Battery-free Wideband Spectrum Mapping using Commodity RFID Tags

Mohamed Ibrahim, Atul Bansal, Kuang Yuan, Swarun Kumar, Peter Steenkiste
Carnegie Mellon University

ABSTRACT

This paper introduces *RFIMap*, a system that aims to inexpensively characterize the *spatial* and temporal distribution of RF spectrum occupancy of any indoor space at fine granularity (tens of centimeters). *RFIMap* builds rich wide-band indoor spectrum occupancy maps using low-cost and battery-free commodity RFID tags. *RFIMap*'s spectrum maps have wide-ranging applications such as monitoring ambient interference in smart manufacturing, and smart hospitals. *RFIMap* relies on the observation that commodity RFID tags naturally reflect ambient transmission at other frequency bands, without any modification. *RFIMap* uses these reflections to estimate the ambient signal power originally received at these tags. *RFIMap* further performs a careful modeling of indoor multipath to build a dense spectrum map with fine spatial granularity. Our experiments demonstrate spatial spectrum measurement with 2.15 dB of median error at 2.4 GHz, 4.45 dB of median error at 470-700 MHz TV whitespace band, 2.1 dB of median error at 1.8-1.9 GHz in diverse industrial and university settings.

CCS CONCEPTS

• **Networks** → *Network monitoring*.

KEYWORDS

Spectrum Sensing, RFID, Backscattering, Battery-free

ACM Reference Format:
Mohamed Ibrahim, Atul Bansal, Kuang Yuan, Swarun Kumar, Peter Steenkiste. 2023. Battery-free Wideband Spectrum Mapping using Commodity RFID Tags. In *The 29th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '23), October 2–6, 2023, Madrid, Spain.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3570361.3592508

ACM MobiCom '23, October 2–6, 2023, Madrid, Spain

ACM ISBN 978-1-4503-9990-6/23/10.
https://doi.org/10.1145/3570361.3592508

Figure 1: Commercial RFID tags powered by a 915 MHz RFID reader, also backscatter signals at other frequencies. *RFIMap* exploits this to recover the signal power incident at the tag at desired frequencies.

1 INTRODUCTION

In this paper, we consider the classic problem of spectrum sensing with an emphasis on being able to inexpensively monitor wide-spectrum *spatially* at fine granularity – tens of centimeters. We target this long-standing problem in wireless literature but with first of its kind low-cost battery-free easy-to-scale solution. Consider building a spatial heat-map of RF interference over wide bandwidths in domains such as smart manufacturing, smart surgery, or airplanes [32, 33, 50] that are crucial for system reliability and security. A rich real-time spectrum map, say in a smart manufacturing facility, can help to understand how the interference would affect different instruments within the space, and help us further localize the interferer. Such severe interference can halt time-sensitive and/or life-sensitive operations. To illustrate a common example, imagine rapidly identifying and tracking wireless devices held by passengers that have not been switched to airplane mode within an aircraft that may otherwise pose interference to flight control systems. In other words, we seek to design a system that can also support spectrum monitoring applications where measuring the *spatial* distribution of interference matters as much as measuring *spectral* distribution. These dense spectrum maps are also useful to network managers for diagnosing network state, interference and faults. Finally, these spectrum maps could lead to an extreme form of spatial reuse wherein fine-grained unoccupied spectrum holes discovered can enable

the reuse of spectrum over small areas, improving overall throughput.

Despite the rich literature on spectrum sensing, achieving rich spatial granularity and wide-bandwidth results in a natural trade-off, especially under cost constraints. Specifically, spectrum analyzers [56] and more recent software radio based systems [15, 40] offer high bandwidth, but measure spectrum at only one location and are expensive to replicate spatially throughout a space. One could instead use a robot or human to move these instruments around to inspect the whole space periodically to save cost, but this would fail to capture interference maps that change rapidly over time. In contrast, lower-cost software radio platforms [34, 52] tend to trade-off sensed bandwidth for cost. Recent work has proposed building low-power and wideband RF sensing platforms [14, 26], but these require custom hardware that are challenging to scale spatially in the near-term.

This paper delivers wide-band spatial sensing using a familiar battery-free platform that costs only a few cents – commodity passive RFIDs. We present *RFIMap*, which uses multiple off-the-shelf passive RFID tags distributed across an indoor space to perform wideband spectrum sensing and build a spatial spectrum map. Signals from these tags are measured at a *single* wide-band receiver. To the best of our knowledge, this is the first spectrum sensing system using commercial RFID tags to enable a cheap battery-free solution for scalable wideband spatial sensing. We show that *RFIMap* can predict signal power with maximum error of 5 dB at 600-850 MHz, 1.8-1.9 GHz, and 2.4GHz in different indoor settings.

At a high level, *RFIMap* operates by deploying commodity RFID tags across a space where a spectrum map is desired (see Fig. 1). Each tag harvests energy from a commodity 915 MHz RFID reader deployed in the environment. *RFIMap*'s key idea is built on the observation that commodity passive RFIDs backscatter signals, not only from a 915 MHz RFID reader, but also other frequency bands in their vicinity (indeed, a similar observation has been made in prior work on RFID localization [31] and cross-frequency communication [5]). In fact, 915 MHz RFIDs backscatter in bands well beyond where they are intended to resonate, albeit with less efficiency but nevertheless quite detectable.

This fact turns a passive tag as a reflector for the signals at the wide range of frequencies present in the environment, albeit with different reflection coefficients. *RFIMap* captures these backscatter signals from each tag at a single wide-band receiver co-located with the reader that senses the spectrum well outside the 915 MHz ISM band (e.g., the 2.4 GHz Wi-Fi band). *RFIMap* uses these measurements to obtain a wideband spectrum map at each location where a tag is deployed, as well as interpolates these measurements for locations in-between.

The rest of this paper tackles the various challenges in designing *RFIMap*. To begin with, we consider an obvious challenge – since *RFIMap* uses commodity RFIDs, it can never directly measure the received signal power from ambient transmitters to tags. Instead, *RFIMap* measures the signal power along the indirect backscatter path that goes from the ambient transmitter, to the tag, and onto the wide-band receiver (see Fig. 1). Said differently, this backscatter signal is attenuated along two distinct paths: (1) The signal path from the transmitter to the tag (i.e., what we seek to measure; shown in green in Fig. 1); and (2) The signal path from the tag to the receiver (i.e., what we seek to eliminate; shown in red in Fig. 1). *RFIMap* must therefore somehow estimate and eliminate the signal path attenuation from the tag to the wide-band receiver. To do so, *RFIMap* relies on a completely different signal measurement that nearly takes a path identical to the one, we seek to eliminate. Specifically, consider the 915 MHz backscatter signal from the RFID reader to the tag – shown in blue in Fig. 1. We note that provided the wide-band receiver is co-located to the reader, this path is extremely similar to the one, we seek to eliminate. *RFIMap*'s key idea is therefore to use signal measurements of the blue path to estimate and eliminate attenuation from the red path. The result is the desired signal power measurement along the green path from any ambient transmitting source to a tag in the environment.

However, transforming signal measurements from the blue path to that of the red path is quite challenging. Besides, the blue path is a round-trip path operating at 915 MHz, which is quite different from the red path (e.g., which may be at 2.4 GHz). To deal with this difference, *RFIMap* must perform channel estimation at a desired band (e.g., 2.4 GHz) using only measurements at the 915 MHz ISM band that RFID readers operate on. To do so, we choose to model the physical paths traversed by the signal. The key idea here is to rely on signal measurements at 915 MHz to estimate the locations of dominant reflectors surrounding the RFID reader. One can then rely on ray-tracing signal models that use these dominant reflector locations to estimate wireless channels at the desired frequency band (e.g., 2.4 GHz). To disambiguate reflectors that are close to each other, *RFIMap* can also be extended to hop on TV whitespace frequencies to improve the resolution at which the dominant reflector locations are estimated, at the expense of the latency. We can therefore use this strategy to estimate the signal along the red path (at say 2.4 GHz) from that of the blue path at 915 MHz (Sec. 4). We further show how *RFIMap* can use ray-tracing models to generate rich spatial spectrum occupancy

output by interpolating channel measurements even at locations in between RFID tags (Sec. 5).

Limitations: We concede that commodity RFID tags have a limited range of about 15 meters that limits the overall spatial coverage of a system with one wide-band reader. This could be remedied, in part, using recent work on long-range commodity RFIDs [48], however, we leave this for future work. *RFIMap* further explores ways to model the impact of RFID tag orientation, radar cross section, and improving multipath-resilience by leveraging the TV whitespaces in addition to the 915 MHz ISM band (see Sec. 8).

We implement and evaluate *RFIMap* on commercial RFID tags [1], an RFID reader [2], and USRP software radios serving as wide-band receivers. We build a spectrum map in different industrial and lab indoor settings. Further, we use USRPs as receivers, acting as ground truth for tags and wideband receivers for the readers. Our results show: (1) An 8 dB overall improvement in predicting spatial signal power at a particular location over a single USRP estimate deployed at a different location. (2) Our multipath-aware interpolation outperforms linear interpolation of the estimated received signal with a 3.4 dB improvement. (3) *RFIMap* can predict signal power with a median error of 3.19 dB at 600-950 MHz, 1.7-1.9 GHz, and 2.4 GHz in different indoor settings.

Contributions: This paper contributes:

- To our knowledge, the first spatial wide-band spectrum sensing system using COTS passive RFIDs.
- An approach to measure spatial wide-band RFID spectral characteristics using measurements made at the 915 MHz ISM band.
- A detailed system implementation and evaluation in diverse indoor multipath-rich environments, including an industrial space.

2 RELATED WORK

Spectrum sensing is an extensively studied area. To the best of our knowledge, *RFIMap* is the first work to perform high spatial resolution and wide-band spectrum sensing using commodity RFIDs. We broadly categorize related work into the following:

Low-Cost Spectrum Sensing: Recent work proposes to reduce the cost of each spectrum sensor [14, 34, 38, 43, 52], which is crucial for large-scale and spatial spectrum sensing. QuickSense [52] employs analog bandwidth filters and energy detectors to provide an energy-efficient and low-cost spectrum monitoring approach. Prior solutions [34, 38] also have used the low-cost RTL-SDR connected to smartphones or Raspberry-Pis to perform crowdsourced spectrum measurements. Sitara [43] further developed a fully-integrated portable software radio which has a battery life up to a week and only costs $38 each. While these solutions demonstrate great advances toward large-scale spatial spectrum sensing deployments, commodity RFIDs offer an order-of-magnitude improvement in cost and are battery-free. Specifically, we use Alien Squiggle ALN 9640 tags [1] which cost $0.22 per tag compared to prior low-cost spectrum sensors that cost several tens of dollars such as QuickSense [52] ($100), [38] and Sitara [43] ($38). While this paper uses a USRP as the receiver, it can be replaced, in production, by other lower-cost SDR platforms and receivers [34]. For instance, if a narrowband sensing is enough for the intended application, narrowband low-cost SDRs such as RTL-SDR or QuickSense [52] can be used instead of a USRP. Low-cost wideband sensing can also be enabled by adopting other cheaper complementary platforms such as S3 [14].

Battery-Free Backscatter: Passive backscatter has several advantages: low-cost, no batteries, and the ability to integrate various sensors. There is much prior work on traditional backscatter technologies such as RFID [9, 16, 31, 46] and NFC [25, 47, 58]. In recent years, researchers have developed backscatter systems on non-traditional frequency bands such as WiFi [4, 8, 11, 55], LoRa [17, 18, 22, 37], FM Radio [20, 45], TV whitespaces [27, 36], etc. Further, there also have been novel backscatter sensing systems proposed for motion and vibration sensing [10, 51], localization [24, 29, 30, 42, 49], body health monitoring [21], etc. Perhaps closest to *RFIMap* is [12], a short vision paper that motivates the need of having a wideband spectrum sensing solution using backscatter solutions. However, to the best of our knowledge, prior work has not explored deploying a COTS RFID backscatter system to perform wideband and spatial spectrum sensing.

Cross-Frequency Channel Estimation: Cross-frequency channel estimation has been proposed as an important solution to eliminate feedback overhead in Frequency Domain Duplexing (FDD) cellular networks. In such systems, base stations infer the downlink channel based on the uplink channel which operates in another frequency band. R2F2 [44] models the underlying multipath using the uplink channels of a linear antenna array, and infers the corresponding downlink channel without any feedback. OptML [6] further applies machine learning to obtain the multipath which reduces the computational complexity of the optimization process of R2F2, and also supported signal antenna devices. FIRE [28] trains an end-to-end generative machine learning model to predict downlink channel without inferring the intermediate multipath, which significantly improves the channel prediction accuracy. Besides cellular networks, Chime [13] estimates optimal frequency configuration in LoRa systems by estimating multipath using a single LoRa packet and using distributed base stations.

Figure 2: System workflow of *RFIMap*. In Step 1, we estimate the channel as well as dominant reflectors between the RFID tags and the reader. In Step 2, we estimate the signal power incident at the RFID tag at an ambient source transmitter frequency. In Step 3, we estimate the location of the ambient source transmitter. In Step 4, we interpolate the spectrum measurements to other locations via a smart multipath-aware interpolation algorithm.

RFIMap builds on this work but operates in a different context – using 915 MHz RFID backscatter signals and relying on multipath estimation from a distributed array of passive RFID tags.

Wideband Spectrum Sensing: Promising progress have been achieved in recent years to push the limits of spectrum sensing systems to real-time wideband sensing. Such work is either based on smart sweeping algorithms to scan wideband spectrum using narrowband sensors [15, 40, 53], or sampling below the Nyquist rate using the Sparse Fourier Transform [19, 41] or compressive sensing [39, 54, 57]. For example, SweepSense [15] modifies the USRP to enable it to sweep 5 GHz bandwidth in 5 ms, which achieves wideband sensing and high-time resolution. Sparse FFT-based approaches such as BigBand [19] and the compressive sensing-based approaches such as [39] also achieve hundreds of MHz of sensing bandwidth, when the spectrum is sparsely occupied. More recently, S^3 [14] achieves over 418 MHz spectrum sensing in real-time based on adopting MEMS acoustic resonators with only cheap and low-power ADCs. In comparison with these works, *RFIMap* is solving a different problem: building a dense spectrum occupancy map across wideband frequencies at a low cost. These systems can be viewed as a complementary part to our standard wideband receiver to further improve the temporal resolution of wideband sensing.

3 SYSTEM OVERVIEW

This section provides a brief overview of *RFIMap*. *RFIMap* is a battery-free spectrum sensing system that aims to build a dense wideband RF spectrum occupancy map with fine spatial granularity. To achieve this goal, we deploy multiple RFID tags across an indoor space where a spectrum map is desired. An RFID reader and a wideband receiver are co-located and used respectively to power the tags and receive wideband backscatter signals for real-time signal processing.

Fig. 2 presents the workflow of *RFIMap* to obtain a dense spectrum occupancy map. In step 1 (Sec. 4.2), we first estimate the channel between each RFID tag and the reader using 915 MHz ISM band signals, and further model the multipath by identifying dominant reflectors in the environment. In step 2 (Sec. 4.3), we seek to accurately measure the signal power at each tag incident from the ambient transmitter source at any frequency. To achieve this, we use the multipath model to estimate the channel at the desired frequency, and then eliminate the undesired signal attenuation from the received backscatter signal. In step 3 (Sec. 5.1), we use the signal received by the reader from the ambient source transmitter along with the reflections from all tags and the estimated channels to localize that ambient transmitter. In step 4 (Sec. 5.2), we further improve the spatial granularity of the spectrum map by interpolating the signal power of the vacant locations between two tags based on the the multipath model and the ambient source location.

4 ESTIMATING SIGNAL POWER AT RFIDS

In this section, we will explain how we estimate the signal power at each of the RFID tag locations due to ambient transmitters operating at any frequency.

We leverage a key observation: Commodity passive RFID tags can backscatter RF signals at any frequency, provided that they are turned ON by an external energy source. This observation has already been made in prior work in the context of RFID localization [31] and cross-frequency communication [5] for about a 200 MHz bandwidth around 915 MHz ISM band. To further motivate this observation at other frequencies, we measure the frequency response of a commodity RFID tag at all frequencies ranging from 600 MHz to 2.5

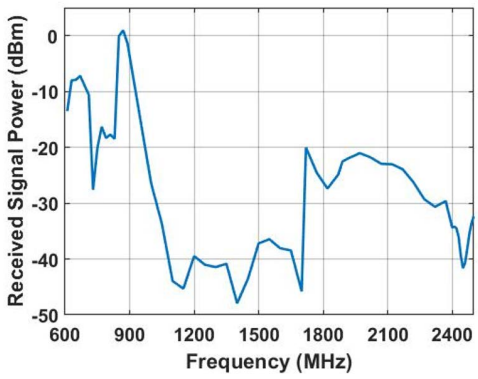


Figure 3: Frequency response of a commodity RFID tag evaluated at frequencies from 600 MHz to 2.4 GHz

GHz (refer Fig. 3). We do this by sending multiple sine tones at different frequencies and then measuring the SNR of RFID backscattered received signal. To enable this backscattering, we ensure that the RFID tag is powered ON at all times using an RFID reader. Further, we performed this experiment in an anechoic chamber to minimize any multipath effects. In addition, the SNR received was appropriately calibrated to remove any attenuation from different filter characteristics at different frequencies. We observe that there are resonant frequencies close to the 500-700 MHz and 1.8-2.4 GHz band for a 915 MHz RFID tag, consistent with observations made in the prior work [5]. Furthermore, the extended transition band around these resonant frequencies allows us to transmit at a wide range of frequencies with only a slight attenuation. There exists a range of frequencies (1.2 GHz to 1.7 GHz) where the frequency response of an RFID tag is very poor. This is due to the impedance mismatch of the RFID tag antenna at those frequencies. Thus, we can use these passive tags to backscatter signals at a wide range of frequencies except for certain frequencies in between where the response is poor.

We will now elaborate on how we exploit this observation to build a wideband battery-free spectrum sensing system below. For ease of exposition, we will assume that there is only a single ambient transmitter source present in the space and all the spectrum measurements correspond to this single transmitter. We will deal with the general case (i.e multiple transmitter sources) in Sec. 5.

4.1 System Setup

Consider the setup shown in Fig. 4 where we have a single tag (represented by 'T') and an RFID reader (represented by 'R') deployed in the space where a spectrum map is desired. A wideband receiver with frequency a range from 600 MHz to 2.4 GHz (not shown in the figure for clarity) is also deployed exactly at the same location as the RFID reader. The

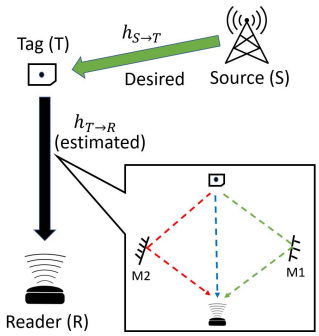


Figure 4: System setup for a single transmitter source present in the environment. We want to indirectly estimate the signal incident at tag T, by eliminating the channel $h_{T\to R}$ from the signal received at the wideband receiver R

RFID reader acts as a power source for the RFID tag and the wideband receiver collects signal measurements at all frequencies.

Now, given an ambient transmitter source (denoted by 'S' in Fig. 4 and described as 'source' hereafter) at a frequency f, the received signal at the wideband receiver can have 2 channels - 1) direct channel from the source to the receiver (S->R) and 2) the channel which goes through the RFID tag to the receiver (S->T->R). Since the RFID tag is powered ON, the switching of its antenna impedance also modulates the source signal incident on the tag which can then be captured by the wideband receiver R allowing it to disambiguate this channel from the direct channel. (specifically, we get $h_{S\to T}(f)\times h_{T\to R}(f)\times x$ where x is the transmit source signal).

However, to create a spatial spectrum map, we need to measure the signal power incident at the RFID tag which is given by $|h_{S\to T}(f)\times x|$. Thus, we need to eliminate the channel effect of the direct path between the tag T and the receiver R ($h_{T\to R}(f)$) from the measured signal $h_{S\to T}(f)\times h_{T\to R}(f)\times x$. This allows us to indirectly measure $h_{S\to T}(f)\times x$, which can then be further interpolated across all tags present in the space to create a spectrum map. To achieve this elimination, we first need to estimate the channel between the receiver R and the tag T at the source frequency ($h_{T\to R}(f)$) and then eliminate this from the measured channel at the receiver. We describe how we do this in the steps mentioned below.

4.2 Receiver-Tag Channel Estimation

A naïve way to estimate the Receiver-Tag channel at a frequency f could be to transmit a sine wave at this frequency from the receiver location and receive the backscattered signal response from the tag. The round-trip channel would then be given by $h^2_{T\to R}(f)$, taking the square root of which

provides us with $h_{T\to R}(f)$. However, this method has several disadvantages. First, it incurs an additional overhead to measure the channel between the receiver and a tag at the source transmitter frequency every time the source pops up. A possible workaround could be to calibrate the system at the space where it is deployed and store the receiver to tag channel information at all frequencies. However, these measurements can quickly become stale due to the dynamic nature of the channel. Second, even if we are to accept the overhead, this method requires us to transmit sine waves at the source frequency we want to measure, which adds interference to the already existing transmission from the source. This completely goes against our goal of sensing the spectrum in the desired space as it will give us an erroneous spectrum measurements at the source frequency. Thus, we need an efficient (with low or no overhead) and an interference-free method to find the channel between the tag T and the receiver R at an arbitrary source transmitter frequency f.

Before we move ahead, note that the commodity RFID reader present at the receiver location operates on the 902-928 MHz ISM band to power ON and communicate with the RFID tag. Furthermore, FCC regulations in the US dictates that the RFID reader has to hop multiple frequencies in the ISM band to communicate with the tag.

Our approach: The main disadvantage of the naïve approach earlier was the extra overhead of transmission from the receiver location at all frequencies. Yet, we observe that there is a certain transmission that is ON at all times, i.e. the RFID reader signal. The RFID reader at the 902-928 MHz ISM band also hops in frequency within this band. This diversity in frequency allows us to model the multipath present in the environment, which when generalized to other frequencies can be used to estimate any channel at that frequency. The key challenge in doing that is to decouple a large number of signal paths using channel measurements from a finite number of frequencies. Fortunately, our results in Sec. 7 demonstrate that wireless channels tend to have a small number of dominant paths and as a result, *RFIMap* can exploit this sparsity to identify dominant paths using only a finite number of frequencies.

To model the multipath present in the environment, *RFIMap* uses a Maximum Likelihood approach to identify the best propagation characteristics that fit the observed channels at multiple frequencies. For each tag, *RFIMap* iterates over a set of m reflector coordinates (x_i, y_i, z_i) for $i = 1, 2...m$ which denotes the candidate locations of the reflectors present in the environment. Using this set of candidate reflector coordinates, *RFIMap* then calculates the optimal phase shifts and attenuations for each assumed reflector. *RFIMap* then uses the set of candidate reflector coordinates,

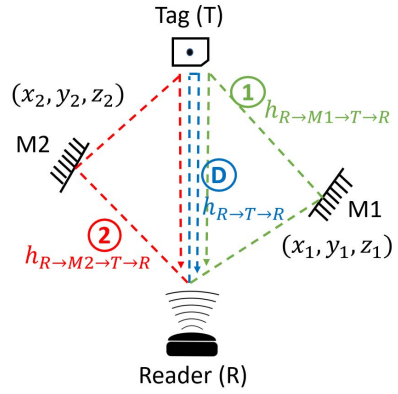


Figure 5: Estimating the channel between the reader and the tag at any arbitrary frequency by modeling multipath using 915 MHz RFID reader transmissions

optimal phase shifts and attenuations to find the optimal reflector locations which best fit the channels at all frequencies.

Mathematically, given the tag T location, (x_T, y_T, z_T), the reader/receiver R location, (x_R, y_R, z_R) and reflectors location (x_i, y_i, z_i) for $i = 1, .., m$ (Refer to Fig. 5, $m = 2$ in this figure; $m = 6$ in our implementation, refer to Sec. 7.2 for the reason), for a given frequency $f \in$ [902 MHz, 928 MHz], the measured channel $h_{T\to R}(f)$ between the receiver and the tag is:

$$\begin{aligned} h^2_{T\to R}(f) &= h_{R\to T\to R}(f) + h_{R\to M2\to T\to R}(f) + \\ &\qquad h_{R\to M1\to T\to R}(f) \\ &= h_{Direct}(f)h_{Direct}(f) + h_{Direct}(f)h_{T\to M_1\to R}(f) + \\ &\qquad h_{Direct}(f)h_{T\to M_2\to R}(f) \end{aligned}$$

Generally, with m reflectors:

$$h^2_{T\to R}(f) = \frac{\lambda_f^2}{d_{TR}^2} e^{-4\pi j \frac{d_{TR}}{\lambda_f}} + \sum_{i=2}^{m+1} \frac{a_{i-1}\lambda_f^2}{d_{TR}d_{TM_iR}} e^{-2\pi j \frac{(d_{TR}+d_{TM_iR})}{\lambda_f}} \quad (1)$$

where $d_{TR} = ||(x_T, y_T, z_T) - (x_R, y_R, z_R)||$ represents the distance between the Tag and the Reader, $d_{TM_iR} = ||(x_T, y_T, z_T) - (x_i, y_i, z_i)|| + ||(x_R, y_R, z_R) - (x_i, y_i, z_i)||$ is the path distance traversed by the signal going through the i^{th} reflector, a_{i-1} is the reflection coefficient of the i^{th} reflector, λ_f is the wavelength at the frequency f, and $j = \sqrt{-1}$.

We have made three simplifying assumptions here: (1) The reflectors present in the environment are large and therefore common for all frequencies (2) Reflectors are planar and infinite (an assumption we can potentially relax as described at the end of this section) (3) Paths with more than one reflection are severely attenuated and do not contribute to the channel model. The validity of our assumptions is discussed later in the section.

Extending Eqn. 1 to n hopped frequencies in the 902-928 MHz ISM band, we can formulate the following minimization problem which tries to find the complex a_i values based on how well they fit the measured channels at all frequencies:

$$\min_{\mathbf{a}} \left\| \left[h^2_{T\to R}(f_k)\right]_{1\times n} - [\mathbf{a}]_{1\times(m+1)}\, H_{(m+1)\times n} \right\|$$

where

$$H_{1,k} = \left[\frac{\lambda_k^2}{d_{TR}^2} e^{-4\pi j \frac{d_{TR}}{\lambda_k}} \right]_{k=1\ldots n}$$

and

$$H_{i,k} = \left[\frac{\lambda_k^2}{d_{TR} d_{TM_iR}} e^{-2\pi j \frac{(d_{TR}+d_{TM_iR})}{\lambda_k}} \right]_{i=2\ldots(m+1);k=1\ldots n}$$

Given d_{TR} and d_{TM_iR}, the above optimization can be solved in close form using a least squares fit:

$$\mathbf{a}^{est} = \left[h^2_{T\to R}(f_k)\right]_{1\times n} (H^\top H)^{-1} H^\top \tag{2}$$

Now, we can estimate the goodness of fit of the assumed reflectors locations $(x_i, y_i, z_i); i = 1, .., m$ based on how well they fit the observed channels. We define the goodness-of-fit of reflector coordinates as:

$$G((x_i, y_i, z_i)_{i=1\ldots m}) = 1/\left\| \left[h^2_{T\to R}(f_k)\right]_{k=1\ldots n} - \mathbf{a}^{est} H \right\|$$

Thus, our problem of modelling the multipath reduces to finding the set of coordinates of the reflectors in the geographical domain $\mathfrak{D}$, which gives the best performance in the goodness-of-fit. Specifically,

$$M_{opt} = \underset{\{(x_i,y_i,z_i)_{i=1\ldots M} \in \mathfrak{D}}{\operatorname{argmax}} G((x_i, y_i, z_i)_{i=1\ldots m})$$

Note here that this optimization is performed for every tag individually. This is done to ensure that we only model the dominant reflectors for every tag. These dominant reflectors are likely to lie very close to the tag's location and thus, a dominant reflector for a particular tag can be a weak reflector for another tag, with no or minimal contribution to its channel estimate.

Having estimated the reflector locations for a particular tag in the environment, *RFIMap* can now estimate the channel between the wideband receiver and the tag at any other source transmitter frequency f. Specifically, we now have the estimate $h^{est}_{T\to R}(f)$ given by:

$$h^{est}_{T\to R}(f) = \frac{\lambda_f}{d_{TR}} e^{-2\pi j \frac{d_{TR}}{\lambda_f}} + \sum_{i=2}^{m+1} \frac{a^{est}_{i-1}\lambda_f}{d_{TM_i^{opt}R}} e^{-2\pi j \frac{d_{TM_i^{opt}R}}{\lambda_f}}$$

Modeling varying tag characteristics across frequencies: The RFID tag can show varying reflection characteristics across frequencies due to changing impedance of the tag antenna across these frequencies. *RFIMap* tackles these variations in the calibration phase itself. Since we perform calibration for each frequency, the frequency-varying tag characteristics can directly and separately be modeled.

Sensing spectrum at 915 MHz ISM band: One may ask if *RFIMap* is using the 902-928 MHz ISM band to estimate channels at other frequencies, then how does it sense transmitters within this ISM band? This is done by choosing the hopping frequencies carefully. The wideband receiver co-located with the RFID reader can instruct the reader on the frequencies to hop to by looking at its own spectrum measurements.

Dominant reflectors close to each other: For many indoor scenarios, it is possible to have multiple dominant reflectors which are very close to each other and cannot be disambiguated using the hopped frequencies in the 900 MHz ISM band because of the limited 26 MHz bandwidth. We note that *RFIMap* remedies the impact of this limited bandwidth to an extent, by making a sparsity assumption on multipath – i.e. modeling a few dominant reflectors as opposed to all reflectors. Our results show that this super-resolution approach helps mitigate the impact of multipath to an extent, albeit could still impact accuracy in environments with densely spaced reflectors. To tackle such cases, *RFIMap* can be extended to replace the off-the-shelf RFID reader with a wideband receiver emulating an RFID reader that hops on TV whitespace frequencies as well as 915 MHz ISM. This extra bandwidth improves the resolution and allows more multipath reflectors to be disambiguated at the expense of latency in hopping a few extra frequencies (see Sec. 7.2). It is worth mentioning that *RFIMap* checks TV whitespace databases every day and uses only the vacant frequencies.

Multiple, Non-Linear, and Finite Reflectors: We have assumed that the reflectors in the environment are linear. While this may not be true in the real world, multiple reflections off of a non-linear reflector can be modeled as a single composite linear reflector. Note here that a signal with more than one reflection is ignored in our formulation as such reflections suffer from a quite high attenuation. We also assumed that the reflectors we have are planar and infinite. To encode the finite nature of the reflectors, each reflector can be composed of a set of finite points and these points can be added as extra variables in the optimization formulation. This will lead to an increase in search space and a possible solution can be found with a moderate increase in computational complexity.

4.3 Signal Power estimation at the tag

Now, given an ambient source transmitter S transmitting at a frequency f_s, the wideband receiver can distinguish the signal coming from the tag from the direct path by using the tag's standard RN16 preamble. Furthermore, since every commodity RFID tag has a unique EPC (i.e. unique ID),

the wideband receiver can easily distinguish the signals received from every tag in the case of multiple tags. Thus, we can write the received signal from every tag T_t:

$$y_R^t(f_s) = h_{S\to T_t}(f_s)h_{T_t\to R}(f_s)x \quad (3)$$

$\forall t = 1 \ldots g$, where x is the transmit source signal and g is the total number of tags. Using our Receiver-Tag Channel estimation algorithm, for every tag T_t, we estimate $h^{est}_{T_t\to R}(f_s)$.

Dividing Eq. 3 by this quantity, we can get the estimated received signal at tag T_t:

$$y_t^{est}(f_s) = h_{S\to T_t}(f_s)x \quad (4)$$

If we take the $abs(y_t^{est}(f_s))$, we get the estimated signal power incident at the tag T_t. In the following section, we detail how these measurements can be further interpolated to create a spectrum map.

5 MULTIPATH-AWARE INTERPOLATION

There has been a plethora of work in developing spatial spectrum sensing systems in the literature [34, 38], where researchers try to create a spectrum map over an area by deploying multiple sensors at different locations. However, these systems lack the spatial diversity required to accurately generate spectrum maps for an area. This can be attributed to the limited number of deployed spectrum sensors (due to cost, power etc.), which constrains the total information we can get from these spatially distributed systems. *RFIMap* tackles this problem by replacing conventional spectrum sensors such as SDRs with countless cheap and battery-free RFID tags and distributing them in the desired space, allowing it to gain more spatial information as compared to conventional systems. Thus, in this section, we want to exploit this rich spatial information to create a dense and accurate spectrum map over the whole area.

In the literature, various interpolation techniques such as nearest neighbors, linear, cubic interpolation, etc. have been extensively used to estimate spectrum measurements at any desired location. However, these techniques cannot model multipath signal propagation indoors with sudden variations of the received signal over short distances. *RFIMap* instead, builds on the multipath model generated in Sec. 4, to interpolate measurements at any location taking the environment's effect into account. In other words, since we already know the location of major reflectors around a given location, we can accurately estimate the effect of these reflectors on the signal power at a desired location.

The rest of this section describes two key challenges in using this multipath modeling to perform interpolation at new locations. First, *RFIMap* estimates the unknown location of the transmitting source using the multipath model we developed in the Sec. 4. Second, *RFIMap* uses this location and the same multipath model to interpolate the channel at the desired location. We describe both these steps below.

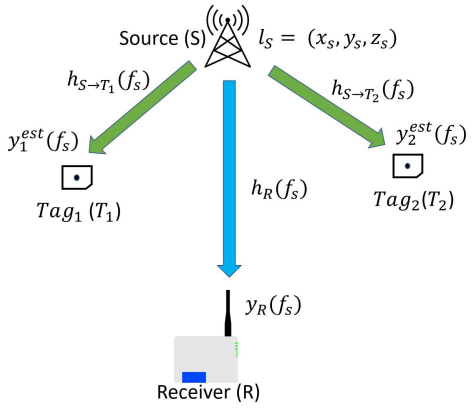


Figure 6: *RFIMap*'s multipath aware interpolation. *RFIMap* first estimates the location of the source l_S and then estimates the signal power at any queried location using the multipath model in Sec. 4.

5.1 Localization of the transmitter source

Because of the multipath model estimated in Sec. 4, we know the location of all the dominant reflectors present in the environment for every tag. We also get the estimated received signal at every tag location. *RFIMap* then uses these received signals to calculate multiple relative channels between every tag and the source transmitter relative to the wideband receiver channel and then trilaterates the location of the transmitter source by removing the effects of the estimated reflectors from the relative channels.

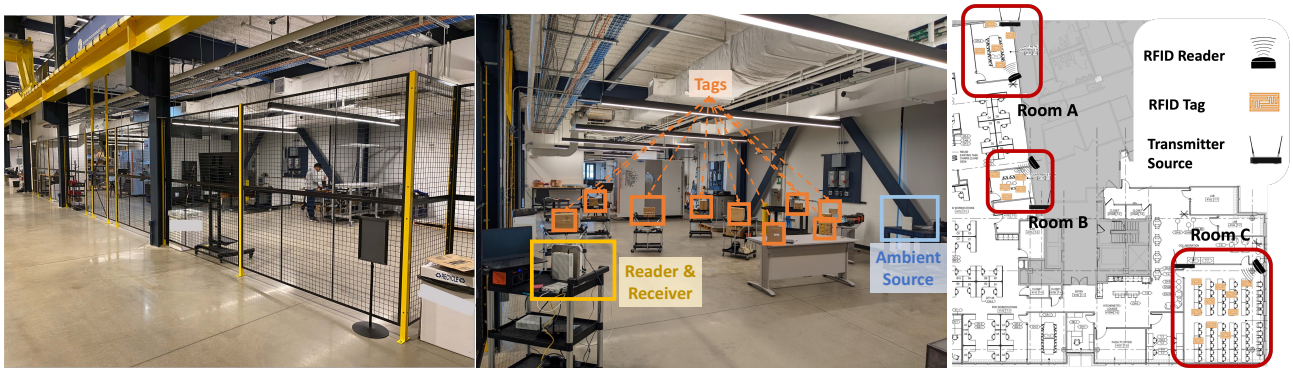
To understand this mathematically, consider Fig. 6. From Eq. 4, we have the estimated received signal at tag T_t as:

$$y_t^{est}(f_s) = h_{S\to T_t}(f_s)x$$

$\forall t = 1 \ldots g$, where g is the total number of tags, f_s is the frequency of transmission from the source S and x is the unknown transmit signal. Taking the direct signal received at the wideband receiver (specifically, given by $y_R(f_s) = h_R(f_s)x$) as the reference, we can estimate the relative channel at every tag T_t given by (assuming noise power is negligible as compared to the signals received):

$$h^t_{rel}(f_s) = \frac{h_{S\to T_t}(f_s)}{h_R(f_s)} \approx \frac{y_t^{est}(f_s)}{y_R(f_s)}$$

$\forall t = 1 \ldots g$. Note here that this relative channel also eliminates effects of the frequency offset between the ambient source and the wideband receiver. Now, since we know the location and characteristics of the reflectors (given M^t_{opt} and $\mathbf{a}^t_{est}$ for every tag from Sec. 4), we find the location of the



(a) (b) (c)

Figure 7: We deploy our system on different testbeds of different sizes and shapes: (a) Our industrial setting. (b) Our industrial testbed deployment. (b) Different conference rooms in a university building.

source transmitter by solving this optimization problem:

$$l_S = \arg\min \sum_t \left\| h^t_{rel}(f_s) - h^{est}_{rel}(f_s, (M^t_{opt}, \mathbf{a}^t_{est}), l_s, l_t) \right\|^2 \quad (5)$$

where $h^{est}_{rel}(f_s, (M^t_{opt}, \mathbf{a}^t_{est}), l_s, l_t)$ can be easily estimated at a given frequency f_s for a candidate transmitter location $l_s = (x_s, y_s, z_s)$, tag T_t location $l_t = (x_t, y_t, z_t)$ and the given reflector locations and characteristics $(M^t_{opt}, \mathbf{a}^t_{est})$. This optimization problem is then solved using the Nelder-Mead simplex algorithm [23].

5.2 Interpolation at Query Location

Next, given a queried location l_Q, where the spectrum measurement is required, we first find the closest tag to the queried location termed as t_{opt} out of all tags present in the environment. Assuming that the queried location shares the same reflectors as the reflectors for the closest tag t_{opt}, we can write:

$$y_{l_Q}(f_s) = h^{est}(f_s, (M^{t_{opt}}_{opt}, \mathbf{a}^t_{est}), l_S, l_Q)x$$

The above quantity, therefore, represents the desired spectrum estimate at locations even where tags are not deployed. *RFIMap* therefore, allows rich visualizations of spatial RF signal power measurements that are significantly denser than the deployment granularity of the tags.

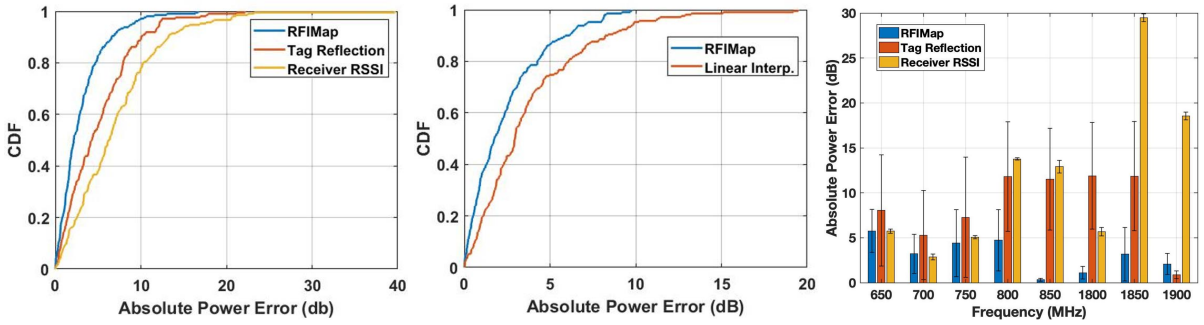
Presence of multiple transmitter sources: The above analysis assumes that there is only a single transmitter source at a frequency f_s in the environment. What if multiple transmitter sources are transmitting at the same frequency? Even if multiple sources are simultaneously transmitting signals at the query frequency, our formulation approximates and combines these source locations into a virtual source location. *RFIMap* then uses this estimated source location and the estimated locations of major reflectors, to find the received signal power at the query location l_q. We validate this capability of *RFIMap* at 2.4GHz by predicting the signal received at various indoor locations while a transmitter source and ambient WiFi access points exist.

6 IMPLEMENTATION AND EVALUATION

We implement *RFIMap* using a commodity RFID reader[2] and multiple commodity RFID tags (Alien ALN 9640 [1]). The reader is configured to excite and query the RFID tag by using Java Octane SDK[3]. Commodity RFID readers continuously frequency hop in the 902-928MHz as per US FCC regulations. The ambient transmitter source and the wideband receiver are implemented using multiple Ettus USRP N210s. Although USRP N210 can only support a maximum of 40 MHz bandwidth, we emulate the wideband behavior by frequency hopping across all frequencies where *RFIMap* can work. We use circularly polarized panel antenna for the reader and omnidirectional antennas at different frequencies such as TV whitespaces, WiFi, and 915 MHz ISM band for our wideband receiver.

Testbeds. We evaluate our system in diverse indoor industrial and university settings. In a university setting (see Fig. 7c), we deployed 5 tags each in two different rooms: room A (6.9 m × 4.8 m × 3.4 m) and room B (4.7 m × 3.5 m × 3.4 m), and 10 tags in room C (8.9 m × 11.4 m × 2.8 m). In the industrial setting, we set up 10 tags in an enclosed area (6 m × 15 m × 5 m, see Fig. 7b).

Ground Truth & Baseline. We co-locate each tag with an Ettus USRP N210 as a ground truth receiver to measure the received signal power at that location. For ground truth location of the reader and the tags, we use a Bosch laser rangefinder to survey our testbeds. We use absolute power error as a metric for evaluating our estimated received power at the tags and other locations. We use two baselines to compare with *RFIMap*: a) **Tag Reflection**: use the tag's reflection power received at our receiver as an approximation of the power of the source signal received at



(a) (b) (c)

Figure 8: Overall Results: (a) CDF of the absolute error in predicting the signal power incident at all the deployed RFID tags with the source operating at 2.4 GHz band. (b) CDF of the absolute error in the multipath aware spatial interpolation of the signal power at multiple random locations with the source operating at 2.4 GHz band with the baseline using *RFIMap* tag measurements to interpolate. (c) Absolute error in predicting the signal power incident at RFID tags with the source operating at all frequencies from 650 MHz to 2 GHz.

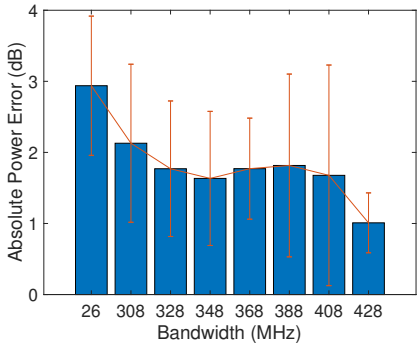


Figure 9: Effect of increasing the bandwidth on the absolute power error.

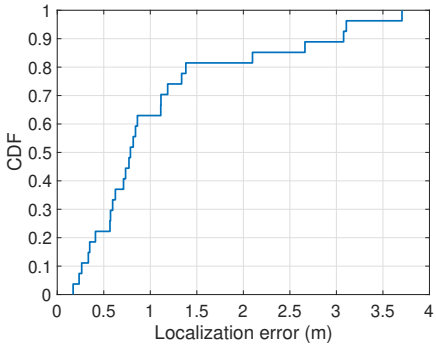


Figure 10: Transmitter source Localization error at various frequencies.

that tag; b) **Receiver RSSI**: use received power at our receiver from the direct signal as an approximation of the power of the source signal received at the tag. We also compare the interpolation algorithm with a standard linear interpolation technique.

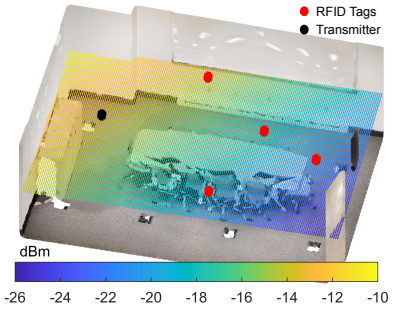
Calibration. Due to the different filter characteristics of different USRP receivers, the power measurements received at each frequency are very different from the estimated power. Therefore, we need to conduct a calibration experiment, where both the ground truth USRP and the receiver USRP are colocated, and receiving the same transmission signal simultaneously. Then, we use the difference in power between the two received signals across frequencies as offsets to be added in our calculations when comparing measurements from the two devices. Note that this one-time calibration has to be performed at all frequencies separately for each tag.

Running Time. We run our code on an AMD 3 GHz 12-core processor that it takes 4.5 s to estimate multipath in the environment (an offline task not to be performed frequently) and 0.9 ms to calculate the incident power at the tag.

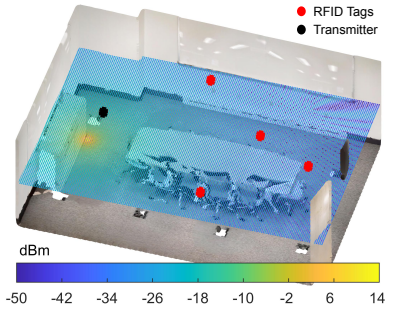
7 EXPERIMENTAL RESULTS

7.1 Overall System Performance

Estimated Received Power at Tags. We collect signal measurements from the wideband receiver from a source at 2.4 GHz. By using our signal power estimation algorithm in Sec. 4, we compare our estimate of the signal power to the ground truth. The ground truth was collected by placing a USRP N210 at the location of each tag receiving at the source frequency. The CDF of the error between our estimate and the ground truth is shown in Fig. 8a. *RFIMap* achieves 2.15 dB median error, and a 95% percentile error of 8.9 dB, compared to 4.26 dB median error, and a 95% percentile error of 12.1 dB for tag reflection baseline and 6.27 dB median error, and a 95% percentile of 17.6 dB for tag reflection baseline. These results confirm the validity of the multipath model



(a) Linear interpolation of the signal power estimation at tags suffer from inaccurate spectrum measurements



(b) Multipath-aware interpolation to generate a spectrum map with a peak close to the true transmitter location

Figure 11: Spectrum maps for a conference room using different techniques

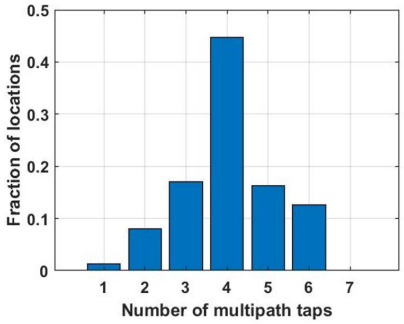


Figure 12: Number of multipath taps in different locations

generated using our signal power estimation algorithm at the tag.

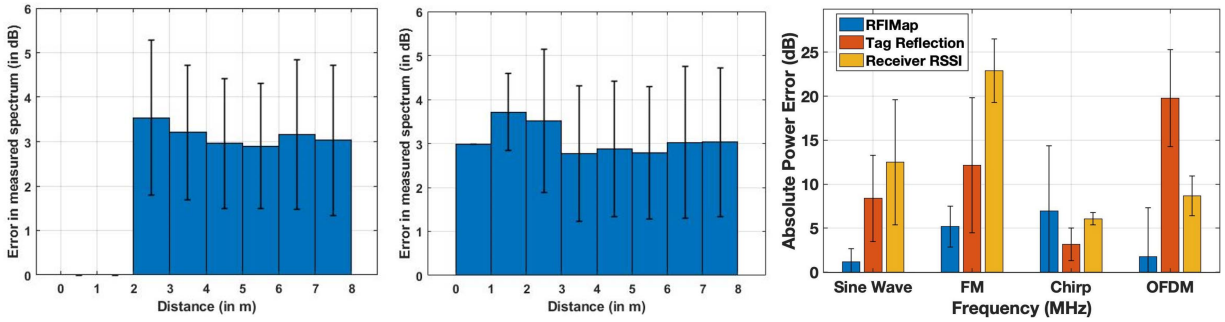
Interpolation Error. Next, using our existing multipath model of the environment, *RFIMap* can estimate the spectrum power at any arbitrary location by first, performing localization of the ambient transmitter and then using the multipath model to estimate signal power at the queried location. We compare the estimated power at the queried location with a ground truth receiver operating at the source frequency. Fig. 8b represents the CDF of the absolute power error between our estimated signal power and the ground truth. The baseline is calculated using a simple linear interpolation of the estimated signal power at all tags. Moreover, we also depict the estimated signal power and show a system-generated visualization of the spectrum map using both *RFIMap* and our baseline at one of our testbeds shown in Fig. 11. *RFIMap* shows a median interpolation error of 1.8 dB and 95% percentile of 7.8 dB compared to 3 dB median error, and 95% percentile of 11.2 dB using linear interpolation.

Wideband Sensing. In this experiment, we show that *RFIMap* is capable of detecting tag reflections and predicting received power at these tags for a wideband of frequencies. To show this, we apply our signal power estimation algorithm across all frequencies to estimate the signal power at a tag by varying the source transmitter frequency from 650 MHz to 2 GHz. Fig. 8c confirms that *RFIMap* can sense large swath of frequency bands showing less than 5 dB error. It is worth mentioning that accuracy of *RFIMap* is limited by the reflectivity of the tag at different frequencies which we presented in Fig. 3 as it performs the best in the 915 MHz ISM band and the 1.8-2 GHz band with less than 5 dB of error.

7.2 Other System parameters

Hopping frequencies at TV white spaces. To mitigate dominant reflectors close together, *RFIMap* hops over TV whitespaces to improve the resolution and allow these reflectors to be disambiguated. To study hopping over the TV whitespaces, we replace the commodity RFID reader with a wideband receiver (a USRP in our implementation) and emulate the RFID protocol behavior at the TV whitespaces. Fig. 9 illustrates this effect by increasing the emulated bandwidth (resulting from an increase in the number of frequencies hopped) for multipath estimation and shows the corresponding error for predicting the incident power at the tags at the 2.4 GHz band. As expected, we see a decreasing trend of the error as we increase the effective bandwidth. However, as the number of major reflectors are limited (as we show in the next section), the error saturates after separating these major reflectors using enough bandwidth. It is worth mentioning that even with the 26 MHz bandwidth at the 915 MHz band, *RFIMap* gets an approximation of the location of the reflectors in the environment and can estimate reasonably how the signal attenuates from the tag to the reader, owing to its sparsity assumption that enables super-resolution multipath disambiguation.

Locating transmitter source. Part of *RFIMap* is to locate the transmitter source to better interpolate its interference profile at different locations other than the deployed tags as well as finding out the source of that interference. RF interference is not always caused by a malicious or known transmitter, sometimes is caused by malfunctioning electronic devices. In Fig. 10, we show the localization error for a transmitter source. We conduct this experiment in which we vary the location of the transmitter in various environments as well as varying the transmission frequency. *RFIMap* can achieve a median error of 0.78 m and a 95% percentile of



(a) (b) (c)

Figure 13: System Analysis Results: (a) Mean Power Error with Distance from the Reader (b) Mean Power Error with Distance from the Transmitter source (c) Absolute Power Error with different signals.

3.2 m. It is worth mentioning here that there exist ambient sources, that transmit at the same frequency as our transmitter source, which degrades localization accuracy.

Sparsity assumption of multipath. To validate the sparsity assumption of multipath in Sec. 4.2, we transmit wideband chirps of about 20 MHz bandwidth at 915 MHz ISM band using a USRP N210 in multiple different indoor environments like a kitchen, conference room, living room, etc. Another USRP is used to receive these wideband chirps which are correlated with the transmitted chirp to estimate the multipath channel. Fig. 12 represents the histogram of the number of channel taps obtained using this correlation across all the environments. We observe that all the locations had at most 6 channel taps which represent the number of multipath reflectors present in the environment. Thus, for all of our tags we use the number of reflectors m to be equal to 6 and we estimate the reflector locations using our algorithm in Sec. 4 by hopping 50 frequencies in the ISM band.

Tag to Reader Distance. We varied the distance between an RFID tag and the RFID reader for a fixed source location and estimated the signal power incident at the tag at the source transmitter frequency. We compare this estimation with the signal power obtained through a USRP co-located at the tag location. We construct a histogram of these different distances and take the average of all estimated power lying inside each bin. Fig. 13a shows how the mean power error of the estimated received signal varies with the distance between a tag and the reader. The mean error is around 3 dB with no clear trend while varying distance between tag and reader up to 8 m as the error is mainly related to reflector characteristics at each location.

Source to Tag Distance. Similarly, we now vary the distance between the transmitter source and the tag keeping the RFID reader at a fixed location. The estimated signal power at the tag was compared to the ground truth signal power obtained using a USRP placed at the tag location. Fig. 13b illustrates the effect of varying the distance between a tag and the transmitter source. We observe that the mean error is 2.8 to 3.7 dB with an increase in error variance when increasing the distance between the tag and the source up to 8 m. This happens because of the decrease in SNR at the tag location with the increase in distance, which impacts variance.

Source Signal Modulation. We also evaluate our system for different signal modulations at the source transmitter. Fig. 13c shows how the modulation of the source signal can affect the error of estimated signal power at the tags. We illustrate this effect for four different source signals: sine wave, FM waves (used in SigFox, NB-IoT), Chirp Spread Spectrum Modulations (used in LoRa), and OFDM modulations (Cellular and WiFi). The absolute power error is the lowest value sine waves while error increases to the maximum for Chirp Spread Spectrum Modulation. This is due to the frequency-varying nature of the CSS waves, making it difficult for the wideband receiver to disambiguate the amplitude variations due to the RFID tag. The other modulations presented can be thought of more naturally as combinations of multiple sine tones and thus perform quite similar to sine waves.

8 DISCUSSION AND LIMITATIONS

We discuss open areas for improving *RFIMap*.

Limited RFID UHF Bandwidth: The Ultra-high frequency RFIDs have a limited bandwidth of 26 MHz, which can limit the resolution (11.5m) of RFIMap to accurately locate the reflectors in the environment, especially when the major reflectors are closer than this resolution. To break this limit, our reader can be extended to hop over the TV whitespaces

available from 470 MHz to 697 MHz to model the multipath in the environment.

RFID Radar Cross Section: The differential radar cross section of a tag that controls the power of the modulated backscattered tag signal can vary significantly based on the incident signal received at the tag [7, 35]. In other words, the on-to-off modulation difference that the tag encodes on top of the reader signal can vary based on the power of the received reader signal. However, this doesn't apply to the transmitter source signal and our reader can see variations of the modulated signal that is only controlled by the reader hopping behavior at the 915 MHz band. In contrast, RFIMap considers the reflected signal path loss from each tag which can be inferred from the absolute power reflected off the tag at the frequencies that the reader hops at.

Tag orientation to the transmitter: At the setup phase of the tags, given that the location of the transmitter is unknown, each tag orientation relative to the transmitter may impact wireless signal measurements. Since the antennas of these RFID tags are semi-directional, a transmitter may reside in or near the nulls of some of these tags. We can address this problem by placing multiple tags in different orientations at approximately the same location given the small size, low cost of these tags, and their ability to scale spatially. For example, we can direct the orientation of one tag to cover the nulls of the other tag, targeting omni-directional angular sensitivity.

Orientation of the reader and tags: Since the commodity RFID reader antennas are directional, *RFIMap* requires the deployed tags to face the RFID reader so that enough power can be incident on the tag to turn it ON. Thus, this limits the deployment of RFID readers to walls only with a wide field of view covering all the RFID tags deployed in the space. This is a reasonable assumption as generally most of the commercial RFID readers are deployed on walls with a wide field of view.

Frequency scanning of the wideband receiver: *RFIMap* use off-the-shelf USRP with tens of MHz of instantaneous bandwidth that allow for sequentially scanning a wide spectrum. A USRP generally needs to take more than 60 seconds to scan 1 GHz of bandwidth, which provides comparatively low temporal resolution when there are multiple desired frequencies across wideband. Future work can replace USRPs with recent software radio platforms that allow for rapid wideband sensing [15] or deploying other wideband spectrum sensors (e.g. S^3 [14]) as receivers.

Sensing range: The range of our system is the range of an RFID reader which is around 15 meters. This is limited by the signal attenuation of the tag response. For indoor room-scale deployments, this limitation is quite reasonable. However, for a wide-area spectrum map, *RFIMap* would require multiple readers to be deployed in the area. A reasonable solution for this problem is to deploy low-cost OTS readers, along with low cost receivers that ease the deployment *RFIMap* over large spaces. An alternative would be to co-optimize *RFIMap* with recent long-range RFID solutions [48].

Dependency on the reader type: Other than differences in the readers' range, *RFIMap* is agnostic to the type of the commercial reader. *RFIMap* can perform its tasks as long as the tags are energized and queried, which in turn enables the tags to start to reflect ambient signals.

Receiver cost: While building and evaluating *RFIMap*, we use a USRP as a wideband receiver. However, this can be replaced, in production, by any low-cost SDR platform[34] or receiver. The choice of what type of receiver to be used is directly related to the application in mind. For example, in a smart manufacturing scenario, a narrowband receiver is required to be tuned only to the frequency band in which the machinery communicates at. On the other hand, a wideband receiver is needed for enforcing radio quiet zones.

Extreme/Dynamic multipath: *RFIMap* chooses to model the multipath as a finite number of static dominant reflectors. However, this assumption may not hold under dense multipath. In these situations, the number of surrounding dominant reflectors can be much higher than our parameters in the optimization algorithm for channel estimation (Sec. 4.2). Performing accurate model estimation based on the RFID tag's response in such scenarios continues to remain an open problem for future work.

9 CONCLUSION

This paper present *RFIMap*, the first system that builds wideband fine-grained spectrum map using COTS battery-free RFID tags. *RFIMap* achieves this by receiving and processing the backscatter signal across a wide spectrum of distributed deployed RFID tags. We show how to obtain the signal power measurement at each tag of different frequencies by modeling signal paths using the 915 MHz ISM band transmission of the RFID reader. We deployed and evaluated *RFIMap* in diverse indoor environments, including industrial and office spaces. Comprehensive experiments demonstrate the potential of employing *RFIMap* for the various applications desiring a dense RF spectrum map, such as monitoring ambient interference in smart manufacturing and airplanes. We believe that further improving time resolution and sensing range remain important problems for future work.

Acknowledgments: We thank NSF (2030154, 2106921, 2007786, 1942902, 2111751), ARL, DARPA-TRIAD and MFI for their support.

REFERENCES

[1] [n. d.]. ALIEN passive tags. https://www.alientechnology.com/products/tags/squiggle/. ([n. d.]). Accessed: 2023-2-9.

[2] [n. d.]. Impinj Speedway RFID Reader. https://www.impinj.com/products/readers/impinj-speedway. ([n. d.]). Accessed: 2021-3-10.

[3] [n. d.]. Octane SDK. https://support.impinj.com/hc/en-us/articles/202755268-Octane-SDK. ([n. d.]). Accessed: 2021-4-15.

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

[5] Zhenlin An, Qiongzheng Lin, and Lei Yang. 2018. Cross-Frequency Communication: Near-Field Identification of UHF RFIDs with WiFi!. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. Association for Computing Machinery, New York, NY, USA, 623–638. https://doi.org/10.1145/3241539.3241569

[6] Arjun Bakshi, Yifan Mao, Kannan Srinivasan, and Srinivasan Parthasarathy. 2019. Fast and Efficient Cross Band Channel Prediction Using Machine Learning. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 37, 16 pages. https://doi.org/10.1145/3300061.3345438

[7] Nicolas Barbot, Olivier Rance, and Etienne Perret. 2021. Differential RCS of Modulated Tag. *IEEE Transactions on Antennas and Propagation* 69, 9 (2021), 6128–6133. https://doi.org/10.1109/TAP.2021.3060943

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

[9] Michael Buettner, Richa Prasad, Alanson Sample, Daniel Yeager, Ben Greenstein, Joshua R. Smith, and David Wetherall. 2008. RFID Sensor Networks with the Intel WISP. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys '08)*. Association for Computing Machinery, New York, NY, USA, 393–394. https://doi.org/10.1145/1460412.1460468

[10] Han Ding, Chen Qian, Jinsong Han, Ge Wang, Zhiping Jiang, Jizhong Zhao, and Wei Xi. 2016. Device-free detection of approach and departure behaviors using backscatter communication. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 167–177.

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

[12] Gregory D Durgin, Michael A Varner, Mary Ann Weitnauer, John Cressler, Manos M Tentzeris, Alenka Zajic, Saeed Zeinolabedinzadeh, Reza Zekavat, Kaveh Pahlavan, Ulkuhan Guler, et al. 2021. Digital Spectrum Twinning and the Role of RFID and Backscatter Communications in Spectral Sensing. In *2021 IEEE International Conference on RFID Technology and Applications (RFID-TA)*. IEEE, 89–92.

[13] Akshay Gadre, Revathy Narayanan, Anh Luong, Anthony Rowe, Bob Iannucci, and Swarun Kumar. 2020. Frequency Configuration for Low-Power Wide-Area Networks in a Heartbeat. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. USENIX Association, Santa Clara, CA, 339–352. https://www.usenix.org/conference/nsdi20/presentation/gadre

[14] Junfeng Guan, Jitian Zhang, Ruochen Lu, Hyungjoo Seo, Jin Zhou, Songbin Gong, and Haitham Hassanieh. 2021. Efficient Wideband Spectrum Sensing Using MEMS Acoustic Resonators. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. USENIX Association, 809–825. https://www.usenix.org/conference/nsdi21/presentation/guan

[15] Yeswanth Guddeti, Raghav Subbaraman, Moein Khazraee, Aaron Schulman, and Dinesh Bharadia. 2019. SweepSense: Sensing 5 GHz in 5 Milliseconds with Low-cost Radios. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. USENIX Association, Boston, MA, 317–330. https://www.usenix.org/conference/nsdi19/presentation/guddeti

[16] Jeremy Gummeson, James Mccann, Chouchang (JACK) Yang, Damith Ranasinghe, Scott Hudson, and Alanson Sample. 2017. RFID Light Bulb: Enabling Ubiquitous Deployment of Interactive RFID Systems. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 2, Article 12 (jun 2017), 16 pages. https://doi.org/10.1145/3090077

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

[18] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. 2021. Efficient Ambient LoRa Backscatter With On-Off Keying Modulation. *IEEE/ACM Transactions on Networking* (2021).

[19] Haitham Hassanieh, Lixin Shi, Omid Abari, Ezzeldin Hamed, and Dina Katabi. 2014. GHz-wide sensing and decoding using the sparse Fourier transform. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*. 2256–2264. https://doi.org/10.1109/INFOCOM.2014.6848169

[20] Jia Hu, Linling Zhong, Tao Ma, Zhe Ding, and Zhanqi Xu. 2021. Long-Range FM Backscatter Tag With Tunnel Diode. *IEEE Microwave and Wireless Components Letters* 32, 1 (2021), 92–95.

[21] Haotian Jiang, Jiacheng Zhang, Xiuzhen Guo, and Yuan He. 2021. Sense Me on the Ride: Accurate Mobile Sensing over a LoRa Backscatter Channel. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*. 125–137.

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

[23] Jeffrey C Lagarias, James A Reeds, Margaret H Wright, and Paul E Wright. 1998. Convergence properties of the Nelder–Mead simplex method in low dimensions. *SIAM Journal on optimization* 9, 1 (1998), 112–147.

[24] Antonio Lazaro, Marc Lazaro, and Ramon Villarino. 2021. Room-level localization system based on LoRa backscatters. *IEEE Access* 9 (2021), 16004–16018.

[25] Antonio Lazaro, Ramon Villarino, and David Girbau. 2018. A survey of NFC sensors based on energy harvesting for IoT applications. *Sensors* 18, 11 (2018), 3746.

[26] Yilong Li, Yijing Zeng, and Suman Banerjee. 2021. Enabling wideband, mobile spectrum sensing through onboard heterogeneous computing. In *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*. 85–91.

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

[28] Zikun Liu, Gagandeep Singh, Chenren Xu, and Deepak Vasisht. 2021. FIRE: Enabling Reciprocity for FDD MIMO Systems. In *Proceedings of*

the 27th Annual International Conference on Mobile Computing and Networking (MobiCom '21). Association for Computing Machinery, New York, NY, USA, 628–641. https://doi.org/10.1145/3447993.3483275

[29] Zhihong Luo, Qiping Zhang, Yunfei Ma, Manish Singh, and Fadel Adib. 2019. 3D Backscatter Localization for {Fine-Grained} Robotics. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 765–782.

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

[31] Yunfei Ma, Nicholas Selby, and Fadel Adib. 2017. Minding the Billions: Ultra-Wideband Localization for Deployed RFID Tags. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17)*. Association for Computing Machinery, New York, NY, USA, 248–260. https://doi.org/10.1145/3117811.3117833

[32] Mohamed R Mahfouz, Gary To, and Michael J Kuhn. 2012. Smart instruments: Wireless technology invades the operating room. In *2012 IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS)*. IEEE, 33–36.

[33] Truong X Nguyen. 2005. Cumulative interference to aircraft radios from multiple portable electronic devices. In *24th Digital Avionics Systems Conference*, Vol. 2. IEEE, 10–pp.

[34] Ana Nika, Zengbin Zhang, Xia Zhou, Ben Y. Zhao, and Haitao Zheng. 2014. Towards Commoditized Real-Time Spectrum Monitoring. In *Proceedings of the 1st ACM Workshop on Hot Topics in Wireless (HotWireless '14)*. Association for Computing Machinery, New York, NY, USA, 25–30. https://doi.org/10.1145/2643614.2643615

[35] Pavel V Nikitin, KVS Rao, and Roberto D Martinez. 2007. Differential RCS of RFID tag. *Electronics Letters* 43, 8 (2007), 1.

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

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

[38] Damian Pfammatter, Domenico Giustiniano, and Vincent Lenders. 2015. A Software-Defined Sensor Architecture for Large-Scale Wideband Spectrum Monitoring. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks (IPSN '15)*. Association for Computing Machinery, New York, NY, USA, 71–82. https://doi.org/10.1145/2737095.2737119

[39] Moslem Rashidi, Kasra Haghighi, Ashkan Panahi, and Mats Viberg. 2011. A NLLS based sub-nyquist rate spectrum sensing for wideband cognitive radio. In *2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 545–551. https://doi.org/10.1109/DYSPAN.2011.5936245

[40] Lixin Shi, Paramvir Bahl, and Dina Katabi. 2015. Beyond Sensing: Multi-GHz Realtime Spectrum Analytics. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. USENIX Association, Oakland, CA, 159–172. https://www.usenix.org/conference/nsdi15/technical-sessions/presentation/shi

[41] Lixin Shi, Haitham Hassanieh, and Dina Katabi. 2014. D-BigBand: Sensing GHZ-Wide Non-Sparse Spectrum on Commodity Radios. In *Proceedings of the 6th Annual Workshop on Wireless of the Students, by the Students, for the Students (S3 '14)*. Association for Computing Machinery, New York, NY, USA, 13–16. https://doi.org/10.1145/2645884.2645887

[42] Kaumudi Singh, DN Tejeshwini, Sanmay Patel, Sourav Sudhir, Zuhaib M Ahmed, TV Prabhakar, and Joy Kuri. 2020. Localization of Life Safety Vests in an Aircraft Using Backscattering RFID Communication. *IEEE Journal of Radio Frequency Identification* 4, 3 (2020), 234–245.

[43] Phillip Smith, Anh Luong, Shamik Sarkar, Harsimran Singh, Aarti Singh, Neal Patwari, Sneha Kumar Kasera, and Kurt Derr. 2021. A Novel Software Defined Radio for Practical, Mobile Crowd-sourced Spectrum Sensing. *IEEE Transactions on Mobile Computing* (2021), 1–1. https://doi.org/10.1109/TMC.2021.3107409

[44] Deepak Vasisht, Swarun Kumar, Hariharan Rahul, and Dina Katabi. 2016. Eliminating Channel Feedback in Next-Generation Cellular Networks. In *Proceedings of the 2016 ACM SIGCOMM Conference (SIGCOMM '16)*. Association for Computing Machinery, New York, NY, USA, 398–411. https://doi.org/10.1145/2934872.2934895

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

[46] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, and Jizhong Zhao. 2018. Towards Replay-Resilient RFID Authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. Association for Computing Machinery, New York, NY, USA, 385–399. https://doi.org/10.1145/3241539.3241541

[47] Jingxian Wang, Junbo Zhang, Ke Li, Chengfeng Pan, Carmel Majidi, and Swarun Kumar. 2021. Locating everyday objects using nfc textiles. In *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)*. 15–30.

[48] Jingxian Wang, Junbo Zhang, Rajarshi Saha, Haojian Jin, and Swarun Kumar. 2019. Pushing the Range Limits of Commercial Passive RFIDs. In *Proceedings of the 16th USENIX Conference on Networked Systems Design and Implementation (NSDI'19)*. USENIX Association, USA, 301–315.

[49] Chao Yang, Xuyu Wang, and Shiwen Mao. 2019. SparseTag: High-precision backscatter indoor localization with sparse RFID tag arrays. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 1–9.

[50] Hui Yang, Soundar Kumara, Satish TS Bukkapatnam, and Fugee Tsung. 2019. The internet of things for smart manufacturing: A review. *IISE Transactions* 51, 11 (2019), 1190–1216.

[51] Lei Yang, Yao Li, Qiongzheng Lin, Xiang-Yang Li, and Yunhao Liu. 2016. Making sense of mechanical vibration period with sub-millisecond accuracy using backscatter signals. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. 16–28.

[52] Sungro Yoon, Li Erran Li, Soung Chang Liew, Romit Roy Choudhury, Injong Rhee, and Kun Tan. 2013. QuickSense: Fast and energy-efficient channel sensing for dynamic spectrum access networks. In *2013 Proceedings IEEE INFOCOM*. 2247–2255. https://doi.org/10.1109/INFCOM.2013.6567028

[53] Tevfik Yucek and Huseyin Arslan. 2009. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys Tutorials* 11, 1 (2009), 116–130. https://doi.org/10.1109/SURV.2009.090109

[54] Zeinab Zeinalkhani and Amir H. Banihashemi. 2012. Iterative recovery algorithms for compressed sensing of wideband block sparse spectrums. In *2012 IEEE International Conference on Communications (ICC)*. 1630–1634. https://doi.org/10.1109/ICC.2012.6364377

[55] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings*

of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM. 259–271.

[56] Tan Zhang, Ning Leng, and Suman Banerjee. 2014. A vehicle-based measurement framework for enhancing whitespace spectrum databases. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. 17–28.

[57] Xingjian Zhang, Yuan Ma, and Yue Gao. 2016. Adaptively Regularized Compressive Spectrum Sensing from Real-Time Signals to Real-Time Processing. In *2016 IEEE Global Communications Conference (GLOBECOM)*. 1–6. https://doi.org/10.1109/GLOCOM.2016.7841570

[58] Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu, and Ming Zhang. 2020. 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 '20)*. Association for Computing Machinery, New York, NY, USA, 694–707. https://doi.org/10.1145/3387514.3406219