Detection of radio receivers: An experimental evaluation approach

J. Manco-Vásquez, J. Ibáñez, J. Vía, I. Santamaría
E-mail: {juliocesar, jesus, jvia, nacho}@gtas.dicom.unican.es
Dept. of Communications Engineering, University of Cantabria, Spain

***Abstract*— This paper considers the problem of detecting extremely low power emissions due to local oscillator (LO) leakage. This challenging problem arises in cognitive radio (CR) networks when trying to detect a primary user in reception mode (the hidden node problem), and also in physical layer security applications when trying to determine the presence of an eavesdropper. In contrast to the numerous works on the detection of an active radio transmitter, the problem addressed in this paper still requires further research. As a matter of fact, previous studies focus on the theoretical analysis of the detection strategies, and the reported performances do not take into account the additional limitations imposed by the existing hardware technologies. In this paper, we provide an experimental evaluation of two different detectors based on the averaged periodogram or the total energy, respectively. Moreover, we propose practical guidelines to overcome the hardware limitations and maximize the detection performance. Our experimental measurements using Universal Software Radio Peripheral (USRP) boards reveal that the widely employed energy detector is outperformed by the periodogram-based detector.**

I. Introduction

A key component of any practical CR system consists on a spectrum sensing procedure able to detect the temporal and spatial "holes" or, equivalently, the parts of the spectrum which are actually exploited by primary transmitters. Recent works on the subject focus on the detection of (moderately) weak signals from primary transmitters, and nowadays the detection of primary transmitters can be viewed as a (partially) solved problem [1]–[3]. On the other hand, the detection of primary receivers is a much more challenging and less explored problem, which has recently attracted research interest [4]–[7]. For instance, it is also becoming a subject of research for physical layer security applications, where the detection of a eavesdropper operating in reception mode is required, since it aims to extract private information from a legitimate transmitter-receiver pair [7].

In this work, we explore the possibility of detecting primary receivers by exploiting the LO power leakage emitted by the RF front end. This feature is believed to be employed for the detection of TV license fee evaders in United Kingdom [8]. In fact, the feasibility of a primary receiver detection technique based on the LO leakage is addressed in [4], where a low cost sensor placed in close proximity to the primary receivers provides a proof-of-concept. Based on this approach, reported studies in [5]–[7] propose and evaluate novel algorithms in more complex scenarios. However, these studies overlooked the real-life hardware constraints, which could lead to misleading conclusions on the performance of the proposed innovative schemes. Thus, the inclusion of all the relevant features of LO leakage signals will allow us to establish more precise tradeoffs between detection range and accuracy, in order to show the feasibility of LO detection.

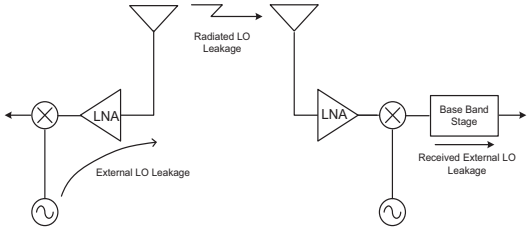

Fig. 1. Scenario: Radiated LO leakage and the measuring device

This paper is organized as follows: A description of the LO leakage signal model and the proposed statistical tests are presented in Section II. General guidelines for the experimental evaluation are exposed in Section III. We provide a detailed description of the experimental setup and the obtained results in Section IV. Finally, our main conclusions are summarized in Section V.

II. LO Leakage Detection

In a modern radio receiver with a direct conversion architecture, the incoming RF signal is converted directly down to baseband. In this down-conversion stage, a LO tuned to a certain frequency is mixed with the RF signal. However, an unavoidable leakage in the LO provokes that a small fraction of LO power is radiated out of the antenna as it is shown in Fig.1. This leakage signal is radiated to the environment by any radio regardless of the underlying architecture and is generally very weak. For instance, according to the authors of [7], [9], [10], it varies between -90dBm and -50dBm at the receiver antenna port and it can be further boosted for multi-antenna receivers. [1].

[1]Notice that in the demodulation of a LO leakage signal, we will have our own LO leakage signal altogether with the measured one. However, here we only focus on the external LO leakage since our own LO leakage can be easily identified during previous measurements, or it can be assumed to be known.

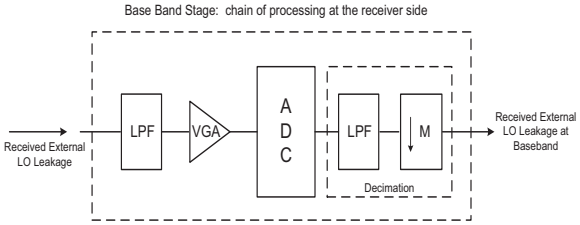

Fig. 2. Measuring device at baseband: LO leakage at baseband.

A. LO Leakage Signal Model

Taking into account the mentioned features of a LO leakage signal, a suitable and general signal model is given by

$$s(t) \quad = \quad A_o(t)\ \cos(\omega_o(t)\, t + \phi_o(t)) \tag{1}$$

where A_o, ω_o, and ϕ_o denote the amplitude, frequency and phase of the LO leakage, respectively. In this manner, other inherent features of the LO such as the phase noise, or the LO drift, which varies slowly over time, can be better described. A more simplified signal model found in the literature is typically given by a deterministic signal with unknown parameters

$$s(t) \quad = \quad A_o \cos(\omega_o\, t + \phi_o) \tag{2}$$

where A_o, ω_o and ϕ_o are considered unknown constants. The signal model given by (2) is particularly useful for short periods of time. Therefore, we will consider these two models simultaneously to explain the obtained results.

B. Proposed Detectors

After downconversion and sampling at the Nyquist rate, the hypothesis testing problem can be written as

$$\begin{aligned} \mathcal{H}_0 \quad &: x[n] \quad = w[n], \qquad n = 0, 1, ..., N-1 \\ \mathcal{H}_1 \quad &: x[n] \quad = s[n] + w[n], \qquad n = 0, 1, ..., N-1 \end{aligned}$$

where $s[n]$ is the discrete-time version of $s(t)$ at baseband, $w[n]$ denotes the additive Gaussian noise, and N is the number of samples acquired during the sensing period. In the absence of any knowledge about the LO signal, an energy detector turns out be a suitable detector. However, some knowledge about the expected frequency range of the LO peak power can be usually incorporated into the detection procedure. In this way, an energy detector in the frequency domain is obtained as,

$$T_{ED}(\mathbf{x}) = \sum_{k=\omega_1}^{\omega_2} |X_\omega[k]|^2 > \gamma \tag{3}$$

where $\mathbf{x} = \{x[0], x[1], x[2], \ \ldots, \ x[N-1]\}$ is the set of N complex samples obtained during the sensing period, X_ω denotes the PSD of $\mathbf{x}$, and $[\omega_1 \ \ \omega_2]$ is the expected frequency range. A more tailored detector can be derived by assuming that the amplitude, frequency, and phase noise are unknown constants in (1). The statistic test under these assumptions is given by

$$T_{MP}(\mathbf{x}) = \max_{\omega \in \{\omega_1 \ \omega_2\}} I(\omega) > \gamma, \tag{4}$$

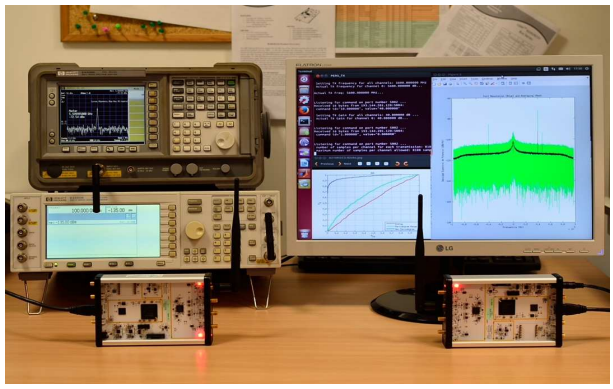

Fig. 3. Setup: B210 USRPs for emitting and measuring the LO leakage

where $I_l(\omega) = \frac{1}{L}\left|\sum_{n=0}^{L-1} x_l[n]\exp(-j\omega n)\right|^2$,

$$I(\omega) = \frac{1}{N_w}\sum_{l=1}^{N_w} I_l(\omega)$$

is the averaged (over N_w windows of length L) periodogram, and T_{MP} denotes the maximum of the averaged periodogram.

III. Measurement Methodology

The detection of a very low-power LO leakage signal requires the selection of the sensing parameters providing maximum sensitivity, and it consists of setting the maximal gain at the measuring device, and at the same time, a large time of acquisition. Moreover, it poses stringent requirements on the transceiver hardware. For instance, the bandwidth must be wide enough to account for uncertainty in the frequency of the LO leakage, while at the same time narrow enough to allow large sensing periods. This bandwidth can be usually known in advance, since it is given by the maximal clock error between the external LO leakage and the LO associated with the measuring device [2].

Setting the Gains and Sampling Rate: In order to provide the maximum sensitivity, the receiver architecture must be taken into account (See Fig. 2). The gain of a variable gain amplifier (VGA) may lead the signal to saturation after the ADC. In fact, after the ADC the signal undergoes a process of decimation that involves two stages: a low-pass filter followed by a downsampling of the signal. This process can mask the saturation, and thus the establishment of the right gain to be applied in the VGA and LNA without provoking saturation should avoid any process after the ADC. For this reason, it is advisable to utilize the smallest possible decimation factor to identify the maximum gain. In addition, this gain should allow us to have a suitable margin for the detection of the LO leakage signal even when its power is below the noise level.

[2] As an indicative example, the standard IEEE 802.11 a/g/n specifies that the clock error shall be ± 20 ppm maximum for the 5 GHz band and $\pm$ 25 ppm maximum for the 2,4 GHz band. Thus, depending on the operating carrier frequency, the required bandwidth is directly proportional to the employed sampling frequency F_s and the maximum clock error in ppm.

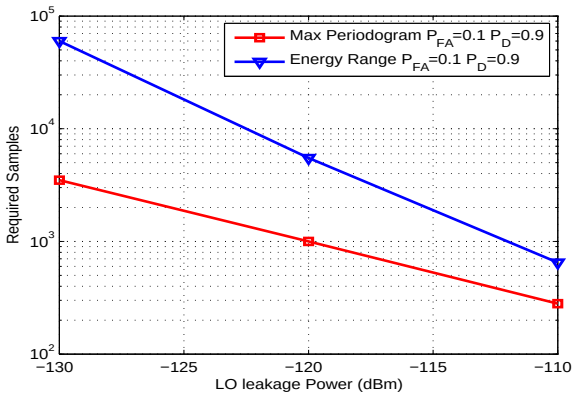

Fig. 4. N versus LO leakage power: The number of required samples to achieve a $P_D = 0{,}9$ and $P_{FA} = 0{,}1$, with $F_s = 520$ kHz and a receiver gain of 73dB for two detectors

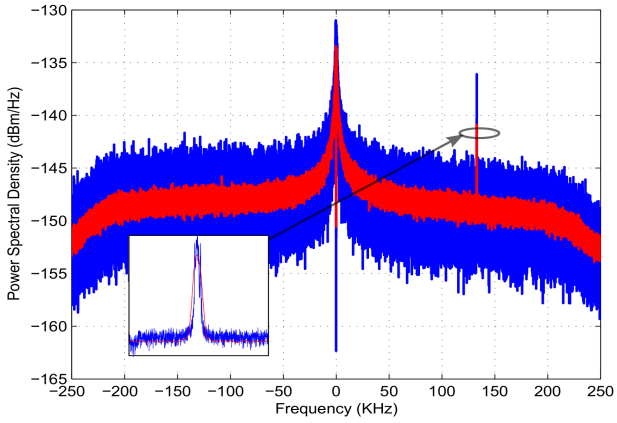

Fig. 5. Measurement under hypothesis H_1: Average PSD of the noise signal measured by a B210 USRP, with a $F_c = 5{,}6$ GHz, $F_s = 520$ kHz, $N =$ 10e6, $L =$ 1e6 in blue, and $L =$ 10e4 in red, for a distance of 50cm.

On the other hand, long sensing periods of time involve low sampling rates F_s and large values of captured samples N. The sampling rate is given by $F_s = ADC_{clock}/M$, where ADC_{clock} refers to the sample rate of the ADC, and M to the decimation factor. Therefore, low values of ADC_{clock} are desirable, and higher decimation factors M would then be considered depending on the selected values for the ADC_{clock}. Nevertheless, hardware impairments impose even more restrictions around a DC frequency where we expect to have a peak power corresponding to the radiated LO. For instance, due to the own internal leakage, DC offsets, filter transients, AC coupling, and high pass filters. For that end, we demodulate the received signal with a frequency offset f_o far from the frequency range $[0 \quad \pm\rho]$, where ρ is around some kHz (e.g. $\rho = 18$ kHz for a B210 USRP). By doing this, a peak power centered around f_o is observed, while the spectrum corresponding to the noise remains almost flat avoiding the aforementioned hardware impairments. Hence, based on these new restrictions, the sampling rate should be selected according to $F_s \geq 2(\rho + w_2 - w_1)$ to avoid hardware impairments and at the same time cover the expected bandwidth of the LO signal given by ω_1 and ω_2. Finally, the non-ideality of the RF part also introduces some undesirable spikes which can be easily characterized to discard them (they remain at the same frequency positions over time) during the detection procedure.

IV. Experimental Results

We consider two setups: An initial configuration using a signal generator and a B210 USRP connected by means of a cable; and a practical configuration based on two B210 USRPs and OTA transmissions to provide a proof concept for the proposed detectors. Taking into account the previously described guidelines which are independent of the particular board (e.g. the same procedure can be applied to the N210 USRP). A B210 USRP is configured with a $F_c = 5{,}6$ GHz and a receiver gain of 62dB. We consider a guard frequency range around DC of $\rho = 18$ kHz, and a LO drift $w_2 - w_1 =$ 224 kHz (i.e. 40 ppm at 5,6 GHz), which makes us set a $f_o = 130$ kHz and an approx. $F_s = 520$ kHz given by an $ADC_{clock} = 25$Msps with $M = 48$.

A. *Setup 1: Signal Generator and B210 USRP*

The generation of the radiated LO leakage is emulated by a Agilent E4438C ESG Vector Signal Generator to start characterizing both the USRP and the radiated LO leakage. In Fig.4, we show the required number of samples to achieve a given performance in terms of the detection and false alarm probabilities versus the LO leakage power. As can be seen, the detection procedure based on the averaged periodogram (T_{MP}) is able to achieve the required performance with a reduced number of samples (and therefore a shorter sensing period). This is due to the fact that the signal model assumed for this detector is closer to the particular characteristics of the LO leakage signal. Moreover, it can be seen that for lower LO leakage powers, the measured slope of a T_{MP} detector indicates that it would be a feasible detector for applications with more stringent requirements in sensing time or capacity of storage, while having an affordable computational cost.

B. *Setup 2: Measurements between two B210 USRPs*

With OTA measurements between two B210 USRPs, we observe that the received leakage power has a bandwidth of 10 Hz for short periods of time (e.g. 20 milliseconds), and a bandwidth of approximately 120 Hz for longer periods of time (e.g. 2 or more seconds). Such LO inaccuracies can be better explained with the signal model given in (1). By connecting two USRPs with a cable, the LO leakage power measured at the output port was found to be -96 dBm. The PSD of the captured signals in the presence of an external LO leakage is shown in Fig. 5 which also supports our mentioned

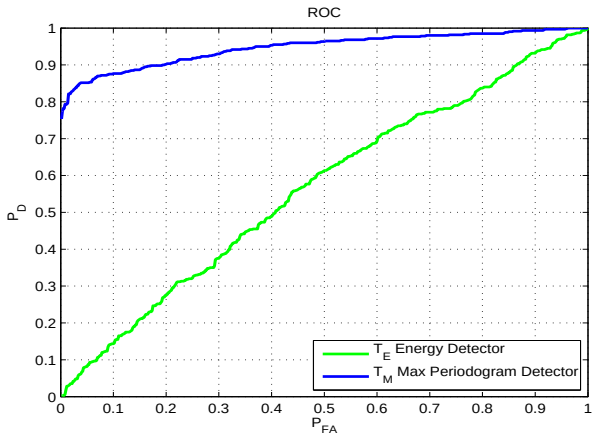

Fig. 6. ROC curve P_D versus P_{FA} for two detectors, with a $F_c = 5{,}6$GHz, $F_s = 520$ kHz, $N = 40$e4, a receiver gain 62dB, for a distance of 50cm, and a radiated LO leakage

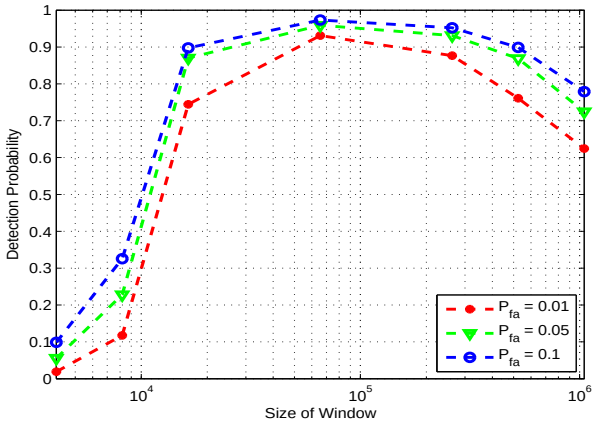

Fig. 7. Detection probability versus L: P_D versus the size of the window L in the periodogram for the T_M detector, with a $F_c = 5{,}6$GHz, $F_s = 520$ kHz, and $N = 1$e6, and for a distance of 10cm

observations about the bandwidth of the LO leakage [3]. As can be seen, the LO leakage is found around 136 kHz, which is partially due to our choice of frequency offset $f_o = 130$ kHz for avoiding the effects in the frequencies close to DC.

The practical performance of the proposed detectors is first evaluated by means of the receiver operating curve (ROC), which is shown in Fig. 6. In this experiment, the two B210 USRPs are separated a distance of $d = 50$ cm. Our results show that the energy detector (T_{EN}) is clearly outperformed by the method based on the averaged periodogram (T_{MP}).

Finally, we analyze the effect of the window length L on the performance of a T_{MP} detector. The results are shown in Fig. 7, where we can see that the performance of the proposed periodogram-based detector is not very sensitive to this parameter. Obviously, very low values of L make the proposed procedure similar to the energy detector. On the other hand, a too large value of L does not allow the reduction of the noise impact due to the averaging, and at the same time leads to an excessive increase of the frequency resolution, thus losing the ability of "integrating" on the frequency range of the LO leakage signal.

V. Conclusions

In this paper, we have evaluated the performance of two techniques for the detection of the LO leakage of an external receiver. We conducted some preliminary experiments with a signal generator and a B210 USRP device to check the performance of the proposed techniques in favorable situations. As a consequence of these experiments, we have been able to identify some departures from the ideal conditions, and also to provide guidelines for the optimal selection of the main parameters involved in the experimental setup. A second set of more realistic experiments, based on OTA transmissions, allowed us to conclude that the idea of detecting receivers by exploiting their LO leakage is practically feasible. Moreover, we have corroborated that a relatively simple technique, based on the averaged periodogram, is able to accurately exploit the spectral properties of the LO leakage signal, as well as its particularities due to the imperfections of the involved hardware.

[3]We employ the Welch method to estimate the PSD. This method divides the signal into several segments of length L which are weighted by a window (e.g. a Hamming window) that reduces the sidelobes. Finally, these segments are averaged discarding unwanted spurious emissions.

References

[1] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, First 2009.

[2] D. Cabric, A. Tkachenko, and R. Brodersen, "Spectrum sensing measurements of pilot, energy, and collaborative detection," in *Proc. of IEEE Military Communications Conference (MILCOM)*, Oct 2006, pp. 1–7.

[3] L. Lu, X. Zhou, U. Onunkwo, and G. Li, "Ten years of research in spectrum sensing and sharing in cognitive radio," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 28, 2012.

[4] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks DySPAN*, Nov 2005, pp. 124–130.

[5] S. Park, L. Larson, and L. Milstein, "Hidden mobile terminal device discovery in a UWB environment," in *IEEE International Conference on Ultra-Wideband*, Sept 2006, pp. 417–421.

[6] P. Sanghoon, L. Larson, and L. Milstein, "An RF receiver detection technique for cognitive radio coexistence," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 8, pp. 652–656, Aug 2010.

[7] A. Mukherjee and A. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 2012, pp. 2809–2812.

[8] (2014, September) Tv detection. [Online]. Available: http://www.bushywood.com/tv_detector_vans.htm

[9] N. C. Hamilton, "Aspects of direct conversion receiver design," in *Fifth International Conference on HF Radio Systems and Techniques*, Jul 1991, pp. 299–303.

[10] R. Wolff, "An assessment of the potential terrestrial interference due to direct broadcast satellite television receivers," *IEEE Journal on Selected Areas in Communications*, vol. 3, no. 1, pp. 148–154, January 1985.