A Portable Handheld Fine-Grained RFID Localization System with Complex-Controlled Polarization

by

Laura Dodds

S.B., Electrical Engineering and Computer Science
Massachusetts Institute of Technology (2021)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2022

Author . . . .
Department of Electrical Engineering and Computer Science
August 6, 2022

Certified by . . . .
Fadel Adib
Associate Professor
Thesis Supervisor

Accepted by . . . .
Katrina LaCurts
Chair, Master of Engineering Theses Committee

A Portable Handheld Fine-Grained RFID Localization System with Complex-Controlled Polarization

by

Laura Dodds

Submitted to the Department of Electrical Engineering and Computer Science
on August 6, 2022, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

There is significant interest in fine-grained RFID localization systems. Existing systems for fine-grained RFID localization require infrastructure support, either in the form of extensive reference tags deployed in the environment or a deployed antenna infrastructure, such as antenna arrays, to localize RFID tags within its radio range. Yet, there remains a need for fine-grained RFID localization solutions that are in a compact, portable, mobile form, that can be held by users as they walk around areas to map them, such as in retail stores, warehouses, or manufacturing plants.

We present the design, implementation, and evaluation of EveryFind, a portable handheld system for fine-grained RFID localization. Our system introduces two key innovations that enable robust, accurate, and real-time localization of RFID tags in challenging environments. The first is *complex-controlled polarization (CCP)*, a mechanism for localizing RFIDs at all orientations through software-controlled polarization of two linearly polarized antennas. The second is *joint tag discovery and localization (JTDL)*, a method for simultaneously localizing and reading tags with zero-overhead regardless of the tag's orientation. Building on these two techniques, we develop an end-to-end handheld system that addresses a number of practical challenges in self-interference cancellation, efficient inventorying, and self-localization. Our evaluation over hundreds of RFID locations demonstrates that EveryFind achieves a median accuracy of few centimeters in each of the x/y/z dimensions and a 90^{th} in practical indoor environments.

Thesis Supervisor: Fadel Adib
Title: Associate Professor

Acknowledgments

To start, I would like to thank everyone in Signal Kinetics. Your friendship and support has made the last year and a half incredibly fun. It has been great to work with and learn from all of you.

Thank you to Prof. Fadel Adib. You have consistently gone above and beyond in your mentorship and guidance, and I am very grateful for your support. Thank you for taking the time to answer all of my questions throughout the last year and a half.

I would also like to thank my family, for answering all of my questions for the past 22 years, and for their continued support throughout my education.

To Holly, thank you for your friendship throughout our time at MIT. I would not have made it without you keeping me sane.

And finally, for always keeping me grounded, I'd like to thank the Signal Kinetics tables (and every other piece of metal in the lab).

The research is sponsored by the National Science Foundation (NSF), the Sloan Research Fellowship, and the MIT Media Lab.

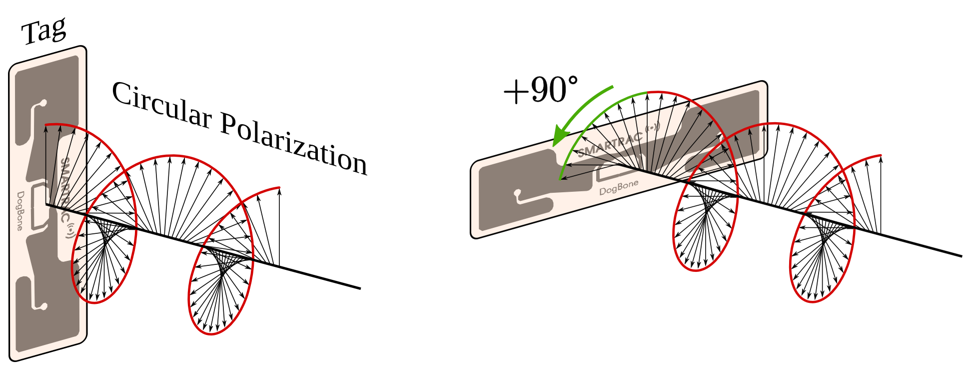
Contents

List of Figures

List of Tables

Chapter 1

Introduction



(a) Phase of Vertical Tag. (b) Phase Offset for Horizontal Tag.

Figure 1-1: Impact of Tag Rotations. (a) shows how a linearly polarized tag will reflect a circularly polarized signal when it is parallel to its polarization. (b) shows that when the tag is rotated, it will reflect the circularly polarized signal at a different point, leading to a phase offset.

Fine-grained RFID localization has attracted much attention from the mobile and sensor computing community, due to its numerous applications spanning retail, manufacturing, warehousing, entertainment, and more [14, 7, 23, 25, 20, 16]. In this thesis, we set out to build an RFID localization system is 1) *portable*, 2) *accurate*, 3) *robust*, and 4) *efficient*. We envision that a user of our system can walk around a typical indoor environment, such as a warehouse or a retail store, carrying a portable device that scans and accurately localizes all RFID-tagged items in its vicinity with fine-grained accuracy (10-20 centimeters). Such a capability would allow retailers, manufacturers, and warehouse operators to map all RFID-tagged items in their buildings, making operational processes such as search, retrieval, and putaway more efficient, and providing them with new analytics and traceability capabilities.

Existing RFID systems fall in two main categories, neither of which can realize the above properties simultaneously. The first consists of state-of-the-art RFID localization systems which leverage bulky antenna arrays [23, 24, 14, 9]; these can achieve high accuracy but need to be deployed as an infrastructure, making them unsuitable for handheld mobility. The second category consists of commercial handheld RFID readers from companies like Zebra, Bluebird, and AsReader [3, 6, 5]; these can be easily held by a user but cannot accurately localize RFIDs as they only detect the presence of tags, not their location. And while there have been proposals to leverage mobility in RFID localization [25, 20, 7, 23, 13], most of these proposals require either moving the reader (or the tag) on predefined trajectories (e.g., by a robot), making them unsuitable for handheld human mobility.

We present EveryFind, a portable handheld RFID localization system that is accurate, robust, and efficient. As a user carrying our device walks around an indoor environment, the device can self-localize, as it reads and localizes RFIDs within its radio range. This information allows it to create digital twins of indoor environments that are populated with the tagged items in 3D space.

A major challenge we faced in developing EveryFind was localizing RFIDs across different orientations. Existing portable RFID readers typically rely on circularly polarized antennas, which allow them to power up and read tags irrespective of their orientation. However, the circular polarization adds an intractable phase to the RFID as it rotates (even if the RFID remains in the same location), which makes localizing it difficult.[1] Specifically, state-of-the-art fine-grained localization systems rely on accurate phase measurements, meaning that phase distortions would make accurate localization very challenging. In principle, one could replace circularly polarized an-

[1]Interestingly, this phase-based issue is not a problem for antenna arrays (or SAR-based systems) because the localization there is based on phase differences between antenna elements, allowing them to cancel out the orientation phase.

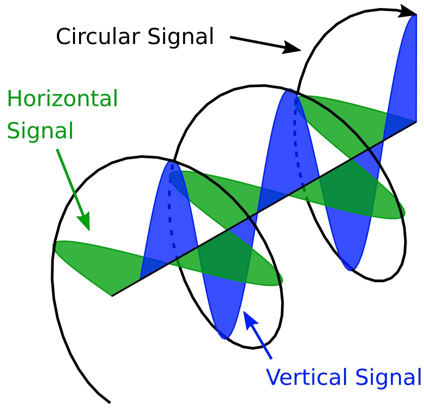


Figure 1-2: Constructing Circularly Polarized Signals. When two perpendicular signals are transmitted with a 90° phase shift, their vector addition (red) traces out a circularly polarized signal.

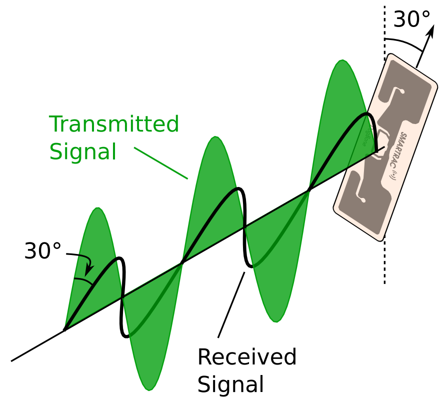


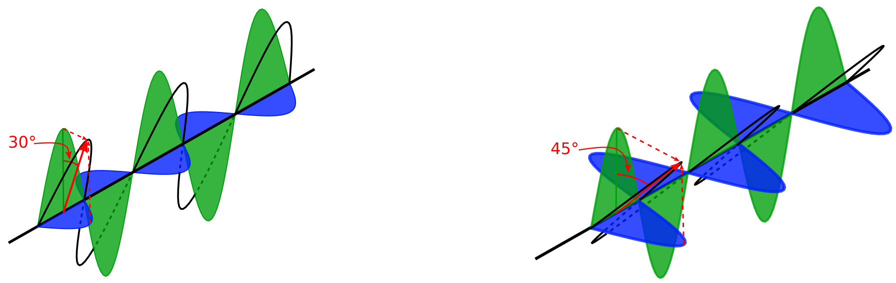
Figure 1-3: Polarization Mismatch. An RFID tag will only harvest energy from the portion of a signal parallel with its polarization, leading to *Polarization Mismatch*.

tennas with linearly polarized ones, but these cannot read tags that are in orthogonal (or near orthogonal) orientations, which could lead to missing up to half the tags in the environment and is the reason why portable readers rely on circularly polarized antennas in the first place.

To see why localizing RFIDs using circularly polarized antennas suffers from an unknown phase offset, consider the illustrative example shown in Fig. 1-1. In circularly polarized transmissions, the electric field (shown as the black vectors) rotates as the signal travels in space. Since RFIDs are linearly polarized,[2] they power-up (and respond) when the received electric field is aligned with their orientation. Thus, as shown in Fig. 1-1a, a vertical RFID tag would reflect the signal when the electric field is vertical. On the other hand, if the RFID is rotated, as shown in Fig. 4-1b, then the received electric field vector is not aligned anymore, and the signal needs to travel longer for the field to be aligned with the tag, indicated by the additional green arc. This adds a fictitious distance and creates a phase offset that is dependent on the RFID's orientation.[3] This is why today's handheld readers, which leverage circularly polarized antennas, are incapable of performing accurate phase-based localization.

[2]Some circularly polarized RFIDs exist, but these are more expensive and larger than linearly polarized, which is why the vast majority of existing tags are linearly polarized

[3]It is worth noting that only the rotation in the plane of the circular polarization is the one that impacts the phase. A rotation around the RFID axis or horizontal plane doesn't as it does not impact the overall distance, as we illustrate in §2.



(a) Constructing Linearly Polarized Signals. (b) Changing the Angle.

Figure 1-4: Constructing Arbitrary Linearly Polarized Signals. (a) how two perpendicular signals can be used to construct a linearly polarized signal at 45 degrees. (b) shows that by changing the relative amplitudes, one can construct a linearly polarized signal at any arbitrary angle.

So how can we read *and* accurately localize RFID tags independent of their orientation? We introduce a technique called *complex-controlled polarization* (CCP). Our approach relies on two orthogonal, linearly polarized antennas with independent phase and amplitude control. Let us start by discussing how EveryFind can read RFIDs across orientations. Rather than using a single circularly polarized antenna, EveryFind generates a circularly polarized signal by feeding the same signal to both linearly polarized antennas, with a 90° phase shift between them, as shown in Fig. 1-2.[4] This approach allows EveryFind to generate a circularly polarized signal using two linearly polarized antennas, and power up the RFID at any angle.

Next, let us see how this approach can be used to localize tags across orientations. Recall that using circularly polarized antennas would introduce an unknown phase offset, which limits the localization accuracy. If the tag is vertical or horizontal, then one can simply transmit along the vertically-polarized or horizontally-polarized reader antenna, respectively. However, if the tag is at 30° as shown in Fig. 1-3, then if we use the vertical antenna alone, it would receive only a fraction of the power. Ideally, we would like to generate a linearly polarized signal whose orientation is aligned with the tag. To do so, we perform independent amplitude control across the two antennas. Specifically, rather than transmitting from only one of the antennas, we transmit the same signal but with cos(30) amplitude along vertical antenna and

[4]Note that feeding the same signal to both without the phase shift results in a vector addition that results in a 45-degrees linearly polarized signal, which cannot power up tags whose angle is around -45 degree or 135 degree.

sin(30) along horizontal antenna (with no phase offset), as shown in Fig. 1-4a. This allows generating a linearly polarized signal at the corresponding angle of 30, matching that of the tag. The same approach can be applied at any angle, as shown by the second example in Fig. 1-4b allowing EveryFind to achieve the highest signal-to-noise ratio (SNR) across orientations, and receive a response without a phase offset, enabling accurate localization.

To translate the above technique into a practical working system, EveryFind introduces a number of algorithms and mechanisms to enable an efficient, accurate, robust, and portable RFID localization. At the core of our system is a mechanism for *joint tag discovery and localization* (JTDL) that allows estimating the time-of-flight for each RFID tag as part of the standard RFID EPC-Gen2 protocol. Building on past work called dual-frequency excitation, the system decouples powering the RFIDs from localizing them. This is done by transmitting a high-power frequency in the UHF ISM band to power up the tag, while the localization is done by transmitting another low-power signal outside the ISM band. Since the two frequencies occupy different bands, they can be simultaneously transmitted from the same CCP antennas without interfering with each other's polarization. Specifically, the in-band is generated in a circularly polarized fashion while the out-of-band can be generated in a linearly polarized manner. Our implementation takes this idea a step further by transmitting different frequencies from the horizontal and vertical antennas and combining them in post-processing to synthesize any orientation. Finally, our system integrates mechanisms for self-interference cancellation to deal with leakage from both the circularly polarized and linearly polarized transmissions.

We built a proof-of-concept prototype of EveryFind. The prototype leverages a built-in tracking camera that allows it to self-localize in the environment. As the user moves around, the discovery algorithm continuously runs, the devices measures distances from the user's trajectory, and combines them in post-processing to localize the RFIDs in the environment. We built the prototype of EveryFind using bladeRF software radios connected to a raspberry pi. We also fabricated compact wideband antennas that have the desired gain and bandwidth properties needed for wideband

RFID localization.

Our experimental evaluation demonstrates the following:

- Our approach for circularly polarized transmissions allows us to power up and read tags irrespective of their orientation. In comparison, for tags placed at the same distance, a linearly polarized antenna cannot power (or read) up to 30% of the tag angles.

- Our approach for linearly polarized transmissions is able to read the tag's phase without a phase shift, achieving a 90^{th} percentile phase change of 0.2 radians in the presence of tag rotations up to 90°. In contrast, if we use a circularly polarized antenna, the tag's response has an unknown phase shift, ranging anywhere from 0.02 to 3.1 radians, (roughly π radians, as expected for a 90° rotation).

- Our system can localize RFID tags with a median accuracy of 12cm and 90^{th} percentile of 25cm, independent of the tag's orientation, as a user carrying the device performs normal RFID inventorying. Thus, our system meets its requirements of portability, accuracy, robustness, and efficiency.

Contributions: This thesis presents EveryFind, a portable, handheld RFID localization system that is accurate, robust, and efficient. It introduces multiple innovations. First is complex-controlled polarization (CCP), an approach to localize RFID tags under random orientations using a handheld device with two linearly polarized antennas. Second is a mechanism to jointly perform discovery and time-of-flight estimation with zero overhead, independent of the tag orientation. This thesis also contributes a proof-of-concept prototype implementation and experimental evaluation demonstrating the method's accuracy and efficiency.

Chapter 2

Localizing Across All Angles

In this chapter, we will first describe the challenges associated with reading and locating tags at different orientations. Next, we will describe how EveryFind's design overcomes these challenges to localize tags irrespective of their orientation.

2.1 The Tag Orientation Problem

The majority of RFID readers rely on circularly polarized antennas because they can power and read tags regardless of orientation. However, in the presence of arbitrary tag rotations, these circularly polarized antennas often fail entirely for localization. Recall from §1 that the issue arises from the fact that most accurate localization systems rely on the phase of the tag's response to measure the distance to the tag. However, the phase of the response for a circularly polarized signal depends on the orientation of the tag, making it difficult to recover the distance. In fact, certain tag rotations can cause phase offsets up to 2π, resulting in localization errors up to several meters.[1]

To understand the impact of tag orientations, consider the three different rotations: rotations around the X, Y, and Z axes (also known as pitch, roll, and yaw, respectively), as shown in Fig. 2-1. First, changing the tag's roll will create a phase

[1] We note that some solutions, such as antenna arrays, can still operate in the presence of this phase offset. However, these approaches typically require extensive infrastructure, making them ill-suited for a portable RFID reader.

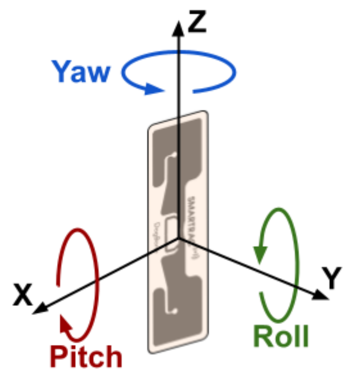


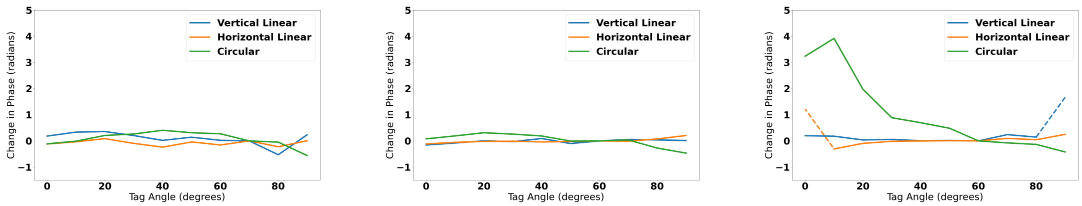
Figure 2-1: Tag Rotations. This figure shows the axes of the three different tag rotations: pitch (red), roll (green), and yaw (blue).

offset for circularly polarized signals. This phenomenon, as shown in Fig. 1-1, is due to the fact that the tag's strongest reflection occurs when the tag is parallel to the signal's eletric field. Fig. 1-1a shows a circularly polarized signal (shown by the red spiral) incident to a linearly polarized tag. The phase of the response is determined by the point where the electric field (black vectors) becomes parallel with the tag. When the tag is rotated to a new angle, as shown in Fig. 4-1b, the signal will need to travel a further distance until it is parallel with the tag, as indicated by the additional green arc. This introduces a phase offset proportional to the rotation of the tag.[2] In contrast, changing the tag's pitch or yaw does not induce a phase offset. This is because these rotations do not change the direction of the tag's polarization relative to the circularly polarized signal.

We demonstrated this phenomenon in a real-world experiment by measuring the impact of tag rotation on the phase of the tag's response. In these experiments, we placed the tag and our reader at fixed locations 0.5 m apart. We rotated the tag in intervals of 10 degrees in each of the 3 directions (roll, pitch, and yaw). At each angle, we queried the tag multiple times and computed the average phase and signal-to-noise ratio (SNR) across the measurements.[3] We repeated the experiment with a vertical linearly polarized antenna (blue), a horizontal linearly polarized antenna (orange) and a circularly polarized antenna (green).

[2] We note that the tag will reflect a portion of the signal even when it is not parallel with the signal. However, these reflections will average out over the course of a full period, and therefore do not change the overall phase.

[3] We discarded the minimum and maximum 3 measurements to remove outliers



(a) Pitch (X). (b) Yaw (Z). (c) Roll (Y).

Figure 2-2: Impact of Tag Rotations. These plots show change in the phase of the tag's response as a function of the tag's angle. The results are shown for a horizontal linearly polarized antenna (orange), vertical linearly polarized antenna (blue), and a circularly polarized antenna (green). (a) shows the impact of changing the tag's pitch. (b) shows the impact of changing the tag's yaw. (c) shows the impact of changing the tag's roll.

Fig. 2-2 plots the change in phase of the tag's response (relative to the tag's response at an initial orientation) as a function of the tag's angle for each of the three rotation directions. We focus on the range of 0° to 90°, since the remaining angles follow the same pattern. In these plots, a solid line indicates that the SNR at that angle was above a threshold and the dotted lines indicate that the SNR was below that threshold.[4] We make a few observations:

- Fig. 2-2a and Fig 2-2b show that for pitch and yaw, respectively, the phase remains consistent (i.e., the change in phase remains near 0) for the circularly polarized signal.
- Fig. 2-2c demonstrates the issue that arises for changes in the tag's roll. The phase changes drastically, from 3.2 radians to -0.42 radians, for the circularly polarized signal, despite the distance to the tag remaining fixed. This means that the total change in phase is 3.6 radians, i.e., more than a full π radians. This large of a change in phase would result in meters of error in phase-based localization.
- In contrast, for linearly polarized signals, *if the tag is powered up*, then the phase remains the same across all three rotations. This is expected since the relative rotation between the signal's electric field and the tag remains fixed over time. Therefore, the phase of the tag's response does not change as the tag is rotated.

[4]For these experiments, we used an SNR threshold of -0.25dB.

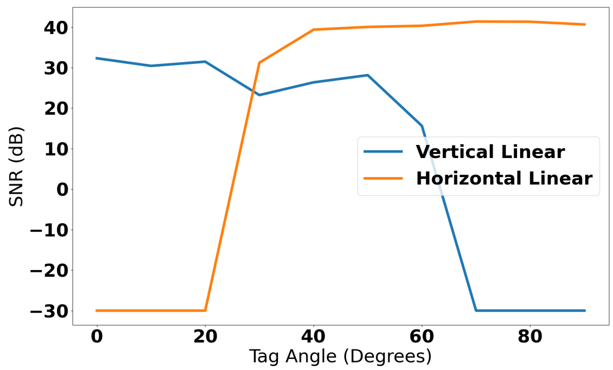


Figure 2-3: SNR of Tag Response. This plot shows the SNR of the tag's response as a function of the tag's roll angle for both a horizontal (orange) and a vertical linearly polarized antenna (blue).

The above experiment demonstrates that if we replace the circularly polarized antenna with a linearly polarized, we can eliminate the unknown phase offset. However, a linearly polarized antenna is unable to power tags at all angles. This is due to a phenomenon known as *polarization mismatch*, where the tag only harvests energy from the portion of a signal that is parallel with its polarization. As a result, when the polarization is perpendicular (or near perpendicular) with the tag, the tag will not be able to harvest enough energy to power on.

To investigate the impact of polarization mismatch on the ability to power up a tag, we conducted an experiment, where we placed the tag and our reader 0.5 m apart and rotated the tag in intervals of 10 degrees in the Y dimension (roll). At each angle, we read the tag 30 times and measured the SNR of each response. If the tag was unable to be successfully read,[5] then we capped the measurement SNR at a minimum of -30dB.

Fig. 2-3 plots the SNR versus the tag's angle when the tag is rotated along the y-axis. We repeat the experiment for reader antennas with 2 polarizations: vertically polarized antenna (blue) and horizontally polarized (orange). Here, we make two remarks:

- When the tag angle is orthogonal to the polarization, the antenna cannot read the tag (and the SNR is set to -30dB). Specifically, the horizontal (90°) antenna

[5]We declared a tag to be read successfully if the packet's CRC (the tag's checksum for error detection) was correct

is unable to read the tag (i.e., the SNR is -30dB) for all tag angles ranging from 0° to 20°. Similarly, the vertical (0°) cannot read tags from 70° to 90°.

- On the other hand, when the tag angle is not orthogonal to the polarization, the antennas can read the tag. For example, the vertical antenna (0°) can read tags with high SNR between 0°and 60°.

This demonstrates that the polarization mismatch of a linearly polarized antenna prevents it from reading a tag when the polarization is within 20° of being perpendicular to the tag's orientation.

2.2 Complex-Controlled Polarization

So far, we have described the challenges associated with reading and localizing tags at different orientations. To overcome these challenges, EveryFind introduces *Complex-Controlled Polarization (CCP)*. Our technique leverages perpendicular, linearly polarized antennas[6] with independent phase and amplitude control. In the remainder of this chapter, we will describe how CCP enables both reading and locating tags at all orientations. For simplicity, we will first discuss these two steps independently then we will describe how we combine them in §3

2.2.1 Reading Tags with CCP.

Recall from §2.1 that circularly polarized signals can power tags regardless of their orientation (but they add an unknown phase offset to localization). Instead of using a circularly polarized antenna, EveryFind leverages its two linearly polarized antennas to generate a circularly polarized signal.

Fig. 1-2 shows how EveryFind is able to construct the circularly polarized signal. EveryFind sends a horizontal signal (blue) and a vertical signal (green) simultaneously, with a 90 degree phase offset between the two signals. At each point in time,

[6] In our design, we used 2 transmit antennas and 2 receive antennas. However, we note that the design could be reduced from four to two antennas by using the same antennas for transmitting and receiving through a circulator.

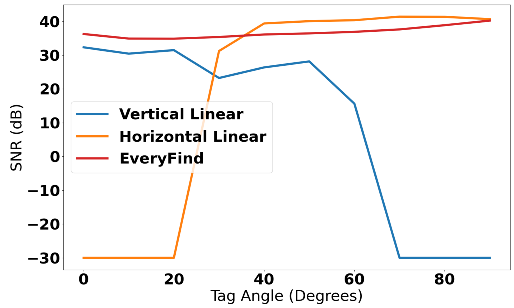


Figure 2-4: SNR of EveryFind's Design. This plot shows the SNR of the tag's response as a function of the tag's roll for EveryFind (red), a horizontal linearly polarized antenna (orange), and a vertical linearly polarized antenna (blue).

the resulting signal is the vector addition of these two signals, as shown by the red arrows. As the signals travel, their phase offset causes this vector to rotate, creating a circularly polarized signal (traced out in black). This signal can be used to power tags across orientations in the same way as a separate circularly polarized antenna. Formally, we send the following signals:

$$TX_1 = x \tag{2.1}$$

$$TX_2 = xe^{j\pi/2} \tag{2.2}$$

where TX_1 and TX_2 are the transmitted signals on the two perpendicular antennas, and x is the time-domain (modulated) RF signal. It is worth noting here that this approach is inherently different from typical MIMO (multi-input multi-output) systems in both theory and design [21]. This is because, in MIMO systems, antennas typically have the same polarization, and adding a phase offset does would not induce a time-varying polarization change of the transmitted signals.

Beyond powering the tag, EveryFind also needs to receive the tag's response in order to successfully read it. Similar to transmission, we receive a circularly polarized signal to by combining the received signals from each antenna with a 90° phase shift. This ensures that we can read the tag regardless of its orientation.

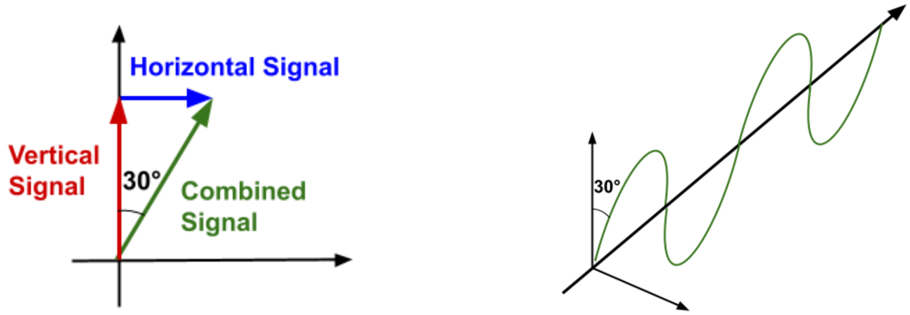
To demonstrate the effectiveness of this technique, we repeated the SNR experiment from §2.1 to measure the SNR of the tag's response as a function of the tag's roll angle. Fig. 2-4 shows the results for EveryFind (red). The previous results for the horizontal and vertical linearly polarized signals are shown again for comparison. Unlike either of the individual linearly polarized signals, EveryFind is able to achieve a high SNR (over 34dB) across all tag angles, demonstrating that this design successfully creates circularly polarized signals that can power and read tags at all angles.

2.2.2 Localizing Tags with CCP

While EveryFind's circularly polarized signal performs well for powering all tags, recall that this signal cannot be used to accurately locate tags in the environment because it adds an unknown phase offset. Instead, EveryFind employs a linearly polarized signal to localize. For simplicity of exposition, let us assume that the RFID has been powered up, and that our goal is to use linearly polarized antennas to measure the phase of its response.

The problem with simply using linearly polarized signals is that they suffer from polarization mismatch, causing a large drop in the SNR when the tag is near perpendicular to the signal. Recall that we observed this phenomenon in the experiment of Fig. 2-2c, whereby the dashes lines of in the figure denoted a very low-SNR. The low-SNR was observed when each of the horizontally and vertically polarized antennas measured when the tag was near-orthogonal to the signal polarization. Such drop in SNR would impact the channel estimates and result in an inaccurate location estimate.

To overcome the reduction in SNR from polarization mismatch, EveryFind can construct a linearly polarized signal that aligns with to the tag's orientation, minimizing losses from polarization mismatch. Fig. 1-4 shows how EveryFind is able to construct different linearly polarized signals. It simultaneously sends a vertical signal (green) and a horizontal signal (blue). Unlike the circularly polarized signal described above, these two signals are sent with no phase offset. Again, the resulting signal is a vector addition of the two signals, shown by the red arrow. In Fig. 1-4b, when sending signals of equal magnitudes, the final signal (shown in black) is a linearly



(a) Constructing Arbitrary Angles. (b) Resulting Signal.

Figure 2-5: Constructing Linearly Polarized Signals. (a) shows two perpendicular signals (blue and red) with different amplitudes. The combined signal (green) is the vector sum of the two signals, whose angle is determined by the relative amplitudes of the two signals. (b) shows the resulting linearly polarized signal.

polarized signal at 45°.

In order to change the orientation of this linearly polarized transmission, EveryFind changes the relative amplitudes of the two signals. Fig. 2-5a shows an example where the horizontal signal (blue) and vertical signal (red) are sent with different amplitudes. The combined signal (green) is the vector sum of the two individual signals. In this example, the combined signal is at 30°, resulting in the linearly polarized signal shown in Fig. 2-5b. Therefore, through its independent amplitude control, EveryFind can construct a linearly polarized signal at any angle.

To generate a signal at a given angle θ, EveryFind needs to compute the necessary amplitudes. To do so, we note that the resulting signal is the hypotenuse of the right triangle formed by the two perpendicular signals. Therefore, to construct a signal at angle θ, we can send:

$$TX_{horiz} = cos(\theta)x \tag{2.3}$$

$$TX_{vert} = sin(\theta)x \tag{2.4}$$

where TX_{horiz} is the signal sent on the horizontal antenna, TX_{vert} is the signal sent on the vertical antenna, and x is the modulation of the signal being sent.

Once the tag has backscattered this signal, EveryFind will receive the response on its two perpendicular receive antennas. Each antenna will receive only the component of the tag's response that is parallel to its polarization, again resulting in polarization mismatch. In theory, one could simply use the signal with the strongest response for localization. However, doing so would lose information from the other antenna, limiting the SNR. For example, when the tag is at 45°, each receive antenna will receive the same amount of power from the tag's response, so dropping one the received signal from any of the antennas would result in losing half of the received power.

Instead, EveryFind combines the two responses to construct a linearly polarized receive signal that matches the tag's orientation. This combination optimizes the power of the received signal, maximizing the SNR and therefore allowing accurate localization at further ranges. To combine these signals, we project the received signals onto an angle θ in a similar manner to the transmitted signal. Formally,

$$RX_{comb} = cos(\theta)RX_{horiz} + sin(\theta)RX_{vert} \tag{2.5}$$

where RX_{comb} is the combined received signal, RX_{horiz} is the received signal on the horizontal antenna, and RX_{vert} is the received signal on the vertical antenna.[7]

Here, one might wonder whether adding a phase offset - rather than an amplitude offset - between the transmitted signals on the vertical and horizontal antennas may be a more appropriate approach for generating linearly polarized signals at different orientations. In practice, adding a phase offset would not lead to linearly polarized signals but rather circularly polarized ones. This is because a phase offset is equivalent to adding a delay between the transmitted signals, causing them to rotate with respect to each other over time. Indeed, our approach for generating a circularly polarized signal in §2.2.1 relied on a 90° phase offset between the signals transmitted on the two antennas. Similarly, other phase offsets would result in elliptical polarizations with different major and minor axes (rather than horizontal polarizations).

2.3 Validating CCP

Using these techniques, EveryFind can overcome polarization mismatch while still using linearly polarized signals to avoid phase offsets.

[7] See Appendix A for a proof that this combination provides optimal received power

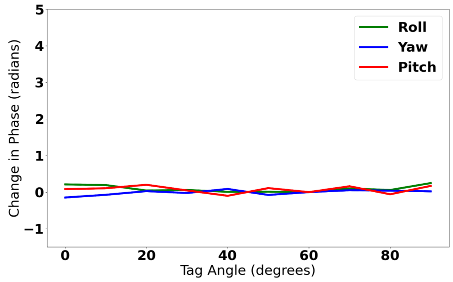


Figure 2-6: EveryFind's Change in Phase. This plot shows the change in phase of the tag's response as a function of the tag angle when using EveryFind's design. The results for rotations in the pitch (red), roll (green), and yaw (blue) are shown.

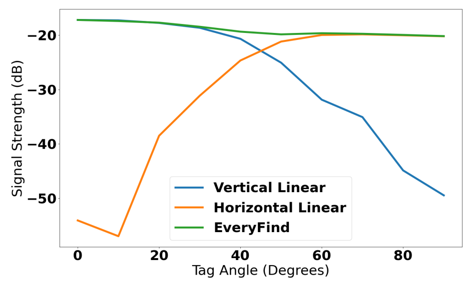


Figure 2-7: EveryFind's Signal Strength. This plot shows the signal strength as a function of the tag's roll angle. The results for EveryFind (green), a horizontal linearly polarized antenna (orange), and a vertical linearly polarized antenna (blue).

To evaluate this design, we assessed EveryFind's ability to read both a consistent phase and a strong tag response regardless of orientation through two real-world experiments. First, we investigated whether this design reads the tag's phase independent of orientation. We repeated the experiment from §2.1, where the reader and tag were placed at a fixed distance and the tag was rotated in all 3 directions. We measured the *change* in phase (relative to the response at an initial orientation) for each rotations using EveryFind's design. Fig. 2-6 plots the change in phase as a function of the tag's angle in the pitch (red), roll (green), and yaw (blue) dimensions. The range of the phase across all tag angles is below 0.3, 0.2, and 0.2 radians for the X, Y, and Z dimensions, respectively. These variations are minimal, and significantly smaller than those observed with the circularly polarized antennas (specifically in Fig. 2-2c). The consistency of the phase across tag rotations demonstrates that EveryFind's CCP design can read tag phases independent of orientation, which is critical for accurate tag localization.

Next, we investigated EveryFind's ability to receive equivalent power across all tag rotations. We placed the tag and our reader at a fixed distance and rotated the tag in intervals of 10 degrees around the Y axis (roll). To ensure the tag was powered for every trial, we placed separate antennas near the tag for powering and reading the tag. We measured the channel strength at each angle.[8] We compare this to the

[8] To avoid outlier measurements, we measured the channel strength 30 times and plot the median channel strength.

signal strength when using a single linearly polarized antenna, both horizontal and vertical.

Fig. 2-7 plots the signal strength as a function of tag's roll angle for EveryFind (green), a horizontal antenna (orange), and a vertical antenna (blue). For both the horizontal (90°) and vertical (0°) antenna, the impact of polarization mismatch can be seen by a significant decline of over 25dB in signal strength as the tag angle moves closer to perpendicular. For EveryFind, the signal strength remains consistent across all tag angles, varying by less than 5dB. This demonstrates the effectiveness of CCP for overcoming polarization mismatch.

Chapter 3

Joint Discovery and Localization

In the previous chapter, we described how EveryFind leverages CCP to construct both circularly polarized signals for powering tags and linearly polarized signals for localizing tags. In this chapter, we describe how EveryFind combines these techniques to simultaneously read and localize tags.

A key goal of our design is to localize tags *during* a standard RFID inventorying process and without additional overhead for localization. To realize this goal, EveryFind starts by building on a technique known as dual-frequency excitation [14]. In this technique, two signals of different frequencies are sent to the RFID tag: one high-power signal in the UHF ISM band to read the tag and one low-power signal for sensing. While the high-power signal must remain within the tag's narrow bandwidth to successfully read the tag, the sensing signal can be sent at any frequency. Since the RFID tag is frequency agnostic, it will reflect both signals. Therefore, by varying the sensing frequency across a wide bandwidth, this technique can be used to measure ultra-wideband (UWB) channel estimates for accurate localization.

Building on the above technique, EveryFind sends both its circularly polarized signal to power the tag and a separate linearly polarized signal to localize. Since these signals are at different frequencies, we can send both from the same CCP antennas without them impacting each others polarizations. Furthermore, to efficiently localize tags during discover, we introduce a technique called *Joint Tag Discovery and Localization* (JTDL), where we leverages the CCP technique to simultaneously

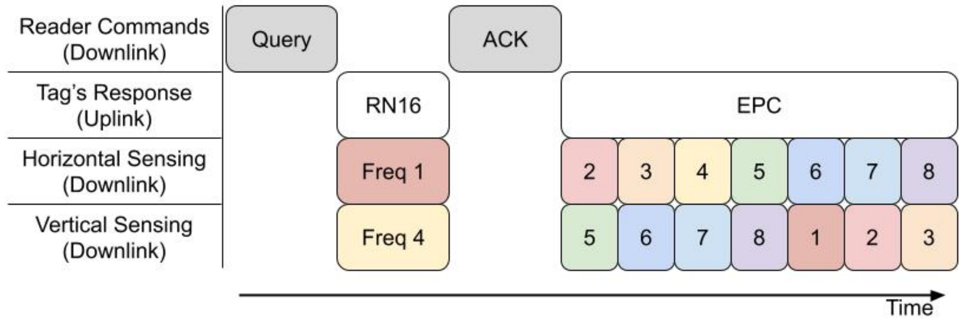


Figure 3-1: Protocol Timing. This figure shows the timing of one round of EveryFind's joint discovery and localization. The first two rows show the reader's downlink commands and the tag's uplink responses. The last two rows show the two linearly polarized sensing signals. Different frequencies (shown by different colors) are sent at different times to avoid interference between the two signals.

perform tag discovery and UWB sensing, collecting over 200MHz of bandwidth within a single tag read.

One major challenge with performing joint discovery and localization with CCP is that the orientation of each tag is unknown a priori, making it infeasible for EveryFind to construct a linearly polarized transmit signal that matches the tag's angle as described in §2.

To overcome this challenge, our high-level approach is to send any given frequency on each of the antennas at different times, and combine the received signals in post-processing. Such an approach allows EveryFind to measure both the horizontal and vertical components of the tag's response. Then, EveryFind can combine the signals in post processing to achieve optimal SNR.

This technique is illustrated in Fig. 3-1 and follows the following three-step process:

1. **Transmission.** As described above, since the angle of the tag is unknown, EveryFind instead transmits the horizontal and vertical signals at different times. However, separating the two transmit signals would require twice the transmission time, making it difficult to fit within the tight timing constraints of the tag discovery algorithm. Instead, EveryFind transmits different permutations of its frequencies on its two transmit antennas simultaneously. Fig. 3-1 shows an example of the schedule used to fit all frequencies within one round of the standard EPC Gen2 [1] discovery protocol. The first two rows shows

the reader's downlink commands and the tag's uplink responses. This process starts with a query from the reader. The tag then responds with a 16-bit random number called an RN16. The reader decodes this response and sends an acknowledge (ACK) with the RN16. Upon receiving the correct RN16, the tag begins backscattering it's ID number, known as an EPC. During this process, EveryFind can measure the tag's channel whenever the tag is backscattering (i.e., the RN16 and EPC). The bottom two rows show the transmitted frequencies for each of the two antennas, with each color showing a different frequency. Since the different frequencies are independent, they will not interfere with each other and can be sent simultaneously. With this approach, EveryFind is able to measure over 200MHz of bandwidth within one tag read, sufficient for accurate localization [14].[1] This process is repeated until all tag's within the device's radio range are read.

2. **Angle Detection.** Next, EveryFind estimates the tag's roll angle. To do so, we leverage the fact that each antenna only receives the parallel portion of the tag's reflection. Therefore, their relative channel magnitudes form a right triangle with the tag's angle, and can be used to estimate the tag's angle.

   First, we estimate the tag's channel using the tag's known packet $p(t)$ and its received signal $y(t)$ as follows:

$$\hat{h} = \sum_t y(t) p^*(t) \tag{3.1}$$

   where $\hat{h}$ is the estimated channel and $p^*(t)$ is the conjugate of the tag's packet.

   Using this, EveryFind estimates the tag's angle as:

$$\hat{\theta} = \tan^{-1}\left(\frac{|\hat{h_{vert}}|}{|\hat{h_{horiz}}|}\right) \tag{3.2}$$

[1] Note that if the same frequencies were sent simultaneously, then they would combine to construct a linearly polarized signal at 45 degrees, which would experience large polarization mismatch with tags near -45 degrees.

where $\hat{\theta}$ is the estimate of the tag's angle, $\tan^{-1}$ is the inverse tangent, $\hat{h_{vert}}$ is the estimate of the channel from the vertical antenna, and $\hat{h_{horiz}}$ is the estimate of the channel from the horizontal antenna.[2]

3. **Distance Estimation.** Finally, for each frequency, EveryFind estimates the channel from both antennas using Eq. 3.1. It then combines the channel measurements at each frequency using Eq. 2.5 and its estimated $\hat{\theta}$. With its UWB channel estimates, it can now invert the channel to estimate the time-of-flight to the tag and measure the 1D distance using the same methods applied in past work [14, 13, 7]. EveryFind repeats this process (i.e., estimating the angle and computing the distance estimate) for every tag that it read during the discovery round.

The above three-step process allows EveryFind to compute the 1D distance estimate for each tag during a standard inventory process, thus resulting in a highly-accurate and efficient localization. In §5, we describe how EveryFind leverages these 1D measurements to robustly estimate the 3D locations of tags in the environment.

[2]In our implementation, $\hat{h_{vert}}$ and $\hat{h_{horiz}}$ are the estimated channels for the 6th frequency in the ultra-wideband sensing

Chapter 4

Addressing Self-Interference

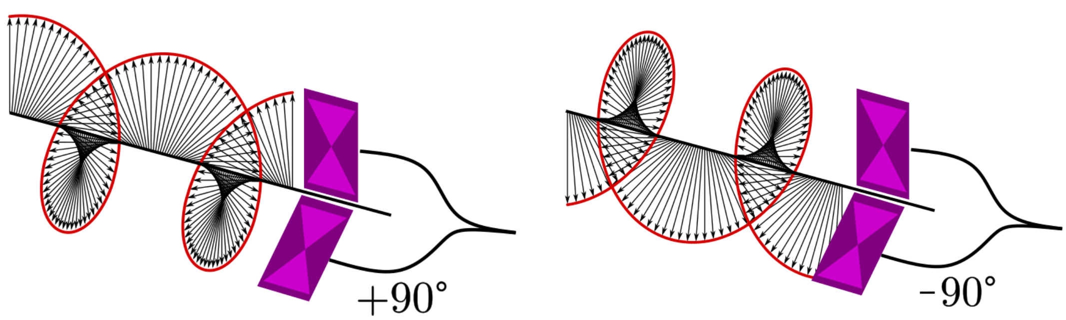
A well-known problem in the design of compact RFID readers is self-interference [12]. Specifically, since RFID readers are full duplex (i.e., they transmit a continuous wave signal at the same time as they receive the modulated backscatter response), the transmitted signals leak back into the receiver. Since this leakage is much stronger than the backscatter response, it can overwhelm the receiver, preventing successful decoding. To deal with this leakage, RFID readers either separate the transmitter and receiver by some distance (e.g., half a meter) or employ some self-interference cancellation scheme [18, 8, 4], whose choice depends on the reader implementation, bandwidth, antenna design, and so on. Since we want to build a compact handheld reader, we cannot separate our antennas by a large distance to mitigate leakage, so we need to incorporate cancellation mechanisms into our design.

Bringing self-interference cancellation to EveryFind faces two key challenges. The first one is that the system needs to not only cancel the self-interference from a typical RFID reader signal, but also from the UWB out-of-band signal, making the problem much more difficult (since it is more difficult to cancel wideband signals than typical narrowband RFID signals [11]). The second challenge is that EveryFind has two different modes for transmission that happen simultaneously: the in-band is transmitted as a circularly polarized signal, and the out-of-band is transmitted as a linearly polarized one. This adds further complexity to the cancellation as we need to cancel two different types of signals that are transmitted simultaneously.

In this chapter, we describe EveryFind's self-interference cancellation schemes. For simplicity of exposition, we first focus on how we cancel the circularly polarized in-band signal, then the linearly-polarized out-of-band one. In designing these schemes, we sought to identify mechanisms that are simple and effective, which makes implementing them easy in a compact handheld reader.

4.1 Dealing with Circularly Polarized Interference

First, EveryFind aims to limit the self-interference from the circularly polarized signal used to power the tags. To do this, our approach is to leverage a method called *cross-polarization* in the context of circularly polarized antennas. At a high level, cross-polarization means that if a transmitter and receiver have orthogonal polarizations, then the transmitted signal is significantly attenuated at the receiver. Indeed, we saw this in §2.1, where a horizontally polarized reader antenna could not power up a vertical RFID tag. While this phenomenon is problematic in the context of powering RFIDs, we harness it to cancel self-interference of our in-band signal.



(a) RHCP. (b) LHCP.

Figure 4-1: Generating Different Circular Signals (a) shows how EveryFind generates an RHCP signal using a 90° phase shift. (b) shows how EveryFind generates an LHCP siganl using a -90° phase shift.

To harness cross-polarization, we start by noting that our in-band transmitted UHF signal is circularly polarized. In our implementation, we transmit with right-hand circular polarization (RHCP), which means that the electric field rotates counter-clockwise, as shown in Fig. 4-1a. Interestingly, the cross-polarization of a right-hand circurlarly polarized transmission is left-hand circular polarization

(LHCP), which rotates in the opposite direction as shown in Fig. 4-1. Intuitively, receiving using a right-hand polarization means that as the transmitted signal rotates in one direction (counter-clockwise) over time, the receiver is trying to receive a signal that is rotating in the opposite direction (clockwise). Thus, over time, the transmission and reception remain almost orthogonal to each other, minimizing the received signal.

Next, let us mathematically formalize this concept. Based on the earlier discussion, any polarization can be described using a two-dimensional complex vector $[E_v, E_h]$, where the two coordinates correspond to the vertical and horizontal (complex) numbers that are applied to the transmitted vector. An RHCP polarization can be realized as $E_{RHCP} = [1, e^{j\pi}]$. An LHCP can be realized as $E_{LHCP} = [1, e^{-j\pi}]$. Since the received signal is a projection of the transmitted polarization on the received polarization, the resulting signal in the ideal case is:

$$\langle E_{RHCP}, E^*_{LHCP} \rangle = \begin{bmatrix} 1, e^{j\pi} \end{bmatrix} * \begin{bmatrix} 1 \\ e^{j\pi} \end{bmatrix} = 0 \tag{4.1}$$

To implement LHCP at the receiver using two linearly polarized antennas, we used a similar method as for generating an RHCP transmit signal. Recall that we implemented RHCP by adding a 90° phase shift between the two transmitted signals. Similarly, we add a 90° phase between the two receive signals to create an LHCP at the receiver.[1]

To investigate the impact of our cross-polarization mechanism on cancelling the leakage, we ran an experiment to measure the isolation (i.e., attenuation of the leakage) between the transmitter and reciever. To do so, we placed the setup in a large, open space with RF absorbers on the floor and covering all equipment (to mitigate the impact of reflections off the surrounding environment). Using a vector network analyzer, we measured the isolation between the transmitter and receiver. We measured the isolation for 30MHz centered at 900MHz (the frequency range where the

[1]It is worth noting that transmitting an LHCP signal would require adding a -90° phase. However, since reception is a projection (i.e., multiplication by complex conjugate), we apply a 90° phase. This can also be seen in Eq. 4.1.

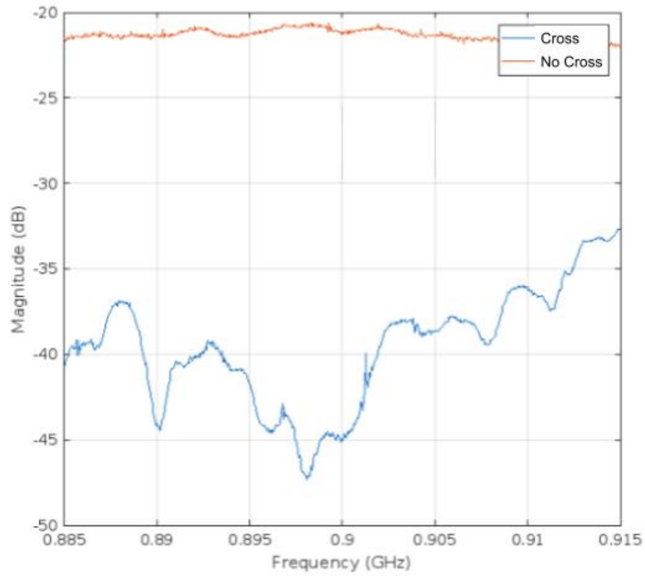


Figure 4-2: Isolation of Circularly Polarized Signal. This plot shows the isolation for the circularly polarized signal. It plots the isolation when using EveryFind's cross polarized transmit and receive signals (blue) compared to when the two signals have matching polarization (red).

tag powers). Fig. 4-2 plots the isolation with (blue) and without (red) the cross polarization as a function of frequency. When receiving without cross polarization at 900MHz, the design only achieves -21dB of isolation.[2] In comparison, EveryFind's design with cross-polarization achieves -45dB of isolation, demonstrating a more than 2x improvement.

Finally, one might wonder whether using this cross-polarization mechanism would not only mitigate the (harmful) self-interference signal, but also attenuate the received backscatter response. Thankfully, that is not the case. The reason is that once the signal arrives at the RFID and gets backscattered, it becomes linearly polarized. A circularly polarized antenna can receive a linearly polarized signal, regardless of its polarization. Indeed, that is why we used circular polarization in the first place in our design of the in-band transmitter as described in §2.

[2]This is the natural isolation due to the spacing of the antennas and losses in the cables.

4.2 Dealing with Linearly Polarized Interference

In addition to the circularly polarized signals, EveryFind needs to minimize the self interference from the linearly polarized signals used for localization.

One might wonder if we can apply a self-interference cancellation mechanism similar to the cross-polarization that we used for the in-band circularly polarized signal. While a cross-polarized receive antenna (i.e., a horizontal receive antenna for the vertical transmit antenna) would attenuate the leakage, this would also significantly attenuate the tag's response. For example, consider a vertical tag. When transmitting on a vertical antenna, the tag's backscatter response will be strong. However, a horizontal antenna will not be able to receive the response due to the polarization mismatch (as demonstrated in §2.1). Similarly, when transmitting on the horizontal antenna, the reflected signal will be weak due to the polarization mismatch, preventing a vertical receive antenna from measuring a strong signal. In this case, EveryFind would be unable to measure the tag's response from either of its antenna pairs. Therefore, EveryFind must use parallel transmit and receive antennas, leading to a high level of leakage. This intuition can be easily formalized using the same polarization formulation used in §4.1.

To overcome this, EveryFind leverages over-the-wire nulling, inspired by past work [4]. At a high level, this process works by sending a second "nulling" signal over a wire and combining it with the signal from the antenna such that it destructively interferes with the leakage. We explain this process in 2 steps and refer the reader to [22] for more details.

1. **Channel Estimation.** First, EveryFind estimates the channel of both the self-interference (over the air) and the wire used for nulling. It does this by sending a known signal $x(t)$ over the air and computing the channel of the self interfrence as

$$\hat{h_{air}} = \sum_t y(t)x^*(t) \tag{4.2}$$

where $\hat{h_{air}}$ is the estimated channel, $y(t)$ is the received signal, and $x^*(t)$ is the conjugate of the transmitted signal. EveryFind repeats this processes to estimate the channel of the wire, $\hat{h_{wire}}$.

2. **Nulling.** Next, EveryFind simultaneously sends its normal transmission over the air and its nulling transmission over the wire. For the nulling signal x_{null}, it sends

$$x_{null} = \frac{-\hat{h_{air}}}{\hat{h_{wire}}} x_{air} \tag{4.3}$$

where x_{air} is the transmission over the air. This signal will destructively interfere with the self interference. We refer readers to Appendix B for the derivation of this equation.

To enable wideband nulling, EveryFind repeats this process for each frequency. We perform this wideband over-the-wire nulling independently for both the vertical and horizontal antenna pairs.

To investigate the impact of the over-the-wire nulling, we ran an experiment where we measured the isolation between the parallel antennas. For this experiment, we transmitted a fixed signal and measured the amplitude of the response (i.e., the magnitude of the leakage). In order to quantify the isolation provided by the nulling, we repeated this with and without the nulling and compared the amplitudes of each response. [3] We repeated this measurement for all frequencies used during localization.

Isolation (dB)									
	Frequency (MHz)								
	763	**790**	**817**	**844**	**871**	**952**	**979**	**1006**	**Avg**
Vertical	20.5	23.8	26.5	21.2	24.5	22.1	25.9	21.2	23.2
Horizontal	25.6	21.4	24	20.8	30.5	18.9	31.4	16.2	23.6

Table 4.1: **Nulling Isolation.** The table shows the isolation achieved with over-the-wire nulling for all frequencies and the average across all frequencies. It shows the results for both the vertical antennas and horizontal antennas.

Table 4.1 reports the average isolation (across three trials) for both the vertical pair of antennas and the horizontal pair of antennas. It shows the isolation for each

[3] We ensured that the gains of the receiver did not allow the signal to reach the maximum value (i.e., clip).

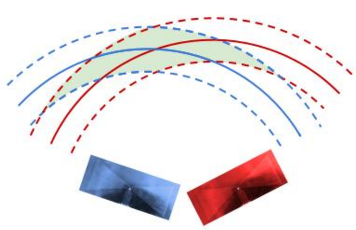
frequency, as well as the average isolation across all frequencies. With an average isolation of 23dB for each of the antenna pairs, EveryFind is able to significantly mitigate the self-interference between parallel antennas.

Chapter 5

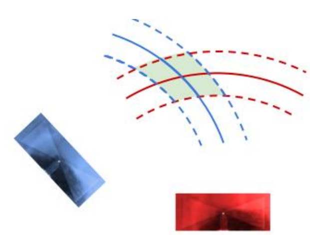
Robust 3D Localization

So far, we have described how EveryFind enables compact, efficient 1D localization for all tags regardless of orientation. Next, we will describe how EveryFind incorporates this into a mobile handheld RFID reader that combines 1D distance estimates to estimate each tag's 3D location.

At a high level, we built EveryFind's design into a handheld device that a user can move around the environment. This reader continuously runs JTDL in order to collect multiple 1D measurements for each tag in the environment. Simultaneously, the location of the device is tracked over time to determine where each measurement was taken from. Using the 1D measurements and the device locations, EveryFind performs trilateration to derive the 3D location of each tag in the environment.



(a) Poor DoP.



(b) Good DoP.

Figure 5-1: Dilution of Precision (DoP). Two antenna locations (blue and red) and their corresponding 1D distance measurements (solid lines) are shown. The dotted lines show the margin of error for these measurements. The green area shows the possible tag locations given these two measurements and their uncertainty. (a) shows a case with poor DoP where the measurements are close together. The area of possible tag locations is large. (b) shows a case with good DoP where the measurements are far apart, and the area of possible tag locations is small.

Robustly locating the tags with this approach faces a few challenges. First, there are likely to be measurements with high error that may throw off the trilateration. Second, if multiple measurements are taken from very similar locations then the accuracy of the localization will be very low. This well-known phenomenon, known as *Dilution of Precision* (DoP), can be seen in Fig. 5-1. The red and blue antennas show two measurement locations, and the solid lines show their 1D distance measurements. Due to noise in the system, each of these measurements have some error, indicated by the dotted lines. The overlap between the two measurement's error bounds define the possible locations of the tag (highlighted in green). Fig. 5-1a shows the case when the two measurement are taken from close locations (poor DoP). The area of possible tag locations in this case is large, showing the potentially low accuracy of trilateration when using these measurements. On the other hand, Fig. 5-1b shows the case when the two measurement locations are far away (good DoP). Here, even with the same error magnitude, the area of possible tag locations is much smaller. This shows that with these measurement locations, we are able to compute the location of the tag with higher accuracy. While we showed this phenomenon in 2D with only 2 measurements, the same principles apply to 3D with more measurements.

To overcome these challenges, we introduce a design of an algorithm that intelligently selects a subset of its 1D measurements to use for trilateration. The goal of this selection is to maximize DoP and measurement SNR (in order to minimize the likelihood of erroneous measurements for each tag and thus improve the robustness of localization). Our measurement selection algorithm consists of the following three steps, which are detailed in Alg. 1:

1. **Initial Filtering.** First, we run an initial filtering step to remove all measurements with an SNR below a threshold τ.[1] This helps eliminate poor measurements that are likely to have high error. Formally, for each measurement m_i, it only keeps the measurement if:

$$SNR_i < \tau \tag{5.1}$$

[1] In our implementation, τ is 4dB

where SNR_i is the SNR of measurement m_i and τ is the SNR threshold.

2. **Measurement Sorting.** Next, we sort all measurements for a given tag based on their location in space. This will allow it to select measurements that provide a good DoP. To do this, we compute the bounding box that contains all measurement locations for this tag. It then splits this bounding box into a 3x2x3 grid, evenly dividing it in each dimension. It assigns each measurement to the grid space where it was taken.

3. **Measurement Selection.** Finally, for each grid space, our algorithm selects the measurement with the highest SNR. If a grid square is empty, it does not select any measurement. Formally, for each grid space g_j, we select the measurement as:

$$sel\_meas_j = \texttt{argmax}_{s.t. g_k = g_j} SNR_k \tag{5.2}$$

   where sel_meas_j is the selected measurement for grid space, and SNR_k is the SNR of the k^{th} measurement.

After selecting 1D measurements, we perform trilateration with outlier rejection similar to [7] to compute a final 3D location. This is repeated for every tag in the environment.

Algorithm 1 Measurement Selection Algorithm

```
for Tag in Tags do
    INITIAL FILTERING
    for m_i in measurements do
        if SNR_i < τ then
            Remove m_i
        end if
    end for

    MEASUREMENT SORTING
    Compute bounding box of all measurements
    Split bounding box evenly into a grid of 3x2x3
    for m_i in measurements do
        g_i ← grid space where m_i was taken
    end for

    MEASUREMENT SELECTION
    for g_j in grid spaces do
        sel_meas_j ← argmax_{s.t. g_k = g_j} SNR_k
    end for

    TRILATERATION
    Perform Trilateration with all sel_meas
end for
```

Chapter 6

Implementation and Evaluation

6.1 Implementation

RFID Reader. We implemented a proof-of-concept prototype of EveryFind with a wideband RFID reader design similar to [14]. We extended the design to use 3 Nuand BladeRF software defined radios [17]: one for the circularly polarized powering signal, one for the horizontal component of the linearly polarized sensing signal and one for the vertical component. For the circularly polarized signal, we used two ZX10Q-2-13-S+ RF power splitters[27] to apply 90° phase shifts. To generate the cross-polarization described in §4, we connected the splitters such that the transmit and receive chains had the same phase shift[1]. At each antenna, the signals for the circular and linear polarization were combined (or split at the reciever) using ZAPD-21-S+ [26] RF power splitters.

We used 4 custom designed bowtie antennas, shown in Fig. 6-1. They were simulated using Ansys High Frequency Simulation Software (HFSS) in order to choose the dimensions that provided an operation between 700MHz and 1GHz, yielding dimensions of 4.5cm by 11cm. The antenna was fabricated on FR4 substrate with a thickness of 0.2cm. A balun was added to the center of the antenna to connect the balanced structure to the unbalanced coaxial cable. The antennas were mounted on acrylic. They were organized in a pinwheel shape so that each antenna was placed in

[1]Since the receiver is the conjugate of the transmission.

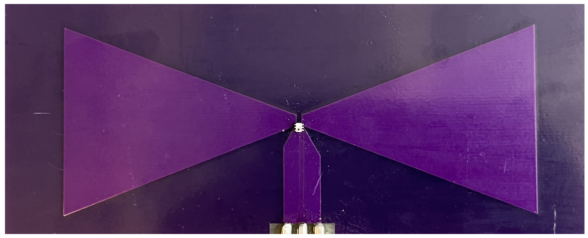


Figure 6-1: Bowtie Antenna. This figure shows EveryFind's custom designed bowtie antenna.

the null of the adjacent antennas, minimizing antenna coupling. We note that while our implementation used four antennas (two transmit and two receiver), the design could be reduced to two antennas by using a circulator.

We implemented the over-the-wire nulling described in §4 using ZAPD-21-S+[26] RF power splitters and the algorithm described in [4].

We note that all cables used in the RFID reader were identical. This prevented large phase offsets that may have impacted the polarizations of the transmitted or recieved signals.

3D Localization. For 3D localization, we tracked the location of the device using an Intel Realsense T265 camera[10] as the user moved throughout the environment.

Software. We connected the BladeRFs to a raspberry pi to collect RFID measurements. We processed the RFID measurements and computed 3D location estimates using an Ubuntu 20.04 computer. We used the SciPy [19] library to perform the trilateration.

6.2 Evaluation

We evaluated EveryFind by placing multiple tags at angles ranging from 0° to 360° on a wooden shelf filled with everyday objects. The shelf was placed in a multipath-rich office environment filled with tables and chairs. We tested our device using Alien Squiggle RFID tags[2]. These are standard off-the-shelf UHF RFID tags that cost around 3 cents.

Ground Truth. We measured the ground truth locations relative to an initial calibration point. For each experimental trial, the device was started at the same initial point to ensure consistency between trials.

Chapter 7

Microbenchmarks

7.1 Change in Phase

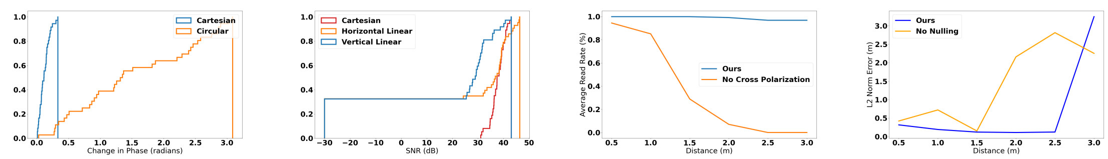
In our first microbenchmark, we evaluated EveryFind's ability to measure the phase of an RFID tag independent of its orientation.

Baseline: We compared our design to the performance of a standard circularly polarized antenna. We used an MTI MT-242025 patch antenna[15] and placed it at the same distance from the tags as our system.

Experiment: We placed the reader and our tag 0.5m apart, and rotated the tag in intervals of 10° around the Y axis (roll). At each angle, we measured the change in phase of the tag (relative to the tag's phase at 60 degrees). We repeated these measurements for multiple frequencies (in the same way that EveryFind collects channel estimates at multiple frequencies). For these experiments, we powered the tag with a separate antenna to ensure that the tag was powered for all trials.

Result: Fig. 7-1a plots a CDF of the change in phase across all measurements for EveryFind (blue) and a circularly polarized antenna (orange). We make the following remarks:

- EveryFind is able to consistently read the tag's phase, with a median change in phase of 0.1 radians and a 90^{th} percentile of 0.2 radians. This demonstrates the ability of EveryFind to read tag phases independent of orientation.



(a) Change in Phase. (b) SNR of Response. (c) Benefit of Cross-Polarization. (d) Benefit of Nulling.

Figure 7-1: Microbenchmarks. (a) plots a CDF of the change in phase across various rotations around the Y axis (roll) for EveryFind (blue) and a circularly polarized antenna (orange). (b) plots the SNR of the tag's response across various rotations around the Y axis (roll) for EveryFind (red), a vertical linear antenna (blue), and a horizontal linear antenna (orange). (c) plots the read rate as a function of distance for EveryFind (blue) compared to a system that does not leverage cross-polarization (orange). (d) plots the 2D localization accuracy as a function of distance for EveryFind (blue) compared to a system that does not leverage over-the-wire nulling (orange).

- In contrast, a circularly polarized antenna has a change in phase ranging from 0.02 to 3.08 radians. This is expected since the tag was rotated at most 90 degrees in these experiments, which would result in an expected change in phase of π radians.[1]

This result demonstrates that circularly polarized antennas fail to read tag phase independent of orientation, and demonstrates the need for EveryFind's approach for localizing RFID tags using acurrate phase measurements.

7.2 Tag SNR

Recall from §2 that EveryFind's leverages a CCP design to generate circularly polarized signals that can read tags across orientations. We evaluated this design's ability to read tags at all angles.

Baselines: We compared EveryFind to two baselines: *Vertical Linear* where a vertical linearly polarized signal was used to read the tag and *Horizontal Linear* where a horizontal linearly polarized signal was used to power the tag.

Experiment: In this experiment, we placed the reader and our tag 0.5m apart and rotated the tag from -180 to 180 degrees in intervals of 10 degrees around the Y axis (roll). At each angle, we measured the signal-to-noise ratio of the tag's response. If

[1]Note that the expected change is phase is twice the tag's rotation. This is because both the transmitter and receiver are circularly polarized, so the phase offset is applied twice

the tag's CRC checksum was incorrect, then the tag could not be successfully read and the measurement was assigned an SNR of -30dB.

Result: Fig. 7-1b plots a CDF of the SNRs across all measurements for EveryFind (red), *Vertical Linear* (blue), and *Horizontal Linear* (orange). We make the following remarks:

- EveryFind is able to achieve a 10^{th}, 50^{th}, and 90^{th} percentile SNR of 35dB, 37dB, and 41dB, respectively. This shows that EveryFind's approach for reading tags is able to perform consistently across all tag orientations.

- *Vertical Linear* and *Horizontal Linear* both had a 30^{th} percentile of -30dB, showing that they were unable to read the tag due to polarization mismatch at more than 30% of the angles.

This microbenchmark demonstrates the importance of EveryFind's design in order to successfully read tags at all angles.

7.3 Measuring Impact of Cross-Polarization

Recall from §4 that EveryFind leverages cross-polarization between its in-band transmitter and receiver to mitigate self-interference. In our next microbenchmark, we evaluated the improvement that this cross-polarization provides in the read range of the device.

Baselines: We compared EveryFind to a partial implementation of our system that does not leverage cross-polarization (i.e., it both transmits and receives RHCP signals). Due to the higher level of self-interference in this implementation, we had to decrease the transmit and receive gains to ensure that the signal was not clipping. [2]

Experiment: We placed more than 30 tags in a 2D plane in the environment at various angles ranging from 0° to 360°. We moved our reader in a 2D plane parallel to the tags at a fixed distance, continuously reading tags in the environment. We

[2] We first decreased the receive gain to the minimum gain.

repeated this experiment at different distances, each time measuring the read rate (i.e., percentage of tags in the environment that were successfully read) for a given distance.

Result: Fig. 7-1c plots the average read rate across all trials as a function of distance for EveryFind(blue), and the system without cross-polarization (orange). We make the following remarks:

- EveryFind's design is able to consistent read tags at all distances up to 3 m, with the read rate only dropping from 100% to 97% over this range.

- In contrast, when not using cross-polarization, the read rate drops significantly as the distance increases. For example, it is only able to read 29% of tags at 1.5m, and cannot read any tags at 2.5m and beyond.

This demonstrates the importance of EveryFind's cross-polarization design for enabling long RFID read ranges.

7.4 Measuring Impact of Over-the-Wire Nulling

Next, we evaluated the impact of EveryFind's over-the-wire nulling. Recall from §4 that EveryFind uses over-the-wire nulling to cancel the self-interference between parallel antenna pairs.

Baseline: We compared EveryFind's performance to that of a partial implementation that did not leverage nulling. Due to the higher level of self-interference, we had to decreased the transmit gain of the system without nulling to ensure the signal did not clip.

Experiment: We placed 6 tags in a 2D plane at various angles. We moved the reader in a 2D plane parallel to the tags at a fixed distance and continuously collected 1D measurements for each tag in the environment. Since our measurements are constrained to two dimensions, we measure the accuracy of a 2D localization process (i.e., we provide one dimension of the ground truth).

Result: Fig. 7-1d plots the 90^{th} percentile 2D error as a function of distance for EveryFind (blue) and the partial implementation (orange). We make the following remarks:

- EveryFind is able to accurately locate tags at long ranges, with only 12cm error at 2.5 m. It is worth noting that beyond 3 m, the error increases because we cannot transmit higher power due to FCC regulations [14].

- In contrast, when not using nulling, the partial implementation is unable to accurately localize past 1.5m, with an error of 2.2m at 2 m.

This demonstrates the importance of EveryFind's over-the-wire nulling for enabling RFID localization at a longer range.

Chapter 8

Performance Results

8.1 Localization Accuracy

To evaluate EveryFind's overall localization performance, we conducted an experiment where different RFID tags were placed in different areas in a fully-furnished indoor environment and across different orientations ranging from 0° to 360°. Each experimental trial included at least 25 RFIDs in the environment. In this experiment, a user carried a EveryFind device and moved around in the environment. During each experimental trial, the system self-localizes using computer vision, estimates the time-of-flight to different tags from each location, and then combines the estimates over space to estimate each tag's 3D location. We captured over 75 location measurements in total. Each RFID's location was accurately measured to obtain the ground truth, and the error is computed as the difference between EveryFind's estimated location and each RFID's ground truth location along each of the x/y/z dimensions.

Fig. 8-1 plots a CDF of the localization error in the X (blue), Y (orange), and Z(green) dimensions. We make the following remarks:

- EveryFind can localize RFID's with a median accuracy of 6 cm, 6 cm, and 7 cm in each of the x, y, and z dimensions respectively. This shows that EveryFind can achieve very high (sub-10 cm) median accuracy in challenging indoor environments.

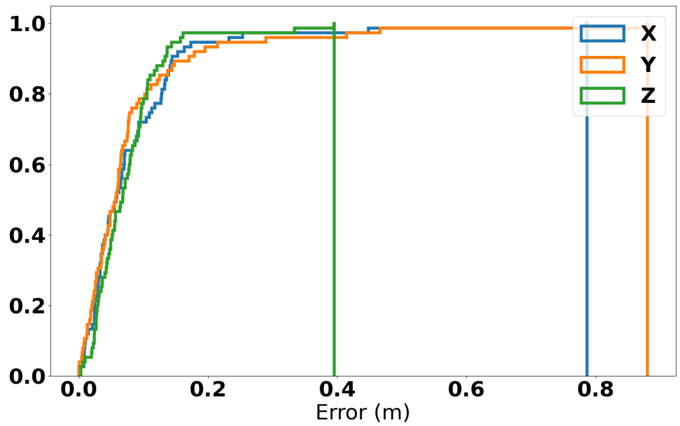


Figure 8-1: Localization Accuracy. This CDF shows the error in the X (blue), Y (orange), and Z (green) dimensions for EveryFind.

- EveryFind's 90$^{\text{th}}$ percentile localization accuracy is 14 cm, 16 cm, and 13 cm in the X, Y, and Z dimensions, respectively. This demonstrates that EveryFind is localization is robust to different locations and orientations.

Comparison to Partial Implementations: Next, we compared the localization accuracy of EveryFind to two partial implementations. The *Vertical Only* baseline relies on only the vertical antennas (transmit and receive) for localizing RFID tags and the *Horizontal Only* relies on only the horizontal antennas. To isolate the impact of powering up the tags from localization, our partial implementations incorporated EveryFind's approach for powering (i.e., by generating circularly polarized signals) but not its approach for localization. Furthermore, to ensure that the comparisons were fair, we used the exact same measurements obtained from the above experiment, the main difference being that we used either the signals obtained from only vertically polarized or only horizontally polarized antennas.

Fig. 8-2 plots a CDF of the L2 norm localization error across all trials and all tags for EveryFind (blue), the *Vertical Only* partial implementation (orange), and the *Horizontal Only* partial implementation (green). We make the following remarks:

- EveryFind's full implementation achieve a median accuracy of 12cm and a 90$^{\text{th}}$ percentile accuracy of 25cm. Note that the L2 norm here matches what one

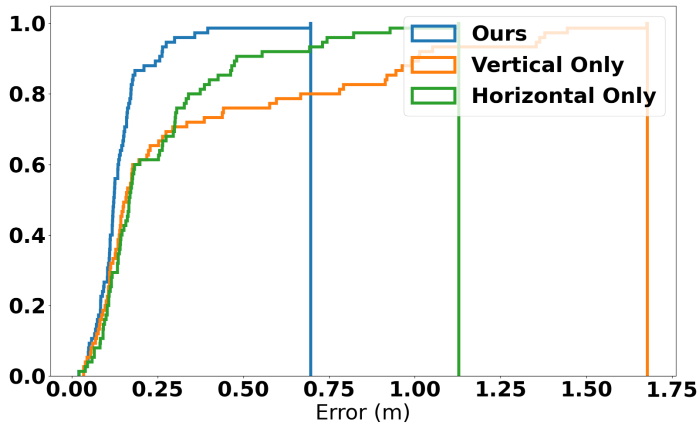


Figure 8-2: Localization Accuracy. This CDF shows the L2 norm error for EveryFind (blue), *Vertical Only* (orange), and *Horizontal Only* (green).

would expect from the earlier reported numbers in the x/y/z dimensions, and demonstrates EveryFind's high 3D localization accuracy

- The *Vertical Only* and *Horizontal Only* partial implementations achieve a median accuracy of 16 cm and 17 cm, respectively. This high accuracy in the median is expected because theses implementations can obtain good SNR across more than half the orientations as per our earlier investigation in Fig. 2-3.

- However, the partial implementations have much poorer 90^{th} and 95^{th} percentile accuracy than EveryFind's full implementation. Specifically, they achieve a 90^{th} percentile of 100cm and 48cm, for vertical and horizontal respectively. And, their 95^{th} percentile is 73 cm and 136 cm respectively, while EveryFind's is 28 *cm*. These errors (nearly two times and four times that of EveryFind) are due to the polarization mismatch between these antennas and some of the tags in the environment, which causes low SNRs. This demonstrates the importance of EveryFind's CCP design to *accurately* and *robustly* localize tags across all angles.

Finally, it is worth noting that we did not evaluate a partial implementation that uses circularly polarized transmit and receive antennas (rather than linearly polarized) since the phase obtained using such antennas is random (as demonstrated in Fig. 2-

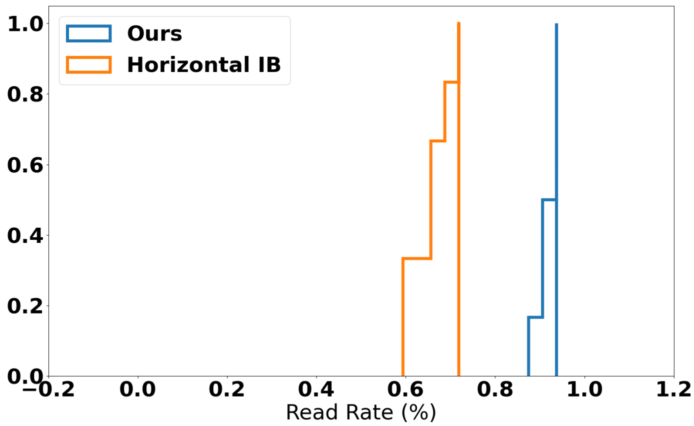


Figure 8-3: Localization Accuracy. This CDF the read rate for EveryFind(blue), and *Horizontal IB* (orange).

2c). Thus, such a partial implementation would lead to random locations and would not be an appropriate baseline.

8.2 Read Rate

Finally, we evaluated EveryFind's ability to read all tags in the environment. Recall from §2 that EveryFind generates a circularly polarized signal in order to read tags regardless of orientation.

We compared EveryFind's performance to a baseline, *Horizontal IB*. In this baseline, we used horizontally polarized signals to read the tags, as opposed to EveryFind's design for generating circularly polarized signals.

In this experiment, we placed RFID tags in different locations and across different orientations (from 0° to 360°). Each experimental trial included at least 30 RFID tags. For each trial, a user carried a EveryFind device around the environment and the device continuously queried tags in the environment. We measured the read rate of each trial (i.e., the percentage of tags that were read). We ran a 6 trials for both EveryFind and *Horizontal IB*. To ensure a fair comparison, each trial followed the same trajectory for both systems.

Fig. 8-3 plots a CDF of the read rate across all experiments. We make the following remarks:

- EveryFind is able to achieve a read rate over 87% in all trials. Additionally, it is able to read over 90% of the tags in 80% of the trials.
- In contrast, *Horizontal IB* only achieves a median of 66% and is never able to read more than 72% of the tags. This is due to the fact that the horizontal signal has a large polarization mismatch with some tags in the environment, preventing them from being powered up (as demonstrated previously in Fig. 2-3).

This result demonstrates the importance of EveryFind's CCP design for robustly reading tags across all orientations.

Chapter 9

Conclusion

In this thesis, I presented the design, implementation and evaluation of EveryFind, a portable hand-held RFID reader that is *efficient*, *accurate*, and *robust*. The major challenge in the design of EveryFind was accurately reading and locating all tags in the environment. Specifically, while circularly polarized antennas are ideal for robustly reading tags, they are ill-suited for localization. On the other hand, linearly polarized signals perform well for localization but fail to read tags at certain orientations. To overcome this challenge, I introduced two techniques: complex-controlled polarization (CCP) and joint tag discovery and localization (JTDL). First, EveryFind leverages two orthogonal linearly polarized antennas to generate both circular and linear polarizations at any angle with CCP. This provides the benefits of both signals and enables accurate and robust RFID reading and localization. Second, to perform these steps simultaneously, I introduced JTDL, an efficient mechanism to measure ultra-wideband channel estimates during a standard RFID discovery round with zero overhead. I demonstrated the benefits of these two techniques, showing that the localization accuracy and read rate of EveryFind significantly outperforms those of the baselines.

Appendix

A: Ideal Combination of Recieved Signals

We show that Eq. 2.5 combines two linearly polarized received signals for optimal recieved power. For each antenna, the received signal is the dot product of the incident signal and the antenna's polarization. Formally,

$$RX_{horiz} = cos(\theta)hx \tag{9.1}$$

$$RX_{vert} = sin(\theta)hx \tag{9.2}$$

where RX_{horiz} is the received signal of the horizontal antenna, RX_{vert} is the received signal of the vertical antenna, h is the channel, and x is the transmitted signal.

Therefore, when combining the signals using Eq. 2.5, we will get

$$RX_{comb} = cos(\theta)cos(\theta)hx + sin(\theta)sin(\theta)h \implies RX_{comb} = hx \tag{9.3}$$

which matches the received signal when there is no polarization mismatch, and therefore is the maximum receive power possible.

B: Proof of Over-the-Wire Nulling

We show that transmitting Eq. 4.3 during over-the-wire nulling will destructively interfere with the self-interference.

First, if EveryFind sends x_{air} over the air, its received signal will have two components: the self-interference and the response from the tag. Formally, the received signal y_{air} is:

$$y_{air} = h_{air}x_{air} + h_{tag}x_{air} \tag{9.4}$$

where h_{air} is the channel of the self interference and h_{tag} is the channel of the tag's response.

When EveryFind sends its nulling signal, it will receive a signal y_{wire}:

$$y_{wire} = h_{wire}x_{wire} \tag{9.5}$$

where h_{wire} is the channel of the wire and x_{wire} is the transmitted nulling signal.

Since the signal from the antenna and the nulling signal are combined, the overall received signal y will be:

$$y = y_{air} + y_{wire} \tag{9.6}$$

$$y = h_{wire}x_{wire} + h_{air}x_{air} + h_{tag}x_{air} \tag{9.7}$$

Substituting in Eq. 4.3 for the transmitted nulling signal x_{wire}, we get:

$$y = h_{wire}\frac{-\hat{h_{air}}}{\hat{h_{wire}}}x_{air} + h_{air}x_{air} + h_{tag}x_{air} \tag{9.8}$$

Assuming that the channel estimates $\hat{h_{air}}$ and $\hat{h_{wire}}$ are perfect estimates, then the overall recieved signal is:

$$y = h_{tag}x_{air} \tag{9.9}$$

Therefore, the self-interference is cancelled and EveryFind is left with only the tag's response.

Bibliography

[1] EPC UHF Gen2 Air Interface Protocol. http://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/2-0-1.

[2] ALN-9640 Squiggle Inlay. http://www.alientechnology.com/wp-content/uploads/Alien-Technology-Higgs-3-ALN-9640-Squiggle.pdf, 2014. Alien Technology Inc.

[3] Zebra MC3190-Z. https://www.zebra.com/us/en/products/spec-sheets-latest/rfid/rfid-handheld/mc3190-z-spec-sheet-en.html, 2022. Zebra Technologies.

[4] Fadel Adib and Dina Katabi. See through walls with Wi-Fi! In *ACM SIGCOMM*, 2013.

[5] AsReader ASR-L251G. https://asreader.com/products/asr-l251g/, 2022.

[6] Bluebird Handheld RFID Reader. https://www.bluebirdcorp.com/products/RFID-Solutions/Handheld-RFID-Reader, 2022.

[7] Tara Boroushaki, Isaac Perper, Mergen Nachin, Alberto Rodriguez, and Fadel Adib. Rfusion: Robotic grasping via rf-visual sensing and learning. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, pages 192–205, 2021.

[8] S. Gollakota, F. Adib, D. Katabi, and S. Seshan. Clearing the RF smog: Making 802.11 robust to cross-technology interference. In *ACM SIGCOMM*, 2011.

[9] Impinj xArray RFID Gateway. https://www.impinj.com/products/readers/impinj-gateways, 2022.

[10] Intel RealSense T265. https://www.intelrealsense.com/tracking-camera-t265/, 2017.

[11] M. Jain, J.I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha. Practical, real-time, full duplex wireless. In *ACM MobiCom*, 2011.

[12] Gregor Lasser and Christoph F. Mecklenbräuker. Self-interference noise limitations of rfid readers. In *2015 IEEE International Conference on RFID (RFID)*, pages 145–150, 2015.

[13] Zhihong Luo, Qiping Zhang, Yunfei Ma, Manish Singh, and Fadel Adib. 3d backscatter localization for fine-grained robotics. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, pages 765–782, 2019.

[14] Yunfei Ma, Nicholas Selby, and Fadel Adib. Minding the billions: Ultra-wideband localization for deployed rfid tags. In *Proceedings of the 23rd annual international conference on mobile computing and networking (MobiCom)*, pages 248–260, 2017.

[15] MTI MT-242025. https://www.atlasrfidstore.com/mti-mt-242025-trh-a-rhcp-outdoor-rfid-antenna-865-956-mhz/, 2022.

[16] Lionel M. Ni, Yunhao Liu, Yiu Cho Lau, and Abhishek P. Patil. Landmarc: Indoor location sensing using active rfid. *Wireless Networks*, 10:701–710, 2003.

[17] Nuand, BladeRF 2.0 Micro. https://www.nuand.com/bladerf-2-0-micro/, 2021.

[18] Taneli Riihonen, Stefan Werner, and Risto Wichman. Mitigation of loopback self-interference in full-duplex mimo relays. *IEEE Transactions on Signal Processing*, 2011.

[19] SciPy. https://scipy.org/, 2022.

[20] Longfei Shangguan and Kyle Jamieson. The design and implementation of a mobile rfid tag sorting robot. In *Proceedings of the 14th annual international conference on mobile systems, applications, and services (MobiSys)*, pages 31–42, 2016.

[21] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[22] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[23] Jue Wang and Dina Katabi. Dude, where's my card? rfid positioning that works with multipath and non-line of sight. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pages 51–62, 2013.

[24] Jue Wang, Deepak Vasisht, and Dina Katabi. Rf-idraw: virtual touch screen in the air using rf signals. In *ACM SIGCOMM*, 2015.

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

[26] ZAPD-21-S+. https://www.minicircuits.com/pdfs/ZAPD-21+.pdf, 2022.

[27] ZX10Q-2-13- S+. https://www.minicircuits.com/pdfs/ZX10Q-2-13-S+.pdf, 2022.