RF-CHORD: Towards Deployable RFID Localization System for Logistic Networks

Bo Liang, *Peking University and Alibaba Group;* Purui Wang, *Massachusetts Institute of Technology;* Renjie Zhao, *University of California San Diego;* Heyu Guo, *Peking University;* Pengyu Zhang and Junchen Guo, *Alibaba Group;* Shunmin Zhu, *Tsinghua University and Alibaba Group;* Hongqiang Harry Liu, *Alibaba Group;* Xinyu Zhang, *University of California San Diego;* Chenren Xu, *Peking University, Zhongguancun Laboratory, and Key Laboratory of High Confidence Software Technologies, Ministry of Education* (*PKU*)

https://www.usenix.org/conference/nsdi23/presentation/liang-bo

This paper is included in the Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation.

April 17–19, 2023 • Boston, MA, USA

978-1-939133-33-5

RF-Chord: Towards Deployable RFID Localization System for Logistics Network

Bo Liang[ℙ𝔸], *Purui Wang*[𝕄], *Renjie Zhao*[𝕌], *Heyu Guo*[ℙ], *Pengyu Zhang*[𝔸], *Junchen Guo*[𝔸]
Shunmin Zhu[𝕋𝔸], *Hongqiang Harry Liu*[𝔸], *Xinyu Zhang*[𝕌], *Chenren Xu*[ℙℤ𝕂✉] [*]
[ℙ]*Peking University* [𝔸]*Alibaba Group* [𝕄]*Massachusetts Institute of Technology* [𝕌]*University of California San Diego* [𝕋]*Tsinghua University*
[ℤ]*Zhongguancun Laboratory* [𝕂]*Key Laboratory of High Confidence Software Technologies, Ministry of Education (PKU)*

Abstract – RFID localization is considered the key enabler of automating the process of inventory tracking and management for the high-performance logistic network. A practical and deployable RFID localization system needs to meet *reliability*, *throughput*, and *range* requirements. This paper presents RF-Chord, the first RFID localization system that simultaneously meets all three requirements. RF-Chord features a multisine-constructed wideband design that can process RF signals with a 200 MHz bandwidth in real-time to facilitate one-shot localization at scale. In addition, multiple SINR enhancement techniques are designed for range extension. On top of that, a kernel-layer near-field localization framework and a multipath-suppression algorithm are proposed to reduce the 99th long-tail errors. Our empirical results show that RF-Chord can localize up to 180 tags 6 m away from a reader within 1 second and with 99th long-tail error of 0.786 m, achieving a 0% miss reading rate and ~0.01% cross-reading rate in the warehouse and fresh food delivery store deployment.

1 Introduction

Today's major e-commerce companies like Alibaba and Amazon need to handle a package volume that is tens of billions per year [1], calling for increasingly high-performance automated logistics operations in their network. Considering a typical warehouse in which tens or even hundreds of packages pass through each checkpoint – the packages need to be verified, recorded, sorted, and tracked when checking in/out. In widely adopted barcode-based logistic networks, the worker spends 1~3 seconds on scanning one package. Although this operation can be automated by robots [2], the line-of-sight and field of view requirements of vision-based approaches limits work range and scalability fundamentally. RFID technology, since its invention, has been carrying the vision of replacing inefficient labor and automating inventory management with zero power, near-zero cost, and high throughput.

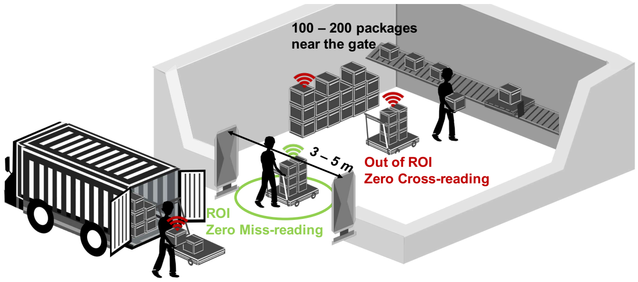


Figure 1: In a typical logistic scenario, the packages are discharged from the truck, scanned at an inventory gate and sorted for warehouse check in. The RFID-based inventory gate should meet *reliability*, *throughput*, and *range* requirements at the same time.

Towards a highly practical and deployable RFID empowered automated logistic network shown in Fig. 1, there are three key considerations: *i) Reliability.* The classic ROI (range of interest) reading task requires the reader to scan all the RFID tags within the ROI (*i.e.,* near-zero miss-reading rate) while excluding any tag out of the ROI (*i.e.,* near-zero cross-reading rate); *ii) Throughput.* The packages come to the checkpoint in a burst (*i.e.,* 100~200 per pallet) [1] while all the logistic operations, including verification and recording need to be finished within 2~3 seconds before check-in/out; *iii) Range.* A single reader should cover tags within 3~5 m, which is the typical width of the check-in/out aisle.

Unfortunately, today's read-or-not inventory systems, both industrial products and research prototypes, all have limitations in meeting these three requirements simultaneously. Industry-grade RFID systems (*e.g.,* Impinj) suffer from miss-reading and cross-reading when deployed in the logistic warehouses. RFGo [3] reports 99.8% recall with 10 carrier-level synchronized antennas and neural network based classifier but limits its operating range to sub-meter. NFC+ [4] achieves a sharp inventory boundary with magnetic resonance engineering that meets the reliability (*i.e.,* miss-reading rate of 0.03% and cross-reading rate of 0%) and range (~3 m) requirements but cannot achieve the desired throughput. No current inventory-based solutions can support automatic package management in a practical logistics network.

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

[*] Bo Liang and Purui Wang are the co-primary student authors. Purui Wang was affiliated to Peking University and Alibaba Group during which he contributed to this work.
✉: chenren@pku.edu.cn

[1] Even though one trailer can carry up to 50 packages, the reader should be able to cover all the tags (100~200 tags) near the gate (including passed trailer and undischarged packages) to ensure to read all the passing packages.

ROI reading depends on localization accuracy. However, the legitimate narrow frequency band (*i.e.,* 26 MHz ISM band within 902~928 MHz) of RFID fundamentally limits its capacity of combating multipath and ambiguity [5]. To improve the localization accuracy, approaches like fingerprinting [6] and synthetic aperture radar (SAR) based hologram [7, 8] have been proposed. However, they suffer from prolonged latency due to lots of tag inventory, especially at scale. Cross-frequency based approaches utilize higher frequency band to overcome the bandwidth limitation (*e.g.,* 2.4 GHz [9, 10], millimeter wave [11], UWB [12, 13]) but introduce extra tag manufacturing cost due to wider frequency response and higher power attenuation. More recently, sniffer-based RFID architecture [14, 15] has been proposed to leverage the advantage of wideband (*e.g.,* 100~200 MHz) near 915 MHz to boost location accuracy without violating FCC regulation. Despite the potential, these systems either suffer from latency issues due to the lack of hardware support on multi-band parallel information capture [14], or report limited sub-meter range [15].

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

RF-CHORD ensures *high reliability* (*i.e.,* near zero miss reading and cross reading) by high-accuracy localization. Our study (§5.1) shows that the multipath profile causes long-tail localization errors. Therefore, we design the fine-grained distance resolution hardware and multipath-suppression algorithm to handle these long-tail errors. Considering that the distance resolution is inversely proportional to bandwidth (*i.e.,* $\frac{c}{2B}$), the distance resolution of a conventional UHF RFID reader, which works on a 26 MHz wide ISM band, is only 5.78 m. RF-CHORD introduces an extra active sniffer-based reader to help UHF RFID reader realize 200 MHz parallel wideband localization (§3.2). However, the distance resolution of 200 MHz (0.75 m) is still not enough in all situations. RF-CHORD exploits a kernel-layer-based near-field localization algorithm framework to handle corner cases. The kernel function characterizes the location estimation from a single channel, and layer functions coherently combine multiple channels into a final location estimation. This framework supports choosing different kernel and layer functions suitable for various deployment scenarios to achieve multipath suppression and ambiguity reduction (§5.3). For example, in RF-CHORD's deployment in the warehouse, the work range is fixed so it can be taken as prior information for direct path enhancement to effectively suppress the multipath effect (§5.4).

RF-CHORD ensures *high throughput* by one-shot channel measurement and one-shot location estimation. The hardware supports concurrent phase and amplitude capture across multiple antennas and wide bandwidth. Therefore, RF-CHORD can obtain the necessary information (*i.e.,* wideband channel estimation across multiple antennas) for localization within only one shot measurement. It is challenging because: i) directly capturing the wideband signal from a large array will result in a huge amount of real-time data (~64 Gbps); ii) the commercial reader does not support real time synchronization (*i.e.,* synchronizing with our sniffer-based reader at each slot [18]). Utilizing the essence that the wideband backscattered signal is a combination of scattered narrowband signals, RF-CHORD distills 4 MHz valid bandwidth from 200 MHz bandwidth to reduce the data rate by 50x without information loss (§3.4). Meanwhile, we develop a GPU-based wideband decoder to ensure real time decoding and channel estimation. In other words, the sniffer-based reader has an independent decoder and does not depend on any specific commercial reader interface. It makes our design adaptive to any ISM band commercial reader, which primarily serves as a power activator and multiple access handler (§4). Finally, RF-CHORD supports one-shot localization with 8 antennas and 16 frequencies across 200 MHz in ~5 ms.

RF-CHORD ensures *long range* (up to 6 m) with multisine waveform sniffer and sophisticated wideband channel information estimation. To follow the FCC regulation, the strength of the sniffer excitation signal needs to be *smaller than -13.3 dBm* (see §A for the calculation), which is 50 dB weaker than that of commercial readers. RF-CHORD features the following designs for signal-to-interference-plus-noise ratio (SINR) enhancement without modifying the tag chip: i) It exploits a multisine waveform, which constructs a whole 200 MHz band by taking samples with multiple narrow bands, to significantly reduce the noise bandwidth (§4.1); ii) It handles the high dynamic range requirements introduced by self-interference through high-resolution digital channelization and a low crest factor waveform design (§4.2); iii) It further exploits the integration gain of full packet matching (§4.3) and performs accurate tag clock offset mitigation (§4.4) and decoding with channel diversity (§4.5).

We deploy RF-CHORD and our results show that RF-CHORD presents the first RFID (localization) system meeting all the requirements (*i.e.,* reliability, throughput, and range) in the logistic network (Tab. 1). The key results are:

- **Reliability.** We evaluate RF-CHORD's performance at 384 locations and collect over 20k tag responses in the lab environments. Its 99% localization error is 0.786 m. We deploy RF-CHORD in the dock door of a warehouse and the scanning gate of a fresh food delivery store. We find that it could read 100% of the tags passing the checkpoint (0% miss-reading rate). Its cross-reading rate is only 0.0025%~0.0154%, which is up to 12x improvement compared to state-of-the-art [3, 4].
- **Throughput.** RF-CHORD can localize up to 180 tags per second, which is very close to pure inventory devices [16] and

Requirements Solutions	Throughput (> 100 tags/s)	Range (> 3 m)	Reliability (Near Zero Miss-reading & Cross-reading)	Commercial Tag
Barcode (widely deployed)	No (~1 tag per second)	No (~1 m)	High (depend on the human labor)	Yes
xSpan [16] (Inventory based)	Yes (~185 tags/s with 142 mode)	Yes (~10 m)	Low (~6% miss reading and ~2% cross reading)	Yes
RFgo [3]	No (TDMA-based)	No (sub-meter)	High (99.8% recall)	Yes
NFC+ [4]	No data reported	Yes (~3 m)	High (0% miss reading and ~0.03% cross reading)	No
PinIt [6]	No data reported	Yes (> 5 m)	Median (a few decimeters)	Yes
RF-IDraw [17]	No data reported	Yes (> 5 m)	Low (sub-meter)	Yes
Tagoram [7]	No (0.2 second for one tag)	No (~2 m)	Median (a few decimeters)	Yes
MobiTagbot [8]	No data reported	No (~1.5 m)	High (a few centimeters)	Yes
NLTL tags [9]	No (depend on switching)	No (~1 m)	High (a few millimeters)	No
mmwave RFID [11]	No data reported	No data reported	Median (a few decimeters)	No
RFind [14]	No (6.4 second for one tag)	Yes (> 5 m)	High (a few centimeters)	Yes
TurboTrack [15]	No data reported	No (sub-meter)	High (a few centimeters)	Yes
RF-Chord (Our system)	**Yes (180 tags/s)**	**Yes (6 m)**	**High (0% miss reading and ~0.01% cross reading)**	**Yes**

Table 1: Comparing RF-Chord with state-of-the-art wireless systems for logistic network requirements.

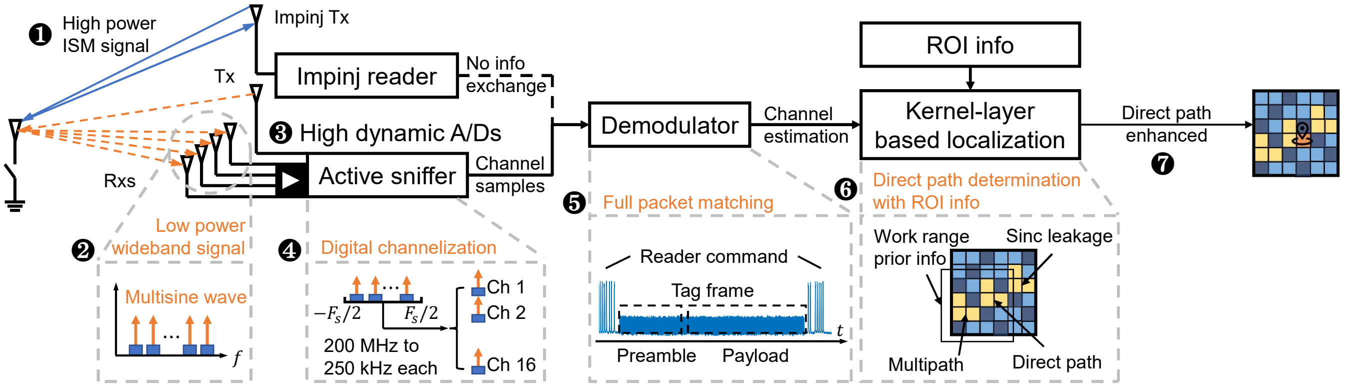


Figure 2: RF-Chord system overview.

two to three orders of magnitude faster than state-of-the-art localization systems [7, 14].

- **Range.** RF-Chord can localize tags 6 m away from the reader with transmit power below -15 dBm. There is no obvious throughput and reliability loss with distance increasing.

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

2 RF-Chord's System Overview

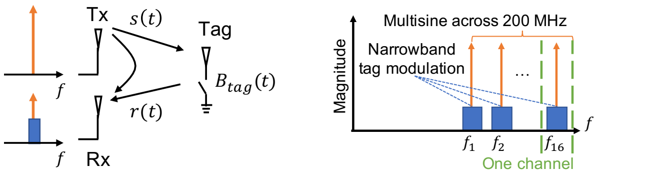
A high level operational flow of RF-Chord is shown in Fig. 2. RF-Chord embraces any ISM-band reader ❶ as the tag activator that is capable of charging, coordinating multiple access over EPC Gen II tags. Active sniffer reader observes tags by emitting a low power (-15 dBm) wideband multi-sine waveform to pick up tag responses over a wide frequency band. Specifically, we build the RF frontend and FPGA hardware ❷ as a scalable platform that can receive the tag response from 8 antennas and 16 frequencies of carriers simultaneously. Furthermore, despite the strict legal emission power limit, we still achieve a long range in sniffing the tag response in the wideband without exchanging any information (*e.g.,* EPC ID) with the ISM-band reader. RF-Chord achieve independent decoding and channel estimation by using dynamic range optimization ❸, digital channelization ❹ in hardware, and a real-time full packet matching ❺ in software. After one-shot tag inventory, RF-Chord obtains adequate information from both frequency and spatial domains, which are important for robust localization in a multipath-rich environment. RF-Chord also uses a kernel-layer-based near-field localization algorithm to suppress the multipath effect. This algorithm identifies the direct path with the time of flight profile and prior knowledge (region of interest or ROI information in our paper) ❻. Then it enhances the direct path and estimates the location with a summation layer (a form of near-field AoA+ToF localization) ❼.

3 One-shot Wideband with Multisine Wave

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

3.1 Backscatter Signal Model Primer

The basic backscatter operation in RFID systems is shown in Fig. 3a. A device emits a high-power single-tone excitation signal $s(t)$ to power the tag and act as a carrier. This carrier will be modulated by the baseband signal $B_{\text{tag}}(t)$ of the tag.



(a) Single-tone Backscatter. (b) Multisine Excitation Signals.

Figure 3: Model of Multisine Backscatter.

The resulting (mixed) backscattered signal is:

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

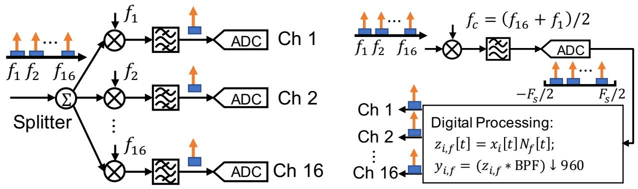
Note that the bandwidth of $r(t)$ is the summation of that of s(t) and $B_{\text{tag}}(t)$, and $B_{\text{tag}}(t)$ is typically a narrowband signal[2] for low power purpose according to the EPC Gen II standard. Therefore, the backscattered signal $r(t)$ will also be narrowband given that $s(t)$ is a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

3.2 Backscattering with Wideband Multisine Wave

When applying a wideband signal $s(t)$, one can retrieve a wideband backscatter signal $r(t)$. Following this idea, RF-CHORD adopts a multisine signal as $s(t)$. The multisine signal is a combination of multiple single tones across wide band with the same amplitude $s(t) = \sum_i \sin(f_i t + \phi_i)$. The backscattered signal will be $r(t) = \sum_i B_{\text{tag}}(t) \cdot \sin(f_i t + \phi_i)$. RF-CHORD adopts 16 carriers with different frequencies across a 200 MHz band in the practical implementation. Fig. 3b shows the spectrum of multisine signal $s(t)$ with backscatter signal $r(t)$. Since the difference between each carrier frequency is much larger than the bandwidth of $B_{\text{tag}}(t)$, the received signal can be treated as multiple copies of $B_{\text{tag}}(t)$ modulated on different carrier f_i. Therefore, on Rx, $r(t)$ can be sliced to 16 individual narrowband channels without information loss, and then the channel information at each carrier frequency f_i can be extracted by using a well-explored RFID processing mechanism (*e.g.,* mixing and demodulating) in parallel. In a nutshell, we sample the wideband with multiple narrowband signals, enabling RF-CHORD to construct the wideband channel information within one shot.

3.3 Why Multisine Wave

The multisine waveform has two advantages. First, the multisine waveform is adaptive to conventional narrowband decoding and channel estimation because the signal in each channel is still narrowband. Extracting these narrowband signals can achieve excellent data rate compression (§3.4). Second, the multisine waveform is amenable to noise and interference reduction because of the low noise bandwidth and low chances of being interfered with, resulting in SINR enhancement, which improves the work range (§4.1). Compared with the two alternative well-known wideband waveform choices, frequency hopping [14] and OFDM signal [15], the multisine waveform is more efficient because it avoids the time overhead in switching between carriers introduced by the former one, and uses the same bandwidth as the (tag) modulation bandwidth, which is 250 kHz out of the full 200MHz bandwidth used by the latter one. In fact, this wideband but narrow sample signal can introduce 29 dB gain on the SINR compared to the full wideband signal (see §4.1), which means around 5× range under the same transmit power. Furthermore, since the multisine wave captures all the backscatter signals in the time domain, the whole packet of tags can be fully utilized for integration gain to improve the SINR (see §4.4).



(a) Analog Channelization. (b) Digital Channelization.

Figure 4: Two channelization approaches.

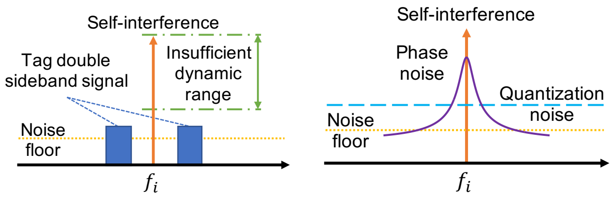
3.4 Digital Wideband Channelization

RF-CHORD utilizes channelization, which enables one-shot capturing of wideband signals across multiple antennas and reduces the amount of data to be processed during real-time operation. Channelization is a process of extracting effective narrowband signals from a received signal. When a wideband tag signal is received, the aggregated bandwidth of 8 antennas will be 1.6 GHz, resulting in a total of 64 Gbps data (16-bit IQ sample, 1.25× Nyquist). It is challenging to process such massive data in real time. However, recall that with a multisine excitation signal, the effective tag signal is only located around the carrier frequencies, as shown in Fig. 3b. Therefore, the effective bandwidth of the system should be 8 × 16 × 250 kHz = 32 MHz, only 1/50 of the full 200 MHz bandwidth, so that channelization can compress the data validly without information loss.

There are two channelization schemes to extract these narrowband signals: analog channelization and digital channelization. As shown in Fig. 4a, the sniffer with analog channelization has multiple RF chains for the corresponding channels. Each RF chain uses one carrier frequency f_i as its local oscillator (LO) for down-conversion and a filter at the baseband to filter the signal from other channels out. Alternatively, digital channelization finishes all the aforementioned functions in the digital domain as shown in Fig. 4b.

RF-CHORD adopts digital channelization – the sniffer will generate and capture the whole multisine wave with one RF chain. On the Rx side, an ADC/DAC with a 245.76 MHz sampling rate captures all tag signals simultaneously. Further channel extraction can be achieved by digital down-conversion and digital filtering. Digital channelization offers two significant benefits over analog channelization: First, it has better scalability because it only needs one RF chain for each antenna, regardless of the number of channels (and sine

[2] We take 250 kHz as the bandwidth $B_{\text{tag}}(t)$ for the whole paper according to the standard [18].



(a) Dynamic Range.

(b) Unpredictable Noise.

Figure 5: Two issues caused by self-interference.

tones) are required, while in analog channelization, each channel needs an exclusive RF chain with bulk components (*e.g.,* mixer, PLL, and VCO). Second, it is precisely synchronized among different tones in the multisine wave, while analog channelization needs extensive engineering efforts to synchronize among a large amount of ADCs/DACs and LOs. Nevertheless, analog channelization still has it own advantages, including the convenience of extending or switching bandwidth by changing the carrier frequency and the lower requirements of ADC bandwidth. RF-Chord also embraces these advantages through the high-speed ADC and low crest factor multisine waveform, which will be introduced in §4.

4 SINR Improvement for Long Range

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

4.1 External Noise Suppression

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

RF-Chord adopts the tag signal with reduced bandwidth for lower chances of in-band interference and lower noise. The relationship between thermal noise P_{noise} and signal bandwidth B at room temperature can be expressed as $P_{\text{noise}} = -174 + 10\log_{10}(B)$ [19]. As described in §3.4, the digital channelization at the receiver separates a combined 200 MHz wideband signal into multiple 250 kHz narrowband signals. This means that the thermal noise can be reduced from -91 dBm to -120 dBm (29 dB gain). Furthermore, the reduced bandwidth also reduces the probability of being interfered with by other devices working in the same band.

4.2 Self-interference Canceling

Besides the external interference from other devices, the self-interference caused by the natural full-duplex operation of our active sniffer will also limit the SINR. RF-Chord's multisine waveform and low power transmission reduce the complexity of self-interference cancellation. As shown in Fig. 5a, the self-interference in one channel is just a single tone after channelization. A commercial tag uses double-sideband modulation with a subcarrier to differentiate the tag signal from the single-tone excitation signal. Therefore, RF-Chord uses filters to cancel the self-interference caused by the single tone.

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

Dynamic Range. Dynamic range is the ratio between the largest and smallest values that the received signal can assume. Specifically, the largest value is the self-interference, and the smallest signal is the targeted wideband tag signal. As shown in the Fig. 5a, even though the tag signal strength is higher than the noise floor and interference, it can still be buried if the dynamic range is not large enough. RF-Chord meets the requirement of dynamic range by adopting the following strategies: First, it adopts a high-resolution ADC because the dynamic range of the receiver will be bottlenecked by the dynamic range of the ADC. The theoretical dynamic range of the receiver is 6.02 N + 1.76 dB [20], where N is the resolution of the ADC. Therefore, a fundamental way to solve the issue is to increase the resolution of the ADC. RF-Chord adopts 16-bit ADC, which has the largest resolution in 2022 when satisfying the 200 MHz bandwidth requirement. Secondly, it adopts a carefully designed low crest factor multisine wave on the transmission side to relax the dynamic range requirement of the Rx. The intuition behind this is that since the dynamic range requirement on the ADC is more related to the peak amplitude of the self-interference signal instead of the average signal power, it can be relaxed by using a lower peak signal while remaining the average power. The crest factor is the peak amplitude divided by the RMS value of the waveform, and for a multisine signal, it has been well studied that the crest factor can be reduced by tuning the phases ϕ_i in the multisine signal. Following the methods mentioned in [21], the crest factor of the multisine waveform adopted by RF-Chord can be reduced from 4 to 1.24 (or peak-to-average power ratio from 12 dB to 1.87 dB).

Unpredictable Noise. The unpredictable noise is caused by the response of self-interference in the circuit. As illustrated in Fig. 5b, the noise floor may be dominated by the phase noise, DAC quantization noise, *etc.* along with the self-interference. Fortunately, RF-Chord does not require a dedicated cancellation circuit like [22] because the power of RF-Chord's self-interference is much lower than that of a commercial RFID reader. Moreover, RF-Chord utilizes Analog Devices ADRV9009 transceiver of 16-bit ADC [23] and HMC7044 VCXO-based clock tree [24], ensuring an optimal quantization and clock phase noise below the noise floor. Therefore, the RF frontend of RF-CHORD's receiver is not saturated, and the noise will only go through the air instead of the feedback path of the receiver. The noise experienced by RF-CHORD is not dominated by unpredictable noise.

4.3 Full Packet Matching

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

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

where $r(t)$ is received tag response and $\hat{I}(t)$ is a template. In most RFID systems, only the pilot signal part (RN16) is used for clock and phase estimation, and the main part of the tag signal (EPC ID) is left unused. RF-CHORD utilizes the full packet signal, including RN16 and EPC ID. The length of the signal will be extended from 0.31 ms to 2.31 ms when assuming the backscatter link frequency (BLE) of the tag is 250 kHz and the EPC ID length is 96 bits [25]. By doing the full packet matching, RF-CHORD can achieve $10\log_{10}\frac{2.31}{0.31} = 8.7$ dB integration gain.

We need to generate a noiseless template of the full packet for full packet channel estimation. However, unlike the predefined pilot signal, the template of the packet changes depending on the tag's EPC ID. Collecting EPC ID and timestamp from a commercial reader device in real-time is unsupported due to the interface limitation: i) the available interface from a commercial reader is usually done by using asynchronous communication, which hinders real-time processing; ii) the timing information is usually not reported by commercial readers. Therefore, RF-CHORD needs to decode the wideband signal into EPC ID independently.

4.4 Clock Offset Mitigation

Accurate decoding needs to mitigate the clock offset of the RFID tag signal. Specifically, the protocol tolerates up to ± 10% frequency offset and ± 2.5% frequency fluctuation during backscattering (refer to Tab. 6.9 of [18]). For example, say we read a tag that is 2.5% faster than nominal BLF. For a typical randomized uplink packet of 128 bits with a perfect match at the start of the frame, the received signal will be ahead of the template by one bit at the 32nd bit, and the remaining 96 bits thereafter contribute useless fluctuations to channel estimation, as figured out in Fig. 6. RF-CHORD needs to analyze the clock and estimate the offset parameters for mitigation, which can be described by:

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

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

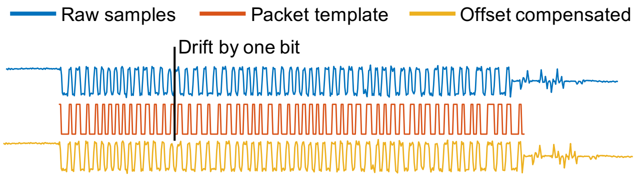


Figure 6: The waveforms of the tag signal with clock offset, the reference, and recovery signal from the offset.

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

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

PLL to Track $\alpha(t)$ Variation. After eliminating α_0, the clock still has residual offset $\alpha(t)$, which comes from the tag clock fluctuation during the communication and may be significant in the long packet. Because the Miller code of RFID [18] is a self-clocked and modulated bandpass signal, RF-CHORD can extract the subcarrier of the line code to track the clock frequency offset accurately. RF-CHORD adopts a feedback-based digital Costas PLL [26] to track the clock continuously.

After compensating estimated clock $\tau(t)$, the clock offset is mitigated (the last waveform shown in Fig. 6). We can see that the signal is well synchronized with the template.

4.5 Decoding with Channel Diversity

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

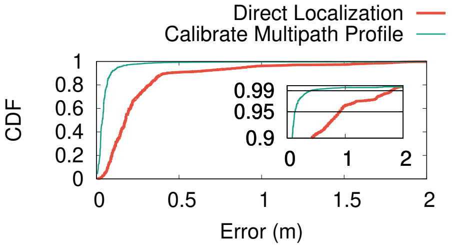


Figure 7: Eliminating the multipath effect reduces the 99th long-tail error.

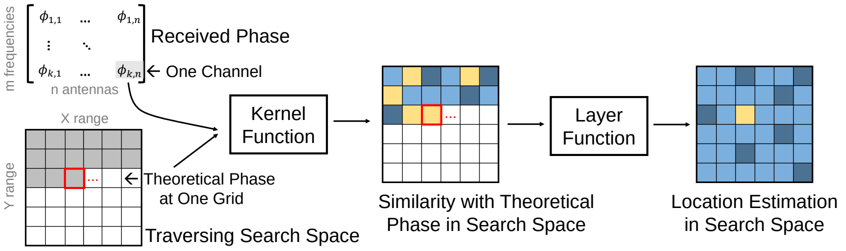

m frequencies
$\phi_{1,1}$ ... $\phi_{1,n}$
$\phi_{k,1}$ ... $\phi_{k,n}$
n antennas
Received Phase
← One Channel
X range
Y range
← Theoretical Phase at One Grid
Traversing Search Space
Kernel Function
Similarity with Theoretical Phase in Search Space
Layer Function
Location Estimation in Search Space

Figure 8: Kernel-Layer Framework.

5 Localization with Kernel-Layer Framework

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

5.1 Long-tail Errors Source Demystification

We conduct a validation experiment to confirm that multipath is the primary source of long-tail localization errors. In this experiment, we put five tags at a distance of 4 m from the reader. We use 16 carriers evenly spaced across 200 MHz bandwidth, 8 antennas, and a hologram-based localization algorithm (see details in §5.2). There is a metallic heater 1.5 m from the tag as the multipath source. Fig. 7 shows that the 99th localization error (red line) is 1.798 m, too large to ensure reliable usage in industry settings. The theoretical analysis explains this observation – the 200 MHz bandwidth is only able to differentiate paths that have a propagation distance difference larger than $c/(2B) \approx (3\times10^8\ \text{m/s})/(2\times 200\ \text{MHz}) = 0.75$ m. Once the propagation distance of two paths is smaller than 0.75 m, which is common for many indoor deployments, 200 MHz is insufficient for differentiating one from the other.

Then we evaluate the performance without the multipath effect to check our results double. We keep the experiment setup, conduct RF measurement of a reference tag close to target tags and extract its phase offset from the groundtruth. Considering that the multipath profiles of nearby tags are similar, we subtract each tag's channel estimation with the offset from the reference tag. The 99th localization error of the same set of tags decreases to 0.400 m (green line in Fig. 7). It proves that multipath is the primary factor determining the long-tail performance of the RFID localization system, even with 200 MHz bandwidth.

5.2 Near-field Localization with Hologram Algorithm

Like most recent RFID localization systems, RF-CHORD locates a tag under the *near-field* condition, which differs from locating a distant target. Considering the Fraunhofer distance [27], a target is at near-field when its distance d from the antenna array meets:

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

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

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

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

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

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

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

5.3 Kernel-layer Framework

Beyond the basic hologram algorithm [28], there are many hologram variants [7, 8, 29, 30]. We find that two key factors determine the performance of hologram-based localization algorithms, namely, kernel and layer:

Definition 1. Kernel is the function that measures the similarity between the received signal and the theoretical signal

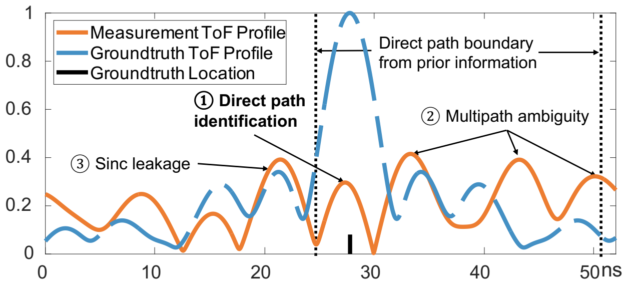


Figure 9: Direct Path Identification with ROI Information.

from one channel (*i.e.,* single carrier from a single antenna). For example, the $e^{j(\phi-\theta)}$ in Eqn. 1 is a kernel function that measures the phase similarity with an exponential function.

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

We introduce a kernel-layer framework that tells us how kernel and layer affect the localization performance. Fig. 8 summarizes our kernel-layer framework, which describes the fundamentals of hologram-based algorithms. This framework can be used following these steps:

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

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

5.4 RF-Chord's Kernel and Layer

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

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

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

ToF Profile Layer. By using the wideband bandwidth captured, this layer computes the time-of-flight profile of the received signal. The computation follows Eqn. 2 where ϕ is the empirically measured phase value, f_l is the frequency, and τ is the propagation delay of each path.

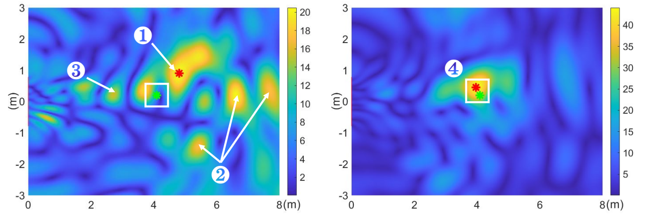
$$\text{ToF estimation layer: } S(\tau)=\sum_{l=0}^{L} e^{-j(\phi_l-2\pi f_l\tau)} \tag{2}$$

Direct Path Identification Layer. It is still challenging to identify the direct path in the ToF profile layer in Fig. 9 because there are three interfering factors: ① If the difference is smaller than 0.75 m, we can only observe one mixed peak in the time-of-flight profile of the received signal. ② If the difference is larger than 0.75 m, there will be ambiguity from multipath at the locations farther from the groundtruth. ③ The sample on the frequency domain, which is a sinc function on the time domain, may leak its side lobe and form fake peaks at a nearer location than the groundtruth. To address these problems, RF-Chord leverages a key observation: prior information. In practical logistic deployment, we can employ the size of the scanning area, the track of tags, *etc.* to help localization. RF-Chord constructs a layer that leverages this prior information for direct path identification. Fig. 9 shows an example of this layer with scanning range [a,b] in meters as prior information, which is common in warehouse deployment. The corresponding algorithm is shown in Alg. 1. In this example, we first compute the bound of the theoretical propagation time in this range $\tau_a = a/(3\times10^8)$ and $\tau_b = b/(3\times10^8)$. The prior information, τ_a and τ_b, acts as a filter that eliminates any multipath with a propagation time smaller than τ_a or larger than τ_b, which helps us identify the right direct path (right peak) rather than nearer one from sinc leakage or farther one from multipath.

Algorithm 1 Direct path identification layer

```
Input: 1. ToF profile: $[S(\tau_1), S(\tau_2), ..., S(\tau_s)]_{1\times s}$
    2. Prior info: scanning area in meters [a,b]
    3. Peak threshold: p
Output: Direct path distance rough estimation $\tilde{d}_0$
    1. $\tilde{d}_0$ = 0, $\tau_a = \frac{a}{3\times10^8}$, $\tau_b = \frac{b}{3\times10^8}$;
    2. L = find $\tau_i$ closest to $\tau_a$ in [$\tau_1$, $\tau_2$, ..., $\tau_s$], return index;
    3. R = find $\tau_i$ closest to $\tau_b$ in $[\tau_1, \tau_2, ..., \tau_s]$ , return index;
    4. $S(\tau) \leftarrow S(\tau)$[L : R];
    5. $path \leftarrow S(\tau)[0 : \text{end}-1] - S(\tau)[1 : \text{end}]$
    for $i \leftarrow 1$ to $s-1$ do
        if $path[i] > 0$ & $path[i-1] < 0$ & $S(i) >$ p then
            $\tilde{d}_0 = \tau_i \times 3\times10^8$;
            break;
        end if
    end for
```

Direct Path Enhancement Layer. RF-Chord uses a across-frequency phase redress algorithm to further enhance the signal quality of the direct path signal. RF-Chord first identifies potential multipath – if there are multiple peaks (identified by



(a) Basic Hologram. (b) RF-CHORD's Algorithm.

Figure 10: RF-CHORD can suppress sinc leakage, multipath ambiguity, and enhance direct path for finer resolution compared to basic hologram algorithms in Eqn. 1.

2D peak find algorithm [31]) in the basic hologram results, the location estimation is likely affected by the multipath effect. Instead of using the empirically measured phase ϕ, RF-CHORD combines the direct path signal from all frequencies and constructs an enhanced phase $\tilde{\phi}_l$. This process is done by the layer function of Eqn. 3. See §C for detailed mathematical derivation.

Direct path enhancement layer: $\tilde{\phi}_l = \angle \sum_{i=1}^{L} e^{j\phi_i} e^{j\frac{2\pi}{c}(f_i - f_l)\tilde{d}_0}$ (3)

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

Summation layer: $P(g_{(i,j)}) = \left| \sum_{l=0}^{L} \sum_{k=0}^{K} e^{-j(\tilde{\phi_{l,k}} - \theta(g_{(i,j)}, l, k))} \right|$ (4)

Putting Everything Together. All above layers and kernel work together as our multipath suppression algorithm. Fig. 10 shows an visual example. The heatmaps are the location likelihood with the basic summation layer in Eqn. 1 (Fig. 10a) and with our direct path enhancement algorithm (Fig. 10b). The green cross is groundtruth and the red cross is location estimation. If we only use the simple summation layer, there are three factors disturbing the localization accuracy. RF-CHORD handles them with customized kernel-layer algorithm design. The peak of location estimation ① is the superimposed responses from all the paths within distance resolution nearer the direct path. RF-CHORD utilizes coherent summation layer with full 200 MHz bandwidth to increase distance resolution to 0.75 m. The paths with large distance differences from the direct path will generate ambiguity at farther arrival distances as multipath ambiguities ② or even at nearer distance as sinc leakage ③. By using prior information of work range (tags are in different check-in passage with different ranges) to clarify the direct path identification and using direct path enhancement to suppress multipath, we obtain the accurate location estimation ④.

6 Implementation

6.1 Active Sniffer

Antenna. We chose a recent variant [32] of the Foursquare patch antenna [33], which is metal-backed and of concentric dual-polarization, as our wideband Tx and Rx antennas for its advantages of small-size, low-cost, and high adaptability to surroundings. The original antenna design is for 1.7~2.7 GHz LTE and we scaled it with HFSS [34] to fit the UHF band 700~1100 MHz. We also attached each Rx antenna to a 915 MHz bandstop filter [35] to suppress the high-power ISM-band leakage from the commercial reader.

Array. We built the Rx array through a laser-cutting sheet of aluminum. The mounting holes and SMA clearances on the sheet define a 1×8 linear array with element spacing of 21 cm. We set a notable 31.5 cm gap in the middle for a 2:3 co-prime array configuration [36] to suppress the grating lobe. We hang two Txs 0.4 m lower than the receiver's horizontal array along its geometric bisection. The right one was wideband Tx and the left one was ISM-band Tx.

Baseband Processor. One of the key implementation challenges towards one-shot inventory is to convert the 31 Gbps I/Q samples from the A/D to the application processor. We developed high throughput baseband with 2 ADRV9009 [23, 37] RF chips and an XCKU060 FPGA SoM [38, 39] in charge of 4 receivers over 200 MHz bandwidth for PCIe streaming.

Application Processor. The host is equipped with a Core-i9 9900 CPU and an RTX 3090 GPU for real-time decoding and CSI acquisition. GPU was used to handle the template matching during the decoding with FFT convolution acceleration and parallelism. We used Process Explorer [40] to measure resource utilization and report the results in Tab. 2. The decoder is developed with C++/Eigen except that the most compute-intensive part, *i.e.,* the full packet matching algorithm, is implemented on GPU with CUFFT [41].

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

Table 2: Hardware Resource Utilization.

6.2 RFID Tags

In order to ensure compatibility and low-cost, we used a commercial RFID IC Impinj Monza-M4A [42] and implemented a bandwidth extension technique [43] to redesign the metal inlay (antenna) on 80 × 80 mm single-sided PCB. The CAD of the RFID antenna is shown at the top left of Fig. 11 and its direction gain (similar to dipole antenna) is shown in Fig. 15a. It works on 700~1000 MHz, whose copper geometry can be transferred to flexible inlay for massive production.

7 Evaluation

7.1 Experimental Setup

Testing Environment. We evaluate RF-CHORD in an office with multiple reflectors (*e.g.,* metal furniture, low ceilings,

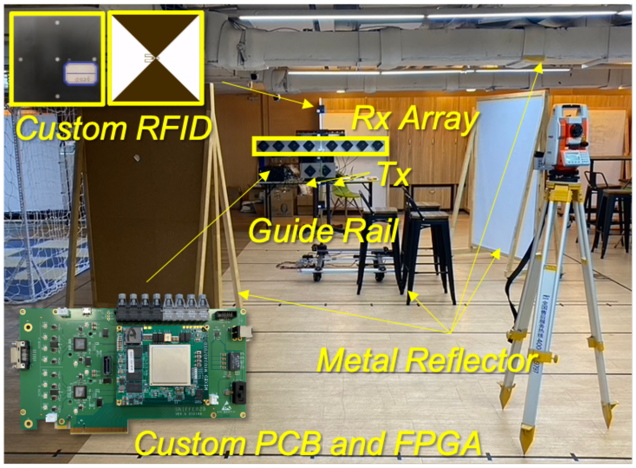


Figure 11: Experimental setup for evaluating performance. Five tags are mounted on the rail and ~20k tag responses are collected in 384 locations.

and walls). The evaluation range is the area of 6 × 3.2 m ahead of the antenna. We divide the evaluation space into 20 cm grids and use guide rails to move the tags. All the tags are facing the array. The dataset containing about 20k wideband RFID channel information measurements at 384 locations is open-sourced at [44]. The setup is shown in Fig. 11.

Location Groundtruth. Groundtruth is measured from a total station theodolite (TST) [45] with a 2 mm/2″ accuracy.

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

ISM-band Reader. We use an Impinj R700 [46] as the ISM-band reader, which is configured on "Radio Mode 142" (Miller-4 coding and BLF of 256 kHz) and a single linear-polarized antenna aligned with the wideband Tx. We empirically pick this mode since it balances throughput and range. Other coding methods and BLF can also be adopted with few modifications to our system.

7.2 Throughput in One-shot Localization

Fig. 12 shows RF-CHORD's throughput at different distance. RF-CHORD can read and localize ~180 tags per second (97% of the tags read by an Impinj reader) at up to 6 m. RF-CHORD is 1000× faster compared to previous sniffer-based wideband systems with frequency-hopping. For instance, RFind [14] needs 6.4 seconds to localize one tag. We also evaluate RF-CHORD's throughput across emission power. Fig. 13 shows that RF-CHORD's throughput decreases when we reduce its emission peak power from -15 dBm to -35 dBm. It works fine with an emission power above -25 dBm.

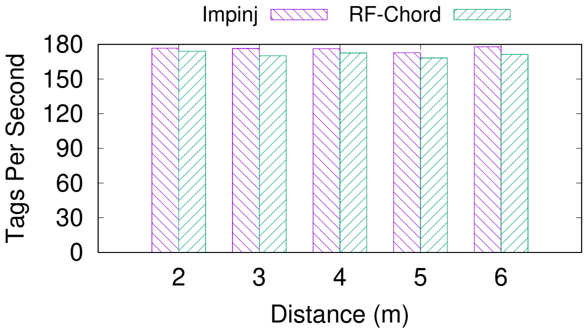


Figure 12: Throughput across distances. RF-CHORD can localize around 180 tags/s with -15 dBm emission power.

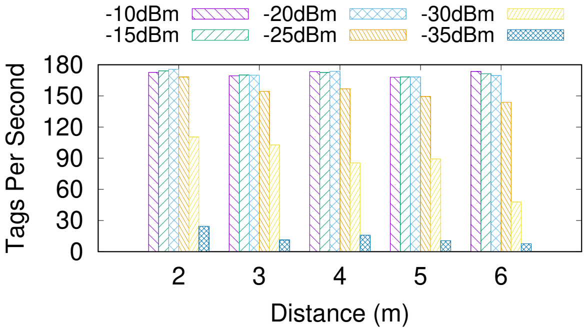


Figure 13: Throughput across distances with different emission power. The performance of RF-CHORD is stable with above -25 dBm emission power.

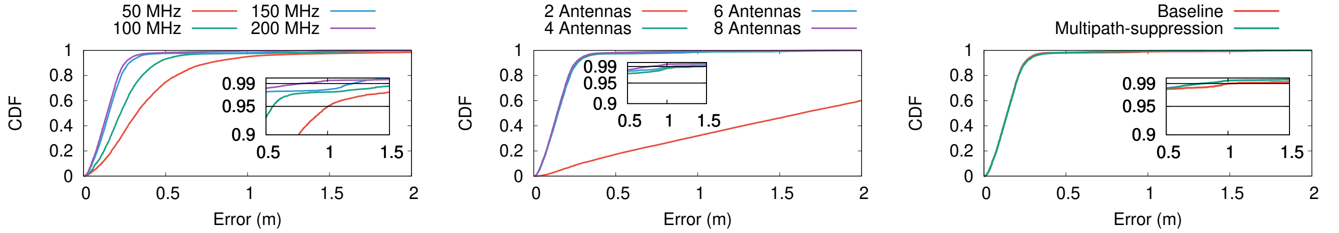
7.3 Localization Performance

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

Bandwidth. We evaluate the localization performance with 8 antennas and different bandwidths. Fig. 14a shows 99th localization errors are 2.398 m, 1.646 m, 1.203 m and 0.786 m with 50 MHz, 100 MHz, 150 MHz and 200 MHz bandwidths. The median errors are 0.325 m, 0.227 m, 0.155 m, and 0.144 m, separately. The results show increasing bandwidth, thus increasing the time resolution, can not only improve the median performance but also reduce the long-tail error. Even when the median performance is close to the upper limit (150 MHz v.s. 200 MHz), the long-tail errors can still be reduced by increasing bandwidth.

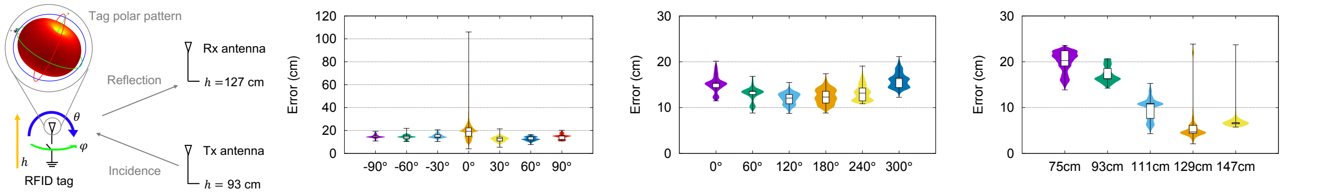
Number of Antennas. We evaluate RF-CHORD's localization performance with 200 MHz bandwidth and different numbers of antennas (thus different array apertures). Fig. 14b shows RF-CHORD's 99th localization errors are 4.513 m, 1.467 m, 1.081 m and 0.786 m when 2, 4, 6 and 8 antennas are used. The performance of the 4, 6, and 8 antennas is very similar on median errors (about 0.14 m). However, their long-tail errors are significantly different. The results

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



(a) Bandwidth. (b) Number of Antennas. (c) Algorithm.

Figure 14: RF-CHORD's localization errors with different bandwidths, antenna numbers, and algorithms.



(a) Orientation Setup. (b) Pitch/Roll Angle (θ). (c) Yaw Angle (ϕ). (d) Height (h).

Figure 15: Microbenchmarks with different tag orientations and heights related to the antennas.

show increasing the number of antennas (from 2 to 8) can always improve long-tail performance. Increasing the number of antennas/apertures strengthens the system's immunity to interference in specific directions and improves the angular resolution for localization.

Algorithms. We take basic hologram (Eqn. 1) as the baseline algorithm and evaluate our multipath-suppression algorithm with 8 antennas and 200 MHz bandwidth. Fig. 14c shows that 99th localization errors of baseline and RF-CHORD are 1.018 m and 0.786 m respectively. The median errors of baseline and RF-CHORD are 0.143 m and 0.144 m, respectively. The algorithm effort can improve long-tail performance by handling more corner cases, but hard to improve median performance. Physical resources (*i.e.,* the bandwidth and the antenna array aperture) fundamentally limit the algorithm's performance, and the long-tail improvement from the algorithm is primarily attributed to the introduction of prior information – it provides an appropriate carrier for making use of prior information.

Orientation. In practice, the orientation of tags will influence the link angle and polarization, thus introducing SINR and phase changes. We evaluate how orientation influences the localization error. We set the target tag at a 1-m fixed distance to the antenna array to eliminate the influence of the multipath effect. Then, we change the pitch angle θ (as same as the roll angle due to the symmetry), yaw angle ϕ, and height of the tags as shown in Fig. 15a for orientation microbenchmark:

- *Pitch/Roll Angle.* In Fig. 15b, we keep $\phi = 0°$ and $h = 111$ cm (at the center between Tx and Rx). The worst performance occurs when the pole of the antenna points to the rx, which rarely happens in practical deployments (to be discussed in §8.1). It is difficult to read tags due to the low SINR, and even if successful, the long-tail error will be more than 1 m.

- *Yaw Angle.* In Fig. 15c, we keep $\theta = 0°$, $h = 111$ cm and change ϕ from 0° to 300°. The errors at different yaw angles are similar because the directional gain across ϕ is symmetrical. The results show that the yaw angle does not affect long-tail localization error (bounded within 30 cm).

- *Height.* In Fig. 15d, we keep $\theta = 0°, \phi = 0°$ and move the tag from 75 cm to 147 cm. The long-tail errors do not change much across different heights, which shows that height is not the key factor affecting long-tail errors.

8 Practical Deployment

8.1 Deployment Constraints

We summarize the practical factors that influence SINR in Fig. 16 and introduce the constraints in real-world logistic scenarios. We also explain how we avoid or utilize them for high-reliability localization.

Orientation. The localization error may be significant if the pitch angle of the tag is closed to 90° according to §7.3. In the deployment shown as Fig. 17, the orientation of tags may not be uniform but unlikely to be completely disordered. All the tags are attached to the sides of boxes or crates and then stacked on the pallet. The chaos of stacking and the movement of the pallet may cause yaw angle (ϕ) change but not cause much pitch/roll angle (θ) change, which only introduces negligible localization errors according to Fig. 15c.

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

NLOS and Tag Coupling. We also stipulate that all the tags should be in the line of sight from one side dock door, which means stacking at most two-column crates on the pallet. It is because the performance of UHF RFID will decrease rapidly with nearby water [47]. This rule excludes severe NLOS occlusion/reflection and severe tag coupling. Most of the pallets

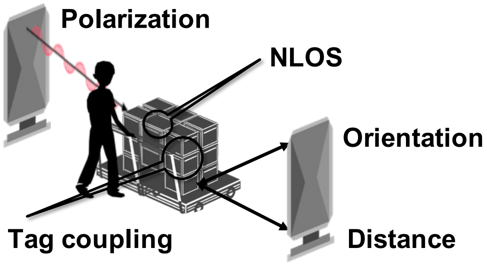


Figure 16: The Factors Affecting Signal Quality.

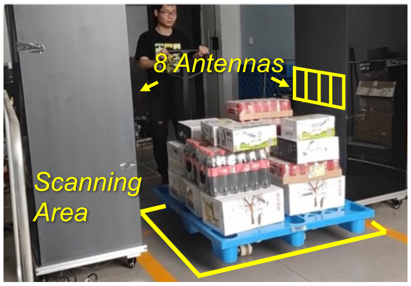


Figure 17: Warehouse Dock Door.

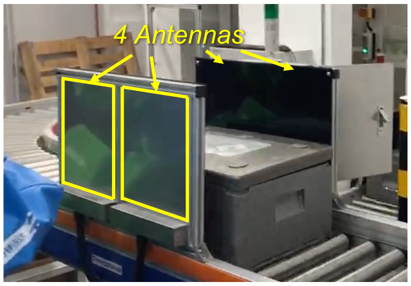


Figure 18: Food Delivery Store.

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

Table 3: Reliability performance in practical deployments.

in our scenes naturally meet this requirement, and in rare cases, we need to waste some space.

8.2 Real World Deployment

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

Warehouse Deployment. We deploy RF-CHORD in a warehouse to understand its performance in logistic check in and out. RF-CHORD is installed in the dock door of the warehouse as shown in Fig. 17. This warehouse's goal is to distribute a large amount of food and daily necessities supplied by the upstream warehouse to city delivery stations. The crates are various and packaged without unified standards. Ideally, RF-CHORD should report all the tags inside of the scanning area and not report any tags outside of the scanning area. Our previous deployment experiments in the same scenario show that commercial read-or-not solution Impinj xSpan [16] has ~6% miss-reading rate and ~2% cross-reading rate in the similar scene. We attached over 10,000 tags to various items, mainly plastic crates, also including water bottles, cans, milk boxes, rice, *etc.* The scanning area is 2 × 1 m between the two poles of the dock door (as ROI) and the user walks through the aisle with about 50~100 tags on a trailer in 1 to 4 seconds. According to Tab. 3, RF-CHORD is able to identify tags inside of scanning area with a 100% accuracy (perfectly no miss reading) and 0.0025% cross reading. Therefore, RF-CHORD can provide sufficient localization accuracy in the warehouse deployment, which significantly outperforms the state-of-the-art commercial solutions.

Fresh Food Deliver Store Deployment. As shown in Fig. 18, we also deploy lightweight RF-CHORD in a fresh food delivery store where fresh food is packaged into a container and transported via a moving belt. Once the RFID tag on the container is scanned, the delivery personnel will be allocated to pick it up. RF-CHORD needs to ensure all the containers on the moving belt are scanned and do not scan any tag outside of the moving belt. Tab. 3 shows that the miss-reading rate of RF-CHORD is 0%, and cross-reading rate is 0.0154%. Therefore, RF-CHORD can achieve sufficient accuracy in the fresh food delivery store deployment.

9 Discussion

Polarization Mismatch. In our scenarios, the work pipeline guarantees the polarization match. However, in more general scenarios, the polarization may be mismatched when the orientation of tags is disordered. The conventional solution is to use circular polarization antenna [48] or dual-polarization switching [16]. RF-CHORD can be adapted to them convenientIy because its wideband four point antenna is inherently dual-polarized. We can plug a polarization switch into each sniffer antenna, which acts synchronously and does not influence throughput and range performance.

Blind Spots. RF-CHORD is free of cross reading, and therefore it can use high transmission power and sensitivity ISM-band reader for achieving nearly zero miss-reading rate. However, miss reading still threatens reliability in certain complex environments. It can be mitigated by switching between antennas or beam patterns [3, 49]. As our Tx is synthesizing multiple tones, it is feasible to add a Tx beamforming array for blind spot suppression.

Integration with Robots. In recent years, logistics robots (*e.g.,* automated guided vehicle (AGV) [50], automated storage and retrieval systems (ASRS) [51], and autonomous mobile robots (AMR) [52]) have been developed rapidly to reduce the movements and operations of sorters and improve efficiency. These robots still need to cooperate with a label identification system (*e.g.,* barcode or QR code). RF-Chord has the potential to replace such system and cooperate with logistics robots to achieve more efficient automation.

Cost. The ultimate goal of deploying RFID is to reduce manual labor and error while improving efficiency, which requires careful cost accounting. We emphasize that although baseband chips and RF circuits will increase the cost of readers to thousands of dollars, the main cost of RFID-based logistics still comes from RFID tags. Considering a medium warehouse with 10k packages delivered every day, the annual cost of tags is approximately \$0.1 × 10,000 × 365 = \$365,000. Our strategy is not modifying the tag chip because most of the manufacturing cost comes from the chip and the assembly process [53]. Therefore, the wideband tag we designed maintains almost the exact cost as current commercial tags when in massive manufacturing.

10 Related Work

Narrowband Localization. There are three main localization approaches to boost accuracy even with the limited time resolution of narrow ISM bandwidth: The first approach is to improve spatial resolution by SAR. Tagoram [7] uses the motion of tags to build multiple virtual antennas, while Mobitagbot [8] exploits antenna motion. The hologram algorithms in these two systems inspired the kernel-layer framework in our paper. Other hologram algorithm variants [29, 30, 54] can also be viewed as different combinations of kernels and layers. However, the assumption of free antennas or tags mobility and lengthy startup time for tracking do not fit the logistic network. The second approach is to acquire prior information by reference tag. PinIt [6] exploits a dense grid of reference tags and determines the nearest reference tag for NLOS localization by dynamic time wrapping. However, reference tags share time slots, which influences the throughput and scalability. The third approach is to increase the number of links by tag array. Attaching more tags to the target can increase the number of links and improve localization performance. Tagyro [55], and RF-Dial [56] utilize the phase difference of the tag array to solve orientation ambiguity and improve localization performance. Trio [57] models the equivalent circuits of coupled tag and uses the tag interference for refined localization. Liu et al. [58] uses spatial-temporal phase profiling for relative RFID localization. These tag array based localization approaches are accurate but may be error-prone in a complex environment. Unlike these proposals, RF-CHORD is a sniffer-based wideband localization system that improves time resolution for fundamental performance enhancement.

Wideband Localization. Wideband RFID localization has been proposed to overcome the time resolution limitation. RFind [14] uses a low-power sniffer antenna by frequency hopping to collect the narrow sample channel state information across 220 MHz. Turbotrack [15] develops an OFDM-based one-shot wideband channel estimation approach and a Bayesian space-time super-resolution algorithm to achieve fine-grained localization. However, these systems need multiple shots in the channel estimation or the algorithm to converge for fine location estimation, thus very slow startup for localization or tracking. Modifying tags to work on other frequencies (*e.g.,* Wi-Fi [59], millimeter-wave [11], UWB [12, 13]) or cross-frequency based approaches (*e.g.,* communicate with Wi-Fi [10], communicate at 1.4~2.4 GHz [60]) are also expected as the solutions for both finer localization and higher throughput, but their tags are not ready for massive manufacturing at low cost due to the complicated RF frontend and control circuits. Inspired by these works, RF-CHORD develops a multisine waveform to realize one-shot localization without modifying the commercial tag chips, resulting in high accuracy with no throughput loss or cost increase.

RFID Reader. Commercial RFID readers [46, 61, 62] have heavily optimized RF analog frontend, decoder, and protocol stack but do not support real-time tag critical information (*i.e.,* EPC ID, timestamp) retrieval. There are a series of open-source RFID reader systems. Buettner et al. implemented EPC Gen II downlink stack [63] and the full functional reader [64], respectively. Kimionis et al. implemented a GNU radio-based reader, which supported OOK and noncoherent FSK [65]. However, their energy and edge detection algorithms are too simple to decode applicable code (*e.g.,* miller-4 coding). A recent reader designed by Kragas et al. [66] is featured by coherent detection and initial duration deviation search but only supports simple FM0 encoding. There are other research projects featured by multisine waveform [67], parallel sensing support [68], and active transmit leakage cancellation [69]. However, they only focus on specific optimization and do not provide source code. In a nutshell, no out-of-box reader design meets our requirements of high throughput and low decoding threshold, so we develop a wideband reader with a customized RF frontend and decoder while reusing the MAC layer of the commercial reader for slot arrangement and collision handling. It supports our wideband localization with high efficiency, sensitivity, and compatibility.

11 Conclusion

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

Acknowledgments

We are grateful to the reviewers for their constructive critique, and our shepherd, Vikram Iyer in particular, for his valuable comments, all of which have helped us greatly improve this paper. We also thank Xieyang Xu and Weicheng Wang for providing an early implementation version of the work. We are grateful to Yunfei Ma for the thoughtful suggestions based on the early version of the work. This work is supported in part by National Key Research and Development Plan, China (Grant No. 2020YFB1710900), National Natural Science Foundation of China (Grant No. 62022005, 62272010, and 62061146001) and Alibaba Innovative Research. Chenren Xu and Shunmin Zhu are the corresponding authors.

References

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

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

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

[4] Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu, and Ming Zhang. Nfc+ breaking nfc networking limits through resonance engineering. In *ACM SIGCOMM*, 2020.

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

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

[7] 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 *ACM MobiCom*, 2014.

[8] Longfei Shangguan and Kyle Jamieson. The design and implementation of a mobile rfid tag sorting robot. In *ACM MobiSys*, 2016.

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

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

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

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

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

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

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

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

[17] Jue Wang, Deepak Vasisht, and Dina Katabi. Rf-idraw: virtual touch screen in the air using rf signals. In *ACM SIGCOMM*, 2014.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[35] 902-928 Cavity Band Rejection Filter WT-A3678-R10. https://www.wtmicrowave.com/en/product/WT-A3678-R10.html.

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

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

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

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

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

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

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

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

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

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

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

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

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

[49] Jingxian Wang, Junbo Zhang, Rajarshi Saha, Haojian Jin, and Swarun Kumar. Pushing the range limits of commercial passive rfids. In *USENIX NSDI*, 2019.

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

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

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

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

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

[55] Teng Wei and Xinyu Zhang. Gyro in the air: tracking 3d orientation of batteryless internet-of-things. In *ACM MobiCom*, 2016.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[71] 15.231 - periodic operation in the band 40.66-40.70 mhz and above 70 mhz. https://www.law.cornell.edu/cfr/text/47/15.231.

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

A FCC Compliance

RF-CHORD adopts a 200 MHz bandwidth in the UHF band, much wider than the 902~928 MHz ISM band. We need to reduce the power of the signal emitted in the licensed band to follow the FCC regulation [70]. Similar operations exist in other systems, such as RFind [14]. RFind adopts a duty-cycled single-tone signal with a peak power of -3 dBm and average power of -13.3 dBm. However, due to the throughput requirement of the localization, RF-CHORD's sniffer should always be ready to localize a tag, which means duty cycling is unacceptable. Therefore, RF-CHORD adopts a hard limit of -15 dBm per tone and can be even lower with similar performance. One may concern that the multiple carrier operation will not be the same as RFind [14] since the total bandwidth is larger than the 0.25% bandwidth limitation in FCC 15.231 (c) [71]. However, RF-CHORD can adopt the alternative method mentioned in [72], which calculates the total bandwidth by summing the individual occupied bandwidths of each carrier frequency. Since we did not apply any modulation to the carriers, the sum of respective bandwidths will be extremely small, which can comply with the FCC regulation. Other modulated waveforms (*e.g.,* OFDM) cannot follow this alternative method and may potentially violate the regulation.

B Kernel-layer Combinations for Different Localization Algorithms

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

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

$$\begin{aligned} &\text{Kernel: } e^{-\boldsymbol{j}(\phi_l-\theta_l)} = e^{-\boldsymbol{j}(\phi_l-2\pi f_l d/c)} = e^{-\boldsymbol{j}\phi_l} e^{2\pi f_l \tau} \\ &\text{Layer: } \sum_{l=0}^{n} S(\tau) = \sum_{l=0}^{n} e^{-\boldsymbol{j}\phi_l} e^{2\pi f_l \tau} \end{aligned} \tag{5}$$

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

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

$$\begin{aligned} &\text{Kernel: } e^{-\boldsymbol{j}(\phi_k-\theta_k)} = e^{-\boldsymbol{j}(\phi_k-2\pi f k\Delta d sin(\psi)/c)} \\ &\text{Layer: } \sum_{k=1}^{m} S(\psi) = \sum_{k=0}^{m} e^{-\boldsymbol{j}\phi_k} e^{2\pi f k\Delta d sin(\psi)/c} \end{aligned} \tag{6}$$

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

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

C Direct Path Enhancement

We enhance the direct path and suppress the influence from multipath with a frequency domain algorithm [14]. Assume there are N paths with distances of $d_0, d_1, d_2, \ldots, d_N$, and d_0 is the direct path. The channel h_l of lth carrier can be expressed as:

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

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

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

If we have a rough estimation of d_0, called $\tilde{d_0}$, we can use this algorithm to enhance the part of $a_0 e^{-j\frac{2\pi}{c} f_l d_0}$ (direct path) and suppress the part of $\sum_{i=1}^{N} a_i e^{-j\frac{2\pi}{c} f_l d_i}$ (multipaths) for a better location estimation. In more detail, we use the prior knowledge of ROI to help determine the rough estimation of direct path $\tilde{d_0}$ with Alg. 1. Then we enhance the direct path profile and suppress profiles of other paths by Eqn. 3 because the enhanced phase $\tilde{\phi_l}$ can be written as:

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

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

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

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

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

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