Indoor Passive Device Ranging by Low-directivity Antennas with Centimeter Precision

Yunfei Ma, *Student Member, IEEE,* Xiaonan Hui, *Student Member, IEEE,* Pragya Sharma, *Student Member, IEEE,* and Edwin C. Kan, *Senior Member, IEEE*

***Abstract*—Compared to the high-directivity patch and horn antennas, miniaturized omni-directional antennas allow more flexible integration with portable devices because of their smaller size, lower cost, broader angle coverage and less phase center variations. However, locating passive tags with low-directivity antennas in indoor environment becomes even more challenging due to more multi-paths and weaker line-of-sight (LoS) path. We propose a simple solution by digital beamforming with just 2-element antennas in a broadband harmonic multi-static backscatter system to achieve reliable indoor ranging. The broadband backscatter operation is obtained by adding nonlinearity to RFID tag and we propose a simple design based on the wireless identification and sensing platform (WISP) open-source hardware platform to help facilitate research and development with such devices. To fight against dense multi-paths environments, our system employs sensing frequencies that are separated wider than typical indoor coherence bandwidth and therefore, we show that ranging robustness can be further enhanced by estimating angles of arrival (AoA) gap, i.e., unreliable measurements from dominant multi-paths can be distinguished and rejected. Millimeter-precision ranging in weak LoS environment is reliably achieved in a broad and sparse frequency scheme with omni-directional antennas which offer peak and average gain of 0.5dBi and -1.9dBi respectively. We present the fundamental theory, simulation and experiments with a homodyne harmonic RFID reader in a rich scattering environment.**

***Index Terms*—Beamforming, harmonic frequency, indoor locating, multi-paths, RFID, omni-directional antenna, WISP.**

I. Introduction

In addition to an integration platform for logistics and short-range communication, todays radio frequency identification (RFID) system is evolving towards a powerful network that is low cost and ubiquitous. Precise locating of passive tags is a key capability for many applications such as robotics, health care and the Internet of Things (IoT).

In recent years, RFID locating has received increasing attentions. Early works relied on measurement of the received signal strength (RSS) [1]–[3]. The accuracy of RSS based method is limited to meter-level due to the fact that RSS is not a sensitive function of distance and the interference introduced by indoor multi-paths. Compared to RSS based methods, carrier phase-based methods are preferred for their ultra-high sensitivity as a function of distance [4] and many techniques can be inherited from the relative mature outdoor radar technology. For example, when an RFID tag moved along a fixed trajectory, holographic RFID localization [5] adopted inverse synthetic aperture radar (ISAR) techniques to form a large virtue antenna array to collect the phase and amplitude of the received tag response and compute the image of "hologram" which could help pin down the initial position of an RFID tag. A measured median error about 30cm was reported. Tagoram [6] improved the performance of holographic RFID localization by adopting a technique called differential augmented hologram (DAH) and reported measured median localization error about 5mm. The major problem with holographic RFID localization, Tagoram and other ISAR and SAR based locating systems is that they required relative motions between tag and reader, which in many cases, cannot be easily implemented. The ability of locating a static RFID tag is highly desired. For static object locating, the most straightforward method is trilateration, which is the process of determining absolute or relative locations of points by measurement of distances and is widely applied in systems such as the global positioning system (GPS). Trilateraion requires measuring the distance from a tag to receiving antennas directly which we refer to as "ranging" process in this paper.

Although the measured carrier phase of an RFID tag response is very sensitive to distance, in practice, measured phase value always falls within $[0, 2\pi)$, and therefore cycle ambiguity exists when the distance is longer than one wavelength. In other word, when the measured phase is θ, the actual phase can be $\theta + 2n\pi$ where n is the unknown cycle integer which must be correctly solved in order to reduce the ambiguity. To deal with such a problem, BackPos [7], instead of directly determining the ambiguous cycle integer n, constrained the tag motion within a region of "interrogation zone", where the differential distance from two reader antennas to the target tag falled within half wavelength, however, at the expense of limited reading zone and rigid antenna configuration. Broadband harmonic backscatter proposed in [8] solved the cycle integer problem directly by selecting heuristic optimized sparse multi-frequency (HMFCW) sequence which was designed to offer the highest phase error tolerance for a given bandwidth. It has been shown that as long as the phase error is smaller than $90^\circ \times \mathrm{BW}\%$ [8], the cycle integer computation is 100% reliable which offered a median ranging error of 6mm in indoor environment.

Previous research has shown drastic accuracy improvement using phase-based method. However, all of the proposed measurements [4], [6]–[8] adopted high gain/directivity patch and horn antennas in an attempt to mitigate the phase errors caused by the dense multi-paths in an indoor environment. High-gain antennas such as horn and patch antennas on readers

Y. Ma, X. Hui and E. C. Kan are with the Department of Electrical and Computer Engineering, Cornell University, Ithaca, NY, 14853 USA e-mail: ym274@cornell.edu

and tags are often cumbersome because of their large size, weight and cost. The narrow angle coverage and high phase center variation pose additional difficulties in deployment and calibration [9]. Low-cost, omni-directional antennas such as whip or rubber ducky antennas offer much smaller size and weight, enabling easy integration to portable devices with broad angle coverage and low phase center variation. For example, the Laird S9028PCR 9dBi patch 900MHz antenna has dimension of 259×259×33mm and weight of 793g, while the Taoglas TG22 low-directivity whip antenna at same frequency offers 48mm×6mm∅ and 5.1g.

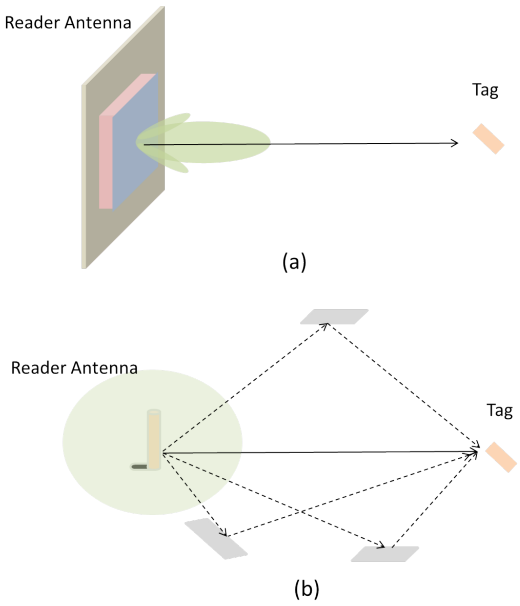

Fig. 1. (a) For large size high gain antennas, indoor multi-paths are much less "seen" due to the high directivity. (b) For small size low-directivity omni-directional antenna, the number of indoor multi-paths "seen" by the antenna dramatically increases.

The biggest challenge of using low-directivity receiving antennas is the increased multi-path interferences and weakened line of sight (LoS) signals compared to its high gain counterparts. As depicted in Fig. 1, even when there exists a clear LoS between the reader antenna and the tag, the multi-paths introduced by grounds, ceilings, walls as well as furniture can cause significant phase errors for low-directivity receiving antennas. In this paper, we ask the following question: **Can we achieve millimeter to centimeter accuracy ranging using low directivity antennas reliably in a dense multi-path indoor environment?** To make it more clear, we will not resort to approache which adopts a large N-element antenna array [10]. It is well known that a high gain antenna can be constructed by a large N-element linear antenna array [10]. However, building a large N-element antenna array will not help us to reduce the size and weight of our system, which are the main motivation why we purse the use of low-directivity antennas.

To achieve such a task, we need to overcome several challenges:
(1): In order to achieve high accuracy ranging, our system need to resolve ambiguous cycle integer correctly.
(2): Our system must be able to tolerate the carrier phase errors brought by the increased multi-paths seen by the low directivity antennas.
(3): Our system needs to handle the extremely poor channel condition. In reality, it is not uncommon that the LoS is overwhelmed by the mulit-paths interference, leading to totally unreliable measurement results. Our system must be able to distinguish between the reliable measurements and the unreliable measurements.

In this paper, we propose a system that meets the above three criteria simultaneously. The key idea of our approach is to empower our system with intelligence, i.e. our system is "smart" to know whether LoS dominates multi-paths (good) or the LoS signal is dominated by the multi-paths (bad). We engineer the concept of wireless channel coherence bandwidth [11] and use the difference of angle of arrival (AoA) from carrier that are separated further than the coherence bandwidth as the measure of wireless channel quality. We show that, instead of building a large N-element array [10], system intelligence can be obtained with just 2-element antenna array and a digital beamforming algorithm which help maintain the minimum complexity. Our system is designed based on the broadband harmonic backscatter [8]. Unlike the conventional backscatter approach, in harmonic backscatter, the uplink response is modulated on the higher order of harmonics generated by the nonlinear elements integrated in a passive tag. The separation of downlink and uplink response fundamentally eliminates the notorious self-jamming problems in an RFID reader and therefore can greatly enhance the bandwidth of operation. With a wide bandwidth of operation, we have the freedom to select optimal sparse ranging frequencies that are pair-wise separated further than the wireless channel coherence bandwidth. Before applying HMFCW ranging algorithm to resolve ambiguous phase cycle integers, we conduct AoA estimation on each carrier frequency by digital beamforming in the 2-element antenna array. The AoA gap (difference between the maximum AoA value and the minimum AoA value across the selected group of frequencies) offer an good opportunity to evaluate multi-paths dominance over LoS. Because mutli-path signals separated by more than the coherence bandwidth of the indoor ambient can be assumed to be independent and thus have very different AoA after beamforming. A threshold on AoA gap can be readily set to reject the measurements with over-dominant multi-paths.

The paper is organized as follows: In section II, we present the overall system description. In section III, we introduce the concept of coherence bandwidth and discuss AoA gap as a measure of channel quality. We briefly introduce recent progress in harmonic RFID and present the proposed Harmonic-Wisp, which is a broadband harmonic RFID tag integrated on the wireless identification and sensing platform (WISP) to help facilitate research and development on harmonic RFID systems in section IV. In section V, we discuss the ranging method in the proposed system including digital beamforming, AoA thresholding and HMFCW ranging algorithm. We present experimental evaluate of our proposed system in Sec. VI and draw our conclusion in Sec. VII.

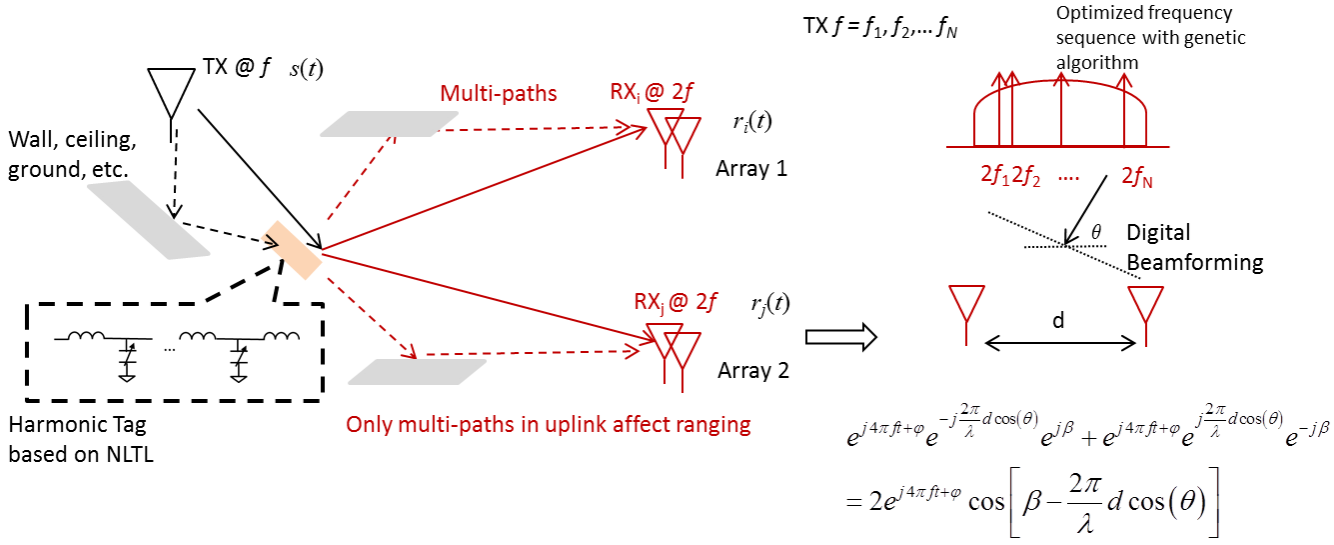

Fig. 2. Overview of the proposed ranging system.

II. System Description

The general approach is illustrated in Fig.2. The reader sends inquiry signal on carrier $\mathbf{f} = (f_1, f_2, \cdot, f_K)$. The tag contains nonlinear circuit elements. When the tag receives the inquiry signal from the reader, due to the nonlinearity, second harmonic signal on $\mathbf{f}_{2nd} = (2f_1, 2f_2, \cdot, 2f_K)$ will be generated and re-radiated back towards reader receiving antennas. Each receiving antenna consists of a 2-element antenna array, where digital beamforming is applied to estimate AoA on each of the received second harmonic carrier. The transmitting frequency sequence was carefully designed so that the second harmonic carriers are separated further than the coherence bandwidth ($|2f_i - 2f_j| > B_c$). When the multi-path is comparable to or stronger than LoS, because mutli-path signals separated by more than the coherence bandwidth of the indoor ambient can be assumed to be independent and thus have very different AoA after beamforming, while is AoA estimations on different carriers are similar when the LoS paths are strong compare to the multi-paths. A threshold on AoA difference can be readily set to reject the measurements with over-dominant multi-paths. Robust ranging is achieved by the phase error reduction in digital beamforming and the high phase error tolerance of the broadband HMFCW ranging method.

A. Coherence bandwidth and AoA gap as a measure of multi-path dominance

Coherence bandwidth is a statistical measure of the range of frequencies over which the channel can be can be considered "flat" [11]. Within coherence bandwidth, two frequencies have a strong potential for amplitude and phase correlation, but when two frequencies are separated larger than coherence bandwidth, their channel responses look more independent. Coherence bandwidth is a phenomenon that is directly related

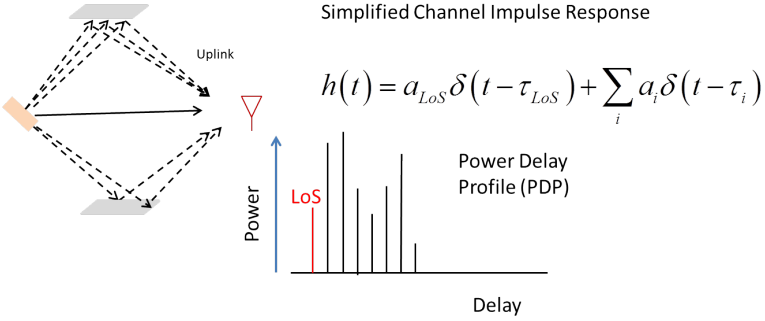

Fig. 3. Simplified wireless channel impulse response and power delay profile

to multi-paths propagation as shown in Fig. 3. For simplicity, a wireless channel impulse response can be written as:

$$h(t) = a_{\text{LoS}}\delta(t - \tau_{\text{LoS}}) + \sum_i a_i \delta(t - \tau_i) \tag{1}$$

where a_{LoS}, τ_{LoS} are the amplitude and delay of the LoS path, while a_i, τ_i are amplitude and delay of the i-th multi-path. For a transmitted signal $s(t)$ at frequency f

$$s(t) = \exp\left(\frac{j2\pi f}{c}t\right) \tag{2}$$

The received signal after multi-paths propagation can be expressed as

$$\begin{aligned} y(t) &= s(t) * h(t) \\ &= a_{\text{LoS}} \exp\left[\tfrac{j2\pi f}{c}(t - \tau_{\text{LoS}})\right] + \textstyle\sum_i a_i \exp\left[\tfrac{2\pi f}{c}(t - \tau_i)\right] \end{aligned} \tag{3}$$

The carrier phase along each multi-path is frequency and delay sensitive, which results in adding constructively and destructively on different frequencies as shown in Fig. 3. The propagation dely of different multi-paths can spread widely

across tens of nano seconds. Therefore, the sign of each multi-path component is very sensitive of the carrier frequency change which leads to a frequency selective channel response. Received signal responses at frequencies that are far apart vary drastically. The coherence bandwidth of multi-path profiles at different frequencies can be measured by the root-mean-square (RMS) multi-path delay spread δ_τ [11], and for the correlation level at 0.5, the coherence bandwidth is

$$B_c = \frac{1}{5\delta_\tau} \tag{4}$$

It is important to note that Eq. (4) is only empirical and

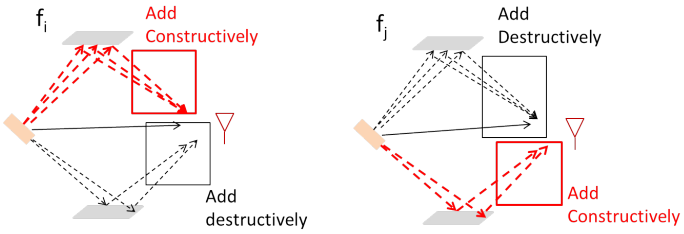

Fig. 4. Frequency selective channel response resulted from multi-paths

in general, spectral analysis techniques and simulation are required to determine the exact impact. However, from Eq. (4), we can see that the coherence bandwidth is inversely proportional to the RMS delay spread. With more multi-paths, the coherence bandwidth B_c tends to shrink which leads to a frequency selective wireless channel. For typical indoor environment with geometry size from 3m to 15m, δ_τ varies from 10ns to 50ns [11], resulting B_c from 4 to 20MHz. The coherence bandwidth gives us an opportunities to tell

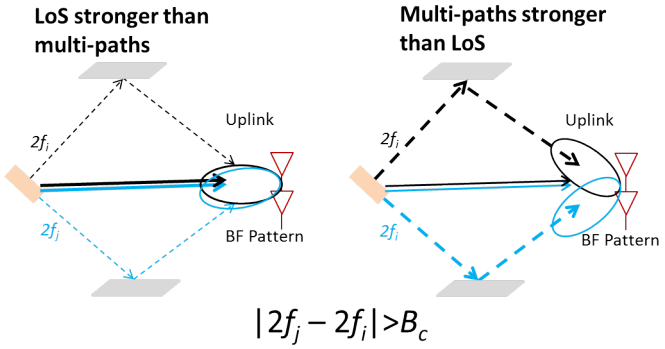

Fig. 5. Channel quality estimate w/ Gap of AoA. When LoS is strong, two frequencies will have close AoA. When multi-paths are strong, two frequencies will have different AoA estimations when separated larger than B_c. We utilize a 2-element antenna array to get the knowledge of AoA.

the channel conditions. We achieve such as task by leverage the "Gap of angle of arrival (AoA)" as shown in Fig. 5. For harmonic frequencies with separation wider than B_c, the strong multi-path signals will have large AoA differences as they are minimally correlated. For the LoS path, different frequencies are always heavily correlated no matter how large the frequency separation is. Therefore, when LoS is strong, AoA calculated from digital beamforming should yield a very similar angle for different frequencies, but when multi-paths are strong, for frequencies separated wider than B_c we expect large AoA gap, which can be used as a measure of multi-path dominance:

$$G_{\text{AoA}} = \max_k \left\{ \max_i(\beta_{k,i}) - \min_i(\beta_{k,i}) \right\} \tag{5}$$

where $\beta_{k,i}$ denotes the estimated AoA for the k-th 2-element antenna array on the i-th harmonic carrier. Please note that in HMFCW which will be discussed later, we are relying a frequency sequence $\mathbf{f}_{2nd} = (2f_1, 2f_2, \cdots, 2f_N)$ to resolve the phase cycle ambiguity problem.

B. Digital beamforming with 2-element antenna arrays

Our system needs to have intelligence to estimate the AoA gap. In order to get AoA information from each carrier, different from previous work using low-directivity antenna for indoor locating purpose [10], which resort to building a large M-element antenna array, we simply use 2-element antenna array. Although with the increased size M, a linear array can be designed with high directivity and super resolution algorithm such as MUSIC can be applied, however, a large M will leads to a heavy and cumbersome infrastructure which contradicts to our motivation of using miniaturized low-directivity antenna instead of cumbersome high directivity antenna. The multi-static ranging system with 2-element low-directivity antenna arrays are illustrated in Fig. 2 and Fig. 5. We strengthen the LoS signal by spatial filtering through digital beamforming with minimum array size of $M = 2$. The center of the beam is rotated by applying weighted sum of signals r_1 and r_2 in the dual channels:

$$r = r_1 e^{j\frac{\pi}{\lambda} d\cos(\alpha)} + r_2 e^{-j\frac{\pi}{\lambda} d\cos(\alpha)} \tag{6}$$

where α is the beam steering angle. For a signal with incident angle θ, the beamforming factor can be expressed as

$$BF = \cos\left\{ \frac{\pi d[\cos(\alpha) - \cos(\theta)]}{\lambda} \right\} \tag{7}$$

The signal phase is computed at α when r attains maximum. The effectiveness of spatial filtering depends on the antenna spacing d, as shown in Fig. 6. Increasing d gives a desirable narrow central beamwidth. However, the ambiguous side lobe with $BF = -1$ may arise which can cause $180°$ in the carrier phase computation and wrong AoA estimation. Notice that due to the broad frequency separation in HMFCW ranging, peaks of ambiguous side lobes spread much wider than the central beam peak. We implemented a two-stage search to avoid this multi-lobe issue. In stage one, we estimated AoA within $0°$ to $180°$ based on maximizing r in Eq. (6), and then used Eq. (7) to compute AoA corresponding to other potential peaks. In the second stage, we constructed groups of peaks by drawing one peak at a time corresponding to each sensing frequency for each group. The group with minimum deviation was selected. Then, we recalculated AoA around the average of the selected group with a reduced search range.

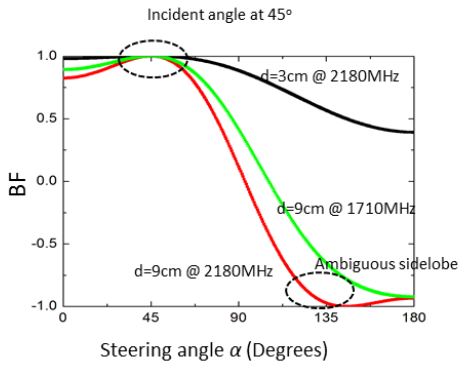

Fig. 6. Beamforming factors with different antenna separation at different frequencies. The incident angle is set at $45°$.

C. Harmonic-WISP passive RFID tag design

The AoA gap computation requires the use of frequency carrier separated further than the coherence bandwidth and hence, the backscatter communication between reader and tag needs to be broadband. However, the problems of self-jamming and interferences pose various design limitations on RFID hardware. Conventional passive RFID tags respond to inquiry signals by switching the tag antenna on and off to modulate the backscatter signal which can then be appropriately distinguished. However, because the uplink (tag to reader) and downlink (reader to tag) are on the same carrier frequency, strong leakage from the transmitter with 4W effective isotropic radiated power (EIRP) to the receiver, unintentional direct reflections from nearby walls and grounds, and backscattering from other tags some of which can be much closer than the present tag cause jamming to the receiver. The strong jamming will require high-isolation circulator, minimal reader antenna reflection S_{11} under all frequencies and ambient variations, and stringent receiver linearity, all of which will result in limited operation bandwidth as shown in Fig. 7(a). Harmonic RFID systems provide an opportunity to resolve these above issues [8], [12]–[16]. The harmonic RFID tag can be considered as a harmonic radar transponder [12] integrated with RFID digital components. Unlike conventional RFID tags, harmonic tags exploit nonlinear components to passively generate harmonics for the uplink response. The frequency separation of downlink and uplink allows ready interference reduction by bandpass filters and diplexers. No special isolation devices are needed at the reader RF front-end. Broadband antenna with relative poor reflection isolation can be adopted to enhance operation bandwidth. The receiver noise floor is set by thermal noise floor rather than the phase noise skirts of leakage signals. The receiver noise floor is set by thermal noise floor rather than the phase noise skirts of leakage signals. Reader-to-reader interference is greatly reduced by separating Tx and Rx on different bands.

In recent years, harmonic RFID systems have attracted much attention. A novel harmonic RFID transponder had been fabricated on standard CMOS which allowed broadband matching and efficient second harmonic generation over GHz bandwidth [14]. Harmonic RFID does not require data modulation to separate Tx and Rx signals and uplink carrier phase information can be readily extracted. By utilizing these harmonic carrier phases information from broadband harmonic responses, millimeter-resolution ranging had been reliably achieved in rich-scattering indoor environment [8], [17]. By embracing both frequency and spatial diversity, centimeter resolution RF imaging of tagelss objects had been reported with multiple ambient harmonic RFID tags [13]. In [15], special antenna was designed to allow third harmonic re-radiation by using nonlinearity in the RF-to-DC converter. A harmonic RFID on low-cost organic materials such as the paper substrate had been investigated in [16]. To facilitate research in harmonic RFID systems, we present Harmonic-WISP, which is the first harmonic RFID tag integrated with the open-source wireless identification and sensing platform (WISP) [18]. The tag architecture of Harmonic-WISP is shown in Fig. 8(a). The system consists of three major subsystems: broadband harmonic generation, WISP signal processing, and power routing.

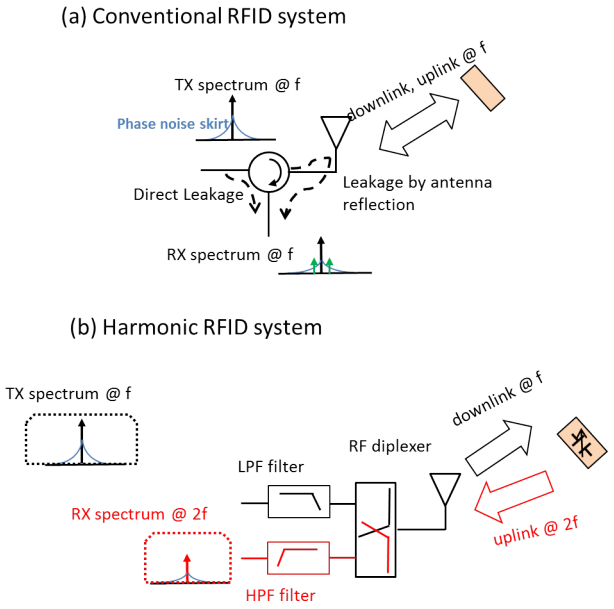

Fig. 7. System architecture comparison between conventional and harmonic RFID systems.

1) Broadband Harmonic Generation Unit: The broadband harmonic generation unit is built on nonlinear transmission lines (NLTL) which consist of periodically loaded inductors and nonlinear varactors [14]. When the signal at the fundamental frequency f is routed to NLTL, the second harmonic signal at $2f$ will be generated and propagate along NLTL. The NLTL has two terminals and one terminal is open-ended so that the harmonic signal is reflected back and then re-radiated from the tag antenna. The characteristic impedance is designed to match 50Ω so that harmonics can be efficiently re-radiated over broadband. The uplink communication is carried on $2f$ using amplitude shift keying (ASK) by turning Switch B in

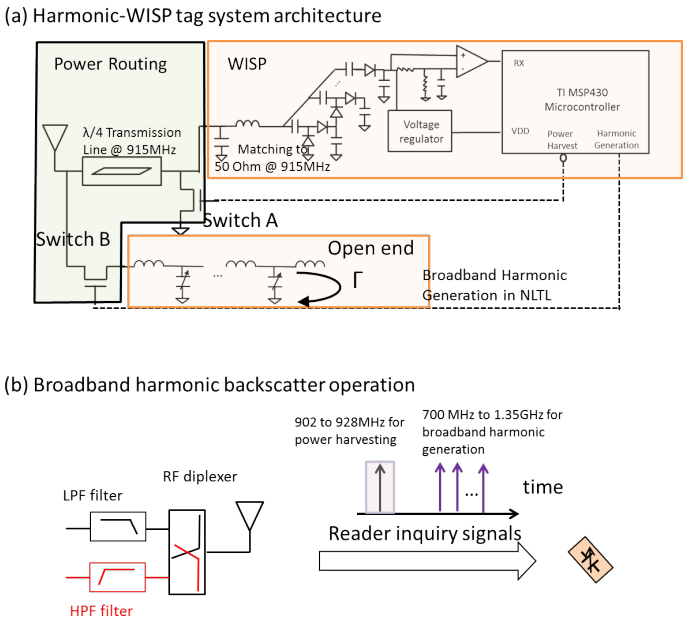

Fig. 8. (a) System architecture of the proposed Harmonic-WISP RFID tag. (b) An example of reader inquiry signal sequence in the broadband harmonic backscatter operation.

Fig. 8 on and off.

2) WISP Unit: The WISP unit is based on WISP 5.0 [18]. It performs the functions of energy harvesting, reader command decoding, computation and protocol control. A matching section in the WISP unit is needed to match the input impedance to 50Ω. This is essential for the power routing unit to work properly. Notice that unlike the harmonic generation unit, the WISP power matching is designed around 915MHz in order to achieve good efficiency in the downlink channels. An operation example of broadband Harmonic-WISP is shown in Fig. 8(b). Reader emits inquiry signal between 902 to 928MHz when the tag is in the start-up or energy harvesting mode. After the tag harvests enough energy, it can then switch to the harmonic generation mode by the power routing unit. During harmonic generation, the reader can pursue operation with broader bands by sending carrier signals from 700MHz to 1.2GHz.

3) Power Routing Unit: The difficult design in a harmonic tag lies on efficient harmonic generation in conjunction with energy harvesting. Harmonic-WISP adopts a novel power routing solution. The power routing unit consists of an antenna to receive signals from the reader, a quarter-wavelength $\lambda/4$ 50Ω meandering micro-strip line, and two RF switches. In the start-up/energy harvesting mode, both Switch A and Switch B are set to off without DC power supply, thus blocking power into NLTL. The WISP power harvesting module is matched to 50Ω and the antenna matching remains after the $\lambda/4$ microstrip line so all power is directed to energy harvesting. In the harmonic generation mode, both Switches A and B are pulled to the on state. The drain node on Switch A is grounded, and the $\lambda/4$ line acts as an impedance transformer so that a large impedance appears at the input end. Meanwhile, Switch B is also on and impedance looking into NLTL is matched at

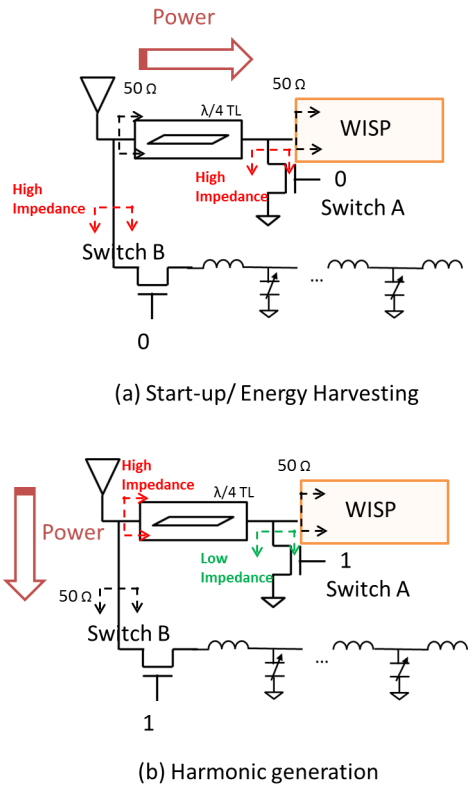

Fig. 9. Power routing in Harmonic-WISP: (a) The start-up/energy harvesting mode; (b) The harmonic generation mode.

50Ω, so all of the received power is routed to generate second harmonics efficiently. The operation of the power routing is depicted in Fig. 9.

D. Ranging Method

Assume Tx is at the fundamental frequency f_k, we utilize a dual 2-element antenna array to estimate the AoA gap G_{AoA} as discussed by Eq.(6-7) . We then apply a AoA gap thresholding. *Measurement is reliable and should be accepted*

$$G_{AoA} < {G_{AoA}}^{th} \tag{8}$$

Measurement is unreliable and should be rejected

$$G_{AoA} \geq {G_{AoA}}^{th} \tag{9}$$

The value of ${G_{AoA}}^{th}$ is empirical. If ${G_{AoA}}^{th}$ set large, one may take unreliable measurements, leading to poor ranging accuracy. If ${G_{AoA}}^{th}$ set small, one may reject measurements that is actually reliable. In our measurements, we find a value of ${G_{AoA}}^{th}$ at 30° to 40° a good number.

We apply HMFCW ranging algorithm as discussed in [8] After AoA gap thresholding, we measure phase of backscatter second harmonic signal on each carrier. For k-th second harmonic carrier, the carrier phase measured is $\theta_k \in [0, 2\pi)$. Then there is an ambiguous cycle integer n_k for measurements on k-th frequency which gives

$$d^{(k)} = \frac{\theta_k}{2\pi}\frac{\lambda_k}{2} + n_k\frac{\lambda_k}{2} \tag{10}$$

where $\lambda_k = c/f_k$ is the wavelength with c equal to the speed of light. Our goal is to correctly computes n_k within a reading range R, where

$$-R/2 < d \leq R/2 \tag{11}$$

The typical R for indoor locating is in the range of several meters. HMFCW first defines the **error tolerance** as a function of **f** and the reading range R Let $\lambda_k = c/f_k$, the error tolerance function is defined as

$$\begin{aligned} T(\mathbf{f}, R) &= \min_{\mathbf{b}=(b_1,\cdots,b_K)} \max_{1\leq k,l\leq K} \pi \frac{|\lambda_k b_k - \lambda_l b_l|}{\lambda_k + \lambda_l} \\ s.t. &\begin{cases} b_k \in \mathbf{Z}, \quad 1 \leq k \leq K \quad \sum_k b_k^2 > 0 \\ \frac{1}{2}|\lambda_k b_k| < R + \frac{1}{2}\lambda_k \end{cases} \end{aligned} \tag{12}$$

Let $\Delta\theta_k$ denote the measured phase error for k-th second harmonic frequency and $\Delta\theta_k \in [-\Delta\theta_{\max}, \Delta\theta_{\max}]$. The measured phase $\theta_k = \theta_k^{\text{ideal}} + \Delta\theta_k$, where θ_k^{ideal} is the "ideal" phase when there is no multi-path error. If

$$\Delta\theta_{\max} < T(\mathbf{f}, R) \tag{13}$$

then HMFCW can resolve cycle integers $\mathbf{n} = (n_1, n_2, \cdots, n_K)$ correctly by finding the integer vector **n** that satisfies

$$-R - \lambda_k < n_k \lambda_k \leq R \quad \forall k \tag{14}$$

and

$$\frac{2\pi|n_k\lambda_k + \frac{\theta_k}{2\pi}\lambda_k - n_l\lambda_l - \frac{\theta_l}{2\pi}\lambda_l|}{\lambda_k + \lambda_l} < T(\mathbf{f}, R) \quad \forall k, l \tag{15}$$

The ranging frequency selection $\mathbf{f} = (f_1, f_2, \cdots, f_K)$ is important. A good frequency combination should maximize the value of $T(\mathbf{f}, R)$ in Eq. (12). HMFCW maximizes phase error tolerance with low computation complexity and small number of frequencies through searching for robust frequency combination heuristically [8]. We selected five frequencies: 1710, 1740, 1798, 1874 and 2180MHz corresponding to fundamental frequencies at 855, 870, 899, 937 and 1090MHz for 3-meter searching range and achieved phase error threshold of 22°. The performance of such HMFCW ranging was shown in Fig. 3(a). By HMFCW spectrally sparse sensing, we robustly achieve average error and median error within a few millimeters even when the phase error is up to 24° and 40°, respectively. The significant difference between the RMS average error and the medianum error indicates that incidence of large error occurs relatively infrequently.

III. Experimental Evaluations

A. Harmonic-WISP prototype

To verify the effectiveness of the proposed system architecture, we prototyped Harmonic-WISP on a printed circuit board as shown in Fig. 11(a). The voltage regulator on WISP consisted of a RF to DC converter and a low-dropout (LDO) regulator as the power supply Vreg to the microcontroller MSP430. The voltage regulator Vreg was set to peak at 3.3 V. The measured peak value of Vreg and the tag received power were shown in Fig. 11(b). The second harmonic generation at different frequencies with 0dBm input was measured and

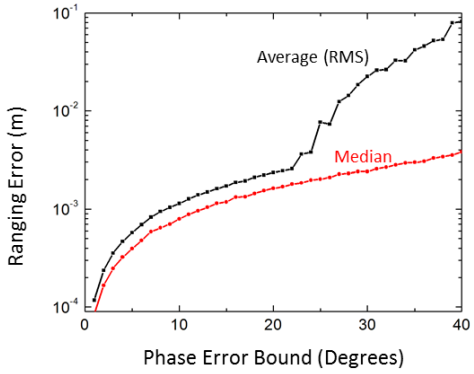

Fig. 10. HMFCW ranging performance by simulation. Phase error is uniformly distributed within $[-\Delta\theta_{max}\ ,\ \Delta\theta_{max}]$, where $\Delta\theta_{max}$ is the phase error bound.

shown in Fig. 11(c). Harmonic-WISP was able to generate second harmonic above -25dBm from 800MHz to 1100MHz (32% bandwidth). The harmonic RFID system has the noise floor set by the thermal noise, so high receiver sensitivity is enabled in comparison with the conventional RFID system. The reading range limited by reader receiving sensitivity is computed according to the measured harmonic generation characteristics in Fig. 4(c) and is shown in Fig. 11(d), where the receiver sensitivity at 4W EIRP reader inquiry power is at -110dBm, tag antenna gain at 0dBi, and reader antenna gain at 6dBi. Harmonic-WISP relies on the reader signal from 902MHz to 928MHz to power up the digital circuits. The tag sensitivity limited reading range on 915MHz is also marked in Fig. 4(d) which is 4.6 meters. At such range we could pursue a broadband harmonic operating frequency range from 700MHz to 1200MHz (53% bandwidth). To demonstrate the Harmonic-WISP tag data waveforms, decoded reader commands (100Kb/s) from ASK-modulated 915MHz carriers in the downlink measured by oscilloscope were shown in Fig. 11(e). The uplink tag second harmonic signals with ASK modulation (150Kb/s) on 1.83GHz were also captured by oscilloscope and shown in Fig. 11(f). The measured spectrum of the uplink tag signal for ASK off and on were shown in Figs. 11(g, h), respectively, at 0dBm input with f=915MHz. The Smith Chart of the measured input impedance at both energy harvesting and harmonic generation states is shown in Fig. 12. Although with small deviation in both inductive and capacitive directions, the overall matching across the operational bandwidth is satisfactory. By our power routing strategy, we were able to fully utilize the received power in both states.

B. Indoor multi-paths effect on low-directivity antenna

We setup an experiment to understand the multi-paths effect in a typical indoor environment. The setup was shown in Fig. 13 (b) with coordinates shown in Fig. 13(a). Dual arrays of 2-element omni-directional antennas (each array contains

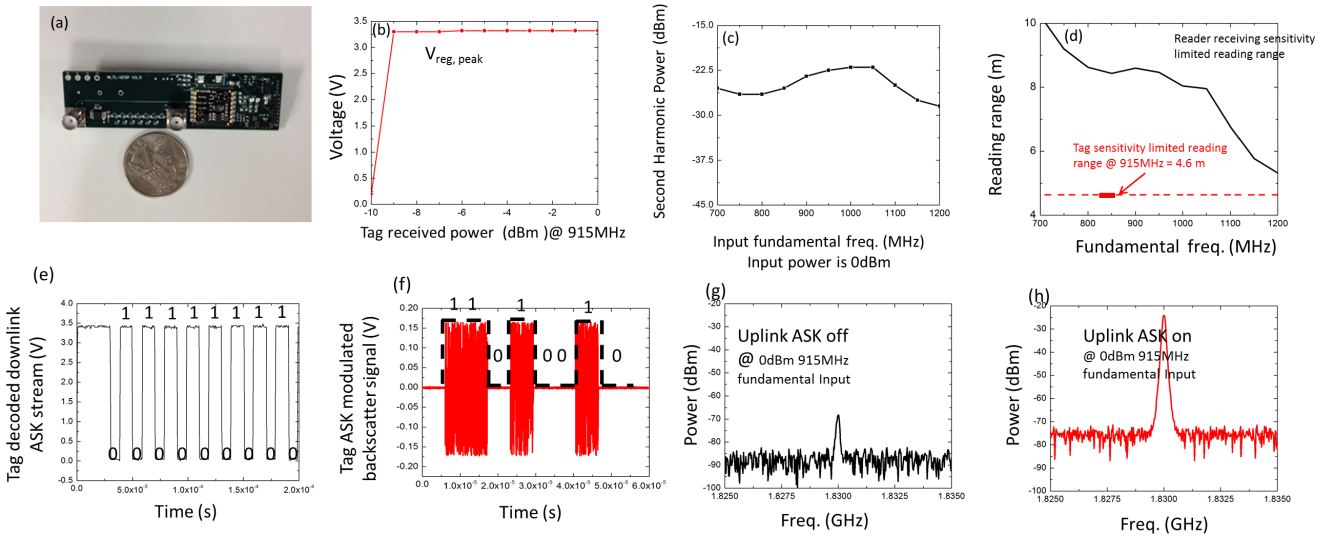

Fig. 11. (a) Photo of the Harmonic-WISP prototype; (b) Measured Vreg,peak v.s. the tag received power at 915MHz; (c) Measured harmonic generation over broadband; (d) Computed range limited by reader sensitivity set at -110dBm from measured results in (c).

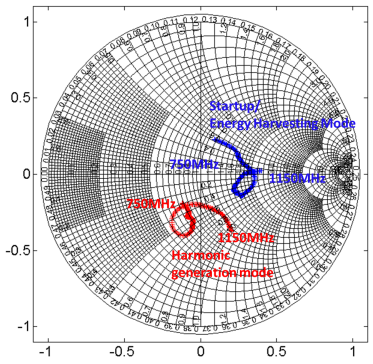

Fig. 12. Measured input reflection coefficient plotted in Smith Chart for energy harvesting mode and harmonic generation mode.

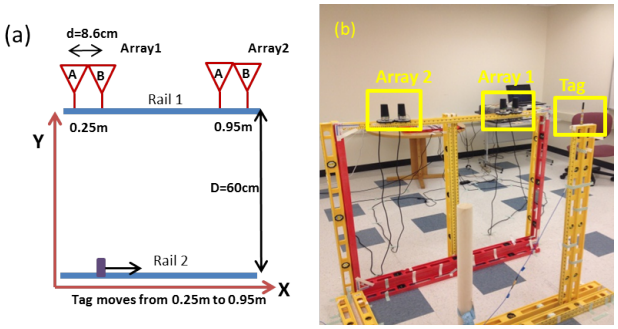

Fig. 13. Experiment setup to help understand indoor multi-paths effect:(a)coordinate; (b)photo of the setup.

antenna A and B) on the reader were Taoglas Shockwave Series of length at 8cm and diameter at 4cm for their easy and stable plug in mounting, which covered frequency band from 700MHz to 2.7GHz and offered peak and average gain of 0.5dBi and -1.9 dBi respectively in the band of our interests. The centers of the two antennas in the same array were separated by 8.6cm and the centers of the two arrays were by 70cm. The tag was mounted on a rail, sliding from 0.25m to 0.95m. The distance from the tag rail to the antenna rail was 0.6m. Because in our approach only uplink errors affect ranging, in order to calibrate the phase deviation in the uplink, we fed the fundamental frequency through an attenuator to the tag so that the input carrier phase in the downlink was kept fixed when the tag slid along the rail. In Fig. 14, the measured signal amplitude ratio between the two antenna elements within each receiving array oscillated between 0.4 and 2.4, which clearly showed the strong multi-path effect. In an ideal situation without multi-paths, the ratio should be constant at 1. In Fig. 15, the measured phase error in the uplink was measured by fixing the phase value of the downlink with a cable feeding. The 2-element array can help reducing the phase error. However, the error can still be as large as 30○. But fortunately, when the LoS is clear, such an error can usually be handled with the HMFCW ranging discussed in the previous chapter.

C. *Effect of dense multi-path*

We need to reject unreliable measurements when multi-paths become stronger than LoS, we study the dense multi-path effect on AoA gap G_{AoA} by creating a much richer scattering environment with an aluminum foil curtain (AC). We showed that the extracted AoA gaps were an effective measure of the multi-path dominance as shown in Fig. 17. The mean, median and maximum AoA gaps were shown in Table I. By setting threshold for AoA gaps, further control of quality in severe multi-paths can be applied.

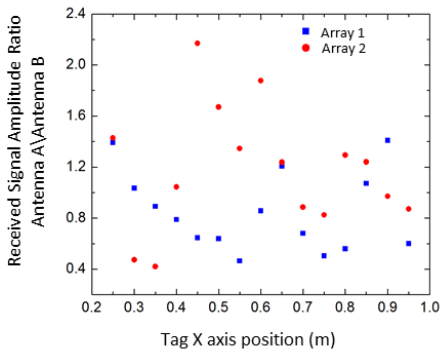

Fig. 14. Received signal amplitude ratio between antennas A and B within each array at 1798MHz to indicate the effect of indoor multi-paths.

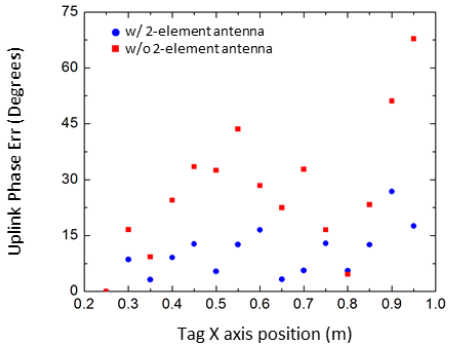

Fig. 15. Received signal phase error under indoor multi-paths

Fig. 16. Received signal phase error under indoor multi-paths

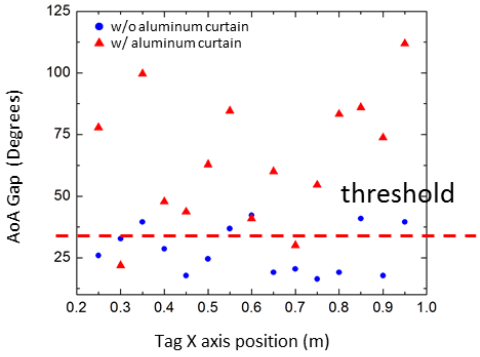

Fig. 17. Received signal phase error under indoor multi-paths

D. Ranging experiment

The ranging experiment setup is shown in Fig. 18. We used the tag shown in Fig. 11 and a PCB reader which was specially designed to harmonic transceiving. The block diagram of the reader is shown in Fig. 19. The reader supports 1 Tx antenna and 2 2-element antenna arrays for ranging purpose. The received harmonic signal is directly converted to the baseband and sampled by the analog to digital converter (ADC) on the Cortex M4 STM 32-bit micro-controller. To allow coherent phase detection, the local oscillator (LO) signal to the mixer is coupled from harmonics of the power amplifier in Tx. The reader employs variable gain amplification in both Tx and Rx to enhance the dynamic range. Our reader can communicate to a host computer by a Bluetooth module. The reader achieve 60dB gain from 1400MHz to 2400MHz for received harmonic signal. The measured Tx output power is 29dBm from 700MHz to 1100MHz. When Tx is at maximum power, the measured interference signal to the receiving is below -90dBm. With the implemented reader, we can pursue a broadband operation over 45% bandwidth.

1) Ranging in the presence of an obstacle: To show how we can utilize AoA gap to reject unreliable measurements. We conducted an experiment as shown in Fig. 20. A bottled can of 20cm height full of water is put in the center of the table as a obstacle. During the experiment, the tag is put a different locations (step #1 to #28) around the can. The direct ranging measurement results and AoA gap are plotted in Fig. 21. Due to the presence of metal can obstacle, not every measurement is reliable and should be accepted. But exploiting coherence bandwidth concept, the AoA gap is a good measure of the reliability of the ranging measurements. Unreliable measurements always correspond to large AoA gap. After applying AoA thresholding at $40°$, we can reject all unreliable measurements while keep 90% of the reliable measurements.

TABLE I
AOA GAP WITH AND WITHOUT ALUMINUM CURTAIN (AC)

AoA Gap	Mean(RMS)	Median	Maximum
With AC	69.8°	62.7°	112°
Without AC	29.6°	25.9°	42.2°

IV. CONCLUSION

The conclusion goes here.

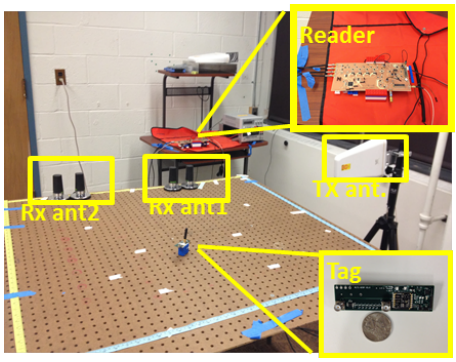

Fig. 18. Ranging experiment setup.

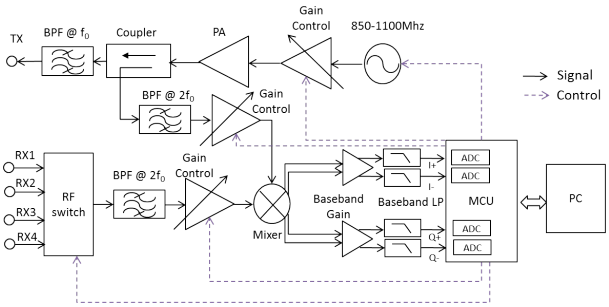

Fig. 19. Simplified reader diagram.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

The authors would like to thank...

References

[1] L. M. Ni, Y. Liu, Y. C. Lau and A. P. Patil. Landmarc: indoor location sensing using active RFID. In *Proc. IEEE PERCOM*, 2003.
[2] C. Xu, et al. Improving rf-based device-free passive localization in cluttered indoor environment through probabilistic classification methods. In *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2012.
[3] P.V. Nikitin and K. V. S Rao. Theory and measurement of backscattering from RFID tags. *IEEE Antennas and Propagation Magazine*, vol. 48, no. 6, pp. 212-218, Dec. 2008.
[4] P. Nikitin, R. Martinez, S. Ramanurthy, H. Leland, G. Spiess and K. V. R. Rao. Phase based spatial identification of UHF RFID tags. In *Proc. IEEE Int. Conf. RFID*, 2010.
[5] R. Miesen, et al. Holographic localization of passive UHF RFID transponders. In *Proc. IEEE Int. Conf. RFID*, 2011.
[6] L. Yang, Y. Chen, X. Li, C. Xiao, M. Li and Y. Liu. Tagoram: Real-time tracking of mobile RFID tags to high precision using cots devices. In *ACM MOBICOM*, 2014.
[7] L. Liu, et al. Anchor-free backscatter positioning for RFID tags with high accuracy. In *IEEE INFOCOM*, 2014.
[8] Y. Ma and E. C. Kan. Accurate Indoor Ranging by Broadband Harmonic Generation in Passive NLTL Backscatter Tags. *IEEE Tran. Microw. Theory Tech.*, vol. 62, no. 5, pp. 1249-1261, May 2014.
[9] P.N. Betjes. An algorithm for automated phase center determination and its implementation. In *Proc. AMTA Conf.*, 2007.

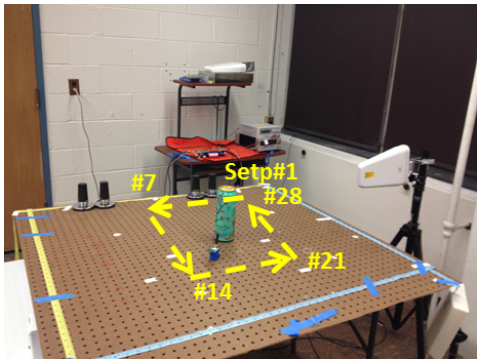

Fig. 20. Ranging in the presence of an obstacle.

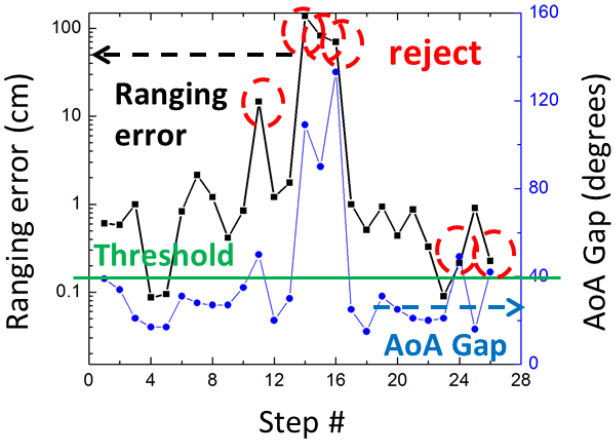

Fig. 21. Ranging with obstacles: direct ranging measurements and AoA gap.

[10] J. Xiong and K. Jamieson. Arraytrack: A fine-grained indoor location system. In *USENIX NSDI*, 2013.
[11] N. Mandayam. Basics of small scale fading: towards choice of PHY,[Online].Available:http://www.winlab.rutgers.edu/ narayan/Course /WSID/wsid-lec1c.ppt.
[12] J. R. Riley, et al. Tracking bees with harmonic radar. *Nature*, 1996.
[13] Y. Ma and E. C. Kan. Ubiquitous tagless object locating with ambient harmonic tags. In *IEEE INFOCOM*, 2016.
[14] F. Yu, K. G. Lyon and E. C. Kan. A novel passive RFID transponder using harmonic generation of nonlinear transmission lines. *IEEE Tran. Microw. Theory Tech.*, vol. 58, no. 12, pp. 4121-4127, Dec 2010.
[15] G. A. Vera, Y. Duroc and S. Tedjini. Third harmonic exploitation in passive UHF RFID. *IEEE Tran. Microw. Theory Tech.*, vol. 63, no. 9, pp. 2991-3004, Sept. 2015.
[16] M. Virili, F. Lolli, F. Alimenti, P. Mezzanotte, M. Dionigi and L. Roselli A way towards an organic frequency doubler for harmonic RFID applications. In *Proc. IEEE Int. Conf. RFID-TA*, pp. 198-202, Nov. 2012.
[17] Y. Ma and E. C. Kan. Passive ranging by low directivity antenna with quality estimate. In *IEEE MTT-S International Microwave Symposium (IMS)*, May. 2015.
[18] Wisp 5 firmware repository. Available: http://www.github.com/wisp/

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.