Cyclostationary Feature Distortion for Secure Underwater Acoustic Transmissions

François-Xavier Socheleau, Christophe Laot, Sébastien Houcke

Cyclostationary Feature Distortion for Secure Underwater Acoustic Transmissions

François-Xavier Socheleau, *Senior Member, IEEE*, Christophe Laot, *Senior Member, IEEE*, Sébastien Houcke

Abstract

Cyclostationary features of communication signals are known to compromise the security of transmissions against eavesdropping attacks. They can be used for signal detection, modulation recognition or for blind estimation of PHY layer parameters. This work presents a method that voluntarily distorts the transmitted signal to hide the cyclostationary patterns. This distortion is obtained with a pseudo-random time-varying filter that combines time warping and dispersive filtering. The proposed method acts as a plugin that is applicable to most existing transmission scheme. It is shown that this distortion can be easily reversed by the cooperative receiver using a simple matched filter combined with resampling. In the context of underwater acoustic communications, numerical results with replay simulations of channels measured at sea illustrate the benefits of the proposed method. For both a coherent and a noncoherent modem, the induced distortion is shown to be robust to existing cyclostationary attacks, at the cost of a slight reduction in data rate. Furthermore, no performance degradation in terms of packet error ratio is observed for cooperative transmissions.

Index Terms

Covert communications, cyclostationarity, TRANSEC, underwater warfare.

The authors with IMT Atlantique, Lab-STICC UMR CNRS 6285, France (e-mail: {fx.socheleau,christophe.laot,sebastien.houcke}@imt-atlantique.fr)

A preliminary version of this paper was presented at the Conference on Underwater Communications and Networking (UComms) in August 2022 [1].

I. Introduction

In its broadest sense, communications security refers to measures taken to ensure the confidentiality, integrity, and availability of communication channels and the information they carry. It involves measures like encryption to ensure that unauthorized individuals cannot access the information but also transmission security (TRANSEC) measures to prevent malicious jamming attacks or to prevent eavesdroppers from collecting intelligence without necessarily having defeated encryption [2].

Until recently, security aspects of underwater acoustic communications (UAC) were mostly limited to the implementation of low-probability of detection and/or low-probability of interception (LPD/LPI) techniques, including spread-spectrum, frequency-hopping or directional transmissions [3]. These TRANSEC protections are used for covert communications but also as a way to mitigate the effects of the challenging propagation conditions experienced at sea (multipath, Doppler effect, noise, interference, etc.) [4]–[6]. With the development of underwater acoustic systems for critical defense and industrial applications, it is now becoming essential to further improve the security of communications. With this in mind, recent works have proposed cryptosecurity solutions and/or countermeasures resistant to specific network attacks [7]–[9].

Despite this progress, most UAC security solutions still allow intelligence to be collected by reverse-engineering the physical layer of the intercepted signal. This includes identifying the modulation format, the framing or the error-correcting code [10]–[14]. Identifying the modulation parameters is critical from an eavesdropper's perspective. It can provide significant intelligence information and is a prerequisite for performing bit-level analysis. With standard modulation format, such an identification can be achieved efficiently by exploiting the cyclostationary (CS) features of communication signals [11], [12], [15]–[19]. Cyclostationarity refers to the periodic behavior of the statistical properties of a signal. For communication signals, such a periodicity can be induced by various design choices such as repetitive pulse shaping or specific framing/coding [12], [20]. From a security perspective, CS features are then considered as weaknesses since they ease the work of eavesdroppers.

A common approach to remove CS features from communication signals is to randomize the symbol period over time, with periods belonging to a predetermined discrete set [21], [22]. Specific features can also be attenuated by introducing a pseudo-random frequency jitter at

the signal generation [23]. An alternative method is also to build signals belonging to the set of nonrelatively measurable functions such that their time-average-based statistical functions are nonconvergent [24]. Although efficient, these techniques are usually applicable to specific modulation formats and require to fully redesign the corresponding receiver. This can affect the complexity and performance of communication systems, and can also be costly, in terms of engineering time, to design, implement, and test these specific waveforms.

In this article, an alternative point of view is introduced. Our idea is to design a low-complexity TRANSEC plugin that can be added to any existing physical layer. More specifically, we propose to add a specific time-varying linear filter just before transmission to strongly distort the CS pattern perceived by an eavesdropper. This filter can be described as the aggregation of two transforms. The first one consists in time-warping the signal to be transmitted with a pseudo-random continuous function. Its effect is to spread the energy in the cyclic domain, the CS signal becoming a time-warped CS process [25]. The second transform is a dispersive filter that changes the original CS signature to prevent a well-informed eavesdropper from finding the inverse warping function that restores the regular cyclicity of the observed signal. In addition to its efficiency in hiding the CS features, it is shown that the effects of these transforms can be easily reversed by the cooperative receiver using a simple matched filter combined with a resampler. The main advantage of this approach is that it can be applied to any modulation format and does not require a complete redesign of existing transmitters and receivers. The downside is a slight reduction in data rate. The method is discussed in the context of UAC and restricted to second-order CS features. Its performance is tested in realistic scenarios with replay simulations of UAC channels measured at sea [26]. To demonstrate the general applicability of the proposed method, it is applied to both a noncoherent and a coherent modem.

The rest of this article is organized as follows. Concepts and definitions related to the second-order cyclostationarity of communications signals in UAC channels are reviewed in Section II. The implementation of intentional warping is presented and illustrated in Section III. It is followed in Section IV by the description of the additional TRANSEC component based on dispersive filtering. Section V briefly presents how the combination of the two transforms can be expressed as a time-varying filter. Performance is illustrated with both a noncoherent and coherent modem in Section VI. Finally, concluding remarks are given in Section VII. In all sections, Alice and Bob denote the cooperative transmitter and receiver, respectively, and Eve

denotes the eavesdropper.

II. Preliminary material

A. Cyclostationarity of UA Communication Signals

A random signal $x(t)$ is said to be almost second-order cyclostationary (ACS) in the wide sense if its mean and autocorrelation are almost-periodic functions of time [10], [27]. 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 ACS, $R_x(t,u)$ admits the following generalized Fourier series expansion

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

where $\mathcal{A}$ denotes the countable set of possibly incommensurate cycle frequencies α and $R_x^\alpha(u)$ is the cyclic autocorrelation function defined as

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

If $\mathcal{A} = \{k/T_s\}_{k\in\mathbb{Z}}$, for some $T_s > 0$, then $x(t)$ is said to be cyclostationary.

The ACS features can also be revealed by the cyclic spectrum and the spectral coherence density, respectively defined as

$$S_x^\alpha(\nu) \triangleq \int_{\mathbb{R}} R_x^\alpha(u)e^{-i2\pi u\nu}\mathrm{d}u \tag{4}$$

$$C_x^\alpha(\nu) \triangleq \frac{S_x^\alpha(\nu)}{\sqrt{S_x^0(\nu)S_x^0(\nu-\alpha)}}. \tag{5}$$

As discussed in [12], most UAC signals exhibit cyclostationary features due to the repetitive use of the same pulse-shaping filter, same spreading sequence, to the redundancy induced by a cyclic prefix or to signaling patterns such as preambles, postambles and time-frequency pilots. However, depending on the characteristics of the propagation channel, theses features can be distorted. For instance, the channel over which mobile and wideband acoustic systems usually communicate can transform cyclostationary signals into a sum of motion-dependent time-warped

cyclostationary processes [25], [28]. More specifically, given an ACS input communication signal $x(t)$ and a time-varying channel impulse response $h_c(\tau, t)$, the received signal $r(t)$ satisfies

$$\begin{aligned} r(t) &= \int_{\mathbb{R}} h_c(\tau, t)x(t-\tau)\mathrm{d}\tau + \eta(t) \\ &= \sum_{\ell=1}^{L} \lambda_\ell(t)s_\ell(t) + \eta(t) \end{aligned} \tag{6}$$

where $\lambda_\ell(t)$ is the random complex attenuation of the ℓ-th channel tap and $\eta(t)$ is the wide-sense stationary additive noise. The time-varying impulse response is assumed to be wide-sense stationary [29] so that $\mathbb{E}\left\{\lambda_\ell^*(t)\lambda_m(t+u)\right\} = R_{\lambda_\ell,\lambda_m}(u)$ does not depend on t. $s_\ell(t)$ denotes a delayed, phase and frequency shifted as well as possibly time-warped version of $x(t)$, that is,

$$s_\ell(t) \triangleq x(\psi_\ell(t) - \tau_\ell)e^{i2\pi f_c(\psi_\ell(t)-\tau_\ell-t)} \tag{7}$$

where τ_ℓ is the initial time-of-arrival of the ℓ-th tap, f_c is the carrier frequency and $\psi_\ell(t)$ is the time-varying delay of the ℓ-th tap due to motion. Over the duration of a communication packet, $\psi_\ell(t)$ is commonly modeled as a deterministic second-order polynomial function [12], [30]

$$\psi_\ell(t) \triangleq \gamma_{1,\ell}t + \gamma_{2,\ell}t^2 \tag{8}$$

where the pair $(\gamma_{1,\ell}, \gamma_{2,\ell})$ models the motion-induced Doppler scaling[1], with $\gamma_{1,\ell}$ depending on the relative velocity between the transmitter and the receiver, and $\gamma_{2,\ell}$ on the relative acceleration. If $(\gamma_{1,\ell}, \gamma_{2,\ell}) = (\gamma_1, \gamma_2), \forall\, \ell$, the channel is said to be single scale-multilag, otherwise it is said to be multiscale-multilag. The value of (γ_1, γ_2) can have a strong impact on the ACS features at reception. More specifically, as shown in [12], the autocorrelation function $R_r(t, u)$ satisfies

$$R_r(t,u) = \sum_{\ell=1}^{L}\sum_{m=1}^{L} R_{\lambda_\ell,\lambda_m}(u)R_{s_\ell,s_m}(t,u) + R_\eta(u) \tag{9}$$

where

$$\begin{aligned} R_{s_\ell,s_m}(t,u) \approx\ & e^{i2\pi f_c(\psi_m(t+u)-\psi_\ell(t)+\tau_\ell-\tau_m-u)} \\ & \times \sum_{\alpha\in\mathcal{A}} R_x^\alpha(\psi_m(u)+\tau_\ell-\tau_m)e^{i2\pi\alpha(\psi_\ell(t)-\tau_\ell)}. \end{aligned} \tag{10}$$

As discussed in [12, Sec. III-B], this approximation is valid provided that the observation interval is not too large (typically on the order of a few seconds for most mobile and wideband acoustic

[1]Note that these parameters also include virtual Doppler scaling due to clock-frequency mismatch between the transmitter and the receiver.

channels, and, possibly, much longer for static low-frequency channels). if $\gamma_{2,\ell} \neq 0$ in (8), then we observe in (10) that $R_r(t,u)$ is not a periodic function of time t but a linear combination of several linear chirp signals whose time-varying phases depend on t^2. The received signal is not ACS in this scenario. It is said to be time-warped cyclostationary. Also, if $\gamma_{2,\ell} = 0$ but $\gamma_{1,\ell} \neq 1$, $r(t)$ is ACS but its cycle frequencies are shifted compared to those of $x(t)$. Although distorted by the channel, the range of values taken by $(\gamma_{1,\ell}, \gamma_{2,\ell})$ can be bounded by physical considerations so that the CS features of $x(t)$ can still be exploited by an eavesdropper using advanced processing of $r(t)$ [12]. For instance, in typical underwater scenarios, the relative velocity is on the order of a few meters per second, the acceleration is bounded by a couple a meters per second squared and the sound speed is around 1500 m.s^{-1} so that $|\gamma_{1,\ell} - 1| \lesssim 1/150$ and $|\gamma_{2,\ell}| \lesssim 1/1500$ s^{-1} (see [12, Sec. III-A] for more details).

B. Cyclic statistic estimators

Cyclostationarity-based signal interception relies on estimators that are briefly reviewed here. As mentioned in the introduction, a vast body of literature is related to cycle frequency estimation and detection. We here only focus on estimators that will be used for illustration purposes and performance measurement in this work. For non UAC-specific estimators, a more detailed analysis, including implementation aspects, can be found in [27, Ch. 5 & 8].

1) Cyclic correlogram: The cyclic correlogram is an estimator of (3) and, over a time interval T_{obs}, is defined as [27, Sec. 5.4.1]

$$\widehat{R}_x^{\alpha}(u) \triangleq \frac{1}{T_{\text{obs}}} \int_0^{T_{\text{obs}}} x^*(t)x(t+u)e^{-i2\pi\alpha t}\mathrm{d}t. \tag{11}$$

It is commonly used to estimate the cycle frequencies by locating the peaks in α of the functions $\max_u \left|\hat{R}_x^{\alpha}(u)\right|$ or $\int_{-u_m}^{u_m} \left|\hat{R}_x^{\alpha}(u)\right|^2 \mathrm{d}u$, where u_m bounds an interval in which $R_x^{\alpha}(u)$ is expected to be significantly nonzero [31]. It is also used as a basis for the design of cyclic detectors such as [32], [33].

2) Approximated dewarped cyclic correlogram: This correlogram is a generalization of (11) to situations where $\gamma_{2,\ell} \neq 0$ in (8). It has been specifically designed for UAC signals and it is defined as [12, Sec. III-D]

$$\widehat{J}_x^{\alpha}(u;\mu_1,\mu_2) = \frac{1}{T_{\text{obs}}} \int_0^{T_{\text{obs}}} x^*(t)x\left(t + \psi_{\mu_1,\mu_2}^{-1}(u)\right) \times e^{-i2\pi\left(\alpha\psi_{\mu_1,\mu_2}(t) + 2\mu_2 u f_c t\right)}\mathrm{d}t \tag{12}$$

where

$$\psi_{\mu_1,\mu_2}(t) = \mu_1 t + \mu_2 t^2 \tag{13}$$

and

$$\psi^{-1}_{\mu_1,\mu_2}(t) = \begin{cases} \frac{1}{2\mu_2}\left(\sqrt{\mu_1^2 + 4\mu_2 t} - \mu_1\right), & \mu_2 \neq 0, \\ \frac{t}{\mu_1}, & \mu_2 = 0,\ \mu_1 \neq 0. \end{cases} \tag{14}$$

$\widehat{J}_x^\alpha(u;\mu_1,\mu_2)$ can be used in the same way as (11) to estimate or detect cycle frequencies but requires an additional maximization over (μ_1,μ_2) to compensate for the Doppler effect.

3) Cyclic periodogram: The cyclic periodogram is an estimator of (4) and can be expressed as [27, Sec. 5.4.2]

$$\widehat{S}_x^\alpha(\nu) \triangleq \int_{\mathbb{R}} \widehat{R}_x^\alpha(u) q\left(u\Delta\nu\right) e^{-i2\pi\nu u} \mathrm{d}u \tag{15}$$

where $\Delta\nu$ denotes the spectral frequency resolution and $q\left(\cdot\right)$ is a tapering window. Based on (15), it is possible to estimate the spectral coherence density as

$$\widehat{C}_x^\alpha(\nu) \triangleq \frac{\widehat{S}_x^\alpha(\nu)}{\sqrt{\widehat{S}_x^0(\nu)\widehat{S}_x^0(\nu-\alpha)}}. \tag{16}$$

Similarly to the correlogram, cycle frequencies can be estimated or detected by maximizing or integrating over ν the magnitude of either (15) or (16) [34].

III. Intentional warping

A. Warping operator

As discussed in the introduction, we suggest to voluntarily distort the time scale of the signal to be transmitted in order to make the ACS features negligible. This distortion can be modeled as a linear time-varying filter of impulse response $h_w(\tau,t) \triangleq \delta\left(\tau - t + w(t)\right)$ such that the new transmitted signal can be expressed as

$$y(t) = \int_{\mathbb{R}} h_w(\tau,t) x(t-\tau) \mathrm{d}\tau = x(w(t)) \tag{17}$$

where $\delta\left(\cdot\right)$ denotes the Dirac delta distribution and $w(t)$ is a strictly increasing continuous time-warping function. If T_{max} denotes the duration of the signal $x(t)$ than $w^{-1}(T_{\text{max}})$ is the duration of the signal $y(t)$.

As opposed to the Doppler-induced time warping, we expect this intentional warping function to be difficult to reverse-engineer by an eavesdropper. Its effect on the ACS features can be

highlighted by looking at the cyclic autocorrelation function or the cyclic spectrum. More precisely, it can be shown that [25, Sec. II-C]

$$R_y(t,u) = \sum_{\beta \in \mathcal{A}} a_\beta(t,u) e^{i\phi_\beta(t)} \tag{18}$$

where $a_\beta(t,u) \triangleq R_x^\beta(w(t+u)-w(t))$ and $\phi_\beta(t) \triangleq 2\pi\beta w(t)$. Therefore, over a finite observation interval T_{obs}, the cyclic autocorrelation function and the cyclic spectrum satisfy, respectively

$$R_y^\alpha(u;T_{\text{obs}}) \triangleq \frac{1}{T_{\text{obs}}} \int_0^{T_{\text{obs}}} R_y(t,u) e^{-i2\pi\alpha t} \mathrm{d}t = \frac{1}{T_{\text{obs}}} \sum_{\beta \in \mathcal{A}} \int_0^{T_{\text{obs}}} a_\beta(t,u) e^{i\phi_\beta(t)} e^{-i2\pi\alpha t} \mathrm{d}t \tag{19}$$

and

$$S_y^\alpha(\nu;T_{\text{obs}}) \triangleq \int_{\mathbb{R}} R_y^\alpha(u;T_{\text{obs}}) e^{-i2\pi u\nu} \mathrm{d}u = \frac{1}{T_{\text{obs}}} \sum_{\beta \in \mathcal{A}} \int_0^{T_{\text{obs}}} A_\beta(t,\nu) e^{i\phi_\beta(t)} e^{-i2\pi\alpha t} \mathrm{d}t \tag{20}$$

where $A_\beta(t,\nu)$ is the Fourier transform with respect to u of $a_\beta(t,u)$. Both (19) and (20) are expressed as the sum of the Fourier transform of amplitude and frequency modulated (AM-FM) signals. This implies that the energy of $y(t)$ will be spread in the cyclic-domain. Also, it can be noticed that the instantaneous frequency of each AM-FM signal is proportional to the derivative of $\phi_\beta(t)$ and therefore to the derivative of the warping function $w(t)$. Consequently, cyclic features become more diffuse as the range of this derivative increases. In other words, the more nonlinear $w(t)$ is, the better the ACS features are hidden.

To quantify the impact of the nonlinear part of $w(t)$, we define the relative cyclostationary index (RCI) as follows

$$\begin{aligned} \text{RCI} &\triangleq \frac{\max\limits_{|\mu|<1} \sum\limits_{\alpha \in \mathcal{A}} \int_{\mathbb{R}} \left| R_y^{(1+\mu)\alpha}(u;T_{\text{obs}}) \right|^2 \mathrm{d}u}{\sum_{\alpha \in \mathcal{A}} \int_{\mathbb{R}} \left| R_x^\alpha(u;T_{\text{obs}}) \right|^2 \mathrm{d}u} \\ &= \frac{\max\limits_{|\mu|<1} \sum\limits_{\alpha \in \mathcal{A}} \int_{\mathbb{R}} \left| S_y^{(1+\mu)\alpha}(\nu;T_{\text{obs}}) \right|^2 \mathrm{d}\nu}{\sum_{\alpha \in \mathcal{A}} \int_{\mathbb{R}} \left| S_x^\alpha(\nu;T_{\text{obs}}) \right|^2 \mathrm{d}\nu}. \end{aligned} \tag{21}$$

This positive index compares the energy of the signal in the cyclic domain before and after warping. The maximization over μ is meant to make the index scale invariant, so that a linear warping function will give an RCI of one, which is the value also obtained without warping.

Another way to analyze the impact of $w(t)$ in the context of communication signals is to derive the expression of the transmission channel as perceived by Eve. Since both the warping function

and the propagation channel are linear operators, the combined effect of the two operators can be modeled with a time-varying impulse response $h_{w\star c}$ such that

$$r(t) = \int_{\mathbb{R}} h_{w\star c}(\tau, t)x(t-\tau)\mathrm{d}\tau + \eta(t) \tag{22}$$

with

$$h_{w\star c}(\tau, t) \triangleq \sum_{\ell=1}^{L} \lambda_\ell(t)\delta\left(\tau - \left(t - w\left(\psi_\ell(t) - \tau_\ell\right)\right)\right) \times e^{i2\pi f_c(\psi_\ell(t)-\tau_\ell-t)}. \tag{23}$$

Eq. (23) results from the merger of (6) and (17). Combined with the real propagation channel, (23) shows that intentional warping is equivalent to creating an artificial channel with multipath arrivals that drift in time as a function of $w(t)$. This is further discussed and illustrated in Sec. III-C.

B. Choice of the warping function and cooperative recovery

The analysis of Sec. III-A shows that $w(t)$ should fluctuate quickly to maximize the security of the transmission. However, the use of warping is not free for the cooperative communication between Alice and Bob. It affects the signal bandwidth and therefore the spectral efficiency. We also have to make sure that it can be reversed at reception.

More specifically, let $\mathrm{IB}_x(t)$ be the instantaneous bandwidth of a signal $x(t)$. It is defined as [35]

$$\mathrm{IB}_x(t) \triangleq K\sqrt{\frac{\int_{\mathbb{R}}\left(\nu - \bar{\nu}_x(t)\right)^2 P_x(t,\nu)\mathrm{d}\nu}{\int_{\mathbb{R}} P_x(t,\nu)\mathrm{d}\nu}} \tag{24}$$

where $P_x(t,\nu)$ denotes the spectrogram of $x(t)$, K is some constant and

$$\bar{\nu}_x(t) \triangleq \frac{\int_{\mathbb{R}} \nu P_x(t,\nu)\mathrm{d}\nu}{\int_{\mathbb{R}} P_x(t,\nu)\mathrm{d}\nu} \tag{25}$$

is the instantaneous central frequency. As shown in App. A, after warping, the instantaneous bandwidth of $x(t)$ is modified such that

$$\mathrm{IB}_y(t) \approx w'(t) \times \mathrm{IB}_x(w(t)) \tag{26}$$

where $w'(t) > 0$ is the derivative of $w(t)$. $\mathrm{IB}_y(t)$ cannot be greater than the available bilateral bandwidth $B_{\max}$ of the transducer for any time t, otherwise part of the signal will not be

transmitted. Therefore, assuming that $x(t)$ is a full-band signal, $w(t)$ must be designed such that, for any t,

$$-\frac{B_{\max}}{2} \leq \frac{\text{IB}_y(t)}{2} + \bar{\nu}_y(t) \leq \frac{B_{\max}}{2}. \tag{27}$$

For centered signals with a constant instantaneous bandwidth such as PSK, QAM, DSSS or OFDM signals, we have $\bar{\nu}_x(t) = 0$ and $\text{IB}_x(t) = B_{\max}$ for all t. In that case, $\text{IB}_y(t) \approx w'(t)B_{\max}$ so that the previous constraint simplifies to

$$0 < \sup_t w'(t) \leq 1. \tag{28}$$

In other scenarios where $\max_t \text{IB}_x(t) < B_{\max}$ or for specific signals like those used in chirp-based transmissions [36], $w'(t)$ can occasionaly be greater than one without violating condition (27). The ratio of spectral efficiency between $y(t)$ and $x(t)$ can be quantified by the following factor

$$\xi_w \triangleq \frac{T_{\max}}{w^{-1}(T_{\max})}. \tag{29}$$

If inequality (28) is satisfied then $y(t)$ is expanded compared to $x(t)$ so that $\xi_w \leq 1$.

By dewarping the received signal using the inverse of $w(t)$, the cooperative receiver can expect to remove the effect of intentional warping. In practice, the warping-dewarping operation is not transparent because of the propagation channel that sits in the middle and that is unknown to Alice and Bob. Therefore, care must be taken in the recovery process as well as in the design of $w(t)$.

First of all, as a consequence of the solution to Cauchy's functional equation [37], if $w(t)$ is not a linear function then it is not possible to inverse the effect of warping without synchronization. In other words, it does not exist a nonlinear and increasing warping function such that $w(w^{-1}(t) - \tau_0) = t - w(\tau_0)$, $\forall\, \tau_0 \in \mathbb{R}$. In practice, this means that dewarping must be applied after the receiver is time-synchronized. This is not a problem since most UAC systems use preambles for detection and synchronization. Even if the preamble is warped, since $w(t)$ is known to the cooperative receiver, this new warped preamble is also known so that it does not impact the detection and synchronization process. The same comment applies for the Doppler scale. It must be compensated at reception before applying the inverse of the warping function $w(t)$. Again, the Doppler scale is usually estimated using the preamble. Its compression/dilation effect is then compensated by performing a sampling rate conversion using an interpolator [38]. For the sake

of simplicity, we illustrate this procedure with a single scale-multilag channel, i.e., $\psi_\ell(t) = \psi(t)$ for all ℓ, and with $\eta(t) = 0$. Based on (23), the received signal is first expressed as

$$r(t) = \sum_{\ell=1}^{L} \lambda_\ell(t) x\left(w\left(\psi(t) - \tau_\ell\right)\right) e^{i2\pi f_c(\psi(t)-\tau_\ell - t)}. \tag{30}$$

After time synchronization and carrier frequency offset compensation it becomes

$$r_1(t) = \sum_{\ell=1}^{L} \lambda_\ell(t) x\left(w\left(\psi(t) - \tilde{\tau}_\ell\right)\right) e^{-i2\pi f_c \tilde{\tau}_\ell} \tag{31}$$

where the $\tilde{\tau}_\ell$ denote the initial time of arrival after synchronization such that there is a tap ℓ_0 satisfying $\tilde{\tau}_{\ell_0} = 0$. After compensating for the Doppler scale by resampling, we then have

$$\begin{aligned} r_2(t) &= r_1(\psi^{-1}(t)) \\ &= \sum_{\ell=1}^{L} \lambda_\ell(\psi^{-1}(t)) x\left(w\left(t - \tilde{\tau}_\ell\right)\right) e^{-i2\pi f_c \tilde{\tau}_\ell}. \end{aligned} \tag{32}$$

Finally, the inverse function of $w(t)$ is applied to get

$$\begin{aligned} r_3(t) &= r_2(w^{-1}(t)) \\ &= \sum_{\ell=1}^{L} \tilde{\lambda}_\ell(t) x\left(w\left(w^{-1}(t) - \tilde{\tau}_\ell\right)\right) e^{-i2\pi f_c \tilde{\tau}_\ell} \\ &= \tilde{\lambda}_{\ell_0}(t) x\left(t\right) + \sum_{\substack{\ell=1 \\ \ell \neq \ell_0}}^{L} \tilde{\lambda}_\ell(t) x\left(w\left(w^{-1}(t) - \tilde{\tau}_\ell\right)\right) e^{-i2\pi f_c \tilde{\tau}_\ell} \end{aligned} \tag{33}$$

where $\tilde{\lambda}_\ell(t) = \lambda_\ell(\psi^{-1}(w^{-1}(t)))$. Note that since there is no analytical expression for the warping function, $w^{-1}(t)$ is obtained numerically. Another way of writing (33) is to consider that $x(t)$ is transmitted over a channel $h_{w\text{-}c\text{-}w^{-1}}(\tau, t)$ defined as

$$h_{w\text{-}c\text{-}w^{-1}}(\tau, t) \triangleq \sum_{\ell=1}^{L} \tilde{\lambda}_\ell(t) \delta\left(\tau - \left(t - w\left(w^{-1}(t) - \tilde{\tau}_\ell\right)\right)\right) \times e^{-i2\pi f_c \tilde{\tau}_\ell} \tag{34}$$

such that $r_3(t) = \int_{\mathbb{R}} h_{w\text{-}c\text{-}w^{-1}}(\tau, t) x(t - \tau) \mathrm{d}\tau$. Eq. (33) shows that the intentional warping-dewarping operation is not transparent to taps other than the one to which the receiver is synchronized. In fact, if no warping were used, i.e, if $w(t) = t$, we would get

$$r_3(t) = \tilde{\lambda}_{\ell_0}(t) x\left(t\right) + \sum_{\substack{\ell=1 \\ \ell \neq \ell_0}}^{L} \tilde{\lambda}_\ell(t) x\left(t - \tilde{\tau}_\ell\right) e^{-i2\pi f_c \tilde{\tau}_\ell}. \tag{35}$$

Since we do not want to sacrifice performance for security, and since our approach must have a minimal impact on the design of existing receivers, we need to make sure that $w\left(w^{-1}(t)-\tilde{\tau}_\ell\right)$ is not so different from $t-\tilde{\tau}_\ell$, at least for the most energetic taps. Therefore, although $w(t)$ must be nonlinear to hide the ACS features according to Sec. III-A, a compromise must be found to avoid performance degradation.

Without loss of generality, a simple and easily customizable way to generate $w(t)$ is considered next. Let the warping function be expressed as

$$w(t) = (1-\rho)t + \epsilon(t) \tag{36}$$

where $\epsilon(t)$ is a slowly varying function such that $\rho - 1 < \epsilon'(t) \leq \rho$ with $\rho = \sup_t \epsilon'(t)$. The level of nonlinearity of $w(t)$ is then controlled by $\rho > 0$ and by the speed of fluctuation of $\epsilon(t)$. To control this speed and making sure that $w(t)$ is random from Eve's perspective, we suggest to generate $\epsilon(t)$ by filtering a white Gaussian noise with a low-pass filter of cut-off frequency ν_ϵ. The fluctuation rate of $\epsilon(t)$ is then characterized by the power spectral density of its derivative which satisfies

$$\text{PSD}\left(\epsilon'(t)\right)(\nu) \propto \nu^2 \Pi_{2\nu_\epsilon}(\nu) \tag{37}$$

where $\Pi_A(\cdot)$ denotes a gate function of width A. Note that the linear part of $w(t)$ does not contribute to the obfuscation of the CS signature, it is only useful to ensure that the instantaneous bandwidth of the warped signal is not greater than the maximum available bandwidth. Moreover, with this design, (28) is always satisfied so that it can be applied to any type of waveforms.

Finally, although the formalism of linear time-varying systems is relevant to perform a theoretical analysis of the effect of warping, in practice, it will be easier to implement warping by resampling the signal to be transmitted prior to digital-to-analog conversion.

C. Illustrations

The effect of intentional warping is illustrated with a noncoherent spread-spectrum modulation scheme. More precisely, the signal $x(t)$ is a communication packet that starts with a preamble made of a 255-chip long M-sequence followed by a quaternary (pseudo) orthogonal signaling. Each data symbol is coded with a 63-chip Gold sequence chosen among a set of 4 possible sequences. This scheme also employs a rate-1/2 convolutional code. A root raised-cosine pulse is used with a roll-off factor of 1/10 at a chip rate of 3636 chip/s so that the symbol period

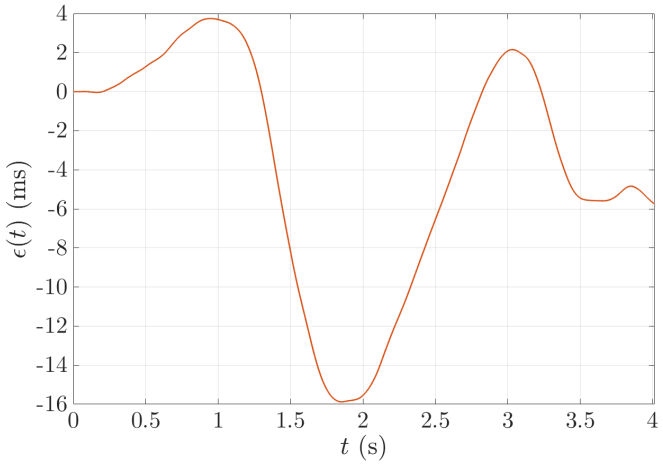


Fig. 1: Sample-path example of the nonlinear part of the warping function, $\rho = 0.05$ and $\nu_\epsilon = 0.5$ Hz.

satisfies $T_s \approx 17.3$ ms. Each packet contains 200 bits with an effective bitrate $R_{\text{eff}} = 52.5$ bit/s so that $T_{\text{max}} = 3.8$ s.

This noncoherent modulation scheme was specifically chosen for illustration because it has a very pronounced pattern in the cyclic domain, making it possible to observe the effect of warping over a wide range of cycle frequencies. In fact, as can be deduced from [12, Eq. (80)], $\left\{-\frac{63}{T_s}, \cdots, 0, \cdots, \frac{63}{T_s}\right\} \subseteq \mathcal{A}$, so that there is a large number of significant cycle frequencies. The warping function $w(t)$ is generated as described in (36) and illustrated in Fig. 1. The effect of $w(t)$ on the theoretical RCI is shown in Fig. 2 as a function of the parameter ρ, defined in (36). The larger ρ, the more the cyclostationary signature is distorted. Since, on average, the data rate loss caused by w is equal to ρ, Fig. 2 shows that we can achieve efficient CS distortions with only a few percent rate loss. For this specific modulation format, note that warping could also be combined with the use of an outer spreading code to generate long-code sequences and further reduce the CS signature [39].

A realistic scenario with replay simulations using a real shallow-water channel is now considered. By convolving input signals with at-sea measurements of impulse responses, channel replay has become a standard procedure to test underwater communication systems [26], [40]–[43]. The channel used for the illustration is the KAU1 channel provided with Watermark [26]. For this channel, $B_{\text{max}} = 4$ kHz and $f_c = 6$ kHz. Fig. 3-(a) shows the time-varying impulse

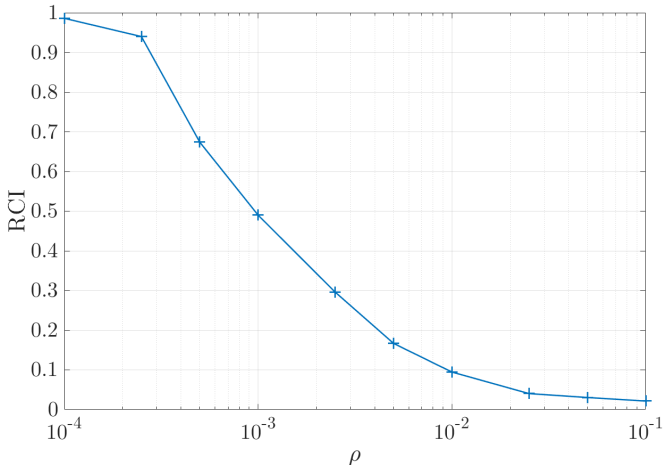
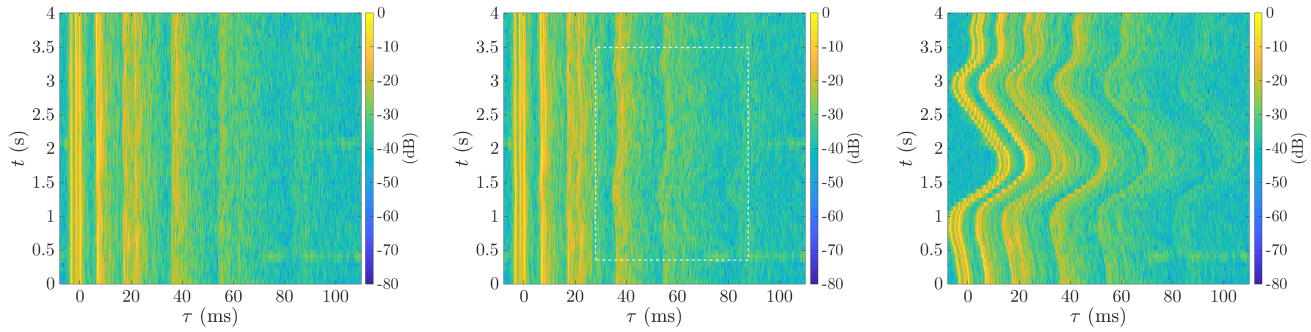


Fig. 2: Relative cyclostationary index as a function of ρ.

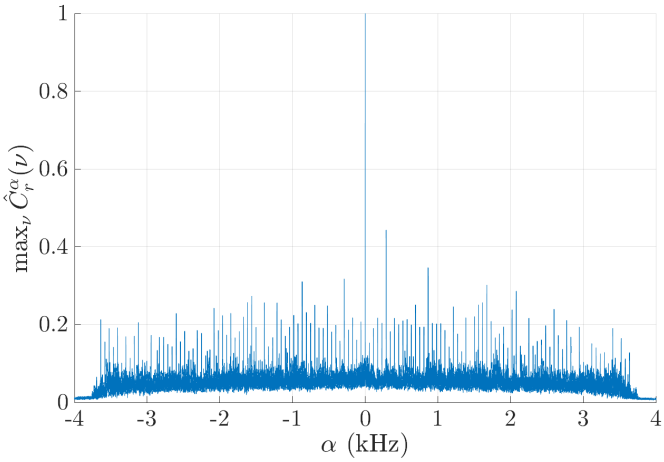


(a) (b) (c)

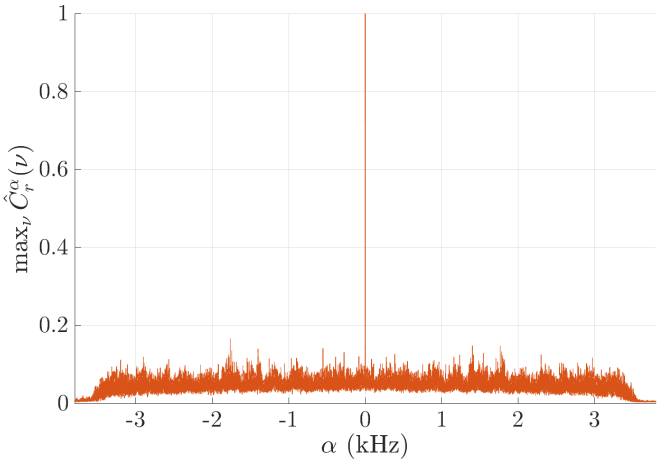
Fig. 3: KAU1 channel impulse response. (a) original measurement, (b) channel as perceived by Bob after dewarping, (c) channel as perceived by Eve.

response of this channel as measured at sea over the duration of a data packet.[2] It is very close to a single-scale channel. As expressed in (34), even though Bob knows the warping function, the equivalent channel $h_{w\to c\to w^{-1}}$ after dewarping may exhibit some artificial Doppler effect for later arrivals. This is illustrated in Fig. 3-(b), where slight fluctuations of late arrivals are visible, as highlighted in the white box. Moreover, in practice, the unintentional warping $\psi(t)$ due to the Doppler effect may not be perfectly corrected by the receiver. As discussed in App. B, this

[2]Note that the mean Doppler scale has been compensated first to better visualize the impulse response, i.e. $h_c\left(\tau+(1-\gamma_1)t, t\right)$ is shown. For more details see [29].



(a)



(b)

Fig. 4: Effect of warping on the spectral coherence density (no noise). (a) no warping, $w(t) = t$, (b) with warping $w(t) = (1 - \rho)t + \epsilon(t)$, $\rho = 0.05$ and $\epsilon(t)$ as shown in Fig. 1.

can also have a small effect on the inversion of $w(t)$. However, as illustrated in Sec. VI, these artifacts have little impact on the performance of the cooperative modem. To complement the analysis, Fig. 3-(c) shows the equivalent channel as perceived by Eve. For better visualization, the linear part ρt of $w(t)$ was compensated first, i.e. $h_{w \star c}(\tau + \rho t, t)$ is shown. As expected, warping creates an artificial channel with w-dependent time-varying drifts of the arrivals.

Finally, Fig. 4 confirms the theoretical result of Fig. 2 by showing the estimated ACS features without and with warping at the channel output. Estimates of the spectral coherence densities are

obtained with the strip spectral correlation analyzer (SSCA) [44], followed by a maximization over frequency ν. The power of the noise $\eta(t)$ was set to zero to focus on the effect of $w(t)$. The cyclic pattern of the original modulation scheme is clearly visible in Fig. 4-(a), where peaks at multiples of the symbol rate $D_s = 1/T_s \approx 57.7$ Bd are manifest. After warping with $\rho = 0.05$, Fig. 4-(b) shows that this pattern disappears, making blind signal identification or parameter estimation using standard cyclic estimators ineffective.

D. Advanced attacks

Although not specifically designed in the context of signal interception, two recent methods could be employed by Eve to mitigate the effect of intentional warping in the blind signal analysis process.

The first candidate approach described in [25, Sec. V] consists in estimating the warping function by angle demodulation. Based on the knowledge of a pair (u_0, α_0) where $R_x^{\alpha_0}(u_0) \neq 0$, the idea is to estimate the unwrapped phase of the signal $r^*(t)r(t+u_0)e^{-i2\pi\alpha_0 t}$ after low-pass filtering. The main advantage of this method is that it is very simple to implement. However, it is sensitive to noise and multipath. Therefore, it may not perform well in the context of covert communications.

An alternative approach, proposed in [45], is to find the inverse warping function that restores the regular cyclicity of the observed signal. Assume that the inverse warping function can be approximated as

$$w^{-1}(t) \approx \varphi(t) \triangleq \sum_{k=1}^{K} \theta_k d_k(t) = \boldsymbol{\theta}^T \mathbf{d}(t) \tag{38}$$

where $\{d_k(t)\}_{k=1,\cdots,K}$ is a linearly independent set of functions chosen according to prior information on w^{-1}. Based on the knowledge of a pair (u_0, α_0) where $R_x^{\alpha_0}(u_0) \neq 0$, the idea is then to find the vector $\boldsymbol{\theta}$ that maximizes the dewarped cyclic correlogram[3]

$$\left| \frac{1}{T_{\text{obs}}} \int_0^{T_{\text{obs}}} r^*(\varphi(t)) r(\varphi(t+u_0)) e^{-i2\pi\alpha_0 t} \mathrm{d}t \right|^2 . \tag{39}$$

In the context of underwater acoustics, this function must be modified to take into account the Doppler effect. By combining (12) and (39), the inverse warping function can be estimated by

[3]Note that a variation of this approach is also proposed in [45].

solving the following optimization problem

$$\max_{\mu_1,\mu_2,\boldsymbol{\theta}} \left| J^{\alpha_0}_{r_\varphi}(u_0) \right|^2 \tag{40}$$

where

$$J^{\alpha}_{r_\varphi}(u) \triangleq \frac{1}{T_{\text{obs}}} \int_0^{T_{\text{obs}}} r^*(\zeta(t)) r(\zeta(t+u)) e^{-i2\pi\alpha_0 t} \times e^{-i2\pi f_c(\varphi(t)-\varphi(t+u)+\zeta(t+u)-\zeta(t))} \mathrm{d}t \tag{41}$$

and

$$\zeta(t) \triangleq \psi^{-1}_{\mu_1,\mu_2}(\varphi(t)). \tag{42}$$

As opposed to the first approach, this attack can be robust to the channel effects and to the noise. However, its applicability depends on the computational complexity of solving the optimization problem (40). The objective function is not convex in $\boldsymbol{\theta}$ and K may be large. As discussed in [45, Sec. 7], the minimum dimension K is obtained with prolate spheroidal wave functions and satisfies $K \geq 4B_{w^{-1}}T_{\text{obs}}$, where $B_{w^{-1}}$ denotes the monolateral bandwidth of $w^{-1}(t)$. If the structure of the generator (36) is known (but not the key) to the eavesdropper, then (38) can be replaced with $w^{-1}(t) \approx t/(1-\rho) + \sum_{k=1}^{K} \theta_k d_k(t)$, where $K \geq 4\nu_\epsilon T_{\text{obs}}$. This inequality shows that the larger the fluctuation rate of $\epsilon(t)$, the larger the number K of basis functions required to dewarp the data. In other words, the complexity of estimating the warping function by Eve increases with ν_ϵ. It may then be tempting for Alice to choose a high value for ν_ϵ, but a compromise must be found as it may also increase the sensitivity of Bob's cooperative dewarping to possible time synchronization errors. The complexity of this attack is further discussed in Sec. VI-B where the method is evaluated in a realistic context.

Although these advanced attacks cannot be applied without prior knowledge of the original cyclostationary signature, we want the transmission to be as secure as possible. Therefore, an additional protection is proposed in the next section.

IV. Dispersive filtering

A. Design

An efficient way to prevent advanced attacks, such as those described in Sec. III-D, is to apply a transformation $\mathbb{D}$ such that the cyclic autocorrelation function of the transmitted signal does

not have energy where it is expected. Let us assume for the moment that no intentional warping is applied and let the set of lags $\mathcal{U}_x$ be defined as

$$\mathcal{U}_x^\alpha = \{u : R_x^\alpha(u) \neq 0\}. \tag{43}$$

Ideally, we would like to build a new signal $z(t) = (\mathbb{D}x)(t)$ such that

$$R_z^\alpha(u) \approx 0, \forall\, u \in \mathcal{U}_x^\alpha. \tag{44}$$

In addition, to maximize resistance to attack, it is desirable that the peak amplitude of the cyclic autocorrelation function be attenuated such that

$$\max_u |R_z^\alpha(u)| < \max_u |R_x^\alpha(u)| \tag{45}$$

for any cycle frequency of interest.

An easy way to do so is to apply, before transmission, a linear filter of impulse response $h_d(t)$ that takes advantage of the following result. Let $\circledast_t$ denote convolution with respect to t, if $z(t) = x(t) \circledast_t h_d(t)$ then [10, Eq. (3.83)]

$$R_z^\alpha(u) = R_x^\alpha(u) \circledast_u A_d^\alpha(u), \tag{46}$$

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

$$A_d^\alpha(u) \triangleq \int h_d^*(t) h_d(t+u) e^{-i2\pi\alpha t} \mathrm{d}t. \tag{47}$$

Based on the convolution expressed in (46), our idea is then to find a function $A_d^\alpha(u)$ that shifts and spreads the cyclic energy along the lag axis u so that (44) and (45) are satisfied. It is also important that the cooperative receiver is able to reverse the filtering process to recover the transmitted signal. This last constraint can be translated into the following requirement. Let B denote the (bilateral) bandwidth of $x(t)$, $h_d(t)$ must be designed such that there exists $u_1 \in \mathbb{R}$ for which

$$\chi_d^\ell(u) \approx K_\ell \mathrm{sinc}\left(\pi B(u - u_1)\right), \forall\, 1 \leq \ell \leq L \tag{48}$$

where K_ℓ is a random variable satisfying

$$\mathbb{E}\{|K_\ell|\} = \mathbb{E}\{|\lambda_\ell|\}, \forall\, 1 \leq \ell \leq L \tag{49}$$

and where $\chi_d^\ell(u)$ denotes the wideband ambiguity function defined as

$$\chi_d^\ell(u) \triangleq \int_{\mathbb{R}} h_d^*(t)\lambda_\ell(t+u)h_d(\psi_\ell(t+u))e^{i2\pi f_c(\psi_\ell(t+u)-(t+u))}\mathrm{d}t. \tag{50}$$

$\chi_d^\ell(u)$ represents the response of a filter matched to $h_d(t)$ when it is received with a delay u, compressed or dilated with a Doppler scale $\psi_\ell(t)$ and modulated with a random time-varying amplitude $\lambda_\ell(t)$. Therefore, if (48) and (49) are satisfied, it means that Bob can reverse the effect of the linear filter $h_d(t)$, to within a delay u_1, by simply applying a matched-filter at reception, while being robust to Doppler scale and Doppler spread. Another way to interpret (48) is that the output of the matched filter must be approximately flat over the bandwidth of interest, even in presence of Doppler. It is also important to note that if (48) is satisfied, the cooperative inversion of the filter $h_d(t)$ can be performed without any form of synchronization, making it easy to implement in practical systems.

Similarly to intentional warping, using a linear filter slightly affects the data rate. The ratio of spectral efficiency between $z(t)$ and $x(t)$ can be quantified by the following factor

$$\xi_g \triangleq \frac{T_{\text{max}}}{T_{\text{max}} + T_d} \tag{51}$$

where T_{max} is the duration of $x(t)$ and T_d denotes the duration of the filter's impulse response.

Without loss of generality, a simple and easily customizable way to satisfy (44), (45), (48) and (49) is to consider the family of dispersive filters that we define, in our context, as filters whose impulse responses satisfy

$$h_d(t) = a(t)e^{i\phi(t)}\mathbb{1}_{[-T_d/2,T_d/2]}(t), \tag{52}$$

with $a(t) \geq 0$. $\mathbb{1}(\cdot)$ denotes the indicator function and T_d is chosen to be greater than the inverse of the smallest cycle frequency of interest. For standard, UAC systems, this means that T_d must be greater than the symbol period T_s. This definition is very general and includes any kind of parametric AM-FM signals. Potential candidates can be found in Radar/Sonar references on ambiguity functions [46] or can even be bio-inspired [47], [48]. A specific example is studied in the next section.

B. Illustrations

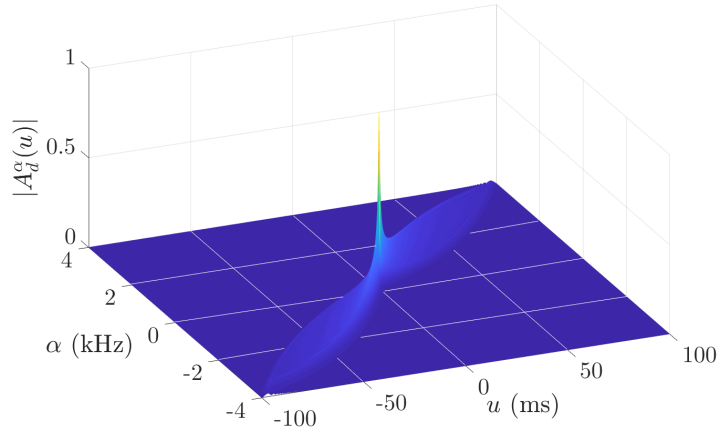
For illustration purposes, we consider the family of chirp-filters as a running example. In this case, $a(t)$ is a low-pass and smooth amplitude function and $\phi(t)$ is an oscillating phase. The main advantage of these filters is that the trade-off between all the constraints listed previously can be easily tuned by changing the value of a few parameters. It is illustrated next with, what we call, a Gompertz chirp, whose phase and amplitude satisfy

$$\begin{aligned} \phi(t) &= \frac{\pi B}{U-L}\left(2\mathrm{Ei}\left(be^{c(t+T_d/2)}\right) - (U+L)(t+T_d/2)\right) \\ a(t) &= \sqrt{e^{\left(be^{c(t+T_d/2)}+c(t+T_d/2)\right)}}, \end{aligned} \tag{53}$$

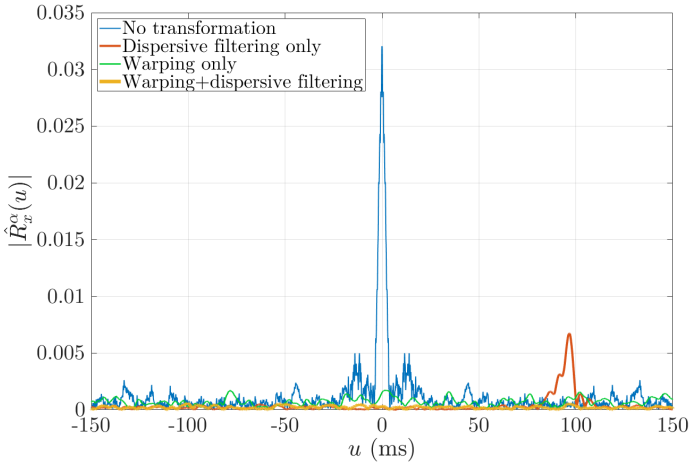
where $\mathrm{Ei}(x) = -\int_{-x}^{\infty} e^{-t}/t \,\mathrm{d}t$, $U = Be^{be^{cT_d}}$ and $L = Be^{b}$. The amplitude $a(t)$ is chosen to be proportional to the square-root of the second-order derivative of the phase to make the power spectral density function of $h_d(t)$ approximately flat in the bandwidth B [49]. We call this filter a Gompertz chirp because its instantaneous frequency is a truncated Gompertz function. It is parameterized by the pair (b, c) which makes it easy to generate a wide range of chirps, from (almost) linear or hyperbolic to sigmoid.

Fig. 5-(a) shows an example of the narrowband ambiguity function corresponding to the Gompertz filter. T_d is set to 100 ms, $B = 4$ kHz and $(b, c) = (-5, -5)$. It is clearly visible that the support of this ambiguity is not centered around $u = 0$ and that its amplitude decreases rapidly with α. Although linear filters do not eliminate cyclostationary features, this means that $h_d(t)$ attenuates, shifts, and spreads the cyclic autocorrelation function of $x(t)$ along the lag axis u so that (44) and (46) are satisfied. This is illustrated in Fig. 5-(b) where the cyclic correlogram (11) is shown for the waveform described in Sec. III-C and for the cycle frequency set to the chip rate. This figure was obtained at transmission, i.e. without a channel and without noise. As expected for such a waveform, if no transformation is applied, the cyclic correlogram has a strong peak around $u = 0$ that can be easily detected to blindly estimate the chip rate [12]. After filtering, this peak is less visible and is not where it is expected to be. Without knowledge of the filter parameters, it then becomes difficult for an eavesdropper to detect, interpret, and exploit this unusual CS signature, especially when combined with intentional warping.

Fig. 6 shows the wideband ambiguity function of the Gompertz chirp. The relative velocity ranges from ± 10 m/s and the relative acceleration was set to 0.1 m/s^2 so that $\gamma_{1,\ell} = 1 \pm 2/3 \cdot 10^{-3}$



(a)



(b)

Fig. 5: (a) Narrowband ambiguity function of the Gompertz filter and (b) its effect on the cyclic correlogram of the spread-spectrum signal described in Sec. III-C, $\alpha = 3636$ Hz.

and $\gamma_{2,\ell} = 1/3 \cdot 10^{-5}$ s^{-1}. 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 [50]. The RMS Doppler spread was set to 1 Hz. This figure shows that the Gompertz chirp is very robust to Doppler scale since the amplitude and the shape of $\chi_d^\ell(u)$ is almost invariant to velocity. A higher velocity only induces a greater static delay u_1, which is not problematic for most applications. For $T_d = 100$ ms, Doppler spread also has a limited effect and causes almost no loss compared to a time-invariant channel

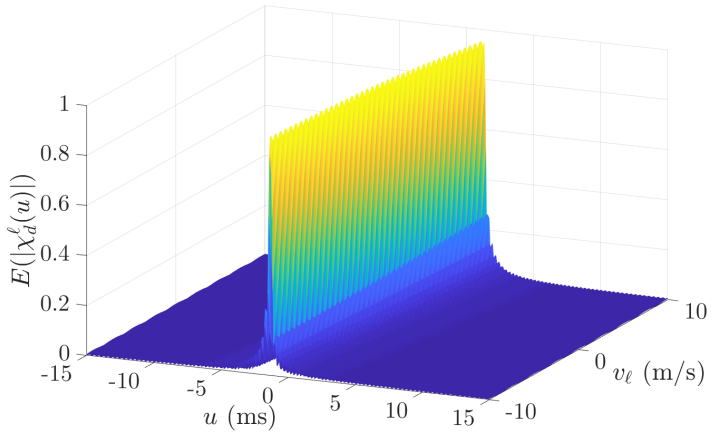


Fig. 6: Wideband ambiguity function of the Gompertz filter.

($\max \mathbb{E}\left\{|\chi_d^\ell(u)|\right\} \approx 1$). As a conclusion, (48) can be satisfied in operational scenarios so that the filtering plus matched filtering process will not affect the performance of the cooperative receiver.

Dispersive filtering also drastically affects the parameters of the transmission channel as perceived by Eve. Conversely, as the process can be reversed by Bob, the channel perceived after matched filtering remains very close to the real one. More precisely, with dispersive filtering but no warping, Bob perceives the following channel:

$$h_{d\to c\to d^*}(t) \triangleq \int_{\mathbb{R}}\int_{\mathbb{R}} h_c(\tau,u)h_d(u-\tau)h_d^*(u-t)\mathrm{d}\tau\mathrm{d}u, \tag{54}$$

whereas, without the knowledge of h_d, Eve perceives

$$h_{d\to c}(t) \triangleq \int_{\mathbb{R}} h_c(\tau,t)h_d(t-\tau)\mathrm{d}\tau. \tag{55}$$

As illustrated in Fig. 7 with the KAU1 channel impulse response measured at sea, the power-delay profile of $h_{d\to c\to d^*}(t)$ is similar to the one of $h_c(\tau,t)$, while it is harsher for $h_{d\to c}(t)$. There are no identifiable individual taps and the time-delay spread is larger. Blind synchronization or equalization will then become more difficult for Eve. Finally, as shown in Fig. 8, applying a dispersive filter will also tend to "Gaussianize" the signal and make it look more like noise. This is very likely to cause modulation classification techniques that are based on statistical moments and cumulants to fail [51].

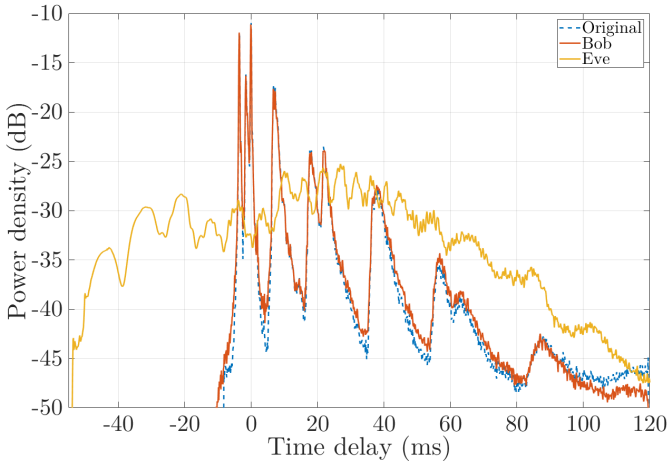


Fig. 7: Power delay profiles of the KAU1 channel as perceived by Bob and Eve after dispersive filtering.

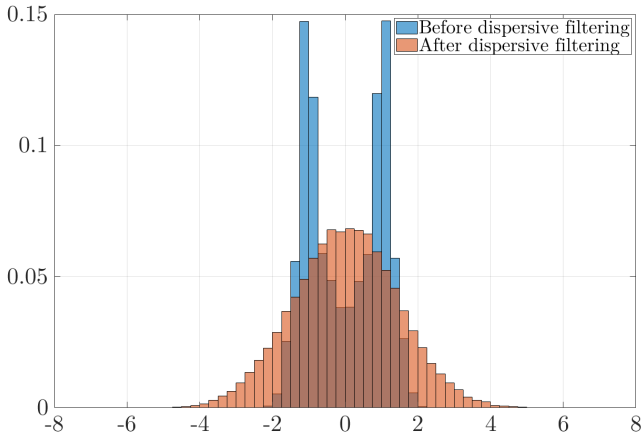
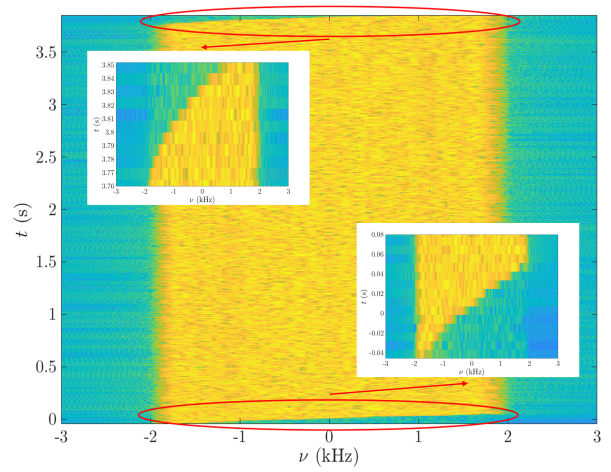


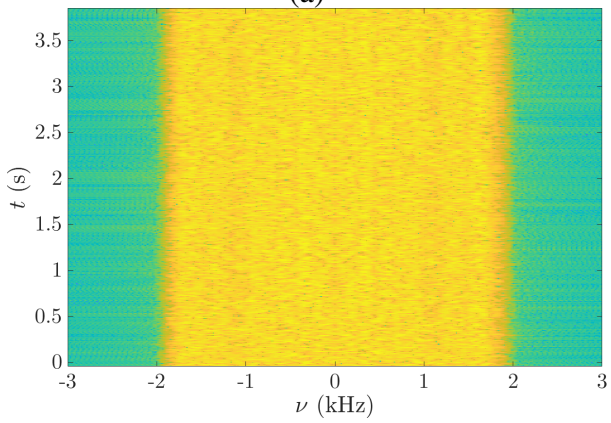
Fig. 8: Effect of the dispersive filter on the histogram of the real part of the noncoherent signal described in Sec. III-C.

C. Implementation aspects

When implementing dispersive filtering, care must be taken to ensure that the filter signature is not visible on time-frequency representations. As illustrated in Fig. 9-(a), during the transient and decay time of the convolution $z(t) = x(t) \circledast_t h_d(t)$, an explicit pattern revealing the presence of a dispersive filter may be visible on the spectrogram if the SNR is good. As shown in Fig. 9-(b), this signature can be easily hidden by adding a signal whose time-frequency signature fills



(a)



(b)

Fig. 9: Spectrogram of the transmitted signal after dispersive filtering. (a) without time-frequency filling, (b) with time-frequency filling.

the blanks of the spectrogram. In practice, such a signal can be obtained by filtering a random signal with the dispersive filter $h_d(t)$ and then adding the last samples at the beginning of $z(t)$ and the first samples at the end of $z(t)$. As shown in Sec. VI, the procedure does not impact the performance of preamble-based communication systems.

V. Unified framework

Since both warping and dispersive filtering can be represented as linear operators, the combination of the two transformations can be modeled as a linear time-varying filter. More specifically, let $y(t) = x(w(t))$ and $z(t) = y(t) \circledast_t h_d(t)$. As shown in Appendix C, the transmitted

signal $z(t)$ can be expressed as

$$z(t) = \int h_{w*d}(\tau, t) x(t-\tau) \mathrm{d}\tau \tag{56}$$

where

$$h_{w*d}(\tau, t) = \left| \left(w^{-1}\right)'(t-\tau) \right| h_d\left(t - w^{-1}(t-\tau)\right). \tag{57}$$

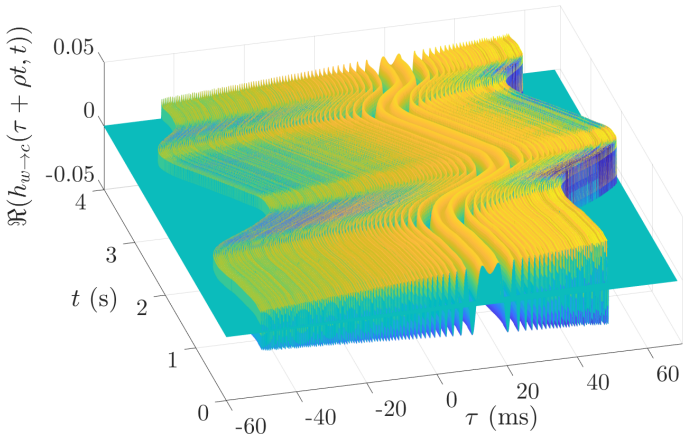
Given the complexity of $h_{w*d}(\tau, t)$, the main assumption of this paper is that its effects cannot be inverted by an eavesdropper without prior information on its parameters. An example of this time-varying impulse response is shown in Fig. 10. Again, to make this figure easier to interpret, the linear part ρt of $w(t)$ has been removed, i.e. $h_{w*d}(\tau + \rho t, t)$ is shown. Once the two transformations are applied, the ratio of spectral efficiency between $z(t)$ and $x(t)$ is

$$\xi_{w*g} \triangleq \frac{T_{\max}}{w^{-1}(T_{\max}) + T_d}. \tag{58}$$

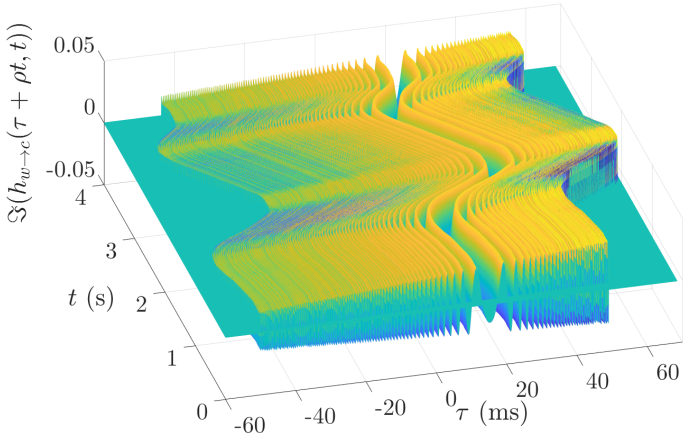
The overall cooperative procedure for transmission and reception is summarized in Fig. 11. The TRANSEC extensions are identified in dotted lines. First, the key generator provides the warping function $w(t)$ and the impulse response $h_d(t)$ of the dispersive filter to both the transmitter and the receiver. Once the data packet is ready to be transmitted by Alice, the signal is warped with the function $w(t)$ and then filtered with $h_d(t)$, or, equivalently, filtered with $h_{w*d}(\tau, t)$. If necessary, the time-frequency filling procedure discussed in Sec. IV-C is also applied. At reception, the matched filter $h_d^*(-t)$ is first applied by Bob and then the existing algorithms for detection, synchronization and Doppler compensation are run. The output signal is dewarped using resampling and then demodulated as well as decoded with the existing signal processing chain. Again, the main advantage of this approach is that it can be applied to any existing packet-based modems with little modifications. If a full black-box approach is desired at the receiver front-end, this can be achieved by encapsulating the existing packet into a super frame with an additional preamble. The cost is a slight reduction in data rate.

VI. Performance

The aim of this section is twofold. Firstly, to verify that the proposed transformations have little impact on the performance of the cooperative receivers and, secondly, that they are robust to possible eavesdropper attacks. Both noncoherent and coherent communication systems are considered and several attack scenarios are tested. The performance is evaluated under realistic



(a)



(b)

Fig. 10: Example of a time-varying impulse response corresponding to the application of both warping and dispersive filtering. (a) Real part (b) Imaginary part.

conditions using replay simulations with the Watermark dataset [26]. This dataset is made of more than 150 channel impulse responses measured at 5 different locations and frequencies. Watermark is run in SISO (single-input single-output) mode and all simulations are performed with an additive white Gaussian noise. To mimic at-sea conditions, the receiver has no prior knowledge about signal start, Doppler scale or channel impulse response. The warping function $w(t)$ is drawn at random for each Monte Carlo run, with $\rho = 0.05$ and $\nu_\epsilon = 0.5$ Hz. The duration of the impulse response of the dispersive filter is set to $T_d = 100$ ms.

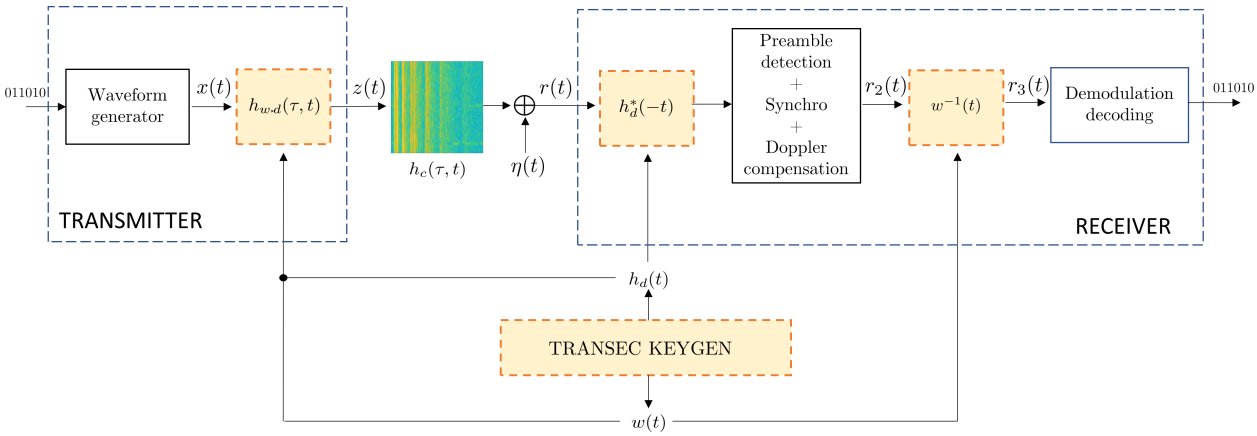


Fig. 11: Baseband representation of the full processing chain between Alice and Bob.

A. *Noncoherent communication*

The noncoherent scheme is the one described in Sec. III-C. The cooperative receiver uses a filter matched to a bank of Doppler-scaled preamble replicas for detection, synchronization and Doppler estimation. A bank of matched-filters combined with a noncoherent rake receiver is also used for symbol detection. The warping function $w(t)$ is inverted using resampling with a cubic spline interpolator. Results are examined versus the in-band SNR defined as

$$\text{SNR} = \frac{R_{\text{eff}}}{B} \times \frac{E_b}{N_0} \tag{59}$$

where E_b is the signal energy per information bit, N_0 is the power spectral density of the additive noise and the bandwidth is set to $B = 4$ kHz.

Fig. 12 shows the packet error ratio (PER) of the cooperative receiver as a function SNR for the five types of Watermark channels. A packet error occurs when one or more bits are in error at the decoder output, or when the packet is not detected. Plain lines represent the output of the replay simulation without transformation and dash lines with the application of $h_{w\star d}(\tau,t)$ and its inverse as described in Fig. 11. As expected, because of the differences in time and frequency selectivity, performance changes from one channel to another but the main observation is that, whatever the channel, the performance of the cooperative receiver is not affected by $h_{w\star d}(\tau,t)$. Therefore, although the equivalent channel after dewarping may exhibit some artificial Doppler for later arrivals (see Sec. III-C), this phenomenon is too small to impact the performance. The only cost is a slight loss in spectral efficiency with $\xi_{w\star g} \approx 0.93$ in this scenario.

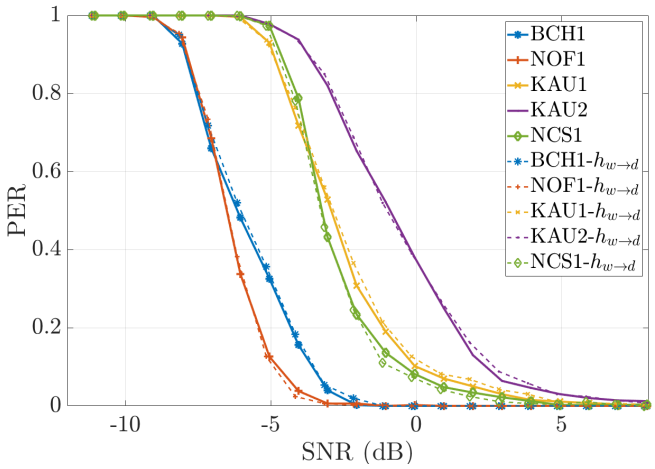


Fig. 12: Packet error ratio of the noncoherent modem.

The robustness to a cyclostationary analysis is illustrated in Fig. 13. We consider the scenario where Eve wants to estimate the symbol duration T_s of the transmitted signal. Since Watermark channels are almost single scales, this estimation is performed using the approach described in [12, Sec. IV-C], which is based on peak detection on the spectral coherence density. The performance is evaluated in terms of probability of correct estimation (PCE), which is defined as the probability that the relative estimation error is less than 1%, that is

$$\text{PCE} = \mathbb{P}\left(\left|\frac{\hat{T}_s - T_s}{T_s}\right| \leq 10^{-2}\right). \tag{60}$$

For each SNR, this probability is estimated with 100 Monte-Carlo trials. If the cyclostationary features are not hidden with $h_{w\to d}$, the symbol duration can be estimated easily in all channels. Excellent performance is achieved even for negative SNRs in the less challenging NOF1 and BCH1 channels. However, as soon as $h_{w\to d}$ is applied, $\widehat{\text{PCE}}$ becomes less than 1% for all SNRs making the cyclostationary analysis ineffective.

B. Coherent communication

Since the transformation is linear time-varying, it is legitimate to wonder whether an eavesdropper would be able to "equalize" this transformation using an advanced receiver. This question is eluded by considering a QPSK modem and a very pessimistic scenario where the eavesdropper knows everything about the transmitted signal (preamble, framing, modulation,

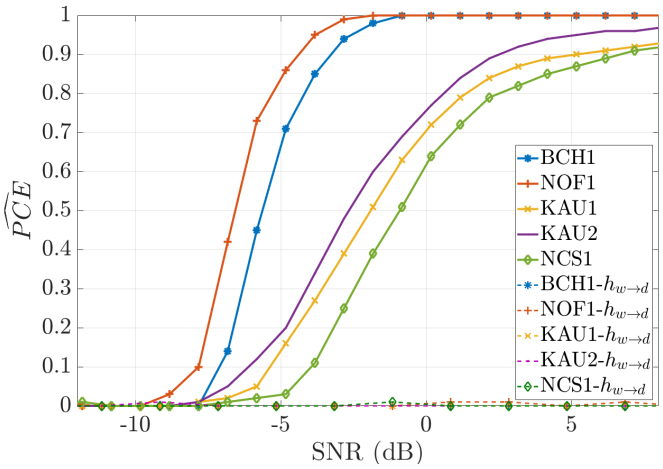


Fig. 13: Correct estimation rate of the symbol duration as a function of SNR.

symbol rate, coding, etc.) except the information bits and $h_{w\to d}$. To try compensate for the effect of $h_{w\to d}$, an adaptive turbo equalizer is used at reception with a PLL and a Doppler tracking loop [52]. The equalizer is trained over 1500 symbols and 1496 information bits per packet are transmitted. The total packet duration is approximately 1.03 s. The symbol rate is set to 3200 Bd and a rate-1/2 convolutional code is also used. At reception, synchronization is performed with a bank of matched filters, similar to the one used by the noncoherent receiver. To focus on the effect of $h_{w\to d}$, simulations are run with the BCH1-Hydrophone #1 channel, which is one of the most stable channel of the Watermark dataset. The PER is considered as the performance metric for this investigation. The outcome of the simulations is shown in Fig. 14, leading to the following observations. Similarly to the noncoherent modem, the use of $h_{w\to d}$ does not affect the performance of the coherent cooperative receiver. Although an advanced receiver is used to compensate for $h_{w\to d}$, the equivalent channel perceived by Eve is way too challenging to make it possible to achieve reasonable performance. 100% of the packets are erroneous.

To further test the robustness of our approach, the advanced attack described in (40) is evaluated. Again, a very advantageous scenario for the eavesdropper is considered. It is assumed that Eve knows the symbol rate and has access to the generator of $w(t)$, as described in (36), without knowing the pseudo-random key of that generator. To help solving (40), it can be shown that the inverse warping function can be well approximated as $w^{-1}(t) \approx \varphi(t) = t/(1-\rho)+\sum_{k=1}^{K} \theta_k d_k(t)$, with $K = 10$ and where $d_k(t)$ are prolate spheroidal functions [45]. The cost function (41) is

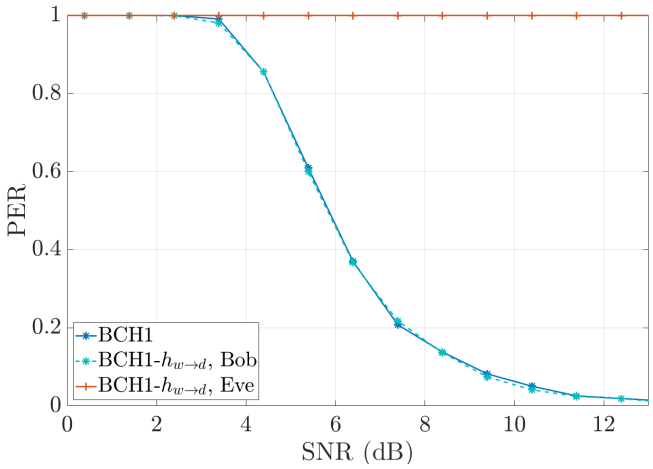


Fig. 14: Packet error ratio of the coherent modem.

evaluated for the warped QPSK signal, without dispersive filtering, at the output of the BCH1 channel for $u = 0$ and a SNR set to 15 dB. Fig. 15 shows an example of this cost as a function of θ_1 and θ_2 when θ_3 to θ_{10} as well as ρ, μ_1 and μ_2 are set to their optimal values. The peak indicates that the inverse warping function could be theoretically estimated using (41) when no dispersive filtering is applied. However, even in this ideal scenario, it also shows that the peak is very sharp and that the optimization problem if highly nonconvex. For a grid search optimization of the full set $\{\theta_k\}_{k=1,\cdots,10}$, we have estimated that the grid size should be greater than 10^{15} to capture the maximum of (41) in the the current scenario. This makes the attack described in Sec. III-D infeasible in practice. Moreover, even if computational complexity was not a problem, the use of a dispersive filter after warping makes the attack inefficient. In this case, $J^{\alpha}_{r_\varphi}(u)$ has no peak for any u because if $z(t) = x\left(w(t)\right) \circledast_t h_d(t)$ then $z\left(w^{-1}(t)\right) \neq x(t) \circledast_t h_d(t)$. In other words, for the eavesdropper to have any chance of success, the effect of the dispersive filter must first be compensated for before attempting to estimate the warping function. The two transformations are not interchangeable.

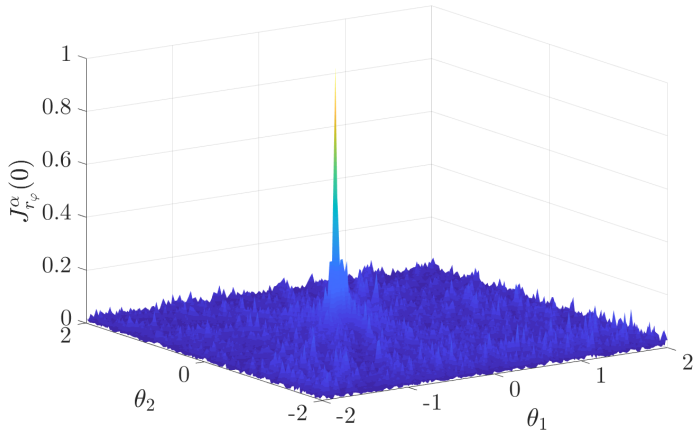


Fig. 15: Example of the cost function (41) when no dispersive filtering is applied.

VII. Conclusions

It is shown in this work that cyclostationary features, as perceived by an eavesdropper, can be easily distorted by applying a well-chosen time-varying filter before transmission. When this filter results from the application of a pseudo-random time warping function combined with a dispersive filter whose impulse response duration is greater than the symbol period, existing cyclostationary attacks are very likely to fail. This can be explained by the fact that the equivalent transmission channel, as perceived by the eavesdropper, becomes much more difficult than the actual propagation channel. There are no identifiable individual taps, the time delay spread is increased, and the arrivals drift very rapidly over time. The time-varying filter also tends to "Gaussianize" the signal and make it look more like noise, which is likely to cause moment and cumulant based modulation recognition techniques to fail. The price to pay for such a protection against attacks is a slight reduction in data rate.

Metrics that characterize the trade-off between the level of intentional distortion and the ability for a cooperative receiver to reverse its effect have been formulated. These metrics have also been illustrated with replay simulation using the Watermark dataset and a noncoherent spread-spectrum modem as well as a QPSK modem. In all scenarios, with a data rate reduction of 7%, the proposed method has been robust to cyclostationary attacks without affecting the packet error ratio of the cooperative transmission.

Moreover, it is important to emphasize that the proposed approach is of reasonable complexity

and can be applied to any existing transmission scheme. It acts as a plugin that does not require the complete design of a specific waveform and/or the implementation of a specific receiver. Therefore, it can be dynamically activated or not depending on the operational context. Finally, while the method is discussed in the context of underwater acoustic communications, we believe that it could easily be transposed to other communication scenarios.

APPENDIX A
EFFECT OF WARPING ON THE INSTANTANEOUS BANDWIDTH

Let $y(t) = x(w(t))$, with $w(t)$ a differentiable and strictly increasing function. Let $q(\cdot)$ denote an analysis function with a support of length T. The short-time Fourier transform of $y(t)$ can be expressed as

$$\begin{aligned} Y(t,\nu) &\triangleq \int_{\mathbb{R}} y(u)q(u-t)e^{-i2\pi\nu u}\mathrm{d}u && (61)\\ &= e^{-i2\pi\nu t}\int_0^T q(u)y(u+t)e^{-i2\pi\nu u}\mathrm{d}u && (62)\\ &= e^{-i2\pi\nu t}\int_0^T q(u)x(w(u+t))e^{-i2\pi\nu u}\mathrm{d}u. && (63)\end{aligned}$$

If $w(\cdot)$ is slowly varying over the interval $[t, t+T]$, using a first-order Taylor expansion, we then have the following approximation

$$w(u+t) \approx w(t) + uw'(t) \tag{64}$$

where $w'(t) > 0$ denotes the derivative of $w(t)$. Consequently

$$\begin{aligned} Y(t,\nu) &\approx e^{-i2\pi\nu t}\int_0^T q(u)x(w(t)+uw'(t))e^{-i2\pi\nu u}\mathrm{d}u && (65)\\ &= \frac{e^{-i2\pi\nu t}}{w'(t)}\int_0^{Tw'(t)} q\left(\frac{u}{w'(t)}\right)x(w(t)+u)e^{-i2\pi\frac{\nu}{w'(t)}u}\mathrm{d}u. && (66)\end{aligned}$$

As discussed in Sec. III-B, the warping must be moderate so as not to reduce the data rate too much. More specifically, if we consider that $\sup_t |w'(t) - 1| \ll 1$ and that the analysis window is slowly varying over the interval $[0, T]$, it is reasonable to assume that

$$\int_0^{Tw'(t)} q\left(\frac{u}{w'(t)}\right)x(w(t)+u)e^{-i2\pi\frac{\nu}{w'(t)}u}\mathrm{d}u \approx \int_0^T q\left(u\right)x(w(t)+u)e^{-i2\pi\frac{\nu}{w'(t)}u}\mathrm{d}u \tag{67}$$

so that

$$|Y(t,\nu)|^2 \approx \left|\frac{1}{w'(t)}X\left(w(t),\frac{\nu}{w'(t)}\right)\right|^2. \tag{68}$$

It then follows that

$$\int_{\mathbb{R}} P_y(t,\nu)\mathrm{d}\nu = \int_{\mathbb{R}} \left|Y(t,\nu)\right|^2 \mathrm{d}\nu \approx \frac{1}{w'(t)} \int_{\mathbb{R}} P_x(w(t),\nu)\mathrm{d}\nu. \tag{69}$$

Based on definition (25), we have

$$\bar{\nu}_y(t) \approx \bar{\nu}_x(w(t))w'(t) \tag{70}$$

so that

$$\int_{\mathbb{R}} \left(\nu - \bar{\nu}_y(t)\right)^2 P_y(t,\nu)\mathrm{d}\nu \approx w'(t) \int_{\mathbb{R}} \left(\nu - \bar{\nu}_x(w(t))\right)^2 P_x(w(t),\nu)\mathrm{d}\nu. \tag{71}$$

Therefore, by injecting (69) and (71) in (24), we can conclude that

$$\mathrm{IB}_y(t) \approx w'(t) \times \mathrm{IB}_x(w(t)). \tag{72}$$

APPENDIX B
EFFECT OF IMPERFECT DOPPLER SCALE COMPENSATION

As discussed in Sec. III-B, the cooperative receiver can only remove the effect of the intentional warping $w(t)$ if the effect of the Doppler scale has been removed first. However, in practice, the unintentional warping due to motion-induced Doppler scaling may not be perfectly estimated by the receiver. A common example is the case where the receiver assume a constant Doppler scale, i.e., $\psi(t) = \gamma_1 t$, whereas the actual Doppler effect is better modeled with $\psi(t) = \gamma_1 t + \gamma_2 t^2$ or even with a higher-order polynomial. This way of operating is generally justified by the fact that once the constant Doppler scale γ_1 is compensated for by resampling, the effect of the remaining terms is considered as an additional Doppler shift that can be tracked using closed-loop narrowband processing.

Let $\hat{\psi}(t)$ be the Doppler-induced warping function estimated by the receiver. If the standard receiver, i.e., without the TRANSEC plugin, has been correctly designed, it means that it is able to compensate the perturbations induced by the imperfect Doppler scale estimation, that is, the perturbations resulting from the effect of $\Delta\psi(t) \stackrel{\Delta}{=} \psi\left(\hat{\psi}^{-1}(t)\right) \neq t$. A way to measure the effect of this imperfect estimation once the TRANSEC plugin has been activated it to compare the function $w\left(\Delta\psi\left(w^{-1}(t)\right)\right)$ with $\Delta\psi(t)$. If there is no significant difference, it means that the performance of the receiver is not affected more by this imperfection than it already is when

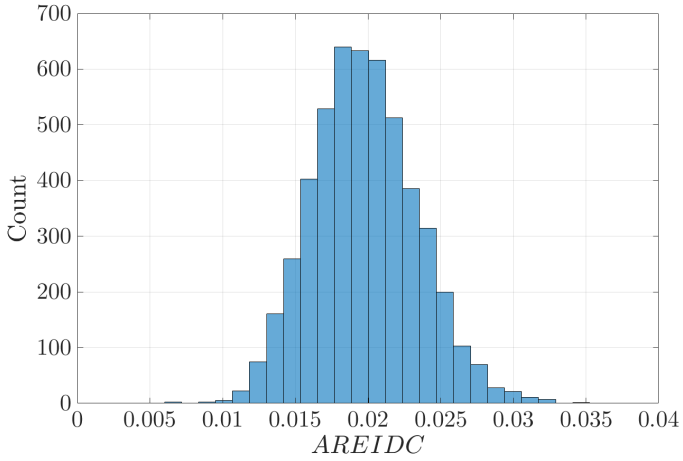


Fig. 16: Histogram of the average relative error due to imperfect Doppler scale compensation.

operating without the TRANSEC plugin. To quantify this difference, we define the average relative error due to imperfect Doppler scale compensation (AREIDC) as follows

$$AREIDC(w, \Delta\psi) = \frac{1}{T_{\text{max}}} \int_0^{T_{\text{max}}} \left| \frac{w\left(\Delta\psi\left(w^{-1}(t)\right)\right) - \Delta\psi(t)}{\Delta\psi(t) - t} \right| \mathrm{d}t. \tag{73}$$

Note that the normalization is done with $\Delta\psi(t) - t$ and not $\Delta\psi(t)$ because the closed-loop processing is usually designed to track the deviation from the nominal time scale t.

Fig. 16 shows the distribution of the AREIDC for a function $\Delta\psi(t)$ expressed as $\Delta\psi(t) = t + \frac{\gamma_2}{\gamma_1}t^2$. This corresponds to the typical scenario where Doppler resampling is applied only to compensate the constant scale γ_1. The result has been obtained with 5000 Monte-Carlo trials and for $T_{\text{max}} = 3.8$ s. At each trial, $w(t)$ is randomly chosen according to (36), with $\rho = 0.05$, and $\frac{\gamma_2}{\gamma_1}$ is chosen uniformly between values corresponding to minimum and maximum accelerations of 0.1 and 0.5 m.s^{-2}, respectively. The main observation is that the AREIDC is on the order of a few percents in this realistic scenario. This is quite small and means that if the receiver is designed to handle $\Delta\psi(t) \neq t$ with closed-loop processing, it should also handle the effect of $w\left(\Delta\psi\left(w^{-1}(t)\right)\right)$ without any modification.

APPENDIX C
COMBINATION OF WARPING AND DISPERSIVE FILTERING

Let $y(t) = x(w(t))$ and $z(t) = y(t) \circledast_t h_d(t)$. The transmitted signal then satisfies

$$\begin{aligned} z(t) &= \int h_d(u) y(t-u) \mathrm{d}u = \\ &\iint h_d(u) \delta\left(v - t + u + w(t-u)\right) x(t-u-v) \mathrm{d}v \mathrm{d}u = \\ &\int \underbrace{\left(\int h_d(\tau - v) \delta\left(\tau - t + w(t-\tau+v)\right) \mathrm{d}v \right)}_{\triangleq h_{w \to d}(\tau, t)} x(t-\tau) \mathrm{d}\tau. \end{aligned} \tag{74}$$

$h_{w \to d}(\tau, t)$ can then be written as

$$h_{w \to d}(\tau, t) = \int h_d(\tau - v) \delta\left(f(v)\right) \mathrm{d}v \tag{75}$$

where $f(v)$ has a root at $v_0(\tau, t) = \tau - t + w^{-1}(t-\tau)$. From the properties of the Dirac delta function, it follows that

$$h_{w \to d}(\tau, t) = \frac{h_d(\tau - v_0(\tau, t))}{|f'(v_0(\tau, t))|}. \tag{76}$$

Therefore,

$$\begin{aligned} h_{w \to d}(\tau, t) &= \frac{h_d(t - w^{-1}(t-\tau))}{|w'\left(w^{-1}(t-\tau)\right)|} \\ &= \left| \left(w^{-1}\right)'(t-\tau) \right| h_d\left(t - w^{-1}(t-\tau)\right). \end{aligned} \tag{77}$$

The last step follows from the inverse function rule [53, Ch. 5.3].

REFERENCES

[1] F.-X. Socheleau and S. Houcke, "Hiding cyclostationarity with dispersive filters for covert underwater acoustic communications," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*. IEEE, 2022, pp. 1–5.

[2] ATIS-0100523.2011, "ATIS Telecom Glossary," 2011.

[3] R. Diamant and L. Lampe, "Low probability of detection for underwater acoustic communication: A review," *IEEE Access*, vol. 6, pp. 19099–19112, 2018.

[4] P. A. van Walree, "Channel sounding for acoustic communications: techniques and shallow-water examples," *Research report, Norwegian Defence Research Establishment (FFI)*, 2011.

[5] A. Mahmood, M. Chitre, and H. Vishnu, "Locally optimal inspired detection in snapping shrimp noise," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1049–1062, 2017.

[6] A. Pottier, F.-X. Socheleau, and C. Laot, "Robust Noncooperative Spectrum Sharing Games in Underwater Acoustic Interference Channels," *IEEE Journal of Oceanic Engineering*, October 2017.

[7] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the development of secure underwater acoustic networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[8] A. et al. Hamilton, "Towards secure and interoperable underwater acoustic communications: Current activities in nato ist-174 research task group," *Procedia Computer Science*, vol. 205, pp. 167–178, 2022.

[9] R. Diamant, S. Tomasin, F. Ardizzon, D. Eccher, and P. Casari, "Secret key generation from route propagation delays for underwater acoustic networks," *IEEE Trans. Inf. Forensics Secur.*, 2023.

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

[11] C. M. Spooner, A. N. Mody, J. Chuang, and J. Petersen, "Modulation recognition using second-and higher-order cyclostationarity," in *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2017, pp. 1–3.

[12] F.-X. Socheleau, "Cyclostationarity of communication signals in underwater acoustic channels," *IEEE Journal of Oceanic Engineering*, 2023.

[13] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal processing*, vol. 89, no. 4, pp. 450–462, 2009.

[14] A. Bonvard, S. Houcke, R. Gautier, and M. Marazin, "Classification based on euclidean distance distribution for blind identification of error correcting codes in noncooperative contexts," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2572–2583, 2018.

[15] 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.

[16] J. A. Snoap, D. C. Popescu, J. A. Latshaw, and C. M. Spooner, "Deep-learning-based classification of digitally modulated signals using capsule networks and cyclic cumulants," *Sensors*, vol. 23, no. 12, pp. 5735, 2023.

[17] Z. Wu and T.C. Yang, "Blind cyclostationary carrier frequency and symbol rate estimation for underwater acoustic communication," in *2012 IEEE ICC*, 2012, pp. 3482–3486.

[18] J. Renard, L. Lampe, and F. Horlin, "Spatial sign cyclic-feature detection," *IEEE Transactions on signal processing*, vol. 61, no. 18, pp. 4521–4531, 2013.

[19] 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 WCNC*. IEEE, 2014, pp. 624–629.

[20] F.-X. Socheleau, S. Houcke, P. Ciblat, and A. Aissa-El-Bey, "Cognitive OFDM system detection using pilot tones second and third-order cyclostationarity," *Signal processing*, vol. 91, no. 2, pp. 252–268, 2011.

[21] Z. E. Ankaralı and H. Arslan, "Cyclic feature suppression for physical layer security," *Physical Communication*, vol. 25, pp. 588–597, 2017.

[22] G. Kaddoum, S. Gagné, and F. Gagnon, "Removing cyclostationary properties in a chaos-based communication system," *Circuits, Systems, and Signal Processing*, vol. 30, no. 6, pp. 1391–1400, 2011.

[23] M. Bouanen, F. Gagnon, G. Kaddoum, D. Couillard, and C. Thibeault, "An lpi design for secure ofdm systems," in *MILCOM 2012-2012 IEEE Military Communications Conference*. IEEE, 2012, pp. 1–6.

[24] J. Leśkow and A. Napolitano, "Nonrelatively measurable functions for secure communications signal design," *Signal processing*, vol. 87, no. 11, pp. 2765–2780, 2007.

[25] A. Napolitano, "Time-warped almost-cyclostationary signals: characterization and statistical function measurements," *IEEE Transactions on Signal Processing*, vol. 65, no. 20, pp. 5526–5541, 2017.

[26] 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.

[27] A. Napolitano, *Cyclostationary processes and time series: theory, applications, and generalizations*, Academic Press, 2019.

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

[29] P. A. van Walree, P. Jenserud, and M. Smedsrud, "A Discrete-Time Channel Simulator Driven by Measured Scattering Functions," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1628–1637, 2008.

[30] J. Li, Y. V. Zakharov, and B. Henson, "Multibranch autocorrelation method for Doppler estimation in underwater acoustic channels," *IEEE Journal of Oceanic Engineering*, vol. 43, no. 4, pp. 1099–1113, 2017.

[31] P. Ciblat, P. Loubaton, E. Serpedin, and G. B. Giannakis, "Asymptotic analysis of blind cyclic correlation-based symbol-rate estimators," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1922–1934, 2002.

[32] A. V. Dandawate and G. B. Giannakis, "Statistical tests for presence of cyclostationarity," *IEEE Transactions on signal processing*, vol. 42, no. 9, pp. 2355–2369, 1994.

[33] P. Jallon, "An algorithm for detection of DVB-T signals based on their second-order statistics," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, pp. 1–9, 2007.

[34] 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 DySPAN*. IEEE, 2007, pp. 212–215.

[35] B. Boashash, "Estimating and interpreting the instantaneous frequency of a signal. I. Fundamentals," *Proceedings of the IEEE*, vol. 80, no. 4, pp. 520–538, 1992.

[36] A. Carvallo Pecci, C. Laot, and A. Bourre, "Quadratic chirp modulation for underwater acoustic digital communications," in *OCEANS 2015-Genova*. IEEE, 2015, pp. 1–7.

[37] K. Marek, *An introduction to the theory of functional equations and inequalities*, Birkhäuser Basel, 2009.

[38] B.S. Sharif, J. Neasham, O.R. Hinton, and A.E. Adams, "A computationally efficient doppler compensation system for underwater acoustic communications," *IEEE J. Ocean. Eng.*, vol. 25, no. 1, 2000.

[39] T. Fusco, L. Izzo, A. Napolitano, and M. Tanda, "On the second-order cyclostationarity properties of long-code DSSS signals," *IEEE Transactions on Communications*, vol. 54, no. 10, pp. 1741–1746, 2006.

[40] F.-X. Socheleau, C. Laot, and J.-M. Passerieux, "Stochastic Replay of non-WSSUS Underwater Acoustic Communication Channels Recorded at Sea," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4838–4849, 2011.

[41] 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.

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

[43] 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.

[44] R. S. Roberts, W. A. Brown, and H. H. Loomis, "Computationally efficient algorithms for cyclic spectral analysis," *IEEE Signal Processing Magazine*, vol. 8, no. 2, pp. 38–49, 1991.

[45] W. A. Gardner, "Statistically inferred time warping: extending the cyclostationarity paradigm from regular to irregular

statistical cyclicity in scientific data," *EURASIP Journal on Advances in Signal Processing*, vol. 2018, no. 1, pp. 1–25, 2018.

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

[47] R. A Altes and E. Titlebaum, "Bat signals as optimally doppler tolerant waveforms," *The Journal of the Acoustical Society of America*, vol. 48, no. 4B, pp. 1014–1020, 1970.

[48] F.-X. Socheleau, E. Leroy, A. Carvallo Pecci, F. Samaran, J. Bonnel, and J.-Y. Royer, "Automated detection of antarctic blue whale calls," *The Journal of the Acoustical Society of America*, vol. 138, no. 5, pp. 3105–3117, 2015.

[49] P. Flandrin, "Time frequency and chirps," in *Wavelet Applications VIII*. International Society for Optics and Photonics, 2001, vol. 4391, pp. 161–175.

[50] 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.

[51] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: classical approaches and new trends," *IET communications*, vol. 1, no. 2, pp. 137–156, 2007.

[52] C. Laot and P. Coince, "Experimental results on adaptive mmse turbo equalization in shallow underwater acoustic communication," in *OCEANS'10 IEEE SYDNEY*. IEEE, 2010, pp. 1–5.

[53] J. Marsden and A. Weinstein, *Calculus I*, Springer Science & Business Media, 1985.