Signal detection using watermark insertion
Matthieu Gautier, Dominique Noguet

To cite this version:
Signal detection using watermark insertion

Matthieu Gautier and Dominique Noguet
1IRISA, INRIA, University of Rennes, France
2CEA-LETI, Minatec, Grenoble, France
matthieu.gautier@irisa.fr, dominique.noguet@cea.fr

Abstract—This paper analyses signal detection using watermark insertion, which is artificially embedded into the digital modulated signal. When a signal does not contain intrinsic information, its detection is hard to achieve using blind detectors. For that kind of signals, we propose to insert a low-power watermark that will be detected by a matched filter based detector. The system design is a trade-off between the watermark insertion strength (i.e., reducing the transmission quality) and the detection sensitivity. This trade-off is discussed in this paper and simulations results show the advantage of the watermark insertion.

I. INTRODUCTION

Cognitive radio systems [1] can use different approaches to determine the spectrum occupancy. The first is to query a database of the positions of the radio transmitters and their parameters (power, frequency) in order to deduce a map of the spectrum occupation. Another approach is to directly detect the signals using spectrum sensing techniques. If the first can protect perfectly the incumbents, it cannot help the management of resource allocation among opportunistic users. Detection techniques must be specifically adapted to the opportunistic users. The detection of opportunistic users may be considered by the joint approach of the design of the physical layer of opportunistic users and the design of their detection.

In the literature, many detection techniques have been proposed [2]. Those that offer the highest levels of sensitivity for a given detection time are those that use a priori information of the signal. However, some signals do not contain many intrinsic signatures, in that case only blind algorithms can detect them, such as the energy detector [3].

The solution proposed in this paper relies on the following: the detection can be assisted by the explicit introduction of a specific signature (or watermark) in the transmitted signal. The introduction of signatures in the transmitted signal has already been addressed in the literature [4][5]: they propose to insert cyclostationary signatures on some carriers of the signal to obtain an efficient detection of the signal. These solutions are highly dependent on the modulation used (OFDM [6], FilterBank MultiCarrier (FBMC) [7], ...) and reduce the spectral efficiency of the system. Unlike [4][5], the proposed scheme is to insert a signature independent of the modulation used. It does not insert cyclostationary features into the signal but adds a watermark [8][9]. The detection scheme differs from conventional detectors because it relies on the detection of the watermark, not the detection of the useful signal.

In our approach, the watermark is inserted with a very low power not to alter the signal significantly. Thus, a receiver must be able to demodulate the signal without any knowledge on the watermark. Only the detector uses the watermark to detect the signal.

This paper consists of 5 parts. Section II describes the system model and introduces the watermark based detector. In Section III, a theoretical analysis of the detector is introduced in order to set the system. Simulation results are given in Section IV. Finally, conclusions are drawn and outlook is provided.

II. SYSTEM MODEL

In order to introduce the system, we consider the study case where an opportunistic user “User 1” wants to use the spectrum white spaces of incumbent systems. Before performing its communication, this user want to detect whether or not the free bands are already occupied by another opportunistic user “User 2”. The principle of the proposed detection is to insert a watermark in the transmitted signal and to use this watermark to help the detection of User 1 by other opportunistic users.

Fig. 1 describes the system model of the watermark insertion in the signal of User 1 and its detection by User 2. Two communication paths are described:

- the transmission of User 1 through Channel 1 in order to test the influence of the watermark insertion on the quality of the User 1 demodulation,
- the transmission of User 1 through Channel 2 in order to test the quality of the detection of User 1 by User 2.

Under specific circumstances where User 2 wants to detect and demodulate the modulated signal, Channel 1 and Channel 2 are identical.

A. Watermarking the transmitted signal

The proposed watermarking scheme is inspired from the watermarking of audio signals described in [9] where the hidden information is embedded inside into an audio signal. The watermarking consists in adding the signal w(t) with

![Fig. 1. System model of the watermark insertion in the signal of User 1 and its detection by User 2.](image-url)
the signal \( s(t) \) as shown in Fig 1. The watermark power being normalized \( \sigma_w^2=1 \), the power of the watermark insertion in the signal \( s(t) \) depends only on the coefficient \( \alpha \) and is characterized by the ratio WSR (Watermark to Signal Ratio) given by:

\[
WSR = 10. \log_{10} \left( \frac{\alpha^2}{\sigma_n^2} \right),
\]

with \( \sigma_n^2 \) the power of the transmitted signal.

Considering the transmission between the modulation and the demodulation of User 1, the Signal-to-Noise Ratio (SNR) in an AWGN (Additive White Gaussian Noise) channel characterizes the transmission quality by:

\[
SNR = 10. \log_{10} \left( \frac{\sigma_s^2}{\sigma_n^2 + \alpha^2} \right),
\]

with \( \sigma_n^2 \) the noise power.

**B. Watermark detection**

The watermark inserted into User 1 should improve its detection by other users. The aim of the detector is to detect the presence of the watermark, not to detect the signal itself. Thus, the detection can be stated as the following hypothesis (in the case of an AWGN noise \( n_2(t) \)):

\[
H_0 : r_2(t) = n_2(t) \\
H_1 : r_2(t) = s(t) + \alpha w(t) + n_2(t),
\]

where \( H_0 \) is the null hypothesis for the event “free band” and \( H_1 \) is the alternative hypothesis for the event “occupied band”. The detection is performed by the matched filter to the watermark. The correlation between the received signal and the watermark is computed so that the receiver must know the watermark. The output of the correlation \( u \) is given by:

\[
u = \frac{\langle r_2, w^* \rangle}{N_s} = \begin{cases} 
\frac{\langle n_2, w^* \rangle}{N_s} & \text{if } H_0, \\
\frac{\langle s, w^* \rangle}{N_s} + \alpha & \text{if } H_1.
\end{cases}
\]

\( N_s \) is the detection duration i.e. the number of samples used to compute the correlation.

Finally, the decision variable \( T \) is computed:

\[
T = \max \left( E[u] \right),
\]

where \( E[u] \) is the mathematical expectation operator.

**C. Implementation issues**

In a practical implementation, the watermark will be inserted in the baseband signal just before the digital to analog conversion (DAC). Fig. 2 shows the digital model used to test our detection scheme. At the transmitter side, a pattern code \( c(t) \) is repeated to generate the infinite-duration signal \( w(t) \). The digital expression of \( w(t) \) is:

\[
w[n] = c \ast \delta_L[n] \quad \text{with} \quad \delta_L[n] = \sum_{k=-\infty}^{+\infty} \delta[n-kL],
\]

with \( L \) the number of samples of the code \( c[n] \) and, \( \delta \) and \( \delta_L \) the Dirac and the Dirac comb functions respectively.

The choice of the code is important. It is characterized by its length \( L \) and must have good auto-correlation/cross-correlation properties to be easily detectable. It must also be uncorrelated with the useful signal.

In our simulations, we first consider that the watermark is a Gaussian random sequence i.e., \( w(t) \sim N(0, \sigma_s^2) \). This leads to ideal autocorrelation property. Then, we used the codes of literature conventionally used in spread spectrum systems [10] as the UMTS i.e. the Hadamard codes. These codes are orthogonal, however this feature is not essential and, we could also use pseudo-random codes, non-orthogonal, such as the Gold codes.

To set the system, the most important parameter is the insertion power \( \alpha \) characterized by the ratio WSR defined in (1). This ratio should be as low as possible so that the insertion has the least influence on the useful transmitted signal. Typically, the simulation results show that a ratio of -15 dB does not degrade system performance (see Section 3).

At the signal detection side in Fig. 2, the correlation between the received signal and the code used at the transmitter side is performed. Then the expectation operation in (5) is estimated. The correlation \( u[n] \) is computed using the matched filter of the code:

\[
u[n] = r_2 \ast c^*[n].
\]

The expectation operation is performed by a first order IIR (Infinite Impulse Response) filter \( A_N \):

\[
A_N[n] = \sum_{k=0}^{N} \delta[n-kL].
\]
The length of the filter is $N$ and is directly responsible of the signal duration needed to provide the decision. 

$L$ is the number of taps of the matched filter, the number of samples $N_s$ used for the detection is:

$$N_s = N \times L.$$  \hspace{1cm} (9)

By increasing $N$, the accuracy of the estimation is improved and therefore the algorithm can detect the presence of the watermark with a lower $SNR$. Fig. 3 illustrates how the detector operates by showing the output of the averaging filter.

Once the average performed, we come to the decision by comparing the maximum output of the filter to a decision threshold $\lambda$.

### III. THEORETICAL PERFORMANCE

This section presents the theoretical performance of the proposed system and a validation with simulation results. These results are important to set the system’s parameters.

#### A. Watermark insertion sensitivity

First, the influence of the watermark on the transmission quality of User 1 must be evaluated. Taking Gaussian assumptions ($s(t) \sim N(0, \sigma^2_s)$), theoretical Bit Error Rate ($BER_{th}$) is:

$$BER_{th} = \frac{1}{2} \text{erfc} \left( \sqrt{\frac{E_b}{N_0 + 2\alpha}} \right),$$  \hspace{1cm} (10)

with $E_b$ the energy per bit, $N_0$ the spectral density of the noise $n_1(t)$ and $\text{erfc}$ the well known complementary error function. Fig. 4 shows the theoretical BER for different $WSR$. Performance are compared with simulation results. For the simulations, the signal $s(t)$ is an OFDM modulation with 4-QAM non-coded symbols per subcarriers. The number of subcarriers is set to 1024, producing a zero-mean Gaussian signal due to the central limit theorem [6]. The watermark $w(t)$ is also a Gaussian signal.

Fig. 4 shows that the simulation performance perfectly match the theoretical curves. The results show that the watermark insertion leads to a $E_b/N_0$ degradation lower than 1 dB (for a target BER of $10^{-3}$) and for $WSR$ less than -15 dB.

#### B. Signal detection characteristics

The performance of the watermark detection are evaluated. Taking Gaussian assumptions for the signal, the code and the noise, the correlation output statistics could be derived from (4):

$$u \sim \begin{cases} N(0, \sigma^2_n) & \text{if } H_0, \\ N\left(0, \frac{\sigma^2_s + \sigma^2_n}{N_s}\right) + \alpha & \text{if } H_1. \end{cases}$$  \hspace{1cm} (11)

Fig. 5 shows the density of probability of the correlation output $u$ for both hypothesis $H_0$ and $H_1$ (with $N_s=128$, $WSR=-5$ dB and $SNR=-15$ dB). $H_0$ density average is 0 while $H_1$ density average is $\alpha \times N_s=51$ samples.

The probability of detection $p_D$ depends directly on the choice of the detection threshold $\lambda$. This choice is a tradeoff between false alarms and good detections as shown in Fig 5. Non-detections represent the red area on Fig. 5.
The watermarking is performed using an Hadamard code with 11.5 dB for a WSR of -15 dB and for several duration of detection N. In both results, the fixed threshold leads to a false alarm probability of 10%.

Simulations results in Fig. 7 show that the watermark allows the detection of signals with SNR down to -20 dB could be detected. 

**IV. SIMULATION RESULTS**

In this section, FBMC modulation with 256 subcarriers is performed on 4-QAM non-coded symbols. It has been shown [11] that this modulation is a good candidate for the secondary use of the spectrum. Furthermore, this modulation suffers from its lack of cyclostationary features so being a good study case for the watermarking technique proposed herein. The watermarking is performed using an Hadamard code with L=1024.

The main feature of a detector is its sensitivity level expressed in SNR. In the following, the sensitivity is the minimum SNR that the detector could sense with $P_d = 95\%$ and $P_{fa} = 10\%$.

The first results shows how increasing the detection sensitivity using 2 parameters of the systems: the insertion strength WSR and the detection time N. Simulation results are introduced in Fig. 7 and Fig. 8. Fig. 7 shows the detection probability as a function of SNR for several insertion strengths WSR and N=1. Fig. 8 shows the detection probability as a function of SNR for a WSR of -15 dB and for several duration of detection N. In both results, the fixed threshold leads to a false alarm probability of 10%.

Fig. 6 shows the theoretical $P_{fa}$ and the theoretical $P_{nd}$ for different WSR. Performance are compared with simulation results. The simulation settings are the same as for Fig. 4. The detector uses $N_s = 8192$ samples with a code length $L = 1024$. 

**Fig. 6.** False alarm probability and non-detection probability versus detection threshold $\lambda$.

**Fig. 7.** Detection probability versus $SNR$ for different WSR.

**Fig. 8.** Detection probability versus $SNR$ for different integration time $N$. 

Finally, the detection probability $P_d$ is given by:

$$P_d = 1 - P_{nd}. \quad (14)$$

False alarms represent the blue area on Fig. 5. The theoretical false alarm probability is given by:

$$P_{fa} = Prob(c \geq \lambda|\mathcal{H}_0) = \frac{1}{2} \text{erfc} \left( \frac{\lambda}{\sqrt{2} \sigma_n^2 \sqrt{N_s}} \right). \quad (15)$$

**Fig. 6.** False alarm probability and non-detection probability versus detection threshold $\lambda$.
tivity in $SNR$ as a function of the integration time $N$ for both watermark detector and energy detector. The sensitivity increases faster for the watermark detection than for the energy detection. Thus, for an integration time higher than 8, the watermark detector outperforms the energy detector. For $N = 16$, a 3.4 dB gain is achieved.

V. CONCLUSIONS

This paper proposes the initial study of a new signal detector for cognitive radio systems. It detects the watermark that has been inserted in the transmitted signal at a very low power. Theoretical performance and implementation discussion allow the setting of the system through the tradeoff between the signal detection performance and the degradation of the communication quality. In realistic conditions, simulation results show that the proposed detector outperforms the energy detection and could detect $SNR$ down to -11 dB with a reasonable detection duration.

Future work is to include the proposed technique in a cooperation scheme among secondary users. All opportunistic users will be watermarked and will use this signature to allocate free spectrum in a fair and efficient way.

ACKNOWLEDGMENT

The research leading to these results was derived from the European Community’s Seventh Framework Program (FP7) under Grant Agreement number 248454 (QoSMOS).

REFERENCES