Listening to Tags: Uplink RFID Measurements with an Open-Source Software-Defined Radio Tool

Danilo De Donno, Fabio Ricciato, Member, IEEE, and Luciano Tarricone, Senior Member, IEEE

Abstract—We present the Software-Defined Radio (SDR) implementation of an RFID Listener, a passive receive-only device that decodes the signals exchanged between the RFID Reader and the interrogated Tag following the EPC Class-1 Generation-2 standard. Our RFID Listener is based on the open-source project GNU Radio. It provides complete flexibility and full control over the entire protocol stack down to the physical layer. As such, it can be used as a powerful but inexpensive tool for testing and measuring the performance of RFID systems in real operating conditions. In this work, we leverage the SDR Listener for a number of experiments that, taken collectively, are illustrative of the potential of such tool for RFID research. First, we use it to test comparatively different Timing Recovery schemes for the reception of the Tag signal in uplink, through the analysis of bit error statistics measured experimentally. We find that the scheme proposed by Harris and Rice based on Polyphase Filter Bank (PFB) displays excellent performance in this context, very close to the theoretical bound and with a gain of 5 dB over the more common Mueller and Muller scheme. Second, we use the Listener to evaluate the impact of frequency nulls in the uplink RFID channel for different indoor scenarios. We find that frequency nulls are pronounced especially in the presence of metal objects and obstructions of the Fresnel zone, but frequency hopping is effective in counteracting the problem. Our experiments show that the signal backscattered by a passive Tag can be correctly received up to a distance of 35 meters, with low-cost equipment and without highly directional antennas.

Index Terms—RFID, Software-Defined Radio, Timing Recovery, GNU Radio, Polyphase Filter Banks, read range, fading.

I. INTRODUCTION

The emerging Radio Frequency Identification (RFID) technology is being adopted in a diverse and growing range of application fields. The ISO/IEC 18000 standard [3] defines the air interface and classifies RFID systems according to their operating frequency: low frequency (LF) at 125 KHz, high frequency (HF) at 13.56 MHz, ultra-high frequency (UHF) at 860-960 MHz, and microwave at 2.45 GHz. The main driver for the success of RFID technology is cost-effectiveness and software capabilities. As a basis for our experimental study, we use the open-source Software-Defined Radio (SDR) implementation of an RFID Listener compliant with the Gen2 standard, developed in GNU Radio [16], and based on the Open Source Radio Peripheral (USRP) [17]. We use it in conjunction with an SDR Reader developed earlier by Buettner [18], [19] that is also based on the USRP. The total cost of our setup is below 1000$, considerably cheaper than the available commercial ad-hoc platforms (see e.g. [20], [21]) that cost several tens of thousands of dollars. Our experiments show that a commercial Tag can be successfully decoded by our low-cost SDR Listener up to a distance of 35 meters without highly directional antennas, the limiting factor being the loss of sensitivity due to the presence of the strongest CW signal by the Reader. In principle, the listening range can be

commands and the Continuous Wave (CW) to energize the passive Tag. The response backscattered by the Tag constitutes the uplink signal.

In an earlier work [7], we proposed to consider alternative schemes where the downlink transmission (Tx) and uplink reception (Rx) functions are performed by separate devices, respectively the Illuminator (Tx-only) and the Listener (Rx-only). This enables distributed scenarios where Tag signals are received contemporarily by multiple Listeners, possibly but not necessarily cooperating. The use of multiple Listeners can be exploited, for instance, to improve the accuracy of commonly adopted schemes for Tag localization [10]–[12] and RFID-assisted navigation [13], [14]. Another use of the Rx-only Listener device is to sniff radio communications between the Tag and a traditional Tx/Rx Reader, e.g. for protocol analysis and testing but also for other (possibly malicious) purposes [15].

The focus of this work is on the uplink channel, i.e. on the reception of the Tag response. The initial motivation for this study was to measure experimentally the maximum “uplink range” that can be reached with currently available commercial Tags operating in a real environment, and understand what are the limiting factors. In other words, we ask the question: how far can the Tag signal be heard and correctly decoded?

The issue is of interest for existing real-world systems. It has obvious implications for privacy and security of current RFID deployments, but is also an important input for the design of novel distributed systems based on low-cost Rx-only devices like those anticipated in [7]. The answer to the above question depends, among other factors, on the performance of the receiver device itself, hence on its hardware and software capabilities. As a basis for our experimental study, we use the open-source Software-Defined Radio (SDR) implementation of an RFID Listener compliant with the Gen2 standard, developed in GNU Radio [16], and based on the Universal Software Radio Peripheral (USRP) [17]. We use it in conjunction with an SDR Reader developed earlier by Buettner [18], [19] that is also based on the USRP. The total cost of our setup is below 1000$, considerably cheaper than the available commercial ad-hoc platforms (see e.g. [20], [21]) that cost several tens of thousands of dollars. Our experiments show that a commercial Tag can be successfully decoded by our low-cost SDR Listener up to a distance of 35 meters without highly directional antennas, the limiting factor being the loss of sensitivity due to the presence of the strongest CW signal by the Reader. In principle, the listening range can be

Initial versions of this tool were presented earlier in [7], [8]. The latest version resulting from the current work is freely available from [9].
further increased by adopting very directive antennas and/or external transmitters that boost the Reader’s CW [22]. We highlight that RFID users should be aware that Tag readings can be eavesdropped at several tens of meters even with very affordable equipment.

We also use our Listener to evaluate qualitatively the impact of spectral nulls in the RFID band caused by multipath in different environmental conditions. We find that the problem of frequency nulls can be dramatic in presence of metal objects obstructing the Fresnel zone: the Tag signal is completely annihilated on certain frequencies but can still be received with very high probability on other frequencies in the same band, indicating that frequency hopping is effective in counteracting the problem.

During the measurements, it became clear that Timing Recovery is a critical component of the whole uplink reception chain. This is not surprising in our setting, since timing errors can be introduced by the Tag itself but also by the low-cost chain. This is not surprising in our setting, since timing errors can be introduced by the Tag itself but also by the low-cost USRP hardware used for the Reader/Listener platforms. On the positive side, the SDR approach enables the correction in software of the clock drift caused by the hardware, and that magnifies the importance of adopting an effective Timing Recovery algorithm. Our experimental results show that the Timing Recovery scheme based on Polyphase Filter Bank (PFB) proposed by Harris and Rice [1] yields excellent performance, considerably better than the well-known Mueller and Muller (MM) [2], while the simple Zero-Crossing (ZC) scheme performs very poorly. This is an important result, never reported before, that can help engineers and practitioners to improve the sensitivity of (the receive chain of) RFID devices, being commercial Readers and/or testing equipment.

In summary, this paper makes the following contributions:

1) The potential of leveraging freely available SDR implementations of Reader and Listener for testing and performance measurements of real-world RFID systems is presented along with illustrative measurement results.
2) Different Timing Recovery schemes for the reception of the Tag signal in uplink are tested comparatively, showing that PFB outperforms the much more popular MM.
3) The impact of spectral nulls induced by multipath in the uplink RFID channel is evaluated for different indoor scenarios, showing that the problem, if present, can be effectively counteracted by frequency hopping.
4) The maximum “uplink range” of a conventional RFID system is measured and the limiting factors are identified.

The experimental measurements and, most importantly, the free open-source Listener tool presented in this work can help engineers and researchers to gain better understanding of the performances of actual RFID technology in real-world contexts. Moreover, the availability of an affordable Listener device for testing and experimentation can contribute to spur further work and interest in novel unconventional distributed RFID schemes with multiple uplink receivers.

The rest of the work is organized as follows. In §II, neighboring related works are surveyed. The basics of the EPC Gen2 standard are briefly recalled in §III. The experimental setting and the implementation of the Listener are described in §IV, while §V presents selected measurement results. Finally, conclusions are drawn in §VI.

II. RELATED WORK

The idea of investigating RFID communications by means of GNU Radio and the USRP was pioneered by Buettner and Wetherall in [24]. They developed a platform for monitoring the Gen2 RFID traffic by capturing and decoding in real-time only the Reader’s transmissions. The same authors have recently presented [18] and released [19] a GNU Radio implementation of a Gen2-compliant RFID Reader. In a previous study, we showed how the Buettner’s Reader can be turned into a cost-effective tool for evaluating the performance of passive Tags in terms of sensitivity and differential radar cross-section [25], [26]. This is an appealing alternative to commonly adopted solutions based on expensive commercial equipment [27].

The flexibility of SDR has been leveraged by researchers to quickly implement and experiment novel ideas in the processing of RFID signals. Mechanisms for Tag collision recovery have been demonstrated in GNU Radio for LF and UHF systems respectively in [28] and [29]. In [30], GNU Radio implementations are used to demonstrate the feasibility of tracking people by means of RFID fingerprinting. All these works are based on the canonical RFID Reader that interrogates the Tag and receives its signal. No other previous work has considered the role of a third Rx-only device, namely the RFID Listener.

III. GEN2 BACKGROUND

EPC Gen2 [4] in the UHF band — operating frequencies 865-868 MHz in Europe, 902-928 MHz in US, 952-954 MHz in Japan — is, nowadays, the most widely adopted among the existing RFID standards. Gen2 Tags are fully passive: the energy required to activate the internal chip is harvested exclusively from the Continuous Wave (CW) transmitted by the Reader. Passive Tags do not transmit new power but simply backscatter the CW from the Reader and modulate it by changing the reflection coefficient of their antenna.

A Gen2 Reader starts the interrogation procedure by broadcasting a Query command to the Tags. This Query packet not only configures the uplink (from Tag to Reader) communication parameters, such as the encoding scheme (FM0, Miller-2,
Miller-4 or Miller-8) and the frequency of the Amplitude Shift Keying (ASK) modulation, but also announces the number of allocated time slots of the Framed Slotted Aloha (FSA) MAC scheme [31]. A Tag in the interrogation zone of the Reader randomly selects one of these slots and responds with a RN16 packet containing a random 16-bit number. Upon successful reception, the Reader will echo the RN16 in the following acknowledgement message (ACK). If the Tag successfully receives the ACK with the correct RN16 number, it will finally backscatter its 128-bits ID in the Electronic Product Code (EPC) message. Tag EPC packets include a Cyclic Redundancy Check (CRC), and if the EPC passes the checksum a QRep (Query Repeat) message is sent by the Reader. A negative acknowledgement (NAK) message is sent otherwise.

After all Tags have been read, the Reader will power down. We refer to an individual interrogation procedure as an Inventory Round, and the series of inventory rounds between power-down periods as an Inventory Cycle. Figure 1 shows an example of successful Reader-Tag handshake in the first slot of an Inventory Round.

IV. EXPERIMENTAL SETUP

The reference scenario is depicted in Fig. 2. A conventional Gen2 Reader queries and energizes a passive Tag. A third device, the Listener, independently decodes the signals from both the Tag and the Reader. Note that the Listener needs to decode the Reader commands in order to decode the Tag replies, since the uplink signal parameters (bitrate, frequency offset and encoding scheme) are determined by fields in the Reader commands. In other words, our Gen2 Listener captures and decodes both downlink and uplink signals between a conventional Reader and the Tag, and therefore can be used as a passive analyzer (sniffer) for the whole RFID system.

As far as the reception of the Tag signal is concerned, the Rx chains of the Listener and of the Reader are functionally equivalent. For this reason, our study of the uplink receiver conducted on the Listener applies directly also to the Rx chain of any Reader. While in principle the measurements we present could be taken directly at the Reader, the use of a separate Listener brings the advantage of decoupling the uplink channel from the downlink channel. For instance, it is possible to test the uplink channel at distances well beyond the maximum downlink range that is typically limited to approximately 8-10 meters for Tags with sensitivity of -18 dBm [32]

In our setup, we used open-source SDR implementations for both the Reader and the Listener. This ensures flexibility and full control over any aspect of uplink and downlink communications, without incurring into the restrictions that are encountered when experimenting with commercial Readers: rigid configuration, limited data logging, “black-box” implementation of signal processing blocks, etc. For this work, we have used an improved version of our original GNU Radio Listener [7] in conjunction with the GNU Radio Reader developed by Buettner [19], both adopting the USRP as the radio interface.

GNU Radio [16] is a free software toolkit, licensed under General Public License (GPL), to support SDR development in a Linux environment. In GNU Radio, a transceiver is represented by a Python graph, where the vertices maps to signal processing blocks programmed in C++ and the edges represent the data flows between them. The USRP is a cost-effective device developed by Ettus Research LLC [17] that turns a general purpose computer running GNU Radio into a flexible SDR platform. The USRP core is a motherboard with four 12-bit ADCs @64Msamples/sec, four 14-bit DACs @128Msamples/sec, and an Altera Cyclone FPGA. The ADCs/DACs are connected to the RF front-ends located on separate daughterboards, while the FPGA is connected by USB interface to the host PC. Both the Buettner’s Reader and our Listener use the RFX900 daughterboards whose operating frequency range 750-1050 MHz covers the worldwide UHF RFID bands. We used circularly polarized ALR-8610 antennas with 5.5 dBi gain by Alien Technology [32] for both the Reader and the Listener. The passive Tag considered in the experiments is the Impinj Thinpropeller [33] with chip sensitivity -15 dBm.

A simplified block scheme of the Listener Rx chain is depicted in Fig. 3. The RF signal is downconverted and digitalized by the USRP, then passed to the software domain for baseband digital processing. The block Reader_DEC&_TAG_GATE decodes and interprets the Reader signals, from which the temporal position of the following Tag signal (if any) is identified. The latter is then gated to the CLOCK_RECOVERY block that recovers the symbol synchronization, then passed to the TAG_DECODER that implements correlation-based decoding.

In order to test at different noise levels, an Additive White Gaussian Noise (AWGN) source with adjustable power is inserted at the ingress of the software domain as shown in Fig. 3. This allows to inject a controllable amount of synthetic noise on top of the “real” noise level entering the system. The actual SNR is then measured in the successive Reader_DEC&_TAG_GATE block. The amplitude signal resulting from a typical Reader-Tag handshake as recorded by the Listener at the input of such block is plotted in Fig. 4. The noise power $P_n$ is measured by the signal variance during the period $T_1$, where only the CW is present, while the signal-plus-noise power $P_s + P_n$ is measured in the interval...
In our Listener, the Rx chain can be branched: by running two processing branches in parallel on the same stream of baseband samples one can perform a perfectly fair comparison between two different processing choices and/or implementation variants. We have leveraged this feature to evaluate the impact of different Timing Recovery schemes on the uplink reception performance: the output of the READEN_DEC_&_TAG_GATE block was branched and different Timing Recovery algorithms were inserted in each branch, as shown in Fig. 3. Following the same approach, branching can be used to compare different solutions for other modules, e.g. the Tag decoder, but also to perform different sub-tasks on each branch, e.g. Tag decoding and Tag fingerprinting.

V. MEASUREMENT RESULTS

In this section, we present detailed measurements of our Listener performance. Preliminarily to that, it is convenient to recall the possible causes of unsuccessful reception:

- **Tag inactivity**: the Tag fails to activate due to insufficient power harvested from the Reader, e.g. due to fading holes or malfunctionings.
- **Missed Frame**: the Tag signal is not detected by the receiver.
- **Erroneous Frame**: the Tag signal is correctly detected but decoded with one or more bit errors, thus failing the CRC.

In order to prevent Tag inactivity, we placed the Reader at a distance of $r = 2.4$ meters (see Fig. 2), close enough to ensure correct energization with very high probability. Moreover, for each interrogation we verified that the Tag signal was correctly received at the Reader. Therefore, we can completely eliminate this source of error (Tag inactivity) from the measurement data.

One central goal of our measurements was to assess the primary source of reception failure in real operating conditions and with currently available commercial Tags. This allows to evaluate the opportunity of protecting the EPC message with a Forward Error Correction (FEC) code, an approach that was proposed in some previous works [34], [35]. In simple words, FEC can reduce Erroneous Frames, but not Missed Frames. However, the measurements presented hereafter reveal that Missed Frames always dominate over Erroneous Frames in a well-designed Rx chain, hence there is very little room for improvement by introducing FEC.

A. Impact of Timing Recovery schemes

The first version of our SDR Listener [7] adopted a simple Zero-Crossing (ZC) scheme for Timing Recovery [23] along with a simple implementation of the early-late-gate technique. The analysis of bit-error statistics (reported below) for a sample of Erroneous Frames with Miller-8 encoding revealed the following facts:

- Unbalanced errors: the incidence of errors on ‘1’ bits was almost double than for ‘0’ bits.
- Non-uniform localization: bit errors occurred more frequently in the final part of the 128-bit EPC message.
- Bursty patterns: bit errors occurred in groups, and isolated single-bit errors were relatively infrequent.

These are clear indications that bit errors were due to the incorrect recovery of symbol synchronization.

To illustrate the impact of timing errors on the decoding of Miller-8 encoded bits, we plot in Fig. 5 the average modulus of the correlation coefficient\(^3\) between the local copy of ‘0’ and ‘1’ symbols at the receiver and the (oversampled) received signal when the transmitted symbol is ‘0’ (Fig. 5(a)) and ‘1’ (Fig. 5(b)), in absence of noise and for different timing shifts.

\(^3\)Recall that the Miller encoding scheme is bi-orthogonal, i.e. each symbol is associated to a pair of antipodal waveforms [36]. Therefore, only the modulus (not the sign) of the correlation score is relevant for the hard decision.

It can be seen from Fig. 5(a) that a Miller-8 encoded ‘0’ can be correctly decoded (modulus of the correlation score greater than 0.5) up to shifts of 8 samples. On the other hand, a transmitted ‘1’ can be correctly detected only if the shift does not exceed 4 samples, i.e. half symbol period, after which it will be systematically reversed into a ‘0’ (shaded zones in Fig. 5(b)). In summary, with Miller-8 encoding, timing shifts have asymmetric impact on ‘0’ and ‘1’ symbols, the latter suffering systematic errors if the shift exceeds half-symbol period.

Motivated by this early finding, we tested two alternative Timing Recovery schemes:

- the well-known Mueller & Muller (MM) scheme [2] and specifically the implementation available in the GNU Radio block `gr_clock_recovery_mm_ff`\(^4\);
- [Another alternative scheme...

\(^4\)This is the block adopted by the Buettner’s Reader at the time of writing.\]
Fig. 5. Modulus of the correlation score for Miller-8 encoding with 16 samples per symbol when the transmitted symbol is '0' (a) and '1' (b).

Fig. 6. Reception success ratio vs. SNR measured with different Timing Recovery schemes. The dashed line represents the theoretical bound obtained by an ideal receiver with perfect synchronization in a pure AWGN channel.

- the scheme based on Polyphase Filter Bank (PFB) proposed by Harris and Rice in [1], and specifically the implementation available in the GNU Radio block gr_pfb_clock_sync_fff.

We conducted a first set of measurements with the Rx block diagram of Fig. 3 but with a single branch: each Timing Recovery scheme was tested at different noise levels, by varying the amplitude of the artificial baseband noise source. The Listener was kept at \( d = 5 \) meters from the Tag in Line-of-Sight (LoS) as shown in Fig. 2. The Reader was set to perform 1000 Query rounds hopping across five different frequencies stepped by 400 KHz in the European UHF RFID band 865.7-867.5 MHz. Figure 6 plots the fraction of frames correctly decoded by the Listener with successful CRC) averaged across all frequencies versus the measured SNR. Each curve refers to the experiments with a different Timing Recovery block. While ZC requires 11 dB of SNR to achieve 50% success rate, MM and PFB can achieve the same performance respectively a t6d Band1d B.

The near-optimum performance of PFB is confirmed by the analysis of bit error statistics presented hereafter. For each tested scheme, we tuned the input noise at the level that ensures approximately 80% of successful reception probability, i.e., approximately 20% of received Tag frames shall contain one or more bit errors. The Erroneous Frames received in this setting are then compared with the (known) EPC code in order to identify bit errors. The summary statistics are given in Table I, while Fig. 7 reports the empirical histograms of the number of bit errors in each Erroneous Frame.

Notably, ZC produces a non negligible fraction of frames where the majority of bits are wrong: this apparent paradox (even the random channel has at most 50% of bit errors on average) is explained by the systematic error on ‘1’ symbols with Miller-8 encoding caused by inadequate Timing Recovery, as discussed above (ref. Fig. 5). With PFB, instead, the situation is completely different: out of all Erroneous Frames (that are roughly 20% of the total) only approximately 20% have more than one bit error; this result is in agreement with the assumption of error independence that characterizes the ideal AWGN channel with perfect synchronization.

In the following, we analyze the position of bit errors in the 128-bit string. In Fig. 8 we plot for every bit position \( x \in \{1, 2, \ldots, 128\} \) the fraction \( y(x) \) of bit errors observed in the preceding positions. The reference straight line \( y = \frac{x}{128} \) represents the uniform distribution of bit errors that is expected in the ideal AWGN channel with perfect synchronization.

TABLE I

<table>
<thead>
<tr>
<th>% errors on '1'</th>
<th>ZC</th>
<th>MM</th>
<th>PFB</th>
</tr>
</thead>
<tbody>
<tr>
<td>% errors on '0'</td>
<td>71.9</td>
<td>60.5</td>
<td>47.7</td>
</tr>
<tr>
<td>% Errors Frames with 1 bit error</td>
<td>28.1</td>
<td>39.5</td>
<td>52.3</td>
</tr>
<tr>
<td>% Errors Frames with 2 bit errors</td>
<td>2.1</td>
<td>2.7</td>
<td>11.8</td>
</tr>
<tr>
<td>% Errors Frames with &gt; 2 errors</td>
<td>97.9</td>
<td>96.0</td>
<td>6.7</td>
</tr>
</tbody>
</table>

\[ P_b = 2 \cdot Q\left(\sqrt{M \cdot SNR}\right) \cdot \left[1 - Q\left(\sqrt{M \cdot SNR}\right)\right] \]

wherein \( M \) denotes the Miller order (\( M = 8 \) in our case). The absolute performance of PFB is remarkable: only 1 dB away from the ideal theoretical reference (dashed line). It is also somewhat suprising that, in this context, the widely used MM scheme has pretty modest performance: it fails completely below 4 dB, and requires at least 6 dB to achieve 50% success rate.
Fig. 7. Measured number of bit errors in a 128-bit EPC frame for different Timing Recovery schemes.

Fig. 8. Cumulative distribution of bit error positions.

can be seen that PFB approximates well the reference line, indicating that the error probability has no evident correlation with the bit position. Conversely, ZC and (to less extent) MM display concave curves, indicating that errors tend to accumulate towards the end of the frame: the final quarter of the 128-bit string contain about half of all errors with ZC, and one third with MM.

The above results coherently show that PFB Timing Recovery does an excellent job in keeping a high success rate also at low SNR, around 1 dB. In principle, the rate of successful frame decoding could be further increased by encoding the EPC with a FEC. In order to assess the potential gain of adding a FEC, we plot again in Fig. 9 the fraction of correctly decoded frames as a function of the SNR (blue solid line). We also plot the fraction of frames that were decoded with at most one bit error (dashed line) as well as the fraction of frames that were detected (by the preamble) regardless of the number of bit errors in the decoding stage (black solid line). The latter two curves represent the “virtual” success rate that could be achieved respectively by a single-error correcting FEC and by an ideal “oracle” FEC that always corrects all errors. It can be seen that the achievable FEC gain is very modest, only a fraction of dB even for the oracle FEC.

In other words, as far as noise is concerned, we can expect that in practice the signal from a single Tag is either strong enough to be detected and correctly decoded, or otherwise goes completely undetected. The intermediate transition region, when the signal is correctly detected but incorrectly decoded, is relatively thin and does not motivate the adoption of FEC schemes in this context as proposed by some previous works [34], [35].

B. Frequency nulls

European UHF RFID systems can use 10 frequencies in the 865.7-867.5 MHz band. Frequency hopping can be used to counteract frequency nulls and/or to mitigate collisions in dense environments with multiple Readers. The problem of frequency nulls can appear in multipath-rich environments where the different signal replicas might combine destructively at specific frequencies. Therefore, the channel gain displays a variable spectral profile, with fading “holes” (or nulls) at certain frequencies. In case of broadband wireless systems, where the signal bandwidth is larger than (or anyway comparable with) the channel coherence bandwidth, this leads to frequency-selective fading. The latter causes distortion and therefore Inter-Symbol Interference (ISI), and is typically countered by complex equalization techniques. In the context of RFID instead, where the signal bandwidth is very narrow, multipath can cause the signal to be completely canceled if transmitted at frequencies corresponding to the spectral nulls. The presence of frequency nulls around 900 MHz in an indoor environment was experimentally reported in [37]. Frequency hopping is a simple but effective countermeasure in this case, provided that at least one frequency in the RFID band is found with sufficient channel gain. Obviously, the faster the hopping rate, the shorter the expected delay until successful reception.

In the next set of experiments, we investigate the impact of frequency nulls suffered by the uplink RFID receiver in real operating conditions, and to what extent frequency hopping within the RFID band is effective in counteracting the problem. We do not aim at providing here an accurate quantitative assessment of the phenomenon, which would require...
a much more comprehensive campaign of physical channel measurements in a diverse set of operating environments. Instead, we want to evaluate qualitatively the magnitude of the phenomenon in a few sample scenarios, providing indications about whether frequency nulls can be expected in indoor RFID systems, and to what extent frequency hopping can be relied upon for overcoming the problem.

For these experiments, the Reader, Listener and Tag were arranged as shown in Fig. 2 with \( d = 5 \) meters in a large lecture room, furnished with desks and a few metal elements (e.g. wardrobe, archiver). The Reader was set to repeatedly interrogate the Tag, hopping in round-robin across five different frequencies (\( 865.7 + k \cdot 0.4 \) MHz, with \( k \in \{0, 1, 2, 3, 4\} \)). The total duration of the experiment was 20 minutes, divided into four intervals of 5 minutes each. In each of the four intervals, the operating conditions were varied as follows:

- Scenario I : static setting with LoS between the Tag and the Listener antenna.
- Scenario II : people were walking between the Tag and the Listener antenna thus obstructing the Fresnel zone.
- Scenario III : the Listener antenna was slowly rotated in the horizontal plane for a full 360° round.
- Scenario IV : a large metal panel was inserted between the Tag and the Listener antenna, and its orientation was slowly varied manually.

The receive chain (without synthetic noise source) was branched as shown in Fig. 3 in order to test in parallel PFB and ZC, i.e. the two Timing Recovery schemes with the best and worst performance, respectively. The measured success rate is shown in Fig. 10 for PFB (left) and ZC (right). Each data point represents the fraction of successfully decoded frames (with correct CRC) in every 1-minute timebin and for every interrogation frequency, for a total of 25 data points in each of the four intervals. The average success rate across all frequencies in each time bin is indicated by the solid line. The dot-grey line represents the average SNR of correctly decoded frames (values in the right-hand scale). To facilitate the comparison between PFB and ZC, the corresponding data points are reported in the scatterplot in Fig. 11. As expected, PFB always performs equal to or better than ZC.

In LoS conditions (Scenario I), both schemes perform very well on all frequencies, and moving people (Scenario II) do not seem to have a strong impact, especially in case of PFB. Variations in the success rate across the different frequencies appear in Scenario III (antenna rotation) and become dramatic in Scenario IV (obstructing metal panel): here the reception is completely annihilated on some frequencies, while on others the success rate exceeds 90%. In other words, by hopping across different frequencies one can eventually achieve successful reception with very high probability, at the cost of some delay, even in the most adverse conditions (Scenario IV). This holds true for both PFB and ZC, but it is clear from Fig. 11 that the number of frequencies with non-null reception is larger for PFB, hence the number of attempts (or, equivalently, the delay) until the final successful reception will be smaller.

Finally, we found that almost all failed receptions were due to the frame going completely undetected (Missed Frame), with only a handful of instances of frames detected but decoded with bit errors (Erroneous Frame). This is a further confirmation that in all four scenarios the potential improvement achievable by FEC would be negligible.

C. Ranging Measurements

In the last set of experiments, we aim at assessing the listening range, i.e. the maximum distance at which an energized Tag can be decoded by our GNU Radio Listener. In order to reduce interference and multipath, we placed the Reader, Tag and Listener outdoor in a large and isolated farm field. The three elements were arranged in the same topology of
TABLE II

<table>
<thead>
<tr>
<th>Downlink (R → T)</th>
<th>Unit</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader TX power</td>
<td>26</td>
<td>dBm</td>
</tr>
<tr>
<td>Reader antenna gain</td>
<td>5.5</td>
<td>dBi</td>
</tr>
<tr>
<td>Tag antenna gain</td>
<td>2</td>
<td>dBi</td>
</tr>
<tr>
<td>Path loss @ r=2.4m, f=866.5 MHz</td>
<td>39</td>
<td>dB</td>
</tr>
<tr>
<td>Polarization loss factor</td>
<td>3</td>
<td>dB</td>
</tr>
<tr>
<td>Tag RX power</td>
<td>-8.5</td>
<td>dBm</td>
</tr>
<tr>
<td><strong>aggregated</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SNR</strong></td>
<td></td>
<td><strong>SNR</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uplink (T → L)</th>
<th>Unit</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag reflection-efficiency loss</td>
<td>5</td>
<td>dB</td>
</tr>
<tr>
<td>Tag antenna gain</td>
<td>2</td>
<td>dBi</td>
</tr>
<tr>
<td>Listener antenna gain</td>
<td>5.5</td>
<td>dBi</td>
</tr>
<tr>
<td>Path loss @ d=45m, f=866.5 MHz</td>
<td>64</td>
<td>dB</td>
</tr>
<tr>
<td>Polarization loss factor</td>
<td>3</td>
<td>dB</td>
</tr>
<tr>
<td>Listener RX power</td>
<td>-73</td>
<td>dBm</td>
</tr>
<tr>
<td>USRP sensitivity for SNRmin=4 dB</td>
<td>-84</td>
<td>dBm</td>
</tr>
<tr>
<td>Estimated sensitivity degradation</td>
<td>11</td>
<td>dB</td>
</tr>
</tbody>
</table>

![Image](image_url)

**Fig. 12.** Measured Listening range in a free outdoor area.

Fig. 2 and the Listener-Tag distance $d$ was increased in steps of 5 meters. The Reader and Listener antennas and the Tag were kept at height of 2 meters above the terrain in order to avoid obstructing the first Fresnel zone. This justifies the use of free-space loss attenuation in the link-budget computation reported in Table II. For each measurement point we instructed the Reader to repeatedly interrogate the Tag hopping in round-robin across the same five frequencies considered in the previous experiments. In order to quantify the Listener performance, we averaged the following quantities across all the reading cycles: (1) fraction $L_{ok}$ of successfully decoded messages with correct CRC; (2) fraction $L_{crcf}$ of received messages with erroneous CRC; (3) fraction $L_{miss}$ of missed frames (undetected preamble). Clearly $L_{ok} + L_{crcf} + L_{miss} = 1$.

The measured values are reported in Fig. 12 for PFB. For the sake of comparison we also report the value of $L_{ok}$ measured with ZC (red line). In our measurements, the success rate $L_{ok}$ for PFB remains above 80% up to 35 meters, and falls sharply to zero beyond 40 meters. At 40 meters, i.e. at the point of transition, the majority of the frames are detected but incorrectly decoded ($L_{crcf} = 60\%$). At 45 meters and beyond all frames go completely undetected. With ZC the range of successful reception is between 25-30 meters.

At this point, it is natural to ask the question: what is the limiting factor for the uplink range? We focus on the PFB scheme and note that the SNR measured on the detected frames at the distance $d = 40$ meters was still around 4 dB, a value which would be sufficient to guarantee 100% successful decoding according to our previous experiments with artificial noise (ref. Fig. 6 and Fig. 9). This is a first indication that noise is not the limiting factor. After some investigations we concluded that the range limiting factor is the loss of receiver sensitivity due to the presence of the strong CW from the Reader. This problem, often encountered in the design of RFID receivers [38], is caused by the saturation of the Analog-to-Digital-Converter (ADC) dynamic range due to CW leakage. Recall that the input signal to the Listener is the sum of a strong CW from the Reader plus a weaker signal from the Tag, and at 40 meters the Tag signal is received 40 dB below the CW. The dynamic range of the receiver front end must adapt (via the Automatic Gain Control, AGC) to the peak amplitude of the total input signal, but since the latter is dominated by the CW the “useful” Tag signal gets lost into quantization noise. In a recent paper [39], this effect was considered equivalent to an increase of the receiver Noise Figure (NF). Therein, the authors quantify experimentally in 11-15 dB the NF degradation in traditional Readers affected by CW leakage. Our experiments are in good agreement with this value: from the detailed link-budget computation reported in Table II we estimate a loss of sensitivity due to CW around 11 dB.

Note that it is not possible to compensate such effect in the digital domain, e.g. by canceling the (known) CW signal, since the loss of information occurs already in the ADC. A possible way to lift this limit is to employ an ADC with more bits. Another possible approach is to cancel (at least partially) the CW from the Reader. This problem, often encountered in the design of RFID receivers [38], is caused by the saturation of the Analog-to-Digital-Converter (ADC) dynamic range due to CW leakage. Recall that the input signal to the Listener is the sum of a strong CW from the Reader plus a weaker signal from the Tag, and at 40 meters the Tag signal is received 40 dB below the CW. The dynamic range of the reader front end must adapt (via the Automatic Gain Control, AGC) to the peak amplitude of the total input signal, but since the latter is dominated by the CW the “useful” Tag signal gets lost into quantization noise. In a recent paper [39], this effect was considered equivalent to an increase of the receiver Noise Figure (NF). Therein, the authors quantify experimentally in 11-15 dB the NF degradation in traditional Readers affected by CW leakage. Our experiments are in good agreement with this value: from the detailed link-budget computation reported in Table II we estimate a loss of sensitivity due to CW around 11 dB.

VI. CONCLUSIONS

In this study, we have presented a GNU Radio implementation of a low-cost RFID Listener and used it to measure the reception performance of signals backscattered by a Tag interrogated by a separate Reader. During our measurements, we found that Timing Recovery is a critical block of the
receive chain. The analysis of bit-error statistics obtained experimentally revealed that the PFB scheme has excellent performance, yielding error patterns that are close to the ones of an ideal AWGN channel with perfect synchronization. Instead, the most common Mueller-and-Muller scheme remains largely sub-optimal, probably due to the peculiarity of the source signal in this context, that is originated by ultra-low-cost Tags with unstable clock.

Our open-source SDR Listener is freely available from [9]. It can be used as a flexible, powerful and cheap measurement tool for commercial RFID systems. In this study, we have used it to investigate the impact of multipath on the reception of Tag signals for different indoor scenarios. We found that the the problem of frequency nulls becomes serious if metal objects placed between the Tag and the receiver, but frequency hopping can eventually ensure successful reception (after some attempts). We also showed that our SDR Listener can correctly receive Tag signals at distance of 35 meters without highly directional antennas.

Besides serving as a measurement tool, our SDR Listener can be used as a platform for real-world testing of signal processing techniques, e.g. some recently proposed collision recovery schemes [5], [6].

REFERENCES


