Backscatter Signal Blind Detection and Processing for UHF RFID Localization System

Liangbo Xie(✉), Xin Xiong, Qingfei Kang, and Zengshan Tian

School of Communications and Information Engineering,
Chongqing University of Posts and Telecommunications, Chongqing, China
xielb@cqupt.edu.cn

Abstract. Radio frequency identification (RFID) is widely used in many fields and more recently, there has been a continuously growing interest in RFID-based indoor localization. Compared to RSS and AOA based RFID localization algorithms, the carrier phase-based ultra-wideband localization algorithm has better performance. To implement 3D indoor localization with this method, carrier phase of multiple receivers must be obtained in different frequencies. However, existing RFID systems do not meet the requirement. Therefore, this paper proposes a system consisting of a software-defined radio with custom-made RF front-end (SRCF) and ImpinjR420 COTS reader (R420), which can realize data communication between R420 and tags, and achieve the channel coefficient estimation. Moreover, an algorithm is proposed to detect the EPC data backscatter by the tag without any prior information. Experiment results show that the proposed algorithm can correctly decode the EPC data and obtain the channel coefficient information.

Keywords: RFID · SDR · Indoor localization · Signal detection · Carrier phase

1 Introduction

In recent years, RFID-based localization technology is getting more and more attention, especially in the field of virtual reality and factory automation [1], such as warehouse cargo location management, posture detection [2] and other fields. Received signal strength (RSS) [3], angle of arrival (AOA) [4] and carrier phase-based ultra-wideband localization [5], are the most popular RFID localization methods, and carrier phase-based ultra-wideband localization method has better performance than RSS and AOA. The key to carrier phase-based algorithm is how to obtain carrier phase of multiple receivers. Therefore, multiple receivers are needed to receive the data backscattered by tag, as shown in Fig. 1.

M. Jia et al. (Eds.): WiSATS 2019, LNICST 280, pp. 151–159, 2019.
https://doi.org/10.1007/978-3-030-19153-5_14

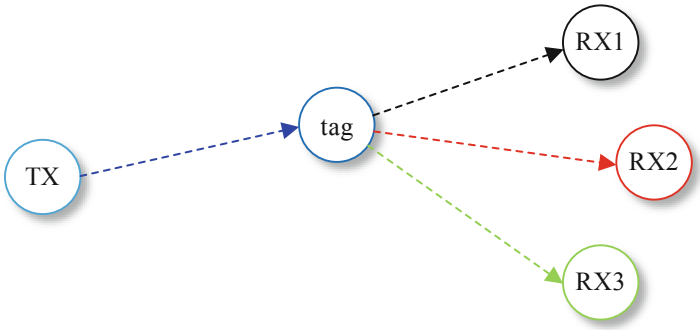

Fig. 1. System structure which is suitable for carrier phase-based ultra-wideband localization algorithm.

At present, we can easily to communicate with tags use a Commercial-Off-The-Shelf (COTS) RFID reader (R420), but the original data cannot be directly obtained and cannot work in ultra-wideband. On the other hand, although physical layer communication between software-defined radio (SDR) and tag at different frequency is implemented [6], but the SDR transmission power is low, and cannot implement a transmitter, multiple receivers, which is not suitable for carrier phase-based localization algorithm.

To solve this problem, this paper proposes a system that uses a R420 to communicate with tag while an SDR with custom-made RF front-end (SRCF) is used to send carrier and receive data backscattered by the tag. When transmitting a high-power signal in ISM and a low-power signal outside ISM the tag is powered up and reflects data both frequencies simultaneously [7]. Thus, if the number of SRCF receivers is enough, the carrier phase of multiple links can be obtained.

The rest of this paper is organized as follows. Section 2 presents the system model when the tag uses FM0 encoding. Section 3 offers signal detection and carrier phase estimation. Section 4 is the experimental results.

2 System Model

When a tag is powered up by R420 at frequency f_1, an SRCF is used to transmit the carrier wave (CW) at frequency f_2. The tag modulates its information on both f_1 and f_2, then reflects, as shown in Fig. 2. In this way, the SRCF receiving antenna will receive four types of signals, directly by SRCF and R420. Due to in different frequencies, we can filter out the signal from the R420 with the frequency f_1, and only the signal with the frequency f_2 is left, but this will leave a small number of harmonic components. The complex baseband equivalent of the received signal at the SDR is [8]:

$$y(t) = [m_{dc} + m_{\text{mod}} x(t)] e^{+j2\pi\Delta ft} + z(t) + n(t) \tag{1}$$

Where the DC component m_{dc} is caused by CW and an unmodulated component scattered back by the tag; the modulated m_{mod} component depends on the channel coefficients of the SRCF transmitting antenna-to-tag and tag-to-SRCF receiving antenna links, the tag antenna reflection coefficients, the tag scattering efficiency and the carrier transmitting power, which the channel coefficients are mainly composed of two parts: amplitude and phase. $x(t)$ is a binary real-valued tag scattered waveform; $z(t)$ is the residual harmonic component of the signal with frequency f_1. Δf is the carrier frequency offset (CFO) between CW transmission and SRCF reception chain. $n(t)$ is the complex thermal (receiver) Gaussian noise. The system of this work is based on a local oscillator for both transmission and reception, so $\Delta f = 0$; Because the difference between f_1 and f_2 is much larger than the frequency of returning data from the tag, thus $z(t) = 0$.

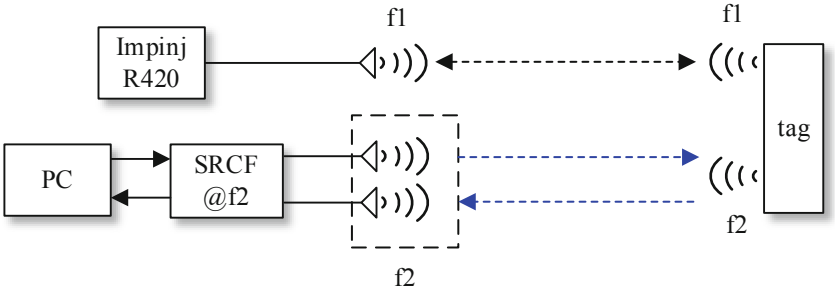

Fig. 2. System structure

3 Signal Detection and Carrier Phase Estimation

3.1 SDR Receive Signal Representation

According to Gen2 [9], in FM0 encoding, level transitions always occur on the bit boundaries. In addition, a level transitions will occur in the middle of the symbol 0, and the symbol 1 will not. Thus, there are 4 waveforms that can be generated per symbol data, as shown in Fig. 3.

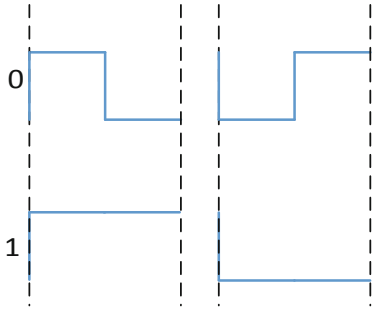

Fig. 3. FM0 symbols

If the starting position of the bit in the received waveform is found and the starting position is shifted back by *T/2*, where *T* is the bit (symbol) period, only two possible pulse shapes can be generated (instead of four) [10], shown in Fig. 4.

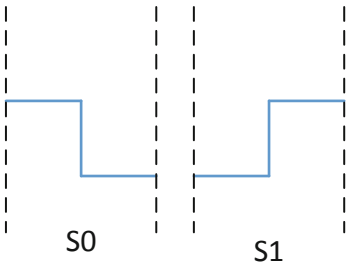

Fig. 4. Tow possible pulse shapes

Finally, differential decoding can be used to detect a transmitted bit.

Assume that the SRCF receiver accurately detects the bit signal reflected by the tag and removes m_{dc} from the received waveform (zero-offset FM0). The received digital signal should be expressed:

$$y[k] = y(kTs) + n(kTs) = hx[k] + n[k], x[k] = \sum_{n=0}^{N} S_{d(n)}[k - nL - \tau] \tag{2}$$

where $n[k]$ is the sampling of Gaussian white noise; *Ts* represents the sampling interval, *T* represents the symbol period, τ represents the delay before tag starts transmitting its information, $L = \frac{T}{Ts}$ represents the number of sampling points of each symbol. $S_{d(n)}$ represents two forms of received waveform:

$$S_0[k] = \begin{cases} 1, if\ 0 \le k < \dfrac{L}{2} \\ 0, if\ \dfrac{L}{2} \le k < L \end{cases}, S_1[k] = \begin{cases} 0, if\ 0 \le k < \dfrac{L}{2} \\ 1, if\ \dfrac{L}{2} \le k < L \end{cases} \tag{3}$$

3.2 Signal Detection and DC Offset

Since the SDR is always transmitting the carrier wave, it does not know when the received data contains the bit sent by the tag. Therefore, the SRCF needs to detect in real time whether the received data contains bit sequence reflected by the tag. Due to the characteristics of FM0 coding, the amplitude spectrum distribution is similar to the pulse signal with a period *T* of *T/2*. By analyzing the amplitude spectrum of the received waveform, it can be determined whether the tag modulation information is included [11].

The double-sided band amplitude spectrum of a pulse signal with a period T of $T/2$ can be expressed as:

$$|F_n| = \frac{A}{2}\left|Sa(\frac{nw_0T}{2})\right| \tag{4}$$

where $w_0 = \frac{2\pi}{T}$, $F_{\pm 1}$ represents the amplitude of the fundamental component when $n = \pm 1$.

Supposing the SDR receives a sequence $y(n)$ of length M, by performing an N-point FFT transformation on $y(n)$, transformed sequence Y(k) can be expressed as:

$$Y(k) = FFT[y(n)]_N \tag{5}$$

Because the characteristics of FFT, if the complex sampling rate of the signal is B Hz, the frequency bandwidth represented by $Y(k)$ after the FFT of the N point is B Hz.

By calculating the ratio of the fundamental frequency w_0 and B, the position of the pulse signal in $Y(k)$ can be determined.

$$k_1 = N/2 + k_w, k_2 = N/2 - k_w, k_w = \left\lfloor \frac{w_0 N}{B} \right\rfloor \tag{6}$$

In the double-sided band amplitude spectrum, k_1, k_2 are symmetric about the midpoint $N/2$. By accumulate the $Y(k)$ near these two positions and the entire $Y(k)$, we can obtain:

$$P_1 = \sum_{n=k_1-a}^{k_1+a} Y(k) + \sum_{n=k_2-a}^{k_2+a} Y(k), P_2 = \sum_{n=0}^{N} Y(k) \tag{7}$$

where a is the summation width. When the received signal contains tag-modulated information, the ratio of P_1 and P_2 should be significantly larger than not included.

Once the tag-modulated bit sequence in the received signal is detected, the bit starting point can be roughly determined with the above method, and the average value of the data point of a certain length before the starting point is regarded as m_{mod}, and then m_{mod} will be removed from the entire piece of data by subtracting this value.

3.3 Synchronization and Phase Estimation

After the previous work is completed, we need to synchronize the receiving bit with a known preamble. The offset of the bit start point and the received data start point can be found by the following equation.

$$\tau = \arg\max_{\tau \in \{0,\ldots,L\}} \left| \sum_{n=0}^{N_p} s_p[n] y[\tau + n] \right| \tag{8}$$

where the s_p is a known 6 symbol lengths preamble, N_p is the number of samples in the preamble.

The channel coefficient h can be estimated by solving a least squares problem:

$$\hat{h} = \arg\min \sum_{k=\tau}^{\tau+N_p-1} \left| y[k] - hs_p[k-\tau] \right|^2 \tag{9}$$

$$= \frac{\sum_{k=\tau}^{\tau+N_p-1} y[k]s_p[k-\tau]}{\left\| s_p \right\|^2} \left(\frac{\pi}{2} - \theta \right) \tag{10}$$

where $\| \bullet \|$ denotes the Euclidean norm.

After the channel coefficient h is known, the phase difference caused by the propagation of the CW in the channel can be calculated as [8].

$$\varphi = angle(h) \tag{10}$$

where φ is a complex value.

When correlation synchronization is completed, a bit sequence with known starting point can be obtained. Through moving the bit start point back by *T/2*, the data can be decoded by differential decoding.

$$b(n) = d(n-1) \otimes d(n), n = 1, \ldots, N \tag{11}$$

when the received signal waveform is S_0, $d(n) = 0$, when it is S_1, $d(n) = 1$. $b(n)$ is the decoded bit. operation $\oplus \leftarrow$ denotes modulo-2 addition (xor).

4 Experimental Results

The experimental platform is shown in Fig. 5, which contains three antennas, a commercial tag, a SRCF and a R420. The backscatter parameters of the tag are set to FM0 encoding with a reverse link rate of 400K by R420. At the SRCF receiver, 4M complex sampling rate is set. Therefore, the sampling point of each symbol is 10. According to Gen2 protocol, the data modulated by the tag including RN16 and EPC,

Fig. 5. Experimental setup.

wherein the sequence length of RN16 is 22, and the sequence length of EPC is 135. We extract phase information from the EPC at the SRCF receiver because EPC is longer than RN16 and has CRC-16 check.

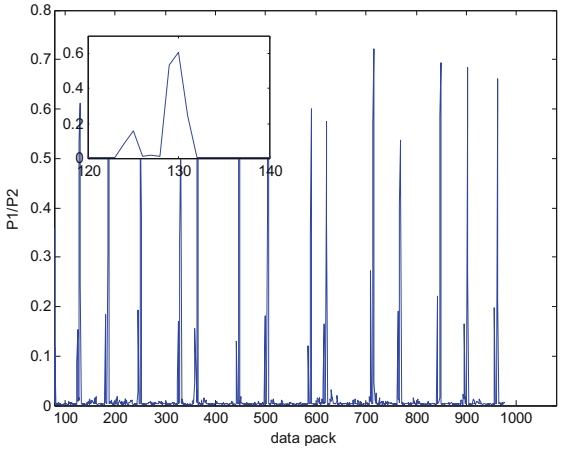

Fig. 6. The P1/P2 of different data pack.

Figure 6 shows the value of P1/P2 under the following experimental conditions, (1) treat 512 samples as a data packet, (2) the SRCF signal transmission power was 17.2 dBm and the R420 signal transmission power was 25 dBm, (3) the distance between tag and SRCF receiver, about 2 meters away. In Fig. 6 a larger peak and a smaller peak can be found in the round frame, which correspond to EPC and RN16, respectively. Because the EPC corresponds to a wider peak width and a larger amplitude, we can easily distinguish between EPC and RN16.

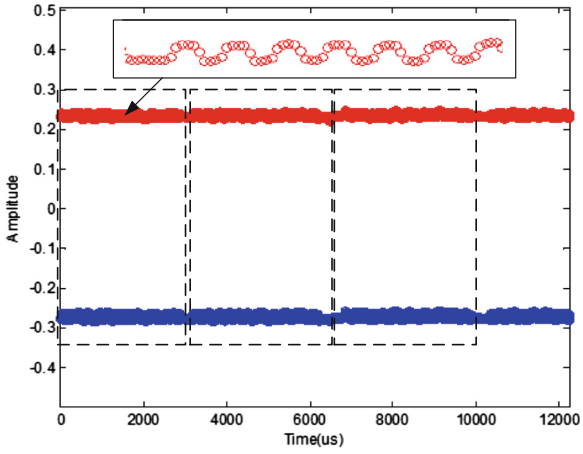

Fig. 7. The dotted box is the EPC sequence detected by the gate block.

Figure 7 shows the data detected by SRCF, which contains EPC. Useful information can be obtained by processing these data.

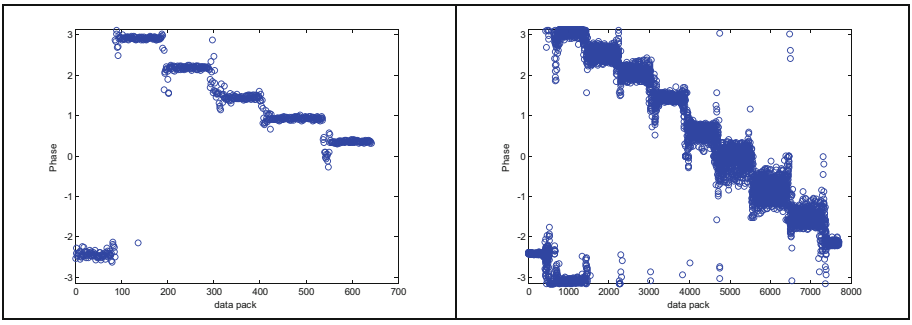

Fig. 8. The *phase* value changes with distance.

In order to validate the correctness of the estimated phase, we move the tag two centimeters at each time, and get multiple carrier phases for each distance. As shown in Fig. 8, the carrier phase changes by about 0.75 for each change of distance, which is in line with the theory. Thus, the proposed channel coefficient algorithm can extract the phase correctly.

5 Conclusion

Existing RFID systems do not meet the requirements of the carrier phase-based ultra-wideband localization algorithm. This paper presents a system consisting of a SRCF and R420, which can be easily extended to one transmitter multiple receivers structures. A channel coefficient estimation algorithm is proposed, which can extract the phase and decode the EPC correctly. Thus, the proposed system is suitable for carrier phase-based ultra-wideband localization algorithm.

Acknowledgement. This work was supported partly by the Scientific and Technological Research Foundation of Chongqing Municipal Education Commission under grant KJ1704083, the National Natural Science Foundation of China under 61704015, the Fundamental and Frontier Research Project of Chongqing under grant cstc2017jcyjAX0380.

References

1. Wang, Y., Man, K.L., Maunder, R.G., et al.: A flexible software defined radio-based UHF RFID reader based on the USRP and LabView. In: SoC Design Conference, pp. 217–218 (2016)
2. Wang, L., Gu, T., Tao, X., et al.: Toward a wearable RFID system for real-time activity recognition using radio patterns. IEEE Trans. Mob. Comput. **16**(1), 228–242 (2017)

3. Ni, L.M., Liu, Y., Lau, Y.C., et al.: LANDMARC indoor location sensing using active RFID. Wirel. Netw. **10**(6), 701–710 (2004)
4. Azzouzi, S., Cremer, M., Dettmar, U., et al.: New measurement results for the localization of UHF RFID transponders using an Angle of Arrival (AoA) approach. In: IEEE International Conference on RFID, pp. 91–97. IEEE (2011)
5. Ma, Y., Selby, N., Adib, F.: Minding the billions: ultra-wideband localization for deployed RFID tags. In: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, pp. 248–260. ACM (2017)
6. Buettner, M., Wetherall, D.: A software radio-based UHF RFID reader for PHY/MAC experimentation. In: IEEE International Conference on RFID, pp. 134–141. IEEE (2011)
7. Kargas, N., Mavromatis, F., Bletsas, A.: Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID. Wirel. Commun. Lett. **4**(6), 617–620 (2015)
8. Kimionis, J., Bletsas, A., Sahalos, J.N.: Increased range bistatic scatter radio. IEEE Trans. Commun. **62**(3), 1091–1104 (2014)
9. EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHZ–960 MHZ, version 2.0.1, EPC Global, Wynantskill, NY, USA (2015)
10. Bletsas, A., Kimionis, J., Dimitriou, A.G., et al.: Single-antenna coherent detection of collided FM0 RFID signals. IEEE Trans. Commun. **60**(3), 756–766 (2012)
11. Joo, T.H., Oppenheim, A.V.: Effects of FFT coefficient quantization on sinusoidal signal detection. In: International Conference on Acoustics, Speech, and Signal Processing, vol. 3, pp. 1818–1821. IEEE (2002)