# Hiding Cyclostationarity with Dispersive Filters for Covert Underwater Acoustic Communications

François-Xavier Socheleau, Sébastien Houcke

# Hiding Cyclostationarity with Dispersive Filters for Covert Underwater Acoustic Communications

François-Xavier Socheleau, Sébastien Houcke
IMT-Atlantique, Lab-STICC, France, {fx.socheleau,sebastien.houcke}@imt-atlantique.fr

***Abstract*—Cyclostationary features of communication signals can be considered as weaknesses from a security point of view. They can be used by eavesdroppers for signal detection, modulation recognition or blind parameter estimation. This work presents a simple approach to make the blind estimation or detection of these features more difficult. It relies on the use of a dispersive filter at transmission that acts as a secret key. This filter is a plugin that is applicable to any existing transmission scheme. Numerical results applied to a DSSS signal with channel replay simulations illustrate the benefits of the proposed method.**

## I. Introduction

Communication signals often exhibit statistical properties that vary cyclically with time. Such a cyclicity can be induced by various design choices such as repetitive pulse shaping or specific framing/coding. In that case, the signals are said to be cyclostationary (CS) [1]. Because they require little prior knowledge on the signal to analyze, CS-based methods are very relevant to detect communication signals and/or reverse-engineer the parameters of their physical layer [2]–[6]. From a security perspective, CS features are then considered as weaknesses since they ease the work of eavesdroppers.

Removing cyclostationarity from communication signals is possible in several ways. For instance, the symbol rate or the pulse-shaping filter can be intentionally changed over time. The drawback of this kind of approach is that a specific waveform must be designed, and, more importantly, it may affect the complexity and/or the performance of the receiver. In this paper, an alternative point of view is introduced. Our idea is to design a low-complexity plugin that can be added to any existing physical layer. More specifically, we propose (i) to add a linear filter before transmission to change the CS pattern perceived by an eavesdropper and (ii) to reverse its effect on the cooperative-receiver side by using a simple matched-filter. The parameters of the filter are then considered as a secret key. The main advantage of this approach is that the design of existing transmitters and receivers does not have to be changed. The limitation is that the CS features are not annihilated, they are simply hidden. It is then important to design a relevant filter to make it difficult for an eavesdropper to recover the CS features. As discussed next, the family of dispersive filters is well adapted to this purpose.

The rest of the paper is organized as follows. The signal model and the assumptions are formulated in Sec. II. Sec. III presents the main characteristics that must be satisfied by the filters. Numerical results with dispersive filters are provided in Sec. IV, followed by conclusions in Sec. V.

## II. Cyclostationarity of UA Communication Signals

A random signal $x(t)$ is said to be second-order cyclostationary (CS) in the wide sense if its mean and autocorrelation are periodic functions of time [1]. More specifically, let $R_x(t,u)$ be the autocorrelation function defined as

$$R_x(t,u) \triangleq \mathbb{E}\left\{x^*(t)x(t+u)\right\}. \tag{1}$$

If $x(t)$ is second-order cyclostationary, $R_x(t,u)$ admits the following Fourier series expansion

$$R_x(t,u) = \sum_{\alpha\in\mathcal{A}} R_x^\alpha(u) e^{i2\pi\alpha t}, \tag{2}$$

where $R_x^\alpha(u)$ is the cyclic-autocorrelation function defined as

$$R_x^\alpha(u) \triangleq \lim_{T\to\infty} \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} R_x(t,u)e^{-i2\pi\alpha t}\mathrm{d}t. \tag{3}$$

$\mathcal{A}$ denotes the countable set of cycle frequencies $\alpha$. If $\mathcal{A} = \{k/T_s\}_{k\in\mathbb{Z}}$ , for some $T_s > 0$, the signal $x(t)$ is said to be cyclostationary with period $T_s$. A CS feature or signature is defined as a subset $\mathcal{S} \subseteq \mathcal{C}$, where $\mathcal{C} = \{(u,\alpha) : R_x^\alpha(u) \neq 0\}$.

Underwater acoustic (UA) communication signals such as PSK, QAM, DSSS or OFDM signals are second-order CS, where $T_s$ denotes the symbol duration. However, UA channels can distort the CS features. For instance, the UA multiscale-multilag channel, over which mobile and wideband systems usually communicate, transforms cyclostationary signals into a sum of motion-dependent time-warped cyclostationary processes [7]. More specifically, given an input signal $x(t)$ and a time-varying channel impulse response $h(\tau,t)$, the received signal $r(t)$ satisfies

$$r(t) = \int_{\mathbb{R}} h(\tau,t)x(t-\tau)\mathrm{d}\tau + w(t) = \sum_{\ell=1}^{L} \lambda_\ell(t)y_\ell(t) + w(t), \tag{4}$$

where $\lambda_\ell(t)$ is the random complex attenuation of the $\ell$-th channel tap and $w(t)$ is the additive noise. Both $\lambda_\ell(t)$ and $w(t)$ are assumed to be (quasi) wide-sense stationary over the observation interval. Their correlation functions are denoted as $R_{\lambda_\ell,\lambda_m}(u)$ and $R_w(u)$, respectively. $y_\ell(t)$ is a delayed, phase and frequency shifted as well as time-warped version of $x(t)$,

$$y_\ell(t) \triangleq x(\psi_\ell(t) - \tau_\ell)e^{i2\pi f_c(\psi_\ell(t)-\tau_\ell-t)}. \tag{5}$$

$\tau_\ell$ denotes the initial time of arrival of the $\ell$-th tap, $f_c$ is the carrier frequency and $\psi_\ell(t)$ is the time-varying delay of the $\ell$-th tap due to motion. It is defined as

$$\psi_\ell(t) \triangleq \left(1 - \frac{v_\ell}{c}\right)t - \frac{a_\ell}{2c}t^2 + o(t^2), \tag{6}$$

where $c$ is the sound speed, $v_\ell$ is the relative velocity between the transmitter and the receiver, and $a_\ell$ is the relative acceleration. By combining Eqs (1) and (4), it can be shown that the autocorrelation function $R_r(t,u)$ satisfies

$$R_r(t,u) = \sum_{\ell=1}^{L}\sum_{m=1}^{L} R_{\lambda_\ell,\lambda_m}(u) R_{y_\ell,y_m}(t,u) + R_w(u) \quad (7)$$

where

$$R_{y_\ell,y_m}(t,u) \approx e^{i2\pi f_c(\psi_m(t+u)-\psi_\ell(t)+\tau_\ell-\tau_m-u)} \times \sum_{\alpha\in\mathcal{A}} R_x^\alpha(\psi_m(u)+\tau_\ell-\tau_m) e^{i2\pi\alpha(\psi_\ell(t)-\tau_\ell)}. \quad (8)$$

If the acceleration is non-negligible in Eq. (6), then we observe that $R_r(t,u)$ is not a periodic function of time $t$ but a linear combination of several chirp signals, whose time-varying phases depend on the time-varying delays $\psi_\ell$ of the channel. The received signal is said to be time-warped cyclostationary. Although distorted by the channel, the CS features of $x(t)$ can still be estimated by an eavesdropper using advanced processing of $r(t)$ [6].

## III. Dispersive filtering

To hide the CS feature of a communication signal, we suggest applying, before transmission, a linear filter that takes advantage of the following result. Let $\circledast_t$ denote convolution with respect to $t$, if $z(t) = x(t) \circledast_t g(t)$ then [1, Eq. (3.83) ]

$$R_z^\alpha(u) = R_x^\alpha(u) \circledast_u A_g^\alpha(u), \quad (9)$$

where $A_g^\alpha(u)$ is the narrowband ambiguity function of $g$, defined as

$$A_g^\alpha(u) \triangleq \int g^*(t) g(t+u) e^{-i2\pi\alpha t} \mathrm{d}t. \quad (10)$$

Our idea is to find a filter that attenuates the amplitude of the peak cycle frequencies perceived by an eavesdropper (Eve), while making sure that a cooperative receiver (Alice) is able to reverse the filtering process so as to recover the transmitted signal. $g(t)$ can then be seen as a secret key used to make it more difficult for Eve to blindly analyze the intercepted signal. Assuming a filter with unit energy, this vague specification can be translated into more specific constraints listed below.

**Constraint 1.** *(Attenuation of cycle frequencies)*

$$max_u \left|A_g^\alpha(u)\right| << 1, \forall |\alpha| \geq \frac{1}{T_s} \quad (11)$$

**Constraint 2.** *(Cooperative recovery)*
*Let $B$ denote the (bilateral) bandwidth of $x(t)$, $\exists\, u_0 \in \mathbb{R}$ such that*

$$\chi_g^\ell(u) \approx \mathbb{E}\left\{|\lambda_\ell|\right\} |sinc\left(\pi B(u-u_0)\right)|, \forall 1 \leq \ell \leq L \quad (12)$$

*where $\chi_g^\ell(u)$ denotes the wideband ambiguity function defined as*

$$\chi_g^\ell(u) \triangleq \mathbb{E}\left\{\left|\int_{\mathbb{R}} g^*(t)\lambda_\ell(t+u) g(\psi_\ell(t+u)) e^{i2\pi f_c(\psi_\ell(t+u)-(t+u))}\mathrm{d}t\right|\right\}. \quad (13)$$

$\chi_g^\ell(u)$ represents the response of a filter matched to $g(t)$ when it is received with a delay $u$, compressed or dilated with a time-warping function $\psi_\ell(t)$ and modulated with a random time-varying amplitude $\lambda_\ell(t)$. Therefore, if constraints C2 is satisfied, it means that Alice can reverse the effect of the secret key by simply applying a matched-filter at reception, while being robust to Doppler scale and Doppler spread. Formally, C1 and C2 are contradictory constraints. C1 indicates that the matched-filter of $g$ must not be robust to frequency shifts (which can be thought as Doppler shifts), whereas C2 requires this filter to be robust to Doppler scale and Doppler spread, the three types of Doppler being closely related. However, in practice, good compromises can be found. A relevant example is that of dispersive filters that we define, in our context, as

$$g(t) = a(t) e^{i\phi(t)} \mathbb{1}_{[-T_g/2, T_g/2]}(t), \quad (14)$$

with $a(t) \geq 0$. $\mathbb{1}(\cdot)$ denotes the indicator function and $T_g >> T_s$ is the filter duration. This definition is very general and includes any kind of parametric or pseudo-random amplitude, phase or frequency modulated (FM) signal, as long as the duration of the filter is much greater than the symbol period $T_s$. It is out of the scope of this paper to discuss the characteristics of all possible dispersive filters. Potential candidates can be found in Radar/Sonar references on ambiguity functions [8]. A specific example is studied in the next section.

## IV. Illustrations

For illustration purposes, we consider the family of FM-filters as a running example (out of many possibilities). In this case, $a(t)$ is a low-pass and smooth amplitude function and $\phi(t)$ is an oscillating phase. The main advantage of these filters is that the trade-off between C1 and C2 can be easily tuned by changing the value of a few phase parameters. A good trade-off is illustrated next with an hyperbolic chirp, whose phase and amplitude satisfy

$$\begin{aligned} \phi(t) &= 2\pi\left(\rho t + \mu \log\left(1+\xi t\right)\right) \\ a(t) &= \frac{1}{|1+\xi t|}, \end{aligned} \quad (15)$$

with $\rho = -6.10^3$, $\mu = 800$, $\xi = 10$. $T_g$ is set to 100 ms and the bandwidth to $B = 4$ kHz.

### A. Ambiguity functions

Fig. 1 shows the narrowband ambiguity function $A_g^\alpha(u)$ of the chirp filter. It is clearly visible that its amplitude quickly decreases with $\alpha$ so that C1 is satisfied for a wide range of symbol periods $T_s$. The impact of the filter $g(t)$ on the cyclic autocorrelation function is illustrated in Fig. 2 with a DSSS signal. More precisely, it is a QPSK signal spread with a maximum-length sequence whose chip-rate is set to 3200 Hz, a symbol period set to $T_s \approx 0.97$ ms (spreading factor $N_c = 3$) and a root-raised cosine filter with a roll-off set to $\eta = 0.25$. As expected [6] and shown in Fig. 2-(a), without the use of a dispersive filter, $R_x^\alpha(u)$ exhibits some significant energy at several cycle frequencies multiples of $1/T_s \approx 1067$ Hz. This energy is concentrated on a range of lags of the order of a few symbol periods. Such a signature can easily be used by

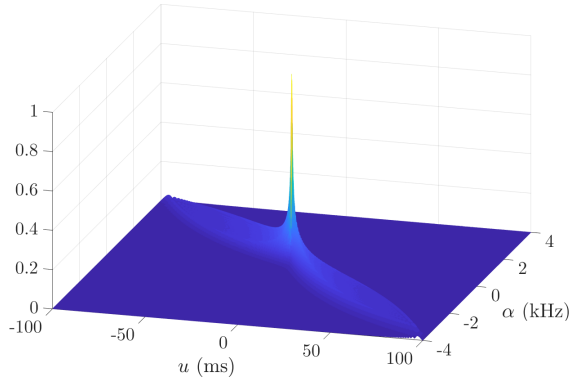
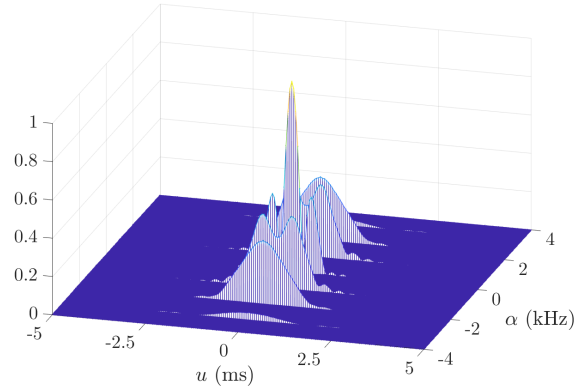
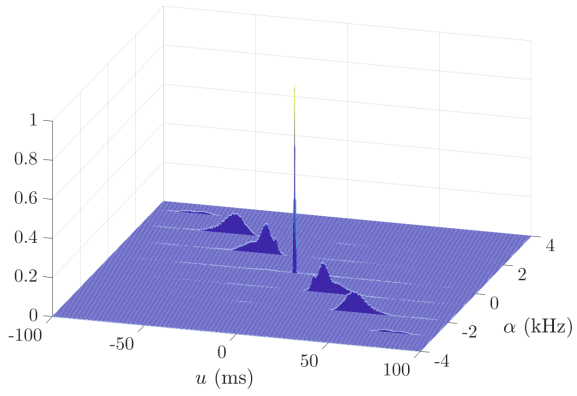



Fig. 1. Narrowband ambiguity function $\left|A_g^\alpha(u)\right|$ of the hyperbolic chirp described in Eq. (15).



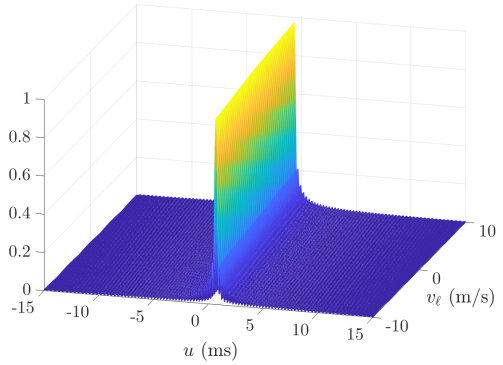

(a)



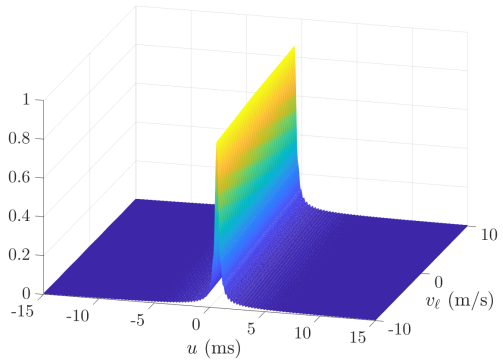

(b)

Fig. 2. Effect of a dispersive filter on the cyclic autocorrelation function of a DSSS signal. (a) $|R_x^\alpha(u)|$, (b) $|R_z^\alpha(u)|$.

Eve as a relevant feature for modulation recognition or signal detection. After filtering, the signal remains cyclostationary but the secret key attenuates, shifts and spreads the cyclic autocorrelation function along the lag-axis $u$. Note that the shift is much larger than the symbol period $T_s$. Without the knowledge of the filter parameters, it then becomes more difficult for Eve to interpret and exploit this unusual CS signature, especially with noisy observations.




(a)




(b)

Fig. 3. Wideband ambiguity function $\chi_g^\ell(u)$ of the hyperbolic chirp described in Eq. (15). (a) RMS Doppler spread = 0.5 Hz, (b) RMS Doppler spread = 5 Hz.

Fig. 3 shows the wideband ambiguity function $\chi_g^\ell(u)$ of the hyperbolic chirp. The carrier frequency was set to $f_c = 6$ kHz, the relative velocity ranges from $\pm 10$ m/s and the relative acceleration was set to 0.1 m/s$^2$. The channel attenuation $\lambda_\ell(t)$ was modeled as a zero-mean complex Gaussian process with a variance set to $4/\pi$ such that $\mathbb{E}\{|\lambda_\ell|\} = 1$. The Doppler spectrum was obtained with a maximum entropy model [9]. The RMS Doppler spread was set to 0.5 Hz and 5 Hz in Fig. 3-(a) and (b), respectively. Both figures show that the hyperbolic chirp is very robust to Doppler scale since the amplitude and the shape of $\chi_g^\ell(u)$ is almost invariant to velocity. A higher velocity only induces a greater static delay $u_0$, which is not problematic for most applications. Doppler spread has a stronger impact but still reasonable. A RMS Doppler spread of 0.5 Hz induces almost no loss compared to a time-invariant channel ($\max \chi_g^\ell(u) \approx 1$). When set to 5 Hz, it is only responsible of a 1.5 dB loss in amplitude and a slight increase of the mainlobe width.

As a conclusion, both constraints C1 and C2 can be satisfied in operational scenarios. This is further illustrated next with real data.

### *B. Validation with channel replay*

The effect of dispersive filtering is validated with replay simulations. By convolving input signals with at-sea measurements of impulse responses, channel replay has become a

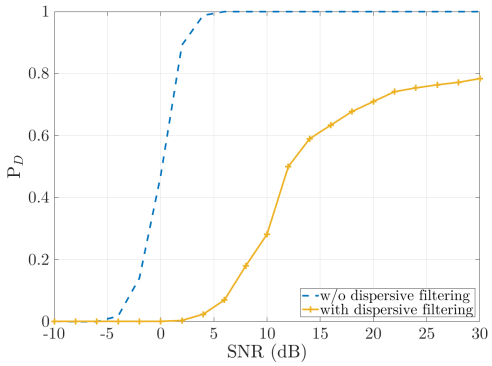



Fig. 4. Effect of dispersive filtering on the detection of the cyclostationary signature of a DSSS signal.

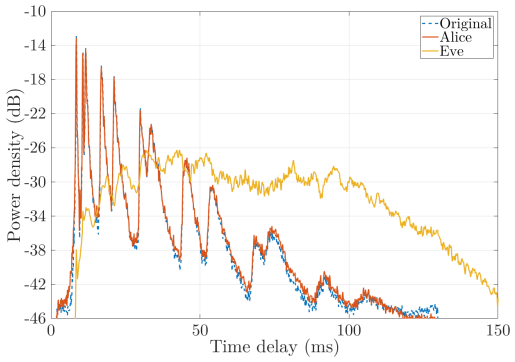



Fig. 5. Power delay profiles of the KAU1 channel (hydrophone #8) as perceived by Alice and Eve.

standard procedure to test underwater communication systems [10]–[13]. The impulse responses used in this section are the one provided with the WATERMARK simulator [13].

*1) Cyclostationary detection:* We here consider the specific scenario where Eve wants to detect a DSSS signal with a specific cyclostationary signature $\mathcal{S}$. Based on the observation $r(t)$ and the knowledge of $\mathcal{S}$, the detection problem is to decide between the following hypotheses

$$\begin{cases} \mathcal{H}_0: & R_x^\alpha(u) = 0, \forall\,(u,\alpha) \in \mathcal{S} \\ \mathcal{H}_1: & R_x^\alpha(u) \neq 0, \forall\,(u,\alpha) \in \mathcal{S}. \end{cases} \tag{16}$$

We consider the same DSSS signal as the one described in Sec. IV-A with a duration set to 1 s. To limit the complexity, the signature is restricted to $\mathcal{S} = \left\{ \left( k\frac{T_s}{4}, \pm\frac{n}{T_s} \right); k = 1,2; n = 1,2 \right\}$. The chosen detector is the approximated de-warped cyclostationary (ADCS) detector presented in [6, Sec. III-D]. Fig. 4 shows the probability of signal detection with and without the use of a dispersive filter. Results are examined versus the in-band SNR defined as SNR $= \frac{E_b}{N_0} \times \frac{2}{N_c(1+\eta)}$, where $E_b$ denotes the energy per bit and $N_0$ the power spectral density of the Gaussian noise. The channel used for the simulation is the KAU1 channel (hydrophone #8) [13] and the false alarm rate was set to $10^{-3}$. Thanks to the KAU1 channel that spreads the CS features along the lag axis, signature detection is still possible for Eve. However, for any targeted detection rate, the use of a dispersive filter results in a huge SNR loss and some high detection rates are not even achievable. Note that this secrecy improvement does not come for free since there is a 10% loss in data rate (duration of $x(t) = 1$ s, whereas duration of $z(t) = 1.1$ s).

*2) Perceived channels:* In addition to hiding the cyclostationarity, dispersive filtering drastically affects the parameters of the transmission channel as perceived by Eve. Conversely, as the process can be reversed by Alice, the channel perceived after matched filtering remains very close to the real one. More precisely, Alice perceives the following channel:

$$\tilde{h}_A(t) = \int_{\mathbb{R}} \int_{\mathbb{R}} h(\tau,u) g(u-\tau) g^*(u-t) \mathrm{d}\tau \mathrm{d}u, \tag{17}$$

whereas, without the key, Eve perceives

$$\tilde{h}_E(t) = \int_{\mathbb{R}} h(\tau,t) g(t-\tau) \mathrm{d}\tau. \tag{18}$$

As illustrated in Fig. 5, the power-delay profile of $\tilde{h}_A(t)$ is similar to the one of $h(\tau,t)$, while it is harsher for $\tilde{h}_E(t)$. There are no identifiable individual taps and the time-delay spread is larger. Blind synchronization or equalization will then become more difficult for Eve. This is further illustrated in Table IV-B2, where the root-mean square (RMS) delay spread of the WATERMARK channels as perceived by Alice and Eve is shown for two filter durations: $T_g = 100$ and 200 ms. It can be noticed that the delay spread for Alice is almost invariant to this duration, which is not the case for Eve. Finally, applying a dispersive filter will also tend to "Gaussianize" the signal and make it look more like noise.

TABLE I
RMS delay spread of the WATERMARK channels as perceived by Alice and Eve.

| Channel | RMS delay spread Alice | | RMS delay spread Eve | |
|---|---|---|---|---|
| | $T_g = 0.1$ s | $T_g = 0.2$ s | $T_g = 0.1$ s | $T_g = 0.2$ s |
| BCH1 | 10.3 ms | 10.3 ms | 30.2 ms | 57.8 ms |
| KAU1 | 17.5 ms | 17.7 ms | 31.5 ms | 56.3 ms |
| KAU2 | 23.5 ms | 23.4 ms | 31.2 ms | 48.0 ms |
| NCS1 | 8.7 ms | 8.7 ms | 31.1 ms | 60.5 ms |
| NOF1 | 13.5 ms | 13.5 ms | 36.1 ms | 67.4 ms |

## V. Conclusion

It is possible to transform the cyclic autocorrelation function of communication signals and attenuate its local maxima by applying, prior to transmission, a dispersive filter whose impulse response duration is much larger than the symbol period. Metrics that characterize the trade-off between the impact of such a filter on the CS features and the ability for a cooperative receiver to reverse its effect have been formulated. With the example of an hyperbolic chirp filter applied to a DSSS signal, numerical results have shown that cyclic-autocorrelation-based signature detection can be made more difficult for an eavesdropper. In addition, the transmission channel, as perceived by the eavesdropper, becomes even more difficult than it already is. There are no identifiable individual taps and the time-delay spread is increased. The proposed approach is low in complexity and can be applied to any existing transmission scheme.

## REFERENCES


[1] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: Half a century of research," *Signal processing*, vol. 86, no. 4, pp. 639–697, 2006.

[2] W. A. Gardner and C. M. Spooner, "Signal interception: performance advantages of cyclic-feature detectors," *IEEE Transactions on Communications*, vol. 40, no. 1, pp. 149–159, 1992.

[3] K. Kim, I. A. Akbar, K. K. Bae, J.-S. Um, C. M. Spooner, and J. H. Reed, "Cyclostationary approaches to signal detection and classification in cognitive radio," in *2007 IEEE international symposium on new frontiers in dynamic spectrum access networks*. IEEE, 2007, pp. 212–215.

[4] Z. Wu and T.C. Yang, "Blind cyclostationary carrier frequency and symbol rate estimation for underwater acoustic communication," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3482–3486.

[5] Q. Li, X.and Han, Z. Liu, and Z. Wu, "Novel modulation detection scheme for underwater acoustic communication signal through short-time detailed cyclostationary features," in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2014, pp. 624–629.

[6] F.-X. Socheleau, "Cyclostationarity of Communication Signals in Underwater Acoustic Channels," *submitted to IEEE J. Ocean. Eng.*, 2022.

[7] F.-X. Socheleau, "Non Data-Aided Estimation of Time-Varying Multi-scale Doppler in Underwater Acoustic Channels," in *Proc. Underwater Communications and Networking (UComms)*, 2021.

[8] N. Levanon and E. Mozeson, *Radar signals*, John Wiley & Sons, 2004.

[9] F.-X. Socheleau, C. Laot, and J.-M. Passerieux, "A Maximum Entropy Framework for Statistical Modeling of Underwater Acoustic Communication Channels," in *Proc. IEEE Oceans'10*, May. 2010.

[10] R. Otnes, P. A. van Walree, and T. Jenserud, "Validation of Replay-Based Underwater Acoustic Communication Channel Simulation," *IEEE J. Ocean. Eng.*, vol. 38, no. 4, pp. 689–700, 2013.

[11] F-X. Socheleau, A. Pottier, and C. Laot, "Stochastic Replay of SIMO Underwater Acoustic Communication Channels," *OCEANS 2015*, pp. 1–6, October 2015.

[12] F-X. Socheleau, C. Laot, and J-M. Passerieux, "Parametric Replay-Based Simulation of Underwater Acoustic Communication Channels," *IEEE J. Ocean. Eng.*, vol. 40, no. 4, pp. 4838–4839, 2015.

[13] P. A. van Walree, F.-X. Socheleau, R. Otnes, and T. Jenserud, "The Watermark Benchmark for Underwater Acoustic Modulation Schemes," *IEEE J. Ocean. Eng.*, vol. 42, no. 4, pp. 1007–1018, Oct 2017.