Cross-Frequency Communication: Near-Field Identification of UHF RFIDs with WiFi!

Zhenlin An, Qiongzheng Lin, Lei Yang
Department of Computing
The Hong Kong Polytechnic University
Kowloon, Hong Kong
{an,lin,young}@tagsys.org

ABSTRACT

Recent advances in Cross-Technology Communication (CTC) have improved efficient cooperation among heterogeneous wireless devices. To date, however, even the most effective CTC systems require these devices to operate in the same ISM band (e.g., 2.4GHz) because of the conventional wisdom that wireless transceivers with different (fundamental) frequencies cannot communicate with one another. Our work, which is called TiFi, challenges this belief by allowing a 2.4GHz WiFi receiver (e.g., a smartphone) to identify UHF RFID tags, which operates at the spectrum between 840 ∼ 920MHz. TiFi does not require changing current smartphones or tags. Instead, it leverages the underlying harmonic backscattering of tags to open a second channel and uses it to communicate with WiFi receivers. We design and implement TiFi with commodity WiFi chipsets (e.g., Broadcom BCM43xx, Murata KM6D280 40, and Qualcomm WCN3990). Our comprehensive evaluation shows that TiFi allows WiFi receivers to identify UHF RFID tags within the range of 2 m and with a median goodput of 95%, which is comparable to today's mobile RFID readers.

CCS CONCEPTS

• **Networks** → **Mobile networks**; **Cyber-physical networks**;

KEYWORDS

Cross-Frequency Communication; Harmonic Backscatter; RFID; WiFi; TiFi

MobiCom '18, October 29-November 2, 2018, New Delhi, India

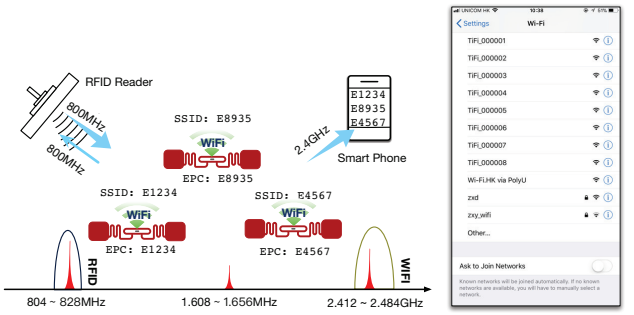
ACM ISBN 978-1-4503-5903-0/18/10…$15.00
https://doi.org/10.1145/3241539.3241569

ACM Reference Format:
Zhenlin An, Qiongzheng Lin, Lei Yang. 2018. Cross-Frequency Communication: Near-Field Identification of UHF RFIDs with WiFi! . In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3241539.3241569

1 INTRODUCTION

As the major enabler of automatic ID technology, Radio-Frequency IDentification (RFID) systems are being increasingly used in everyday scenarios ranging from object tracking, indoor localization [1], and vibration sensing [2], to medical-patient management because of the extremely low cost of commercial RFID tags (e.g., as low as 5 cents per tag). Recent reports show that many industries, such as healthcare and retail, are moving towards deploying RFID systems for object tracking, asset monitoring, and the emerging Internet of Things [3]. A typical UHF RFID system consists of a reader and numerous tags and operates at a frequency band of 840 ∼ 920MHz. The tags are battery-free and harvest energy exclusively from the signals emitted by the reader.

The UHF RFID was once considered as a competitive automatic technology and a replacement of barcode. To date, however, the use of RFID remains limited to a small number of industrial areas (e.g., logistics, warehouses and hospitals, etc) compared with that of the barcode. RFIDs are not widely accepted in the consumer-oriented market mainly because this technology is not supported by currently available personal mobile devices, unlike the barcode, which can be recognized directly by built-in cameras. Consumers have to use special-purpose RFID readers to query tags, and thus, cannot benefit from the convenience provided by their mobile devices. The industry has exerted considerable effort to bridge this gap. For example, Phychips Inc. [4] developed a small reader that can be plugged into a smart phone through its headphone jack. ImpinJ Inc. [5] released a special RFID holder, into which the user can insert his/her smart phone for RFID scanning. Alien Technology integrates WiFi and (or) Bluetooth modules into readers to provide temporary



(a) Architecture (b) iPhone 8 Snapshot

Fig. 1: TiFi architecture. (a) At a high level, TiFi transforms each tag to a WiFi AP, which broadcasts legitimate beacons that regards the tag's EPC as its SSID. Any commercial smart phone could capture and recognize these beacons with a built-in WiFi AP scanner, thereby obtaining these tags' EPCs.; (b) The figure shows a snapshot of the built-in scanner of iPhone 8, which precisely explores our RFID tags. The SSIDs of these tags are in the form of TiFi_XXX.

connection with smartphones. These trade-off solutions (additional details are provided in §2) aim to promote the integration of RFID technology into smart devices. However, they have achieved minimal progress a few years after their introduction because they either introduce extra hardware cost or increase the deployment complexity. Recent Cross-Technology Communication (CTC) systems allow cooperation among heterogeneous wireless devices [6–11] despite their incompatible physical layer modulation. Existing CTCs require these devices, such as Zigbee and Wi-Fi, to operate in the same ISM band (e.g., 2.4GHz). However, the UHF RFID operates at 840 ~ 920MHz of the ISM band, which is far below the spectrum of current mobile devices. Therefore, no existing CTCs can promote the interoperability between RFID and those systems worked in 2.4GHz.

In this work, we introduce a new direction for CTC, named TiFi (i.e., Tag emulated WiFi), which not only operates across protocols but also cross frequency bands. TiFi allows a commercial WiFi receiver (e.g., a mobile phone) to identify the commercial off-the-shelf (COTS) UHF RFID tags in a near field without changing hardware and firmware. Fig. 1 illustrates the usage scenario. At a high level, TiFi turns a tag into a virtual WiFi AP in accordance with the 802.11b protocol. Regarding the Electronic Product Code (EPC) as its service set identifier (SSID), the virtual AP periodically broadcasts *legitimate* WiFi beacons that can be recognized by unmodified WiFi receivers. Consumers can then identify RFIDs using their smartphones in the same way of discovering new APs. In addition, TiFi applies the fact that the near-field signal strength of a tag is hypersensitive to the distance in providing a proximity-based localization service, e.g., Near-Field Communication (NFC) payment.

TiFi allows RFID technology to benefit from the WiFi economies of scale and significantly reduce the barrier of adoption. Thus, TiFi aims to enable new RFID applications. For example, massive assets in a warehouse can automatically broadcast their information to a staff's mobile phone. Consumers can order and pay for snacks in a vending matching by placing their smartphones close to the item they want. People can use smartphones to directly obtain advertisements from the tags embedded in bus stop posters and street signs. However, transforming TiFi into a practical system may be unfeasible because of the following two issues.

- **Cross-Frequency Communication (CFC)**: *How can UHF tags be audible to a WiFi receiver?* The main challenge is the huge frequency gap between RFID and Wi-Fi. We observe that UHF tags resonate the reader's continuous wave (CW) not only at the fundamental frequency (e.g., first at 820MHz) but also at the harmonics (e.g., second at 1.64GHz, third at 2.46GHz) because of the nonlinearity effect of its rectenna. In particular, the absence of nonlinear treatment allows the antennas of RFID tags to radiate the harmonic signals, thereby leading to harmonic backscattering. Unlike the conventional wisdom that considers harmonics as a detrimental 'pollution', TiFi utilizes those around 2.4GHz as a second channel to communicate with WiFi receivers.
- **Cross-Protocol Communication (CPC)**: *How can unnoticed harmonic backscattering carry legitimate WiFi beacons?* Even if the harmonic backscattering is tuned at the WiFi band and is correctly sampled by hardware, a WiFi receiver does not recognize these packets for mismatching WiFi protocol. To transform a tag's packet to a WiFi AP, we craft the reader's continuous wave to simultaneously create RFID Gen2 packets as well as WiFi 802.11b packets, thereby achieving CPC.

Summary of the Results. We implement a prototype of TiFi using Universal Software Radio Peripheral (USRP) N210 software radios and test 7 types of COTS RFID tags. Our evaluation results demonstrate that TiFi allows a commercial WiFi receiver (e.g., a mobile phone) to identify RFID tags within a range of 2m; and presents 50^{th} and 10^{th} goodputs of 93% and 80%, respectively. TiFi performs comparably to the existing commercial mobile RFID reader, and has the additional serviceability to WiFi receivers.

Contributions: The major contributions of this work are presented as follows. First, TiFi leverages RFID tags' harmonic backscattering as a hidden channel to communicate with WiFi receivers. Second, we propose a new CTC technique that allows tags to coexist with WiFi receivers. Finally, this work presents a prototype implementation and evaluation of TiFi to demonstrate its feasibility and effectiveness in a complex environment.

Table 1: Comparison with other techniques[1]

	Cost	CPC	CFC	NFI	Efficiency
HTTP readers	High	Support in APL	Not Support	Not Support	Low
Mobile readers	Median	Support in APL	Not Support	Not Support	Low
Backscatters	High	Support in PHY	Not Support	Not Support	Median
HF-NFC	Median	Not Support	Not Support	Support	High
TiFi	Low	Support in PHY	Support	Support	High

2 MOTIVATION

Existing CTCs fail to work in our scenario for their incompatible CFC. This section thereby mainly examines other potential non-CTC solutions. Our objective is not to complete the list, but to motivate our design.

(a) TSL-1128 (b) ALR-S350 (c) Phychpips

Fig. 2: The solution of mobile reader

Limitations of Mobile Readers: The first type of solutions extends the function of mobile phones to identify UHF RFID tags by using additional accessories. For example, Fig. 2(a) and Figs. 2(b) show two typical mobile readers released from ImpinJ [12] and Alien [13], respectively. The two products function in the similar manner. They can accommodate the user's smart phone through the holder on the top. The user can manipulate the reader through the Bluetooth connection. Fig. 2(c) shows a novel solution from PHYCHIPS [4]. The reader module can be plugged into a smart phone through the headphone jack and manipulated with the acoustic signals. However, these bulky and costly accessories are not appreciated by the current market years after their introduction because of their inconvenience.

Limitations of HTTP Readers: Many industrial grade readers (e.g., ImpinJ R410 [5], Alien ALR-9900+ [14], ThingMagic M6 [15], etc) can provide HTTP web service and work as stand-alone HTTP stations. Mobile phones can access these readers via WiFi or LAN. In general, these readers are usually extremely costly (e.g., thousands of US dollars) because the additional cost is spent for across-network interoperability. For example, the price of ImpinJ R420 is about 2, 200 dollars, which is 4× higher than the non-HTTP reader from ThingMagic USB-6EP [16] (500 dollars). In addition, it is cumbersome for customers to pair its device with a reader in a supermarket especially when a large number of readers are deployed. TiFi allows a user to identify the tagged product instantly when putting its smart device close to the tag.

Limitations of Backscatters: Our work is inspired by a pioneering work (i.e., Passive WiFi [9]), which enables backscatters to emit WiFi signals. Similarly, there are many other backscatters, (e.g., Passive WiFi [9], FM backscatter [17], Ambient backscatter [18], Lora backscatter [19], HitchHike [20], BackFi [21] and Interscatter [22]). TiFi differs from backscatter based solution in three aspects. First, all these backscatters are required to modify the logics of "tags" (i.e., backscatter). TiFi does not have to change but work for commercial RFID tags, billions of which have been deployed around the world. Second, they must operate at the same frequency band with the receivers. Third, TiFi has the unique advantage of dual standard compliance (i.e., WiFi and RFID Gen2).

Limitations of HF-NFC: The near-field identification (NFC) function of TiFi is similar to the HF-NFC that works at 13.56 MHz. Many mobile phones (e.g., iPhone 7/8/x and Samsung Galaxy series) have already integrated an NFC reader for mobile payment. NFC tags are based on inductive coupling instead of electromagnetic signals. Their antennas are made of copper coil that has been turned hundreds of times, and thus, these tags cost nearly 20× UHF tags. Such high cost severely limits the applications of HF RFID. This work aims to supplement the NFC function to UHF RFIDs.

Advantage of TiFi: We summarize the advantages of TiFi over the potential solutions listed in Table 1. In short, TiFi is highly efficient in the physical-layer cross-protocol data exchange without pairing or connection procedure; TiFi provides fine-grained proximity localization, supplementing NFC-similar functions (e.g., mobile payment) to UHF RFIDs; TiFi can enable either non-HTTP or non-WiFi legacy readers to support WiFi communications; particularly, the CFC functionality is a unique feature of TiFi.

3 OVERVIEW

Our design engages with three actors: the reader, tags and mobile device. Only the reader is required to be upgraded. The TiFi reader, which operates in the same manner as RFID system, dominates the entire communication and transmits a persistent CW at approximately 840 MHz. It also performs

[1]The table presents a generalized concept of CPC in which two protocols that can communicate with each other via gateway or directly are considered as CPC. NFI refers to near-field identification, supported by both HF-NFC and TiFi. In particular, the CFC functionality is a unique feature of TiFi.

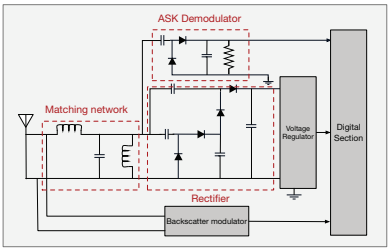


Fig. 3: Simplified RFID tag architecture. The rectenna consists of two or more stages of voltage-doubling rectifier with nonlinearity effect that produces harmonics signals apart from the fundamental.

carrier sense on behalf of the tags and helps coordinate medium access control (MAC) across multiple tags. All communications completely comply with either RFID Gen2 protocol or the WiFi 802.11b protocol. This work considers the most common usage scenario in which tags are attached to the objects in a warehouse or supermarket and covered by readers. Our goal is to provide mobile device with the capability to identify tags by upgrading the readers. Thus, TiFi offers two core techniques:

- **CFC: Entrapping Tags into WiFi Band**. Tags perform backscattering not only at the fundamental frequency but also at harmonics caused by the nonlinearity effect of the tags' rectennas. The first technique (see §4) leverages such underlying physical property to entrap tags into harmonic backscattering within WiFi band to achieve the CFC.
- **CPC: Converting Tags to WiFi APs**. The second technique (see §5) upgrades a reader from physical layer to application layer by modulating its continuous wave. Consequently, the tags backscatter their WiFi beacons periodically and in a timely manner to achieve CPC.

The following sections elaborate the two techniques.

4 CFC: ENTRAPPING TAGS INTO BACKSCATTERING IN WIFI BAND

In this section, we explain how TiFi implements the CFC between tags and a WiFi receiver. A UHF RFID system consists of a reader and multiple tags. The reader continuously generates a high-power continuous wave (CW), from which tags can harvest energy regardless of whether either the reader or the tag is transmitting. Tags will immediately lose the power if they are shielded from the CW even for a while. Reader and tags use ON-OFF keying (OOK) to modulate data.

4.1 Harmonic Backscattering

A passive UHF RFID tag consists of an antenna and an integrated circuit (IC). One of the tasks performed by the IC is the rectification, in which *rectifier* and the *antenna* (i.e., commonly called "rectenna" in literature) convert the alternating current (AC) induced by the CW sent by the reader into a direct current (DC), thereby providing the energy for the other part. Fig. 3 highlights the rectifier section as part of the passive RFID tag architecture. This section contains three common parts: (1) the antenna, (2) the N-stage rectifier circuit, and (3) the antenna-rectifier impedance matching network. In particular, the rectenna is based on a Cockcroft-Walton Circuit that consists of two or more stages of voltage-doubling rectifiers. The nonlinearity effect of these diodes produces *harmonics signals* in addition to the *fundamental signal* [23]. Conventional energy harvesting circuits typically use a harmonic confinement technique to suppress the harmonics and improve their RF-to-DC power conversion efficiency [24]. However, for the commercial interests and usefulness of RFID tags, tag chips and antennas are separately designed and optimized only at the frequency band of UHF RFID. Antenna design begins directly from the knowledge of one impedance value, which is the impedance of the IC at the fundamental frequency described on manufacturer data sheets. The design process then only ensures the matching at the fundamental frequency, and provides *none* treatment for the harmonic currents. Consequently, in accordance with the theory [25] and the measurement [26–28], the *absence* of nonlinear treatment allows the tag antenna to radiate the harmonic signals generated by the rectifier, thereby resulting in *harmonic backcattering*.

Tags can backscatter harmonics when queried with a modulated or unmodulated reader signal. Suppose the input reader's CW is denoted by S. Then, the backscattered signal denoted by S_{out} is given by:

$$S_{\text{out}} = \sum_{k=1}^{\infty} A_k S^k = \overbrace{A_1 S}^{\text{Linear}} + \overbrace{A_2 S^2 + A_3 S^3 + \cdots}^{\text{Nonlinear}} \tag{1}$$

where A_k are the gains of the various components introduced by the rectenna. If the incoming signal S is a sinusoidal signal with frequency f (i.e., fundamental frequency), then it outputs linear component $A_1 S$ with the same frequency f. However, the nonlinearity effect can produce many nonlinear components (i.e., harmonics). In particular, if $S = \cos(2\pi f t)$, then the output signal can be expanded using a trigonometry formula as follows:

$$\begin{aligned} S_{\text{out}} =& A_1 \cos(2\pi t) + A_2 \cos^2(2\pi f t) + A_3 \cos^3(2\pi f t) + \cdots \\ =& \frac{1}{2}A_2 + (A_1 + \frac{3}{4}A_3) \underbrace{\cos(2\pi f t)}_{\text{1st-order}} + \frac{1}{2}A_2 \underbrace{\cos(2\pi (2f) t)}_{\text{2nd-order}} + \\ & \frac{1}{4}A_3 \underbrace{\cos(2\pi (3f) t)}_{\text{3rd-order}} + \cdots \end{aligned} \tag{2}$$

The equation indicates that the frequencies of these harmonics (1st-order, 2nd-order, 3rd-order, $\cdots$) are exactly an

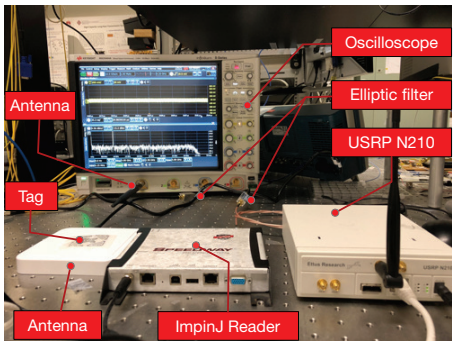


Fig. 4: Experimental setup for the benchmark. A high-definition oscilloscope with 4G bandwidth is used to sniff the backscattered signals.

integral multiple of the fundamental frequency. Imaging that the reader uses an 800MHz carrier, then a tag's backscattering signal will appear mainly at 800MHz, 1.6GHz, 2.4GHz, 3.2GHz, and so on. These backscattered harmonic will not interfere the reader's receiver because creating a filter to reject signals above fundamental frequency is easy. This condition is also another reason why harmonics do not attract considerable attention in RFID systems.

4.2 Feasibility Study

The fundamental idea of TiFi is to modulate the reader's continuous wave, such that the tag can harmonically backscatter at the WiFi band, thereby enabling the cross frequency communication. To investigate the feasibility of this idea, we run an experiment about the harmonic backscattering as below:

Experimental setup. The setup is shown in Fig. 4, where we use a commercial ImpinJ reader (see §6) to perform the continuous reading at 920MHz. The test tag is located at a distance of a few centimeters from the antenna and is oriented towards maximum reception and reradiation. To observe the backscattered harmonics, we use a high-definition Keysight oscilloscope (i.e., MSOS404A) [29] to sniff the backscattered signals. The oscilloscope is equipped with 4GHz bandwidth and up to 20GSa/s sample rate and can produce a power spectral density (PSD) analysis over time-domain communication signals within GHz-level range. In order to prevent the harmonic leakage from the reader's transmitter, we add a *low-pass filter* (see §6).

Results. We first acquire the backscattering spectrum of a `Monza` tag from ImpinJ [5] by using the oscilloscope. The result is presented in Fig. 5, which confirms that the backscattering signals contains numerous harmonics. The low-pass filter cannot attenuate the CW sent from the reader. Thus, the 1st-order signal is extremely stronger than the harmonics. As expected, the harmonics exactly backscatter at the frequencies of integral multiples of the fundamental frequency.

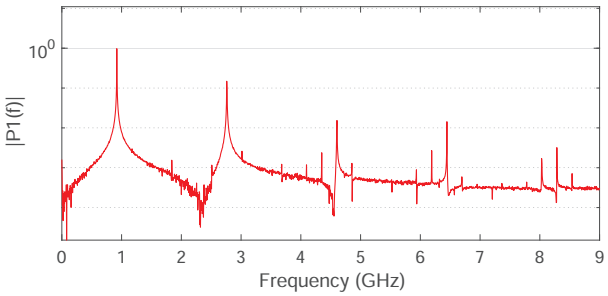


Fig. 5: Spectrum of a tag's backscattering signal. The signal appears at 920 MHz, 2.76 GHz, 4.605 GHz, and 6.445 GHz, when the tag is queried at 920 MHz.

Second, whether the phenomenon is fairly ubiquitous in RFID tags is unclear. Thus, we repeat the aforementioned experiment across seven types of UHF tags, which are the best selling models in current market. We affirmatively observe the similar harmonic backscattering on these tags. Keeping the reader's transmitting power at 30 dBm, Table. 2 lists their power of the first three order signals using the unit of dBm.

4.3 Entrapping Harmonics into WiFi Band

The unavoidable nonlinearity effect results in tags backscattering the third-order harmonic signals at a frequency that is extremely close to the WiFi band. This condition will offer us an opportunity of realizing the cross-frequency communication. WiFi contains in a total of 14 channels with frequencies of 2412MHz, 2417MHz, $\cdots$, and 2484MHz. Each channel has 22MHz band and is spaced 5MHz apart from one another. If we aim to entrap the third-order harmonics into one of these 14 channels, then the reader must operate at the subsequent 14 fundamental frequencies: 803MHz (i.e., 2412/3), 805.6MHz (2417/3), $\cdots$, and 828MHz (2484/3).

Frequency Gap. We investigate the regulated spectrums of UHF RFID systems across 21 countries or areas worldwide. We find that the current legitimate spectrum varies between $840 \sim 928$ MHz. Even the lowest frequency (i.e., 840 MHz used in China) is 12 MHz higher than the highest frequency (i.e., 828 MHz) that we desire. Fortunately, as reported in the work [30], RFID tags are designed to be able to respond in

Table 2: Harmonic Power of Tag Response

#	Manuf.	Model	Size(cm^2)	1st	2nd	3rd
1	`ImpinJ`	QT4	4.8×4.8	-5	-85	-65
2	`ImpinJ`	B45	2×2	-10	-81	-81
3	`Alien`	9640	15.9×1.5	-6	-83	-68
4	`Alien`	9629	2.55×2.55	-6	-84	-72
5	`Alien`	9627	3.2×5	-6	-86	-73
6	`Alien`	9620	3×1.5	-12	-85	-80
7	`Alien`	9610	4.4×1.03	-12	-85	-80

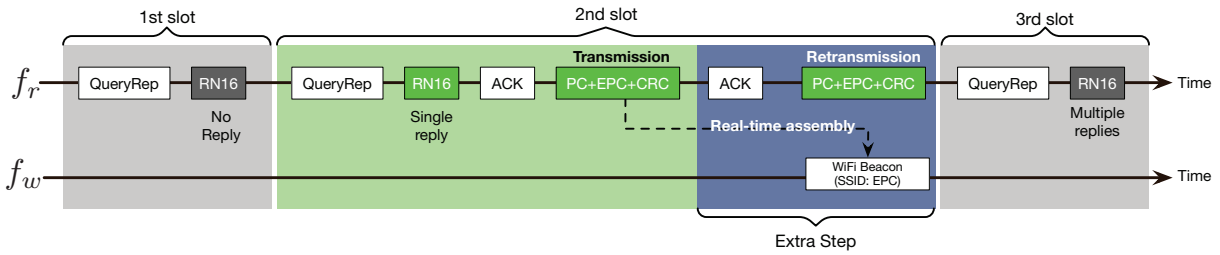


Fig. 6: Illustration of TiFi procedure. This toy example shows three time slots in terms of two frequencies where no tag replies at the first slot, multiple tags reply in the third slot, and a single tag replies in the second slot successfully. The box highlighted in dark blue during the second slot is the extra step (i.e., retransmission) that TiFi inserts into the EPC Gen2 standard procedure.

a wide band (i.e., up to 300 MHz) in order to fit the various specifications although they can only support an extremely narrow communication bandwidth of hundreds of kHz. Our practical experiments confirm this phenomenon. The design of wideband response is reasonable because products with RFID tags are typically transported all around the world and may be queried using a variety of readers, that conform to different regulations.

Dual-Frequency Solution. We adopt a similar dual-frequency solution as proposed in [30] to address the frequency gap. In particular, rather than transmitting a single frequency as common in current RFID protocol, TiFi transmits two single-tone CWs at two frequencies: *primary* frequency f_r (e.g., 840 Mhz which falls within the legitimate UHF RFID band) and *secondary* frequency f_w (e.g., 828 MHz, which is set to one of the 14 frequencies we desire) to decouple RFID and WiFi communications. TiFi uses f_r to power up tags and drive the inventory procedure, and f_w to stimulate tags to reflect WiFi packets. Two frequencies are backscattered by tags respectively. Adopting two frequencies brings an extra benefit: EPC Gen2 protocol requires the reader to hop every hundreds of milliseconds; the hopping of the primary frequency does not affect the WiFi transmission at the secondary frequency at all.

Unlike the solution in [30], which requires two independent transmitters, we notice that our two frequencies get so close (i.e., < 25 MHz for some channels) that a single transmitter is sufficient. For example, the USRP N210 with SBX daughterboard has an instantaneous bandwidth of 40 MHz and the center frequency of current readers can be varied for more than 40 MHz in order to accommodate the differences in regulations on the UHF band across regions and countries [30]. Therefore, despite the use of dual frequencies, TiFi's design will unlikely requires hardware upgrade.

In addition, f_w is outside the legitimate RFID band, its power must be considerably lower than that of f_r to comply with FCC regulations. We refer to [30] for details. This setting will enable the emulated WiFi signals attenuate fast, and thus can be recognized by WiFi receiver in a relatively shorter range, e.g., dozens of centimeters. This setting is exactly what we want for the near-field identification, namely, to control the signals within a small region.

5 CPC: CONVERTING TAGS TO WIFI APS

We cannot control tags or WiFi receivers, so we have to craft the CW at f_w such that WiFi beacons transmitted at f_w are harmonically backscattered by tags to a WiFi channel at $3f_w$. In this process, the reader plays double roles: acting as an RFID reader to transmit RFID commands (e.g., `Query`) and acting as an assistant to generate WiFi packets (e.g., beacons).

5.1 High-Level Procedure

To better understand our design, we illustrate the high-level procedure of TiFi in Fig. 6. TiFi integrates the advertisement of WiFi beacons into the EPC Gen2 protocol seamlessly, by initiating a retransmission after a tag replies its long reply successfully. The beacon is assembled with the `EPC` acquired in the first transmission. TiFi reader transmits the assembled WiFi beacon at the frequency f_w exactly during the retransmission. In this way, the WiFi beacon can be harmonically backscattered by the *right* tag to WiFi receivers. From the high-level, it seems that this tag broadcast its WiFi beacon at 2.4GHz like a normal AP. The following section introduces how the reader integrates two different protocols with this procedure.

5.2 WiFi versus RFID

Although many versions of WiFi protocols are available, our design only targets at an early version, 802.11b, which is far enough to meet our demand, that is, broadcasting a short 96-bit `EPC`. Current WiFi chipsets are all backward compatible with this version. More importantly, the modulation of 802.11b is based on PSK, which doest not conflict with the OOK of RFID. In terms of RFID, our design targets at the EPCglobal Gen2 air protocol, which has been adopted world widely. We begin our design by briefly introducing these two protocols as follows.

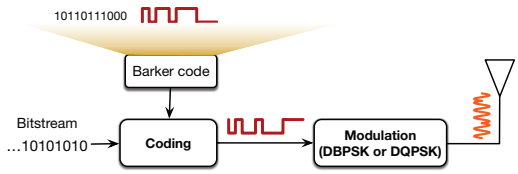


Fig. 7: How a WiFi transmitter works

WiFi Transmission. 802.11b is a set of WiFi physical layer specifications that use spread spectrum modulation. 802.11b PHY uses DBPSK/DQPSK at the physical layer and achieves 4 bit rates using different spreading codes, i.e., DSSS or CCK. We focus on the DSSS, which enables 1Mbps or 2Mbps transmission depending on the modulation. Fig. 7 shows how a WiFi transmitter operates. To improve the reliability, 802.11b uses pseudo-noise codes to spread the spectrum. It XORs each data bit with a Barker sequence (i.e., 10110111000), which is generated at a data rate of 11Mbps, achieving a spread spectrum of over 22MHz. In particular, data bit '0' and '1' are converted to '10110111000' and '01001000111', respectively. Each of these coded bits is then modulated onto the carrier using DBPSK or DQPSK, which offers 1Mbps or 2Mbps transmissions. DBPSK modulation carries '0' and '1' by changing the phase to either 0 or π, whereas DQPSK carries a pair of bits by changing the phase to one of $\{0, \pi/2, \pi, 3\pi/2\}$.

RFID Transmissions. The EPC Gen2 requires a reader to continuously generate a high-power CW. Two links are involved. The first link is data transmission from reader to tag, which is often called *downlink* transmission. The second link is the opposite, which is called as *uplink* transmission. Both links modulate data by OOK (i.e., changing the amplitudes of the CW), but involve different channel coding methods.

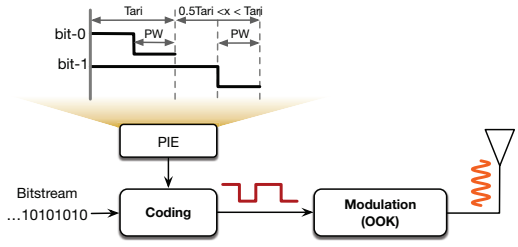


Fig. 8: How a reader transmitter works

- *Downlink*: A reader encodes the data bits using Pulse-Interval Encoding (PIE) for the downlink. As Fig. 8 shows, the PIE coding has three user-defined parameters: `Tari`, `PW` (Pulse Width) and `X`, where `Tari` is the reference interval for the downlink signaling. The duration of a bit '0' should be between $6.25\mu s \sim 25\mu s$. `PW` indicates the time duration of the lower edge, which can be set to a value between `0.265Tari` and `0.525Tari` but is capped at $2\mu s$. The duration of the bit '1' is `X`-μs longer than that of bit '0' and `X` must be between `0.5Tari` and `Tari`. The downlink rate varies between 27Kbps and 128Kbps with respect to the parameter choice.
- *Uplink*: A tag uses either FM0 or Miller coding [31], both of which are highly similar to PIE. We omit the coding details because tags cannot be controled in our design. Without traditional transceivers, tags adopt backscattering based modulation: transmitting a "1" bit by changing the impedance on their antennas to reflect the reader's signal; and a "0" bit by remaining in their initial silent state [32], as aforementioned.

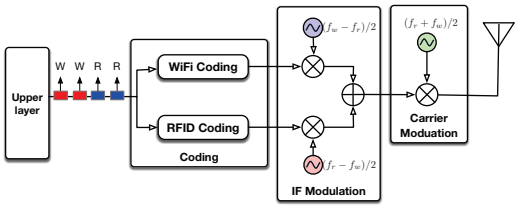


Fig. 9: Physical-layer data flow of TiFi. It adopts dual-coding and dual-keying schemes to support the transmissions of WiFi and RFID packets.

Fig. 10 shows an example of the RFID transmission, which illustrates 300*ms* baseband signals including downlink and uplink transmissions, acquired by a USRP reader.

Challenges: A TiFi reader is required to transmit RFID or WiFi packets with a *single* transmitter. Thus, *sharing the baseband processing is the heart of our design.* After comparing two types of transmissions, we find that achieving this goal is hindered by three main challenges. First, the data rate of an RFID system is limited to hundreds of Kpbs, whereas that of 802.11b is up to 2 Mbps. Second, the reader uses amplitude-shift keying (i.e., OOK) , whereas WiFi uses phase-shift keying (either DBPSK or DQPSK). Third, the battery-free tags cannot hear from one another, hence, the reader is responsible for performing carrier sense on behalf of tags when conducting the cross-technology communication. In responds to these challenges, we elaborate the design of a TiFi reader from the physical layer to the application layer subsequently.

5.3 PHY: Creating RFID and WiFi Packets

Fig. 9 illustrates the design of TiFi's PHY. The baseband receives data from upper layer where each bit is labeled with "R" or "W", which represents the RFID or WiFi data respectively. The baseband encodes the input bits based on their labels. The coded bits are first modulated onto two intermediate frequencies respectively. The combination of the two bit streams are finally modulated onto the RF carrier.

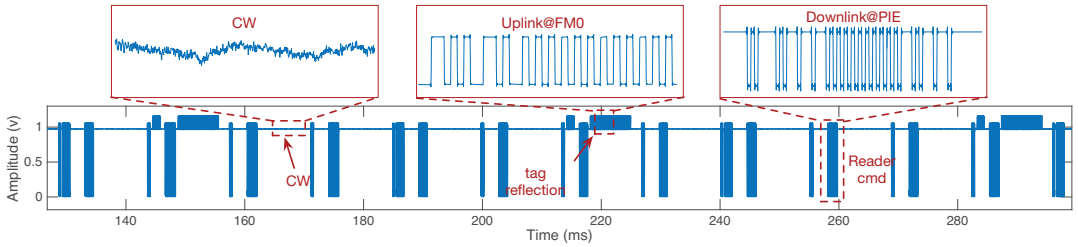


Fig. 10: RFID baseband signals. The figure shows a 300*ms* baseband signal, acquired by a USRP reader. The reader transmit a CW persistently. Both reader and tag modulate data on the CW by OOK but uses different coding methods (reader→ tag, downlink@PIE; tag→reader, uplink@FM0); zooming into the signal allows us to observe data coding of the reader and tags.

5.3.1 Dual Coding Solution. As aforementioned, EPC Gen2 allows user to define three PIE interval parameters. For simplicity, we set `Tari`, `PW` and `X` to 25μs, 2μs and 25μs as an example setting, leading to 25μs bit zeros and 50μs bit ones. In particular, the bit zero flips from high-voltage (HV) to low voltage (LV) at the 23μs and the bit one flips at the 48μs are expressed as follows:

$$\begin{cases} \text{PIE bit zero} = 23\mu s \text{ HV} + 2\mu s \text{ LV} \\ \text{PIE bit one} = 48\mu s \text{ HV} + 2\mu s \text{ LV} \end{cases} \tag{3}$$

Other settings are permissible provided that they are in compliant with EPC Gen2. Here, we use this setting as an example only.

To bridge the rate mismatch, existing CTCs typically use the high-rate transmission to emulate the low-rate transmission [7]. We adopt a similar idea, that is, using the WiFi transmission to emulate the RFID transmission. In particular, TiFi reader spreads the incoming bits based on their labels as follows:

- **[WiFi]**: If the label is "W", then the reader directly spreads it with the Barker sequence directly. Each code bit has an interval of $1/11\mu s$.
- **[RFID]**: If the label is "R", then the reader uses a stream of constant "1"s or "0"s to emulate the PIE coding, which is equivalent to spreading the RFID bits with special spread codes. As shown in Eqn. 3, the PIE bit zero has 23μ HV and 2μs LV. Therefore, the reader spreads the incoming bit zero by $23 \times 11 = 253$ code "1"s plus $2 \times 11 = 22$ code "0"s. Therefore, the reader spreads the incoming bit "0' by $48 \times 11 = 528$ code "1"s plus $2 \times 11 = 22$ code "0"s.

Although no data originates from the upper layer, the reader must still maintain a high-level CW at f_r to keep the tags alive. In this case, the reader must mimic a series of meaningless bit "1"s. In addition, the WiFi beacon packets are always transmitted only during when tag is backscattering. At that moment, the reader maintains a single-tone at f_r.

5.3.2 Dual Keying Schemes. Generally, a carrier signal can be written as $(I(t) + jQ(t))e^{j2\pi f_c t}$ where f_c is the center frequency and $I(t)$ and $Q(t)$ correspond to the in-phase and quadrature-phase components of the coded WiFi or RFID data, respectively. *Keying* is the process of translating the input coded bits into a pair of (I, Q). The two types of packets use two different keying schemes:

- **[WiFi]**: 802.11b modulates the coded data using either DBPSK or DQPSK. Both schemes change the phase of the carrier signal to represent different bits. To do so, TiFi shifts the carrier by one of the four distinct phases: 0, $\pi/2$, π and $3\pi/2$. In particular, (1) DBPSK: the coded "1" and "0" bits are translated to the IQ pairs, $(1, 0)$ and $(-1, 1)$, respectively. This results in two possible carrier signals: 1 and $e^{j\pi}$. (2) DQPSK: two consecutive bits are translated to one of the four IQ pairs: $\{(1, 0), (0, 1), (-1, 0), (0, -1)\}$. This process results in four possible carrier signals, 1, $e^{j\frac{\pi}{2}}$, $e^{j\pi}$ and $e^{j\frac{3\pi}{2}}$.
- **[RFID]**: The reader uses the OOK to modulate coded data. OOK is the simplest form of amplitude-shifting keying that represents digital data at the presence or absence of an RF carrier. In this case, the coded one and zero bits are translated to $(1, 0)$ and $(0, 0)$ respectively. This process results in a constant zero $Q(t)$, and $I(t)$ of 1 or 0, which correspond to a high or low voltage at the tags.

5.3.3 Dual Modulation Solutions. Modulation is the processing of moving the data onto the RF carrier and further propagating it in the air. The reader transmits data at two carrier frequencies (i.e., f_r and f_w) for the RFID and WiFi transmission, respectively. The naive approach is to adopt two transmitters (such as those used in [30]). An RF transceiver typically has over 40 MHz instantaneous bandwidth (e.g., USRP SBX Daughterboard), whereas the frequency difference between f_w and f_r is less than 40 MHz. Therefore, one RF transceiver is sufficient to simultaneously send data at two central frequencies. In this regard, we perform an *intermediate modulation* before modulating them onto the UHF carrier. In particular, the two intermediate frequencies (denoted by f_I^w and f_I^r) are set to $f_I^w = (f_w - f_r)/2$ and $f_I^r = (f_r - f_w)/2$ for WiFi and RFID data stream, respectively. Meanwhile, the final central carrier frequency is set to $f_c = (f_r + f_w)/2$.

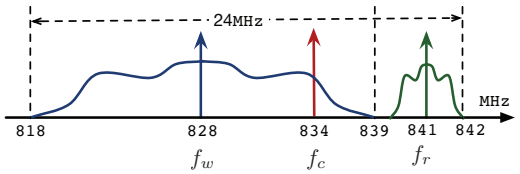


Fig. 11: Dual modulation. Both WiFi and RFID data are carried onto a single RF carrier frequency.

Consequently, the final carrier signal is expressed as:

$$\begin{aligned}&\left\{[I^w(t)+jQ^w(t)]e^{j2\pi f_I^w t}+[I^r(t)+jQ^r(t)]e^{j2\pi f_I^r t}\right\}e^{j2\pi f_c t}\\=&[I^w(t)+jQ^w(t)]e^{j2\pi(f_I^w+f_c)t}+[I^r(t)+jQ^r(t)]e^{j2\pi(f_I^r+f_c)t}\\=&[I^w(t)+jQ^w(t)]e^{j2\pi f_w t}+[I^r(t)+jQ^r(t)]e^{j2\pi f_r t}\end{aligned}$$

where $f_I^w + f_c = (f_w - f_r)/2 + (f_r + f_w)/2 = f_w$ and $f_I^r + f_c = (f_r - f_w)/2 + (f_r + f_w)/2 = f_r$ because of the careful design of the two intermediate frequencies. The modulated results are transformed into two central frequencies: f_w and f_r.

In addition, we also study if the two types of data interfere with each other in terms of the bandwidth. In particular, WiFi and RFID have approximately 22MHz and 2MHz respectively, as shown in Fig. 11. It is easy to find that a blank of 1MHz still remains even if the highest WiFi channel is targeted (i.e., 828MHz). Actually, when the reader transmits WiFi packets, only a single tone at the RFID band exists for keeping tags alive. Thus, both types of transmission do never interfere with each other in any manner.

5.4 MAC: Backscatterring WiFi Packets

The design of MAC layer is to answer the question: *when does the reader transmit WiFi beacons*? The integration timing must meet three rigorous prerequisites. First, the reader should acquire the tag's `EPC` already, because TiFi reader uses the `EPC` as the `SSID` and MAC address of the beacon. Second, the beacon packet must be transmitted exactly during the period when the tag is backscattering, because the WiFi receiver can sense the harmonic backscattering only at this moment. Third, only a single tag is allowed to backscatter WiFi beacons at any given moment; otherwise the mobile device is completely unaware of which tag is transmitting.

Suppose the tag is ready to transmit its `EPC`. It first sends an `RN16` reply that contains a 16-bit random number, after receiving the `Query` or `QueryAdjust` commands. As an acknowledgement, the reader sends back an `ACK` command. The acknowledged tag then starts to transmit a *long reply* including its `EPC`. Our design adopts a less commonly used function, i.e., *retransmission*, which allows the reader to request a retransmission of the long reply by re-sending the `ACK` command. Note that the retransmission request must strictly follow after the last one in less than 20×`Tari`.

The procedure is illustrated in Fig. 12. TiFi is integrated into the EPC Gen2 Protocol as follows.

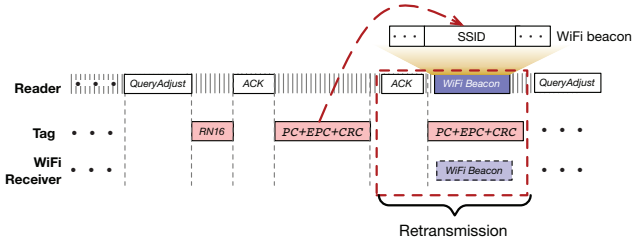


Fig. 12: Reflection of WiFi beacons. TiFi broadcasts the WiFi beacons during the tag's retransmission.

(1) The reader initiates a reading session by broadcasting a `Query` or a `QueryAdjust` command; the tag transmits its `RN16` reply.

(2) As a response, the reader sends back an `ACK` command to request the tag's long reply; the tag transmits the long reply including `EPC`.

(3) After decoding the long reply, the reader immediately resends the previous `ACK` to the tag for triggering a retransmission of its long reply; the tag transmits its long reply again.

(4) During the retransmission, the reader transmits the WiFi beacon, whose `SSID` and MAC fields are assembled with the `EPC` decoded previously.

The only difference with the existing procedure is that TiFi adds a retransmission phase during which the WiFi packets are transmitted. Evidently, selecting a tag's retransmission as the timing to transmit its WiFi beacon efficiently meets the above timing constraints. Fig. 13 presents an example of the baseband signals that follow the aforementioned procedure, as acquired by the TiFi reader. The final effect appears similar to a tag backscatters its `EPC` and WiFi beacon simultaneously.

Discussion. The procedure presented above may elicit the following concerns.

• *Is the time is sufficient to transmit an entire WiFi beacon during retransmission?* A long reply of a tag contains 128 bits, which are encoded via FM0 or Miller. When a general RFID setting is considered, a tag should take at least $128 \times 25\mu s = 3.2ms$ to backscatter the long reply. An 802.11b beacon contains 576 bits and takes $576 \times 1\mu s = 0.576ms$ on transmission. Therefore, a $3.2ms$ backscattering window is sufficiently large to transmit a 0.576ms WiFi beacon 5 times.

• *How frequently are WiFi beacons broadcasted?* The reader is typically configured to continuously and repeatedly scan tags round by round. Suppose that n tags exist. Each tag is queried and thereby generates a WiFi transmission every $(1/ne\ln(n))$ seconds [33]. For example, if 100 tags are available, then the WiFi beacons are broadcasted every $1.8ms$, which is considerably more frequent that the default $100ms$ setting of real WiFi APs.

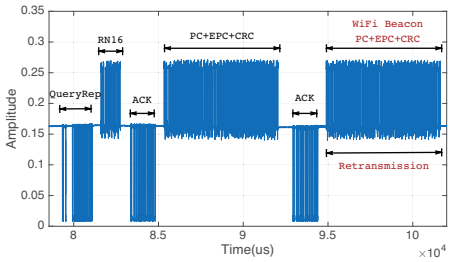


Fig. 13: Baseband signals acquired by a TiFi reader. After decoding the long reply of the tag, TiFi reader riggers a retransmission, during which the WiFi beacon assembled with the EPC is transmitted such that it can be harmonically backscattered by the tag at a WiFi channel.

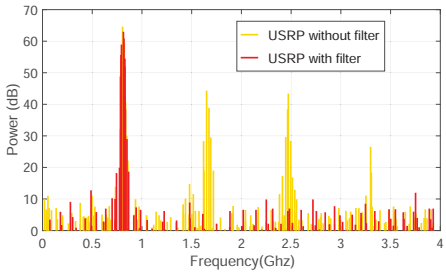


Fig. 14: Harmonic signals from USRP reader. We add an elliptical lowpass filter to suppress the 1.6G and 2.4G harmonics leaked from the USRP devices.

• *How does the transmission of EPC affect a WiFi beacon?* Regardless of whether FM0 or Miller coding is used, the tag reflects its data by changing the amplitude of the CW similar to the PIE in downlink. By contrast, WiFi beacons are modulated by changing the phases (i.e., DBPSK or DQPSK). The final backscattering signal turns into APSK (Amplitude and phase-shift keying). However, the WiFi receiver can still successfully decodes the WiFi beacon because the changes in amplitude do not affect the phase. The decoding of the two types of packets does not affect each other.

• *How does TiFi deal with multiple tags?* TiFi does not need extra efforts to deal with multiple tags but uses the existing EPC Gen2 Q-adaptive algorithm for anti-collision. As shown in Fig. 6, TiFi reader inserts the harmonic backscattering after when a tag is successfully identified, and does not act if the slot is empty or collided.

5.5 APL: Near-Field Identification

Suppose that the signal strength output from the reader is P_r. Then, the signal strength at the WiFi receiver, P_w, can be modeled using Friis path loss [9] as follows:

$$P_w = \left(\frac{P_r G_r}{4\pi d_1^2}\right)\left(\frac{\lambda_r^2 G_t^2}{4\pi}\frac{|\Delta\Gamma|^2}{4}\alpha_w\right)\left(\frac{1}{4\pi d_2^2}\frac{\lambda_w^2 G_w}{4\pi}\right) \quad (4)$$

The preceding equation describes two signal propagations: reader → tag → WiFi receiver. G_r, G_t and G_w are the antenna gains of the reader, the tag and the WiFi receiver, respectively. d_1 and d_2 are the distances among the three components. λ_r and λ_w are the wavelengths of the RFID and WiFi signals. $|\Delta\Gamma|^2$ is the backscatter coefficient. α_w indicates the loss in energy loss in the desired harmonics. Suppose that P_r, G_r, G_t, and G_w are set to 30 dBm, 8 dBi, 2 dBi, and 0 dBi, respectively. Then, $|\Delta\Gamma|^2$ and α_w are around 1.1 dB and 3.3 dB, respectively. After simulation, two key points are obtained. (1) The received power increases when the tag gets close to either the WiFi receiver or the reader, because maximizing the signal strength requires minimizing the product of $d_1 d_2$. (2) The effective coverage range of TiFi is approximately $2m$, and power decreases by about 1dBm each time the tag is moved 10cm away from the WiFi receiver. This condition perfectly fits the demand of near-field identification, such as NFC, which requires distinguishing objects' locations via signal strength within a small area.

6 PERFORMANCE EVALUATION

We describe our implementation and the results of our experimental evaluation in this section.

6.1 Implementation

We implement a prototype of TiFi using a USRP N210 software radio and test it on a variety of commercial RFID tags and WiFi receivers.

• **TiFi Reader.** We implement the reader on a USRP N210, which is equipped with an SBX Daughterboard and an 8dBi directional antenna. Fig. 4 shows the implementation compared with that of a commercial reader (i.e., ImpinJ R420). In particular, UHD gain and baseband signal amplitude are set to 15dB and 0.5, respectively. The sampling rate is set to 25 MHz. The implemented prototype is built and executed on GNU Radio 3.7.10 under Linux Ubuntu 16.04 LTS operating system powered by an Intel Core i5-7200U processor, clocked at 2.50 GHz and a RAM memory of 12 GB. The source code of TiFi reader is released in our project website [34].

• **Reader-Side Harmonic Suppression**. The harmonics caused by the nonlinearity effect are not unique to RFID tags, but widely exist among electronic amplifiers. The commercial RFID readers should manage the harmonics to avoid RF interferences to other devices. We measure the signal spectrums of the TiFi reader with respect to its harmonic leakage. Fig. 14 illustrates the spectrum of the reader when it broadcasts query command without tag reply. We can observe that so many harmonics are leaked from the TiFi reader (without filter). This is because the reader is based on the USRP device, which is not optimized for commercial use. To block the harmonics from the reader, we customize an RF *elliptical lowpass*

#	Technology	Max Range	Frequency
1	TiFi	2 m	2.4 GHz
2	USRP Reader [35]	3m	840 MHz
3	TSL-1128 Reader [12]	1.5m	840 MHz
4	ALR-S350 Reader [13]	1.5m	840 MHz
5	Phychips Reader [4]	0.2m	840 MHz
6	R420 Reader [36]	10 m	840 MHz
7	NFC (HF RFID) [37]	0.9m	13.56 MHz
8	Passive WiFi [9]	15.24m	2.4 GHz
9	FM Backscatter [17]	18.29m	92.1 MHz
10	Ambient Backscatter [18]	1.8m	539 MHz
11	Lora Backscatter [19]	2.8km	900 MHz
12	HitchHike [20]	54m	2.4 GHz
13	BackFi [21]	7m	2.4 GHz
14	Interscatter [22]	27.4m	2.4 GHz

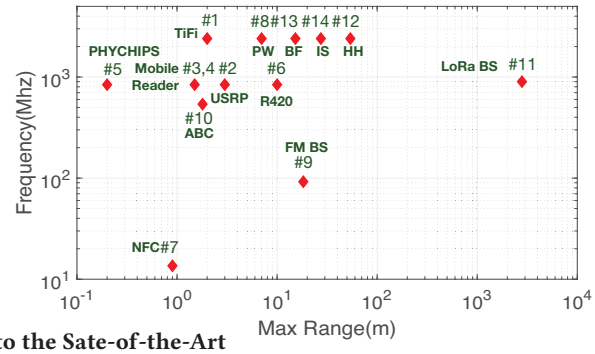


Table 3: Comparison to the Sate-of-the-Art

filter, i.e., a hardware component for harmonic suppression. The filter is designed to have a cutoff frequency of 1 GHz and 0.5 dB in-band ripple. Its restraint outside of the band at 2.4 GHz is over 50 dB. As Fig. 4 shows, the filter is used to bridge the reader and the antenna. Revisiting Fig. 14, we can see that the harmonics of the TiFi reader equipped with the filter are reduced exactly to the noise level (< 10 dB) by the filter. We use the filter in our experiments to ensure that tags are the sole devices that emit harmonic signals.

• **Commercial RFID tags**. Unless noted otherwise, our experiments are performed with the most widely deployed type: ImpinJ Monza 4 QT [5]. To demonstrate the generality of our technique, we also test 6 types of commercial tags, which are produces by two different manufactures, as listed in Table. 2. Each of these tags costs 5 − 10 cents.

• **Commercial WiFi Receiver**. iOS provides extremely limited APIs for dealing with WiFi, such as acquiring RSSI; thus, our evaluation focuses on the Android platform. We use the Huawei P10 (equipped with the WiFi chipset of Broadcom BCM43596) as our default WiFi receiver, and test the diversity across seven types of commercial tags.

6.2 Experimental Setup

We deploy the TiFi reader and test tags with a distance of $2m$ by default in our office. The tag is placed at the position of $50cm$ away from the receiver. Unless otherwise noted, the WiFi and RFID carrier frequencies are configured to 841MHz and 828MHz by default. The UHD gain is set to 20dB. In our experiments, we number the `EPC`s of tags from one. The WiFi beacon packets have a payload of 68 bytes where the SSID is set to the form of `TiFi_XXX` and `XXX` indicates the last few bits of tag's `EPC`. To measure the RSSI values of WiFi beacons, we use a third party Android app called WiFi analyzer [38].

6.3 Comparison to Sate-of-the-Art

For comparison, we profile existing related radio technologies in Table. 3 with respect to the dimensions of frequency and max range. The comparisons show the following findings.

- **USRP Reader**: The USRP reader is implemented using the Open Project [35], which decodes `EPC`s of tags by using USRP at RFID frequency band. TiFi achieves nearly the same range as of the USRP reader (3m). This finding appears "surprising" because the USRP reader uses the 1st-order singal for the communication, which is 50 ∼ 60dB stronger than the 3rd-order harmonic backscattering used by TiFi. This can be explained by the sensitivity. The USRP has a 30dB weaker sensitivity than a mobile phone. It is a little hard for USRP reader to resolve the weak signals of below −60dBm. By contrary, current mobile phone has a quite sensitive transceiver, which can easily deal with signals of down to −90dBm. This ability extends the detection range of TiFi compared with USRP reader.
- **Mobile Reader**: The commercial mobile RFID readers (e.g., TSL-1128 [12] and ALR-S350 UHF readers) have mean ranges of 1.5m, which is even 0.5m shorter than TiFi's. This result show that TiFi can be exactly employed as good substitutes for specialized RFID mobile readers.
- **HTTP Reader**: TiFi achieves the one-fifth of the range of a commercial HTTP reader (e.g., R420 [36]). Unlike USRP reader, these commercial readers have good RF sensitivities as mobile phones. Their 1st-order communications are 60dB-higher than the 3rd-order communications, as listed in Table. 2.
- **HF-NFC**: The HF-NFC operates at the lowest frequency (13.56MHz), which determines its inductive coupling-based communication approach. The energy attenuation of this method is proportional to the cube of the distance. Therefore, the range of HF-NFC is upper bound at approximately 1m. We use the built-in NFC reader of the Moto X+1 phone for the test.
- **Backscatters**: Backscatters typically have a long communication range (> 10m) because they are equipped with large capacitors, which absorb a considerable amount of

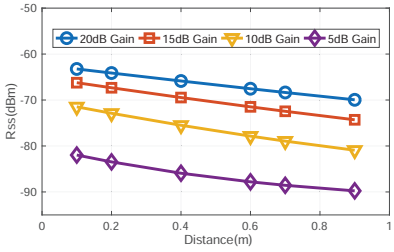


Fig. 15: RSSI

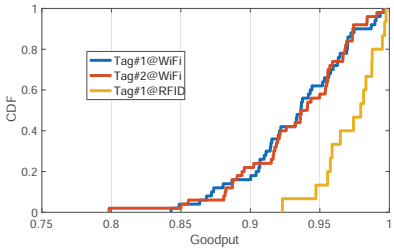


Fig. 16: Goodput

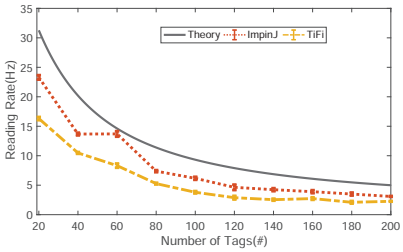


Fig. 17: Reading rate

energy from the air. In particular, Lora backscatter can achieve a maximum range of up to 2.8Km. In contrast to backscatters, TiFi is not required to modify tags (i.e., backscatters).

In summary, TiFi operates at the WiFi spectrum, similar to most of the backscatters, but performs comparably to the commercial mobile readers and better than HF-NFC in terms of the maximal range.

6.4 Characterizing TiFi's NFI

We evaluate the RSSI as a function of distance with different transmitting gains (i.e., a parameter of UHD). In the experiment, we hold the mobile phone in our hand and measure the reported RSSI values by moving the phone away from the test tag under a specific gain setting. Measurements are taken at increments of 10cm. Fig. 15 presents the results of four gain settings, from which we can observe that TiFi exhibits a good quality of linearity where the RSSI decreases as the distance increases, and the rate of decline is approximately 0.086 ± 0.0125dBm per cm. The finding indicates that RSSI has over 1 dBm changes when moving the mobile phone 10cm away from the tag. Note that RSSI is in the unit of dBm, which takes logarithm of the received power (defined in 4). This characteristics is derived from the backscattering communication, which is hypersensitive to the distance. It provides the experimental basis for NFI or proximity localization that the tag nearest to the WiFi receiver achieves the strongest RSSI.

A higher gain setting allows the transmitter to acquire stronger power, thereby extending the reading range. This finding is confirmed by our experimental results. The maximum gain of USRP N210 is up to 31dB. However, As reported in [39], when going beyond a 20dB gain for frequencies below 1.5GHz, USRP device exhibits a severe distortion on harmonics, even given a single tone wave waveform. This hardware defect constrains our experiment results. We believe the commercialized TiFi with customized hardware components would have longer range.

In summary, leveraging the signal strength of WiFi beacon backscattered from tags for near-field identification is completely feasible and effective.

6.5 Coexistence with WiFi Devices

A major concern might be about coexistence between virtual APs and nearby WiFi devices. It can be seen from Fig. 15 that the power of our virtual AP is below -60dBm even when the gain of USRP is set to the maximum (i.e., 20dB). Actually, the power of harmonic backscattering is about 30dB lower than that of the fundamental signals employed in real APs. With respect to the 2m effective range, virtual APs hardly exert any interference on nearby WiFi devices. Thus, TiFi is not a threat to normal WiFi devices.

On the other hand, *how does TiFi deal with interference from nearby WiFi devices?* As aforementioned, TiFi uses the standard Q-adaptive algorithm for anti-collision. This algorithm identifies tags in a random way, resulting that WiFi beacons are broadcasted randomly and repeatedly. Even if one broadcast is interfered, the smart device will find another time slot in the future to receive the beacon correctly. The similar case happens to the real APs, whose beacons are interfered by nearby WiFi devices sometimes. However, we can still find out them in a certain time.

6.6 Evaluation on Goodput

We evaluate the goodput of WiFi transmission, which is defined as the percentage of beacons that are successfully decoded relative to the total transmitted WiFi beacons. The WiFi analyzer cannot provide such rate; hence, we use a USRP based WiFi receiver for the experiment. We let the TiFi reader continuously query the test tag and send 100 WiFi beacons. We perform 50 experimental trails and plot the CDF of goodput across two types of tags (Tag#1 and Tag#2) in Fig. 16. The two tags exhibit similar performance and their median goodput of is 93%. The lowest goodput is still maintained above 80%. This experiment demonstrates that TiFi can provide reliable beacon transmissions for WiFi receiver through the backscattering of harmonics. We also plot the corresponding goodput of the TiFi' reader with respect to the

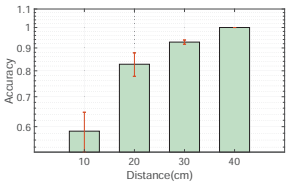


Fig. 18: Proximity

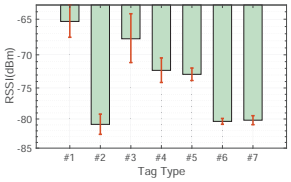


Fig. 19: Tag diversity

EPC (@840MHz) in the figure for comparison. The reader has a median goodput of 97.9%, which is 4% higher than that of WiFi. This is reasonable because the assembly of WiFi beacon depends on the resolution of EPCs. TiFi's reader can almost achieve the goodput as good as its the first-order transmission.

6.7 Evaluation on Scalability

Next, we evaluate the scalability of TiFi in terms of the number of tags, i.e., how many tags does TiFi support? Since TiFi tightly integrates into Gen2 protocol, its scalability mainly depends on that of the Gen2 protocol. In theory, Gen2 protocol can read any number of tags as long as it is given enough time. In practice, we usually use a classic metric called *reading rate* (i.e., the number of reading times per second per tag) to imply the scalability.

To obtain the reading rate, TiFi reader and ImpinJ reader are configured to inventory all tags continuously and repetitively for 10 minutes in the experiments. Their average reading rates are shown in Fig. 17. It can be seen from the figure that the rate drops approximately linearly as the number increases. This is because more tags' participations incur more collisions and further lower the rate. The reading rate of TiFi is lower than the ImpinJ reader because each tag must transmit its *long reply* twice (see Fig. 13). We also plot the theoretical rate presented in [33] for reference. From the perspective of reading rate, we could present the scalability under a time constraint as follows: if each tag must advertise its WiFi beacons at least once *within one second* (i.e., 1Hz reading rate), TiFi can support about 200 tags; if advertising at least once *within* 100*ms* (i.e., 10Hz reading rate), about 42 tags are supported.

6.8 Proximity based Localization

We next attempt to localize two tags by using the signal strength of their WiFi beacons, i.e., the tag with higher RSSI is considered being closer to the WiFi receiver. In the experiment, we place two ImpinJ QT4 tags and the mobile phone in a row. Both the mobile phone and the reader are deployed on the left side of the two tags. Fixing a distance of two tags, we perform 30 experimental trails, each of which outputs the order based on two tags' RSSIs. We calculate the accuracy, defined as the percent of trails outputting the right order. The results are shown in Fig. 18. We find that the accuracy is up to 99% when two tags are spaced with 40cm or above. The accuracy reduces to 93% and 83% when the distance is set to 30cm and 20cm respectively. This is mainly because the mobile device only reports integral RSSI by truncating the fractions, making the RSSI insensitive to the distance. Even so, such accuracy is sufficient for coarse-grained localization in daily life, e.g., locating a book on a shelf or inside a box.

6.9 Impacts of System Configurations

Next, we evaluate TiFi's RSSI as a function of different system configurations:

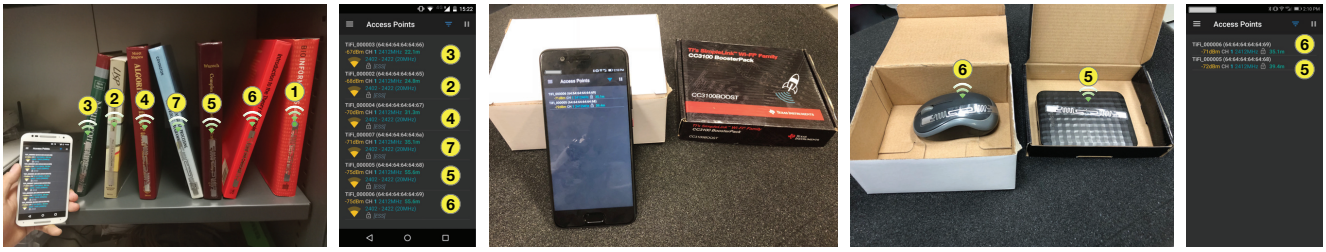
• **Receiver:** Table 4 lists the 7 types of WiFi receivers that we have tested. In particular, BCMxxx, KMDxxx and WCNxxx are the WiFi chipsets from Broadcom, Murata and Qualcomm respectively. Among which, Apple MacBookPro has a maximum range (*MR*) of 2.6 m, which has the strongest RSSI at the 10 cm distance (i.e., *R10*, −60 dBm) because the WiFi receiver of the laptop is considerably more powerful than mobile devices. The tests demonstrate that the WiFi receivers do not impose evident impact on RSSI.

• **Tag:** Fig. 19 shows the impact of tag type on RSSI and their hardware information are listed in Table 2. In the experiment, tags are placed in front of the reader antenna with a distance of 10*cm*. We observe considerable differences among different types. In particular, tag#1 achieves the highest RSSI. This type tag adopts the antenna design of circular polarization, which is composed of a pair of perpendicular linear antennas. Thus, it can absorb energy or backscatter signals from various perspectives. However, although tag#2 also adopts circular polarization, its antenna area is only a half of that of tag#1 and thereby shows lower RSSI. This group of experiments suggests that one should employ a same type of tags for the proximity based localization or payment because the RSSI depends on tag types.

• **Frequency:** We fix the positions of mobile devices, but broadcast 14 WiFi fundamental frequencies, whose 3rd-order harmonics of which correspond to the 14 WiFi channels. This experiment demonstrates that our design completely supports any of the 14 WiFi channels.

Table 4: Receiver Diversity

Manuf.	Model	OS	Chipset	MR.	R10
Apple	MackBookPro	OSX	BCM43xx	2.6m	−60
Huawei	Mate 9	AN 8	BCM43455	2.3m	−65
Huawei	P10	AN 8	BCM43596	2.3m	−66
Lenovo	Moto X+1	AN 5	Unknown	2.3m	−67
Samsung	S8	AN 7	KM6D28040	2.1m	−63
Xiaomi	Mi 6	AN 7	WCN3990	2.2m	−64



(a) Books on shelf (b) APs (c) Closed box (d) Open box (e) APs

Fig. 20: TiFi in real-world applications. (a) shows RFID-tagged books on on shelf. (b) shows identification results of books by the analyzer. (c) shows using a mobile phone to identify objects in boxes. (c) shows the RFID-tagged objects after removing the occlusions. (d) shows the identification results of objects inside box.

7 APPLICATIONS

Finally, we qualitatively test TiFi in two real-world scenarios: identifying RFID-tagged books on shelf and RFID-tagged objects in closed box. Across the two applications, TiFi could achieve the same level of effectiveness reported in the quantitative results above. In particular, the second scenario also shows the ability of TiFi to identify the RFID tags through their WiFi beacons in NLOS scenarios.

8 RELATED WORK

We review the related works from the three fields.

• **Harmonic Backscattering.** Although the study and the exploitation of utilization of nonlinearity in diode based devices are not new, the harmonics in RFID system have only elicited attention in recent years. The harmonic phenomenon in RFIDs was reported in [32, 40–46]. The work [26] characterized the harmonic signals in UHF RFID with extensive experiments. [40] and [47] are the most related works to ours. Similar to TiFi, [40] also explores the harmonics as a secondary communication channel. However, by virtue of harmonic backscattering, TiFi targets at talking with WiFi receiver while [40] is to enhance the communication between the reader and tags. This work [47] uses the harmonics to achieve the multi-frequency continuous wave ranging and further localize tags in 3D space. Unlike these prior work, our work utilizes the 3rd harmonics for cross-frequency communication.

• **CTC.** Recently, many works have investigated CTC [7, 11, 48–50]. Some of these works [7, 11, 48–50] have studied the cross communication between Wi-Fi and ZigBee. WEBee [7] uses a high-speed wireless radio (e.g., WiFi OFDM) to emulate the desired signals of a low-speed radio (e.g., ZigBee). FreeBee [11] establishes CTC by modulating the interval of WiFi beacons. Esense [48] modulates the lengths of WiFi frames to establish communication channels from WiFi to ZigBee. HoWiES [50] transmits data with combinations of WiFi frames. Our work achieves the cross-frequency communication between RFID and WiFi in physical layer, which was never done before.

• **Backscatters.** Similar to the RFID tags, backscatters are the battery-free devices that modulates data by reflecting the source signals. Dozens of backscatters have been proposed in the past five years [9, 17–22]. The closest to our work is a recent work called Passive WiFi [9], which generates the 802.11b packets. However, Passive WiFi requires FPGA for signal processing which takes higher energy consumption. Unlike backscatters, our design is based on the commercial low-cost and lightweight RFID tags.

9 CONCLUSION

This work presents TiFi, a system that enables commercial WiFi receivers working at 2.4GHz to identify 800MHz UHF RFID tags. Leveraging the harmonic backscattering for communication is a challenging technical problem. TiFi has taken an important step toward addressing this problem. However, the current version of TiFi still has two main limitations: first, the identification range is relatively short because of the severe harmonic attenuation and FCC spectrum constraint. Second, the identification still depends on readers, limiting the usage scenario in practice.

While there is scope for many improvements, we believe TiFi advances the state of the art in crosse-technology communication by using the harmonic backscattering of tags. The key innovation of this work involves two unique techniques, CFC and CPC - enabling tags to backscatter WiFi AP beacons without changing the hardware or firmware of RFID tags and mobile devices. This work will inspire plenty of new applications over UHF RFID systems.

Acknowledgments. The research is supported by NSFC General Program (NO. 61572282), UGC/ECS (NO. 25222917), Shenzhen Basic Research Schema (NO. JCYJ20170818104855702), and Alibaba Innovative Research Program. We thank all the anonymous reviewers and shepherd for their valuable comments and helpful suggestions.

REFERENCES

[1] 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 *Proc. of ACM MobiCom*, 2014.

[2] Lei Yang, Yao Li, Qiongzheng Lin, Xiang-Yang Li, and Yunhao Liu. Making sense of mechanical vibration period with sub-millisecond accuracy using backscatter signals. In *Proc. of ACM MobiCom*, 2016.

[3] Frost and Sullivan. Global rfid healthcare and pharmaceutical marke. *Industry Report*, 2011.

[4] Phychips Technologies. http://www.phychips.com/applications-main/.

[5] ImpinJ, Inc. http://www.impinj.com/, 2017.

[6] Zicheng Chi, Yan Li, Hongyu Sun, Yao Yao, Zheng Lu, and Ting Zhu. B2w2: N-way concurrent communication for iot devices. In *Proc. of ACM SenSys*, 2016.

[7] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *Proc. of ACM MobiCom*, 2017.

[8] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Joshua R Smith, and Shyamnath Gollakota. Inter-technology backscatter: Towards internet connectivity for implanted devices. *GetMobile: Mobile Computing and Communications*, 21(3):35–38, 2017.

[9] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. Passive wi-fi: Bringing low power to wi-fi transmissions. In *Proc. of ACM NSDI*, volume 16, pages 151–164, 2016.

[10] Wenchao Jiang, Zhimeng Yin, Song Mim Kim, and Tian He. Transparent cross-technology communication over data traffic. In *Proc. of IEEE INFOCOM*, 2017.

[11] Song Min Kim and Tian He. Freebee: Cross-technology communication via free side-channel. In *Proc. of ACM MobiCom*, 2015.

[12] TSL-1128 Handled Reader. https://www.impinj.com/platform/connectivity/tsl-1128/.

[13] ALR-S350 Handled Reader. http://www.alientechnology.com/products/readers/alr-s350/.

[14] Alien. http://www.alientechnology.com, 2017.

[15] ThingMagic M6. https://www.atlasrfidstore.com/thingmagic-m6-uhf-rfid-reader-4-port/.

[16] ThingMagic Non-HTTP Reader. https://www.atlasrfidstore.com/thingmagic-vega-ruggedized-rfid-reader/.

[17] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. Fm backscatter: Enabling connected cities and smart fabrics. In *Proc. of ACM NSDI*, 2017.

[18] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: wireless communication out of thin air. In *Proc. of ACM SIGCOMM*, 2013.

[19] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *arXiv preprint arXiv:1705.05953*, 2017.

[20] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proc. of ACM SenSys*, 2016.

[21] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. Backfi: High throughput wifi backscatter. *Proc. of ACM SIGCOMM*, 2015.

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

[23] Dahmane Allane, Gianfranco Andia Vera, Yvan Duroc, Rachida Touhami, and Smail Tedjini. Harmonic power harvesting system for passive rfid sensor tags. *IEEE Transactions on Microwave Theory and Techniques*, 64(7):2347–2356, 2016.

[24] T-W Yoo and Kai Chang. Theoretical and experimental development of 10 and 35 ghz rectennas. *IEEE Transactions on Microwave Theory and Techniques*, 40(6):1259–1266, 1992.

[25] Gianfranco Andía Vera, Yvan Duroc, and Smail Tedjini. Analysis of harmonics in uhf rfid signals. *IEEE Transactions on Microwave Theory and Techniques*, 61(6):2481–2490, 2013.

[26] Gianfranco Andia Vera, Yvan Duroc, and Smail Tedjini. Analysis and exploitation of harmonics in wireless power transfer (h-wpt): passive uhf rfid case. *Wireless Power Transfer*, 1(2):65–74, 2014.

[27] Pavel V Nikitin and KVS Rao. Harmonic scattering from passive uhf rfid tags. In *Antennas and Propagation Society International Symposium, 2009. APSURSI'09. IEEE*, pages 1–4. IEEE, 2009.

[28] Gianfranco Andia Vera, Yvan Duroc, and Smail Tedjini. Redundant backscattering modulation of passive uhf rfid tags. In *Microwave Symposium Digest (IMS), 2013 IEEE MTT-S International*, pages 1–3. IEEE, 2013.

[29] KYEINSIGHT Technologies. https://www.keysight.com.

[30] Yunfei Ma, Nicholas Selby, and Fadel Adib. Minding the billions: Ultra-wideband localization for deployed rfid tags. In *Proc. of ACM MobiCom*, 2017.

[31] EPCglobal Gen2 Specification. www.gs1.org/epcglobal, 2004.

[32] Daniel M Dobkin. *The RF in RFID: UHF RFID in Practice*. Newnes, 2012.

[33] Qiongzheng Lin, Lei Yang, Huanyu Jia, Chunhui Duan, and Yunhao Liu. Revisiting reading rate with mobility: Rate-adaptive reading in cots rfid systems. In *Proc. of ACM CoNEXT*, CoNEXT '17, 2017.

[34] TiFi Project. https://tifi.tagsys.org.

[35] USRP Reader. https://github.com/nkargas/Gen2-UHF-RFID-Reader.

[36] ImpinJ R420. https://www.impinj.com/platform/connectivity/speedway-r420/.

[37] Lenovo Moto X Phone. https://www3.lenovo.com/ae/en/phone/moto-phone/phones/Moto-X-Style/p/WMD00000239.

[38] Wi-Fi Analyzer. https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer.

[39] Rafik Zitouni, Stefan Ataman, Marie Mathian, and Laurent George. Radio frequency measurements on a sbx daughter board using gnu radio and usrp n-210. In *Measurements & Networking (M&N), 2015 IEEE International Workshop on*, pages 1–5. IEEE, 2015.

[40] Gianfranco Andíia Vera, Yvan Duroc, and Smail Tedjini. Third harmonic exploitation in passive uhf rfid. *IEEE Transactions on Microwave Theory and Techniques*, 63(9):2991–3004, 2015.

[41] Sudarshan Vasudevan, Donald Towsley, Dennis Goeckel, and Ramin Khalili. Neighbor discovery in wireless networks and the coupon collector's problem. In *Proc. of ACM MobiCom*, 2009.

[42] Matthew S Trotter, Joshua D Griffin, and Gregory D Durgin. Power-optimized waveforms for improving the range and reliability of rfid systems. In *RFID, 2009 IEEE International Conference on*, pages 80–87. IEEE, 2009.

[43] A Collado and A Georgiadis. Optimal waveforms for efficient wireless power transmission. *IEEE Microwave and Wireless Components Letters*, 24(5):354–356, 2014.

[44] Alírio Boaventura, Ana Collado, Nuno Borges Carvalho, and Apostolos Georgiadis. Optimum behavior: Wireless power transmission system design through behavioral models and efficient synthesis techniques. *IEEE Microwave Magazine*, 14(2):26–35, 2013.

[45] Nuno Borges Carvalho, Apostolos Georgiadis, Alessandra Costanzo, Hendrik Rogier, Ana Collado, José Angel García, Stepan Lucyszyn, Paolo Mezzanotte, Jan Kracek, Diego Masotti, et al. Wireless power transmission: R&d activities within europe. *IEEE Transactions on Microwave Theory and Techniques*, 62(4):1031–1045, 2014.

[46] Zhenjiang Li, Yaxiong Xie, Mo Li, and Kyle Jamieson. Recitation: Rehearsing wireless packet reception in software. In *in Proc. of ACM MobiCom*, pages 291–303, 2015.

[47] Yunfei Ma, Xiaonan Hui, and Edwin C Kan. 3d real-time indoor localization via broadband nonlinear backscatter in passive devices with centimeter precision. In *in Proc. of ACM MobiCom*, pages 216–229, 2016.

[48] Kameswari Chebrolu and Ashutosh Dhekne. Esense: Communication through energy sensing. In *Proc. of ACM MobiCom*, 2009.

[49] Xinyu Zhang and Kang G Shin. Gap sense: Lightweight coordination of heterogeneous wireless devices. In *Proc. of IEEE INFOCOM*, 2013.

[50] Yifan Zhang and Qun Li. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In *Proc. of IEEE INFOCOM*, 2013.