency response of the coil is not sharp and its bandwidth is wide as shown in



(a) Coil frequency response when Q is small. **(b)** Coil frequency response when Q is large.

Figure 3.5. Frequency response of coils with different quality factors. To use high Q coils, we use different coils for transmission and reception. The TX coils are tuned to 13.56 MHz and the RX coils are tuned to 13.11 MHz or 14.01 MHz.

Fig. 3.5a. Therefore, tag-to-reader data communication can sustain.

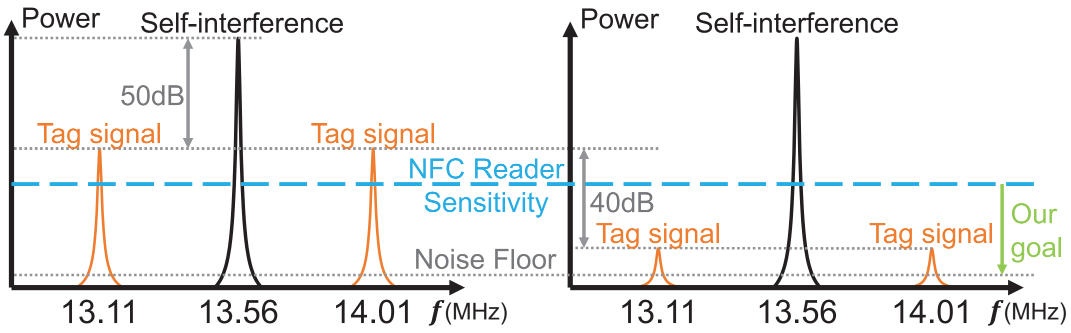
Although Eq. 3.7 tells us that a large Q improves the magnetic strength, the frequency response of the coil becomes sharp as shown by the blue dotted curve in Fig. 3.5b. As a result, the tag-to-reader communication suffers because the frequency of the backscattered signal sits outside of the bandwidth of the coil. How to increase the Q factor without compromising the communication link?

3.4.2 Support high Q coils via T/R separation

Instead of using a single coil for both transmission and reception, NFC+ achieves high-quality factors by using at least two coils, one for transmission and one for reception. We do so because we want to unleash the power of Q by decoupling transmission and reception.

Let us first look at the quality factor of the TX coil. The reader-to-tag downlink transmission adopts pulse position modulation with an $T_b = 9.44\ \mu s$ pulse width (ISO 15693 protocol), which suggests that the bandwidth required for reader-to-tag link is around $1/T_b = 106$ kHz [160]. Since the center frequency of the TX coil is around 13.56 MHz, the Q of the TX coil can be increased to 13.56 MHz$/$106 kHz $=$ 128, 16× larger than that of a typical commercial NFC reader.

Unlike commercial NFC systems where RX operates around 13.56 MHz, as shown in



(a) Received signal strength when tag is 10cm away.

(b) Received signal strength when tag is 1m away.

Figure 3.6. Self-interference experienced by a reader when a tag is placed at different distances from the reader.

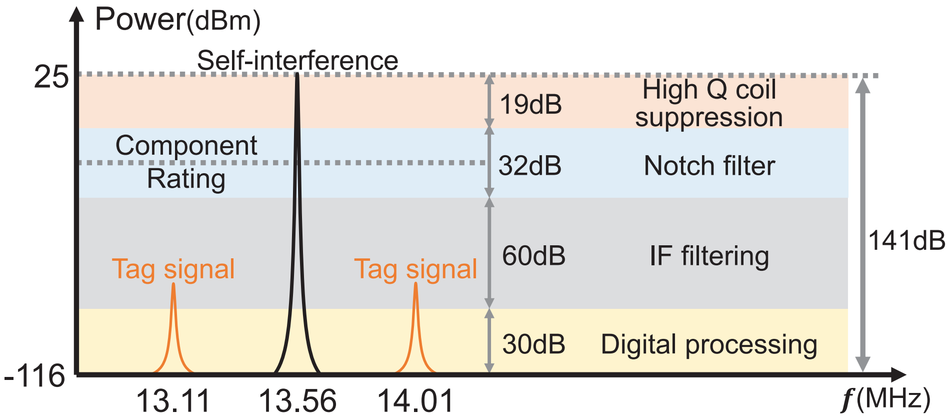


Figure 3.7. NFC+ uses high Q coils, notch filters, IF filters and digital baseband processing for self-interference cancellation.

Fig. 3.5b, we tune the RX coil to operate around 13.11 MHz or 14.01 MHz, corresponding to the lower/upper sideband frequencies used in the tag-to-reader communication link. The tag performs FSK modulation at 6.7 kbps with a 423 kHz or 484 kHz subcarrier. The minimum sampling bandwidth required by the reader to decode the information is $(484-423)+2\times6.7=74.4$ kHz. As a result, the RX coil can have a $Q = 14.01$ MHz$/74.4$ kHz $= 188$. Overall, using a $Q = 128$ TX coil and a $Q = 188$ RX coil can extend the reader-to-tag link range by 1.6× and tag-to-reader link range by 1.7× compared to the $Q = 8$ coils used by state-of-the-art commercial NFC readers.

3.4.3 Passive self-interference cancellation

To further increase the link budget and boost the range, we need to handle self-interference to improve the RX sensitivity. This RX side improvement is needed because the strength of reader received signal will suffer two times of "path loss" and easily become bottleneck when distance increase. Self-interference, which is the leakage from the TX to the RX chain, is one of the main factor that limits the RX sensitivity. In this section, we will discuss why this issue is not solved in commercial NFC systems and how we can use simple passive circuits to address the problem.

Commercial NFC readers do not have self-interference cancellation circuits mainly because it is unnecessary to have a sensitive receiver for short-range ($\leq$10 cm) applications [186]. To understand the impact of self-interference, we use the Tagformance Pro platform from Voyantic [190] to measure the tag signal strength as well as the strength of self-interference by feeding the RX path into a spectrum analyzer. The results are illustrated in Fig. 3.6. When a tag is 10 cm away from the reader, the backscattered signal is only about 50 dB lower than the self-interference from the reader and is well above the noise floor. Therefore, the majority of commercial readers with amplitude and phase detectors [95] performing non-coherent demodulation [166] can still successfully decode the tag signal even without self-interference cancellation.

However, when the tag moves away from the reader, the backscattered signal becomes very weak while self-interference remains the same. Following the model in Eq. 3.7, when the tag-to-reader distance moves from 10 cm to 1 m, the strength of the tag's backscattered signal will decrease by 40 dB [5]. As illustrated in Fig. 3.6, the backscattered signal will be much lower than the self-interference. In such a condition, self-interference cancellation becomes important to design a near-to-noise-floor sensitivity receiver.

NFC+ introduces a simple but novel passive circuit to address this issue. Our passive

[5] The maximum read range of Tagformance Pro is 30 cm. Therefore, we calculate signal strength at 1m based on measured results at 10 cm.

circuit includes *three parts*: high Q coil suppression, notch filter and IF filter. We first explain how we use high Q coils to suppress the self-interference. As discussed in Sec. 3.4.2, we tune the TX coil and RX coil to operate around 13.56 MHz and 14.01 MHz (or 13.11 MHz), respectively. Because of the bandwidth and Q trade-off in Eq. 3.3, the high Q RX coil will suppress the signal outside 14.01 MHz (or 13.11 MHz) band. As a result, the 13.56 MHz self-interference from the TX coil will be suppressed by the high-Q RX coil. To illustrate such a high-Q suppression effect, we used two high Q coils separated by 2 m and measure the self interference when the RX coil is tuned to 13.56 MHz and 14.01 MHz, respectively. The results are shown in Fig. 3.7. We can see that the combination of high Q TX and RX coils can suppress the strong self interference by 19 dB. Note that such a 19 dB suppression is extremely important since it deals with high-power jamming signals which may damage the following components.

Even though the self-interference is reduced by 19 dB, the remaining self-interference is still very large compared to a tag's backscattered signal and also higher than the component rating power which may destroy the front-end components in a receiver. One may consider using the active cancellation techniquein UHF RFID and full-duplex communication systems to further suppress the self-interference [45]. Active cancellation can be achieved by controlling the phase and amplitude of a copy of signal from the TX chain, so as to produce a signal which is exactly the opposite of the interference signal. However, during the procedure of searching such an opposite phase and amplitude, the coupled signal might get constructively combined with the self-interference and cause damage to the component.

To overcome the barrier, our key insight is that the frequency of the excitation signal is relatively low (13.56 MHz). Therefore, we design a crystal notch filter that has 15 dB sharp rejection around 13.56 MHz and very low loss (less than 1 dB) near 13.10 MHz or 14.01 MHz. In addition, we cascade several notch filters to achieve near 32 dB interference rejection. Combining high Q coils and cascaded notch filters, the self-interference is suppressed by 50 dB.

In addition to passive circuits described, NFC+ leverages IF filtering and digital baseband processing, such as digital filtering, to further suppress the self-interference. The overall 141dB

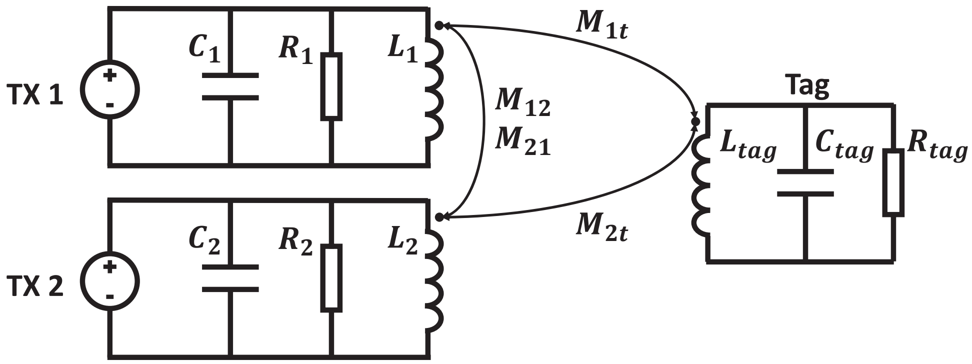


Figure 3.8. Circuit model of two TX coils setup.

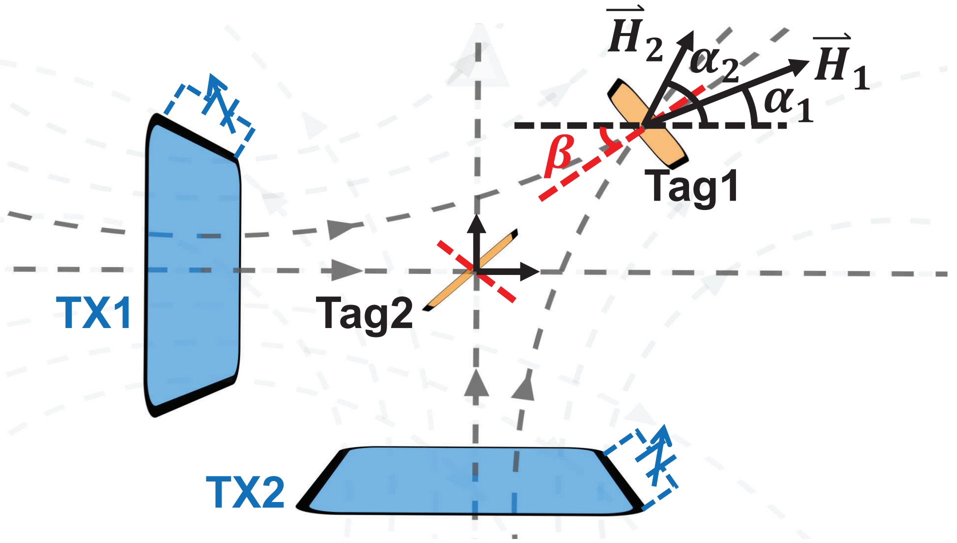


Figure 3.9. Two perpendicular TX coils setup and the vectors on the coordinate system.

self-interference suppression can reduce the self-interference near to the -120 dBm thermal noise floor, which makes the reader sensitive enough for decoding a weak backscattered signal even when the tag is far from the reader.

3.5 Inventory misoriented tags

Another limitation of existing NFC systems is that a reader can only read tags with specific orientations. In this section, we introduce how NFC+ leverages multi-coil diversity to meet the challenge. We note that existing NFC systems are designed to work in short range only and a single coil suffices. Therefore, a multi-coil system entails non-trivial design choices to maximize diversity gain and avoid destructive interference.

3.5.1 Model of multi-coil system

NFC+ borrows the high-level idea of antenna diversity from far-field radar systems, which sweep through beam patterns to broaden the angular coverage. But in doing so, we must first deal with the mutual inductance intrinsic to near-field communication systems. As shown in Fig. 3.8, the mutual inductance exists between (1) the reader and the tag, e.g. M_{1t}, M_{2t} and (2) the reader's multiple coils, e.g. M_{12}, M_{21}. From a circuit perspective, mutual inductance creates additional load to a signal source which in turn affects the current amplitude and phase distributed on the reader coil. In Appendix B, we show the mutual inductance between the reader coils can be accounted for without compromising the simplicity of our model, so that we could treat the TX coils as uncoupled "current loops". On the other hand, the tag-to-reader mutual inductance is much smaller compared to that of the reader coils. Therefore, the loading effect caused by the tag to the reader can be ignored.

Another issue is that unlike the electromagnetic wave in the far-field, the magnetic field is a vector instead of scalar. Therefore, in what follows, we explicitly model and discuss the behaviour of magnetic field signal. As illustrated in Fig. 3.9, The currents on TX1 and TX2 produce magnetic field $\vec{H}_1$ and $\vec{H}_2$ at Tag1's location $\mathscr{R}$. α_1 and α_2 denote the corresponding vector directions of $\vec{H}_1$ and $\vec{H}_2$. Then the two vectors at n^{th} time slot can be expressed as:

$$
\begin{aligned}
\vec{H}_1(n,\mathscr{R}) =& [a_1(n,\mathscr{R}) sin(\omega t + \phi_1(n)) cos(\alpha_1(\mathscr{R})),\\
& a_1(n,\mathscr{R}) sin(\omega t + \phi_1(n)) sin(\alpha_1(\mathscr{R}))]\\
\vec{H}_2(n,\mathscr{R}) =& [a_2(n,\mathscr{R}) sin(\omega t + \phi_2(n)) cos(\alpha_2(\mathscr{R})),\\
& a_2(n,\mathscr{R}) sin(\omega t + \phi_2(n)) sin(\alpha_2(\mathscr{R}))]
\end{aligned}
\tag{3.8}
$$

where $a_i(n,\mathscr{R})$ and $\phi_i(n)$ denote the magnitude and phase, respectively. The magnitude depends on the location $\mathscr{R}$ and the excitation current whose magnitude is $A_i(n)$. The amplitude can be further expressed as the multiplication of a location-dependent factor and a time-varying factor, i.e., $a_i(n,\mathscr{R}) = k_i(\mathscr{R}) A_i(n)$. The phase is determined by the excitation current phase $\theta_i(n)$ on the

TX coils. In the near field regions, *the phase change introduced by propagation can be ignored [43] which implies $\phi_i(n) = \theta_i(n)$*. Then the combined magnetic field $\vec{H}_s(n)$ can be written as:

$$\begin{aligned}\vec{H}_s(n,\mathscr{R}) =&[k_1(\mathscr{R})A_1(n)sin(\omega t+\theta_1(n))cos(\alpha_1(\mathscr{R}))\\ &+k_2(\mathscr{R})A_2(n)sin(\omega t+\theta_2(n))cos(\alpha_2(\mathscr{R})),\\ &k_1(\mathscr{R})A_1(n)sin(\omega t+\theta_1(n))sin(\alpha_1(\mathscr{R}))\\ &+k_2(\mathscr{R})A_2(n)sin(\omega t+\theta_2(n))sin(\alpha_2(\mathscr{R}))]\end{aligned} \tag{3.9}$$

Let β denote the angle of the normal of the tag plane, i.e. the orientation of the tag. We show in the Appendix C that from Eq. 3.9 and by using $\theta_1(n)$ as the phase reference, the power of the combined signal received by the tag can be written as:

$$\begin{aligned}P_{H,2}(n,\mathscr{R},\beta) =&\big(b_1(n,\mathscr{R},\beta)+b_2(n,\mathscr{R},\beta)cos(\theta_2(n)-\theta_1(n))\big)^2+\\ &\big(b_2(n,\mathscr{R},\beta)sin(\theta_2(n)-\theta_1(n))\big)^2\end{aligned} \tag{3.10}$$

where $b_i(n,\mathscr{R},\beta) = S_ik_i(\mathscr{R})A_i(n)cos(\alpha_i(\mathscr{R})-\beta)$, S_i is a factor corresponding to the property of the tag coil, such as the coil size, number of turns etc. When extending to N TX coils, the power of the tag received signal will be:

$$\begin{aligned}P_{H,N}(n,\mathscr{R},\beta) =&\big(b_1(n,\mathscr{R},\beta)+\sum_{i=2}^{N}b_i(n,\mathscr{R},\beta)cos(\theta_i(n)-\theta_1(n))\big)^2+\\ &\big(\sum_{i=2}^{N}b_i(n,\mathscr{R},\beta)sin(\theta_i(n)-\theta_1(n))\big)^2\end{aligned} \tag{3.11}$$

From the equation above, it can be seen that the final signal strength associated with a specific location and orientation is determined by the amplitudes $A_i(n)$ and the phases $\theta_i(n)$ of TX coils. As a result, we could borrow the codebook concept from far-field RF beamforming [220]. In particular, we design a two-dimension codebook the n^{th} entry of which represents a $(A_i(n), \theta_i(n))$ combination. Then, by iterating over the different entries, we are able to cover the whole spatial region. In the following section, we introduces the detailed codebook design.

3.5.2 Magnetic beamforming

In its simplest form, the codebook is designed as follows: the amplitude $A_i(n)$ should take the maximum available value and remain the same across the codebook; the phase should take all the permutation of $\theta_i - \theta_1 = 0$ or π, $k = 2 : N$.

Since larger $A_i(n)$ means larger $b_i(n,\mathscr{R},\beta)$, the amplitude design choice is straightforward. Therefore, we will mainly focus on proving how the phase design can cover all the maximum combination. It is noteworthy that the following proof applies to arbitrary tag location and arbitrary orientation, because they only influence the amplitude value $b_i(n,\mathscr{R},\beta)$. We will thus remove $\mathscr{R}$ and β to ease the exposition.

Starting with 2 TX coils, by taking the derivative of Eq. 3.10 with respect to the phase difference $\Delta\theta_2(n) = \theta_2(n) - \theta_1(n)$, we can see that $P_{H,2}(n)$ is maximized when $\Delta\theta_2(n)$ equals 0 or π. Therefore, the two TX coils only need to try two values of $\Delta\theta_2(n)$, *i.e.* 0 or π, in order to identify the phase offset configuration that achieves optimal magnetic beamforming.

Now, we prove when extending the number of TX coils to N based on Eq. 3.11. By controlling the phase difference between the ith coil and the 1st coil $\Delta\theta_i(n) = \theta_i(n) - \theta_1(n)$ and traversing $\Delta\theta_i(n) = 0$ or π, N TX coils can deliver the following amount of power to a tag:

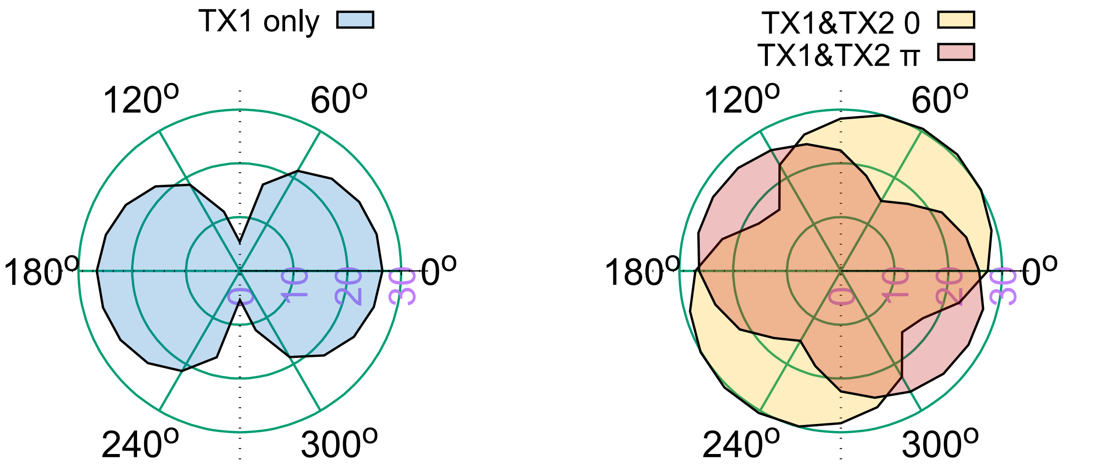
$$P_{H,N,0+\pi}(n) = \big(|b_1(n)| + \sum_{i=2}^{N} |b_i(n)|\big)^2 \tag{3.12}$$

Next, we prove $P_{H,N,0+\pi}(n)$ is maximum. By subtracting $P_{H,N}(n)$ from $P_{H,N,0+\pi}(n)$, we get

$$\begin{aligned} &P_{HN,0+\pi}(n) - P_{HN}(n) \\ &= 2|b_1| \sum_{i=2}^{N} |b_i(n)| \big(1 - sign(b_1(n)b_i(n))cos(\Delta\theta_i(n))\big) \\ &+ 2\sum_{i\neq j} |b_i(n)||b_j(n)| \big(1 - sign(b_i(n)b_j(n))cos(\Delta\theta_i(n) - \Delta\theta_j(n))\big) \end{aligned} \tag{3.13}$$

where $sign(\cdot)$ indicates the sign of a number. Since both sign value $sign(b_1(n)b_i(n))cos(\Delta\theta_i(n))$ and $sign(b_i(n)b_j(n))cos(\Delta\theta_i(n) - \Delta\theta_j(n))$ are smaller than 1, we have $P_{H,N,0+\pi}(n) \geq P_{H,N}(n)$. Therefore, N TX coils can deliver the maximum amount of power to tags by setting the phase of each TX coil to either 0's or π's. In practice, an $N \leq 6$ will suffice for activating the tags in the region of interests. Hence, the codebook size (or searching complexity) for NFC+'s beamforming system is just $2^{N-1} \leq 32$, which can be sweeped through in a very short amount of time.

We now conduct a simple experiment to illustrate the effectiveness of NFC+'s magnetic beamforming. Using the setup in Fig. 3.9, we place a pick up loop at the tag2 location. Then,



(a) Single TX coil

(b) Two TX coils with 0 or π phase difference.

Figure 3.10. Beam patterns when using a single TX coil and two coils with magnetic beamforming.

we rotate the pickup loop while measuring the captured signal strength. We compare our beamforming method with the single coil setup. Fig. 3.10 shows that a single fixed $\Delta\theta$ cannot cover all of the orientations which explains why commercial NFC cannot read tags with undesired orientations. In our case, by switching between $\Delta\theta = 0$ and $\Delta\theta = \pi$, our magnetic beamforming algorithm is able to achieve the strongest strength across all the orientations.

3.6 Passive mag-repeater

The real-world environments of logistics operations are dynamic and unpredictable. To overcome the ”last mile” challenge and achieve overall reliability $> 99.9\%$, NFC+ further introduces a magnetic repeater (mag-repeater) to compensate range and angle coverage and eliminate ”dead spots”. With the help of the mag-repeater, NFC+ is able to deliver energy and communicate to tags that are trapped in extremely unfavorable conditions. Unlike the conventional RF relays [135], *the* NFC+*'s mag-repeater is a passive, battery-free device.* Specifically, as illustrated in Fig. 3.11, mag-repeater is a one-turn coil (in green color) that is remotely coupled to either the TX or the RX coils of the reader (in blue color). The mag-repeater forms a ”slave-master” relationship with the reader and spontaneously repeats a reader’s action even though it does not have a battery. The passive nature of NFC+'s mag-repeater allows it to be easily deployed in various harsh environments. In the following analysis, we will show how this mag-repeater interacts with the TX coil and how it can act like an independent TX coil without the need of active components. The analysis focuses on the TX but it also applies to the RX.

As shown in Fig. 3.12a, suppose a reader's TX coil produces a magnetic field flux that passes through the one-turn circular repeater coil denoted in green color with radius R_{rep}. Because wavelength (22 m) at 13.56 MHz is large, the phase of the magnetic field remains nearly constant within the operating range of the TX coil. Therefore, as shown in Fig. 3.12b, the magnetic flux produced at the repeater by a current $Isin\omega_c t$ on the TX coil can be written as $\Phi sin\omega_c t$, where $\Phi = B_{TX}\pi R_{rep}^2$ and B_{TX} is the average magnetic field strength passing through the mag-repeater's coil. The time-varying magnetic flux induces an electromotive force in the repeater coil following Maxwell's equation [155]. Along the positive direction of the magnetic flux in Fig. 3.12, the electromotive force e is

$$e = \frac{d\Phi}{dt} = \omega_c \Phi cos\omega_c t, \tag{3.14}$$

which can be treated as an equivalent signal source. Therefore, we can model the passive mag-repeater as a serial RLC circuit driven by a voltage source as shown in Fig. 3.12b. Then the current through the inductor (the coil) becomes

$$i = -\frac{e}{Z} = -\frac{e}{j\omega_c L + R_s + \frac{\omega_0^2 L}{j\omega_c}} \tag{3.15}$$

where ω_0 is the resonant frequency of the mag-repeater, which will impact how the mag-repeater collaborates with the TX coil.

Let's take a look at the normalized amplitude and differential phase response of the current on the repeater with respect to a reader coil resonating at 13.56 MHz. Fig. 3.13a shows that the elicited current amplitude in a mag-repeater attains maximum when its resonant

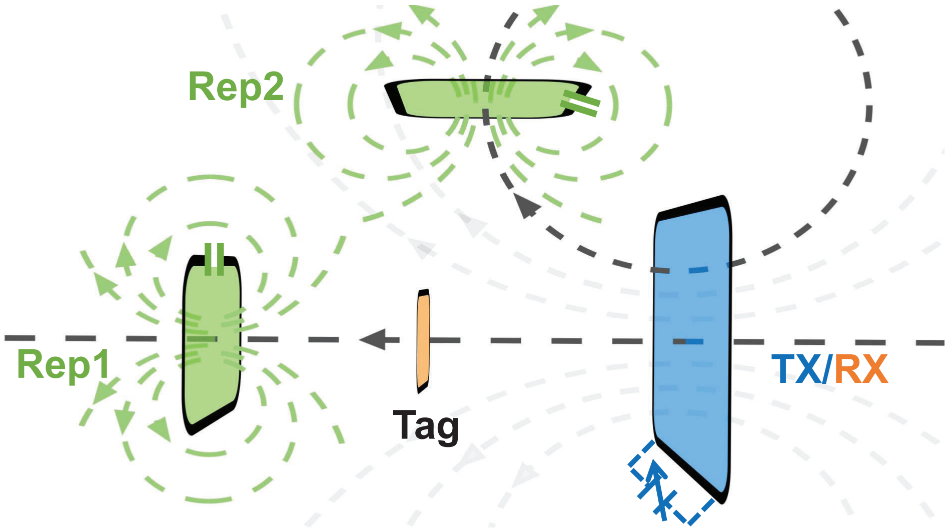
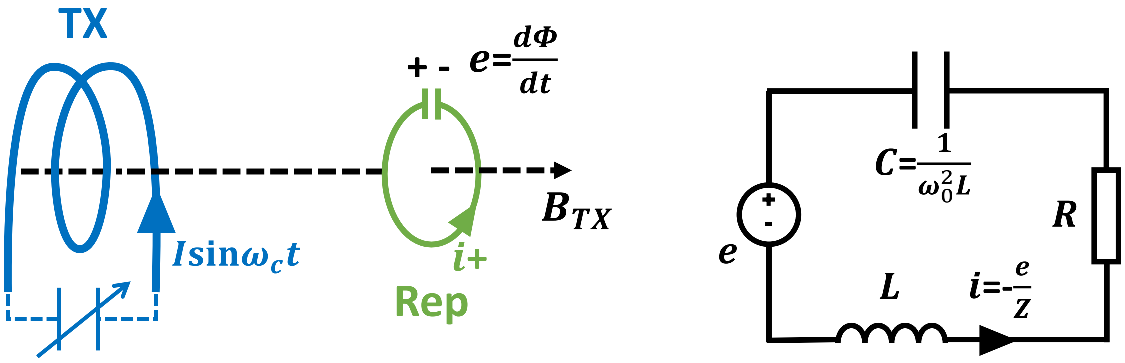


Figure 3.11. TX coil, mag-repeater placement and magnetic field line from TX coil and mag-repeater.



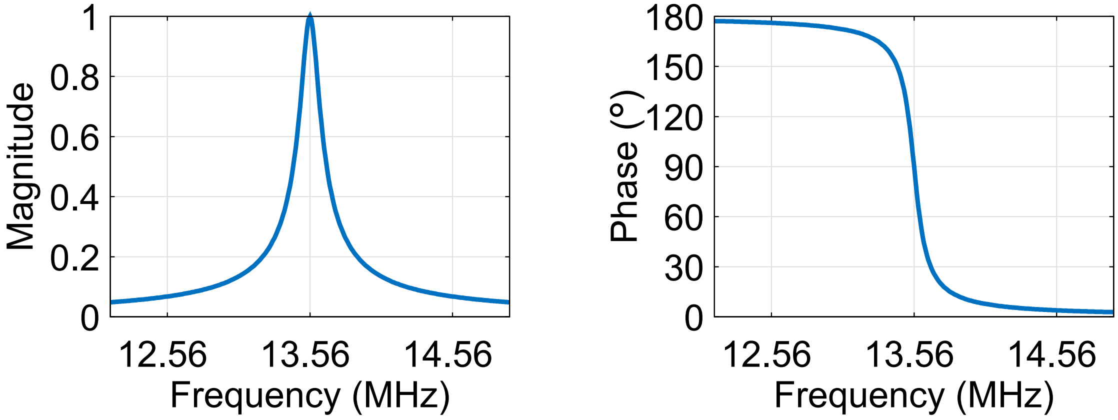
(a) Mag-repeater excited by a TX coil.

(b) Simplified circuit of mag-repeater.

Figure 3.12. Simplified circuit model of mag-repeater.

frequency is equal to that of a TX coil, and the amplitude response will quickly drop if the repeater's resonant frequency deviates from 13.56 MHz. Moreover, Fig. 3.13b shows that the phase of the signal elicited by the mag-repeater has a 90° phase difference compared to the 13.56 MHz signal from the TX coil when the repeater is resonating at 13.56 MHz.

By taking $\theta_2(n) - \theta_1(n) = 90^\circ$ in Eq. 3.10, the final power will be $\left(b_1(n,\mathscr{R},\beta)\right)^2 + \left(b_2(n,\mathscr{R},\beta)\right)^2$. This means the 90° phase difference does not introduce destructive combination although it deviates from the optimal phase combination discussed in Sec. 3.5.2. In fact, the gain on amplitude response when resonating at 13.56 MHz will be higher than the maximum



(a) Mag-repeater current magnitude response. **(b)** Phase difference between TX and mag-repeater.

Figure 3.13. Magnitude and differential phase response over frequency of a repeater with respect to a reader coil resonating at 13.56 MHz.

constructive combination, because when the phase equals to 0 or π (repeater is resonating at higher or lower frequency) the amplitude response will drop a lot. So having the repeater resonating at the carrier frequency 13.56 MHz is a better choice when it is design for helping TX. Moreover, if the repeater is located in an appropriate region with a sufficient Q, its elicited currents can be as large as that in the original TX coil (several amps), which subsequently generate strong magnetic fields (can be even higher than that from the TX coils when the location is near to the repeater). With this modeling, *the passive mag-repeater acts equivalently as a TX coil*, introducing more diversity and helping eliminate "dead spots" undiscovered by the reader.

3.7 Implementation

In this section, we describe the implementation of NFC+, which consists of a multi-channel reader, high-Q resonant loop coils and passive mag-repeaters. Fig. 3.14 gives the photo of the reader PCB. It contains the TX module, RX module and the central processing unit which runs the physical and MAC layer protocol.

TX module. The TX module supports 4 concurrent TX paths. It employs a phase controller that tune phase independently in each path to perform the magnetic beamforming (Sec. 3.5.2). The

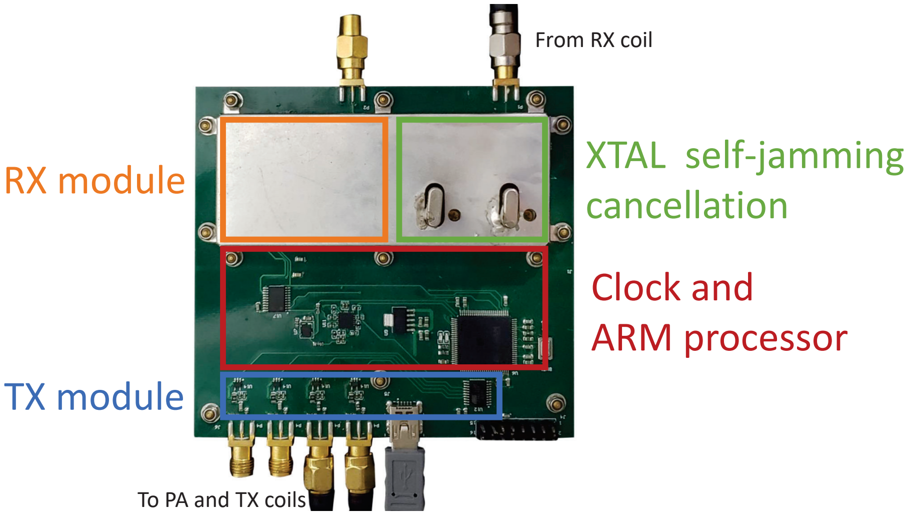


Figure 3.14. Photo of the NFC+'s reader PCB

phase controller includes 4 flip-flop-based QPSK modulators that run on a 13.56 MHz $\times$ 4 = 54.24 MHz clock, which is generated from an ATF16V8A PLD to obtain different phase values. After the carrier with the desired phase value is generated, ASK modulation is applied to encode downlink data using RF switch. The output signal power delivered to TX coils is set at 5 W.

RX module. In the RX module, a 2-stage crystal notch filter with 13.56 MHz nulling-frequency is inserted before the amplification module to suppress the large self-jamming from TX. The notch filter uses air-core inductors to avoid saturation in order to achieve low insertion loss (measured 0.3 dB total). The signal output from the notch filter is amplified by a low noise amplifier (LNA) PHA-13HLN+ and then fed into an image-rejection LC bandstop filter. As discussed in Sec. 3.4.2, the standard NFC tag modulates on both sidebands at 13.11 MHz and 14.01 MHz. Therefore, we design NFC+'s RX module to be reconfigurable so that it can support two sets of configurations. These uplink sidebands are down-converted to an IF at 10.7 MHz for IF processing. We apply two 10.7 ± 0.18 MHz ceramic filters SFECF10M7GA00 to further attenuate the interference and reduce the noise bandwidth. We use a 16-bit ADC to sample the IF signals. The digital samples are processed by the controller which performs digital filtering, frame synchronization, and coherent demodulation.

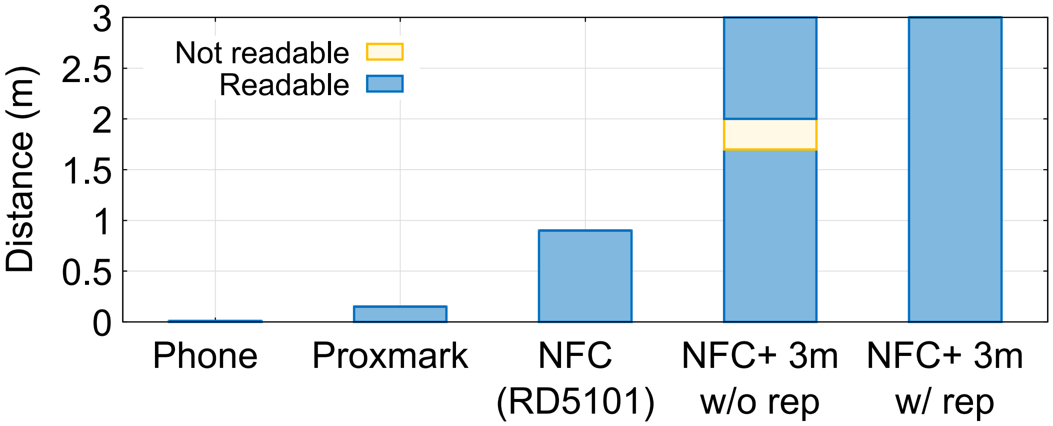


Figure 3.15. Comparative maximum operational distance.

Protocol & processing unit. The processing unit is an STM32 ARM Cortex-M7 MCU, in which we implement ISO 15693 [96] compatible physical-layer (de-)modulation and MAC-layer protocol in C++. The MAC protocol implements collision detection and can support ¿50 tag/s read-rate which is sufficient for logistic applications. All modules are clocked from single PLL-DLL clock generator Si5351A which provides multiple clock frequencies derived from one crystal reference. This reference clock sharing helps avoid the carrier frequency offset issue in the tag signal decoding.

High-Q coils. The resonant TX/RX coils use aluminum gamma-loop [210]. Each coil has a 0.9 m×1.1 m dimension, high power rating, and a tunable Q value up to 300 which perfectly satisfies our high Q and high power requirement.

Mag-repeater. The repeater loop is a customized one-turn loop using a copper tube with a diameter of 9.42 mm. It is connected to a PCB board with external (variable) shunt and series capacitors for tuning and impedance-matching.

Tags. NFC+ communicates with *standard low-cost battery-free NFC tags that support ISO 15693 protocol*, such as the tags built on NXP ICODE and the MIFARE family chipsets [151].

3.8 Evaluation

In this section, we will show NFC+ can read commercial NFC tags at different distances and various orientations.

3.8.1 NFC+'s operational distance

We compare the reading range of NFC+ against 3 baseline NFC systems: a smartphone NFC reader [79], Proxmark [165] (an open-source NFC reader that has evolved over 10 years), and Andea Electronics RD5101 [130] (a commercial NFC reader that claims decimeter level reading range). Fig. 3.15 summarizes the results. Since the smartphone, Proxmark, and RD5101 use only one coil for both transmission and reception, we place a tag parallel to the coil (i.e., the most favorable orientation) and gradually move the tag away. Then, we measure whether the tag can be read across distances.

The smartphone can only read tags around 1 cm away because it is primarily used for secure payment which does not operate at a long distance. Proxmark can read tags at a distance of no more than 15 cm. As a result, it is mainly used as a tool for the sniffer and debugging. To our knowledge, RD5101 reaches the longest reading range of NFC reader. Using 8 W output power and an 80 cm$\times$50 cm coil, RD5101 can read tags up to 90 cm away, which is still not sufficient for the 2.5 m range needed by many logistics network applications. Note that current RD5101 hardware only supports one coil. Therefore, it cannot leverage the high Q coils used in NFC+ since the communication symbols is distorted due to the narrow bandwidth. Moreover, even if RD5101's hardware is modified to support two coils, one for transmission and one for reception, its RX sensitivity is not sufficient due to lack of self-interference cancellation design.

Since NFC+ support multiple coils, we place one RX coil 3 m away from the TX coil. Then, we place a tag between the TX and RX coils and move it away from the TX coil. When the repeater is not used, the tag can be read when it is 0$\sim$170 cm and 200$\sim$300 cm away from the TX coil. Tag inventory fails for distance 170$\sim$200 cm because the summation of the downlink

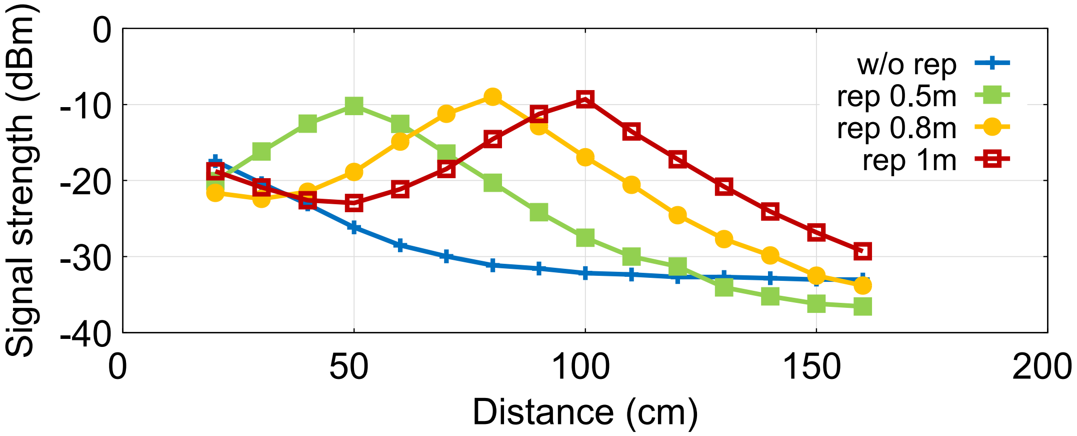


Figure 3.16. Mag-repeater helps improve the signal strength at long distances.

and uplink budget is the smallest at these locations.

Then, we place a mag-repeater between TX and RX coils and keep the repeater to tag distance as 50 cm. With this setup, NFC+ can consistently read tags across the whole 3 m region between the TX and RX coils. This *reliable operational distance* is 3× longer than RD5101, 20× over Proxmark and 300× over the smartphone NFC reader. Therefore, NFC+ is the first system that can operate at a relatively long distance that enables the inventory of bulk commodities in retail/warehouse settings.

To understand how a mag-repeater helps improve the operational distance of NFC+, we place a mag-repeater 0.5 m, 0.8 m, and 1 m away and in parallel to the TX coil. Then, we increase the TX-tag distance and measure the power received by the tag using a pickup loop. As Fig. 3.16 shows, without the mag-repeater, the received power decreases monotonically over distance. However, with a mag-repeater, the received power is significantly improved by 16-23 dB, and maximized when the tag is close to the mag-repeater. Improvement occurs within ±50 cm range of the repeater.

3.8.2 Handling undesired orientation

We also benchmark NFC+'s performance when tags are placed with different orientations. As Fig. 3.9 shows, we place two TX coils (TX1 and TX2) perpendicular to each other and

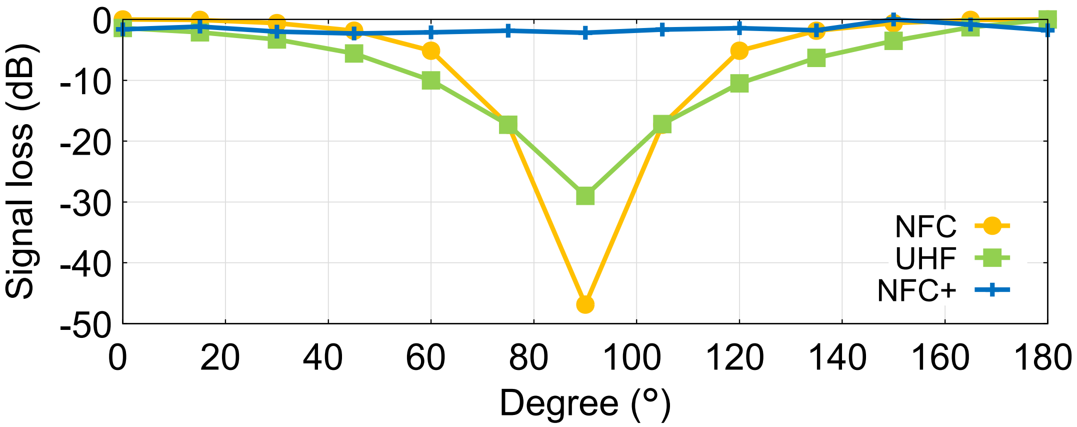


Figure 3.17. Performance of NFC+, state-of-the-art NFC, and UHF RFID with different tag orientations.

Table 3.1. Signal strength degradation when an NFC or UHF tag is attached to different products.

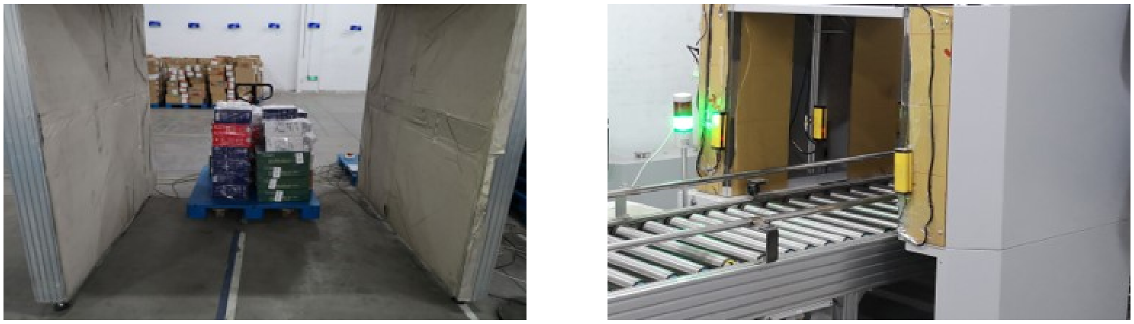
Products	Bottle water		Can coke		Bottle Coke		Boxed milk		Bottle Beer	
Tag loc.	front	back	front	back	front	back	front	back	front	back
NFC+	0dB	0dB	6.6dB	8.6dB	0dB	0dB	5.6dB	7.6dB	0dB	0dB
UHF	9dB	24dB	13dB	24dB	14dB	21dB	16dB	26dB	6dB	14dB

separated by 1.75 m from center to center. Then, we place two RX coils parallel to the TX coils with the same distances of 2.5 m. An NFC tag is further placed at the center (tag2 location in Fig. 3.9).

Fig. 3.17 shows the loss of signal experienced by a tag compared to its optimum orientation. Signal loss is chosen to compare the performance of heterogeneous NFC, UHF and NFC+ platforms. We can see that NFC+'s tag harvests a strong magnetic flux from TX coils and repeater. Even in the worst case, it only experiences around 3 dB signal strength degradation, i.e., NFC+*'s signal quality is almost invariant to the tag orientation*[6].

As a comparison, we evaluate the performance of RD5101 NFC and UHF RFID when the reader sits at TX1 in Fig. 3.9 and the tag sits at the same location as the NFC+ tag. We can

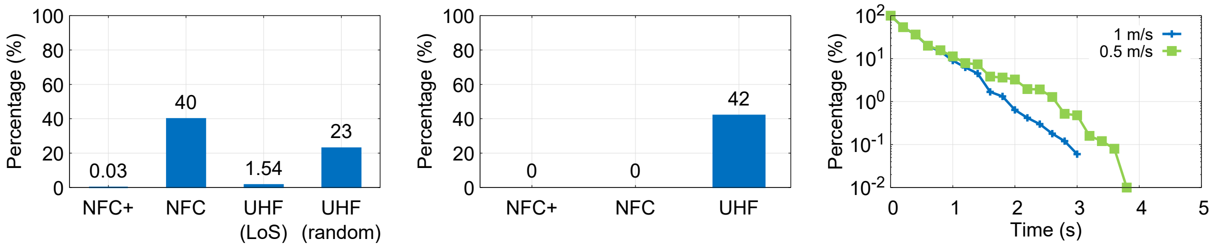
[6] This result happens at a specific location where the strength from multiple coils are balanced. For other locations where the direction and amplitude of magnetic field are changed, the amplitude $b_i(n,\mathscr{R},\beta)$ will not be the same. Then, the combined strength result will not be that flat. But it will still have a larger absolute strength comparing to the single coil setup because of the constructive combination.



(a) Warehouse deployment.

(b) Supply chain deployment.

Figure 3.18. Deploying NFC+ in practical logistic networks.



(a) Miss-reading rate.

(b) Cross-reading rate.

(c) Miss-reading rate over time.

Figure 3.19. NFC+'s performance in a warehouse. Over 10k tags are used. NFC+ can read over 1-0.03%=99.97% desired tags and does not any undesired tags. In comparison, commercial NFC systems and UHF RFID suffers from severe miss-reading or cross-reading.

see that both the UHF RFID tag and NFC tag experience more than 30 dB signal strength loss when its antenna is perpendicular (90°) to the reader antenna. As a result, it is very hard for the UHF RFID reader and RD5101 NFC reader to read tags that are misoriented at around 90°.

3.8.3 Comparing NFC+ and UHF RFID

We now compare the performance of NFC+ and UHF RFID when the tags are attached to the front and backside of various products, corresponding to LoS and NLoS between the reader and tag. Table 3.1[7] summarizes the signal strength difference when the tag is or is not attached to a product.

When the NFC tag is attached to liquid products, such as bottled water, coke, and beer, the received power does not degrade at all. In contrast, UHF suffers from 4-16 dB degradation even

[7] Boxed milk 1 and boxed milk 2 are both packaged in aluminum foil, but the package sizes are different.

under LoS, and much larger (14-26 dB) when the tag is attached to the back of the product. Such a low signal quality makes the UHF tags unreadable even at a short range. The received power of NFC+ degrades when the tag is attached to metallic products, such as Can Coke (6.6-8.6 dB loss) and boxed milk whose packages contain metallic materials. Nonetheless, NFC+'s power degradation is much smaller compared to UHF tags. In addition, as in typical magnetic NFC systems, the problem can be alleviated by simply adding a thin substrate layer [114] between the NFC tag and the product. Such a substrate is well-known and we will not cover its design in paper.

3.9 Logistic network evaluation

We evaluate NFC+ in a warehouse deployment and a supply chain deployment, as illustrated in Fig. 3.18, to understand its performance in practical logistics networks.

3.9.1 Warehouse deployment

In the warehouse setting, the NFC+ reader's coils are embedded on the left, right and top part of a scanning gate, while the mag-repeater is integrated into a moving cart illustrated in Fig. 3.18a. We used over 10,000 tags and attached them to various products that are stored and shipped in the warehouse, including water, milk, cans, beer, bread, oil, etc. Then, we place these products on the moving cart (Fig. 3.18a). The number of products per cart varies depending on the shipping volume, and their orientations are random. We do see some cases where a tag is closely packed between two products, e.g., boxed milk and a box of bottled water. We push the cart through the scanning gate and record the products read by NFC+.

Fig. 3.19 shows NFC+'s performance. We observe that NFC+ can read over 1 - 0.03% = 99.97% of the tags passing through the gate. Much better than the commercial RD5101 NFC system which only reads 1 - 40% = 60%. When UHF tags are placed on purpose, i.e., all tags have LoS with the reader, the UHF RFID system can read 1 - 1.54% = 98.46% of the products. Even though the reading rate seems close to the 99.9% requirement of many logistic applications, such minor tailing error may translate into non-trivial revenue loss for the big warehouses. Moreover, ensuring LoS tag placement costs lots of labor and cannot be guaranteed in practical deployment due to labor shortage and unprofessional worker operation. When products are placed with random orientation, the miss-reading rate of UHF RFID jumps from 1.54% to 23% due to its low reliability under the blockage of products.

To evaluate the cross-reading rate, we define a 4 m×4 m ROI surrounding the TX and RX coil/antenna, and then place tags randomly around the border. From the result in Fig. 3.19b, we can see that neither NFC+ nor the commercial NFC read ANY tag that sits beyond the ROI. In contrast, the UHF RFID experiences a 42% cross-reading rate. The poor cross-reading performance is an inevitable sacrifice when the UHF RFID is tasked to achieve a high reading rate for tags in the ROI, especially those misoriented ones.

In summary, NFC+ is the only system that can achieve over 99.9% accuracy when reading desired tags placed within the ROI while not reading ANY undesired tags outside the ROI. We are unaware of any RFID system that has proven to simultaneously achieve low miss-reading and cross-reading rate, with a large number and diverse type of products. Therefore, we believe that NFC+ is the correct approach for building the next generation of logistic networks.

An additional observation from our experiments is that the speed of a moving cart impacts NFC+'s performance. As summarized in Fig. 3.19c, when the cart passes through the gate at 1 m/s, NFC+ achieves less than 0.1% miss-reading rate (over 99.9% accuracy) within around 2.8 seconds. At a slower speed of 0.5 m/s, NFC+ can achieve less than 0.01% miss-reading rate (over 99.99% accuracy) within around 3.6 seconds. The results imply that slower moving speed does help reduce the miss-reading rate. Such a result is expected for the following two reasons: (1) The magnetic fields form closed loops so when an object traverses the fields, it "sees" more diversified angular coverage. (2) The reader samples tags at a rate of 50-tags/s. Therefore, for a specific tag, a slower motion means more opportunities to be sampled at different orientations which helps reduce miss-reading rate. It is worth noting that the time needed by the reader to sample a tag is on the order of milliseconds which translates to a spatial displacement of

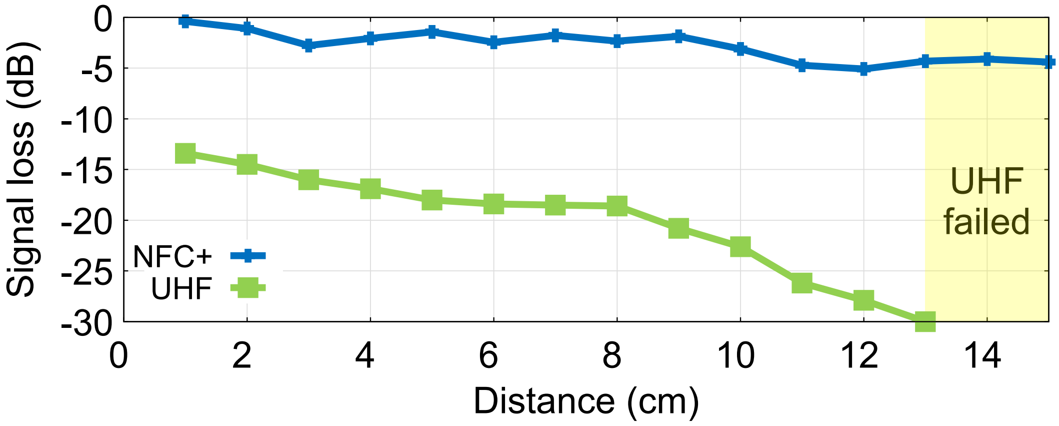


Figure 3.20. Signal degradation when tags are immersed in water. NFC+'s signal does not degrade a lot over distance while UHF RFID signal degrades significantly.

several millimeters when cart motion is involved. Therefore, regular motion will not interrupt NFC communication session because the magnetic strength is almost invariant during a specific sampling period. From the result, even with a faster speed of 1 m/s, NFC+'s miss-reading rate is still much lower than the NFC and UHF RFID systems.

3.9.2 Supply chain deployment

We also evaluate NFC+'s performance in a supply chain system where products in a water tank pass through a conveyor scanning gate, as illustrated in Fig. 3.18b. Fig. 3.20 shows the signal strength degradation when the tag is immersed at different levels of depth (in water), in comparison with an empty tank. We can see that NFC+'s magnetic signal does not degrade a lot as water depth increases. For example, when the tag is 15cm away from the edge of the water tank, the signal degradation is only 3dB, close to its airborne path loss. However, a UHF tag at the same location experiences more than 30dB signal degradation which fails the RFID operation. This experiment epitomizes NFC+'s capability to operate in a harsh environment where UHF RFID ceases to operate.

3.10 Related Work

RFID communication. RFID has been considered as a key enabler for numerous IoT applications [72, 136]. However, through substantial efforts in realistic deployments over the past years, reliability issues of RFID have been discovered and widely reported by industry practitioners [78, 62, 93, 162]. The read rate of RFID was found to be dramatically reduced by the contents of a package. For example, [62] reported that only 25% of tags on containers of water bottles could be read. The readability and range is also heavily impacted by tag orientation [205]. In addition to the miss-reading problem caused by unfriendly materials, another challenge was found to be the cross-reading error [48]. In fact, one major motivation of UHF RFID localization was to address the cross-reading problem [208, 173, 197] by excluding the tags which are out-of-region. Unfortunately, past localization works could not solve the problem. They not only requires tags movement to combat multipath fading, but also could only localize tags in LoS conditions. So they were not applicable to complex industrial environments, especially for the applications that require high reliability. Another line of research tried to improve the efficiency of RFID protocols [195] and extending the communication distance via beamforming techniques [193]. However, these works were mainly based on algorithmic innovations and hence could not address the reliability issue that roots in the physical nature of the technology. In contrast, NFC+ takes a fresh look at this problem and addresses the above challenges with both physical and algorithmic innovations.

Backscatter networking. Both RFID and NFC rely on the physical principle of backscatter. Backscatter networking have also gained a lot of attention in recent years [212, 126, 189, 212, 134]. The low power nature [214] of backscatter made it unique to enable new applications ranging from machine-to-machine communications [126], low-power and low-cost WiFi connectivity [107] to in-body and on-body communications [189, 214, 134]. Unlike NFC+, past proposals extended backscatter principle to novel applications, so the reliability of RFID applications was not their focus. In addition, in order to optimize their specific usages, most of these proposals relied on customized circuit or antennas on the tag side. In contrast, NFC+ is fully compatible with ISO 15693 which is supported by most of today's commercial NFC chips, so it does not require changing NFC tags. Therefore, NFC+ is a ready-to-deploy solution which can be directly applied to many RFID applications.

Magnetic wireless power transfer. NFC+ is also closely related to magnetic wireless power transfer [184, 112, 53]. Magnetic wireless power transfer was initially discovered by Nikola Tesla in 1914 [184]. Tesla designed tesla-coils to show that energy could be moved efficiently between these coils when strong inductive coupling was present. It was later discovered that [112] via strong magnetic resonance, efficient energy transfer could also be obtained even under weak inductive coupling conditions. In addition to leveraging resonance, other researchers proposed to use multiple coils [98, 111, 180] to beam-form energy. For example, MagMIMO [98, 176] showed that one could use multiple coils to charge a cellphone more efficiently than a regular single-coil charging pad. NFC+ leverages the knowledge from these past works but differs in the following aspects. *First*, none of the past systems was designed to work with miniaturized passive devices like NFC tags. In NFC+, the resonance effect on the tag side is usually very limited so it cannot establish strong resonant coupling with the transmit coil like what was needed in [112]. *Second*, in NFC+, we must charge a large number of devices at the same time but unlike a cellphone, these devices are passive and therefore, it is not feasible to obtain the the feedback matrix from them and use iterative beam-forming algorithm as described in [176]. *Last*, the goal of these past proposals was purely wireless charging. They delt with only transmitting but not receiving, so they did not have to satisfy the constraints required by both power link and data link that NFC+ handles at the same time.

3.11 Discussion

Tag Costs. Recent breakthroughs have brought the cost of an NFC tag down to $5 cents [152]. We expect the cost of an NFC tag to further shrink if it is applied to logistic networks for the following reasons: (1) The volume of tags needed by logistic networks is extremely large [158], which will drive down the cost [105]. (2) The minimum length of memory required by logistics (96-bit GID [65]) is much less than what is needed in contact-less payments, which means much smaller die size for an NFC chip and hence lower cost. Therefore, there is a strong economic incentive for logistics network to adopt NFC instead of UHF RFIDs.

Reader Costs. The amortized deployment cost of practical RFID readers is always much less than that of RFID tags, because one reader can be used to read millions of tags. Hence, for logistic network applications, the cost of readers is usually considered negligible. In our prototype, the manufacturing cost of NFC+ reader is about \$1000. The additional cost compared to commercial NFC is due to the specialized multi-coil design and dedicated high sensitivity receiver design. However, we would like to point out that as the reader is built with off-the-shelf components, we expect the cost to shrink drastically once NFC+ is moved into mass production.

Human Safety. The signal used by NFC+ is a non-radiating magnetic field and the strength required to activate a NFC tag is 0.15 A/m or 0.19 µT [96], much lower than the head and limb safety limits of 0.205 mT specified by IEEE standard [63]. NFC+'s reader supports 4 TX channels with 5 W peak output power per channel, consuming a total power around 20 W, which is smaller than commercial wireless charging devices such as Witricity WiT-2000M and Energizer Qi [98].

Design trade-off. We choose to use high-Q coil to improve the range coverage. However, higher Q leads to narrower bandwidth, which means the coil will need more careful tuning and can be more sensitive to the environments (e.g., its resonating frequency may be affected by temperature). To address these issues, a typical solution in magnetic communication is to use a smart auto-tuner [73], i.e., a servomotor that rotates the shaft of the vacuum capacitor according to Standing Wave Ratio (SWR) sensor readout. We leave such enhancement for our future work.

Reading rate. We use unmodified standard ISO 15693 tags. This NFC standard mandates a binary-tree MAC protocol to resolve collision between tags. It allows a reading rate of up to 50 tags/s, which we found to be sufficient for typical logistic applications. Existing research has investigated techniques to improve the reading rate, but these are beyond the scope of our work.

New applications enabled by NFC+. We envision the techniques introduced by NFC+ to enable a variety of novel applications. First, NFC+ enables digital-IDs to be applied in not only the entire life-cycle of a supply chain, but also the interaction with end-consumers. Today's smart phones such as iPhones are already equipped with NFC capabilities, so customers are able to directly obtain logistic information once NFC is used to manage supply chain at large-scale. In addition, as magnetic signals can easily traverse human body, NFC+ opens new opportunities to achieve deep-tissue power delivery and communication with implantable devices for medical applications [189, 134].

3.12 Conclusion

In summary, we present the design and implementation of NFC+, the first system that can do RFID tag inventory with sufficient accuracy and high reliability. NFC+ leverages magnetic field to ensure that it can read 99.9% tags within ROI, even when these tags are attached to or blocked by RFID unfriendly objects, such as milk, cans, water, etc. In addition, NFC+ does not cross-read ANY tag that sits outside the ROI. Our large-scale evaluation in a warehouse shows that NFC+ not only enables using RFID in logistics networks but also paves the way for other other novel applications such as automated new retail and implantable medical devices.

3.13 Acknowledgements

This chapter contains material from "NFC+: Breaking NFC Networking Limits through Resonance Engineering", by Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu and Ming Zhang, which appears in Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication

(SIGCOMM), 2020. The dissertation author was the primary investigator and author of this paper.

Chapter 4

Multi-antenna Wideband UHF RFID for Reliable Localization

4.1 Introduction

Today's major e-commerce companies like Alibaba and Amazon need to handle a package volume that is tens of billions per year [13], calling for increasingly high-performance automated logistics operations in their network. Considering a typical warehouse in which tens or even hundreds of packages pass through each checkpoint – the packages need to be verified, recorded, sorted, and tracked when checking in/out. In widely adopted barcode-based logistic networks, the worker spends 1˜3 seconds on scanning one package. Although this operation can be automated by robots [18], the line-of-sight and field of view requirements of vision-based approaches limits work range and scalability fundamentally. RFID technology, since its invention, has been carrying the vision of replacing inefficient labor and automating inventory management with zero power, near-zero cost, and high throughput.

Towards a highly practical and deployable RFID empowered automated logistic network shown in Fig. 4.1, there are three key considerations: *i) Reliability.* The classic ROI (range of interest) reading task requires the reader to scan all the RFID tags within the ROI (*i.e.* near-zero miss-reading rate) while excluding any tag out of the ROI (*i.e.* near-zero cross-reading rate); *ii) Throughput.* The packages come to the checkpoint in a burst (*i.e.* 100˜200 per pallet) [1] while

[1] Even though one trailer can carry up to 50 packages, the reader should be able to cover all the tags (100˜200

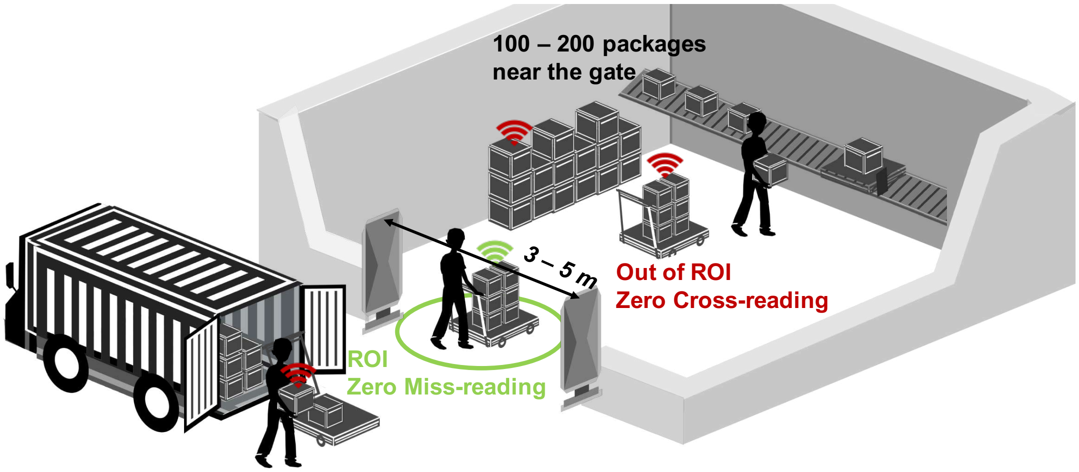


Figure 4.1. In a typical logistic scenario, the packages are discharged from the truck, scanned at an inventory gate and sorted for warehouse check in. The RFID-based inventory gate should meet *reliability*, *throughput*, and *range* requirements at the same time.

all the logistic operations, including verification and recording need to be finished within 2˜3 seconds before check-in/out; *iii) Range.* A single reader should cover tags within 3˜5 m, which is the typical width of the check-in/out aisle.

Unfortunately, today's read-or-not inventory systems, both industrial products and research prototypes, all have limitations in meeting these three requirements simultaneously. Industry-grade RFID systems (*e.g.* Impinj) suffer from miss-reading and cross-reading when deployed in the logistic warehouses. RFGo [47] reports 99.8% recall with 10 carrier-level synchronized antennas and neural network based classifier but limits its operating range to sub-meter. NFC+ [219] achieves a sharp inventory boundary with magnetic resonance engineering that meets the reliability (*i.e.* miss-reading rate of 0.03% and cross-reading rate of 0%) and range (˜3 m) requirements but cannot achieve the desired throughput. No current inventory-based solutions can support automatic package management in a practical logistics network.

RFID localization technique offers an alternative approach toward the same goal by filtering out the reading outside the ROI. Compared with the inventory-based system, the tag location brings a new dimension of information, which can realize a more flexible and accurate

tags) near the gate (including passed trailer and undischarged packages) to ensure to read all the passing packages.

ROI reading. The reliability of ROI reading depends on localization accuracy. However, the legitimate narrow frequency band (*i.e.* 26 MHz ISM band within 902˜928 MHz) of RFID fundamentally limits its capacity of combating multipath and ambiguity [116]. To improve the localization accuracy, approaches like fingerprinting [196] and synthetic aperture radar (SAR) based hologram [208, 173] have been proposed. However, they suffer from prolonged latency due to lots of tag inventory, especially at scale. Cross-frequency based approaches utilize higher frequency band to overcome the bandwidth limitation (*e.g.* 2.4 GHz [132, 34], millimeter wave [30], UWB [37, 67]) but introduce extra tag manufacturing cost due to wider frequency response and higher power attenuation. More recently, sniffer-based RFID architecture [136, 131] has been proposed to leverage the advantage of wideband (*e.g.* 100˜200 MHz) near 915 MHz to boost location accuracy without violating FCC regulation. Despite the potential, these systems either suffer from latency issues due to the lack of hardware support on multi-band parallel information capture [136], or report limited sub-meter range [131].

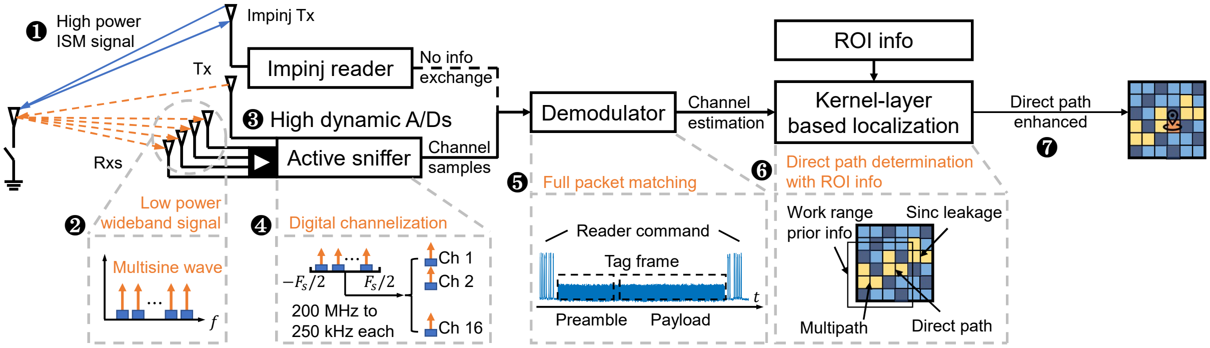


Figure 4.2. RF-CHORD system overview.

This paper introduces the design and implementation of RF-CHORD, an active sniffer-based wideband RFID localization system that tackles the above challenges. RF-CHORD exploits wideband signal and a hologram-based localization algorithm to realize *high reliability*. It employs lossless data stream compression and a GPU-based decoder to guarantee real-time decoding and channel estimation for *high throughput*. It utilizes a customized wideband waveform, full packet matching integration, fine-grained clock offset mitigation, and channel diversity decoding

Table 4.1. Comparing RF-CHORD with state-of-the-art wireless systems for logistic network requirements.

	Throughput (> 100 tags/s)	Range (> 3 m)	Reliability (Near Zero Miss-reading & Cross-reading)	COTS Tag
Barcode (widely deployed)	No (˜1 tag per second)	No (˜1 m)	High (depend on the human labor)	Yes
xSpan [15] (Inventory based)	Yes (˜185 tags/s with 142 mode)	Yes (˜10 m)	Low (˜6% miss reading and ˜2% cross reading)	Yes
RFgo [47]	No (TDMA-based)	No (sub-meter)	High (99.8% recall)	Yes
NFC+ [219]	No data reported	Yes (˜3 m)	High (0% miss reading and ˜0.03% cross reading)	No
PinIt [196]	No data reported	Yes (> 5 m)	Median (a few decimeters)	Yes
RF-IDraw [197]	No data reported	Yes (> 5 m)	Low (sub-meter)	Yes
Tagoram [208]	No (0.2 second for one tag)	No (˜2 m)	Median (a few decimeters)	Yes
MobiTagbot [173]	No data reported	No (˜1.5 m)	High (a few centimeters)	Yes
NLTL tags [132]	No (depend on switching)	No (˜1 m)	High (a few millimeters)	No
mmwave RFID [30]	No data reported	No data reported	Median (a few decimeters)	No
RFind [136]	No (6.4 second for one tag)	Yes (> 5 m)	High (a few centimeters)	Yes
TurboTrack [131]	No data reported	No (sub-meter)	High (a few centimeters)	Yes
RF-CHORD (Our system)	Yes (180 tags/s)	Yes (6 m)	High (0% miss reading and ˜0.01% cross reading)	Yes

to improve SINR for *long range*.

RF-CHORD ensures *high reliability* (*i.e.* near zero miss reading and cross reading) by high-accuracy localization. Our study (Sec. 4.5.1) shows that the multipath profile causes long-tail localization errors. Therefore, we design the fine-grained distance resolution hardware and multipath-suppression algorithm to handle these long-tail errors. Considering that the distance resolution is inversely proportional to bandwidth (*i.e.* $\frac{c}{2B}$), the distance resolution of a conventional UHF RFID reader, which works on a 26 MHz wide ISM band, is only 5.78 m. RF-CHORD introduces an extra active sniffer-based reader to help UHF RFID reader realize 200 MHz parallel wideband localization (Sec. 4.3.2). However, the distance resolution of 200 MHz (0.75 m) is still not enough in all situations. RF-CHORD exploits a kernel-layer-based near-field localization algorithm framework to handle corner cases. The kernel function characterizes the location estimation from a single channel, and layer functions coherently combine multiple channels into a final location estimation. This framework supports choosing different kernel and layer functions suitable for various deployment scenarios to achieve multipath suppression and ambiguity reduction (Sec. 4.5.3). For example, in RF-CHORD's deployment in the warehouse, the work range is fixed so it can be taken as prior information for direct path enhancement to effectively suppress the multipath effect (Sec. 4.5.4).

RF-CHORD ensures *high throughput* by one-shot channel measurement and one-shot location estimation. The hardware supports concurrent phase and amplitude capture across multiple antennas and wide bandwidth. Therefore, RF-CHORD can obtain the necessary information (*i.e.* wideband channel estimation across multiple antennas) for localization within only one shot measurement. It is challenging because: i) directly capturing the wideband signal from a large array will result in a huge amount of real-time data (˜64 Gbps); ii) the commercial reader does not support real time synchronization (*i.e.* synchronizing with our sniffer-based reader at each slot [11]). Utilizing the essence that the wideband backscattered signal is a combination of scattered narrowband signals, RF-CHORD distills 4 MHz valid bandwidth from 200 MHz bandwidth to reduce the data rate by 50x without information loss (Sec. 4.3.4). Meanwhile, we develop a

GPU-based wideband decoder to ensure real time decoding and channel estimation. In other words, the sniffer-based reader has an independent decoder and does not depend on any specific commercial reader interface. It makes our design adaptive to any ISM band commercial reader, which primarily serves as a power activator and multiple access handler (Sec. 4.4). Finally, RF-CHORD supports one-shot localization with 8 antennas and 16 frequencies across 200 MHz in ˜5 ms.

RF-CHORD ensures *long range* (up to 6 m) with multi-sine waveform sniffer and sophisticated wideband channel information estimation. To follow the FCC regulation, the strength of the sniffer excitation signal needs to be *smaller than -13.3 dBm* (see Sec. D for the calculation), which is 50 dB weaker than that of commercial readers. RF-CHORD features the following designs for signal-to-interference-plus-noise ratio (SINR) enhancement without modifying the tag chip: i) It exploits a multisine waveform, which constructs a whole 200 MHz band by taking samples with multiple narrow bands, to significantly reduce the noise bandwidth (Sec. 4.4.1); ii) It handles the high dynamic range requirements introduced by self-interference through high-resolution digital channelization and a low crest factor waveform design (Sec. 4.4.2); iii) It further exploits the integration gain of full packet matching (Sec. 4.4.3) and performs accurate tag clock offset mitigation (Sec. 4.4.4) and decoding with channel diversity (Sec. 4.4.5).

We deploy RF-CHORD and our results show that RF-CHORD presents the first RFID (localization) system meeting all the requirements (*i.e.* reliability, throughput, and range) in the logistic network (Tab. 4.1). The key results are:

- **Reliability.** We evaluate RF-CHORD's performance at 384 locations and collect over 20k tag responses in the lab environments. Its 99% localization error is 0.786 m. We deploy RF-CHORD in the dock door of a warehouse and the scanning gate of a fresh food delivery store. We find that it could read 100% of the tags passing the checkpoint (0% miss-reading rate). Its cross-reading rate is only 0.0025%˜0.0154%, which is up to 12x improvement compared to state-of-the-art [47, 219].

- **Throughput.** RF-CHORD can localize up to 180 tags per second, which is very close to pure inventory devices [15] and two to three orders of magnitude faster than state-of-the-art localization systems [136, 208].
- **Range.** RF-CHORD can localize tags 6 m away from the reader with transmit power below -15 dBm. There is no obvious throughput and reliability loss with distance increasing.

We open sourced the RF-CHORD's hardware and software as well as the evaluation dataset in https://soar.group/projects/rfid/rfchord.

4.2 RF-CHORD's System Overview

A high level operational flow of RF-CHORD is shown in Fig. 4.2. RF-CHORD embraces any ISM-band reader ❶ as the tag activator that is capable of charging, coordinating multiple access over EPC Gen II tags. Active sniffer reader observes tags by emitting a low power (-15 dBm) wideband multi-sine waveform to pick up tag responses over a wide frequency band. Specifically, we build the RF frontend and FPGA hardware ❷ as a scalable platform that can receive the tag response from 8 antennas and 16 frequencies of carriers simultaneously. Furthermore, despite the strict legal emission power limit, we still achieve a long range in sniffing the tag response in the wideband without exchanging any information (*e.g.* EPC ID) with the ISM-band reader. RF-CHORD achieve independent decoding and channel estimation by using dynamic range optimization ❸, digital channelization ❹ in hardware, and a real-time full packet matching ❺ in software. After one-shot tag inventory, RF-CHORD obtains adequate information from both frequency and spatial domains, which are important for robust localization in a multipath-rich environment. RF-CHORD also uses a kernel-layer-based near-field localization algorithm to suppress the multipath effect. This algorithm identifies the direct path with the time of flight profile and prior knowledge (region of interest or ROI information in our paper) ❻.

Then it enhances the direct path and estimates the location with a summation layer (a form of near-field AoA+ToF localization) ❼.

4.3 One-shot Wideband with Multisine Wave

This section explains why we select multisine wave as the wideband signal and how RF-CHORD acquires fine-grained tag responses in one shot. We review the primer of the backscatter signal model and its fundamental narrowband constraint. Then we present our design of constructing a wideband backscatter signal with the multisine waveform on Tx and slicing it for real-time parallel processing on Rx.

4.3.1 Backscatter Signal Model Primer

The basic backscatter operation in RFID systems is shown in Fig. 4.3a. A device emits a high-power single-tone excitation signal $s(t)$ to power the tag and act as a carrier. This carrier will be modulated by the baseband signal $B_{\text{tag}}(t)$ of the tag. The resulting (mixed) backscattered signal is:

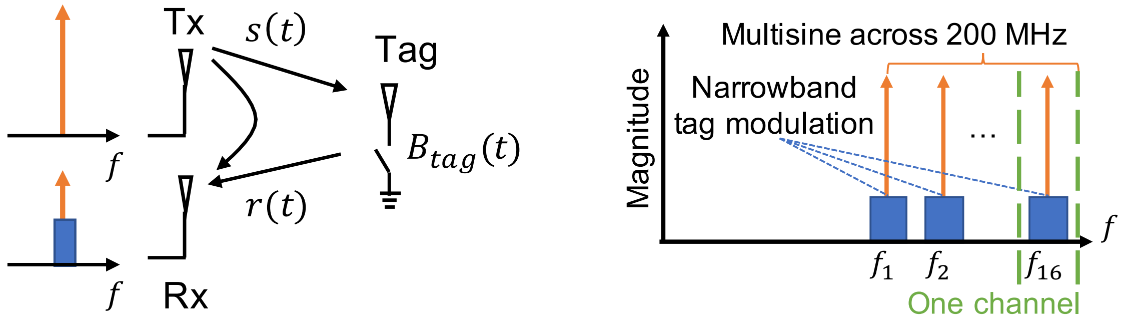
$$r(t) = s(t) \cdot B_{\text{tag}}(t)$$

Note that the bandwidth of $r(t)$ is the summation of that of s(t) and $B_{\text{tag}}(t)$, and $B_{\text{tag}}(t)$ is typically a narrowband signal[2] for low power purpose according to the EPC Gen II standard. Therefore, the backscattered signal $r(t)$ will also be narrowband given that $s(t)$ is a single tone.

4.3.2 Backscattering with Wideband Multisine Wave

When applying a wideband signal $s(t)$, one can retrieve a wideband backscatter signal $r(t)$. Following this idea, RF-CHORD adopts a multisine signal as $s(t)$. The multisine signal is a combination of multiple single tones across wide band with the same amplitude $s(t) = \sum_i \sin(f_i t + \phi_i)$. The backscattered signal will be $r(t) = \sum_i B_{\text{tag}}(t) \cdot \sin(f_i t + \phi_i)$. RF-CHORD adopts 16 carriers with different frequencies across a 200 MHz band in the practical implementation.

[2] We take 250 kHz as the bandwidth $B_{\text{tag}}(t)$ for the whole paper according to the standard [11].



(a) Single-tone backscatter.

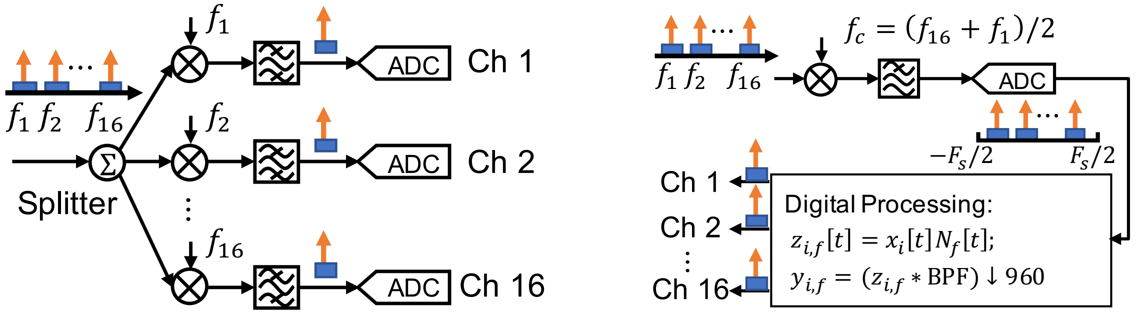
(b) Multisine excitation signals.

Figure 4.3. Model of multisine backscatter.

Fig. 4.3b shows the spectrum of multisine signal $s(t)$ with backscatter signal $r(t)$. Since the difference between each carrier frequency is much larger than the bandwidth of $B_{\text{tag}}(t)$, the received signal can be treated as multiple copies of $B_{\text{tag}}(t)$ modulated on different carrier f_i. Therefore, on Rx, $r(t)$ can be sliced to 16 individual narrowband channels without information loss, and then the channel information at each carrier frequency f_i can be extracted by using a well-explored RFID processing mechanism (*e.g.* mixing and demodulating) in parallel. In a nutshell, we sample the wideband with multiple narrowband signals, enabling RF-CHORD to construct the wideband channel information within one shot.

4.3.3 Why Multisine Wave

The multisine waveform has two advantages. First, the multisine waveform is adaptive to conventional narrowband decoding and channel estimation because the signal in each channel is still narrowband. Extracting these narrowband signals can achieve excellent data rate compression (Sec. 4.3.4). Second, the multisine waveform is amenable to noise and interference reduction because of the low noise bandwidth and low chances of being interfered with, resulting in SINR enhancement, which improves the work range (Sec. 4.4.1). Compared with the two alternative well-known wideband waveform choices, frequency hopping [136] and OFDM signal [131], the multisine waveform is more efficient because it avoids the time overhead in switching between carriers introduced by the former one, and uses the same bandwidth as the (tag) modulation



(a) Analog channelization.

(b) Digital channelization.

Figure 4.4. Two channelization approaches.

bandwidth, which is 250 kHz out of the full 200MHz bandwidth used by the latter one. In fact, this wideband but narrow sample signal can introduce 29 dB gain on the SINR compared to the full wideband signal (see Sec. 4.4.1), which means around 5× range under the same transmit power. Furthermore, since the multisine wave captures all the backscatter signals in the time domain, the whole packet of tags can be fully utilized for integration gain to improve the SINR (see Sec. 4.4.4).

4.3.4 Digital Wideband Channelization

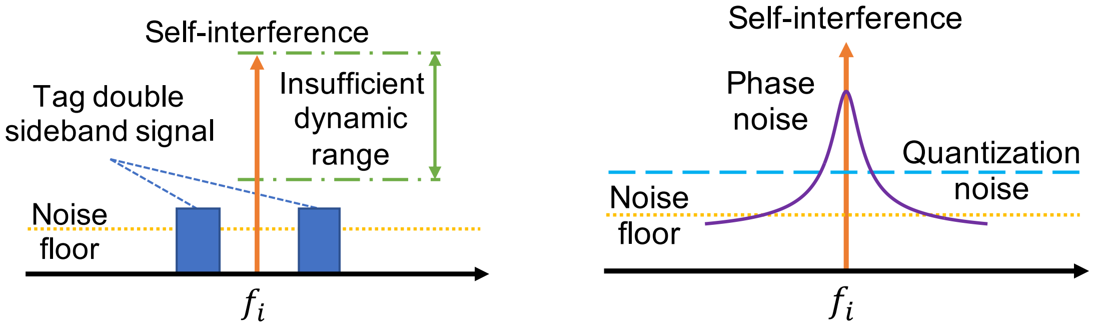
RF-Chord utilizes channelization, which enables one-shot capturing of wideband signals across multiple antennas and reduces the amount of data to be processed during real-time operation. Channelization is a process of extracting effective narrowband signals from a received signal. When a wideband tag signal is received, the aggregated bandwidth of 8 antennas will be 1.6 GHz, resulting in a total of 64 Gbps data (16-bit IQ sample, 1.25× Nyquist). It is challenging to process such massive data in real time. However, recall that with a multisine excitation signal, the effective tag signal is only located around the carrier frequencies, as shown in Fig. 4.3b. Therefore, the effective bandwidth of the system should be 8 × 16 × 250 kHz = 32 MHz, only 1/50 of the full 200 MHz bandwidth, so that channelization can compress the data validly without information loss.

There are two channelization schemes to extract these narrowband signals: analog channelization and digital channelization. As shown in Fig. 4.4a, the sniffer with analog channelization has multiple RF chains for the corresponding channels. Each RF chain uses one carrier frequency f_i as its local oscillator (LO) for down-conversion and a filter at the baseband to filter the signal from other channels out. Alternatively, digital channelization finishes all the aforementioned functions in the digital domain as shown in Fig. 4.4b.

RF-CHORD adopts digital channelization – the sniffer will generate and capture the whole multisine wave with one RF chain. On the Rx side, an ADC/DAC with a 245.76 MHz sampling rate captures all tag signals simultaneously. Further channel extraction can be achieved by digital down-conversion and digital filtering. Digital channelization offers two significant benefits over analog channelization: First, it has better scalability because it only needs one RF chain for each antenna, regardless of the number of channels (and sine tones) are required, while in analog channelization, each channel needs an exclusive RF chain with bulk components (*e.g.* mixer, PLL, and VCO). Second, it is precisely synchronized among different tones in the multisine wave, while analog channelization needs extensive engineering efforts to synchronize among a large amount of ADCs/DACs and LOs. Nevertheless, analog channelization still has it own advantages, including the convenience of extending or switching bandwidth by changing the carrier frequency and the lower requirements of ADC bandwidth. RF-CHORD also embraces these advantages through the high-speed ADC and low crest factor multisine waveform, which will be introduced in Sec. 4.4.

4.4 SINR Improvement for Long Range

This section first presents how RF-CHORD improves SINR under long work range by reducing the external noise and canceling self-interference. It next explains how RF-CHORD exploits the full tag packet to incorporate the integration gain, which is based on the multiple channel decoder with clock offset mitigation.



(a) Dynamic range. **(b)** Unpredictable noise.

Figure 4.5. Two issues caused by self-interference.

4.4.1 External Noise Suppression

To follow the FCC regulation, the signal strength of each frequency component in the multisine is -15 dBm, which is 51 dB lower than the 36 dBm excitation signal in the ISM band (see details in Sec. D). With the low signal strength limitation but the long range requirement, we need to reduce the external noise and interference as much as possible.

RF-CHORD adopts the tag signal with reduced bandwidth for lower chances of in-band interference and lower noise. The relationship between thermal noise P_{noise} and signal bandwidth B at room temperature can be expressed as $P_{\text{noise}} = -174 + 10\log_{10}(B)$ [161]. As described in Sec. 4.3.4, the digital channelization at the receiver separates a combined 200 MHz wideband signal into multiple 250 kHz narrowband signals. This means that the thermal noise can be reduced from -91 dBm to -120 dBm (29 dB gain). Furthermore, the reduced bandwidth also reduces the probability of being interfered with by other devices working in the same band.

4.4.2 Self-interference Canceling

Besides the external interference from other devices, the self-interference caused by the natural full-duplex operation of our active sniffer will also limit the SINR. RF-CHORD's multisine waveform and low power transmission reduce the complexity of self-interference cancellation. As shown in Fig. 4.5a, the self-interference in one channel is just a single tone after channelization. A commercial tag uses double-sideband modulation with a subcarrier to differentiate the tag signal from the single-tone excitation signal. Therefore, RF-CHORD uses filters to cancel the self-interference caused by the single tone.

However, given the wideband signals are too weak (*i.e.*-15 dBm), there remain two practical challenges. First, the dynamic range of the receiver may not be large enough to detect the tag signal. Second, any unpredictable noise, such as phase noise and circuit noise from Tx, will be transmitted along with the $s(t)$ and may bury the wideband signal. Then we'll go over how to deal with these issues.

Dynamic Range. Dynamic range is the ratio between the largest and smallest values that the received signal can assume. Specifically, the largest value is the self-interference, and the smallest signal is the targeted wideband tag signal. As shown in the Fig. 4.5a, even though the tag signal strength is higher than the noise floor and interference, it can still be buried if the dynamic range is not large enough. RF-CHORD meets the requirement of dynamic range by adopting the following strategies: First, it adopts a high-resolution ADC because the dynamic range of the receiver will be bottlenecked by the dynamic range of the ADC. The theoretical dynamic range of the receiver is 6.02 N + 1.76 dB [22], where N is the resolution of the ADC. Therefore, a fundamental way to solve the issue is to increase the resolution of the ADC. RF-CHORD adopts 16-bit ADC, which has the largest resolution in 2022 when satisfying the 200 MHz bandwidth requirement. Secondly, it adopts a carefully designed low crest factor multisine wave on the transmission side to relax the dynamic range requirement of the Rx. The intuition behind this is that since the dynamic range requirement on the ADC is more related to the peak amplitude of the self-interference signal instead of the average signal power, it can be relaxed by using a lower peak signal while remaining the average power. The crest factor is the peak amplitude divided by the RMS value of the waveform, and for a multisine signal, it has been well studied that the crest factor can be reduced by tuning the phases ϕ_i in the multisine signal. Following the methods mentioned in [209], the crest factor of the multisine waveform adopted by RF-CHORD can be reduced from 4 to 1.24 (or peak-to-average power ratio from 12 dB to 1.87 dB).

Unpredictable Noise. The unpredictable noise is caused by the response of self-interference in the circuit. As illustrated in Fig. 4.5b, the noise floor may be dominated by the phase noise, DAC quantization noise, *etc.* along with the self-interference. Fortunately, RF-CHORD does not require a dedicated cancellation circuit like [9] because the power of RF-CHORD's self-interference is much lower than that of a commercial RFID reader. Moreover, RF-CHORD utilizes Analog Devices ADRV9009 transceiver of 16-bit ADC [3] and HMC7044 VCXO-based clock tree [14], ensuring an optimal quantization and clock phase noise below the noise floor. Therefore, the RF frontend of RF-CHORD's receiver is not saturated, and the noise will only go through the air instead of the feedback path of the receiver. The noise experienced by RF-CHORD is not dominated by unpredictable noise.

4.4.3 Full Packet Matching

RF-CHORD estimates each channel in parallel and then combines them into a wideband channel estimation. The standard channel estimation techniques for one channel can be expressed as follows:

$$h_i = \sum_t r(t)\hat{I}^*(t)$$

where $r(t)$ is received tag response and $\hat{I}(t)$ is a template. In most RFID systems, only the pilot signal part (RN16) is used for clock and phase estimation, and the main part of the tag signal (EPC ID) is left unused. RF-CHORD utilizes the full packet signal, including RN16 and EPC ID. The length of the signal will be extended from 0.31 ms to 2.31 ms when assuming the backscatter link frequency (BLE) of the tag is 250 kHz and the EPC ID length is 96 bits [10]. By doing the full packet matching, RF-CHORD can achieve $10\log_{10}\frac{2.31}{0.31} = 8.7$ dB integration gain.

We need to generate a noiseless template of the full packet for full packet channel estimation. However, unlike the predefined pilot signal, the template of the packet changes depending on the tag's EPC ID. Collecting EPC ID and timestamp from a commercial reader

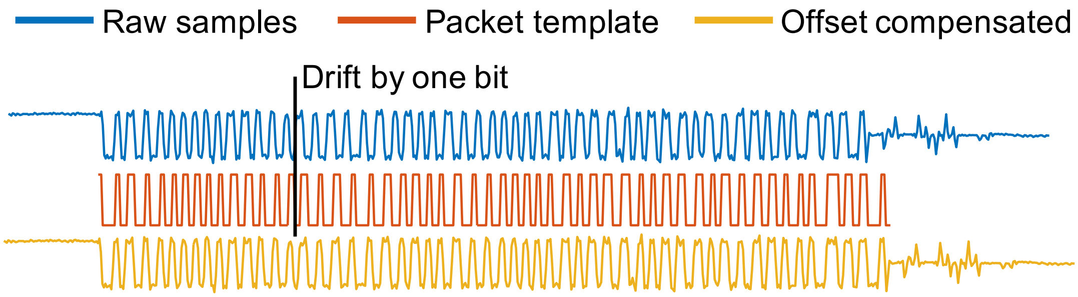


Figure 4.6. The waveforms of the tag signal with clock offset, the reference, and recovery signal from the offset.

device in real-time is unsupported due to the interface limitation: i) the available interface from a commercial reader is usually done by using asynchronous communication, which hinders real-time processing; ii) the timing information is usually not reported by commercial readers. Therefore, RF-CHORD needs to decode the wideband signal into EPC ID independently.

4.4.4 Clock Offset Mitigation

Accurate decoding needs to mitigate the clock offset of the RFID tag signal. Specifically, the protocol tolerates up to ± 10% frequency offset and ± 2.5% frequency fluctuation during backscattering (refer to Tab. 6.9 of [11]). For example, say we read a tag that is 2.5% faster than nominal BLF. For a typical randomized uplink packet of 128 bits with a perfect match at the start of the frame, the received signal will be ahead of the template by one bit at the 32nd bit, and the remaining 96 bits thereafter contribute useless fluctuations to channel estimation, as figured out in Fig. 4.6. RF-CHORD needs to analyze the clock and estimate the offset parameters for mitigation, which can be described by:

$$\tau(t) = \mathrm{Square}((f_{\mathrm{BLF}} - \alpha_0 - \alpha(t))(t - t_0))$$

Where t_0 is the actual start of frame (SOF), α_0 is the initial clock frequency offset (CFO) from prescribed BLF, and $\alpha(t)$ is the fluctuation of the clock. Next, we introduce RF-CHORD's components which estimate these parameters.

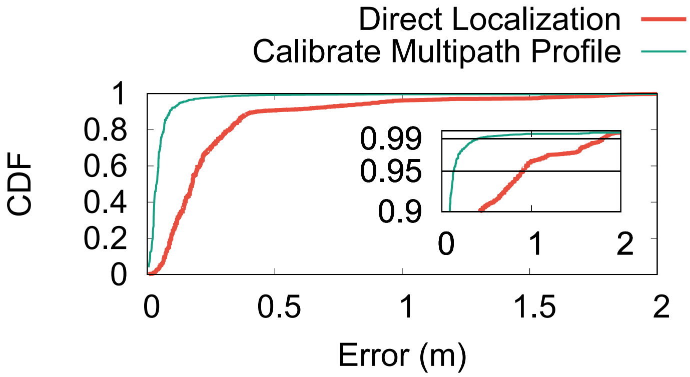


Figure 4.7. Eliminating the multipath effect reduces the 99th long-tail error.

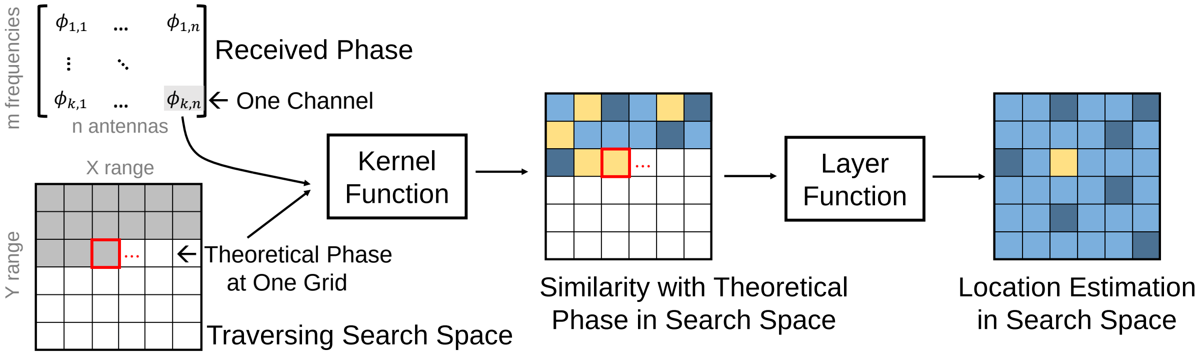

m frequencies
$\phi_{1,1}$ ... $\phi_{1,n}$
$\phi_{k,1}$ ... $\phi_{k,n}$
n antennas
Received Phase
One Channel
X range
Y range
Theoretical Phase
at One Grid
Traversing Search Space
Kernel Function
Similarity with Theoretical Phase in Search Space
Layer Function
Location Estimation in Search Space

Figure 4.8. Kernel-layer framework.

Preamble Matching for t_0 and α_0. RF-Chord first estimates the t_0 and α_0 by adopting a standard sliding window correlator with a known preamble $p(t)$. Specifically, we derive the initial estimation of $\hat{t_0}$ and $\hat{\alpha_0}$ by this correlation calculation, where the $x(t)$ is the received samples, $p_\alpha(t)$ is the reference template tuned to a clock frequency of $f_{\text{BLF}} - \alpha_0$:

$$\{\hat{t_0}, \hat{\alpha_0}\} = \underset{t_0, \alpha_0}{\operatorname{argmax}} \left| \int_0^{T_p} p^*_{\alpha_0}(t) x(t + t_0) \mathrm{d}t \right|$$

PLL to Track $\alpha(t)$ Variation. After eliminating α_0, the clock still has residual offset $\alpha(t)$, which comes from the tag clock fluctuation during the communication and may be significant in the long packet. Because the Miller code of RFID [11] is a self-clocked and modulated bandpass signal, RF-Chord can extract the subcarrier of the line code to track the clock frequency offset accurately. RF-Chord adopts a feedback-based digital Costas PLL [164] to track the clock continuously.

After compensating estimated clock $\tau(t)$, the clock offset is mitigated (the last waveform shown in Fig. 4.6). We can see that the signal is well synchronized with the template.

4.4.5 Decoding with Channel Diversity

After clock offset mitigation, we can decode the full packet, extract the correct template $\hat{I}(t)$, and assemble the decoder. Because the tag baseband signals on all channels are the same, RF-CHORD can apply nulling and beamforming algorithms to utilize the diversity across frequencies and antennas to make a joint decoder. RF-CHORD combines the signals from all channels into one *steered* single-channel signal – it first performs an adaptive maximum signal-to-noise ratio (MSNR) beamforming over the array of each frequency to null the major jammer in the spatial domain and then performs maximum-ratio combining (MRC) beamforming across the frequency domain to improve the SINR further. With this cleaned steered single channel, RF-CHORD exploits a Viterbi decoder to decode the EPC ID. It then applies the EPC ID to make accurate channel estimations on all the channels. A series of efforts introduced in this section, including suppressing external noise, canceling self-interference, matching full packet, mitigating clock offset, and decoding with diverse channels, guarantees RF-CHORD to extract wideband channel estimations at a long distance even with the ultra-low power emission signal.

4.5 Localization with Kernel-Layer Framework

In this section, we first conduct empirical experiments which show: i) multipath is the primary factor that confines the long-tail performance of the RFID localization system once the tag is successfully inventoried; ii) 200 MHz bandwidth is not sufficient to eliminate all the long-tail errors caused by multipath. To address these problems, we propose a kernel-layer framework for localizing RFID tags in the near field. It can suppress long tail errors from multipath by enhancing the direct path and incorporating prior knowledge from logistics.

4.5.1 Long-tail Errors Source Demystification

We conduct a validation experiment to confirm that multipath is the primary source of long-tail localization errors. In this experiment, we put five tags at a distance of 4 m from the reader. We use 16 carriers evenly spaced across 200 MHz bandwidth, 8 antennas, and a hologram-based localization algorithm (see details in Sec. 4.5.2). There is a metallic heater 1.5 m from the tag as the multipath source. Fig. 4.7 shows that the 99th localization error (red line) is 1.798 m, too large to ensure reliable usage in industry settings. The theoretical analysis explains this observation – the 200 MHz bandwidth is only able to differentiate paths that have a propagation distance difference larger than $c/(2B) \approx (3 \times 10^8 \text{ m/s})/(2 \times 200 \text{ MHz}) = 0.75$ m. Once the propagation distance of two paths is smaller than 0.75 m, which is common for many indoor deployments, 200 MHz is insufficient for differentiating one from the other.

Then we evaluate the performance without the multipath effect to check our results double. We keep the experiment setup, conduct RF measurement of a reference tag close to target tags and extract its phase offset from the groundtruth. Considering that the multipath profiles of nearby tags are similar, we subtract each tag's channel estimation with the offset from the reference tag. The 99th localization error of the same set of tags decreases to 0.400 m (green line in Fig. 4.7). It proves that multipath is the primary factor determining the long-tail performance of the RFID localization system, even with 200 MHz bandwidth.

4.5.2 Near-field Localization with Hologram Algorithm

Like most recent RFID localization systems, RF-CHORD locates a tag under the *near-field* condition, which differs from locating a distant target. Considering the Fraunhofer distance [170], a target is at near-field when its distance d from the antenna array meets:

$$d < \frac{2D^2}{\lambda}$$

where D is the aperture of the antenna array, and λ is the signal's wavelength. The wavelength of the 915 MHz signal is around 30 cm. When using an antenna array or SAR, the aperture can easily span to 1 m for adequate spatial resolution. $(2D^2)/(\lambda) = (2 \times 1 \text{ m}^2)/(0.3 \text{ m})$ = 6.7 m and $d < 6.7$ m under most circumstances. Therefore, the response from a tag does not form a plane wave when reaching different elements in the antenna array.

We propose to develop our localization algorithm on top of hologram-based localization framework, which essentially identifies the most likely location as the location estimation, independent of plane wave incidence conditions. In the basic hologram algorithm, the theoretical phase $\theta(g_{(i,j)}, A_k, f_l)$ of a tag at location $g_{(i,j)}$ received by an antenna A_k at frequency f_l can be written as:

$$\theta(g_{(i,j)}, k, l) = \frac{2\pi f_l}{c}(d_{Tx-Tag} + d_{Tag-Rx}) \pmod{2\pi}$$

where d_{Tx-Tag} and d_{Tag-Rx} are the distance between the tag and the transmitter and receiver, respectively. For location $g_{(i,j)}$, its likelihood $P(g_{(i,j)})$ of being the tag's true location can be measured by the similarity between empirically received phase $\phi_{k,l}$ from lth carrier at kth antenna and the theoretically modeled phase $\theta(g_{(i,j)}, k, l)$. The hologram algorithm makes the similarity comparison across multiple antennas and frequencies. $P(g_{(i,j)})$ can be written using the following equation:

$$P(g_{(i,j)}) = \left| \sum_{l=1}^{L} \sum_{k=1}^{K} e^{-j(\phi_{k,l} - \theta(g_{i,j}, k, l))} \right| \tag{4.1}$$

Then we can estimation the location of the tag by choosing (i, j) with maximum P.

4.5.3 Kernel-layer Framework

Beyond the basic hologram algorithm [144], there are many hologram variants [208, 173, 207, 206]. We find that two key factors determine the performance of hologram-based localization algorithms, namely, kernel and layer:

Definition 1. Kernel is the function that measures the similarity between the received signal and the theoretical signal from one channel (*i.e.* single carrier from a single antenna). For example, the $e^{j(\phi-\theta)}$ in Eq. 4.1 is a kernel function that measures the phase similarity with an exponential function.

Definition 2. Layer is a function that determines how to combine kernels from multiple channels (*i.e.* multiple carriers from multiple antennas) and obtain the location estimation. For example, the $\sum_{l=1}^{L}\sum_{k=1}^{K}$ in Eq. 4.1 is a layer function.

We introduce a kernel-layer framework that tells us how kernel and layer affect the localization performance. Fig. 4.8 summarizes our kernel-layer framework, which describes the fundamentals of hologram-based algorithms. This framework can be used following these steps:

- *Model* calculates the theoretical channel information (*e.g.* propagation phase) for each location.
- *Measurement* obtains the empirical channel information (*e.g.* propagation phase and RSSI) by interrogating the tags.
- *Kernel* function profiles the similarity between the theoretical and empirical channel information.
- *Layer* function combines kernel function output from different antennas and frequencies.
- *Output* picks the location with the maximum likelihood as the estimated location.

Different kernels and layers can be combined into various near-field localization algorithms. See more examples in Sec. E.

4.5.4 RF-CHORD's Kernel and Layer

We design our localization algorithm based the kernel-layer framework. When designing RF-CHORD's kernel and layer, we want to reduce the impact of multipath for low long-tail error, which can be achieved with the carefully designed kernel, layer, and prior information from the

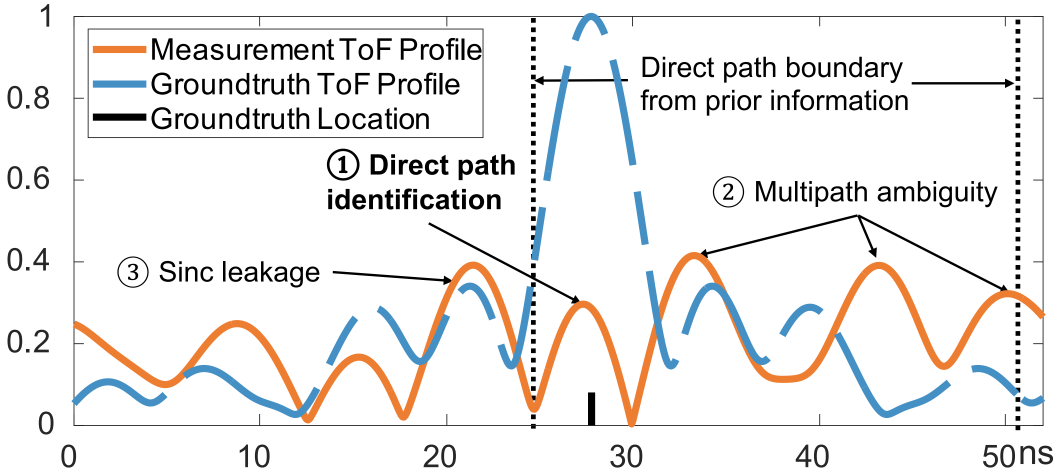


Figure 4.9. Direct path identification with ROI information.

logistic scenario. RF-CHORD's kernel is similar to basic hologram algorithms:

$$\text{RF-CHORD's kernel: } e^{-j(\phi-\theta)}$$

RF-CHORD has 4 layer functions: ToF estimation layer, direct path identification layer, direct path enhancement layer, and summation layer. These layers work together to suppress the multipath and combat long-tail localization errors.

ToF Profile Layer. By using the wideband bandwidth captured, this layer computes the time-of-flight profile of the received signal. The computation follows Eq. 4.2 where ϕ is the empirically measured phase value, f_l is the frequency, and τ is the propagation delay of each path.

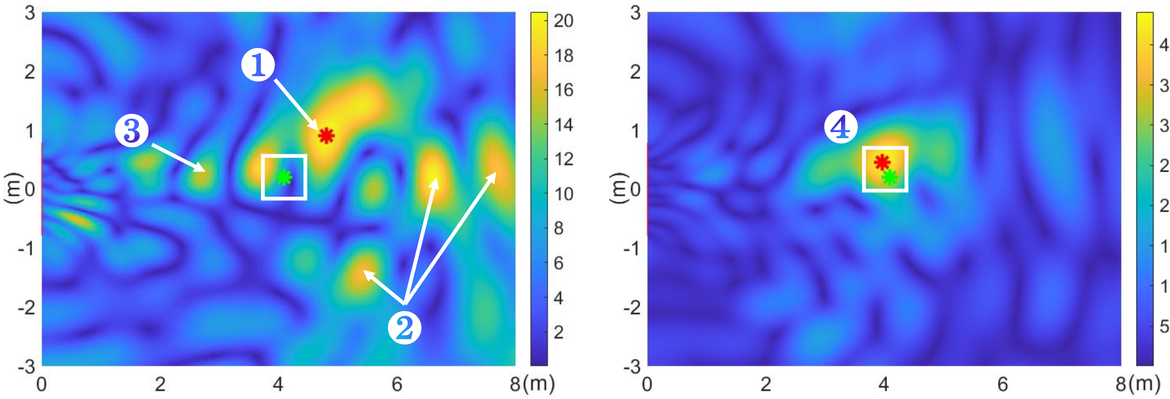
$$\text{ToF estimation layer: } S(\tau) = \sum_{l=0}^{L} e^{-j(\phi_l - 2\pi f_l \tau)} \tag{4.2}$$

Direct Path Identification Layer. It is still challenging to identify the direct path in the ToF profile layer in Fig. 4.9 because there are three interfering factors: ① If the difference is smaller than 0.75 m, we can only observe one mixed peak in the time-of-flight profile of the received signal. ② If the difference is larger than 0.75 m, there will be ambiguity from multipath at the locations farther from the groundtruth. ③ The sample on the frequency domain, which is a sinc function on the time domain, may leak its side lobe and form fake peaks at a nearer location than the groundtruth. To address these problems, RF-CHORD leverages a key observation: prior information. In practical logistic deployment, we can employ the size of the scanning area, the track of tags, *etc.* to help localization. RF-CHORD constructs a layer that leverages this prior information for direct path identification. Fig. 4.9 shows an example of this layer with scanning range [a,b] in meters as prior information, which is common in warehouse deployment. The corresponding algorithm is shown in Alg. 1. In this example, we first compute the bound of the theoretical propagation time in this range $\tau_a = a/(3\times10^8)$ and $\tau_b = b/(3\times10^8)$. The prior information, τ_a and τ_b, acts as a filter that eliminates any multipath with a propagation time smaller than τ_a or larger than τ_b, which helps us identify the right direct path (right peak) rather than nearer one from sinc leakage or farther one from multipath.

Algorithm 1. Direct path identification layer

```
Input: 1. ToF profile: $[S(\tau_1), S(\tau_2), ..., S(\tau_s)]_{1\times s}$
    2. Prior info: scanning area in meters [a,b]
    3. Peak threshold: p
Output: Direct path distance rough estimation $\tilde{d_0}$
    1. $\tilde{d_0}$ = 0, $\tau_a = \frac{a}{3\times10^8}$, $\tau_b = \frac{b}{3\times10^8}$;
    2. L = find $\tau_i$ closest to $\tau_a$ in [$\tau_1$, $\tau_2$, ..., $\tau_s$], return index;
    3. R = find $\tau_i$ closest to $\tau_b$ in $[\tau_1, \tau_2, ..., \tau_s]$ , return index;
    4. $S(\tau) \leftarrow S(\tau)[\mathrm{L:R}]$;
    5. $path \leftarrow S(\tau)[0:\mathrm{end}-1] - S(\tau)[1:\mathrm{end}]$
    for $i \leftarrow 1$ to $s-1$ do
        if $path[i] > 0$ & $path[i-1] < 0$ & $S(i) >$ p then
            $\tilde{d_0} = \tau_i \times 3\times10^8$;
            break;
        end if
    end for
```

Direct Path Enhancement Layer. RF-CHORD uses a across-frequency phase redress algorithm to further enhance the signal quality of the direct path signal. RF-CHORD first identifies potential multipath – if there are multiple peaks (identified by 2D peak find algorithm [12]) in the basic hologram results, the location estimation is likely affected by the multipath effect. Instead of



(a) Basic hologram.

(b) RF-Chord's algorithm.

Figure 4.10. RF-Chord can suppress sinc leakage, multipath ambiguity, and enhance direct path for finer resolution compared to basic hologram algorithms in Eq. 4.1.

using the empirically measured phase ϕ, RF-Chord combines the direct path signal from all frequencies and constructs an enhanced phase $\tilde{\phi}_l$. This process is done by the layer function of Eq. 4.3. See Sec. F for detailed mathematical derivation.

$$\text{Direct path enhancement layer: } \tilde{\phi}_l = \angle \sum_{i=1}^{L} e^{j\phi_i} e^{j\frac{2\pi}{c}(f_i - f_l)\tilde{d}_0} \tag{4.3}$$

Summation Layer. The last layer in RF-Chord is the summation layer, which combines information from all L frequencies and K antennas and computes the likelihood of the tag position. For every location $g_{(i,j)}$, RF-Chord computes the likelihood $P(g_{(i,j)})$ and choose the position with the highest likelihood as the estimated result.

$$\text{Summation layer: } P(g_{(i,j)}) = \left| \sum_{l=0}^{L} \sum_{k=0}^{K} e^{-j(\tilde{\phi_{l,k}} - \theta(g_{(i,j)}, l, k))} \right| \tag{4.4}$$

Putting Everything Together. All above layers and kernel work together as our multipath suppression algorithm. Fig. 4.10 shows an visual example. The heatmaps are the location likelihood with the basic summation layer in Eq. 4.1 (Fig. 4.10a) and with our direct path enhancement algorithm (Fig. 4.10b). The green cross is groundtruth and the red cross is location estimation. If we only use the simple summation layer, there are three factors disturbing the localization accuracy. RF-CHORD handles them with customized kernel-layer algorithm design. The peak of location estimation ① is the superimposed responses from all the paths within distance resolution nearer the direct path. RF-CHORD utilizes coherent summation layer with full 200 MHz bandwidth to increase distance resolution to 0.75 m. The paths with large distance differences from the direct path will generate ambiguity at farther arrival distances as multipath ambiguities ② or even at nearer distance as sinc leakage ③. By using prior information of work range (tags are in different check-in passage with different ranges) to clarify the direct path identification and using direct path enhancement to suppress multipath, we obtain the accurate location estimation ④.

4.6 Implementation

4.6.1 Active Sniffer

Antenna. We chose a recent variant [222] of the Foursquare patch antenna [178], which is metal-backed and of concentric dual-polarization, as our wideband Tx and Rx antennas for its advantages of small-size, low-cost, and high adaptability to surroundings. The original antenna design is for 1.7˜2.7 GHz LTE and we scaled it with HFSS [5] to fit the UHF band 700˜1100 MHz. We also attached each Rx antenna to a 915 MHz bandstop filter [2] to suppress the high-power ISM-band leakage from the commercial reader.

Array. We built the Rx array through a laser-cutting sheet of aluminum. The mounting holes and SMA clearances on the sheet define a 1×8 linear array with element spacing of 21 cm. We set a notable 31.5 cm gap in the middle for a 2:3 co-prime array configuration [183] to suppress the grating lobe. We hang two Txs 0.4 m lower than the receiver's horizontal array along its geometric bisection. The right one was wideband Tx and the left one was ISM-band Tx.

Baseband Processor. One of the key implementation challenges towards one-shot inventory is to convert the 31 Gbps I/Q samples from the A/D to the application processor. We developed high throughput baseband with 2 ADRV9009 [140, 3] RF chips and an XCKU060 FPGA SoM

[28, 24] in charge of 4 receivers over 200 MHz bandwidth for PCIe streaming.

Application Processor. The host is equipped with a Core-i9 9900 CPU and an RTX 3090 GPU for real-time decoding and CSI acquisition. GPU was used to handle the template matching during the decoding with FFT convolution acceleration and parallelism. We used Process Explorer [21] to measure resource utilization and report the results in Tab. 4.2. The decoder is developed with C++/Eigen except that the most compute-intensive part, *i.e.* the full packet matching algorithm, is implemented on GPU with CUFFT [8].

Table 4.2. Hardware resource utilization.

CPU (Utilization)	GPU (Utilization)	I/O Bandwidth	Memory
Core-i9 9900 (16.1%)	RTX 3090 (38.0%)	520.1 MBps	4.1 GB

4.6.2 RFID Tags

In order to ensure compatibility and low-cost, we used a commercial RFID IC Impinj Monza-M4A [20] and implemented a bandwidth extension technique [66] to redesign the metal inlay (antenna) on 80 × 80 mm single-sided PCB. The CAD of the RFID antenna is shown at the top left of Fig. 4.11 and its direction gain (similar to dipole antenna) is shown in Fig. 4.17a. It works on 700˜1000 MHz, whose copper geometry can be transferred to flexible inlay for massive production.

4.7 Evaluation

4.7.1 Experimental Setup

Testing Environment. We evaluate RF-CHORD in an office with multiple reflectors (*e.g.* metal furniture, low ceilings, and walls). The evaluation range is the area of 6 × 3.2 m ahead of the antenna. We divide the evaluation space into 20 cm grids and use guide rails to move the tags. All the tags are facing the array. The dataset containing about 20k wideband RFID channel

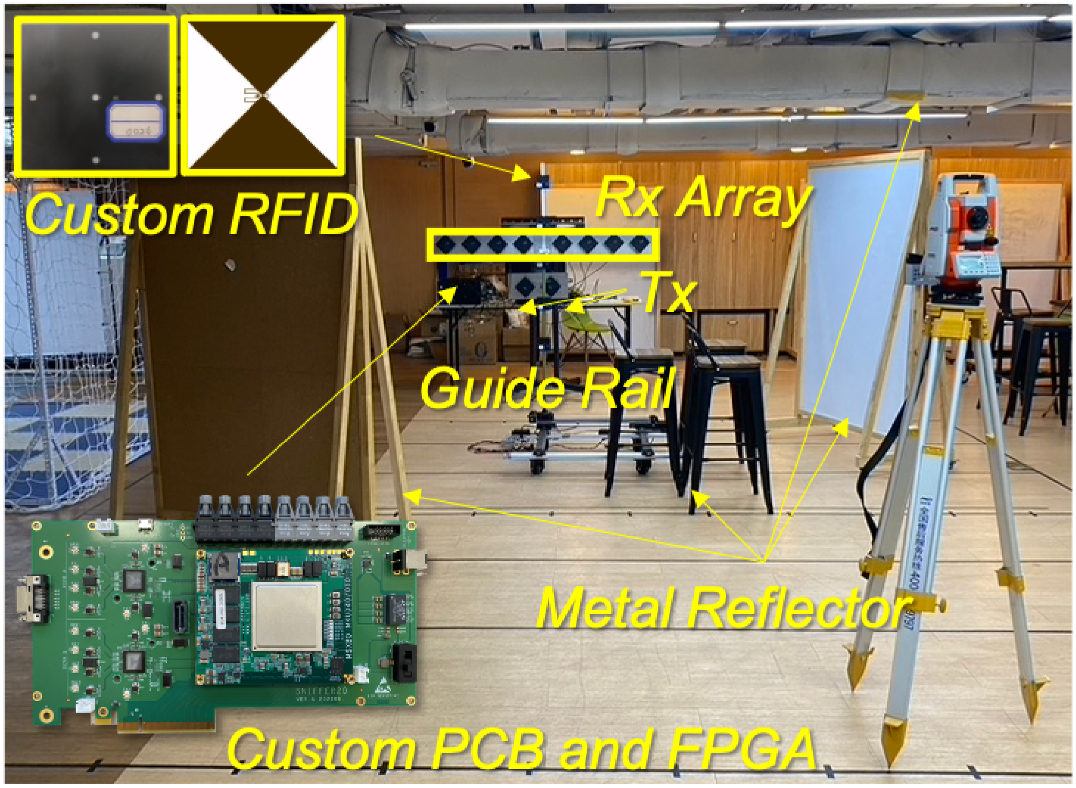


Figure 4.11. Experimental setup for evaluating performance. Five tags are mounted on the rail and ˜20k tag responses are collected in 384 locations.

information measurements at 384 locations is open-sourced at [26]. The setup is shown in Fig. 4.11.

Location Groundtruth. Groundtruth is measured from a total station theodolite (TST) [25] with a 2 mm/2″ accuracy.

Frequency Band Configuration of Active Sniffer. We use the band of 787˜987 MHz and avoid selecting carriers in ISM band 902˜928 MHz. The carriers are almost evenly selected with spacing of 11.1 MHz[3]. The spectrum analyzer shows the inter-modulation distortion of carriers is very little.

ISM-band Reader. We use an Impinj R700 [16] as the ISM-band reader, which is configured on

[3] The frequency set of carriers is {787.1, 798.2, 809.3, 820.4, 831.5, 842.6, 853.7, 864.8, 875.9, 887.0, 898.1, 942.5, 953.6, 964.7, 975.8, 986.9 MHz}.

“Radio Mode 142” (Miller-4 coding and BLF of 256 kHz) and a single linear-polarized antenna aligned with the wideband Tx. We empirically pick this mode since it balances throughput and range. Other coding methods and BLF can also be adopted with few modifications to our system.

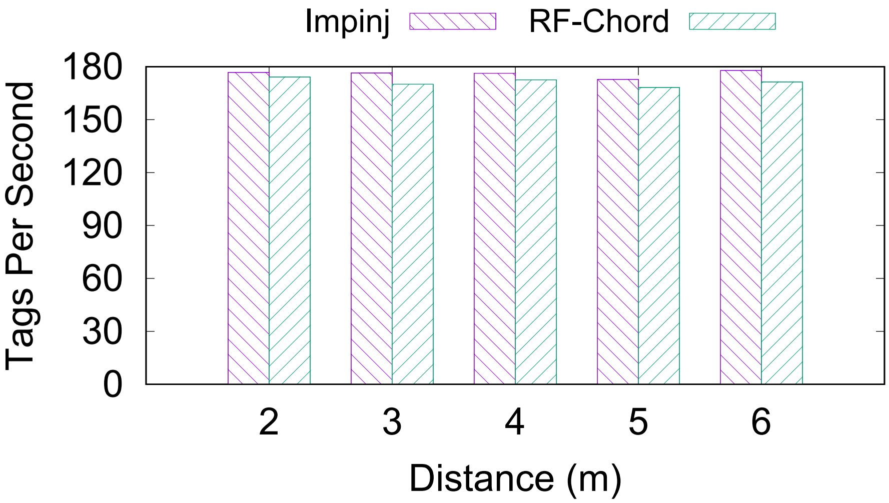


Figure 4.12. Throughput across distances. RF-CHORD can localize around 180 tags/s with -15 dBm emission power.

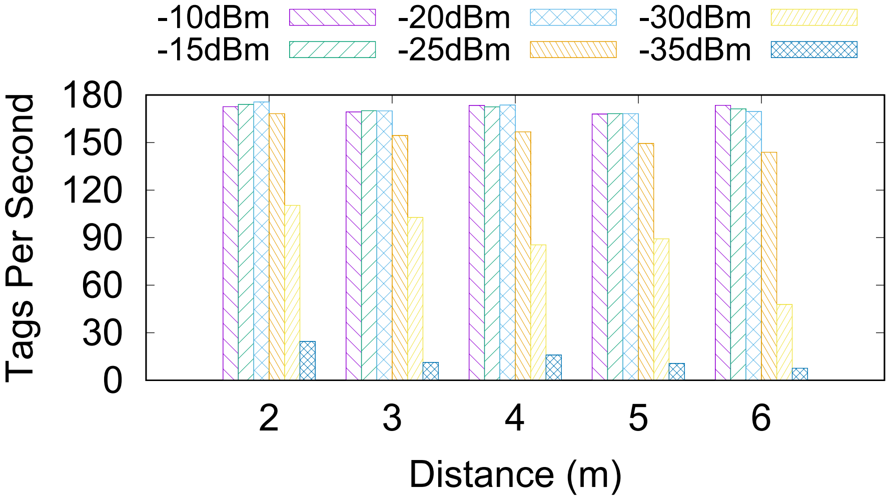


Figure 4.13. Throughput across distances with different emission power. The performance of RF-CHORD is stable with above -25 dBm emission power.

4.7.2 Throughput in One-shot Localization

Fig. 4.12 shows RF-CHORD's throughput at different distance. RF-CHORD can read and localize ~180 tags per second (97% of the tags read by an Impinj reader) at up to 6 m. RF-CHORD is 1000× faster compared to previous sniffer-based wideband systems with frequency-hopping. For instance, RFind [136] needs 6.4 seconds to localize one tag. We also evaluate RF-CHORD's throughput across emission power. Fig. 4.13 shows that RF-CHORD's throughput decreases when we reduce its emission peak power from -15 dBm to -35 dBm. It works fine with an emission power above -25 dBm.

4.7.3 Localization Performance

RF-CHORD utilizes large bandwidth, multiple antennas, and the multipath-suppression algorithm to realize one-shot and high-reliability localization. We conduct microbenchmarks to evaluate how physical resources (frequency and spatial domain), algorithms, and orientation influence the localization.

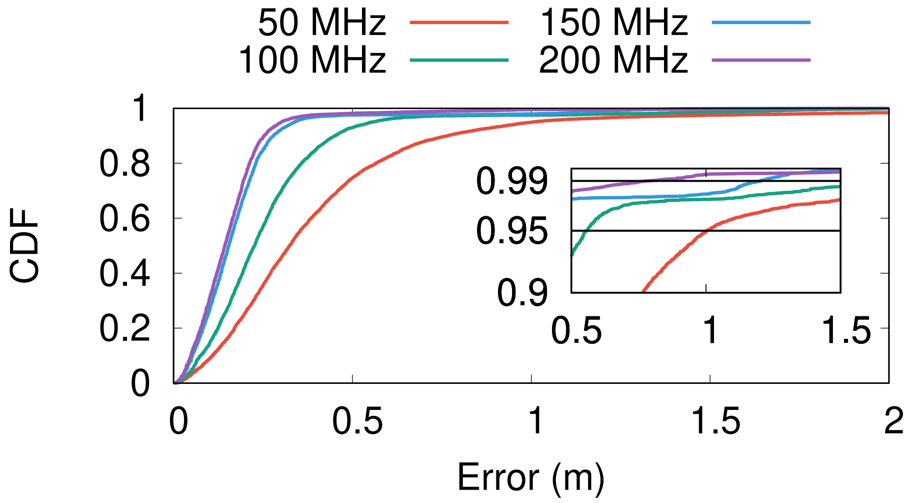


Figure 4.14. RF-CHORD's localization errors with different bandwidths.

Bandwidth. We evaluate the localization performance with 8 antennas and different bandwidths. Fig. 4.14 shows 99th localization errors are 2.398 m, 1.646 m, 1.203 m and 0.786 m with 50

MHz, 100 MHz, 150 MHz and 200 MHz bandwidths. The median errors are 0.325 m, 0.227 m, 0.155 m, and 0.144 m, separately. The results show increasing bandwidth, thus increasing the time resolution, can not only improve the median performance but also reduce the long-tail error. Even when the median performance is close to the upper limit (150 MHz v.s. 200 MHz), the long-tail errors can still be reduced by increasing bandwidth.

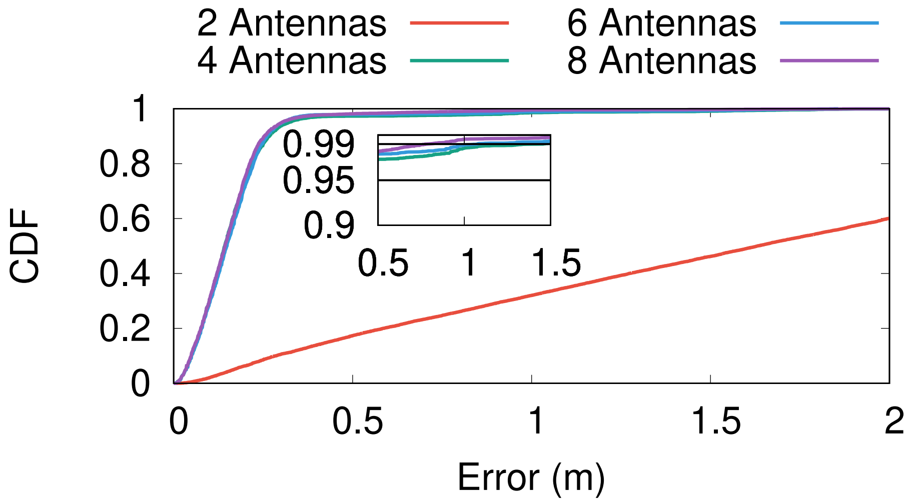


Figure 4.15. RF-CHORD's localization errors with different antenna numbers.

Number of Antennas. We evaluate RF-CHORD's localization performance with 200 MHz bandwidth and different numbers of antennas (thus different array apertures). Fig. 4.15 shows RF-CHORD's 99th localization errors are 4.513 m, 1.467 m, 1.081 m and 0.786 m when 2, 4, 6 and 8 antennas are used. The performance of the 4, 6, and 8 antennas is very similar on median errors (about 0.14 m). However, their long-tail errors are significantly different. The results show increasing the number of antennas (from 2 to 8) can always improve long-tail performance. Increasing the number of antennas/apertures strengthens the system's immunity to interference in specific directions and improves the angular resolution for localization.

Algorithms. We take basic hologram (Eq. 4.1) as the baseline algorithm and evaluate our multipath-suppression algorithm with 8 antennas and 200 MHz bandwidth. Fig. 4.16 shows that 99th localization errors of baseline and RF-CHORD are 1.018 m and 0.786 m respectively.

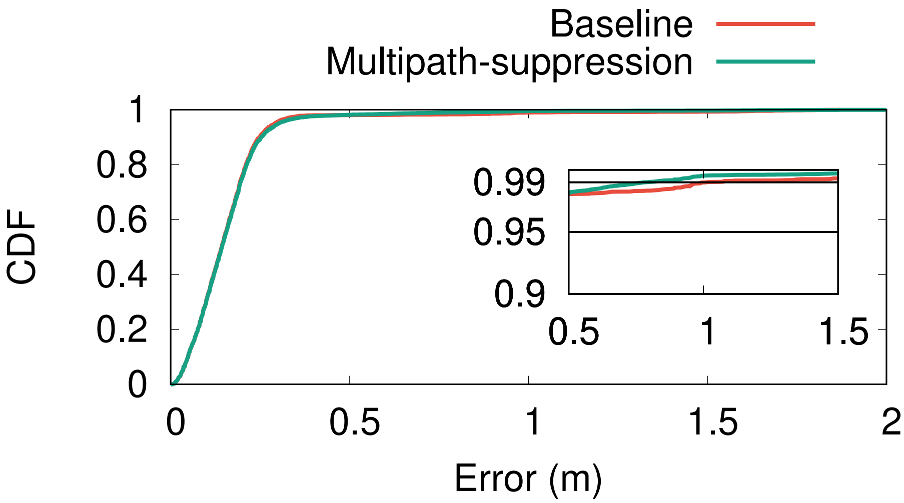
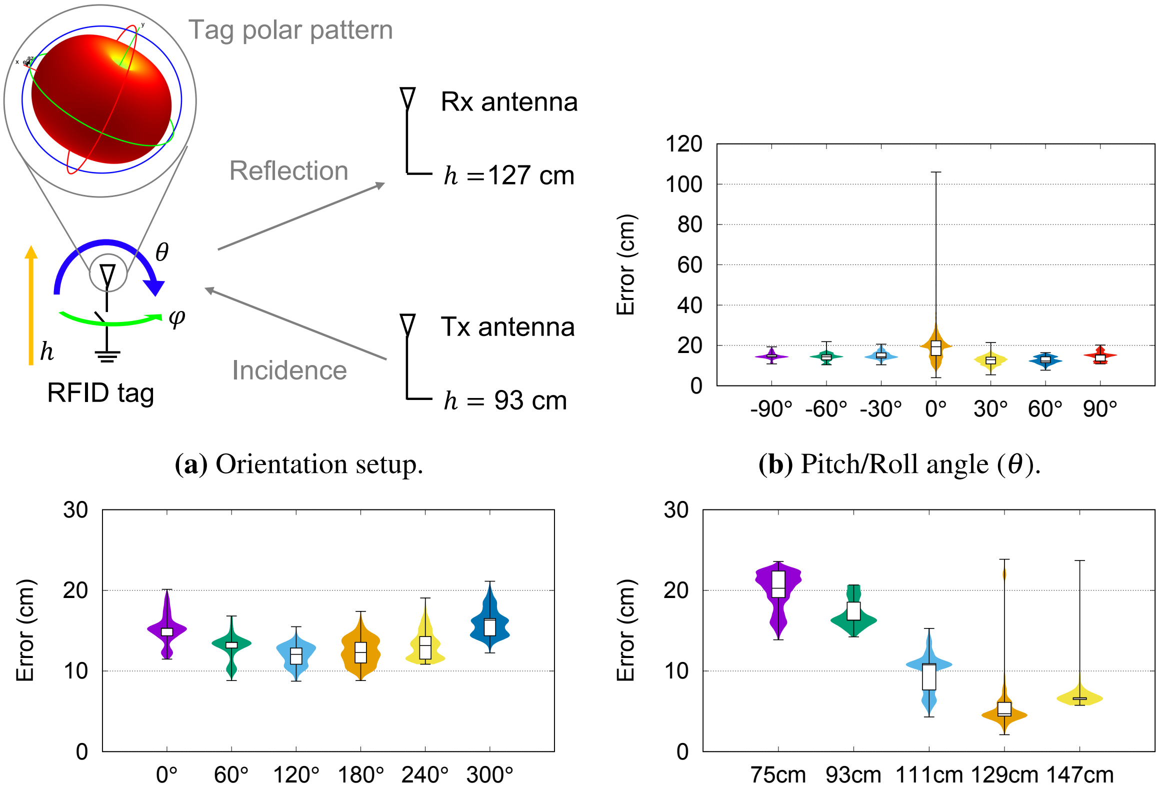


Figure 4.16. RF-CHORD's localization errors with different algorithms.

The median errors of baseline and RF-CHORD are 0.143 m and 0.144 m, respectively. The algorithm effort can improve long-tail performance by handling more corner cases, but hard to improve median performance. Physical resources (*i.e.* the bandwidth and the antenna array aperture) fundamentally limit the algorithm's performance, and the long-tail improvement from the algorithm is primarily attributed to the introduction of prior information – it provides an appropriate carrier for making use of prior information.

Orientation. In practice, the orientation of tags will influence the link angle and polarization, thus introducing SINR and phase changes. We evaluate how orientation influences the localization error. We set the target tag at a 1-m fixed distance to the antenna array to eliminate the influence of the multipath effect. Then, we change the pitch angle θ (as same as the roll angle due to the symmetry), yaw angle ϕ, and height of the tags as shown in Fig. 4.17a for orientation microbenchmark:

- In Fig. 4.17b, we keep $\phi = 0°$ and $h = 111$ cm (at the center between Tx and Rx). The worst performance occurs when the pole of the antenna points to the rx, which rarely happens in practical deployments (to be discussed in Sec. 4.8.1). It is difficult to read tags due to the low SINR, and even if successful, the long-tail error will be more than 1 m.



(a) Orientation setup.

(b) Pitch/Roll angle (θ).

(c) Yaw angle (ϕ).

(d) Height (h).

Figure 4.17. Microbenchmarks with different tag orientations and heights related to the antennas.

- Yaw Angle. In Fig. 4.17c, we keep $\theta = 0°$, $h = 111$ cm and change ϕ from 0° to 300°. The errors at different yaw angles are similar because the directional gain across ϕ is symmetrical. The results show that the yaw angle does not affect long-tail localization error (bounded within 30 cm).

- Height. In Fig. 4.17d, we keep $\theta = 0°, \phi = 0°$ and move the tag from 75 cm to 147 cm. The long-tail errors do not change much across different heights, which shows that height is not the key factor affecting long-tail errors.

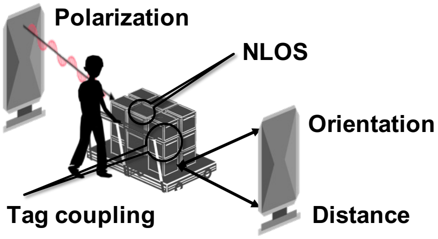


Figure 4.18. The factors affecting signal quality.

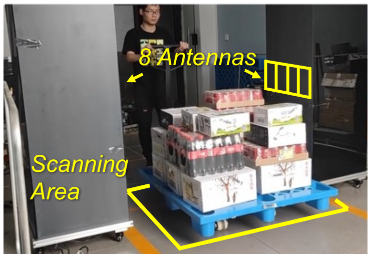


Figure 4.19. Warehouse dock door.

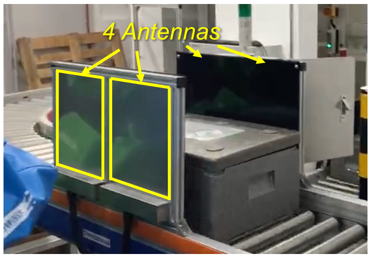


Figure 4.20. Food delivery store.

4.8 Practical Deployment

4.8.1 Deployment Constraints

We summarize the practical factors that influence SINR in Fig. 4.18 and introduce the constraints in real-world logistic scenarios. We also explain how we avoid or utilize them for high-reliability localization.

Orientation. The localization error may be significant if the pitch angle of the tag is closed to 90° according to Sec. 4.7.3. In the deployment shown as Fig. 4.19, the orientation of tags may not be uniform but unlikely to be completely disordered. All the tags are attached to the sides of boxes or crates and then stacked on the pallet. The chaos of stacking and the movement of the pallet may cause yaw angle (ϕ) change but not cause much pitch/roll angle (θ) change, which only introduces negligible localization errors according to Fig. 4.17c.

Polarization. We set the tags and sniffer antennas all vertically polarized, so horizontal tags can not be read. Similar to orientation, no tag will be misplaced in our scene because the pallet stack constraints the crate direction.

NLOS and Tag Coupling. We also stipulate that all the tags should be in the line of sight from one side dock door, which means stacking at most two-column crates on the pallet. It is because the performance of UHF RFID will decrease rapidly with nearby water [38]. This rule excludes severe NLOS occlusion/reflection and severe tag coupling. Most of the pallets in our scenes naturally meet this requirement, and in rare cases, we need to waste some space.

Table 4.3. Reliability performance in practical deployments.

	Miss Reading Rate	Cross Reading Rate
Warehouse	0	0.0025%
Food delivery	0	0.0154%

4.8.2 Real World Deployment

We deployed the full-fledged RF-CHORD (*i.e.* 200 MHz bandwidth and 8 antennas) in the warehouse dock door and lightweight RF-CHORD (*i.e.* 200 MHz bandwidth and 4 antennas) in the fresh food delivery store according to cost and scene conditions for operational evaluation.

Warehouse Deployment. We deploy RF-CHORD in a warehouse to understand its performance in logistic check in and out. RF-CHORD is installed in the dock door of the warehouse as shown in Fig. 4.19. This warehouse's goal is to distribute a large amount of food and daily necessities supplied by the upstream warehouse to city delivery stations. The crates are various and packaged without unified standards. Ideally, RF-CHORD should report all the tags inside of the scanning area and not report any tags outside of the scanning area. Our previous deployment experiments in the same scenario show that commercial read-or-not solution Impinj xSpan [15] has ˜6% miss-reading rate and ˜2% cross-reading rate in the similar scene. We attached over 10,000 tags to various items, mainly plastic crates, also including water bottles, cans, milk boxes, rice, *etc.* The scanning area is 2 × 1 m between the two poles of the dock door (as ROI) and the user walks through the aisle with about 50˜100 tags on a trailer in 1 to 4 seconds. According to Tab. 4.3, RF-CHORD is able to identify tags inside of scanning area with a 100% accuracy (perfectly no miss reading) and 0.0025% cross reading. Therefore, RF-CHORD can provide sufficient localization accuracy in the warehouse deployment, which significantly outperforms the state-of-the-art commercial solutions.

Fresh Food Deliver Store Deployment. As shown in Fig. 4.20, we also deploy lightweight RF-CHORD in a fresh food delivery store where fresh food is packaged into a container and transported via a moving belt. Once the RFID tag on the container is scanned, the delivery personnel will be allocated to pick it up. RF-CHORD needs to ensure all the containers on the moving belt are scanned and do not scan any tag outside of the moving belt. Tab. 4.3 shows that the miss-reading rate of RF-CHORD is 0%, and cross-reading rate is 0.0154%. Therefore, RF-CHORD can achieve sufficient accuracy in the fresh food delivery store deployment.

4.9 Discussion

Polarization Mismatch. In our scenarios, the work pipeline guarantees the polarization match. However, in more general scenarios, the polarization may be mismatched when the orientation of tags is disordered. The conventional solution is to use circular polarization antenna [89] or dual-polarization switching [15]. RF-CHORD can be adapted to them conveniently because its wideband four point antenna is inherently dual-polarized. We can plug a polarization switch into each sniffer antenna, which acts synchronously and does not influence throughput and range performance.

Blind Spots. RF-CHORD is free of cross reading, and therefore it can use high transmission power and sensitivity ISM-band reader for achieving nearly zero miss-reading rate. However, miss reading still threatens reliability in certain complex environments. It can be mitigated by switching between antennas or beam patterns [47, 193]. As our Tx is synthesizing multiple tones, it is feasible to add a Tx beamforming array for blind spot suppression.

Integration with Robots. In recent years, logistics robots (*e.g.* automated guided vehicle (AGV) [6], automated storage and retrieval systems (ASRS) [19], and autonomous mobile robots (AMR) [7]) have been developed rapidly to reduce the movements and operations of sorters and improve efficiency. These robots still need to cooperate with a label identification system (*e.g.* barcode or QR code). RF-Chord has the potential to replace such system and cooperate with logistics robots to achieve more efficient automation.

Cost. The ultimate goal of deploying RFID is to reduce manual labor and error while improving efficiency, which requires careful cost accounting. We emphasize that although baseband chips and RF circuits will increase the cost of readers to thousands of dollars, the main cost of RFID-based logistics still comes from RFID tags. Considering a medium warehouse with 10k packages delivered every day, the annual cost of tags is approximately \$0.1 × 10,000 × 365 = \$365,000. Our strategy is not modifying the tag chip because most of the manufacturing cost comes from the chip and the assembly process [179]. Therefore, the wideband tag we designed maintains almost the exact cost as current commercial tags when in massive manufacturing.

4.10 Related Work

Narrowband Localization. There are three main localization approaches to boost accuracy even with the limited time resolution of narrow ISM bandwidth: The first approach is to improve spatial resolution by SAR. Tagoram [208] uses the motion of tags to build multiple virtual antennas, while Mobitagbot [173] exploits antenna motion. The hologram algorithms in these two systems inspired the kernel-layer framework in our paper. Other hologram algorithm variants [206, 207, 215] can also be viewed as different combinations of kernels and layers. However, the assumption of free antennas or tags mobility and lengthy startup time for tracking do not fit the logistic network. The second approach is to acquire prior information by reference tag. PinIt [196] exploits a dense grid of reference tags and determines the nearest reference tag for NLOS localization by dynamic time wrapping. However, reference tags share time slots, which influences the throughput and scalability. The third approach is to increase the number of links by tag array. Attaching more tags to the target can increase the number of links and improve localization performance. Tagyro [205], and RF-Dial [49] utilize the phase difference of the tag array to solve orientation ambiguity and improve localization performance. Trio [71] models the equivalent circuits of coupled tag and uses the tag interference for refined localization. Liu et al. [174] uses spatial-temporal phase profiling for relative RFID localization. These tag array based localization approaches are accurate but may be error-prone in a complex environment. Unlike these proposals, RF-CHORD is a sniffer-based wideband localization system that improves time resolution for fundamental performance enhancement.

Wideband Localization. Wideband RFID localization has been proposed to overcome the time resolution limitation. RFind [136] uses a low-power sniffer antenna by frequency hopping to collect the narrow sample channel state information across 220 MHz. Turbotrack [131] develops an OFDM-based one-shot wideband channel estimation approach and a Bayesian space-time super-resolution algorithm to achieve fine-grained localization. However, these systems need multiple shots in the channel estimation or the algorithm to converge for fine location estimation, thus very slow startup for localization or tracking. Modifying tags to work on other frequencies (*e.g.* Wi-Fi [108], millimeter-wave [30], UWB [37, 67]) or cross-frequency based approaches (*e.g.* communicate with Wi-Fi [34], communicate at 1.4˜2.4 GHz [133]) are also expected as the solutions for both finer localization and higher throughput, but their tags are not ready for massive manufacturing at low cost due to the complicated RF frontend and control circuits. Inspired by these works, RF-CHORD develops a multisine waveform to realize one-shot localization without modifying the commercial tag chips, resulting in high accuracy with no throughput loss or cost increase.

RFID Reader. Commercial RFID readers [16, 17, 4] have heavily optimized RF analog frontend, decoder, and protocol stack but do not support real-time tag critical information (*i.e.* EPC ID, timestamp) retrieval. There are a series of open-source RFID reader systems. Buettner et al. implemented EPC Gen II downlink stack [50] and the full functional reader [51], respectively. Kimionis et al. implemented a GNU radio-based reader, which supported OOK and noncoherent FSK [110]. However, their energy and edge detection algorithms are too simple to decode applicable code (*e.g.* miller-4 coding). A recent reader designed by Kragas et al. [103] is featured by coherent detection and initial duration deviation search but only supports simple FM0 encoding. There are other research projects featured by multisine waveform [46], parallel sensing support [204], and active transmit leakage cancellation [106]. However, they only focus on specific optimization and do not provide source code. In a nutshell, no out-of-box reader design meets our requirements of high throughput and low decoding threshold, so we develop a wideband reader with a customized RF frontend and decoder while reusing the MAC layer of the commercial reader for slot arrangement and collision handling. It supports our wideband localization with high efficiency, sensitivity, and compatibility.

4.11 Conclusion

We illustrate the three key requirements in reliability, throughput, and range to meet the industry-grade standard of the logistic network, and present RF-CHORD, the first RFID system that considers all these factors from wideband signal and baseband processing to localization algorithm framework development. We believe our real-world empirical results demonstrate that RF-CHORD paves the way for the practical hardware-software methodological solution of RFID localization-based logistic network and makes an important step towards large-scale operational deployment.

4.12 Acknowledgements

This chapter contains material from “RF-Chord: Towards Deployable RFID Localization System for Logistic Networks”, by Bo Liang, Purui Wang, Renjie Zhao, Pengyu Zhang, Xinyu Zhang, Hongqiang Harry Liu and Chenren Xu, which appears in the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2023. The dissertation author was the primary investigator and author of this paper.

Chapter 5

Summary and Future Work

The vision of connecting everything in the physical world along with the digital world requires hyperscale IoT networks, consisting of trillions of IoT devices. However, the existing tethered or even battery-powered design is not feasible for IoT at scale due to the unaffordable maintenance cost and environmental hazards. Self-powered battery-free IoT is the ultimate means of attaining hyperscale IoT. With the advances in RFIC fabrication, low-power communication, and wireless energy harvesting, we are now at an important juncture to explore the system-level challenges of battery-free IoT.

5.1 Dissertation Summary

This dissertation explores fundamental factors that limit the communication and sensing reliability of battery-free IoT applications. Based on the thorough understanding of the whole system, from the application down to the analog and digital circuits, we have employed a set of techniques, including hardware design, wireless communication, and operating systems, to significantly improve the reliability of battery-free IoT systems.

We first designed systems that improve the reliability of battery-free IoT communication. In SlimWiFi [218], we proposed a novel simplified active radio architecture that has more robust performance compared to backscatter communication. To address the compatibility problem with the existing wireless infrastructure, we proposed a novel asymmetric communication scheme that enables COTS Wi-Fi devices to directly communicate the simplified active radio. Through a careful codesign of the signal modulation scheme and reverse processing of the Wi-Fi data, SlimWiFi enables existing Wi-Fi access points to modulate/demodulate on-off keying (OOK) waveform sent by an extremely low-power IoT tag. With this measure, SlimWiFi radically simplifies the IoT radio architecture, evading power-hungry components such as data converters and high-stability carrier generators. Through collaboration with RFIC experts, we taped out the integrated chip version of SlimWiFi radio and verified it can perform active data transmission at sub-100 µW power, 3 orders of magnitude lower than standard IoT radios! The final system can achieve a robust communication performance with around 100 kbps goodput up to a range of 50 m.

We further explored the methods to improve the reliability of RFID in logistic network applications. We found the root cause of the reliability issue lies in the UHF signal properties. The high carrier frequency electromagnetic signal will be inevitably blocked by RF-unfriendly items like water/metal containers (which leads to miss-reading) and will experience strong reflections in the indoor environment (which leads to cross-reading). Therefore, we designed a novel system called NFC+ [219] which uses the lower carrier frequency magnetic waves of near-field communication (NFC) systems. Traditional NFC systems work in a very short range, which has hampered their deployment in practice. In contrast, NFC+ is a new NFC reader hardware architecture, leveraging resonance engineering and MIMO techniques to reach commercial NFC tags at a long range. Compared to UHF RFID, NFC+ can reduce the miss-reading rate from 23% to 0.03%, and the cross-reading rate from 42% to 0, for randomly oriented objects within a range of 3 meters. NFC+ works even in RF-adverse settings, e.g., tracking water bottles and objects shielded by metal. NFC+ is in the process of being integrated into Alibaba's latest logistic network for online shopping, grocery delivery and local life services.

Finally, we developed a system that can localize battery-free UHF RFID tags with higher reliability. We found that the existing UHF RFID localization techniques are not reliable enough for industry settings, due to RFID's narrow bandwidth and hence coarse time/distance resolution.

To address the high reliability requirements, we designed a system called RF-CHORD which consists of COTS UHF RFID readers and our own UHF RFID sniffer hardware which can capture the tag signal across multiple antennas and wide bandwidth. We further incorporated FPGA and GPU acceleration to process the signal in real time. Combined with a multipath-suppression algorithm, RF-CHORD can determine whether the tag is in the range of interest with extremely high confidence. It can localize up to 180 tags 6 m away from a reader within 1 second and with a 99th long tail error of 0.786 m. RF-CHORD was demonstrated at Alibaba Apsara Conference 2021 and received lots of interest from the attendees in the supply chain industry.

5.2 Future Work

My previous work has shown the potential of radical system architectures to approach extremely low power without overhauling the existing infrastructure. I would like to continue to explore research problems related to battery-free IoT. Below I describe three research directions I will pursue in the near future.

5.2.1 ULP Joint Communication and Sensing

Joint communication and sensing is a promising technology for 6G that facilitates environment awareness and highly efficient connectivity. To take this vision to the next level, leveraging ULP IoT devices can be an effective approach. In fact, our work on RF-CHORD [119] has demonstrated a method to repurpose existing UHF RFID tags for joint communication and sensing. However, the limited available bandwidth in the UHF band poses a challenge, as the system cannot reliably determine the location when there are multipath scenarios with a path length difference smaller than 0.75 m (the range resolution corresponding to a 200 MHz bandwidth). To overcome this limitation, we need to explore the next generation of RFID technology that utilizes ultra-wideband (UWB) signals, enabling enhanced RFID sensing latency and location resolution. There are two potential directions I would like to investigate further.

The first direction involves sub-µW ultra-wideband backscatter, which can serve as an extension of the UHF RFID standard. This approach would enhance the capabilities of UHF RFID by incorporating UWB functionality, enabling improved sensing and communication capabilities.

The second direction focuses on µW active UWB tags that are compatible with commercially available off-the-shelf (COTS) UWB devices. This approach would involve the development of UWB tags with low power consumption, allowing them to work seamlessly with existing UWB devices.

By exploring these two directions, we aim to push the boundaries of battery-free IoT on sensing latency and location resolution, paving the way for advanced joint communication and sensing capabilities in future wireless systems.

5.2.2 Joint Powering and Clocking

Clocking is expected to be a significant power bottleneck for battery-free IoT applications. While existing commodity and ambient backscatter systems consume relatively low power (around 10s of µW) during modulation, they require a highly accurate clock to generate precise frequency shifts and standard-compliant phase modulation. This necessitates the use of an accurate reference clock, such as a crystal oscillator. For instance, Wi-Fi-compatible backscatter approaches [109, 97, 211, 74] typically require tens of MHz frequency shifts and propose reference clocks of up to 11 MHz [109] or 16 MHz [74]. However, driving a 10s of MHz crystal oscillator can consume more than 100 µW [203], exceeding the power consumption of backscatter modulation itself. Moreover, the need for additional off-chip components complicates the circuitry compared to crystal-less UHF RFID tags, which only consist of a chip and an antenna. This complexity leads to higher costs and poses scalability challenges. In my previous work, such as SlimWiFi, I explored techniques to eliminate the requirement for an accurate clock by enabling asymmetric demodulation. However, this approach resulted in a degradation of communication performance.

An alternative and promising direction that I find intriguing is shifting the generation of the reference clock from the IoT device to the host device. Given that wireless powering offers flexible and stable power sources, we can potentially deliver power and clock simultaneously without introducing an additional link. However, this approach presents several system design challenges that need to be addressed. For example, determining the optimal method for delivering the clock, integrating the functions of power delivery and clocking, and jointly designing the signal to optimize power delivery efficiency and clocking reliability are among the key considerations.

Addressing these challenges will require innovative solutions, including efficient clock delivery mechanisms, integrated power and clocking functionalities, and signal design optimizations. By exploring this direction, we can potentially overcome the power bottleneck associated with clocking in battery-free IoT applications and pave the way for more efficient and scalable systems.

5.2.3 The Internet of Bodies

Recently, computers are beginning to ”walk” inside the human body. The Internet of Bodies (IoB) wirelessly connects such implanted computers and enable a leap forward in health monitoring, disease treatment, new human-machine interaction, etc. I am interested in tackling the new challenge pertaining to this field. Examples include miniaturizing the radio devices without compromising radiation efficiency, combating the high signal loss through tissue, efficiently and safely powering the implanted devices, etc. My experience in ultra-reliable IoT communications (e.g., NFC+) and the neuron monitoring system (it is an ongoing project in the early stage and thus not discussed in this dissertation) has equipped me with the sophisticated skill sets needed for IoB. I will also seek collaboration with other researchers on solving interdisciplinary challenges such as brain-machine interfaces, neuromorphic AI chips for efficient IoB data processing, remote control and powering of implanted micro-robots, etc.

Appendix A

FEC Errors in Asymmetric Demodulation

In this section, we discuss the behavior of BCC and LDPC when decoding a non-Wi-Fi frame which supports our design in Sec. 2.3.4

A.1 BCC

Viterbi algorithm is widely adopted for BCC decoding. To achieve the maximum likelihood decoding, the algorithm searches among all valid codewords $\{C\}$, to identify the codeword C^l which has the shortest Hamming distance with the input bit sequence. It then outputs the decoded bit sequence Y which can generate the codeword C^l by performing BCC encoding. This means that when we use the decoded bits Y to get the regenerated bits, the regenerated bits $X' = C^l$ will be the exact codeword that has the shortest hamming distance with the original bit sequence X. Since the demodulated bit sequence X has a very low chance to be the same as a valid codeword, the mismatch between X' and X is almost inevitable. However, we found that the number of mismatches between regenerated bit sequence X' and demodulated bit sequence X has an upper limit. Here we provide a quick proof.

For the BCC code with the basic coding rate 1/2, the codewords are generated by bitwise XOR in Eq. A.1 where $d[k]$ is the k-th input data bit and $c_1[k]$ and $c_2[k]$ are the corresponding bits in the codeword.

$$\begin{aligned} c_1[k] &= d[k] \oplus d[k-2] \oplus d[k-3] \oplus d[k-5] \oplus d[k-6] \\ c_2[k] &= d[k] \oplus d[k-1] \oplus d[k-2] \oplus d[k-3] \oplus d[k-6] \end{aligned} \tag{A.1}$$

Consider a data sequence $D = \{d[1], d[2], ..., d[K]\}$ where K is the length of the input sequence. The corresponding codeword will be $C = \{c_1[1], c_2[1], \cdot, c_1[K], c_2[K]\}$. For one valid codeword C^l generated by D^l, the bitwise inverted version (complementary codeword) $\bar{C}^l = C^l \oplus 1$ will also be a valid codeword whose corresponding data bits is $\bar{D}^l = D^l \oplus 1$. When we get the regenerated bit sequence $X' = C^l$, if the mismatch number between X' and X is more than 1/2 of the total bit number, the mismatch number between $\bar{C}^l$ and X will be smaller than 1/2 of the total bit number. Therefore, the hamming distance between X' and X will be higher than $\bar{C}^l$ and X, which is against the shortest hamming distance principle of the decoder. Therefore, the number of mismatches between regenerated bit sequence X' and demodulated bit sequence X should be lower than 1/2 of the total bit number. Fig. A.1 gives an example that illustrates the proof.

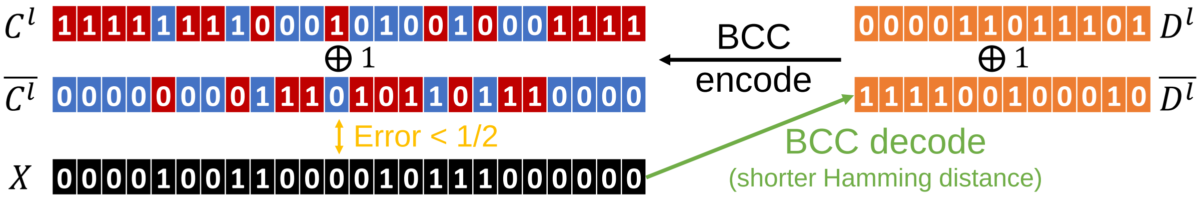


Figure A.1. An example of the BCC decoding with complementary codewords at 1/2 coding rate.

For a higher coding rate, the codeword is generated by puncturing the codeword generated by the basic coding rate. Fig. A.2 provides an example of how the puncturing is conducted with a 3/4 coding rate while processing the same sequence in Fig. A.1. So the proof still holds, but only for the depunctured sequence. Therefore, to reduce the number of mismatches, we should choose the highest coding rate of 5/6.

In the previous proof, we only explained the BCC decoding with a hard decision and optimal maximum likelihood decoding. In practice, the error number might vary when considering the soft decision and imperfect maximum-likelihood decoder implementation. But the variation

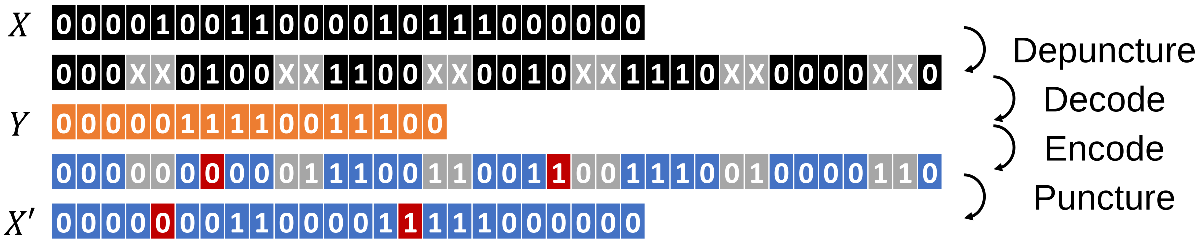


Figure A.2. An example of the BCC decoding and regeneration at 3/4 coding rate.

will not diverge the claim.

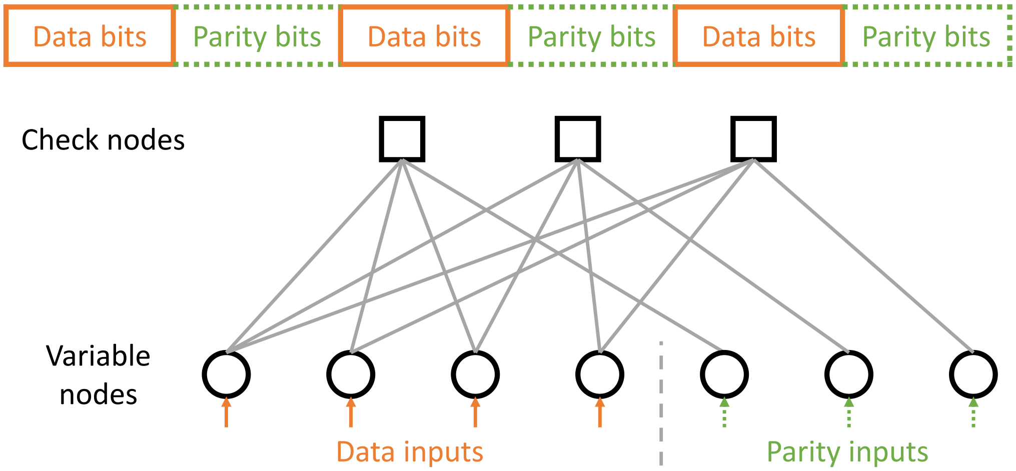


Figure A.3. Bit sequence slicing of LDPC coding and an example connection between data bits and parity bits corresponding to one parity-check matrix.

A.2 LDPC

As illustrated in Fig. A.3, an LDPC-coded bit sequence is organized into blocks. Each block consists of data bits and parity bits. A predefined parity-check matrix characterizes the connection between variable nodes and check nodes. For LDPC decoding, belief propagation decoders based on the message-passing algorithm are widely adopted. For a soft decision decoder, the inputs of the variable nodes are log-likelihood of the corresponding bits instead of quantized bits. The decoder iteratively updates the log-likelihood of the variable nodes and check nodes based on the inputs and the previous status of the nodes by using the sum-product or min-sum algorithm. After iteratively repeating the log-likelihood update, whether the data or parity bits should be flipped will be determined by the final bit log-likelihood of the variable nodes. The bit-flip of the variable nodes happens when the sum of the log-likelihood from the connected check nodes is larger than the input, which in exchange requires that the inputs have a predefined relation corresponding to the parity-check matrix.

Specific to the SlimWiFi asymmetric demodulation, the bit-flip ratio will be extremely low. This is mainly because the inputs are from the OOK signal which does not have the aforementioned relation. Under such conditions, the LDPC decoder is ineffective when decoding, and thus an extremely limited number of the demodulated bits will be falsely “corrected”. A theoretical proof of this conclusion can be found in [125]. Therefore, the data bits part of the regenerated bit sequence will be nearly the same as that of the demodulated bit sequence.

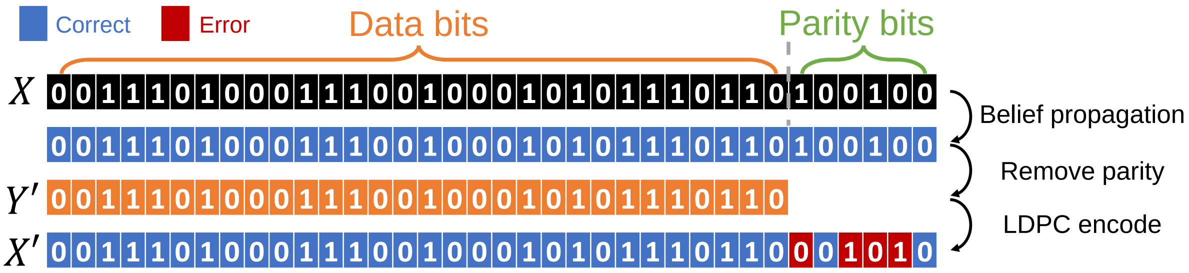


Figure A.4. An example of LDPC decoding procedure and the regenerated bit sequence at 5/6 coding rate.

One thing to note is that even though the parity bits part will not be falsely corrected by the decoder, they will be removed after decoding. Since the original data bits do not have a high correlation with the parity bits, the parity bits part of the regenerate bits are not related to that of the demodulated bits. Thus the parity bits part should be treated as unreliable after the regeneration. Then, all bit errors introduced by decoding will be on the parity bits part as illustrated in Fig. A.4. Therefore, it is preferable for SlimWiFi to reduce the ratio of parity bits which requires a higher coding rate.

Appendix B

Coupling between multiple TX coils

In this section, we discuss the influence of TX coils mutual coupling and how to deal with it.

In the long range NFC communication scenario, the value of TX to tag coupling is pretty small compared to the inter-TX magnetic couplings. Therefore, the influence of the tags to a reader coil's impedance is negligible and the behaviour of TX coils can be simply modeled as:

$$\text{TX Equation:} \quad \vec{v}_T = Z_T \vec{i}_T \tag{B.1}$$

where $\vec{v}_T$ and $\vec{i}_T$ are the TX voltages and currents, Z_T is the TX impedance and inter-TX magnetic couplings.

In the near field, the amplitude and phase of magnetic field is determined by the TX currents $\vec{i}_T$. Therefore, we need to control the amplitude and phase of $\vec{i}_T$ to achieve the magnetic field control as discussed in Sec. 3.5.2. However, in the practical hardware implementation of reader, the supply which we can directly control is $\vec{v}_T$. Since the complex matrix Z_T will introduce phase and amplitude distortion from $\vec{v}_T$ to $\vec{i}_T$, the phase and amplitude in $\vec{v}_T$ will not result in the same phase and amplitude in $\vec{i}_T$.

Theoretically, when we know the value of Z_T, the influence of TX coupling can be compensated by having flexible control on the TX coils input like in [176].

Appendix C

Magnetic beamforming

In this section, we describe the details on how to get Eq. 3.10 from Eq. 3.9. We drop n, $\mathscr{R}$ and β for simplicity. Since the signal we look at is the magnetic signal, it generates an electromotive force on the tag. Following the Faraday's law of induction, the tag's received signal is proportional to the dot product of combined vector $\vec{H}_s$ in Eq. 3.10 and the unit normal vector of tag plane $\vec{e}_\beta$, i.e.:

$$\begin{aligned} R_{tag} =& S_1 a_1 sin(\omega t + \phi_1)(cos\alpha_1 cos\beta + sin\alpha_1 sin\beta) + \\ & S_2 a_2 sin(\omega t + \phi_2)(cos\alpha_2 cos\beta + sin\alpha_2 sin\beta) \\ =& S_1 a_1 cos(\alpha_1 - \beta) sin(\omega t + \phi_1) + \\ & S_2 a_2 cos(\alpha_2 - \beta) sin(\omega t + \phi_2) \end{aligned} \tag{C.1}$$

where S_i is the factor in Faraday's law of induction which is corresponding to the properties of the tag, such as coil size, number of turns etc. Take ϕ_1 as reference and $b_i(n,\mathscr{R},\beta) = S_i k_i A_i cos(\alpha_i - \beta)$, we can get

$$\begin{aligned} R_{tag} =& b_1 sin(\omega t) + b_2 sin(\omega t + \phi_2 - \phi_1) \\ =& \big(b_1 + b_2 cos(\phi_2 - \phi_1)\big) sin\omega t + \big(b_2 sin(\phi_2 - \phi_1)\big) cos\omega t \end{aligned} \tag{C.2}$$

For a signal $xsin\omega t + ycos\omega t$, the power is equal to $x^2 + y^2$. Therefore, we obtain Eq. 3.10 from Eq. C.2.

Appendix D

FCC Compliance

RF-CHORD adopts a 200 MHz bandwidth in the UHF band, much wider than the 902˜928 MHz ISM band. We need to reduce the power of the signal emitted in the licensed band to follow the FCC regulation [27]. Similar operations exist in other systems, such as RFind [136]. RFind adopts a duty-cycled single-tone signal with a peak power of -3 dBm and average power of -13.3 dBm. However, due to the throughput requirement of the localization, RF-CHORD's sniffer should always be ready to localize a tag, which means duty cycling is unacceptable. Therefore, RF-CHORD adopts a hard limit of -15 dBm per tone and can be even lower with similar performance. One may concern that the multiple carrier operation will not be the same as RFind [136] since the total bandwidth is larger than the 0.25% bandwidth limitation in FCC 15.231 (c) [1]. However, RF-CHORD can adopt the alternative method mentioned in [23], which calculates the total bandwidth by summing the individual occupied bandwidths of each carrier frequency. Since we did not apply any modulation to the carriers, the sum of respective bandwidths will be extremely small, which can comply with the FCC regulation. Other modulated waveforms (*e.g.* OFDM) cannot follow this alternative method and may potentially violate the regulation.

Appendix E

Kernel-layer Combinations for Different Localization Algorithms

Kernel-Layer near-field localization framework supports various localization algorithms because of the flexibility of measuring the similarity between receiving signal and theoretical signal and combining information across channels. For example, traditional ToF and AoA estimation algorithms can be implemented under the near-field condition with different kernels and layers.

Kernel and Layers for ToF Estimation. ToF estimation can be done by choosing the following kernel and layer, where ϕ_l and θ_l are the empirical and theoretical phases at frequency f_l respectively, and d is the distance between tag and reader.

$$\begin{aligned}&\text{Kernel: } e^{-j(\phi_l-\theta_l)} = e^{-j(\phi_l-2\pi f_l d/c)} = e^{-j\phi_l} e^{2\pi f_l \tau}\\&\text{Layer: } \sum_{l=0}^{n} S(\tau) = \sum_{l=0}^{n} e^{-j\phi_l} e^{2\pi f_l \tau}\end{aligned} \tag{E.1}$$

When using the above kernel and layer functions, $S(\tau)$ is the inverse Fourier transformation of the empirically measured phase value $\phi_1, \phi_2, ..., \phi_n$. Therefore, $S(\tau)$ is the time-of-flight expression of the empirically measured phases.

Kernel and Layers for AoA Estimation. Similar to the ToF estimation, we can also design kernel and layer functions to extract angle-of-arrive (AoA) estimation. For the AoA estimation, we can use the following kernel and layer functions, where ϕ_k and θ_k are the empirical and theoretical phases at antenna k, respectively. Δd is the distance between two neighboring antennas.

$$\text{Kernel: } e^{-j(\phi_k-\theta_k)} = e^{-j(\phi_k-2\pi fk\Delta dsin(\psi)/c)}$$
$$\text{Layer: } \sum_{k=1}^{m} S(\psi) = \sum_{k=0}^{m} e^{-j\phi_k}e^{2\pi fk\Delta dsin(\psi)/c} \tag{E.2}$$

$S(\psi)$ measures the similarity of the theoretical signal coming from angle ψ and the empirically measured phase value $\phi_1,\phi_2,...,\phi_m$ received by m antennas. Therefore, correct AoA ψ is identified when $S(\psi)$ is maximized.

The summation layer, which sums up all the channels first by row and then by column, combines all the information for the final result. In this case, it combines near-field ToF and AoA estimations. We can develop more complex algorithms with the kernel-layer framework, such as the multipath-suppression algorithm in our paper.

Appendix F

Direct Path Enhancement

We enhance the direct path and suppress the influence from multipath with a frequency domain algorithm [136]. Assume there are N paths with distances of $d_0, d_1, d_2, \ldots, d_N$, and d_0 is the direct path. The channel h_l of lth carrier can be expressed as:

$$h_l = a_0 e^{-j\frac{2\pi}{c} f_l d_0} + \sum_{i=1}^{N} a_i e^{-j\frac{2\pi}{c} f_l d_i}$$

a_i is the propagation attenuation of the ith path. To simplify the derivation without loss of generality, we assume $a_0 = a_i = 1,\ (i = 1, 2, 3, \ldots)$, and what we measure is the phase of channel response:

$$\phi_l = \angle h_l = \angle \{ e^{-j\frac{2\pi}{c} f_l d_0} + \sum_{i=1}^{N} e^{-j\frac{2\pi}{c} f_l d_i} \}$$

If we have a rough estimation of d_0, called $\tilde{d_0}$, we can use this algorithm to enhance the part of $a_0 e^{-j\frac{2\pi}{c} f_l d_0}$ (direct path) and suppress the part of $\sum_{i=1}^{N} a_i e^{-j\frac{2\pi}{c} f_l d_i}$ (multipaths) for a better location estimation. In more detail, we use the prior knowledge of ROI to help determine the rough estimation of direct path $\tilde{d_0}$ with Alg. 1. Then we enhance the direct path profile and suppress profiles of other paths by Eq. 4.3 because the enhanced phase $\tilde{\phi_l}$ can be written as:

$$
\begin{aligned}
\tilde{\phi}_l &= \angle \sum_{i=1}^{n} e^{j\phi_i} e^{j\frac{2\pi}{c}(f_i - f_l)\tilde{d}_0} \\
&= \angle\{ e^{-j\frac{2\pi}{c} f_l d_0} \sum_{i=1}^{N} e^{j\frac{2\pi}{c}(f_i - f_l)\left(\tilde{d}_0 - d_0\right)} \\
&+ \sum_{i=1}^{N} [e^{-j\frac{2\pi}{c} f_l d_i} \sum_{i=1}^{N} e^{j\frac{2\pi}{c}(f_i - f_l)\left(\tilde{d}_0 - d_i\right)}]\}
\end{aligned}
$$

$\tilde{d_0} \approx d_0$ so $(\tilde{d_0} - d_0)\Delta f/c \ll 1$, and it leads to:

$$\sum_{i=1}^{N} e^{j\frac{2\pi}{c}(i-l)\Delta f\left(\tilde{d_0} - d_0\right)} \approx \sum_{i=1}^{N} 1 = N$$

For multipath whose d_i is different from $\tilde{d_0}$, $\tilde{d_0} - d_i$ is large so

$$\left| \frac{\sum_{i=1}^{N} e^{j\frac{2\pi}{c}(f_i - f_l)\left(\tilde{d_0} - d_i\right)}}{N} \right| \approx \left| \operatorname{sinc}\left[B\left(\tilde{d_0} - d_i\right)/c \right] \right| \ll 1$$

The part of the direct path is much larger than the part of other paths, so the direct path is reinforced. $\tilde{d_0}$ helps to get rid of the leakage interference from multipath, and the following summation layer can make a better estimation of d_0 as the final output. Besides using the prior knowledge, other methods (*e.g.* fingerprinting-based algorithm, Bayesian-based algorithm) can also be used to determine the rough estimation $\tilde{d_0}$, which is beyond the scope of this paper.

Bibliography

[1] 15.231 - periodic operation in the band 40.66-40.70 mhz and above 70 mhz. https://www.law.cornell.edu/cfr/text/47/15.231.

[2] 902-928 Cavity Band Rejection Filter WT-A3678-R10. https://www.wtmicrowave.com/en/product/WT-A3678-R10.html.

[3] Adrv9009. https://www.analog.com/en/products/adrv9009.html.

[4] Alien alr-9900+. https://www.alientechnology.com/products/files-2/alr-9900/.

[5] Ansys hfss. https://www.ansys.com/products/electronics/ansys-hfss.

[6] Automated guided vehicle. https://en.wikipedia.org/wiki/Automated_guided_vehicle.

[7] Autonomous mobile robot technology and use cases. https://www.intel.com/content/www/us/en/robotics/autonomous-mobile-robots/overview.html.

[8] Cufft library. https://docs.nvidia.com/cuda/cufft/index.html.

[9] Developing a uhf rfid reader rf front end with an analog devices solution. https://www.analog.com/en/technical-articles/developing-a-uhf-rfid-reader-rf-front-end-with-an-analog-devices-solution.html.

[10] Dogbone monza r6. https://rfid.averydennison.com/content/dam/rfid/en/products/rfid-products/data-sheets/datasheet-Dogbone-Monza-R6.pdf.

[11] Epc(tm) rfid class-1 gen-2 protocol. https://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_2_0-standard-20080511.pdf.

[12] Fast 2d peak finder. https://www.mathworks.com/matlabcentral/fileexchange/37388-fast-2d-peak-finder.

[13] Global parcel volumes expected to double by 2026 on e-commerce boom. https://rogistics.net/global-parcel-volumes-on-course-to-double-by-2026/.

[14] Hmc7044. https://www.analog.com/en/products/hmc7044.html.

[15] Impinj dual-polarized xspan rfid reader. https://support.impinj.com/hc/article_attachments/360002045159/xSpan_Overview_Datasheet_including_Software_Tools_Accessories_and_Specifications_20190405.pdf.

[16] Impinj r700 rain rfid reader for enterprise-grade iot solutions. https://www.impinj.com/products/readers/impinj-r700.

[17] Impinj speedway rain rfid readers for flexible solution development. https://www.impinj.com/products/readers/impinj-speedway.

[18] Inside an amazon robotic sortation center: How automation is changing the 'middle mile'. https://www.geekwire.com/2022/inside-an-amazon-robotic-sortation-center-how-automation-is-changing-the-middle-mile/.

[19] Maximize warehouse storage with as/rs. https://www.bastiansolutions.com/solutions/technology/asrs/.

[20] Monza 4 datasheet. https://support.impinj.com/hc/en-us/articles/202756908-Monza-4-Datasheet.

[21] Process-explorer. https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer.

[22] Quantization noise: An expanded derivation of the equation, snr = 6.02 n + 1.76 db. https://www.analog.com/media/en/training-seminars/tutorials/MT-229.pdf.

[23] Section 15.231, operating on multiple carrier frequencies. https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=41685&switch=P.

[24] Third party xcku060 som (in chinese). https://detail.tmall.com/item.htm?id=654943824333.

[25] Total station instrument tutorial. https://www.aps.anl.gov/files/APS-Uploads/DET/Detector-Pool/Beamline-Components/Lecia_Optical_Level/Surveying_en.pdf.

[26] Towards deployable rfid localization system for logistics network. https://soar.group/projects/rfid/rfchord/.

[27] Understanding the fcc part 15 regulations for low power, non-licensed transmitters. https://transition.fcc.gov/oet/info/documents/bulletins/oet63/oet63rev.pdf.

[28] Xilinx ultrascale series fpga. https://www.xilinx.com/support/documentation/selection-guides/ultrascale-fpga-product-selection-guide.pdf.

[29] 3GPP. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072.

[30] Ajibayo O Adeyeye, Jimmy Hester, and Manos M Tentzeris. Miniaturized millimeter wave rfid tag for spatial identification and localization in internet of things applications. In *IEEE EuMC*, 2019.

[31] ALFA Network Inc. AWUS036ACM. https://www.alfa.com.tw/products/awus036acm.

[32] Erkan Alpman, Ahmad Khairi, Richard Dorrance, Minyoung Park, V. Srinivasa Somayazulu, Jeffrey R. Foerster, Ashoke Ravi, Jeyanandh Paramesh, and Stefano 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.

[33] Amazon. 2 x 8dBi WiFi RP-SMA Male Antenna 2.4GHz 5.8GHz Dual Band. https://www.amazon.com/Antenna-Pigtail-Wireless-Routers-Repeater/dp/B07R21LN5P/ref=pd_lpo_1?pd_rd_i=B07R21LN5P&psc=1.

[34] Zhenlin An, Qiongzheng Lin, and Lei Yang. Cross-frequency communication: Near-field identification of uhf rfids with wifi! In *ACM MobiCom*, 2018.

[35] Analog Devices. HMC8038. https://www.analog.com/en/products/hmc8038.html.

[36] Analog Devices. LT5534. https://www.analog.com/en/products/lt5534.html.

[37] Daniel Arnitz, Klaus Witrisal, and Ulrich Muehlmann. Multifrequency continuous-wave radar approach to ranging in passive uhf rfid. *IEEE transactions on microwave theory and techniques*, 57(5), 2009.

[38] Supreetha Rao Aroor and Daniel D Deavours. Evaluation of the state of passive uhf rfid: An experimental approach. *IEEE Systems Journal*, 1(2), 2007.

[39] ASUSTeK Computer Inc. RT-AC68U. https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RTAC68U/.

[40] ASUSTeK Computer Inc. RT-AX3000. https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/.

[41] Masoud Babaie, Feng-Wei Kuo, Huan-Neng Ron Chen, Lan-Chou Cho, Chewn-Pu Jou, Fu-Lung Hsueh, Mina Shahmohammadi, and Robert Bogdan Staszewski. A fully integrated bluetooth low-energy transmitter in 28 nm cmos with 36% system efficiency at 3 dbm. *IEEE Journal of Solid-State Circuits*, 51(7):1547–1565, 2016.

[42] Torikul Islam Badal, Mamun Bin Ibne Reaz, Mohammad Arif Sobhan Bhuiyan, and Noorfazila Kamal. Cmos transmitters for 2.4-ghz rf devices: Design architectures of the 2.4-ghz cmos transmitter for rf devices. *IEEE Microwave Magazine*, 20(1), 2019.

[43] Constantine Balanis. *Antenna Theory: Analysis and Design*, chapter 5, pages 235–284. John wiley & sons, 2016.

[44] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. Backfi: High throughput wifi backscatter. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 283–296, New York, NY, USA, 2015. Association for Computing Machinery.

[45] Dinesh Bharadia, Emily McMilin, and Sachin Katti. Full duplex radios. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 375–386, New York, NY, USA, 2013. Association for Computing Machinery.

[46] Alírio J Soares Boaventura and Nuno Borges Carvalho. The design of a high-performance multisine rfid reader. *IEEE Transactions on Microwave Theory and Techniques*, 65(9), 2017.

[47] Carlos Bocanegra, Mohammad A Khojastepour, Mustafa Y Arslan, Eugene Chai, Sampath Rangarajan, and Kaushik R Chowdhury. Rfgo: a seamless self-checkout system for apparel stores using rfid. In *ACM MobiCom*, 2020.

[48] Miodrag Bolic, Majed Rostamian, and Petar M Djuric. Proximity detection with rfid: A step toward the internet of things. *IEEE Pervasive Computing*, 14(2):70–76, 2015.

[49] Yanling Bu, Lei Xie, Yinyin Gong, Chuyu Wang, Lei Yang, Jia Liu, and Sanglu Lu. Rf-dial: An rfid-based 2d human-computer interaction via tag array. In *IEEE INFOCOM*, 2018.

[50] Michael Buettner and David Wetherall. An empirical study of uhf rfid performance. In *ACM MobiCom*, 2008.

[51] Michael Buettner and David Wetherall. A software radio-based uhf rfid reader for phy/mac experimentation. In *IEEE RFID*, 2011.

[52] Mengye Cai, Alireza Asoodeh, Yi Luo, and Shahriar Mirabbasi. An ultralow-power crystal-free batteryless tdd radio for medical implantable applications. *IEEE Transactions on Microwave Theory and Techniques*, 68(11):4875–4885, 2020.

[53] Joaquin J Casanova, Zhen Ning Low, and Jenshan Lin. A loosely coupled planar wireless power system for multiple receivers. *IEEE Transactions on Industrial Electronics*, 56(8):3060–3068, 2009.

[54] Sheng-Kai Chang, Zhi-Ting Tsai, and Kuang-Wei Cheng. A 250 khz resistive frequency-locked on-chip oscillator with 24.7 ppm/°c temperature stability and 2.73 ppm long-term stability. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–4, 2020.

[55] Shih-En Chen, Chin-Lung Yang, and Kuang-Wei Cheng. A 4.5 μw 2.4 ghz wake-up receiver based on complementary current-reuse rf detector. pages 1214–1217, 2015.

[56] Xing Chen, Jacob Breiholz, Farah B. Yahya, Christopher J. Lukas, Hun-Seok Kim, Benton H. Calhoun, and David D. Wentzloff. Analysis and design of an ultra-low-power bluetooth low-energy transmitter with ring oscillator-based adpll and 4 × frequency edge combiner. *IEEE Journal of Solid-State Circuits*, 54(5):1339–1350, 2019.

[57] Kuang-Wei Cheng and Shih-En Chen. An ultralow-power ook/bfsk/dbpsk wake-up receiver based on injection-locked oscillator. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 29(7):1379–1391, 2021.

[58] Zicheng Chi, Yan Li, Yao Yao, and Ting Zhu. Pmc: Parallel multi-protocol communication to heterogeneous iot radios within a single wifi channel. In *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, pages 1–10, 2017.

[59] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. Leveraging ambient lte traffic for ubiquitous passive communication. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 172–185, New York, NY, USA, 2020. Association for Computing Machinery.

[60] Hsun-Wei Cho and Kang G. Shin. Bluefi: Bluetooth over wifi. In *Proceedings of the ACM SIGCOMM Conference*, 2021.

[61] CIA. The World Factbook. https://www.cia.gov/the-world-factbook/countries/world/#communications.

[62] Robert H Clarke, Diana Twede, Jeffrey R Tazelaar, and Kenneth K Boyer. Radio frequency identification (rfid) performance: the effect of tag orientation and package contents. *Packaging Technology and Science: An International Journal*, 19(1):45–54, 2006.

[63] IEEE Standards Coordinating Committee. Ieee standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3khz to 300ghz. *IEEE C95. 1-1991*, 1992.

[64] D-Link. DWA-192. https://us.dlink.com/en/products/dwa-192-ac1900-ultra-wi-fi-usb-adapter.

[65] Daniel D Deavours. Uhf epc tag performance evaluation. *RFID Journal [Online], May*, 2005.

[66] Daniel D Deavours. Analysis and design of wideband passive uhf rfid tags using a circuit model. In *IEEE International Conference on RFID*, 2009.

[67] Nicolo Decarli, Francesco Guidi, and Davide Dardari. Passive uwb rfid for tag localization: Architectures and design. *IEEE Sensors Journal*, 16(5), 2015.

[68] Farzan Dehbashi, Ali Abedi, Tim Brecht, and Omid Abari. Verification: Can wifi backscatter replace rfid? In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2021.

[69] Artem Dementyev, Steve Hodges, Stuart Taylor, and Joshua Smith. Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario. In *2013 IEEE International Wireless Symposium (IWS)*, pages 1–4, 2013.

[70] Digilent. Cmod A7. https://digilent.com/reference/programmable-logic/cmod-a7/start.

[71] Han Ding, Jinsong Han, Chen Qian, Fu Xiao, Ge Wang, Nan Yang, Wei Xi, and Jian Xiao. Trio: Utilizing tag interference for refined localization of passive rfid. In *IEEE INFOCOM*, 2018.

[72] Konstantinos Domdouzis, Bimal Kumar, and Chimay Anumba. Radio-frequency identification (rfid) applications: A brief introduction. *Advanced Engineering Informatics*, 21(4):350–355, 2007.

[73] Frank Dörenberg. My small "magnetic" transmitting loop for 80-20 mtrs. https://www.nonstopsystems.com/radio/frank_radio_antenna_magloop.htm.

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

[75] Ecobee. SmartSensor 2-pack. https://www.ecobee.com/en-us/accessories/smart-temperature-occupancy-sensor/.

[76] Everactive. Why are IoT expectations shrinking? https://cdn.everactive.com/content/uploads/2019/06/17103828/EverActive_Infograph_1.pdf.

[77] Raymond M Fish and Leslie A Geddes. Conduction of electrical current to and through the human body: a review. *Eplasty*, 9, 2009.

[78] Dan Gilmore. Did walmart's failed case tagging program set rfid back or move it forward? Supply Chain Digest, 2017.

[79] Google. Pixel 4. https://store.google.com/product/pixel_4_specs.

[80] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Zihao Yu, and Yunhao Liu. Lego-fi: Transmitter-transparent ctc with cross-demapping. *IEEE Internet of Things Journal*, 8(8):6665–6676, 2021.

[81] Mohammad Hasan. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. https://iot-analytics.com/number-connected-iot-devices/.

[82] Honeywell Home. T9 SMART SENSOR. https://www.honeywellhome.com/us/en/products/air/thermostat-accessories/t9-smart-sensor-rchtsensor-1pk-u/.

[83] Huan Hu, Chung-Ching Lin, and Subhanshu Gupta. A 197.1-μw wireless sensor soc with an energy-efficient analog front-end and a harmonic injection-locked ook tx. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(6):2444–2456, 2021.

[84] Pan Hu, Pengyu Zhang, Mohammad Rostami, and Deepak Ganesan. Braidio: An integrated active-passive radio for mobile devices with asymmetric energy budgets. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, page 384–397, New York, NY, USA, 2016. Association for Computing Machinery.

[85] Xiongchuan Huang, Simonetta Rampu, Xiaoyan Wang, Guido Dolmans, and Harmke 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, 2010.

[86] Hugues Anguelkov. Reverse-engineering Broadcom wireless chipsets. https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html.

[87] Shunta Iguchi, Akira Saito, Kazunori Watanabe, Takayasu Sakurai, and Makoto Takamiya. Design method of class-f power amplifier with output power of $-$ 20 dbm and efficient dual supply voltage transmitter. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(10):2978–2986, 2014.

[88] Impinj. Accurate Inventory Visibility with RAIN RFID. https://www.impinj.com/library/blog/2020-in-2020-accurate-inventory-visibility-with-rain-rfid, 2019.

[89] Impinj Inc. Impinj far-field rfid antenna. https://support.impinj.com/hc/article_attachments/360000841520/ANT-DS-S9028PCxx_Impinj1218.pdf.

[90] Melexis Inc. 13.56 mhz rfid systems and antennas design guide. https://www.limpkin.fr/public/NFC/RFID_antennas.pdf, 2004.

[91] Infineon Technologies. BFP720. https://www.infineon.com/cms/en/product/rf/rf-transistor/low-noise-rf-transistors/bfp720/.

[92] InnoPhase. Talaria TWO Modules. https://innophaseinc.com/talaria-two-modules/.

[93] Sozo Inoue, Daisuke Hagiwara, and Hiroto Yasuura. Systematic error detection for rfid reliability. In *First International Conference on Availability, Reliability and Security (ARES'06)*, pages 7–pp. IEEE, 2006.

[94] Texas Instrument. Antenna design guide for the trf79xxa. http://www.ti.com/lit/an/sloa241b/sloa241b.pdf, February 2018.

[95] Texas Instruments. Trf7970a multiprotocol fully integrated 13.56-mhz rfid and near field communication (nfc) transceiver ic. *Datasheet, SLOS743L–REVISED MARCH*, 2017.

[96] ISO. Iso/iec 15693-2:2006 [iso/iec 15693-2:2006]. https://www.iso.org/standard/39695.html, 2006.

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

[98] Jouya Jadidian and Dina Katabi. Magnetic mimo: How to charge your phone in your pocket. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 495–506, 2014.

[99] Daechul Jeong, Hankyu Lee, Taeyoung Chung, Seokwon Lee, Jaesup Lee, and Bumman Kim. Optimized ultralow-power amplifier for ook transmitter with shaped voltage drive. *IEEE Transactions on Microwave Theory and Techniques*, 64(8):2615–2622, 2016.

[100] Woojae Jeong, Jinhwan Jung, Yuanda Wang, Shuai Wang, Seokwon Yang, Qiben Yan, Yung Yi, and Song Min Kim. Sdr receiver using commodity wifi via physical-layer signal reconstruction. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2020.

[101] Wenchao Jiang, Song Min Kim, Zhijun Li, and Tian He. Achieving receiver-side cross-technology communication with cross-decoding. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, page 639–652, New York, NY, USA, 2018. Association for Computing Machinery.

[102] Wenchao Jiang, Zhimeng Yin, Ruofeng Liu, Zhijun Li, Song Min Kim, and Tian He. Bluebee: A 10,000x faster cross-technology communication via phy emulation. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2017.

[103] Nikos Kargas, Fanis Mavromatis, and Aggelos Bletsas. Fully-coherent reader with commodity sdr for gen2 fm0 and computational rfid. *IEEE Wireless Communications Letters*, 4(6), 2015.

[104] Mohamad Katanbaf, Anthony Weinand, and Vamsi Talla. Simplifying backscatter deployment: Full-Duplex LoRa backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2021.

[105] Randy H. Katz. Cost, price, and price for performance. http://bnrg.eecs.berkeley.edu/~randy/Courses/CS252.S96/Lecture05.pdf, 1996.

[106] Edward A Keehr. A low-cost software-defined uhf rfid reader with active transmit leakage cancellation. In *IEEE RFID*, 2018.

[107] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R. Smith, and David Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, page 607–618, New York, NY, USA, 2014. Association for Computing Machinery.

[108] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. In *ACM SIGCOMM*, 2014.

[109] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. Passive Wi-Fi: Bringing low power to Wi-Fi transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016.

[110] John Kimionis, Aggelos Bletsas, and John N Sahalos. Design and implementation of rfid systems with software defined radio. In *IEEE EUCAP*, 2012.

[111] Steven Kisseleff, Ian F Akyildiz, and W Gerstacker. Beamforming for magnetic induction based wireless power transfer systems with multiple receivers. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2015.

[112] Andre Kurs, Aristeidis Karalis, Robert Moffatt, John D Joannopoulos, Peter Fisher, and Marin Soljačić. Wireless power transfer via strongly coupled magnetic resonances. *science*, 317(5834):83–86, 2007.

[113] LAN/MAN Standards Committee of the IEEE Computer Society. Ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pages 1–4379, 2021.

[114] Byungje Lee, Byeongkwan Kim, Frances J Harackiewicz, Byeonggwi Mun, and Hyunwoo Lee. Nfc antenna design for low-permeability ferromagnetic material. *IEEE Antennas and wireless propagation letters*, 13:59–62, 2014.

[115] Thomas H Lee. *The design of CMOS radio-frequency integrated circuits*. Cambridge university press, 2003.

[116] Gang Li, Daniel Arnitz, Randolf Ebelt, Ulrich Muehlmann, Klaus Witrisal, and Martin Vossiek. Bandwidth dependence of cw ranging to uhf rfid tags in severe multipath environments. In *IEEE RFID*, 2011.

[117] Yan Li, Zicheng Chi, Xin Liu, and Ting 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)*, 2018.

[118] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2017.

[119] Bo Liang, Purui Wang, Renjie Zhao, Heyu Guo, Pengyu Zhang, Junchen Guo, Shunmin Zhu, Hongqiang Harry Liu, Xinyu Zhang, and Chenren Xu. RF-Chord: Towards deployable RFID localization system for logistic networks. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*, pages 1783–1799, Boston, MA, April 2023. USENIX Association.

[120] Chung-Ching Lin, Huan Hu, and Subhanshu Gupta. Improved performance tradeoffs in harmonic injection-locked ulp tx for sub-ghz radios. *IEEE Transactions on Microwave Theory and Techniques*, 69(6):2885–2898, 2021.

[121] Linux Wireless. About mac80211. https://wireless.wiki.kernel.org/en/developers/documentation/mac80211.

[122] Linux Wireless. ath9k spectral scan. https://wireless.wiki.kernel.org/en/users/drivers/ath9k/spectral_scan.

[123] Hanli Liu, Dexian Tang, Zheng Sun, Wei Deng, Huy Cu Ngo, and Kenichi Okada. A sub-mw fractional- N adpll with fom of -246 db for iot applications. *IEEE Journal of Solid-State Circuits*, 53(12):3540–3552, 2018.

[124] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. LTE2B: Time-Domain Cross-Technology Emulation under LTE Constraints. In *Proceedings of the 17th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2019.

[125] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Xfi: Cross-technology iot data collection via commodity wifi. In *IEEE International Conference on Network Protocols (ICNP)*, 2020.

[126] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. Ambient backscatter: Wireless communication out of thin air. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 39–50, New York, NY, USA, 2013. Association for Computing Machinery.

[127] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. Verification and redesign of OFDM backscatter. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2021.

[128] Yao-Hong Liu, Johan Van Den Heuvel, Takashi Kuramochi, Benjamin Busze, Paul Mateman, Vamshi Krishna Chillara, Bindi Wang, Robert Bogdan Staszewski, and Kathleen Philips. An ultra-low power 1.7-2.7 ghz fractional-n sub-sampling digital frequency synthesizer and modulator for iot applications in 40 nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(5), 2017.

[129] Lopez Research LLC. An Introduction to the Internet of Things (IoT). https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

[130] Guangzhou Andea Electronics Technology Co. Ltd. Cots long range nfc reader. http://en.gzandea.com/English/Products/126, 2015.

[131] Zhihong Luo, Qiping Zhang, Yunfei Ma, Manish Singh, and Fadel Adib. 3d backscatter localization for fine-grained robotics. In *USENIX NSDI*, 2019.

[132] Yunfei Ma, Xiaonan Hui, and Edwin C Kan. 3d real-time indoor localization via broadband nonlinear backscatter in passive devices with centimeter precision. In *ACM MobiCom*, 2016.

[133] Yunfei Ma and Edwin Chihchuan Kan. Accurate indoor ranging by broadband harmonic generation in passive nltl backscatter tags. *IEEE transactions on microwave theory and techniques*, 62(5), 2014.

[134] Yunfei Ma, Zhihong Luo, Christoph Steiger, Giovanni Traverso, and Fadel Adib. Enabling deep-tissue networking for miniature medical devices. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pages 417–431, 2018.

[135] Yunfei Ma, Nicholas Selby, and Fadel Adib. Drone relays for battery-free networks. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, pages 335–347, 2017.

[136] Yunfei Ma, Nicholas Selby, and Fadel Adib. Minding the billions: Ultra-wideband localization for deployed rfid tags. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 248–260, 2017.

[137] Paolo Madoglio, Hongtao Xu, Kailash Chandrashekar, Luis Cuellar, Muhammad Faisal, William Yee Li, Hyung Seok Kim, Khoa Minh Nguyen, Yulin Tan, Brent Carlton, Vaibhav Vaidya, Yanjie Wang, Thomas Tetzlaff, Satoshi Suzuki, Amr Fahim, Parmoon Seddighrad, Jianyong Xie, Zhichao Zhang, Divya Shree Vemparala, Ashoke Ravi, Stefano Pellerano, and Yorgos Palaskas. 13.6 a 2.4ghz wlan digital polar transmitter with synthesized digital-to-time converter in 14nm trigate/finfet technology for iot and wearable applications. In *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 226–227, 2017.

[138] Mango Communications. Wireless Open-Access Research Platform (WARP), 2016.

[139] Matthias Schulz, Daniel Wegemer and Matthias Hollick. Nexmon: The C-based Firmware Patching Framework. https://nexmon.org/.

[140] David J McLaurin, Kevin G Gard, Richard P Schubert, Manish J Manglani, Haiyang Zhu, David Alldred, Zhao Li, Steven R Bal, Jianxun Fan, Oliver E Gysel, et al. A highly reconfigurable 65nm cmos rf-to-bits transceiver for full-band multicarrier tdd/fdd 2g/3g/4g/5g macro basestations. In *IEEE ISSCC*, 2018.

[141] Carla R Medeiros, Jorge R Costa, and Carlos A Fernandes. Rfid reader antennas for tag detection in self-confined volumes at uhf. *IEEE Antennas and Propagation Magazine*, 53(2):39–50, 2011.

[142] Patrick P. Mercier, Saurav Bandyopadhyay, Andrew C. Lysaght, Konstantina M. Stankovic, and Anantha P. Chandrakasan. A sub-nw 2.4 ghz transmitter for low data-rate sensing applications. *IEEE Journal of Solid-State Circuits*, 49(7):1463–1474, 2014.

[143] Patrick P. Mercier, Benton H. Calhoun, Po-Han Peter Wang, Anjana Dissanayake, Linsheng Zhang, Drew A. Hall, and Steven M. Bowers. Low-power rf wake-up receivers: Analysis, tradeoffs, and design. *IEEE Open Journal of the Solid-State Circuits Society*, 2:144–164, 2022.

[144] Robert Miesen, Fabian Kirsch, and Martin Vossiek. Holographic localization of passive uhf rfid transponders. In *IEEE RFID*, 2011.

[145] Wojciech Mrozik, Mohammad Ali Rajaeifar, Oliver Heidrich, and Paul Christensen. Environmental impacts, pollution sources and pathways of spent lithium-ion batteries. *Energy & Environmental Science*, 14(12):6099–6121, 2021.

[146] Carl R. Nave. Magnetic field of current loop. http://hyperphysics.phy-astr.gsu.edu/hbase/magnetic/curloo.html#c4.

[147] NETGEAR. AX1800 WiFi Router (RAX20). https://www.netgear.com/home/wifi/routers/rax20/.

[148] Nordic Semiconductor. NCS36510. https://www.onsemi.com/products/wireless-connectivity/wireless-rf-transceivers/ncs36510.

[149] Nordic Semiconductor. nRF5340. https://www.nordicsemi.com/Products/nRF5340.

[150] Amy Nordrum. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated . https://spectrum.ieee.org/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

[151] NXP. Icode. https://www.nxp.com/products/rfid-nfc/nfc-hf/, 2019.

[152] NXP. Nxp and identiv announce breakthrough in nfc tag pricing. https://www.nfcw.com/2019/02/05/361215/nxp-and-identiv-announce-breakthrough-in-nfc-tag-pricing, 2019.

[153] NXP Semiconductors. QN908x. https://www.nxp.com/products/wireless/bluetooth-low-energy/qn908x-ultra-low-power-bluetooth-low-energy-system-on-chip-solution:QN9080.

[154] SeongJin Oh, SungJin Kim, Imran Ali, Truong Thi Kim Nga, DongSoo Lee, YoungGun Pu, Sang-Sun Yoo, Minjae Lee, Keum Cheol Hwang, Youngoo Yang, and Kang-Yoon Lee. A 3.9 mw bluetooth low-energy transmitter using all-digital pll-based direct fsk modulation in 55 nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(9), 2018.

[155] MIT open courseware. Maxwell's equation, electromagnetic waves. https://ocw.mit.edu/courses/physics/8-03sc-physics-iii-vibrations-and-waves-fall-2016/part-ii-electromagnetic-waves/lecture-12/, 2015.

[156] Jagdish Pandey and Brian P. Otis. A sub-100 μ w mics/ism band transmitter based on injection-locking and frequency multiplication. *IEEE Journal of Solid-State Circuits*, 46(5):1049–1058, 2011.

[157] Giuseppe Papotto, Francesco Carrara, Alessandro Finocchiaro, and Giuseppe Palmisano. A 90-nm cmos 5-mbps crystal-less rf-powered transceiver for wireless sensor network nodes. *IEEE Journal of Solid-State Circuits*, 49(2):335–346, 2014.

[158] Parcel Pending. Package Delivery Statistics: A Global Perspective. https://www.parcelpending.com/blog/package-delivery-statistics/, 2018.

[159] Ani Petrosyan. Number of internet and social media users worldwide as of April 2023. https://www.statista.com/statistics/617136/digital-population-worldwide/.

[160] Florian Pfeiffer, Klaus Finkenzeller, and Erwin Biebl. Theoretical limits of iso/iec 14443 type a rfid eavesdropping attacks. In *Smart SysTech 2012; European Conference on Smart Objects, Systems and Technologies*, pages 1–9. VDE, 2012.

[161] John R. Pierce. Physical sources of noise. *Proceedings of the IRE*, 44(5), 1956.

[162] Vidyasagar Potdar, Pedram Hayati, and Elizabeth Chang. Improving rfid read rate reliability by a systematic error detection approach. In *2007 1st Annual RFID Eurasia*, pages 1–5. IEEE, 2007.

[163] Naser Pourmousavian, Feng-Wei Kuo, Teerachot Siriburanon, Masoud Babaie, and Robert Bogdan Staszewski. A 0.5-v 1.6-mw 2.4-ghz fractional-n all-digital pll for bluetooth le with pvt-insensitive tdc using switched-capacitor doubler in 28-nm cmos. *IEEE Journal of Solid-State Circuits*, 53(9):2572–2583, 2018.

[164] John G. Proakis and Masoud Salehi. *Digital communications*. McGraw-Hill., 2008.

[165] Proxmark. Open-Source NFC. https://proxmark.com, 2020.

[166] Melanie R Rieback, Georgi Gaydadjiev, Bruno Crispo, Rutger FH Hofman, and Andrew S Tanenbaum. A platform for rfid security and privacy administration. In *USENIX LISA*, pages 89–102, 2006.

[167] Mohammad Rostami, Xingda Chen, Yuda Feng, Karthikeyan Sundaresan, and Deepak Ganesan. Mixiq: Re-thinking ultra-low power receiver design for next-generation on-body applications. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2021.

[168] Mohammad Rostami, Jeremy Gummeson, Ali Kiaghadi, and Deepak Ganesan. Polymorphic radios: A new design paradigm for ultra-low power communication. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, page 446–460, New York, NY, USA, 2018. Association for Computing Machinery.

[169] Matthias Schulz, Jakob Link, Francesco Gringoli, and Matthias Hollick. Shadow wi-fi: Teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over wi-fi. In *Proceedings of the 16th ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018.

[170] Krishnasamy T Selvan and Ramakrishna Janaswamy. Fraunhofer and fresnel distances: Unified derivation for aperture antennas. *IEEE Antennas and Propagation Magazine*, 59(4), 2017.

[171] SEMTECH. SX1261. https://www.semtech.com/products/wireless-rf/lora-core/sx1261.

[172] Mohsen Shahmohammadi, Matt Chabalko, and Alanson P Sample. High-q, over-coupled tuning for near-field rfid systems. In *2016 IEEE International Conference on RFID (RFID)*, pages 1–8. IEEE, 2016.

[173] Longfei Shangguan and Kyle Jamieson. The design and implementation of a mobile rfid tag sorting robot. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, pages 31–42, 2016.

[174] Longfei Shangguan, Zheng Yang, Alex X Liu, Zimu Zhou, and Yunhao Liu. Relative localization of rfid tags using spatial-temporal phase profiling. In *USENIX NSDI*, 2015.

[175] Kuan-Yueh Shen, Syed Feruz Syed Farooq, Yongping Fan, Khoa Minh Nguyen, Qi Wang, Mark L. Neidengard, Nasser Kurd, and Amr Elshazly. A flexible, low-power analog pll for soc and processors in 14nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(7), 2018.

[176] Lixin Shi, Zachary Kabelac, Dina Katabi, and David Perreault. Wireless power hotspot that charges all of your devices. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pages 2–13, 2015.

[177] Satyajit Sinha. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. https://iot-analytics.com/number-connected-iot-devices/.

[178] Seong-Youp Suh, WL Stutzman, and WA Davis. Low-profile, dual-polarized broadband antennas. In *IEEE Antennas and Propagation Society International Symposium*, volume 2, 2003.

[179] Gitanjali Swamy. Manufacturing cost simulations for low cost rfid. *Available at SSRN 3690073*, 2020.

[180] Nikolay Tal, Yahav Morag, and Yoash Levron. Magnetic induction antenna arrays for mimo and multiple-frequency communication systems. *Progress In Electromagnetics Research*, 75:155–167, 2017.

[181] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), sep 2017.

[182] TamoSoft. CommView for WiFi. https://www.tamos.com/products/commwifi/.

[183] Zhao Tan, Yonina C Eldar, and Arye Nehorai. Direction of arrival estimation using co-prime arrays: A super resolution viewpoint. *IEEE Transactions on Signal Processing*, 62(21), 2014.

[184] Nikola Tesla. Apparatus for transmitting electrical energy., December 1 1914. US Patent 1,119,732.

[185] The Clemson University Vehicular Electronics Laboratory. Inductance Calculator. https://cecas.clemson.edu/cvel/emc/calculators/Inductance_Calculator/circular.html, 2020.

[186] Sunil K Timalsina, Rabin Bhusal, and Sangman Moh. Nfc and its application to mobile payment: Overview and comparison. In *2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012)*, volume 1, pages 203–206. IEEE, 2012.

[187] TSMC. 65nm RF LP Process. https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_65nm.

[188] Lionel Sujay Vailshery. Internet of things (iot) and non-iot active device connections worldwide from 2010 to 2025. https://www.cisco.com/c/dam/global/pt_br/assets/brand/iot/iot/pdfs/introduction_to_iot_november.pdf.

[189] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi. In-body backscatter communication and localization. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pages 132–146, 2018.

[190] Voyantic. Tagformance pro. https://voyantic.com/products/tagformance-pro.

[191] Rudd J.M. Vullers, Rob van Schaijk, Hubregt J. Visser, Julien Penders, and Chris Van Hoof. Energy harvesting for autonomous wireless sensor networks. *IEEE Solid-State Circuits Magazine*, 2(2), 2010.

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

[193] Jingxian Wang, Junbo Zhang, Rajarshi Saha, Haojian Jin, and Swarun Kumar. Pushing the range limits of commercial passive rfids. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pages 301–316, 2019.

[194] Ju Wang, Liqiong Chang, Omid Abari, and Srinivasan Keshav. Are rfid sensing systems ready for the real world? In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, pages 366–377, 2019.

[195] Jue Wang, Haitham Hassanieh, Dina Katabi, and Piotr Indyk. Efficient and reliable low-power backscatter networks. *ACM SIGCOMM Computer Communication Review*, 42(4):61–72, 2012.

[196] Jue Wang and Dina Katabi. Dude, where's my card? rfid positioning that works with multipath and non-line of sight. In *ACM SIGCOMM*, 2013.

[197] Jue Wang, Deepak Vasisht, and Dina Katabi. Rf-idraw: virtual touch screen in the air using rf signals. *ACM SIGCOMM Computer Communication Review*, 44(4):235–246, 2014.

[198] Kejia Wang, Sravya Alluri, Xinyu Zhang, and Vincent W. Leung. A sub-100μw 2ghz ook pa for iot applications. In *IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS)*, 2022.

[199] Po-Han Peter Wang and Patrick P. Mercier. A 4.4µw -92/-90.3dbm sensitivity dual-mode ble/wi-fi wake-up receiver. In *2020 IEEE Symposium on VLSI Circuits*, pages 1–2, 2020.

[200] Po-Han Peter Wang and Patrick P. Mercier. A dual-mode wi-fi/ble wake-up receiver. *IEEE Journal of Solid-State Circuits*, 56(4):1288–1298, 2021.

[201] Po-Han Peter Wang and Patrick P. Mercier. An interference-resilient ble-compatible wake-up receiver employing single-die multi-channel fbar-based filtering and a 4-d wake-up signature. *IEEE Journal of Solid-State Circuits*, 56(2):416–426, 2021.

[202] Po-Han Peter Wang, Chi Zhang, Hongsen Yang, Dinesh Bharadia, and Patrick 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.

[203] Xiaoyang Wang and Patrick P. Mercier. An 11.1nj-start-up 16/20mhz crystal oscillator with multi-path feedforward negative resistance boosting and optional dynamic pulse width injection. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–4, 2020.

[204] Yanwen Wang, Jiannong Cao, and Yuanqing Zheng. Toward a low-cost software-defined uhf rfid system for distributed parallel sensing. *IEEE Internet of Things Journal*, 8(17), 2021.

[205] Teng Wei and Xinyu Zhang. Gyro in the air: tracking 3d orientation of batteryless internet-of-things. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 55–68, 2016.

[206] Huatao Xu, Dong Wang, Run Zhao, and Qian Zhang. Adarf: Adaptive rfid-based indoor localization using deep learning enhanced holography. *ACM IMWUT*, 3(3), 2019.

[207] Huatao Xu, Dong Wang, Run Zhao, and Qian Zhang. Faho: deep learning enhanced holographic localization for rfid tags. In *ACM SenSys*, 2019.

[208] Lei Yang, Yekui Chen, Xiang-Yang Li, Chaowei Xiao, Mo Li, and Yunhao Liu. Tagoram: Real-time tracking of mobile rfid tags to high precision using cots devices. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 237–248, 2014.

[209] Yuxiang Yang, Fu Zhang, Kun Tao, Benjamin Sanchez, He Wen, and Zhaosheng Teng. An improved crest factor minimization algorithm to synthesize multisines with arbitrary spectrum. *Physiological Measurement*, 36(5), 2015.

[210] Gary R Zanzig. Loop antenna with integral tuning capacitor, 1991. US Patent 5,072,233.

[211] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2016.

[212] Pengyu Zhang, Jeremy Gummeson, and Deepak Ganesan. Blink: A high throughput link layer for backscatter communication. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 99–112, 2012.

[213] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. Freerider: Backscatter communication using commodity radios. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT)*, 2017.

[214] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. Enabling practical backscatter communication for on-body sensors. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, page 370–383, New York, NY, USA, 2016. Association for Computing Machinery.

[215] Qingyun Zhang, Leixian Shen, Jiewen Shao, and Fu Xiao. Rf-track: Real-time tracking of rfid tags with stationary antennas. In *ACM TURC*, 2020.

[216] Xuan Zhang and Alyssa B. Apsel. A low-power, process-and- temperature- compensated ring oscillator with addition-based current source. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 58(5):868–878, 2011.

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

[218] Renjie Zhao, Kejia Wang, Kai Zheng, Xinyu Zhang, and Vincent Leung. SlimWiFi: Ultra-Low-Power IoT radio architecture enabled by asymmetric communication. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*, pages 1201–1219, Boston, MA, April 2023. USENIX Association.

[219] Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu, and Ming Zhang. Nfc+: Breaking nfc networking limits through resonance engineering. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM)*, 2020.

[220] Renjie Zhao, Timothy Woodford, Teng Wei, Kun Qian, and Xinyu Zhang. M-Cube: A Millimeter-Wave Massive MIMO Software Radio. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom)*, New York, NY, USA, 2020.

[221] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing 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.

[222] Dong-Ze Zheng and Qing-Xin Chu. A wideband dual-polarized antenna with two independently controllable resonant modes and its array for base-station applications. *IEEE Antennas and Wireless Propagation Letters*, 16, 2017.

[223] Jim Zyren and Al Petrick. Tutorial on Basic Link Budget Analysis. http://www.sss-mag.com/pdf/an9804.pdf.