Enabling Multi-Frequency and Wider-band RFID Sensing using COTS Device

Zhao, Cui; Li, Zhenjiang; Ding, Han; Wang, Ge; Xi, Wei; Zhao, Jizhong

Published in:
IEEE/ACM Transactions on Networking

Online published: 06/05/2024

Document Version:
Post-print, also known as Accepted Author Manuscript, Peer-reviewed or Author Final version

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.1109/tnet.2024.3394974

Publication details:
https://doi.org/10.1109/tnet.2024.3394974

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.

https://doi.org/10.1109/tnet.2024.3394974
Abstract—RFID shows great potentials to build useful sensing applications. However, current RFID sensing can obtain mainly a single-dimensional sensing measurement from each reader-to-tag query, such as phase, RSS, etc. This is sufficient to fulfill the designs that are bound to the tag’s movement, e.g., the localization of tags. However, it imposes inevitable uncertainty on many sensing tasks relying on the features extracted from the RFID signals. These traditional sensing measurements limit the fidelity of RFID sensing fundamentally and prevent its broader usage in more sophisticated sensing scenarios. This paper presents RF-Wise to push the limit of RFID-based sensing, motivated by an insightful observation to customize RFID signals. RF-Wise can enrich the existing single-dimensional feature measure to a channel state information (CSI)-like measure with up to 150-dimensional samples across different frequencies concurrently. More importantly, RF-Wise is a software solution atop the standard EPC Gen2 protocol without using any extra hardware. It requires only one tag for sensing and works within the ISM band. RF-Wise, so far as we know, is the first system of such a kind. Extensive experiments show that RF-Wise does not impact underlying RFID communications, while by using the features extracted by RF-Wise, applications’ sensing performance can be improved remarkably. The source codes of RF-Wise are available at https://cui-zhao.github.io/RF-WISE/.

Index Terms—Internet of things, RFID, wireless sensing.

I. INTRODUCTION

We have recently witnessed a surge of research that leverages the wireless signals for sensing [1]–[3], among which RFID (Radio Frequency Identification) is an important and widely adopted such technique. RFID employs passive tags as the sensors usually [4]. These tags are battery-free, small-in-size, and low-cost, which are suitable to achieve long-term and large-scale deployment for plenty of useful applications in practice. For instance, food safety [5], the contactless human-computer interaction (HCI) [6], the smart manufacturing [7], etc.

Motivation. RFID reader queries tags following an Aloha-based MAC from the EPC Gen2 protocol [8]. The reading rate (the frequency to collect the sensing samples) is moderate merely, e.g., 40~200 times per sec. Hence, the sensing quality from each query becomes more crucial. However, the current RFID sensing can obtain mainly a single-dimensional sensing measurement from each query, such as phase, RSS, etc. This is sufficient for the designs bounded to the tag’s movement, e.g., the localization of tags [9], vibration counting [10], etc. Nevertheless, it imposes inevitable uncertainties on a large spectrum of sensing tasks relying on the detailed features extracted from the RFID signals: 1) Recognizing the diluted alcohols or fake/expired food materials with subtle differences to ensure food safety [1]. 2) Capturing fast or subtle gestures for contactless human-computer interactions [11]. 3) Sensing dense goods in manufacturing, etc. Thus, traditional single-dimensional sensing measurement limits the fidelity of RFID sensing fundamentally, and prevents its broader usage in more sophisticated and realistic sensing scenarios.

To overcome these limitations, great efforts have been made to increase the sensing sample’s diversity by using frequency hopping [12] or tag array [13], which however are not effective due to the inherently large latency between two sample collections (Section VI). Some recent work [1] proposes to utilize an extra device to transmit additional wide-band (500 MHz) signals to improve the sensing fidelity. The cost (from the extra transmission device) and overhead (to synchronize this extra signal with the RFID signal) cannot be neglected. In essence, previous multi-frequency and wideband RFID sensing suffer from three limitations, including i) large time latency, ii) higher cost and overhead, and iii) signal interference (discussed in Section VI). We thus wonder naturally whether we can improve RFID sensing without such extra costs and overhead?

Observation. The system proposed in this paper, RF-Wise, brings a positive answer. It can enrich the single-dimensional sensing measurement to a fine-grained channel state information (CSI)-like measure, composed of a series of independent sensing samples obtained across frequencies. RF-Wise can further enhance this sensing fidelity by harnessing more usable bandwidth in RFID. More importantly, RF-Wise is a purely software solution atop the standard RFID system without using any extra hardware. It requires only one tag for sensing, works within the ISM band, is compatible with the EPC Gen2 protocol, and is a generic design to be integrated into many existing applications to improve their performance directly. RF-Wise is designed based on the following observation.

The RFID signal contains a continuous wave to power tag’s backscattering, which is configured with a constant amplitude value usually. In this paper, we observe that the
tag’s backscattering is not sensitive to the waveform format of the continuous wave — even it is designed to be another type of sequence with enough energy, tags may still be activated and functioned normally. This observation inspires us to “customize” the continuous wave by employing frequency multiplexing so that we can collect multiple sensing samples over frequencies concurrently from each query (no frequency hopping). For example, the sensing dimension can be increased from 1 to 16 to fully cover the typical 2 MHz band with a frequency spacing of 125 KHz. Moreover, improved by using more allowable or usable bandwidth in RFID, e.g., 26 MHz in the U.S., the sensing dimension can be increased up to 150 further, which thus fundamentally breaks the limit in the current RFID sensing.

However, to realize this idea in a real system, we need to address the following three challenges.

1) Protocol-compatible frequency multiplexing. Frequency multiplexing is a mature wireless technique, e.g., in Wi-Fi [14]. But, to enable it for RFID, we need to ensure the RFID signal still adheres to the EPC Gen2 protocol after our customization, such that RF-Wise is compatible with the commercial-off-the-shelf (COTS) tags and does not impair the inherent RFID communications.

2) Hardware imperfection and constraints. In order to take full advantage of frequency multiplexing, we observe a severe and unique cascaded integrator-comb (CIC) roll-off issue [15] as well as other hardware constraints. They can be avoided with the bandwidth commonly adopted in RFID communications, while they appear when more bandwidths are expected to use for sensing. We should address them explicitly.

3) Feature extraction. Finally, we need to figure out how to extract more representative and reliable features from the sensing samples obtained from our design, so that RF-Wise can benefit a variety of sensing applications directly.

Contributions. In this paper, we propose effective techniques to address the above challenges. To validate the efficacy of RF-Wise, we develop a prototype using one USRP X310 software radio with a daughter-board merely, and test it with the COTS passive tags. The underlying communication still follows the EPC Gen2 protocol without impacting its communication efficiency, while the dimension of the sensing samples from each query can be improved up to 150. With such an enhanced sensing ability, we investigate its utility through liquid classification and gesture recognition two concrete applications, and observe the performance gain from 20.2% to 40.7% by replacing the sensing features derived from RF-Wise.

Meanwhile, we have also made great engineering efforts to upgrade the public EPC Gen2 source code [16] to support RF-Wise with several promising new features: i) I/Q modulation for the continuous wave, ii) code optimization to avoid “core dumped error”, and iii) parameter configuration to enable a wider-band RFID transmission of up to 25 MHz bandwidth. So far as we know, no such codes are publicly available yet and we release our codes in [17] to facilitate future studies.

In summary, this paper has made the following contributions:

- To our best knowledge, RF-Wise is the first work to obtain fine-grained CSI-like sensing samples purely from RFID signals to advance RFID sensing. It is a software solution atop standard RFID without using any extra device, compatible with EPC Gen2 within the ISM band, requires one tag for sensing, and is generic for various applications.
- We identify a series of unique challenges encountered in designing RF-Wise. We propose some novel and effective techniques to address these challenging issues.
- We make great engineering efforts for system development. We examine RF-Wise’s efficacy by two applications. Results also suggest that RF-Wise does not impact the efficiency of the underlying RFID communications.

Organization. The rest of this paper is organized as follows. We introduce the preliminaries in Section II and the system design in Section III. The implementation and evaluation are presented in Section IV and V, respectively. We review related works in Section VI before we discuss and conclude in Section VII and VIII.

II. PRELIMINARIES

A. Application Scenarios

In this section, we first discuss the application scenarios that RF-Wise can benefit, including at least:

1) Food safety. Sensing foods or materials in a non-invasive way is a promising and important topic to ensure the food safety. For instance, the diluted alcohols mixed by the cheap methanol could lead to blindness or even death of people [18]. Fake materials (e.g., oil, medicine, etc.) could cause allergy or other diseases [19]. Expired drinks may also cause health issues. To sense foods using RFID, the features are generated by the coupling effect between the food and the tag [20], which can be reflected at different frequencies. RF-Wise can extract such fine-grained features to enable a reliable sensing.

2) Contactless HCI. Contactless human-computer interactions (HCI) become increasingly desired nowadays to reduce the risk of influenza infection. For instance, in public lavatories, users can use their hand gestures in the air to operate the automatic toilet system to avoid a physical touch. At gate entrances, the user’s gesture or speaking features can be used for authentication [21], without removing face masks or typing on the input panel. For these applications, the features from the dynamic gestures can be captured more precisely through the sensing measures of RF-Wise cross different frequencies.

3) Smart manufacturing. RFID sensing can also be applied to achieve the smart manufacturing and industry management. For example, deciding whether the fragile goods are placed slantingly, recognizing worker’ gestures in the air to operate the devices deployed in remote, hash or even dangerous areas, etc.

B. RFID Communication Primer

Before elaborating on the system design, we introduce an RFID communication primer. RFID reader queries tags in an inventory follow the EPC Gen2 protocol, shown in Fig. 1.

\footnote{We utilize the term “waveform format” metaphorically to illustrate the visual representation of a tag’s baseband reply signals.}
1) Reader starts with a “Query” command and waits for the “RN16” reply backscattered by the tag. During this waiting interval, reader transmits an unmodulated radio frequency (RF) carrier, which is the continuous wave, to power the tag’s backscattering for the “RN16” reply.

2) After “RN16” is received, reader sends an “ACK” command and continues to transmit continuous wave for tag to backscatter its “EPC”.

In the rest of this paper, we make the following two notes to facilitate the discussions:

- **Query**: For the representation ease, the term “query” in the rest paper refers to the whole inventory, instead of the “Query” command (Fig. 1) unless specified otherwise.
- **Continuous wave**: For each query, prior sensing samples (e.g., phase, RSS, etc.) are extracted from the “EPC” field in the received signal. We also adopt this field. Hence, our proposed signal operations in next section is only applied to the continuous wave covering the “EPC” field.

III. RF-Wise Design

RF-Wise contains three main components shown in Fig. 2:

1) **Frequency spreading** (Section III-A): multiplexing frequencies by customizing continuous waves to obtain multi-dimensional sensing samples from different frequencies concurrently.

2) **Harnessing wider-band** (Section III-B): harnessing more allowable bandwidth to enrich the sensing samples further, and enhance the timing resolution of sensing as well, after a set of hardware related issues are addressed.

3) **Feature extraction** (Section III-C): extracting representative and effective features from the sensing samples obtained by RF-Wise, to be used by various applications.

Next, we elaborate on the design details of each component in RF-Wise.

A. Multi-carrier Frequency Spreading

In each query, continuous wave (denoted as $s$) is modulated to the carrier wave to provide sufficient energy to activate tag’s backscattering, and $s$ is set with a constant amplitude.

1) **Opportunity**: Through our study, we find tag’s backscattering is not sensitive to the waveform format of $s$. Even $s$ is designed as other type of sequences, when it is strong enough, tags may still be activated and functioned normally. We illustrate this observation in Fig. 3 (test-bed setup is detailed in Section V), in which $s$ is designed as a repeated random sequence. For a clear observation, we customize (or modify) $s$ for the left part only and leave the right part as the standard constant $s$. Fig. 3 shows that reader can still receive the tag’s EPC reply. Compared with the EPC received with the standard $s$, the left-part EPC reply contains some jags, while the EPC bits from both parts can be decoded correctly by the reader.

This observation offers a chance to “customize” $s$ to enrich the sensing dimensions for each query dramatically — We propose to multiplex the frequency of $s$ to build orthogonal subcarriers in parallel, so that independent and multi-dimensional samples can be obtained from these sub-carriers concurrently in each query. For example, with a sub-carrier spacing of 125 KHz and a typical 2 MHz bandwidth, we can obtain 16 (= $\frac{2 \text{MHz}}{125 \text{KHz}}$) samples from each query to cover this 2 MHz band, which is similar as the channel state information (CSI) measure in Wi-Fi [22]. This signal customization is purely software based without using any extra hardware. To build subcarriers for RFID, we adopt the orthogonal frequency-division multiplexing (OFDM) under the RFID-incurred constraints.

2) **Continuous wave meets OFDM**: We first introduce our OFDM symbol generator as shown in Fig. 4, followed by two issues that need to be addressed in the context of RFID.

A dummy binary sequence is generated and mapped on a constellation diagram to produce OFDM symbols using PSK (phase-shift keying) of degree $n$, i.e., the constellation diagram contains $n$ points in total and every $\log_2(n)$ dummy bits are mapped to one constellation point. Fig. 4 shows the case when $n = 4$. Each constellation point $i$ is a complex number $c_i$ in the frequency domain and a series of $\{c_i\}$ are generated from the dummy sequence.

The complex numbers $\{c_i\}$ then go through three routine modules — Serial-to-Parallel (S/P), Inverse Fast Fourier Transform (IFFT) and Parallel-to-Serial (P/S). For IFFT, every $N$ complex numbers $c_i$s are grouped to perform IFFT, where $N$ is the IFFT length and it also equals to the number of subcarriers to occupy different frequencies. Finally, after the “P/S” module, each group of $N$ complex numbers $c_i$s produce one
piece of the signal in the time domain, which is one OFDM symbol \( O_i \). All the OFDM symbols together form the new continuous wave \( s' \).

![Constellation Diagram](Image)

**Problem.** Above OFDM generation is inspired by the frequency multiplexing in Wi-Fi, whereas to apply it for RFID, we need to ensure that the customized \( s' \) is still compatible with the standard RFID EPC Gen2 protocol and hardware.

1) **OFDM symbol length.** RFID tag backscatters a reader’s query using the “ON/OFF” keying (OOK) modulation. During the switch of these two opposite states (Fig. 5), a significant signal fluctuation may overwhelm the sensing features of the targets. This problem could potentially undermine the effectiveness of feature learning by subsequent classifiers, as machine learning or neural networks tend to prioritize extracting more distinct representations. So, within each “ON/OFF” state, at least one complete OFDM symbol should not cross the switching edge of two states. It can be ensured by setting the sub-carrier number \( N \) (Fig. 4) to obtain a proper symbol length.

![Complete OFDM symbols: O(1, 2, 3, 4, 6, 7, 9, ...)](Image)

**Problem.** Above OFDM generation is inspired by the frequency multiplexing in Wi-Fi, whereas to apply it for RFID, we need to ensure that the customized \( s' \) is still compatible with the standard RFID EPC Gen2 protocol and hardware.

1) **OFDM symbol length.** RFID tag backscatters a reader’s query using the “ON/OFF” keying (OOK) modulation. During the switch of these two opposite states (Fig. 5), a significant signal fluctuation may overwhelm the sensing features of the targets. This problem could potentially undermine the effectiveness of feature learning by subsequent classifiers, as machine learning or neural networks tend to prioritize extracting more distinct representations. So, within each “ON/OFF” state, at least one complete OFDM symbol should not cross the switching edge of two states. It can be ensured by setting the sub-carrier number \( N \) (Fig. 4) to obtain a proper symbol length.

![Complete OFDM symbols: O(1, 2, 3, 4, 6, 7, 9, ...)](Image)

For RFID, the number of the signal samples (denoted as \( M \)) in one “ON/OFF” state is determined by both the bandwidth \( B \) and the backscatter link frequency (\( f_{BLF} \)) [23]:

\[
M = B / (\mu \times f_{BLF}) = B \times P_{TRreal} / (\mu \times P_{DR}),
\]

where \( \mu = 1 \) or 2 according to from which bit the OFDM symbols are extracted, because bit “1/0” is formed with two equal-length “ON-or-OFF”/“ON-and-OFF” states under the FM0 coding. For Miller coding, \( \mu \) should equal 2× or 4× of the coding level for bit “1/0”, e.g., \( \mu = 4 \) if an OFDM symbol is extracted from bit “1” towards 2-Miller coding. Discussion about \( \mu \) is detailed in Section III-C. Among Eq. (1), \( f_{BLF} = P_{DR} / P_{TRreal} \), and \( P_{DR} \) (Divide Ratio) and \( P_{TRreal} \) (Tag-to-Interrogator calibration symbol) are two RFID system parameters.\(^2\) To ensure that at least one complete OFDM symbol is in each ON or OFF state, the OFDM symbol length should be no greater than half of the ON/OFF duration. Moreover, at the start and end of a state, there are usually two intermediate behaviors (the process of gradually stabilizing a state) that are also harmful to sensing. To avoid these intermediate behaviors (according to our experiments, each of them covers about 6% of a state), we further set a 15% residual to ensure a more reliable implementation as follows:

\[
N \leq \frac{M}{2} \times 85% = \frac{B \times P_{TRreal} \times 85%}{2 \times \mu \times P_{DR}} = \tilde{N}. \quad (2)
\]

For RFID sensing, a larger \( N \) is desired, such that more sensing samples can be collected from more different sub-carriers. However, Eq. (2) indicates that the increase of \( N \) cannot exceed an upper-bound \( \tilde{N} \) due to “OOK” modulation; Otherwise, the quality of the OFDM symbol cannot be guaranteed. The specific value of \( \tilde{N} \) depends on \( B, P_{TRreal} \) and \( P_{DR} \), whose setting will be discussed in Section III-B.

2) **Coexisted sensing and communication.** The new continuous wave \( s' \) obtained so far complies to RFID’s modulation. However, we find that the average energy of this new \( s' \) itself is small, which cannot activate tags and the sensing cannot be conducted. To overcome this issue, if we scale \( s' \) with a large factor \( \alpha \) directly, its energy could be sufficient, while we observe that this scaled continuous wave \( \alpha \times s' \) will be too noisy and sacrifices the underlying RFID communication, so that RFID reader cannot decode the tag’s replied EPC data.

Therefore, in RF-Wise, we propose to load the generated \( s' \) on top of the standard constant continuous wave \( s \), instead of replacing it. In such a composed \( \tilde{s} (= \alpha \times s' + s) \), \( s \) provides sufficient energy to power the tag’s backscattering, and \( s' \) (with a strength factor \( \alpha \)) is employed for sensing. Meanwhile, we need to ensure the orthogonality of all the sub-carriers so that the sensing can be performed correctly atop such a new \( \tilde{s} \).

To demonstrate the orthogonality of these sub-carriers, we formulate the demodulation process of a certain sub-carrier \( j \), e.g., \( \int \tilde{s} \times \cos(j\omega t) \, dt \) as:

\[
\int (\alpha \times \sum_{i=1}^{N} c_i \cos(i\omega t) + s) \times \cos(j\omega t) \, dt = \alpha \times c_j \int \cos^2(j\omega t) \, dt, \quad (3)
\]

where \( c_i \) denotes the data carried by the \( i \)-th subcarrier \( \cos(i\omega t) \) and \( N \) is the number of sub-carriers. Because it is known that \( \cos(n\omega t) \), \( \cos(2n\omega t) \), ..., \( \cos(n\omega t) \) (n is an integer) are orthogonal, and \( s \times \int \cos(j\omega t) \, dt = 0 \). So only the component of sub-carrier \( j \) is preserved, i.e., \( \alpha \times c_j \int \cos^2(j\omega t) \, dt \neq 0 \), and Eq. (3) indicates the orthogonality among all the sub-carriers. The coexistence of sensing and communication can be thus ensured.

3) **Sensing sample extraction:** With the injected OFDM symbols, we are able to measure the channel frequency response (CFR, denoted as \( H_i \)) from each complete OFDM

\(^2\)Tag measures the duration of \( P_{TRreal} \), which is contained in the preamble of the reader’s query. Meanwhile, \( P_{DR} \) is set to either 8 or 64/3 merely in RFID, which is indicated by one bit in the query command as well. Tag then knows \( f_{BLF} = P_{DR} / P_{TRreal} \) for backscattering.
symbol $\hat{O}_i$ in the received (EPC) signal by $\hat{O}_i = H_i \cdot O_i + e$, where $O_i$ is this OFDM symbol before transmission and $e$ is a noise. We can estimate $H_i$ by mean square error minimization [24]. Each $H_i$ is a $N$-dimensional vector essentially, $H_i = \{h_i(j)\}^N_{j=1}$, where each $h_i(j)$ corresponds to one sub-carrier $j$ and $N$ is the total number of sub-carriers. We note that each $H_i$ measured from an OFDM symbol is similar as each CSI measured from a packet in Wi-Fi. Hence, the raw sensing samples $H$ outputted by RF-Wise from each query are the following set:
\[
H = \{H_i\}^S_{i=1},
\]
where $S$ is the number of complete OFDM symbols $O_i$s extracted from this query. Eq. (4) suggests that:

- RF-Wise expands the sampling sample’s dimensions across frequencies (each $H_i$ is $N$-dimensional), this is where the sensing performance gain comes from.
- It can also do such fine-grained sensing multiple times in each query (e.g., $H_{1,\ldots,S}$) to make sensing more reliable.

Later, we propose two types of features derived from $H$ (Section III-C), which are tailored for different sensing scenarios and can be adopted by different applications directly.

To showcase the benefits of multi-frequency sensing, we make a visualized comparison between traditional RFID and RF-Wise (CSI-like features) towards the same sensing targets. As depicted in Fig. 6 (a), the phase (in radian) information, which is a common sensing feature for RFIDs, only offers a one-dimensional sensing pattern. However, RF-Wise encompasses multiple subcarriers across different frequencies, as illustrated in Fig. 6 (b), thereby possessing the greater potential to distinguish subtle variations in the target (detailed in Section V-A).

![Fig. 6. Illustration of (a) traditional RFID’s sensing features (phases) and (b) RF-Wise’s CSI-like features towards the same targets.](image)

4) Practical Considerations in RF-Wise: To develop RF-Wise as a practical system, we further consider following three aspects related to sensing and communications in our design:

1) DC sub-carrier: Direct current (DC) sub-carrier (covering the central frequency of the signal) is not adopted for sensing, because it suffers from the interference from the local oscillator leak [25], which could cause its sensing sample unreliable. To avoid this issue, we can set this constellation point to “0” in the constellation mapping.

2) OFDM symbol: In principle, our generated OFDM symbols can be obtained from any dummy binary sequences. However, to locate each symbol from received signals, we design the content of OFDM symbols to be highly correlated (e.g., using the training sequence used in Wi-Fi or Barker code [26]) and the same to each other. Researchers may also customize their sequence according to a specific task while ensuring a good correlation.

3) Cyclic prefix: A cyclic prefix needs to be added prior to each OFDM symbol to overcome the inter-symbol/carrier interference (ISI/ICI). Because OFDM symbols in RF-Wise have the same content as stated above, each symbol serves as the prefix of the next one automatically and we do not need to add an extra cyclic prefix in RF-Wise.

4) Non-linearities: Modulating the continuous wave (both amplitude and phase) may cause different behaviors of the tags. In particular, non-linearities [27] can be detrimental to both sensing and communication processes. Since these non-linear phenomena are unrelated to sensing targets, maintaining a consistent customization of the entire continuous wave for each RFID inventory helps limit a constant non-linear factor, thereby minimizing adverse impact on system performance.

B. Harnessing Hardware-constrained Wider-band

Before elaborating the detailed feature designs, we propose to harness wider bandwidth to further augment $H$ first.

1) Opportunity and Problem: Since the number of bits backscattered by tag in each query is small, e.g., 96–128 bits for EPC, the bandwidth used for RFID communications is relatively narrow usually (1~2 MHz), while the total allowable or usable bandwidth for RFID communications is much wider, e.g., 26 MHz (U.S.), 8 MHz (Australia), 5 MHz (China), etc. This inspires us to further spread OFDM symbols to occupy more bandwidth to obtain more concurrent samples from each query, e.g., with the bandwidth of 25 MHz, each $H_i$ can produce 150 samples over this band. On the other hand, a wider bandwidth can increase the timing resolution of each $H_i$ further ($\Delta t \propto 1/B$, the smaller the better). This is beneficial, especially for capturing the object’s or human’s mobility.

Problem. Within an allowable bandwidth upper-bound ($B_u$), we find that the bandwidth $B$ may not be able to simply set as $B_u$, since an inappropriate $B$ will cause a serious cascaded integrator-comb (CIC) roll-off issue [15] and other hardware problems to “pollute” the transmitted signal and undermine the sensing. This is a unique challenge when more bandwidths are leveraged in the RFID sensing.

2) Enlarging the bandwidth: CIC filters are a class of finite-response filters, which are used in both the RF signal transmitting and receiving [28] combined with an interpolator or decimator:

- Transmitting: they are the anti-imaging filters to interpolate signals for increasing the sample rate, e.g., Fig. 7-(top).
- Receiving: they are anti-aliasing filters to decimate signals for reducing the sample rate, e.g., Fig. 7-(bottom).

The purpose of performing interpolation or decimation is to bridge the rate mismatch between the sample rate (whose value equals the bandwidth $B$) and the DAC/ADC rate $r$ (where $r$ is fixed and equals 100/200/400 MHz normally in RFID systems). Fig. 7 depicts the CIC filters in interpolation and decimation, where $D$ is a delay length, $Z$ denotes a Z-domain transfer, and $R = \frac{1}{77}$ which is a key ratio to be determined for
Fig. 7. The CIC filter used for interpolation and decimation.

avoiding the CIC roll-off issue. To this end, we consider the following two aspects:

1) First, to ensure RFID to communicate normally, the ratio $R = \frac{B}{2}$ needs to be an even number according to the hardware characteristic [29]. Otherwise, a strong response will always appear around the central frequency to dominate the signal and undermine the sensing. However, for our sensing design, we find that an even number may not be enough and $R$ should be further in a form of $2^i$, where $i$ is a positive integer, as Fig. 8 depicts. In traditional RFID communications, $B$ is 1~2 MHz usually, satisfying $R$’s requirement thus without suffering the CIC roll-off issue.

2) On the other hand, the value of bandwidth $B$ also impacts the feasible range of other RFID meta parameters $\theta_B$, including $f_{BLF}$, $P_{T_{Real}}$, $P_{T_{tari}}$, etc. These parameters together decide the lengths ($L_j(\cdot)$) of Query, RN16, ACK, and EPC, which must be integers ($\in N_+$). For instance, the length for EPC can be computed by $L_{EPC}(\cdot) = (t_1 + t_2 + t_{epc} \cdot 10^6/f_{BLF}) \cdot B/10^6$, where $t_1$ and $t_2$ are waiting delays before and after the duration of $t_{epc}$.

With above understanding, the solution can be formulated as maximizing bandwidth $B$ subjected to hardware constraints:

$$\max_{\{\theta_B\}} B,$$

subject to:

$$B \leq B_u,$$ (5)

$$\frac{r}{B} \in \{2^i\}, \ i = 1, 2, \ldots,$$ (6)

$$L_j(B, \theta_B) \in N_+, \ j = 1, \ldots, 4,$$ (7)

where Eq. (6) avoids the CIC roll-off issue and Eq. (8) ensures all the lengths of RFID commands to be integers. By solving this problem, we can determine $B$ and leverage this wider bandwidth to augment each $H_i$ in $\mathcal{H}$ to include the sensing samples from more frequencies. Meanwhile, the above constraints also ensure that the underlying RFID communications are not impacted.

**Summary.** With our customized continuous wave $\pi$, we can multiplex frequencies to obtain fine-grained sensing samples from each query (Section III-A). In this subsection, we leverage more allowable bandwidth under hardware constraints for augmenting the number of sensing samples further. As Fig. 9(a) shows, if we simply adopt a wider bandwidth (e.g., 25 MHz) without frequency multiplexing, only the central frequency is strong and other frequency components are too weak to be utilized for sensing. In contrast, with our design, the entire band can be utilized for sensing, as Fig. 9(b) depicts.

Fig. 8. The CIC roll-off issue occurs severely when the ratio $R$ is odd, then becomes moderate ($R$ is even) and disappears ($R$ is power of 2). In the last case ($R = 4$), the subsequently extracted sensing features will not be impaired by the strong peak due to the roll-off issue.

In addition, further expanding the bandwidth can bring more powerful sensing capability for RFID. However, our primary concern lies with the sensing range. Specifically, when transmitting a wideband (out-of-band) signal, the transmitting power is restricted by FCC regulations, which may limit its application scenarios. More discussion can be found in Section VII.

**C. Sensing Feature Extraction**

In Section III-A, we obtain the sensing samples $\mathcal{H} (= \{H_i\})$ from each query, and $H_i$ is the channel frequency response from each complete OFDM symbol $i$. Through our study, we find that under FM0 coding (the default setting of this paper), the “ON/OFF” state lasts for a half of or a whole bit length for bit “0/1”, respectively, as shown in Fig. 10. There are thus two different formats of $H_i$ when OFDM symbols are obtained from different bits with different merits.

1) **Towards static targets:** The first type of sensing feature is $\mathcal{H}^1 (= \{H_i^1\})$, where OFDM symbols are obtained from bits “1” only. In this case, the upper-bound $N$ for the number

![Fig. 10. Duration of “ON/OFF” state for FM0-based bit “0/1”, respectively.](image-url)
of sub-carriers is larger (i.e., the factor $\mu = 1$ in Eqs. (1) and (2)) compared with $N$ in the next case.

The advantage to collect OFDM symbols from only bits “1” is that each $H_j^1$ contains the sensing samples from more subcarriers, e.g., finer-grained sensors across frequencies, while the drawback is that there are no sensing samples from bit “0”, leading to some “empty” sensing spots along the time in the received EPC signal. Fortunately, to sense static targets (e.g., liquid recognition), the frequency granularity (refers to the number of distinct sensing frequencies) dominates the sensing performance rather than the number of $H_j$s. Because different sensing frequencies produce different weak couplings [20] between the tag and object, which is the source of sensing features. Therefore, if RF-Wise is deployed to sense static targets, we propose to configure RF-Wise to collect $H_j^1$ from bits “1” only and then derive the following feature from $H_j^1$ for applications:

$$F_{sta} = \frac{1}{q_1} \sum_{i=1}^{q_1} H_i^1(\text{on}) - \frac{1}{q_2} \sum_{j=1}^{q_2} H_j^1(\text{off})$$

(9)

where $q_1$ and $q_2$ are the numbers of OFDM symbols identified from the “ON” and “OFF” states for bits “1” in each query, respectively.

As $H_j^1(\text{off})s$ include the channel propagation of query signals (containing some environment information), and the $H_j^1(\text{on})s$ involves both the channel propagation and the tag’s backscattering of query signals, computing their difference can alleviate environment impacts and feature offsets caused by hardware [30]. Feature $F_{sta}$ is a $N$-dimensional vector and each element represents a sensing measurement of different frequencies, i.e., different coupling effects happened between the target and tag. We use it for the liquid classification application in our evaluation.

2) Towards dynamic targets: The other option of sensing feature extraction can be $H_j^{0/1} (=\{H_j^{0/1}\})$, where OFDM symbols are obtained from both “0,1” bits. Because the state duration of bit “0” is only half of that of bit “1”, in this case, we have to set $N$ to be half of the $N$ above (i.e., by setting $\mu = 2$ in Eqs. (1) and (2)), and the actual number of subcarriers $N'$ also becomes smaller. However, the advantage is that there will be always two $H_j^{0/1}s$ obtained from each bit (no empty sensing spots), which is suitable to sense the moving targets, e.g., the hand gestures. So, if RF-Wise is used to sense dynamic targets, we propose to collect $H_j^{0/1}$ and treat it as the feature directly:

$$F_{dyn} = H_j^{0/1} = \{H_j^{0/1}\}_{i=1}^{q_3}$$

(10)

where $q_3$ denotes the number of OFDM symbols identified from a series of queries during the sensing task. Feature $F_{dyn}$ is a $N' \times q_3$ matrix to better capture target’s subtle temporal varying, which will be further optimized and used for the gesture recognition in our evaluation.

In particular, since $F_{dyn}$ contains $N'$ sensing measurements from different frequencies towards the same moving target, some of them may contain redundant sensing information. According to our experiments, these redundant measurements have limited contributions to the downstream sensing application designs but introduce unnecessary computation overhead. Moreover, redundant measurements may appear in different frequencies for different sensing tasks. We thus cannot simply decrease $N'$ to a smaller number arbitrarily. To overcome this issue, we propose to extract the most representative frequency components by adopting the principal component analysis (PCA) algorithm [31]. In addition, any dynamic target may not have an exactly same moving speed, leading to a fact that $q_3$ can be different each time. Hence, we further employ sequence warping [32] to unify the feature length for matching the input size of the consequent machine learning method or neural network in our system implementation.

Summary. We note that $F_{sta}$ and $F_{dyn}$ introduced above are two examples for two typical sensing scenarios merely. Users are not forced to use them, which can be modified or even re-designed according to the particular sensing requirements. In summary, RF-Wise is configured by the following two steps for a sensing application:

- After the formulation from Eqs. (5) to (8) is solved, we can first determine the bandwidth $B$ and other meta parameters to ensure RFID’s communications.
- Factor $\mu$ (in Eqs. (1-2)) is then determined based on the sensing scenario: static ($\mu = 1$) or dynamic ($\mu = 2$), so that a suitable feature can be adopted.

In addition, RF-Wise will introduce a range of parameter configurations including both RFID-specific and system-specific parameters (detailed in the next Section). System-specific parameters, such as the number of subcarriers and the strength factor $\alpha$, are configured to fulfill different bandwidth requirements that ensure optimal sensing performance while minimizing computational overhead. So it somewhat characterizes RF-Wise as a setup-dependent system. However, those RFID-specific parameters adhere to RFID standards, their optimization represents a generic and compliant design across different frequency bands and commercial RFID systems. To this end, RF-Wise doesn’t entirely rely on specific setups.

IV. IMPLEMENTATION

A. Experimental Setups

Hardware. RF-Wise is developed using one USRP X310 with one SBX-40 daughterboard. Two directional antennas (Laird S9028PCR with the gain of 8 dBi) are installed to transmit and receive signals to and from the Alien 9640 RFID tag, respectively. USRP is connected to a desktop of an Intel Core i9-9900K CPU, 32 GB RAM, Intel Converged Network Adapter X520-DA1 and 10 Gigabit Ethernet Cable for a high bit-rate sensing data collection.

Software development. The back-end of RF-Wise runs on the EPC Gen2 protocol using GNU Radio 3.7 and UHD 3.15 on Ubuntu 18.04. The public native EPC Gen2 source code [16] does not support the modulation of the complex numbers to encode OFDM symbols into the continuous wave. Therefore, we have also made significant engineering efforts to augment this source code to support the following new features:

- We enhance the implementation of the Reader Block by adding new codes to process complex numbers and enable I/Q modulation on continuous waves.
• The I/Q modulation with complex numbers will increase the volume of the internal signal data to process (the size of “gr_complex” is twice the size of float), which leads to a “core dumped” error. We propose and implement a memory segmentation strategy to address this issue. In particular, by monitoring the memory consumption during the execution of EPC Gen2 protocol, we find that each command from a reader is allocated with a space of about 5000 “gr_complex” samples. However, increasing the bandwidth leads to more baseband samples, and the next command will occur earlier before the current one is fully transmitted. We thus propose to segment them into several sub-spaces to tackle this issue.

• Configuring RFID to work on a wider band, e.g., increased from 2 MHz to 25 MHz, is non-trivial. We add new codes to support the adaptation of RFID’s meta parameters to harness a wider bandwidth.

According to the Ettus USRP document [33], the previous USRP N210 with a 1 GigE interface and a 40 MHz daughter-board provides a usable bandwidth up to 20 MHz only, which is limited by the 1 GigE interface [33]. We thus augment the EPC Gen2 source code for the more recent X310 platform. So far as we know, no prior work has made the engineering efforts above to bring the complex-number modulation to RFID and fully leverage the wider bandwidth yet without impacting the underlying communication.

B. Parameter Configuration

RFID-specific parameters. To adhere to various RFID bandwidth requirements globally, we adopt three typical bandwidth upper-bound ($B_u$) settings for the evaluation:

1) Large: $B_u = 26$ MHz, e.g., in U.S.A.
2) Moderate: $B_u = 10$ MHz, e.g., in Australia.
3) Small: $B_u = 2$ MHz, e.g., China, Japan and Europe.

To solve the formulation from Eqs. (5) to (8), we have tried each RFID meta parameter with small discrete value steps and examined all the combinations. For each $B_u$, the bandwidth $B$ is selected to 25 MHz, 10 MHz, and 2 MHz respectively, and other parameters are the same (listed in Table I). We note that for $B_u = 26$ MHz, other parameters may lead to a higher $B$ but will cause system’s working unstable. We thus still use the parameters in Table I for $B_u = 26$ MHz as well.

<table>
<thead>
<tr>
<th>$f_{BLF}$</th>
<th>$P_{T_{Recal}}$</th>
<th>$P_{T_{Recal}}$</th>
<th>$P_{T_{l}}$</th>
<th>$P_{T_{f}}$</th>
<th>$P_{D_{C}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 KHz</td>
<td>160 µs</td>
<td>60 µs</td>
<td>20 µs</td>
<td>180 µs</td>
<td>380 µs</td>
</tr>
</tbody>
</table>

System-specific parameters. We discuss two parameters used by RF-Wise: the sub-carrier number $N$ and the strength factor $\alpha$ multiplied to our customized continuous wave $s'$.

After the parameters are obtained for each $B_u$, for each type of the sensing features to be used (e.g., $F_{sta}$ or $F_{dyn}$), we can determine the maximal number ($\tilde{N}$) of sub-carriers that can be adopted. However, we find that it is not necessary to set the sub-carrier number $N$ to $\tilde{N}$, because it will increase the computation overhead unnecessarily. For instance, when $B = 25$ MHz, $N$ can be set up to 250, while when it exceeds 150, the obtained feature diversity for $F_{sta}$ improves only marginally, as shown in Fig. 11(a). We thus adopt $N = 150$ to balance the sensing performance and computation cost. In Table II, we list the values of $N$ for all the sensing scenarios in our evaluation. On the other hand, we find that $\alpha$ cannot be set excessive large; Otherwise, the continuous wave $s'$ will become too noisy, which will impact the EPC decoding by the reader, as Fig. 11(b) shows. In Table II, we also list the $\alpha$ values adopted in different sensing scenarios in our evaluation.

![Fig. 11. (a) Feature diversity increases only marginally when $N$ becomes large enough. (b) Large $\alpha$ can impact the decoding rate of RFIDs.](image)

**TABLE I**

<table>
<thead>
<tr>
<th>$f_{BLF}$</th>
<th>$P_{T_{Recal}}$</th>
<th>$P_{T_{Recal}}$</th>
<th>$P_{T_{l}}$</th>
<th>$P_{T_{f}}$</th>
<th>$P_{D_{C}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 KHz</td>
<td>160 µs</td>
<td>60 µs</td>
<td>20 µs</td>
<td>180 µs</td>
<td>380 µs</td>
</tr>
</tbody>
</table>

**TABLE II**

<table>
<thead>
<tr>
<th>$B = 25$ MHz</th>
<th>$B = 10$ MHz</th>
<th>$B = 2$ MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_{sta}$</td>
<td>$F_{dyn}$</td>
<td>$F_{sta}$</td>
</tr>
<tr>
<td>$N = 150$</td>
<td>$N = 100$</td>
<td>$N = 80$</td>
</tr>
<tr>
<td>$\alpha = 6$</td>
<td>$\alpha = 5.5$</td>
<td>$\alpha = 5.5$</td>
</tr>
</tbody>
</table>

V. EVALUATION

We evaluate the performance and the utilities of RF-Wise through two useful applications, and the experimental environment includes typical office furniture and equipment.

1) Liquid classification. As stated in Section II, non-intrusive liquid classification is beneficial to the food safety. In this

![Fig. 12. Setups for (a) liquid classification and (b) gesture recognition.](image)
evaluation, we experiment on 18 different liquids commonly in our daily life, including similar liquids (e.g., coke-pepsi-sprite, beer-wine, skimmed-whole milk, etc.), which are illustrated in Fig. 12(a) and detailed in Fig. 14. For each liquid, we fill it in a plastic container of 200 mL with one tag attached to surface of the container with a thin plastic foam of 1 mm in between (to ensure tag backscatters properly [20]). The antenna-to-tag distance is 50 cm. For each liquid, we collect the sensing data from 250 to 350 times. We then adopt 2/3 of the data to train a classifier (stated below) and the rest data for evaluation.

2) Gesture recognition. Gesture recognition is another useful application to enable contactless HCI. In this evaluation, we invite five users (3 males and 2 females, informed consent is obtained) to conduct the same set of six hand gestures as [34], including to rotate left/right, sweep left/right and zoom in/out. For these gestures, we collect 1200 sensing data in total. We adopt 2/3 of the sensing data for training and the rest for evaluation. The antenna-to-tag distance is also 50 cm, as shown in Fig. 12(b). We also evaluate RF-Wise under various settings, e.g., different hand-to-tag distances, different speeds to perform gestures, etc.

3) Classifier. To understand the effectiveness of RF-Wise’s sensing features, we adopt a lightweight classifier — the random forest in Weka 3.8.5 [35] — for both applications (without using the advanced neural networks). The four main parameters in a random forest are empirically set as $P = 100$, $I = 100$, $V = 0.001$, and $S = 1$. Among them, “P” specifies the number of features to be considered in each decision tree, “I” determines the number of decision trees contained in a random forest, “V” sets the maximum depth of each decision tree, and “S” defines the random seed.

A. Performance in Liquid Classification

We compare the following methods in this application:

- **PAR-PHA** [36]: using one pair of tags (PAR) and the signal’s phase information (PHA) for sensing;
- **PAR-HOP** [12]: using one pair of tags (PAR) with the mechanism of frequency hopping (HOP) for sensing (both RSS and phase, same as ARY-HOP);
- **ARY-HOP** [13]: using both one tag array of eight tags (ARY) and the frequency hopping (HOP) for sensing;
- **RF-Wise**: our proposed method using only one tag and the $F_{sta}$ feature ($B = 25$ MHz by default) for sensing.

1) Overall performance: Fig. 13(a) reports the accuracy among these methods. With the single-dimensional feature from the signal’s phase, PAR-PHA cannot classify 18 liquids reliably with an accuracy of 57.5% only. Upgraded by the frequency hopping, PAR-HOP can improve the accuracy to 87.9%. We find that its performance is mainly limited by the large latency between the hopping at any two frequencies, e.g., 200 ms, so that PAR-HOP only hops seven frequencies [12] for efficient classification. As shown in the next application when the sensing target is moving, such a large latency will degrade the sensing performance significantly. Next, by using eight tags, ARY-HOP further improves the accuracy to 94.6%. In contrast, RF-Wise uses only one tag and achieves the highest accuracy of 98.2%. Compared with PAR-PHA, the fine-grained features from RF-Wise leads to 40.7% gain.

Moreover, Fig. 14 shows the detailed confusion matrix of these 18 liquids classified by RF-Wise. We can see that RF-Wise can achieve an accurate classification, which has errors occasionally for highly similar liquids, e.g., among Coke, Pepsi, and Sprite, or between whole and skimmed milk. To further investigate how RF-Wise can distinguish them, we employ principal component analysis (PCA) to project sensing features into a low-dimensional space for visualization, as depicted in Fig. 15. From the figure, it becomes evident that the distances in feature space between these liquids present our features’ powerful sensing capability (whole/skimmed milk and Coke/Pepsi have similar ingredients, while juice and yogurt are quite different).

2) Performance v.s. bandwidth: The performance of RF-Wise in Fig. 13(a) is achieved by using the bandwidth of 25 MHz. In Fig. 13(b), we further investigate RF-Wise under
other two bandwidth settings. The result shows that even for the common 2 MHz, the fine-grained sensing feature obtained through RF-Wise can lead to a good result already, e.g., 94.8% classification accuracy, which can be further increased to 97.1% when the bandwidth is 10 MHz. Fig. 13(b) indicates that compared with the prior methods, the fine-grained sensing feature across different frequencies is the main source leading to RF-Wise’s performance improvement.

3) Feature’s sensitivity: In Fig. 16, we further introduce two more challenging settings intentionally to demonstrate the necessary to use fine-grained features for liquid classification.

In the first setting, we start from the pure wine and add different volumes of water, e.g., 5 mL (2.5%), 10 mL (5%) and 15 mL (7.5%), and show the features obtained by RF-Wise. From Fig. 16(a), we can see that with different volumes of water mixed into the wine, some sub-carriers exhibit distinct frequency responses, which provides an opportunity to distinguish them. This ability can be used to detect the fake wines, e.g., with 5% or more water mixed, we can achieve the accuracy of over 99% to distinguish them.

In the second setting, we open one bottle of fresh milk and collect its sensing features after one, two and four hours (in the environment with a temperature of 30 ∼ 35°C). Fig. 16(b) depicts that their features show differences across sub-carriers and we highlight the most evident parts by the red circles. Both of these two experiments show the importance of fine-grained features to capture the subtle differences for sensing.

4) Performance v.s. distance: To evaluate how RF-Wise performs at different tag-to-reader-antenna distances, we keep 25 MHz setting and plot the result in Fig. 17. The system maintains robust performance within 1 m, experiences slight degradation between 1.5 ∼ 2.5 m, and exhibits a drop in performance below 90% classification accuracy at 3 m, deteriorating further towards the maximum reading range of 3.5 m. This is reasonable that lower SNR degrades sensing and communication performance. Note that the maximum reading range of 3.5 m (ensures the extraction of multi-frequency sensing features and accurate decoding of tags’ responses) is attributed to constraints inherent in the USRP platform and the native EPC Gen2 codes, rather than our design. This operational range is deemed acceptable for scenarios involving gesture recognition and liquid classification in existing research.

B. Performance in Gesture Recognition

In this application, we compare RF-Wise (using one single tag and the $F_{dyn}$ feature) with PAR-PHA and PAR-HOP as well. For ARY-HOP, we find the large latency in the frequency hopping undermines its sensing performance in the dynamic sensing scenario. Hence, we change it to:

- ARY-PHA [34]: using a tag array of ten tags (ARY) and the signal’s phase (PHA) for sensing.

1) Overall performance: Fig. 18(a) shows the accuracy of recognizing six hand gestures by different methods. PAR-PHA achieves an accuracy of 77.3% (which is higher than the accuracy of 57.5% in the liquid classification, because the number of liquids is much larger than that of the gestures). With frequency hopping, the accuracy of PAR-HOP is even decreased and the reason will be explained soon. With the help of multiple tags, ARY-PHA improves the accuracy to 92.9%, while RF-Wise can achieve 97.5% using one tag only. Compared with PAR-PHA, 20.2% gain is obtained by using the RF-Wise’s fine-grained features with one tag only. In addition, ARY-PHA still faces the issue of collisions. Typically, one ARY-PHA feature is obtained after every tag in an array has been read once. As the number of tags increases, collisions among these tags degrade the sensing rate, resulting in longer acquisition duration for one ARY-PHA feature. This may render ARY-PHA a coarse-grained sensing method for dynamic targets when the tags’ number is much larger.

To understand why the frequency hopping becomes less effective for a dynamic sensing target, we ask a volunteer to perform one gesture three times, and Fig. 19(a) shows the features extracted by PAR-HOP each time. The signal actually senses different parts of the gesture each time due to the
large and uncertain hopping latency. Moreover, and each phase measure leads to a limited number of features to be used. In contrast, the signal from RF-Wise can capture the gesture consistently (without hopping delay) and obtain fine-grained features over frequencies each time (Fig. 19(b)), which thus leads to more reliable sensing results even in the dynamic sensing scenario.

Fig. 19. The feature collected from three queries by using (a) frequency hopping and (b) RF-Wise.

In Fig. 18(b), we examine the RF-Wise’s performance under the other two bandwidth settings. The common 2 MHz can lead to 96.1% which will be further increased to 97.2% when the bandwidth is 10 MHz. Such a result also suggests that the high-resolution and fine-grained sensing features are the main source leading to sensing improvement.

2) Impact of gesture speeds: In the evaluation, we only use the sensing data collected when all the volunteers perform gestures in a normal speed to train the classifier. In Fig. 20(a), we use this classifier to test on the gestures with relatively slower and faster speeds. We can see that the accuracy for both setting is decreased slightly, e.g., 91.7% (slow) and 95% (fast). One possible way to further improve the accuracy is to include a few training data under different speeds. The performance can be improved, e.g., 95.8% (slow) and 96.7% (fast) in Fig. 20(a).

3) Impact of hand-to-tag distances: So far, we only use the sensing data collected with the hand-to-tag distance of 5 cm to train the classifier. In Fig. 20(b), we use it to examine the performance when the distance is prolonged to 15 cm. It is understandable that the accuracy will decrease when this distance increases, while the accuracy is still above 90% at 15 cm. If we add more training data collected from different distances, the accuracy is consistently high across these distances.

C. Micro-benchmarks

1) Compatible to RFID communication: To understand whether RF-Wise impacts on the underlying RFID communication, we conduct a series of micro-benchmarks in this subsection. For a comprehensive understanding, we add two more bandwidth settings of 4 and 20 MHz in this experiment. For each micro-benchmark, we use the performance by running the native EPC Gen2 protocol over a common 2 MHz band as a baseline. Some key parameter configurations include a 915MHz center frequency, 40 KHz BLF, and FM0 coding. The devices (USRP, antenna, tag, etc.) and experimental environments remain consistent with those used for RF-Wise.

Fig. 20. Recognition accuracy v.s. (a) the gesture speed and (b) the hand-to-tag distance.

Fig. 21. Compatibility to RFID communications and computation latency.
bandwidth. The corresponding results for $F_{dy}$ are 2.2 ms, 7.2 ms, and 18.3 ms. It suggests that RF-Wise does not introduce expensive computations.

3) Signal power: According to FCC regulations, the power of the signal should not exceed the maximum threshold (around 36 dBm within the ISM band). Measuring the dBm value of a signal requires a dedicated and expensive measurement device that is not available to us. Therefore, we use another alternative way to measure the power level of our design. Specifically, we use another USRP device as a monitor to measure the power (relative gain in dB) of our transmitted signals and compare it to the power from a standard EPC Gen2 RFID communication (this is viewed as a baseline). As shown in Fig. 23, the baseline produces an average -42.5 dB relative gain, and RF-Wise leads to comparable or even lower powers, such as -51.5 dB to -42 dB when $\alpha = 1 \sim 6$. In particular, RF-Wise is configured for the best sensing performance, i.e., 25 MHz bandwidth and 150 sub-carriers, while all other system settings are the same as the baseline. The result indicates that RF-Wise can ensure a legal execution of EPC Gen2 complied to the FCC regulations.

![Gain (dB) vs. $\alpha$](image)

Fig. 23. Power measures with different $\alpha$ values

4) Environmental impacts: In this experiment, volunteers were instructed to walk both alongside and in front of the system, varying the distances from 0.5 m to 4.5 m. As depicted in Fig. 24, walking in front had more effects compared to walking alongside. For liquid classification, there is about a 30%–40% accuracy reduction at distances less than 1.5 m, while performances recover to about 90% at distances of 3.5 m and 2.5 m for walking in front and alongside, respectively. In contrast, impacts on gesture recognition were less significant. Sensing performance remains moderate (over 90%) at distances exceeding 1 m. Our directional antenna’s field of view is about 72 degrees, resulting in fewer impacts from the side compared to the front. Since this problem is a kind of cross-domain issue, we would like to further discuss it in Section VII.

5) Comparison: To ensure a focused comparison, we primarily considered recent and promising wideband RFID sensing research in Table. III. All these methods require either two devices or hardware integration to improve sensing/localization performance. However, the cost and overhead of extra devices, customized hardware, and system synchronization are relatively higher than RF-Wise. For instance, RFind [37], RF-EATS [1], and POLAR [38] are formed with numerous narrowbands, introducing time latency for acquiring wideband sensing features. While RF-EATS’s liquid classification result is similar to ours requiring about 20×–40× bandwidth. Additionally, TurboTrack [30] transmits a 100 MHz wideband signal, which can be considered as a trade-off between bandwidth and system efficiency/cost. In contrast, our approach is more feasible for implementation in commercial RFID systems, providing multi-frequency and wider-band sensing while preserving RFID’s essential advantages and communication function.

VI. RELATED WORK

In existing RFID systems, reader can obtain accurate phase information from the RF signals, which are leveraged in many designs bounded to tag’s own movements, e.g., localization of tags [39]–[41], vibration counting [10], etc. However, it is not sufficient for a large spectrum of sensing tasks relying on the fine-grained features extracted from the RFID signals.

To advance RFID sensing, one representative family of solutions is to use a tag array of multiple tags and measure the RSS/phase/Doppler-shift information from these different tags to harness their features’ spatial diversity [42]–[44]. In particular, GRFid [45] and RF-finger [34] use 35 and 40 tags

<table>
<thead>
<tr>
<th>TABLE III</th>
<th>COMPARISON TO FOUR RECENT AND PROMISING METHODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>220</td>
</tr>
<tr>
<td>Number of devices</td>
<td>2</td>
</tr>
<tr>
<td>Customized hardware</td>
<td>No</td>
</tr>
<tr>
<td>Maintenance cost/overhead</td>
<td>moderate</td>
</tr>
<tr>
<td>Classification Performance</td>
<td>/</td>
</tr>
</tbody>
</table>
to recognize different gestures. TagScan [13] adopts two linear tag arrays (eight tags for each array) for material sensing and shape imaging. EUIGR [46] and TagSMM [47] utilize four and six tags in their sensing designs. In addition to the deployment overhead of using multiple tags, the main drawback is the collision incurred among tags, which can easily degrade the sensing performance, especially in sensing the moving target.

To overcome such limitations, recent works tend to use fewer tags and employ frequency hopping to increase the sensing fidelity across frequencies [12]. This principle works but the practical hurdle comes from the relatively large latency for hopping between two frequencies in RFID systems. As shown in the evaluation, its improvement is limited, especially in sensing the moving target. To advance prior sensing designs, some recent works [1], [30], [37] propose to transmit wideband (100~500 MHz) signals during the RFID communication, to obtain multi-dimensional and high-resolution sensing information. However, the cost of such an extra transmitting device and the overhead of synchronizing this extra signal with the RFID signal before the feature extraction cannot be neglected.

In summary, leveraging wideband and multi-frequency features to augment sensing performance presents several limitations. i) Large time latency. Frequency hopping usually takes about 200 ms to switch frequencies once, while previous wideband methods are achieved by combining consecutive narrow bands using the band splicing technique [48]. The acquisition of a multi-frequency/wideband sensing feature takes much time. ii) High cost and overhead. To the best of our knowledge, previous studies on multi-frequency and wideband RFID sensing employed two devices or directly integrated two communication systems, which raised higher deployment and maintenance costs. iii) Signal interference. It can be inferred that a wideband (covering the RFID band) sensing signal transmitted by device “A” can cause interference to RFID device/signal [49].

In contrast to existing methods, RF-Wise concentrates on introducing multi-frequency and wider-band sensing capabilities into RFID itself through a lightweight and software-based framework, without the need for additional devices and adhering to commercial RFIDs. RF-Wise is motivated by an insightful observation to customize the RFID signals [50]–[52], while these works mainly add noises to secure RFID signals, which are not related to the frequency multiplexing and do not address the unique challenges encountered in RF-Wise. In the literature, there are also some RFID-based application designs, e.g., authentication [53], temperature monitoring [54], beamforming [55], etc., which are orthogonal to this paper.

VII. DISCUSSION

Harnessing the wide bandwidth. Wideband and even ultra-wideband RFID sensing have been considered promising countermeasures to enhance the sensing capabilities of RFID recently. However, it raises a concern about whether a large bandwidth can be utilized simultaneously. In particular, the Federal Communications Commission (FCC) Regulation, especially in part 15.24x, mainly specifies the upper power limit for the center-frequency signal and harmonics. We have not identified an explicit regulation that prohibits the use of the entire bandwidth for transmission. Conversely, in the RFID standard, frequency hopping is employed to maximize spectral efficiency and minimize signal interference in optional multi/dense-interrogator (RFID reader) operating modes. The reader is required to adopt a channel plan in compliance with local regulations. However, in certain autonomous scenarios like factories, warehouses, and smart homes, without non-RFID systems (in-band) and dense readers, the use of the entire bandwidth (when necessary) for crucial sensing tasks is acceptable. Furthermore, the RFID standard notes that “even within a given regulatory region are prone to ongoing reinterpretation and revision”, suggesting a potential avenue for wideband RFID approval by manufacturers in the future.

Limited working range. RFID stands as a low-cost, low-energy-consumption, and widely deployed identification system in our daily lives. Sticking tags on different products is a natural working manner for RFIDs, making it an ideal method for sensing these objects’ material, location, movement, etc., compared to other RF sensing techniques. Moreover, with the advancement of UHF RFID, which typically operates within several meters using directional antennas, it still holds significant potential for contactless human-computer interaction and smart manufacturing applications. However, for smart services requiring a larger sensing range, such as those extending beyond 10 meters, alternatives like WiFi, millimeter-wave radar, and other RF-based solutions are preferred.

Environmental impacts. For static reflectors, their impact is limited as the offsets they cause in sensing features remain consistent across different targets. However, dynamic reflectors and environmental changes pose challenges for all RF signal-based sensing methods, representing a cross-domain issue. While this problem is a specific research topic, it falls outside the scope of our paper. Our focus is on proposing a lightweight, low-cost, and highly efficient solution that introduces multi-frequency and wider-band sensing capabilities into RFID itself while preserving its normal communication.

VIII. CONCLUSION

This paper presents RF-Wise, a system to push the limit of RFID sensing. The key innovation is that through a purely software-based solution atop standard RFID using one tag, RF-Wise can obtain fine-grained CSI-like sensing samples across frequencies concurrently. Based on this, we further propose novel designs to ensure that the added sensing ability does not impact underlying RFID communications and make great engineering efforts in the development. We finally show the advantages of RF-Wise through two useful applications. A preliminary version of this study has been published in the proceedings of IEEE INFOCOM 2022 [56].

ACKNOWLEDGMENTS

This work was supported by the GRF grant from Hong Kong RGC (CityU 11217420 and CityU 11213622), the NSFC Grant No.62302383, 62372365, 62176205, 62072367, project funded by China Postdoctoral Science Foundation No.2023M742792, and Yong top talent in XJTU JS6J003.
REFERENCES


Cui Zhao received his Ph.D. degree in school of cyber science and engineering from Xi’an Jiaotong University in 2022. He is currently an assistant professor in Xi’an Jiaotong University. His research interests include IoT, smart sensing, and wireless communication.

Zhenjiang Li received the B.E. degree from Xi’an Jiaotong University, China, in 2007, and the M.Phil. and Ph.D. degrees from the Hong Kong University of Science and Technology, Hong Kong, in 2009 and 2012, respectively. He is currently an Assistant Professor with the Department of Computer Science, City University of Hong Kong. He is a member of IEEE and ACM. His research interests include wearable and mobile computing, smart health, deep learning and distributed computing.

Han Ding received her Ph.D. degree in computer science and technology from Xi’an Jiaotong University in 2017. She is currently an associate professor in Xi’an Jiaotong University. Her research interests focus on AlOT, smart sensing, and RFID systems.

Ge Wang is an Assistant Professor at Xi’an Jiaotong University. She received her Ph.D degree at Xi’an Jiaotong University in 2019. She was a visiting student at University of California, Santa Cruz from 2017 to 2019. Her research interests include wireless sensor network, RFID and mobile computing.

Wei Xi received his Ph.D. degree in computer science computer science and technology from Xi’an Jiaotong University in 2014. He is now a professor in Xi’an Jiaotong University. He is a member of CCF, ACM, and IEEE. His research interests focus on wireless networks, smart sensing, and mobile computing.