Wirelessly Retrieving Phase and RSSI of UHF RFID using Commodity SDR Sniffer

Shuai Yang, Richard Penty and Michael Crisp
Department of Engineering
University of Cambridge
Cambridge, United Kingdom

***Abstract*—This paper demonstrates the retrieval of relative phase and RSSI from UHF RFID tag responses using a non-coherent low-cost commodity software-defined radio sniffer. Two common scenarios have been considered: (i) when the tag is stationary and (2) when the tag is moving. The retrieved results have been verified by a commercial RFID reader. Overall, the standard deviations in phase and RSSI estimations in the two cases are up to 8.1° and 0.61 dB respectively. In addition, the phase ambiguity has been increased to 360° by taking the sign of the tag data into account. The approach will enable a range of SIMO approaches to tag localisation using existing RFID readers and multiple sniffers.**

Keywords—UHF RFID; Software Defined Radio (SDR); MIMO; Phase estimation; Localisation.

I. INTRODUCTION

Over the past decade, Radio Frequency Identification (UHF RFID) systems with the ability to provide some localisation or motion detection have attracted intensive interests from both industry and academia. Conventional localisation algorithms are based on detecting received signal strengths (RSSIs) from a tag at a number of spatially distributed antennas. However, the approach becomes unreliable in complicated propagation environments (e.g. indoor) since RSSI is easily affected by multipath fading. In addition, RSSI could also be affected by the properties of the tagged object and the incident power on the tag [1]. Compared to RSSI, phase from a backscattered tag is less affected by cluttering and multipath environments [1-2]. In recent years, different techniques based on phase-of-arrival (PoA) [2], phase-difference-of-arrival (PDoA) [1], and inverse synthetic aperture radar (ISAR, a technique that combines PoA and PDoA) [3] have been developed and achieved much better localisation accuracies on the order of centimetre levels. Due to the challenges around precise localisation, many applications of RFID make do with portals where tags are read as they pass through a narrow opening and allowing location to be inferred as one side of the portal or the other. However, this approach still presents problems detecting the direction of movement and separating tags which have moved through the portal from those which have passed close by. Again, phase information can be used to assist in this application.

Most commercial RFID readers can report both RSSI and phase measurements (with an ambiguity of 180°). Phase is measured relative to the transmitted carrier oscillator. However, the ambiguity means that there are countless two-way paths from the reader transmitter to the receiver via the tag that could result in the measured phase. In order to provide useful information, a number of phase measurements must be taken, either at different antenna locations, different tag positions as a tag moves, with different carrier frequencies [2-3], or a combination of the three. However, this concept is contradictory to what most commercial RFID readers can achieve since a single transceiver is normally time division multiplexed (TDM) across a number of antennas, so only a single phase measurement can be performed on each tag read. As a result, the tag throughput will be reduced as the number of receive antennas or required frequencies increases.

In this paper, we demonstrate a semi-coherent sniffer such that phase and RSSI of a UHF RFID tag can be retrieved by a low-cost, commodity software-defined radio (SDR) via sniffing the reader-tag communications with no external reference signal. Previous sniffer systems have been incoherent due to use of a different reference oscillator in the RFID reader and sniffer, with the objective to only analyse the protocol [4-10]. We exploit the reader signal which is also detected at the sniffer to allow measurement of the phase of the tag signal relative to the reader carrier. Since the phase delay between the reader and sniffer will be fixed if both are in fixed locations, the resulting relative phase will be a function of the tag position.

The SDR itself has an FPGA and an ARM CPU on board and with some further efforts on software development the tag IDs, phases and RSSIs over time can be acquired and uploaded wirelessly to a central database for further processing. By listening to the same reader-tag communications, a number of distributed SDR sniffers could cooperate and provide phase and RSSI information of tags simultaneously from multiple locations, effectively converting a conventional single-input single-output (SISO) RFID system to a wireless single-input multiple-output (SIMO) RFID system. Since no TDM is used, the throughput of tags is not compromised. The lack of required external reference signal results in an easily deployed system.

The rest of the paper is organised as follows. An overview of SDR and its RFID related studies are presented in Section II. Methods to extract the RSSI and phase information from the demodulated baseband IQ signals are introduced in Section III. Section IV details different test scenarios and presents the test results and analyses. Finally, conclusions are drawn in Section V.

II. SOFTWARE-DEFINED RADIO AND RELATED WORK

An SDR is a flexible radio platform which allows digitised in-phase (I) and quadrature (Q) signals to be recovered from an RF carrier for further processing. Much of the radio functionality can be defined and implemented in digital logic and software processing of the IQ samples. The technology allows users to develop various functionalities on a host PC where debugging and visualisation are much easier.

The idea of combining SDR and UHF RFID technologies is not new. The early work carried out by Buettner and Wetherall [4] built the foundation for most SDR-based RFID related research. In [4], the authors developed a complete bistatic RFID reader based on the use of Universal Software Radio Peripheral (USRP) hardware and software developed using the open-source GNU Radio framework. The prototype can read commercial Gen2 RFID tags and offers users control over the PHY and MAC layers of the protocol. In [5] an upgraded SDR-based RFID reader was developed to evaluate the performance of commercial passive tags in terms of sensitivity and differential radar cross-section. Authors in [6] borrowed and modified some GNU radio blocks from [4] and built a fully coherent reader using the USRP2 hardware. Recently the GNU Radio blocks developed by [3] have been implemented on a much cheaper SDR platform [7]. Although the aforementioned SDR-based RFID readers are Gen2 compliant, performing signal generation, modulation, demodulation and processing all in software at the host PC significantly increase system latency compared to conventional hardware transceivers. To date, the backscatter link frequency (BLF) of most SDR based RFID readers has been limited to 40 kHz to meet the strict timing requirements set by the Gen2 protocol.

Using an SDR to monitor the Gen2 traffic was proposed and demonstrated in [8] and [9]. Unlike a full SDR-based reader which requires a fast Tx/Rx turnaround time to meet the timing requirements set by the protocol, a "Gen2 listener" is a receive-only device and only requires the sample rate of the analog-to-digital converter (ADC) to be great enough to ensure all reader and tag packets can be correctly decoded. The platforms developed by the studies provided cheaper alternatives to expensive signal analysers and allowed users to verify the RFID system performances and protocol operation in different operating conditions.

The concept of using a single reader transmitter and multiple Gen2 listeners for tag localisation and navigation was introduced in [10]. We further develop the idea to allow coherent detection such that both phase and RSSI of a tag can be extracted by an SDR. In this work, we use an Aldam PlutoSDR to carry out the feasibility study. The low-cost SDR supports two 12-bit ADCs and can measure analogue RF signals from 325 MHz to 3.8 GHz at a sample rate up to 61.44 MS/s. In addition, it has a Xilinx Zynq Z-7010 FPGA and an ARM CPU onboard, allowing users to write and run a custom firmware directly on it. An Impinj Speedway R420 reader is used to interrogate the tag. The reader supports multiple link profiles, but the Maximum Throughput Mode is selected for demonstrations. The mode supports a reader-to-tag link data rate of 48 kbps and a tag-to-reader link frequency of 436 kHz. The sample rate of the PlutoSDR is therefore sufficient to ensure any tag packet can be correctly decoded.

III. PHASE AND RSSI EXTRACTIONS

Transmitter(s) and receiver(s) of most commercial RFID readers share the same local oscillator (LO) and hence can perform a fully coherent detection to measure both a tag's backscattered power and phase. At the receiver, the complex demodulated voltage comprises (i) the leakage voltage from the transmitter to the receiver, (ii) the scattered voltage from the surrounding environment, and (iii) the backscattered voltages from a tag at different modulation states [1]. Due to (i) and (ii), the received I and Q signals will have some DC components. In addition, the tag backscattered packets

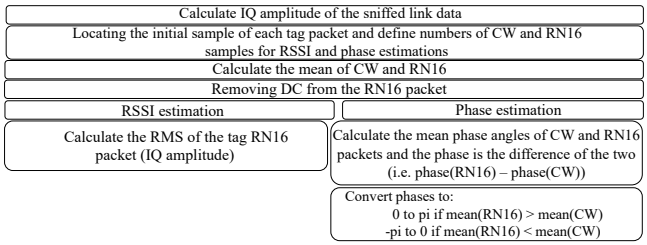

Fig. 1 Flowchart of tag RSSI and phase estimations.

contain both static and modulated components, and thus will also result in some DC, but the contribution is not as strong as the ones caused by (i) and (ii), since the received tag signal strength is usually much weaker. When the DC components in the IQ signals are removed, the remaining AC components can be used to calculate the RSSI and phase of a tag by [1]:

$$RSSI = \frac{{I_{ac}}^2 + {Q_{ac}}^2}{Z_0} \quad (1)$$

$$\varphi = tan^{-1}\left(\frac{Q_{ac}}{I_{ac}}\right) \quad (2)$$

where Z_0 is the input impedance of the receiver.

In a sniffer system, it is likely that there will be a frequency mismatch between the transmitter and the receiver (due to the use of different LO's), in addition to distortions to the IQ signals (see Fig. 2 (a)), an extra (time-varying) phase term will be introduced to the complex IQ data and hence to the calculated phase of the tag. The case will be more complicated if the frequency offset is varying with time. Nonetheless, since the reader is transmitting a CW when the tag is backscattering, the phase offset introduced to each tag packet can be estimated by calculating the average phase of the prior CW packet and hence cancelled out (provided that the frequency mismatch is small). On the other hand, the RSSI will maintain at similar levels regardless of the frequency offset (see Fig. 2 (a)). This is because the extra phase term only appears in the complex exponentials and hence has little impact on the IQ amplitude.

To ensure that the CW and the adjacent tag packets experience the same phase offset in the presence of a small frequency offset, the lengths of the packets must be short and the frequency closely matched. Fig. 1 shows the flowchart to estimate the RSSI and phase of a tag in this work. Since there is a huge power disparity between the tag and the reader leakage signals, they can be separated easily. In addition, since all tag packets start with the same preamble, a matched filter can be used to locate the start (also is the end of the corresponding CW packet) of each tag packet.

IV. MEASUREMENT SETUPS, RESULTS AND ANALYSES

A. Carrier frequency offset estimation

Modern SDRs accept a wide range of frequencies and the LO can be retuned by simply updating the relative register. For the PlutoSDR the minimum LO tuning step size is 2.4 Hz. Any frequency offset can be found between the reader and sniffer LO by observing the FFT of the signal captured from the reader. However, the resolution will be dependent on the FFT size. Moreover, since the reader signal is modulated the captured waveform might be asymmetric which could lead to estimation errors. The frequency estimation accuracy can be improved by exploiting the EPC Gen2 protocol which specifies that before a tag replies, the reader will transmit a continuous wave (CW) that lasts at least ten FM0 symbols (T_1 in Fig. 2 (a)). It is known that an angular frequency $2\pi f$ is a measure of a changing phase θ over time:

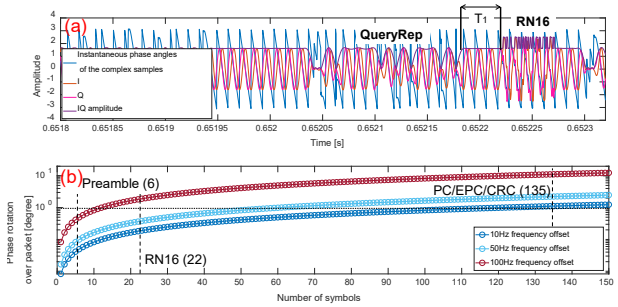

Fig. 2 Effects of frequency offset between the SDR and the reader carrier.

(a) The IQ waveforms of the tag data are distorted by the frequency offset. (b) Phase rotation over different tag packets at 436 kHz BLF.

$$2\pi f = \mathrm{d}\theta/\mathrm{d}t \tag{3}$$

So in the CW period, the frequency offset can then be estimated using a linear fit to the phase of each sample. Since the leakage reader signal at the SDR is usually strong the SNRs of the CW samples should be excellent. In addition, the CW samples contain no modulating components and hence they provide a much better offset estimation.

Even though a frequency correction of the SDR's LO can be performed during each data acquisition, there will always be some residual frequency offset caused by errors in frequency offset estimation and frequency drifts of the oscillators. However, since the packets used for phase and RSSI recoveries are short, the errors induced can be minimised. Fig. 2 (b) shows the theoretical phase rotation over different lengths of tag packets at 436 kHz BLF, with respect to different LO frequency offsets. According to the EPC Gen2 standard, the preamble (6 symbols) is included in all tag packets, at 436 kHz link frequency this packet lasts less than 14 μs and thus the phase rotation over the packet is less than 1°, even with a frequency offset of 100 Hz. An RN16 packet (22 symbols) is several times longer, but the total rotation is just around 2 degrees with the same offset of 100 Hz. In comparison, an EPC packet (135 symbols) is a lot longer, and the corresponding phase rotation is over 10°. It is for this reason that we focus on phase recovery using only the RN16.

B. *Phase and RSSI estimations*

Fig. 3 (a) shows the experimental setup to verify the phase and RSSI estimations of a tag at various locations using the sniffer. To demonstrate the proof of concept and allow repeatable measurements, a controlled method is adopted where the SDR is connected directly to the coupled port of a 10 dB directional coupler, while the output port connects to the RFID reader, and the input port connects to the reader antenna such that the reader and sniffer will see the same tag responses (with a 10 dB offset). The sniffer is able to detect the reader signal due to imperfect directivity. The directivity of the coupler is measured to be 38 dB at 867.5 MHz when the output port is properly terminated (the actual directivity will be affected by the antenna), which could translate to a 2 m separation in free space if the reader and sniffer we to have separate antennas. In practice the PlutoSDR could be placed at much further locations, or at locations without a line-of-sight (LoS) to the reader transmit antenna, the onboard low noise amplifier (LNA, up to 71 dB) can be used to compensate for the free space path loss. A UHF Gen2 tag is initially placed 1 m away from the reader antenna and is moved away and tested in 2 cm steps. The R420 reader is configured to transmit 35 dBm EIRP at 867.5 MHz via a

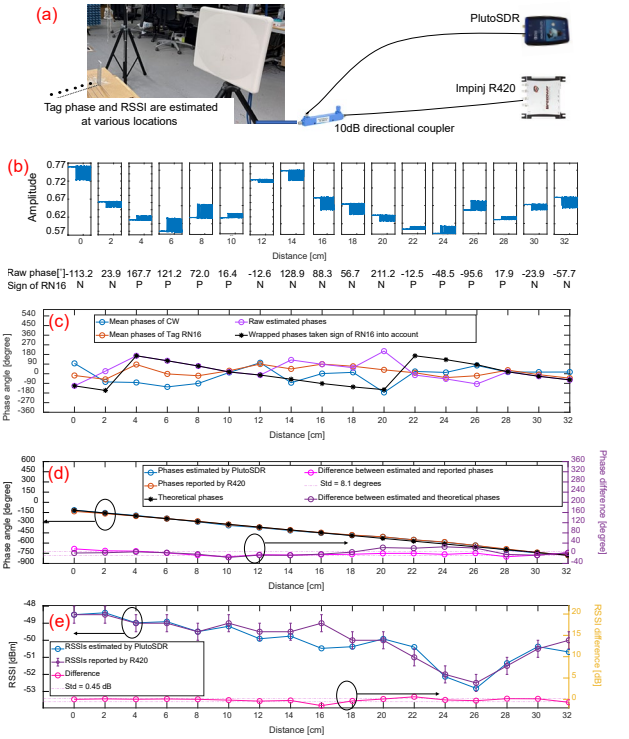

Fig. 3 RSSI and Phase recoveries of a stationary tag at various locations.

(a) Test setup to estimate a tag's RSSI and phase at different locations. (b) Received tag RN16 packets (presented in IQ amplitude) at various locations. (c) 360° phase wrapping by taking sign of the tag data into account. (d) verification of the estimated phases by the R420 reader. (e) verification of the estimated RSSI by the R420 reader.

13 dBi linearly polarised antenna using the Maximum Throughput mode (436 kHz FM0 encoding in the uplink). The SDR's LO is tuned to the same frequency and the ADC sample rate is set to 4.36 MS/s to ensure the tag data can be correctly decoded.

Fig. 3 (b) shows the captured amplitude of the tag RN16 (200 samples) and the prior CW (100 samples) at each location. It can be seen that although the operating environment is static, the overall amplitude of the CW and RN16 packets at each location varies as the tag-reader distance increases. The fluctuations have a periodicity of 18 cm (e.g. two troughs at 6 cm and 24 cm respectively) which equals half the wavelength at 867.5 MHz and are mainly caused by the interference between the leakage signal and the static components contained in the tag backscattered signals. In addition, due to imperfections of the SDR (e.g. IQ imbalances) the amplitude is modulated at a rate of the residual offset frequency and hence could also contribute to some fluctuations.

Most RFID readers have a phase ambiguity of π, i.e. the actual phase is either the reported phase or the reported phase plus π. The reason is that the tag data can be decoded by tracking the transitions in the symbols. Therefore, even if a tag signal is inversed it can still be decoded correctly. As a result, few RFID manufacturers care about the absolute phase of the tag signal. One interesting feature of Fig. 3 (b) is that the tag data appears above and below the CW periodically (typically 8 ~ 10 cm, or ~ λ/4 at 867.5 MHz) as the tag-reader distance increases. One can see from the raw phases (i.e. mean phase angle of the tag RN16 – mean phase angle of the prior CW) that even if two tag phases are 180° apart (e.g. 167.7° and -12.6°), they can still be distinguished by looking at their tag data location with respect to the prior CW. Here we define that if the average of the tag data is above the

prior CW we define it as positive (P), and the raw phase is converted to 0° to 180°; otherwise it is negative (N) and the raw phase is converted to -180° to 0°. By doing this it is possible to achieve a full 360° phase ambiguity. Fig. 3 (c) shows how the phases are processed. From the black curve, we could see that the tag phase rotates by around 360° over 18 cm which is half the wavelength at 867.5 MHz. This is a typical feature of phase angle in any backscatter communications systems.

Theoretically, at 867.5 MHz, the phase will change by 41.6° (i.e. $4\pi/\lambda \cdot \Delta d$) with a 2 cm change in reader-tag distance. To verify if the estimated phases and RSSIs are correct, they are compared with the values reported by the R420 reader (here the phases are unwrapped to ease the comparisons), and the results are shown in Figs. 3 (d) and (e) respectively. It should be noted that the phase and RSSI resolutions for the R420 reader is 0.088° and 0.5 dB respectively. Furthermore, there are fixed offsets between the estimated and reported phases and RSSIs by the sniffer and R420. In practice, a reference tag (here we use the reported phase and RSSI at location 1 as the references) can be used to calibrate the offsets out.

As can been seen the estimations match the reported values well with a standard deviation of 8.1° and 0.46 dB for the phase and RSSI respectively. At 867.5 MHz, an 8.1° phase error could correspond to an error of less than half a centimetre in distance estimation. Although between tag locations at 20 cm and 26 cm the phases estimated by the PlutoSDR deviate more from the theoretical values (dark purple curve in Fig. 3 (d)), they match the values reported by the RFID reader well. It is therefore likely that it is the tag placements that cause deviations to the theoretical values at these locations (e.g. due to multipath).

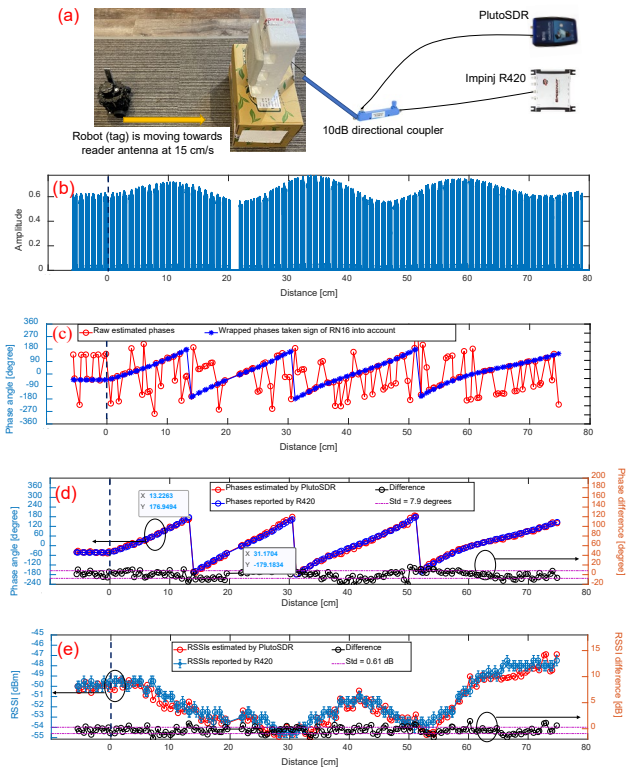

Fig. 4 RSSI and Phase estimations of a tag on a moving robot.

(a) Test setup to estimate the phase and RSSI of a tag on a moving robot. (b) Amplitude of the sniffed waveform. (c) 360° phase wrapping by taking sign of the tag data into account. (d) verification of the estimated phases by the R420 reader. (e) verification of the estimated RSSIs by the R420 reader.

C. *Phase and RSSI estimations of a tag on a moving object*

One possible application of the sniffer would be to determine the direction of motion of a moving tag. To demonstrate that the phases and RSSIs of a moving tag can be retrieved, the tag is mounted on a moving robot that moves towards the reader antenna at 15 cm/s. Similar to previous tests the controlled method is adopted to demonstrate the accuracy of the method. The experimental setup and results are shown in Fig. 4.

Since the tag is stationary in the first 0.5 s, we could see from the figures that the estimated phases and RSSIs remain at similar levels within this period (i.e. the period before 0 cm). After the 1st 0.5 seconds the phase wraps through 360° roughly every 18 cm (see the data tips in Fig. 4 (d)). Fig. 4 (b) shows that the IQ amplitude of the captured data varies in amplitude periodically (~ 18 cm) which again is caused by interferences amongst the leakage reader signal, the reflections caused by the moving robot, and the static components contained in the tag backscattered packets. In addition, due to IQ imbalances in the SDR, the residual offset frequency of around 30 Hz is also seen on the IQ amplitude. However, since up to 300 samples (including 100 CW samples and 200 RN16 samples, total 69 μs) are used for RSSI and phase estimations, the phase rotation caused by the frequency offset is less than a degree (see Fig. 2 (b)). Overall, the estimated phases and RSSIs by the PlutoSDR match the values reported by the R420 reader, with standard deviations of 7.9° and 0.61 dB respectively.

V. CONCLUSIONS

This paper presents a method to extract the relative phase and RSSI of a UHF RFID tag using a non-coherent commodity software-defined radio. The estimated phases and RSSIs have been verified by a commercial RFID reader. In addition, the phase ambiguity has been increased to 360° by taking the sign of the tag data into account. Future work will make use of multiple SDRs or an SDR with multiple receiver channels as a SIMO system to infer tag location and direction of motion for more practical RFID applications.

ACKNOWLEDGEMENT

This work is supported by the xxx through the xxx project.

REFERENCES

[1] P. V. Nikitin *et al.*, "Phase based spatial identification of UHF RFID tags," *2010 IEEE International Conference on RFID,* 2010.

[2] M. Scherhäufl *et al.,* "Indoor Localization of Passive UHF RFID Tags Based on Phase-of-Arrival Evaluation," in IEEE Trans. on Microwave Theory and Techniques, vol. 61, no. 12, pp. 4724-4729, Dec. 2013.

[3] M. Scherhäufl *et al.,* "Localization of passive UHF RFID tags based on inverse synthetic apertures," IEEE International Conference on RFID, pp. 82-88, 2014.

[4] Buettner, M., & Wetherall, D. A Flexible Software Radio Transceiver for UHF RFID Experimentation: UW TR : UW-CSE-09-1002.

[5] D. De Donno *et al.*, "Differential RCS and sensitivity calculation of RFID tags with Software-Defined Radio," *2012 IEEE Radio and Wireless Symposium*, 2012, pp. 9-12.

[6] N. Kargas *et al.*, "Fully-Coherent Reader with Commodity SDR for Gen2 FM0 and Computational RFID", IEEE Wireless Communications Letters (WCL), Vol. 4, No. 6, pp. 617-620, Dec. 2015.

[7] https://github.com/AdamLaurie/Gen2-UHF-RFID-Reader

[8] Michael Buettner and David Wetherall. A "Gen 2" RFID monitor based on the USRP. SIGCOMM Comput. Commun. Rev. 40, 3 (July 2010).

[9] D. De Donno *et al.*, "Design and applications of a Software-Defined listener for UHF RFID systems," *2011 IEEE MTT-S International Microwave Symposium* , pp. 1-4, 2011.

[10] D. De Donno *et al.*, "Challenge: towards distributed RFID sensing with software-defined radio," in Proc. of 6th MobiCom, pp. 97-104, 2010.