Defense against Jamming Attacks in Wide-band Radios using Cyclic Spectral Analysis and Compressed Sensing

T. Nawaz*, L. Marcenaro and C. S. Regazzoni
Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture - DITEN
University of Genova, Italy.
Email: tassadaq.nawaz@ginevra.dibe.unige.it

Abstract—Cognitive radio (CR) is an enabling technology for future wireless spectrum allocation to improve the use of licensed spectrum by enabling unlicensed users equipped with CRs to coexist with incumbent users in licensed spectrum bands while causing no interference to incumbent communication. However, security challenges faced by CR technology are still a research topic. One of the prevailing challenges, is the radio frequency jamming attack, where adversaries are able to exploit on-the-fly reconfigurability potentials and learning mechanism of cognitive radios in order to devise and deploy advanced jamming tactics. These attacks can significantly impact the performance of wireless communication systems and lead to significant overheads in terms of retransmission and increment of power consumption. In this work, a new jammer detection algorithm is proposed for wide-band (WB) radios. The proposed approach assumes a WB spectrum occupied by various narrow-band (NB) signals, which can be either legitimate or jamming signals. First, the received WB signal is recovered from sub-Nyquist rate samples using compressed sensing. Compressed sensing is used to alleviate Nyquist rate sampling requirements at the receiver A/D converter. After the Nyquist rate signal has been recovered, a cyclostationary spectral analysis is performed on this estimated WB signal to compute spectral correlation function (SCF). The alpha profile is then extracted from SCF and used to classify each NB signal as a licit signal or illicit signal. In the end, the performance of the algorithm is shown with the help of Monte-Carlo simulations under different empirical setups.

I. INTRODUCTION

The demand for spectral resources is growing significantly as the radio communication applications become more and more widely used. In recent years, cognitive radio (CR) has attained great attention from the communication society due to its ability of allowing dynamic / opportunistic spectrum access in a spectrum sparse environment [1], [2] that provides a possible solution to spectrum scarcity problem. A CR is a radio system that dynamically interacts with the environment and adjusts its operating parameters with mission of exploiting the spectrum holes without affecting primary (licensed) user activity. To acquire the knowledge of unused spectrum holes, spectrum sensing is the elementary task needed to be performed by a CR terminal [3].

In literature, different spectrum sensing methods have been suggested for CRs, such as, energy detection (ED), cyclostationary feature detection (CFD) and matched filtering detection [4]. Among these spectrum sensing techniques, the CFD is capable of detecting the primary signal from the interference and noise even in very low signal-to-noise ratio (SNR) conditions. This performance is achieved at the cost of increased implementation complexity. ED as a non-coherent technique is easy to implement and does not need prior knowledge of signal, but fails at low SNRs, while matched filtering detector requires a dedicated receiver structure which may not be possible in a practical CR terminal. CFD uses the cyclostationarity of communication signals by detecting spectral peaks in spectral correlation function (SCF) or spectral coherence function (SOF) [5], [6]. Moreover, the cyclic spectral analysis has been used as a robust tool for signal classification when the carrier frequency and bandwidth information is unavailable [7], [8].

When the radios are operating on a wideband (WB), the sensing task become more complex high-rate sampling, analog-to-digital (A/D) requirement. Compressive sensing (CS) [9] is an interesting solution to alleviate requirements of high sampling rates provided that the signal is sparse in a given transform domain. Then, CFD needs to estimate the SCF of the received WB spectrum from sub-Nyquist samples. One approach [10] is to first recover Nyquist samples from sub-Nyquist samples, then estimate the SCF and perform feature extraction. For Nyquist samples recovery, author used modulated wideband converter (MWC) [11]. A different method is adopted in [12], to perform the SCF estimation directly from sub-Nyquist samples by exploiting the sparsity in two dimensional SCF domain.

While CR is introduced as a solution for dynamic spectrum access (DSA), it has introduced many challenges in network security owing to its capability of sensing and exploring a wide range frequencies and opportunistic usage. Due to these advancements, it is easier for the attackers to launch sophisticated attacks in such networks. For example, the attackers may pretend to be a licensed primary user, and carry out the primary user emulation (PUE) attacks [13]. The attackers can also explore the spectrum themselves, and conduct smart jamming [14], [15].
The RF jamming and anti-jamming concepts are classical in wireless communication itself, but recent advancement in CR technology has enabled devising and deploying of more advanced, self-reconfigurable jamming [16] and anti-jamming [17] solutions. Spectrum sensing information plays a key role in anti-jamming systems. This information may be used to detect potential jamming entities [18], [19] and to take proactive measures to ensure communication continuity and security. Moreover, a history of observations can be maintained and used to devise more effective anti-jamming tactics. For example, when a frequency hopping spread spectrum (FHSS) based system is considered, CR may modify its hopping sequence to avoid the channels which are occupied by potential jamming entities [20].

In most of the earlier work, that considered physical layer jamming attacks assume either tone jamming or additive white Gaussian noise (AWGN) jamming [21]. In [22] and [23], the authors analyze modulation based jamming techniques and have shown that these modulated jamming tactics can lead to optimum jamming. Therefore, in order to design the proper anti-jamming system against these attacks, there is a need for a reliable jammer detection algorithm.

In this paper, a novel algorithm is proposed for jammer detection in WB CRs. A WB spectrum is assumed to be formed by multiple sub-bands, each one occupied by a narrow-band (NB) signal. These NB signals can be legitimate signals or jamming signals. The first step of the proposed algorithm is to recover the Nyquist rate WB spectrum from sub-Nyquist samples using compressed sensing. To accomplish this, we used the conventional basis pursuit (BP) technique [24]. Once the WB signal is recovered, it is fed to the CFD to estimate the spectral correlation function (SCF). The alpha profile is extracted from SCF and then compared with corresponding values of the licit signal’s alpha profile, which are stored in a database. Based on this simple comparison, each of the NB signal is classified as a licit or jamming signal. Major advantage of CFD based detector lies in its abilities to perform better than ED at low SNR values and to differentiate different modulated signals. The performance of the algorithm is evaluated for various compression rates at low SNR to observe the effects on classification performance. To the best of our knowledge, this type of jammer detection algorithm has not been presented so far in literature. The rest of the paper is organized as follows. Section II describes the system model and problem formulation, Section III presents proposed algorithm. Experimental results are discussed in section IV. In Section V, paper is concluded along with some future research directions.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We considered a received WB spectrum of $\Delta$ Hz. This WB spectrum can be occupied by various NB signals $n \in \{1, 2, 3,...,N\}$, with different carrier frequencies and modulation types that we want to identify. The received WB signal is an aggregated time-domain signal which can be presented as:

$$r(t) = \sum_{n=1}^{N} h_n(t) \ast S_n(t) + w(t)$$  \hspace{1cm} (1)

Where $S_n(t)$ denotes the $n$-th transmitted signal, $h_n(t)$ is the channel coefficient between $n$-th transmitter and receiver, $\ast$ denotes the convolution operation and $w(t)$ is the additive white Gaussian noise (AWGN) with zero mean and power spectral density $\sigma_w^2$. We assume that NB signals can be generated by different types of modulation schemes, such as, binary frequency shift keying (BFSK), binary phase shift keying (BPSK), quadrature amplitude modulation (QAM), quadrature phase shift keying (QPSK), or any other modulation scheme as shown in Fig. 1(a). The WB is divided into multiple equal bandwidth SBs and each of these SBs can be occupied by NB signals with no spill over energy into neighboring SBs. For our proposed system, a modulated signal is considered as a jamming signal. This jammer can jam any of SBs, either occupied or free as depicted in Fig. 1. When the jammer is in free SB, it can be considered as a PUE attack. The modulated jammers are very successful for power constrained jamming in order to maximize the error probability of digital modulated legitimate signals.

Let us assume that the targeted signal is BPSK-modulated and uncoded, and that targeted system uses the coherent
detection. Then, the error probability \( p_e \) to jam the targeted signal can be given as \[25\]:

\[
p_e = Q\left(\frac{2P_r}{P_n} \left(1 - \frac{2P_j}{P_r} \sin(\theta^j)\right)\right)
\]  

Where \( P_r \) is the received power of targeted signal, \( P_n \) is thermal noise power, \( P_j \) is the jamming signal received power, \( \theta^j \) is the phase of jamming signal, and \( Q \) is the Gaussian Q-function.

### III. PROPOSED ALGORITHM

This section illustrates the proposed algorithm as a solution to the problem formed in Section II. We first introduce cyclostationary spectral analysis, then explain compressed sensing and at the end we will present our newly proposed algorithm.

#### A. Cyclostationary Spectral Analysis

A process \( x(t) \) is said to be wide-sense cyclostationary with period \( T_0 \) if its mean \( E[x(t)] = \mu_x(t) \) and autocorrelation \( E[x(t)x(t+\tau)] = R_x(t,\tau) \) are both periodic with period \( T_0 \), in such case, they can be defined respectively as:

\[
M_x(t+T_0) = M_x(t) ; \quad R_x(t+T_0,\tau) = R_x(t,\tau)
\]  

The autocorrelation function of a wide-sense cyclostationary process can be expressed in terms of its Fourier series components.

\[
R_x(t,\tau) = E[x(t+\tau/2)x^*(t+\tau/2)]
\]  

\[
R_x(t,\tau) = \sum_\alpha R_x^\alpha e^{j2\pi\alpha t}
\]  

Where, \( \alpha = \frac{\theta}{T_0} \) and \( a \) is an integer, \( E[.\) is the expectation operator, \( \alpha \) is the set of Fourier components, and \( R_x^\alpha(\tau) \) represents the cyclic autocorrelation function (CAF) and gives Fourier components. CAF is given by:

\[
R_x(\tau) = \lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{T/2} R_x(t,\tau)e^{-j2\pi\alpha t}dt
\]  

When \( R_x(t,\tau) \) is periodic in \( t \) with period \( T_0 \), \( \alpha \) can be expressed as:

\[
R_x(\tau) = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} R_x(t,\tau)e^{-j2\pi\alpha t}dt
\]  

The Fourier Transform of the CAF is known as SCF and is given by:

\[
S_x(f) = \int_{-\infty}^{\infty} R_x^\alpha(\tau)e^{-j2\pi f \tau}d\tau
\]  

Where \( \alpha \) is cyclic frequency and \( f \) is the angular frequency. The major benefit of spectral correlation is its insensitivity to background noises, since the spectral components of noise are completely uncorrelated in time due to the fact that noise is wide-sense stationary process, such noise does not play significant role in the SCF. This fact allows the spectral correlation of a signal to be accurately calculated even at low SNRs. Furthermore, different types of modulated signals (BPSK, AM, FSK, MSK, QAM, PAM) with overlapping power spectral densities have highly distinct SCFs. The SCF of WB spectrum is shown in Fig. 2. The SCF produces large amount of data which makes it hard to classify the signals in near real time. Therefore, \( \alpha \) profile is extracted from SCF, which is given by \(9\) and depicted in Fig. 3.

\[
I(\alpha) = \max_f |S_x^\alpha|
\]
B. Compressed sensing

The frequency response of the observed WB signal shown in (1) can be obtained by taking N-point discrete Fourier transform (DFT) on r(t), as follows:

\[ r_f = \sum_{n=1}^{N} D^c_h(n_s) f(n_s) + w_f \]  

where \( r_f \) is a \( N \times 1 \) vector of obtained frequency-domain samples, \( D^c_h(n_s) \) is an \( N \times N \) diagonal channel matrix, and \( h_f(n_s), s_f(n_s) \) and \( w_f \) are the frequency-domain samples of \( h_n(t), s_n(t) \) and \( w(t) \), respectively. This model is written in more generalized form as follows:

\[ r_f = H_f \vec{S}_f + w_f \]  

where \( \vec{S}_f = [(S^c_f(1)^T,...,(S^c_f(N)^T)]^T \) is used to denote the spectrum of transmitted signals, and \( H_f = [(D^c_f(1))...(D^c_f(N))] \) to denote the corresponding channel matrix for the receiver. From the expression it can be observed that the spectrum sensing task requires to estimate \( \bar{S}_f \) in (11) provided we have \( \bar{H}_f \) and \( r(t) \). We have WB signal at our disposal, to alleviate Nyquist rate sampling requirements at the receiver A/D converter, we can use signal recovery algorithms to recover Nyquist rate signal from sub-Nyquist samples. Various computationally reasonable algorithms, such as, BP [24], or Orthogonal Matching Pursuit (OMP) [26], were developed to reliably estimate the received signal sampled at su-Nyquist rate sampling. The compressed time-domain samples are required to be collected at receiver. Therefore, a compressed sensing matrix \( S^c \) is constructed as follows to collect a \( K \times 1 \) sample vector \( X_t \) from \( r(t) \):

\[ x_t = S^c r_t \]  

where \( s_t \) is the \( k \times n \) projection matrix and \( r_t \) is the \( N \times 1 \) vector of discrete-time representations of \( r(t) \) at the Nyquist rate with \( K < N \). There are different approaches introduced in literature for compressive sampler such as non uniform sampler [27] and random sampler [28]. It is worth noting that \( r_t = F_N^{-1} r_f \), and given \( K \) compressed measurements, the frequency response \( \bar{S}_f \) can now be estimated in (11), as follows:

\[ x_t = S^c_T F_N^{-1} H_f \bar{S}_f + \bar{w}_f \]  

where \( \bar{w}_f = S^c_T F_N^{-1} w_f \) presents the noise sample vector which is white Gaussian. In the context of cognitive radio networks, due to low spectrum occupancy by licensed users, the signal vector \( \bar{S}_f \) is sparse in frequency domain. The sparsity of signal vector is measured by p-norm \( ||S_f||_p \), \( p \in [0,2] \), where \( p = 0 \) indicates exact sparsity. Thus, equation (11) is a linear regression problem with signal \( \bar{S}_f \) being sparse. The signal \( \bar{S}_f \) can be estimated by solving the following linear convex optimization problem:

\[ \bar{S}_f = \arg\min_{\bar{S}_f} ||\bar{S}_f||_1, \quad s.t. \quad x_t = S^c_T F_N^{-1} H_f \bar{S}_f \]  

This optimization problem can be solved by various approaches, for example, by means of Convex Programming as in BP [26]. After the reconstructed Nyquist rate WB signal has been obtained from sub-Nyquist samples, CFD can be used to estimate the SCF of the reconstructed signal. The estimated SCF in this case is definitely depends on how well the WB signal was estimated from compressed sensing, which in turn, depends on the sparsity of the signal and the compression rate. The procedure of SCF computation is given in Sec.III.A. In this work, we assume that the proposed algorithm has access to a database containing \( \alpha \) profile previously extracted from SCF values of the licit signals. The algorithm the compare the estimated \( \alpha \) profile of WB with database in order to classify each NB signal as licit or jammer. The pseudo-code of the proposed algorithm is outlined in Algorithm 1.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A 50 \( \Delta \text{Hz} \) WB spectrum is assumed to be under observation by a CR terminal. This WB is divided into 5 SBs. These SBs can be either free or occupied by a NB signal. For testing the proposed system, we assume BPSK as legitimate signals and QPSK is treated as a jamming signal. The received signals are considered to be affected by AWGN. The BP algorithm is used for signal recovery through compressive sensing. The sampling rate is set at Nyquist rate of 100 \( \Delta \text{Hz} \). We set SNR at 0 dB and compression rate \( (K/N) \) are varied from 0 to 1.

We configure our system in two different ways: (a) we placed the BPSK signals in SB-1 and SB-5 and jamming signal in SB-3; (b) BPSK signal is in SB-5 while jamming signal jumps to SB-1 to jam the licit BPSK signal. It is assumed that carrier frequencies of legitimate users are known. The classification of the signals is performed at \( \alpha \neq 0 \), where AWGN exhibits no spectral features. The Monte-carlo simulations are run for 1000 iterations for each \( K/N \). The results are shown in the forms of graphs. For first system configuration, the jammer detection rate versus compression ratio is plotted in Fig. 4. It can be seen from this figure that the jammer detection rate is approximately 1 in SB-3 at \( K/N = 1 \). Due to false

**Algorithm 1** Pseudo-code for proposed algorithm

1: \textbf{function} JAMMER DETECTOR
2: \hspace{1em} Initialise all SB states to "free"
3: \hspace{1em} Receive the WB signal
4: \hspace{1em} Set compression rate \( K/N \)
5: \hspace{1em} Construct the measurement matrix \( S^c \)
6: \hspace{1em} Estimate the WB from compressed samples using BP
7: \hspace{1em} Compute the SCF of estimated WB signal
8: \hspace{1em} Extract the \( \alpha \) profile from SCF
9: \hspace{1em} Divide WB into \( i \) SBs
10: \hspace{2em} for \( i = 1 \to I \), do
11: \hspace{3em} \hspace{1em} Access the database
12: \hspace{3em} \hspace{1em} Compare parameters with the database waveforms
13: \hspace{3em} \hspace{1em} Decision \( \leftarrow \) Licit or Jammer
14: \hspace{2em} end for
15: \textbf{end function}
classification (false positive), the jammer detection in SB-1 and SB-5 is 0.076, which intern means that algorithm correctly classified the legitimate signals with 92% accuracy while for 8% algorithm wrongly classified the legitimate signals as jammer. When $K/N$ is decreased, the jammer detection rate for SB-3 decreases while that for SB-1 and SB-5 increases. It is due to the reason that less samples are now available for WB signal recovery, hence recovered signal is less accurate. Therefore, the computed SCF is also different from what is stored in the database, which leads to wrong classification. For example, at $K/N = 0.70$, the jammer detection rate in SB-3 is 0.868 while wrong classification of jammer as BPSK is 0.132. similarly, the jammer detection rate in SB-1 and SB-5 is 0.11. Fig. 5 shows the jammer detection rate versus compression ratio for second system configuration, where the jammer is now jumped to SB-1 to jam licit BPSK signals. It can be observed that jammer detection rate decrease to 0.82 in SB-1 as compared to 1 in SB-3 from previous case. It is because the algorithm is now classifying a mixture of BPSK and Jammer in SB-1 as it also classify BPSK with classification rate of 0.18. The jammer detection rate is also fallen for this system configuration as the compression ratio is decreased due to poor recovery of the WB spectrum at low compression rates. For instance, at $K/N = 0.55$ the jammer detection rate is approximately 0.65 in SB-1 with wrong classifications as BPSK to be 0.35. The proposed algorithm shows a significant performance improvements compare to common techniques of signal classification, which need 10 dB to 20 dB for signal classification even at Nyquist rate sampling [29].

V. CONCLUSION

In this paper, we proposed a cyclic spectral analysis based jammer detection algorithm for WB CR networks. The WB was considered to be occupied by several NB signals with known carrier frequencies. These signals were assumed to be either licit signals or jamming signals. We used compressed sensing to alleviate the A/D complexity. Compressed sensing was employed to recover the Nyquist rate samples of the WB signal from sub-Nyquist sampling. This WB signal is then fed to the CFD to compute the SCF of the signal. Then the parameters in SCF was compared with the SCF of the legitimate waveforms databases to identify jamming waveforms in each SB. In the end, performance of the proposed algorithm is evaluated for different system configurations and compression ratios at low SNR. The algorithm performed well within the limitations, imposed for using classification, based on simple comparison of parameters from database. In future, artificial neural network can be used as a classifier due to its successful applications to pattern recognition problem. This algorithm can be used to formulate intelligent anti jamming strategies for WB cognitive radios.

REFERENCES


