Dictionary-based Spread-Spectrum Modulation for Covert Underwater Acoustic Communications

Aurélien Bonvard, François-Xavier Socheleau, Sébastien Houcke, Philippe Courmontagne

Dictionary-based Spread-Spectrum Modulation for Covert Underwater Acoustic Communications

Aurélien Bonvard*, François-Xavier Socheleau*, Sébastien Houcke*, Philippe Courmontagne†

*IMT Atlantique, LabSTICC UMR CNRS 6285: {aurelien.bonvard,fx.socheleau,sebastien.houcke}@imt-atlantique.fr

†Naval Group: philippe.courmontagne@naval-group.com

***Abstract*—A covert underwater acoustic waveform is presented. The modulation scheme is based on a pseudo-random selection of spread-spectrum sequences from a dictionary. A specific aspect of this scheme is that each sequence has a distinct chip rate. The use of spreading sequences is a means of operating at low SNR, while the use of different chip rates strongly attenuates the cyclostationary signature, the objective being to maximize the robustness against eavesdropping attacks. Simulation results and sea trials show that communication can be successful at negative SNRs while being robust to cyclostationary analysis.**

***Index Terms*—Underwater Acoustic Communication, Covert Communication, Cyclostationarity**

I. Introduction

The underwater acoustic communication strategy described in this paper aims at transmitting short messages such as coordinates or mission orders under the constraint of covertness. Such a strategy is relevant in the context of communication between Autonomous Underwater Vehicles (AUVs) or with a surface vessel, possibly over long ranges.

Due to their propagation characteristics, acoustic waves suffer from a natural incompatibility with discretion. However, techniques known as LPI/LPD (Low Probability of Interception/Low Probability of Detection) have been developed to reduce this indiscretion and improve the security of communicating agents. These techniques can be divided into two main families: low signal-to-noise ratio (SNR) communication methods and methods based on steganography. The former consists in hiding the signal in the ambient noise to make the communication invisible to an eavesdropper. In most cases, the energy is spread over a wide band of the frequency spectrum using spreading sequences [1], [2] or by increasing the number of subcarriers [3]. In the second family, the strategy is to make the signal harmless in the environment from the point of view of an illegitimate observer. In this case, the information is transmitted in signals that mimic animals [4], [5] such as dolphin whistles or clicks, or even anthropogenic sounds such as pile driving [6].

Although attractive, steganography-based schemes are subject to significant implementation and environmental constraints. For instance, the camouflage signal must make sense within the soundscape of the transmission zone. Moreover, recent studies show that synthesizing this type of mimicking signal is technologically challenging due to limitations of the acoustic front-end. Entropy-based detectors are actually able to discriminate between real and synthesized bio-signals [7]. Therefore, to avoid these drawbacks, the method chosen in this study falls within the scope of low SNR communications and is based on a spreading technique.

Although spread spectrum waveforms limit the probability of interception, they remain vulnerable to the blind analysis of their parameters as performed by underwater signal intelligence systems. Among the various signal features that are used to blindly estimate the parameters of a transmitter, cyclostationarity is one of the most relevant [8]. In fact, the periodic behavior of the statistical properties of communication signal is a weakness from a security point of view. It can be used for signal detection, modulation recognition or for blind estimation of PHY layer parameters. Along the line of [9], we propose to integrate a mechanism into our waveform to reduce its cyclostationary signature. The main idea is to transmit a signal that is a concatenation of spreading sequences at different chip rates, pseudo-randomly picked from a dictionary.

This paper is organized as follows. Definitions related to the second-order cyclostationarity of communication signals are reviewed in Section II. Section III presents the dictionary used to generate the waveform and provides some illustrative examples. Finally, simulation and sea trial results are presented to demonstrate the performance of the proposed scheme.

II. Cyclostationarity

Let $X(t)$ be a stochastic process with mean and autocorrelation $\mathbb{E}[X(t)]$ and $R_X(t,\tau) = \mathbb{E}[X(t)X^*(t-\tau)]$ respectively. $X(t)$ is said to be cyclostationary in the wide-sense with period $T_0 > 0$ if its mean and autocorrelation are T_0-periodic functions of time, i.e.:

$$\begin{aligned} \mathbb{E}[X(t)] &= \mathbb{E}[X(t+T_0)], \forall t \in \mathbb{R} \\ R_X(t,\tau) &= R_X(t+T_0,\tau), \forall t,\tau \in \mathbb{R} \end{aligned}$$

Therefore, if $X(t)$ is cyclostationary in the wide sense with period $T_0 > 0$, its autocorrelation admits a Fourier series expansion:

$$R_X(t,\tau) = \sum_{\alpha \in I_X} R_X^\alpha(\tau) e^{j2\pi\alpha t}$$

where $I_X = \{\frac{k}{T_0}, k \in \mathbb{Z}\}$ is the set of cycle frequencies α and the Fourier coefficients $R_X^\alpha(\tau)$ are called cyclic autocorrelation functions defined as

$$R_X^\alpha(\tau) = \frac{1}{T_0}\int_0^{T_0} R_X(t,\tau)e^{-j2\pi\alpha t}dt.$$

Cyclostationary patterns can be revealed through various representations [10]. The one that is used in this work is the spectral coherence defined as

$$\mathcal{C}_X^\alpha(f) = \frac{\mathcal{S}_X^\alpha(f)}{[\mathcal{S}_X(f+\alpha/2)\cdot\mathcal{S}_X(f-\alpha/2)]^{\frac{1}{2}}}$$

where $\mathcal{S}_X$ is the power spectral density of $X(t)$ and $\mathcal{S}_X^\alpha$ is the cyclic spectrum

$$\mathcal{S}_X^\alpha(f) = \int_{\mathbb{R}} R_X^\alpha(\tau)e^{-j2\pi f\tau}d\tau.$$

III. Dictionary-based spread spectrum

We now describe the modulation scheme relying on a dictionary of spreading sequences.

A. Dictionary definition

Let us consider S symbols s_i to be transmitted (with $i \in [\![1, S]\!]$). Each symbol is associated with a signal, called an atom, chosen in a dictionary $\mathcal{D}$. In this study, these atoms are binary spreading sequences filtered with a root-raised cosine filter. For a given transmission, when the symbol alphabet is of size M, this dictionary contains exactly M classes C_m. Each class m is then made of L_m atoms g_l^m. That is

$$\begin{aligned}\mathfrak{D} &= \{C_m \mid m \in [\![1, M]\!]\}\\ \text{s.t. } C_m &= \{g_l^m(t) \mid l \in [\![1, L_m]\!],\, t \in [0, T_l^m[\}\end{aligned}$$

where T_l^m is the duration of the l-th sequence in this class. Each class contains several atoms representing one symbol. The generated waveform consists of concatenated atoms arbitrarily chosen in each class with respect to the associated symbol.

In our case of application, each atom is a binary spreading sequence. We chose to use Gold sequences for their good autocorrelation and cross-correlation properties. Let g be a Gold Sequence of length N_c, the resulting atom is obtained as follows

$$g(t) = \sum_{n=0}^{N_c-1} g[n]h(t-nT_c) \tag{1}$$

where $g[n]$ is the n-th element of the Gold sequence, T_c is the chip duration and h is a pulse shaping filter. Therefore, if the chip duration is the same for each atom, the symbol duration is $T_S = N_cT_c$.

The baseband representation of the transmitted signal is therefore

$$\begin{aligned}x(t) &= \sum_{i=1}^{S} g_{l_i}^{m_i}(t-iT_S)\\ &= \sum_{i=1}^{S}\sum_{n=0}^{N_c-1} g_{l_i}^{m_i}[n]h(t-iT_S-nT_c)\end{aligned} \tag{2}$$

where m_i is the class index associated to the i-th symbol and l_i is the index of the arbitrarily chosen atom in the m_i-th class.

As discussed and illustrated in [8], [11], the fact that a constant chip-rate is used can create a strong cyclostationary pattern. Therefore, to remove such a pattern, we propose to redefine each atom with its own chip duration. More specifically, within each class, we consider a real value coefficient $0 < \beta_l < 2$ such that the chip duration of the l-th atom is $\beta_l T_c$. As a consequence, the duration of a symbol spread by this atom is $T_S = N_c\beta_l T_c$ and, from equation (2), we define the new waveform $y(t)$ as

$$\begin{aligned}y(t) &= \sum_{i=1}^{S}\sum_{n=0}^{N_c-1} g_{l_i}^{m_i}[n]h(t-iN_c\beta_{l_i}T_c-n\beta_{l_i}T_c)\\ &= \sum_{i=1}^{S}\sum_{n=0}^{N_c-1} g_{l_i}^{m_i}[n]h(t-\beta_{l_i}T_c(iN_c-n))\end{aligned} \tag{3}$$

The total length of the generated signal is thus $T = N_cT_c\sum_{i=1}^{S}\beta_{l_i}$.

Within each class, each atom has therefore a different duration and a different spreading code. Through these two levels of diversity (binary Gold sequence and chip duration), the proposed waveform is designed to resist to detectors based on cyclostationary analysis.

B. Examples

To illustrate how this dictionary works, let us consider Table I where two bits are mapped to one symbol. Fig. 1 depicts an example of a dictionary $\mathcal{D}$ with $M = 4$ classes and with $L_m = 4$ atoms per class. It also shows the pointed classes for a given binary sequence to modulate. With respect to Table III-B, the first two bits are mapped to symbol S_1 and thus to class C_1. Notice that bits 3 and 4 are also mapped to S_1. Bits 5 and 6 point to C_0 (S_0), and finally, bits 7 and 8 point to C_2 (S_2). Although the first two two pairs of bits point to the same class C_1, the associated spreading sequences in the transmitted signal can be different. In fact, given a symbol S_i, the associated spreading sequence is pseudo-randomly chosen in C_i. Moreover, since each atom is stretched or compressed by different coefficients β_l ($l \in [\![1, 4]\!]$), the cyclostationary signature is removed.

This impact on the cyclostationary pattern is illustrated in Fig. 2, Fig. 3 and Fig. 4. In these examples, this pattern is observed through the spectral coherence $\mathcal{C}_y^\alpha(f)$ of the transmitted signal maximized with respect to the frequency

TABLE I
Mapping example

Bit 1	Bit 2	Symb.	Class
0	0	S_0	C_0
0	1	S_1	C_1
1	1	S_2	C_2
1	0	S_3	C_3

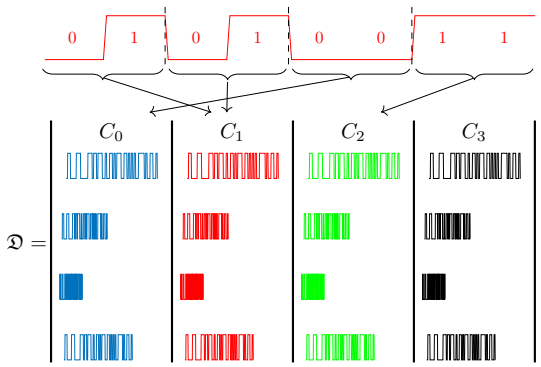

Fig. 1. Illustration of a 4-classes dictionary with 4 atoms per class.

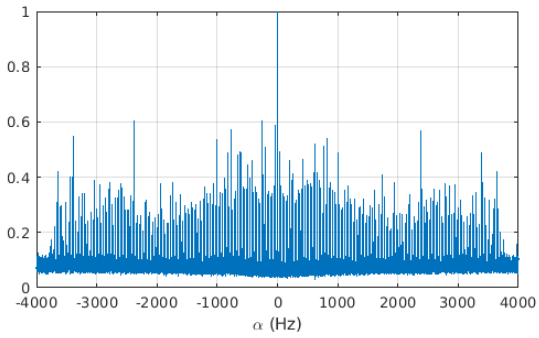

Fig. 2. Spectral coherence of the waveform with a constant chip rate.

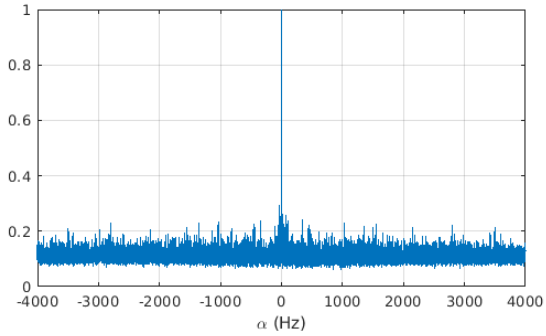

Fig. 3. Spectral coherence of the waveform with varying chip rates.

f [8]. Estimates of the spectral coherence are obtained with the strip spectral correlation analyzer [12]. Fig. 2 shows the scenario with $\beta_l = 1$, for all l, i.e., the same chip rate is used for all sequences. In this case, the cyclic pattern is clearly visible. Peaks at multiples of the symbol rate $D_S = 1/T_S$ are manifest [8], [11], which is a security vulnerability. An eavesdropper can use this pattern to detect the signal and to estimate its modulation parameters. In the case with varying β_l, this periodicity disappears (Fig. 3) and the spectral coherence has a very similar behavior to that of a white Gaussian noise (Fig. 4). The waveform then becomes much more robust against eavesdropping attacks.

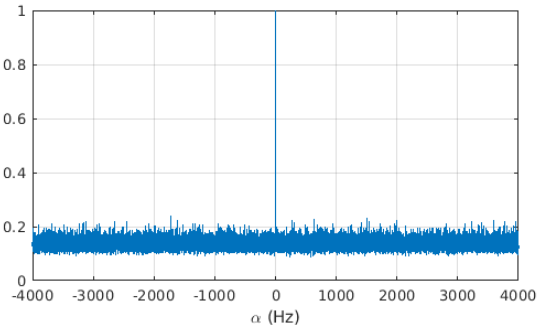

Fig. 4. Spectral coherence of white Gaussian noise.

IV. Simulation Results

The aim of this section is twofold. Firstly, to quantify the effect of the varying scaling factor β_l on the cyclostationary pattern and, secondly, to verify that this factor has little impact on the performance of the cooperative receiver. In all simulations, $y(t)$ is generated from a 4-class dictionary and each class contains 4 different spreading sequences. N_c is set to 63, $T_c \approx 0.25$ ms and 116 symbols are transmitted. A rate-1/2 convolutional code and m-sequence preamble are also used, resulting in a useful data rate of 47 bit/s. The receiver operates in a noncoherent mode. It 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 output of the pseudo-random generator used to pick the spreading sequences within each class is known to the receiver. The performance is evaluated under realistic conditions using replay simulations with the Watermark dataset [13].

A. Relative Cyclostationary Index

To quantify the impact of the scaling factor β_l on the cyclostationary pattern, we use the relative cyclostationary index (RCI) defined as follows [14]

$$\text{RCI} = \frac{\max\limits_{|\mu|<1} \sum\limits_{\alpha \in I_x} \int_{\mathcal{R}} \left| R_y^{(1+\mu)\alpha}(\tau; T_{\text{obs}}) \right|^2 d\tau}{\sum_{\alpha \in I_x} \int_{\mathcal{R}} \left| R_x^{\alpha}(\tau; T_{\text{obs}}) \right|^2 d\tau} \quad (4)$$

where I_x denotes the set of cycle frequency of $x(t)$, i.e., when $\beta_l = 1$, for all l. The cyclic autocorrelation functions are computed over the duration T_{obs} of a packet duration. This positive index compares the energy of the signal in the cyclic domain with and without varying chip duration. The maximization over μ is meant to make the index scale invariant. This means that, for any value β_l, if it is constant and does not depend on the atom index, the RCI will be equal to one, indicating that there is still a strong cyclostationary pattern.

Fig. 5 shows the RCI as a function of the variation range for β_l. This range is controlled by a parameter ϵ such that β_l is uniformly distributed in the interval $[\beta_{min}; \beta_{max}]$, where

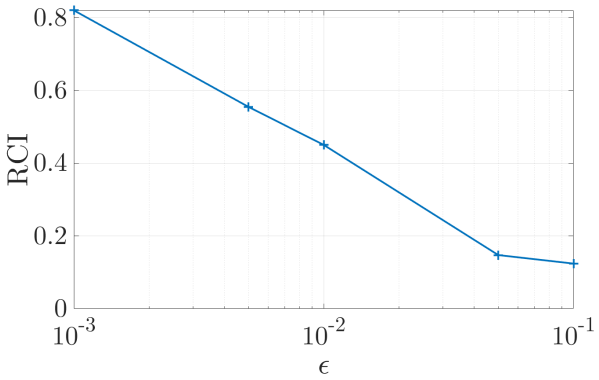

Fig. 5. Relative cyclostationary index as a function of ϵ.

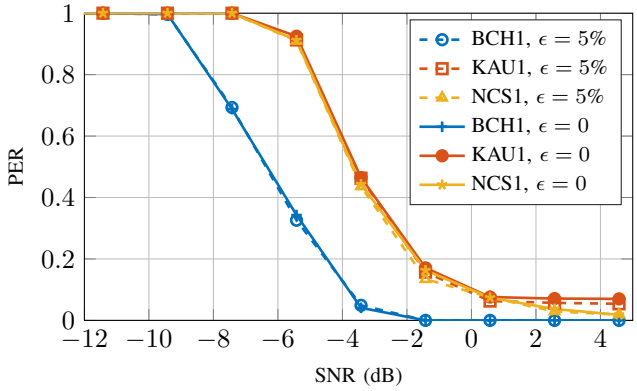

Fig. 6. Packet error ratio (PER) in Watermark channels with a constant chip rate (solid lines) and with a varying chip rate between atoms (dashed lines)

$\beta_{min} = 1 - \epsilon$ and $\beta_{max} = 1/(1-\epsilon)$. As expected, the cyclostationary pattern gets weaker as the variation range increases. In our context, a value of $\epsilon = 5\%$ provides a sufficient protection against cyclostationary analysis.

B. Packet error ratio

A performance comparison of the strategy with varying chip rates (dashed lines), controlled by $\epsilon = 0.05$, with the constant chip rate case with $\epsilon = 0$ (solid lines) is shown in Fig. 6. Performance is evaluated in terms of packet error ratio (PER) as a function of SNR. An error is counted when a packet contains faulty bits after decoding or when a packet is lost. The operating range of each scheme is evaluated for three Watermark channels, namely BCH1, KAU1, NCS1 [13]. These channels are replayed through their time-varying impulse responses measured during sea trials. Here is brief description of these channels.

- NCS1 was measured on Norway's continental shelf: no stable paths, and the coherence time is of the order the 100 ms.
- BCH1 was measured in the commercial harbour of Brest in France: multi-path channel, large number of trailing paths.
- KAU1 was measured in shallow water off the western side of Kauai, Hawaii, USA: clusters of arrivals whose Doppler spread increases with an increasing delay.

For KAU1 and NCS1 channels, we observe a 3 dB loss relative to the performance in the BCH1 channel. This is expected because of the stronger time and/or frequency selectivity of KAU1 and NCS1 compared to BCH1. More importantly, the main observation here is that having a nonconstant β_l does not affect much the performance. In short, the additional security offered by this transmission strategy is not paid back by a loss in performance.

V. Sea trials

A. Test description

The sea trials took place in June 2023 in the Mediterranean Sea, about 60 km off the coast of Toulon, France. The objective was to establish a communication link between two points for different distances in deep water conditions. Transmission and reception were performed at static points. As shown in Fig. 7, the transmitter was submerged at a depth of 50 m. On the receiving side, a hydrophone was positioned at a depth of 110 m. During the experiment, several distances L were tested: 100 m, 500 m, 1500 m, 2500 m, 3500 m and 8000 m. The signal was transmitted in a 4 kHz bandwidth centered at 18 kHz. The waveform parameters were identical to those described in Sec. IV.

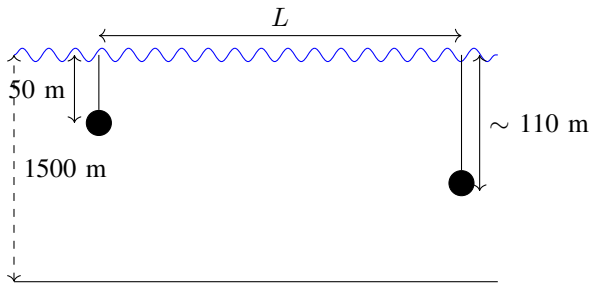

Fig. 7. Sea trial configuration.

B. Performance

The at-sea performance of the proposed scheme is presented in Table II. The first and second line give the PER values with varying and fixed chip duration, respectively. For each configuration, the results are averaged over 10 packets.

TABLE II
AT-SEA PERFORMANCE

L	100 m	500 m	1500 m	2500 m	3500	8000 m
$\epsilon = 0.05$	0	0	0	0.4	0.2	0
$\epsilon = 1$	0	0	0	1	0.3	0

Similarly to the simulation results, changing the chip duration had no impact on the packet error ratio. Moreover, note that in both scenarios, at $L = 2500$ m and $L = 3500$ m,

a large number of packets were lost. Two main causes were responsible for these losses: (i) inter-packet interference due to the long delay of the bottom-refracted path, and (ii) shadow zones where the SNR was too low to detect packets.

VI. Conclusion

We proposed a covert underwater communication strategy based on the pseudo-random picks of binary spread-spectrum sequences in a dictionary. By using sequences with different chip rates, we managed to reduce the cyclostationary signature of such a waveform. Replay-based simulations with the Watermark channels as well as sea trials showed that a chip-rate variation of $\pm$ 5% between sequences is sufficient to defeat standard cyclostationary attacks. We also showed that the objective of covertness is achievable without losing performance in terms of packet error ratio. Future work includes the addition of a coherent mode to increase the data rate, as well as conducting further experiments to determine the operational limit of our solution in terms of distance.

References

[1] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, "Covert underwater acoustic communications," *The Journal of the Acoustical Society of America*, vol. 128, no. 5, pp. 2898–2909, 2010.

[2] H.-P. Ren, C. Bai, Q. Kong, M. S. Baptista, and C. Grebogi, "A chaotic spread spectrum system for underwater acoustic communication," *Physica A: Statistical Mechanics and its Applications*, vol. 478, pp. 77–92, 2017.

[3] G. Leus and P. A. Van Walree, "Multiband ofdm for covert acoustic communications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1662–1673, 2008.

[4] S. Liu, G. Qiao, and A. Ismail, "Covert underwater acoustic communication using dolphin sounds," *The Journal of the Acoustical Society of America*, vol. 133, no. 4, pp. EL300–EL306, 2013.

[5] J. Jia-jia, W. Xian-quan, D. Fa-jie, F. Xiao, Y. Han, and H. Bo, "Bio-inspired steganography for secure underwater acoustic communications," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 156–162, 2018.

[6] S. Liu, M. Wang, T. Ma, G. Qiao, and M. Bilal, "Covert underwater communication by camouflaging sea piling sounds," *Applied Acoustics*, vol. 142, pp. 29–35, 2018.

[7] P. Casari, J. Neasham, G. Gubnitsky, D. Eccher, and R. Diamant, "Acoustic projectors make covert bioacoustic chirplet signals discoverable." *Scientific Report*, vol. 13, 02 2023.

[8] F.-X. Socheleau, "Cyclostationarity of communication signals in underwater acoustic channels," *IEEE Journal of Oceanic Engineering*, pp. 1–23, 2022.

[9] 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)*, 2022, pp. 1–5.

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

[11] 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.

[12] 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.

[13] P. A. van Walree, F.-X. Socheleau, R. Otnes, and T. Jenserud, "The watermark benchmark for underwater acoustic modulation schemes," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1007–1018, 2017.

[14] F.-X. Socheleau, C. Laot, and S. Houcke, "Cyclostationary feature distortion for secure underwater acoustic transmissions," *submitted*, 2024.