Fully-Coherent Reader with Commodity SDR for Gen2 FM0 and Computational RFID

Nikos Kargas, Fanis Mavromatis, and Aggelos Bletsas, *Senior Member, IEEE*

***Abstract*—There has been a continuously growing interest on radio frequency identification (RFID) and more recently, on *computational* RFID, i.e. battery-less sensors that piggyback sensed information, rather than a constant ID bit stream, utilizing Gen2, the physical layer of commercial RFID systems. This work offers a complete software-defined radio (SDR) reader with a) coherent detection without rate degradation, by exploiting already present preambles in Gen2, b) full exploitation of FM0 line coding memory in Gen2 tags, c) careful handling of symbol synchronization and departure of commercial tags from nominal bit duration and d) implementation and testing of Gen2 in a commodity SDR, utilizing a single transceiver card. Continuing recent work [1], this contribution offers an updated prototyping tool that could further unlock the potential of computational RFID and relevant batteryless sensor networks.**

I. Introduction

Recent implementation of Gen2 RFID on commodity software defined radio is based on noncoherent reception, Miller line codes and two transceiver boards (one for transmit and one for receive) [1]. There has also been sniffer (i.e. listener only) implementations as well, mostly based on non-linear processing [2], [3]. A modified version of [1] with a single transceiver board has also been used for performance analysis of RFID tags [4]. These implementations are based on now-obsolete versions of the GNU Radio software platform and the USRP1 SDR. In [5] the reader presented in [1] was ported to a newer version of GNU Radio (v3.6) but can only inventory Wireless Identification and Sensing Platform (WISP) [6]. In [7] the reader software of [1] was ported to the newest version of GNU Radio (v3.7) with USRP2 SDR, targeting commercial RFID tags. However the source code is not available as open-source. Furthermore, custom FPGA-based implementations have also appeared in the literature [8] [9].

This work offers a complete, fully-coherent, full-duplex Gen2 [10] reader for RFID tags with FM0 line coding, utilizing a single transceiver board on a commodity USRP2 (N200) software-defined radio; in sharp contrast to commodity SDR prior art, this work targets *coherent*, linear processing at the reader for RFID tags with optimal exploitation at the detection level of line coding-induced memory [11]; channel estimation for coherent processing is facilitated using already-offered Gen2 preambles, without rate degradation. The reader follows the software architecture of [1] and the code is available online.[1] In that way, commercial RFID tags or battery-less sensors that utilize Gen2 [6], i.e. computationally-intelligent RFID, can be easily read at relatively low-cost, with a useful tool for further research in this exciting area.

Section II presents the system model, tailored to FM0 line coding and memory, Section III offers SDR processing, including detection and synchronization, Section IV presents the reader architecture that accommodates bidirectional communication between Gen2 reader and tags and finally, Section V offers the experimental results.

II. System Model

During uplink (tag-to-reader) communication, the reader transmits a carrier wave (CW) and the RFID tag modulates its information by switching its antenna load between two states; in that way, tag information is binary-modulated on the reflection coefficient changes. The reader receives the superposition of its own transmitted signal and the tag's backscattered signal. The complex baseband equivalent of the received signal at the reader is given by [12, Eqs. (26), (33)]:

$$y(t) = [m_{\rm dc} + m_{\rm mod}\ x(t)]\, e^{+j2\pi\Delta f t} + n(t), \qquad (1)$$

where the DC component $m_{\rm dc} \in \mathbb{C}$ is due to the CW and an unmodulated component scattered back by the tag; the modulated $m_{\rm mod} \in \mathbb{C}$ component depends on the channel coefficients of the reader transmitting antenna-to-tag and tag-to-reader receiving antenna links, the tag antenna reflection coefficients, the tag scattering efficiency and the carrier transmitting power; $x(t)$ is a binary real-valued tag scattered waveform and Δf is the carrier frequency offset (CFO) between CW transmission and reader reception chain (e.g. CW transmitter and receiver could be dislocated or they could employ different oscillators); finally, $n(t)$ is the complex thermal (receiver) Gaussian noise. The system of this work is based on a single transceiver card, with a common oscillation signal for both transmission and reception, thus $\Delta f = 0$.

III. Reader SDR Processing

According to [10], each tag encodes its information using either FM0 or Miller-M ($M \in \{2, 4, 8\}$) line encoding; each Miller-M bit is based on repetition of M FM0-like waveforms. In FM0 encoding, level transitions always occur on the bit boundaries. In addition a transition occurs in the middle of bit "0". Thus, there is memory-based modulation, resulting to

This research has been co-financed by the European Union (European Social Fund-ESF) and Greek national funds through the Operational Program Education and Lifelong Learning of the National Strategic Reference Framework (NSRF) - Research Funding Program: THALES-Investing in knowledge society through the European Social Fund. NK, AB are with Telecom Lab, School of Electronic and Computer Engineering, Technical University of Crete, Chania, Greece 73100. FM is with Electrical & Electronic Engineering Dept., Democritus University of Thrace, Xanthi, Greece 67100 (e-mail: aggelos@telecom.tuc.gr).

[1] Code available at https://github.com/nikosl21/Gen2-UHF-RFID-Reader

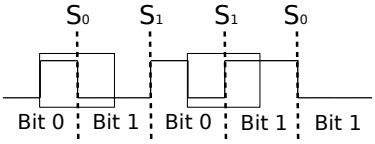


Fig. 1. FM0 line coding signal.

four possible waveforms per bit, as shown in Fig. 1, where bit boundaries are separated by dashed lines.

Work in [2] [13] have shown that after shifted examination of the transmitted waveform by $T/2$ before the beginning of the bit, where T is the bit (symbol) period, only two possible pulse shapes can be generated (instead of four), shown in Fig. 1 marked with rectangles. In order to detect a transmitted bit, the reader has to differentially decode 2 received symbols (using $2T$ signal observation instead of just T), realizing a gain of 3dB compared to maximum-likelihood (ML) symbol-by-symbol detection.

Assuming that the reader can perfectly estimate one of the two tag states and remove it from the received waveform (zero-offset FM0), the received digitized signal from Eq. (1) is expressed as:

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

where $n[k] = n(kT_s) \sim \mathcal{CN}(0, 2\sigma_n^2)$, T denotes the nominal bit duration, τ is the delay before tag starts transmitting its information, $L \triangleq \frac{T}{T_s}$ the oversampling factor and $S_{d(n)}$ can be selected between the following waveforms:

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

The above waveforms are the only possible signals when one observes the zero-offset FM0 signal for a duration of one bit (i.e. T), starting $T/2$ before the start of a bit (up to the middle of the bit), or starting at the middle of the bit (up to $T/2$ after the end of the bit). Detection of those two waveforms, spanning signal duration of $2T$, offers the detection of one of the four possible waveforms for each bit and fully exploits memory induced in FM0. Consequently, the received signal after matched filtering with a square pulse of length $L/2$ samples (i.e. for a half symbol period after synchronization) can be written as:

$$y = \sum_{k=0}^{\frac{L}{2}-1} y[k] = \sum_{k=0}^{\frac{L}{2}-1} \frac{L}{2} hx[k] + \sum_{k=0}^{\frac{L}{2}-1} n[k] = h'x + n', \tag{4}$$

where $x \in \{0, 1\}$ and $n' \sim \mathcal{CN}(0, L\sigma_n^2)$. Thus, each FM0 symbol observed with a $T/2$ shift can be written as a 2×1 complex vector:

$$\mathbf{y} \triangleq \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = h'\mathbf{x} + \mathbf{n}, \tag{5}$$

where $\mathbf{x} \in \{\mathbf{e}_0 \triangleq [1\ 0]^T, \mathbf{e}_1 \triangleq [0\ 1]^T\}$ and $\mathbf{n} \sim \mathcal{CN}(0, L\sigma_n^2\mathbf{I}_2) \equiv \mathcal{CN}(0, \sigma^2\mathbf{I}_2)$. Component y_0 or y_1 of the complex vector $\mathbf{y}$ will be referred to as half bit. The tag signal-to-noise ratio (SNR) is defined as:

$$\text{SNR} \triangleq \frac{|h'|^2}{\frac{L}{2}\mathbb{E}[|n[k]|^2]} = \frac{|h'|^2}{\sigma^2} = \frac{L|h|^2}{2\mathbb{E}[|n[k]|^2]}. \tag{6}$$

A. DC offset and Channel Estimation

In a real time application, the DC component can be estimated during a Gen2-defined interval before the tag starts switching. This interval is known to the reader and is defined by [10] as T_1. Tag is absorbing energy with corresponding reflection coefficient close to zero; thus, the reflected signal corresponding to one of the two tag load states, can be estimated by averaging the received samples acquired in interval T_1.

The estimated component is then subtracted from each sample, offering Eq. (2). A Gen2 tag that uses FM0 line coding transmits a known (real) sequence (preamble) $\mathbf{s}_p$ before sending information bits. This sequence consists of twelve half bits. At first, frame synchronization is performed and the delay τ is estimated by correlating the received signal with the known preamble. Although the duration of T_1 is known to the reader, it is subject to small deviations that are tag-dependent. Thus, the reader can search for a suitable τ in a small interval i.e $\{0, \ldots, L\}$.

$$\tau^* = \underset{\tau \in \{0,\ldots,L\}}{\text{argmax}} \left| \sum_{n=0}^{N_p-1} s_p[n] y[\tau + n] \right|, \tag{7}$$

where N_p is the number of samples in the preamble. The unknown parameter h can then be estimated by solving a least squares problem:

$$\hat{h} = \underset{h \in \mathbb{C}}{\text{argmin}} \sum_{k=\tau^*}^{\tau^*+N_p-1} |y[k] - hs_p[k - \tau^*]|^2 \tag{8}$$

$$= \frac{\sum_{k=\tau^*}^{\tau^*+N_p-1} y[k] s_p[k - \tau^*]}{||\mathbf{s}_p||^2}, \tag{9}$$

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

B. Detection

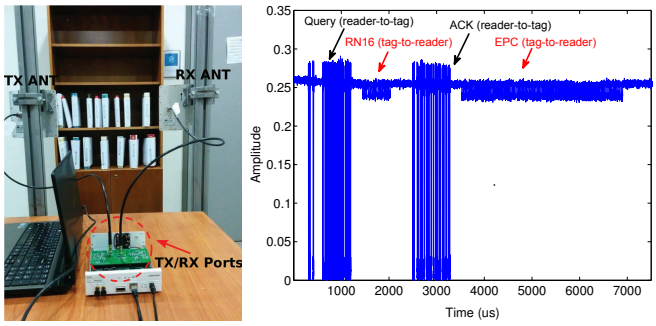
With parameter h' estimated and known, the ML detection rule for system of Eq. (5) becomes:

$$\Re(h'^*(y_1 - y_0)) \underset{S_0}{\overset{S_1}{\gtrless}} 0, \tag{10}$$

where $\Re(z)$ denotes the real part of complex z. The probability of error of the above minimum distance rule can be easily found as $\Pr(e)_T^{\text{coh}} = Q(|h'|/\sigma)$, with $Q(t) = (1/\sqrt{2\pi}) \int_t^{+\infty} e^{-t^2/2} dt$.

Alternatively, the noncoherent rule for the system of Eq. (5), where estimation of h' is not needed, is simplified to:

$$|y_1|^2 \underset{S_0}{\overset{S_1}{\gtrless}} |y_0|^2, \tag{11}$$



(a) Full-duplex SDR reader with one transceiver.

(b) Read-tag bidirectional communication.

Fig. 2. Experimental setup and captured waveform at the reader.

with probability of error $\Pr(e)_T^{\text{ncoh}} = (1/2)\, e^{-|h'|^2/(2\sigma^2)}$ [14].

Having detected $N+1$ FM0 symbols of duration T and time-shifted by $T/2$, based on Eq. (5), the final decision for the transmitted bits $\mathbf{b}$, considering signal duration of $2T$ for each bit is computed as:

$$\hat{b}(n) = \hat{d}(n-1) \oplus \hat{d}(n), \quad n = 1, \ldots, N, \tag{12}$$

where $\hat{d}(n) = 0$ when S_0 is detected and $\hat{d}(n) = 1$, otherwise; operation $\oplus$ denotes modulo-2 addition (xor). The specific rule fully exploits memory of FM0 and results to erroneous bit detection when *exactly* one of the two (shifted) consecutive FM0 symbols is erroneously detected:

$$\Pr(e)_{2T} = 2\Pr(e)_T\left(1 - \Pr(e)_T\right). \tag{13}$$

Fig. 3(d) shows the 3-dB gain of the above differential decoding of coherent detection when signal of $2T$ duration is used to decode each bit, instead of T. Additionally, the advantage of coherent detection compared to noncoherent (broadly used in existing RFID systems) is also shown. It is remarked that coherent detection exploits already-offered preambles in Gen2 and thus, comes at no additional rate loss.

IV. Reader Architecture

A Gen2 reader also transmits towards the tags. Multiple tag access is based on framed slotted aloha (FSA). The Gen2 reader initiates an inventory round by sending a Query command that specifies important communication parameters, such as tag rate, tag data encoding (FM0 or Miller) and number of slots (Fig. 2(b)). Each tag selects a number between 1 and N, where N is the number of slots in the inventory round and transmits a random 16-bit sequence (RN16) in the selected slot, preceded by a known preamble sequence (Fig. 2(b)). The reader acknowledges a single tag by sending an acknowledgement (ACK) command and receives from the tag a 135-bit sequence response, containing the EPC (tag ID of 96 bits) plus additional bits including CRC (Fig. 2(b)). Reader reply to a tag message should be transmitted at most 500 μs after the tag message, when the system is configured to the lowest tag rate of 40KHz, supported in this implementation.

A. Reader Hardware

A commodity USRP N200 software defined radio (SDR) is utilized, equipped with a *single* RFX900 daughterboard (operating between 902-920MHz) and a laptop (Fig. 2(a)). The transmit and receive ports of the RFX900 daughterboard are connected with two circularly-polarized antennas, one for transmitting reader commands and one for capturing tag's reply in full duplex mode. A custom low-noise figure daughterboard was also built and tested. The USRP communicates with the laptop using Gigabit Ethernet.

B. Reader Software

Software is build on top of GNU Radio, following the six-block structure of [1]: USRP source, Matched Filter, Gate, Tag Decoder, Gen2 Logic and USRP sink. The first and last blocks are responsible for the acquisition/transmission of samples from/to the USRP.

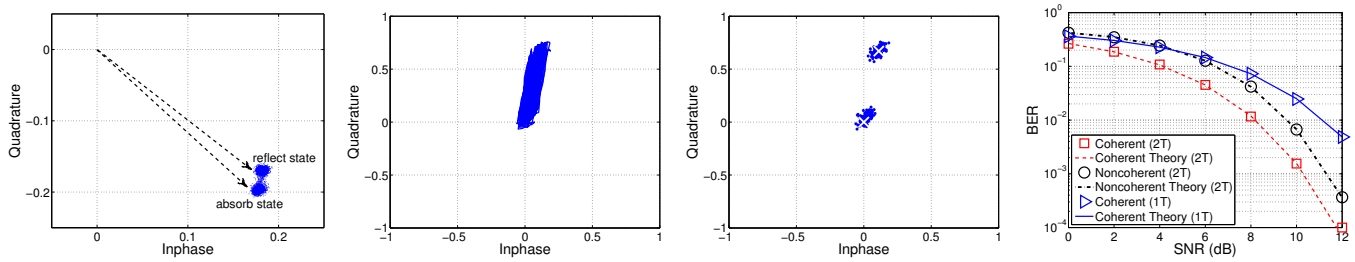
The inphase and quadrature components of a received tag EPC message are shown in Fig.3(a). Notice that two arbitrary I/Q states appear in the constellation diagram corresponding to the two tag states. The Matched Filter block is responsible for filtering the received signal with a square pulse of half symbol period. The Gate block is responsible for identifying the reader queries; by tracking the amplitude of the received signal the reader is able to identify the transmitted commands, and thus process only samples that follow and correspond to the tag's response. Immediately after a reader command has ended, the block estimates the DC offset component and removes it from each sample. These samples are given as input to the next block for further processing. Fig.3(b) shows the output of Gate block for an EPC tag message, with DC component removed.

The Tag Decoder block is responsible for the frame synchronization, channel estimation and detection of the tag responses. Synchronization for the RN16 and tag's ID (EPC) sequences is performed by correlating the received signal with the known preamble. Then channel estimation is performed as described in section III-A. A major problem in RFID readers is the variation in the tag's nominal bit duration. The reader in this work operates at the minimum data rate (40KHz), where these variations are not critical. Error in symbol level synchronization was observed in some cases, when decoding the tag ID (EPC) plus CRC and were due to the large sequence size (135 bits). To deal with that synchronization problem, an initial sampling instant τ^* is obtained, by correlating with the preamble; then the symbol rate T and thus, the right sampling instants are chosen, such that signal energy is maximized:

$$T^* = \underset{T}{\text{argmax}} \sum_{n=0}^{2(N-1)} \left| y_f\left[\tau^* + n\frac{T}{2}\right]\right|^2, \tag{14}$$

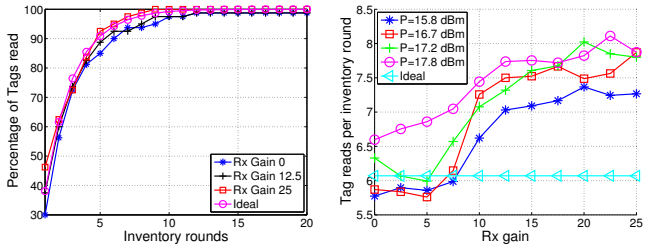
where N is the number of transmitted bits that follow the preamble sequence and y_f the received signal after matched filtering and DC offset removal. The received signal is then sampled at the end of each half symbol period.[2] Fig. 3(c) shows the I/Q constellation diagram after frame synchronization,

[2]Work in [1] uses different symbol duration estimation, based on the Mueller-Muller clock recovery algorithm.



(a) Received samples. (b) Received samples after matched filtering and DC offset removal. (c) Received samples after symbol period estimation and synchronization. (d) BER of detection after matched filtering and synchronization.

Fig. 3. IQ constellation diagram of a tag's EPC response using measurement data and BER of detection techniques.



(a) Reading rate vs round. (b) Reading rate vs gain.

Fig. 4. Reading rate vs time and tx power.

symbol period estimation and sampling. The channel estimate is marked with an x mark. Next, tag decoding is performed.

Finally, depending on the output of the tag decoder block, the reader creates the next command and propagates it to the transmit chain. Currently the commands supported by our reader are the Query, ACK and QueryRep commands.

V. Experimental Results

16 Gen2 tags were attached to books in a bookcase, 1.5 meters away for the reader antennas, as shown in Fig. 2(a). Number of slots per round was set equal to the number of tags. The circularly-polarized antennas used had a gain of 7 dBic. Reader transmission was configured such that a tag replied in each inventory round, regardless of whether it had already been read. The total number of inventory rounds was set to 60 thus, offering a total number of $60 * 16 = 960$ slots. Experiments were repeated for various levels of transmission power at $15.8, 16.7, 17.2$ and 17.8 dBm.

Fig. 4(a) shows the percentage of identified tags when the signal transmission power was 17.8 dBm. In the same Figure we present the performance of an ideal reader which can perfectly decode single tag slots. We observe that the performance of the reader is increased while we increase the receiver gain and reaches the performance of the ideal reader. The read rate is above the expected due to the capture effect i.e slots of collided tag signals can be decoded when there is a significant power difference between them.

Fig. 4(b) shows the reading rate of the reader. The theoretical throughput (reads per round), when the number of slots is equal to the number of tags, is $\rho = N\left(1 - \frac{1}{N}\right)^{N-1} = 6.08$, when $N = 16$ [2].

References

[1] M. Buettner and D. Wetherall, "A software radio-based UHF RFID reader for PHY/MAC experimentation," in *Proc. IEEE Int. Conf. on RFID*, Orlando, FL, Apr. 2011, pp. 134 –141.

[2] A. Bletsas, J. Kimionis, A. G. Dimitriou, and G. N. Karystinos, "Single-antenna coherent detection of collided FM0 RFID signals," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 756–766, Mar. 2012.

[3] D. De Donno, F. Ricciato, and L. Tarricone, "Listening to tags: Uplink RFID measurements with an open-source software-defined radio tool," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 1, pp. 109–118, Jan 2013.

[4] L. Catarinucci, D. De Donno, R. Colella, F. Ricciato, and L. Tarricone, "A cost-effective SDR platform for performance characterization of RFID tags," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 4, pp. 903–911, April 2012.

[5] Y. Zheng and M. Li, "ZOE: Fast cardinality estimation for large-scale RFID systems," in *Proc. IEEE Int. Conf. on Computer Communications (INFOCOM)*, April 2013, pp. 908–916.

[6] A. P. Sample, D. J. Yeager, and J. R. Smith, "Design of a passively-powered, programmable sensing platform for UHF RFID systems," in *Proc. IEEE Int. Conf. on RFID*, Grapevine, TX, Mar 2007.

[7] A. Bothe, C. Schraeder, and N. Aschenbruck, "An UHF RFID performance evaluation architecture based on traces from a software defined transceiver," in *Proc. IEEE Int. Conf. on RFID Technology and Applications (RFID-TA)*, Sept 2014, pp. 72–77.

[8] C. Angerer, "Design and exploration of radio frequency identification systems by rapid prototyping," Ph.D. dissertation, Institut für Nachrichtentechnik und Hochfrequenztechnik, Vienna University of Technology, 2010, Advisor: M. Rupp.

[9] F. Galler, T. Faseth, and H. Arthaber, "SDR based EPC UHF RFID reader DS-SS localization testbed," in *Proc. IEEE 16th Annual Conf. on Wireless and Microwave Technology Conference (WAMICON)*, April 2015, pp. 1–4.

[10] "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," 2015.

[11] N. Kargas, "SDR readers for Gen2 RFID and backscatter sensor networks," M.S Thesis, ECE Dept., Technical University of Crete, July 2015, Advisor: A. Bletsas.

[12] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, March 2014.

[13] M. Simon and D. Divsalar, "Some interesting observations for certain line codes with application to RFID," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 583–586, Apr. 2006.

[14] J. G. Proakis and M. Salehi, *Communication Systems Engineering*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, August 2001.