Covert underwater acoustic communications

Jun Ling, Hao He, Jian Li,[a)] and William Roberts
Department of Electrical and Computer Engineering, University of Florida, Gainesville, Florida 32611

Petre Stoica
Department of Information Technology, Uppsala University, Uppsala SE-751 05, Sweden

(Received 30 June 2010; revised 31 August 2010; accepted 3 September 2010)

Low probability of detection (LPD) communications are conducted at a low received signal-to-noise ratio (SNR) to deter eavesdroppers to sense the presence of the transmitted signal. Successful detection at intended receiver heavily relies on the processing gain achieved by employing the direct-sequence spread-spectrum (DSSS) technique. For scenarios that lack a sufficiently low SNR to maintain LPD, another metric, referred to as low probability of interception (LPI), is of interest to protect the privacy of the transmitted information. If covert communications take place in underwater acoustic (UWA) environments, then additional challenges are present. The time-varying nature of the UWA channel prevents the employment of a long spreading waveform. Furthermore, UWA environments are frequency-selective channels with long memory, which imposes challenges to the design of the spreading waveform. In this paper, a covert UWA communication system that adopts the DSSS technique and a coherent RAKE receiver is investigated. Emphasis is placed on the design of a spreading waveform that not only accounts for the transceiver structure and frequency-selective nature of the UWA channel, but also possesses a superior LPI. The proposed techniques are evaluated using both simulated and SPACE'08 in-water experimental data.

© *2010 Acoustical Society of America.* [DOI: 10.1121/1.3493454]

PACS number(s): 43.60.Dh, 43.60.Bf [EJS] Pages: 2898–2909

I. INTRODUCTION

Achieving reliable communication over underwater acoustic (UWA) channels has long been recognized as a challenging problem owing to the scarce bandwidth available and the double spreading phenomenon, i.e., spreading in both the time (multipath delay spread) and frequency domains (Doppler spread).[1] Delay and Doppler spreading is inherent to many practical communication channels, but are profoundly amplified in UWA environments.[2] Double spreading complicates the receiver structure and makes it difficult to extract the desired symbols from the incoming measurements.

Telemetry systems adopting direct-sequence spread-spectrum (DSSS) based modulation techniques are conventionally referred to as operating at low data rates. Existing literature regarding low data rate UWA communications is extensive.[3–13] By sacrificing the data rate, DSSS techniques exploit frequency diversity in frequency-selective UWA channel and benefit from spreading gain to allow many co-channel users. At the receiver side, decentralized reception schemes encompass nonlinear equalization, including hypothesis-feedback equalization,[7] and linear equalization, including RAKE receivers.[14] Performance comparisons of hypothesis-feedback equalization and RAKE reception are presented by Blackmon *et al.*[8]

In this paper, we consider a single user scenario with a coherent RAKE reception scheme. Although the coherent RAKE receiver cannot sufficiently combat severe inter- or intra-symbol interferences in a frequency-selective UWA channel, the adverse effects of the interferences can be alleviated by carefully designing the spreading waveforms.[15] Good waveform design, which accounts for practical concerns such as the modulation scheme, the channel characteristics, etc., allows for a simple and efficient reception scheme (RAKE, for example). An ideal spreading waveform, whose aperiodic correlations over certain time lags are zero, can effectively suppress inter- or intra-symbol interferences. The m-sequence, for example, is a popular spreading waveform employed in UWA channels due to its good correlation properties.[6] M-sequences, as well as most other existing practical spreading waveforms, are constructed in a deterministic and systematic manner with strict constraints on the chip length. These features, as will be discussed in the sequel, make such waveforms unattractive for covert UWA communications.

In a time-invariant channel, as long as the spreading waveform is long enough and at the cost of a reduced data rate, a DSSS-based modulation scheme can maintain satisfactory detection performance at an arbitrarily low chip SNR. A low chip SNR serves to deter eavesdroppers to detect the presence of the transmitted signal, while still ensuring good detection performance at the intended receivers. This type of covert communication strategy is referred to as a low probability of detection (LPD) scheme.[6,16] The key challenge imposed by LPD communications taking place in UWA environments is proper selection of a waveform length that best suits not only the system requirements, but also the channel conditions. The length of the spreading waveform cannot be increased without explicitly accounting for the

[a)] Author to whom correspondence should be addressed. Electronic mail: li@dsp.ufl.edu time-varying nature of the UWA channel. Although a flexible chip length is preferable, many existing spreading waveforms have strict length constraints. Although considered, LPD does not form the main focus of this paper, as it is difficult to formulate accurately and it depends on knowledge that is generally not available a priori. Such knowledge includes, for example, channel conditions and the locations of eavesdroppers.

Since the processing gain cannot be very large due to channel variations, the incoming chip SNR must be increased to maintain satisfactory detection performance with coherent RAKE. A direct consequence of boosting the incoming chip SNR is degraded LPD performance (i.e., the presence of the transmitted signal can be detected more easily by an eavesdropper). To protect the privacy of the transmitted signal, another metric, referred to as low probability of interception (LPI),[6] can be considered. LPI can be ensured in a variety of ways, for example, via the use of an off-the-shelf encryption technique during the source coding or channel coding stage. In this paper, we investigate the LPI property solely from a spreading waveform design aspect. A spreading waveform that is constructed in a deterministic and systematic manner, such as an m-sequence, is not a viable candidate waveform since an eavesdropper can exhaustively attempt all possible waveforms. A more favorable spreading waveform would possess unrestricted phase values (not from a finite alphabet) and flexible length. Note that solely from an LPI point of view, a random phase spreading waveform (i.e., the phase of each chip involved is independently and uniformly distributed between 0 and 2π) is an attractive candidate waveform. As we will show in numerical examples, the detection performance of different realizations of the random phase waveform exhibits considerable variations due to the unoptimized correlations. Yet, starting with a random phase initialization, the algorithms presented by Stoica *et al.*[17] and Li *et al.*[18] can be adopted to refine the waveform properties. Specifically, aside from the flexible length and the arbitrary phase values originally possessed by the random phase waveform, the so-obtained waveform is further entailed with good correlation properties. Herein, two such algorithms, referred to as the cyclic approach (CA)[18] and the weighted CA new (WeCAN) algorithm,[17] are evaluated.

This paper is organized as follows. Section II formulates the problem. Section III explores the characteristics of the spreading waveforms that facilitate coherent RAKE reception, and provides a general discussion on spreading waveform design. Section IV presents the simulation results, as well as the in-water experimental results using the data gathered in the 2008 Surface Processes and Acoustic Communications Experiment (SPACE'08), which was conducted by the Woods Hole Oceanographic Institution (WHOI) at the coast of Martha's Vineyard, MA. The paper is concluded in Section V.

The main contribution of this paper is an approach to achieve LPI communications via the employment of state-of-the-art waveforms. Specifically, flexible length and random phase ensure LPI, and the optimized correlation properties facilitate the coherent RAKE reception in the sense of effectively and efficiently suppressing the inter- and intra-symbol interferences. Moreover, the effectiveness of such spreading waveforms is verified by SPACE'08 in-water experimental results.

Notations: Matrices and column vectors are denoted, respectively, by boldface uppercase and lowercase letters. $(\cdot)^T$ and $(\cdot)^H$ refer to the transpose and the conjugate transpose of vectors or matrices, respectively. $(\cdot)^*$ denotes the complex conjugate for scalars. $\|\cdot\|$ is the vector Euclidean norm or matrix Frobenius norm and $|\cdot|$ is the scalar norm. $\mathbf{I}$ is the identity matrix with appropriate dimensions, and $\hat{x}$ denotes the estimate of x. Other mathematical symbols are defined after their first appearance.

II. PROBLEM FORMULATION

Suppose a transmitter maps source bits to payload symbols using Gray coded quadrature phase-shift keying (QPSK), and each QPSK payload symbol in $\{s_n\}$ is spread by a common unimodular spreading waveform $\mathbf{x}$ consisting of P chips, i.e., $\mathbf{x}=[x_1 \ldots x_P]^T$. The resulting phase-modulated waveforms $\{s_n\mathbf{x}\}$ are then up-converted to the carrier frequency and transmitted via UWA channels in the presence of a strong noise background. It is well-known that the insertion of a guard interval between two successive phase-modulated waveforms or the use of a cyclic prefixed spreading waveform can effectively combat the inter-symbol interference. These methods, however, are not pursued herein since they are generally not preferable from a data rate efficiency point of view, especially when the channel length is long.

We assume a block-fading channel, in which the channel impulse response (CIR) remains stationary over at least one symbol period, and we let $\mathbf{h}_n=[h(n,1)\ldots h(n,R)]^T$ characterize the CIR vector over the n^{th} symbol period (i.e., during the transmission of $s_n\mathbf{x}$) with R resolved channel taps ($P>R$ in general). We further assume that sampling and synchronization procedures have already been employed, and that the sampled complex baseband signals are available at the receiver (the topic of synchronization will be addressed in Section IV B). Note that although our emphasis is placed on QPSK modulation schemes only, the derivations provided in the following sections can be easily extended to a general M-ary phase-shift keying (PSK) case.

By confining our focus to the detection of the n^{th} QPSK payload symbol s_n, the problem can be formulated as (the same analysis is repeated for all QPSK payload symbols of interest):

$$\mathbf{y}_n = \mathbf{X}_n\mathbf{h}_n + \mathbf{e}_n, \tag{1}$$

where

$$\mathbf{y}_n = [y_1 \ldots y_{P+R-1}]^T \tag{2}$$

contains the $P+R-1$ synchronized measured data samples (i.e., y_1, the first element of $\mathbf{y}_n$, maps to s_nx_1, and so on). Further,

$$\mathbf{e}_n = [e_1 \ldots e_{P+R-1}]^T \tag{3}$$

represents additive noise (thermal or hardware related noise, interferences or jamming, as well as the overwhelming ambient sea noise). Each element of $\mathbf{e}_n$ is assumed to be a circularly symmetric independent and identically distributed (i.i.d.) complex-valued Gaussian random process with zero mean and variance σ^2, denoted as $\mathbf{e}_n \sim \mathcal{CN}(0, \sigma^2 \mathbf{I})$ (the practical validity of this assumption will be verified by analyzing experimental ambient noise, see Section IV B). The matrix $\mathbf{X}_n \in \mathcal{C}^{(P+R-1)\times R}$ in (1) contains multiple shifted replicas of the phase-modulated spreading waveforms, given by

$$\mathbf{X}_n = \begin{bmatrix} s_n x_1 & s_{n-1} x_P & \ldots & s_{n-1} x_{P-R+2} \\ \vdots & s_n x_1 & & s_{n-1} x_{P-R+3} \\ s_n x_P & \vdots & \ddots & \vdots \\ s_{n+1} x_1 & s_n x_P & & s_{n-1} x_P \\ \vdots & s_{n+1} x_1 & \ddots & s_n x_1 \\ s_{n+1} x_{R-2} & \vdots & \ddots & \vdots \\ s_{n+1} x_{R-1} & s_{n+1} x_{R-2} & & s_n x_P \end{bmatrix}, \qquad (4)$$

where s_{n-1} and s_{n+1} denote, respectively, the symbols transmitted before and after the one of current interest.

The problem is then to estimate the QPSK symbol s_n given the incoming measurement vector $\mathbf{y}_n$ and the known spreading waveform $\mathbf{x}$. As mentioned in the previous section, coherent RAKE reception is employed herein. We are particularly interested in designing a waveform $\mathbf{x}$ that not only facilitates the reception scheme considered, but also ensures LPI communications.

III. SPREADING WAVEFORM SYNTHESIS

In this section, we first explore the characteristics of common spreading waveforms that facilitate coherent RAKE reception. Specifically, we assess the impact of the correlation (the aperiodic auto-correlation) properties of the spreading waveform on the outputs of each RAKE finger. Then, we consider two viable state-of-the-art algorithms to generate the spreading waveform with the desirable characteristics.

The matrix $\mathbf{X}_n$ in (4) can be decomposed to isolate the contribution of s_n from its adjacent symbols s_{n-1} and s_{n+1}:

$$\mathbf{X}_n = s_n \mathbf{C} + s_{n-1} \mathbf{B} + s_{n+1} \mathbf{A}, \qquad (5)$$

where the dimensions of $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ conform with those of $\mathbf{X}_n$. The matrix $\mathbf{C}$ contains only the shifted replicas of $\mathbf{x}$ that are relevant to the symbol of current interest s_n:

$$\mathbf{C} = \begin{bmatrix} x_1 & & \mathbf{0} \\ \vdots & \ddots & \\ x_P & & x_1 \\ & \ddots & \vdots \\ \mathbf{0} & & x_P \end{bmatrix}. \qquad (6)$$

$\mathbf{B}$ and $\mathbf{A}$ are composed of the residual chips associated with s_{n-1} and s_{n+1}, respectively:

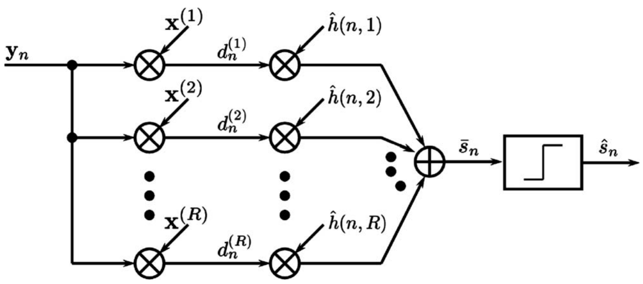


FIG. 1. Structure of a coherent RAKE detector.

$$\mathbf{B} = \begin{bmatrix} 0 & x_P & \ldots & x_{P-R+2} \\ 0 & 0 & & x_{P-R+3} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x_P \\ & & \mathbf{0} & \end{bmatrix}, \quad \mathbf{A} = \begin{bmatrix} & & \mathbf{0} & \\ x_1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ x_{R-2} & & 0 & 0 \\ x_{R-1} & \ldots & x_1 & 0 \end{bmatrix}. \qquad (7)$$

Note that $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are all independent of the symbol index n.

Figure 1 shows the structure of a conventional coherent RAKE detector. The received measurement vector $\mathbf{y}_n$ is first projected onto the vector $\mathbf{x}^{(r)} \in \mathcal{C}^{(P+R-1)\times 1}$, which is a shifted version of the spreading waveform $\mathbf{x}$ associated with the r^{th} channel tap (i.e., the tap represented by $h(n,r)$ over the n^{th} symbol period). The vector $\mathbf{x}^{(r)}$ is the r^{th} column of $\mathbf{C}$, given by

$$\mathbf{x}^{(r)} = \Big[\underbrace{0 \ \ldots \ 0}_{r-1} \quad x_1 \quad x_2 \quad \ldots \quad x_P \quad \underbrace{0 \ \ldots \ 0}_{R-r} \Big]^T, \qquad (8)$$

where $r = 1, \ldots, R$. The correlation function of the spreading waveform $\mathbf{x}$ is defined as

$$\tilde{r}_k = \sum_{n=k+1}^{P} x_n x_{n-k}^* = \tilde{r}_{-k}^*, \qquad k = 0, \ldots, P-1, \qquad (9)$$

where $\tilde{r}_0 = P$ due to the unimodular nature of $\{x_p\}_{p=1}^{P}$.

It can be easily verified that

$$\mathbf{x}^{(r)H}\mathbf{C} = \left[\tilde{r}_{r-1} \ \ \ldots \ \ \tilde{r}_1 \ \ \tilde{r}_0 \ \ \tilde{r}_1^* \ \ \ldots \ \ \tilde{r}_{R-r}^* \right], \qquad (10)$$

$$\mathbf{x}^{(r)H}\mathbf{B} = \Big[\underbrace{0 \ \ldots \ 0}_{r} \quad \tilde{r}_{P-1} \quad \ldots \quad \tilde{r}_{P-R+r} \Big], \qquad (11)$$

and

$$\mathbf{x}^{(r)H}\mathbf{A} = \Big[\tilde{r}_{P-r+1}^* \quad \ldots \quad \tilde{r}_{P-1}^* \quad \underbrace{0 \ \ldots \ 0}_{R-r+1} \Big]. \qquad (12)$$

Based on (1) and (10)–(12), the output of a RAKE finger $d_n^{(r)}$, i.e., the projection of $\mathbf{y}_n$ onto $\mathbf{x}^{(r)}$, follows:

$$\begin{aligned} d_n^{(r)} &= \mathbf{x}^{(r)H}\mathbf{y}_n = \mathbf{x}^{(r)H}(s_n\mathbf{C} + s_{n-1}\mathbf{B} + s_{n+1}\mathbf{A})\mathbf{h}_n + \mathbf{x}^{(r)H}\mathbf{e}_n \\ &= \sum_{q=1}^{r-1}[s_n\tilde{r}_{r-q} + s_{n+1}\tilde{r}^*_{P-r+q}]h(n,q) + \sum_{q=r+1}^{R}[s_n\tilde{r}^*_{q-r} \\ &\quad + s_{n-1}\tilde{r}_{P+r-q}]h(n,q) + s_n\tilde{r}_0 h(n,r) + e_n^{(r)}, \end{aligned} \tag{13}$$

where $r=1,2,\ldots,R$ and $e_n^{(r)}=\mathbf{x}^{(r)H}\mathbf{e}_n$ follows the distribution $\mathcal{CN}(0,\tilde{r}_0\sigma^2)$. We remark that the correlated vectors $\{\mathbf{x}^{(r)}\}$ will translate into correlated Gaussian noise $\{e_n^{(r)}\}$.

The projections $\{d_n^{(r)}\}_{r=1}^R$ over the n^{th} symbol period are then weighted by appropriate channel taps, and summed to form the symbol estimate $\bar{s}_n$ (see Fig. 1):

$$\bar{s}_n = \frac{\sum_{r=1}^{R} d_n^{(r)}\hat{h}^*(n,r)}{\tilde{r}_0\sum_{r=1}^{R}|\hat{h}(n,r)|^2} = \frac{\sum_{r=1}^{R} d_n^{(r)}\hat{h}^*(n,r)}{\tilde{r}_0\|\hat{\mathbf{h}}_n\|^2}. \tag{14}$$

In practice, the true channel taps $\{h(n,r)\}_{r=1}^R$ are generally not known to the receiver a priori. Therefore, they have to be replaced with their estimates $\{\hat{h}(n,r)\}_{r=1}^R$, as done in (14). The hard decision $\hat{s}_n$ is obtained by slicing $\bar{s}_n$, see Fig. 1.

For a general frequency-selective channel with $R>1$ ($R=1$ leads to a flat-fading channel), the correlation functions other than $\tilde{r}_0$ become relevant [see (13)]. Therefore, a spreading sequence with good correlation properties is preferable. In the absence of the a priori information regarding channel characteristics at the transmitter end. (Actually, we can feedback the channel information acquired by the receiver to the transmitter. However, such a feedback scheme complictes system design. Further, feedback is not suitable for the UWA environment since the time-varying nature of the UWA channel causes the newly acquired channel information outdated quickly). The ideal correlation function would be

$$\tilde{r}_k = 0 \quad \text{for} \quad k \in [1,R-1]\cup[P-R+1,P-1]. \tag{15}$$

We assume that $P>2R-2$. The correlation function $\{\tilde{r}_k\}$ over $k\in[R,P-R]$ has no impact on the RAKE performance.

The use of such an ideal spreading waveform leads to uncorrelated $\{e_n^{(r)}\}$ and simplifies (13) to

$$d_n^{(r)} = s_n\tilde{r}_0 h(n,r) + e_n^{(r)}, \quad r=1,\ldots,R. \tag{16}$$

By (16), an ideal spreading waveform effectively decomposes a R-tap frequency-selective channel into R parallel and independent flat-fading channels that do not interfere with each other. As a consequence, there is no interference across RAKE fingers and the symbol estimate is given by (assuming a perfect channel estimate, i.e., $\mathbf{h}_n=\hat{\mathbf{h}}_n$):

$$\bar{s}_n = s_n + \frac{\sum_{r=1}^{R} e_n^{(r)}h^*(n,r)}{\tilde{r}_0\|\mathbf{h}_n\|^2}. \tag{17}$$

Using the fact that $\tilde{r}_0=P$ and $|s_n|=1$, and denoting SNR $=\|\mathbf{h}_n\|^2/\sigma^2$ as the incoming chip SNR before RAKE processing (this notation will be used throughout the rest of the paper unless stated otherwise), SNR, as evidenced in (17), is increased by a factor of P at the output of a coherent RAKE. The chip length P, therefore, is also referred to as the processing gain in the DSSS literature.[14] Note that $\sum_{r=1}^{R} e_n^{(r)}h^*(n,r)\sim\mathcal{CN}(0,\tilde{r}_0\|\mathbf{h}_n\|^2\sigma^2)$. This condition is a direct consequence of uncorrelated $\{e_n^{(r)}\}$, which, as previously mentioned, is true when the spreading waveform satisfies (15).

By assuming that the spreading waveform satisfies (15), the bit error rate (BER) performance by employing the QPSK modulation scheme is given by[19]

$$P_{\text{BER}} = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{P\cdot\text{SNR}}{2}}\right), \tag{18}$$

where $\text{erfc}(\cdot)$ represents the complementary error function.

As previously mentioned, UWA environments, and especially the time-varying nature of underwater medium, constrain the feasible P value that can be used, as the block fading assumption can be easily violated when a long waveform is adopted.[6] For this reason, a spreading waveform with a relatively short chip length is more suitable for UWA environments.

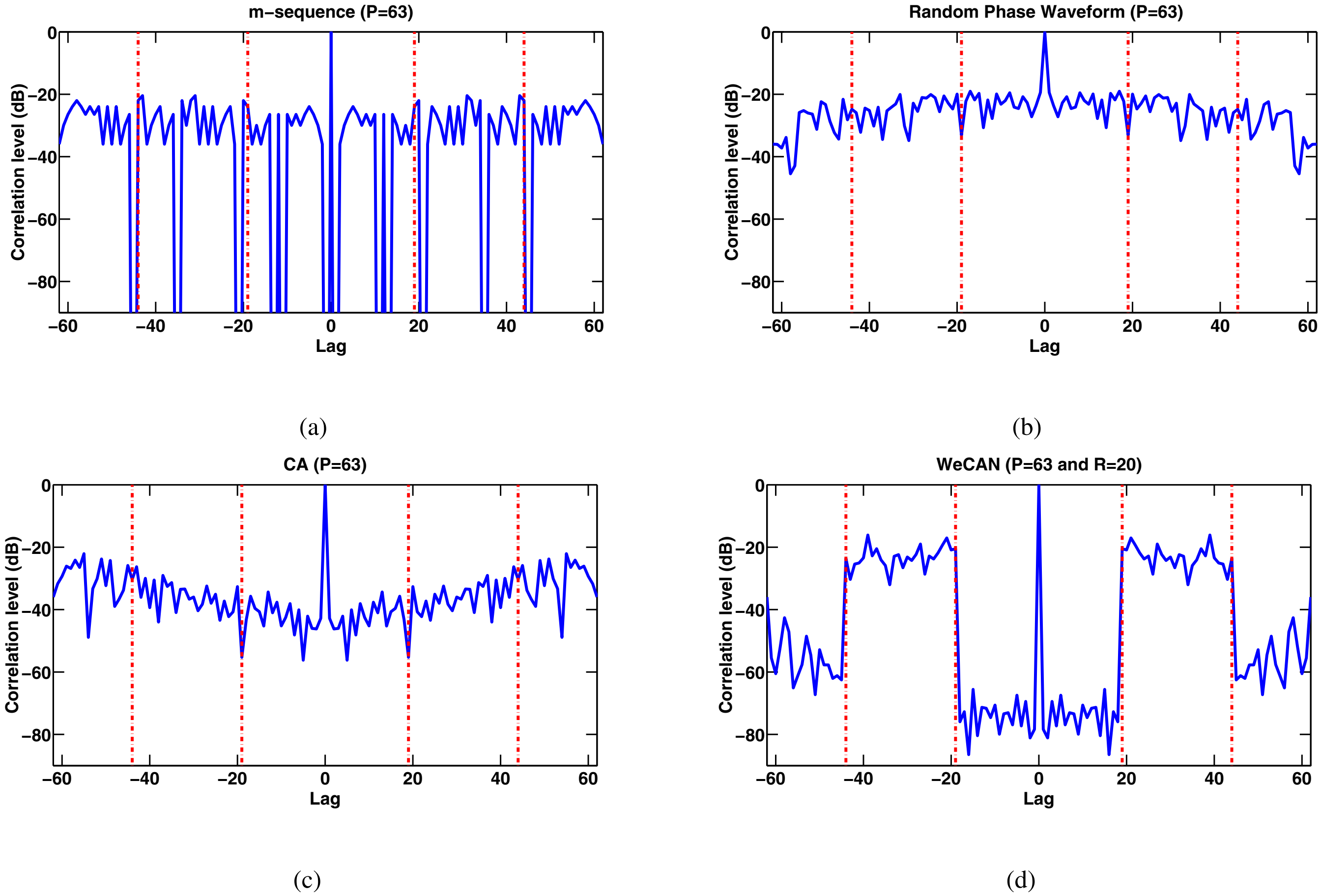
Two algorithms, referred to as WeCAN[17] and CA[18] are viable to approximately achieve the goal presented in (15). Both algorithms make use of a cyclic approach to efficiently minimize correlation-related criteria. Moreover, through different random phase initializations, different waveforms can be obtained.[17] As will be shown in the next section, flexible length and random phase values ensure LPI, and the optimized correlation properties facilitate the coherent RAKE reception in the sense of suppressing the inter- and intra-symbol interferences. Both features make these waveforms especially preferable for covert UWA applications.

Of the two algorithms considered, WeCAN aims to suppress the correlations over only the lag of interest (i.e., $k\in[1,R-1]\cup[P-R+1,P-1]$), and is used under the assumption that $P>2R-2$, see (15). This implicitly requires a priori information on the channel tap number R. For practical UWA communications, either R is not available prior to the experiment or the relationship $P>2R-2$ does not hold (but we still assume $P>R$), which would be the case when a short spreading waveform is used in a severe time-dispersive channel. Thus, we instead aim to suppress the correlation levels over the *entire* time lag (i.e., $[1,P-1]$), in lieu of the union of two separate intervals as in (15). For this purpose, the CA algorithm can be applied.

Finally, we remark that a faster alternative to CA, namely CA new (CAN), has been presented by Stoica *et al.*[17] CAN is based on fast Fourier transform (FFT) operations, making it more computationally efficient than CA. We focus on CA in this paper since only CA spreading waveforms were employed in SPACE'08. Otherwise, CAN would be preferable.

IV. NUMERICAL AND EXPERIMENTAL RESULTS

In this section, we first compare the detection performance of different types of spreading waveforms in terms of



(a)

(b)

(c)

(d)

FIG. 2. (Color online) Correlation levels of the spreading waveforms with $P=63$. The vertical dash-dot lines indicate the lag intervals $[-62,-44]\cup[-19,-1]\cup[1,19]\cup[44,62]$, over which we want to suppress the correlation levels. (a) m-sequence. (b) Random phase waveform. (c) CA waveform. (d) WeCAN waveform. Note that the random phase waveform in (b) is used to initialize the CA and WeCAN algorithms to yield the waveforms in (c) and (d), respectively.

BER using simulated data. Then, the LPI and LPD properties are evaluated based on the SPACE'08 in-water experimentation data.

A. BER performance of simulated data

We will, in this example, compare the BER performance when different spreading waveforms are employed. Among the four different waveforms considered in this section, the chip length P for WeCAN, CA and random phase waveforms can be arbitrarily chosen. However, we choose $P=63$ to meet the length constraint imposed by the m-sequence. The correlation levels of the four waveforms are plotted in Fig. 2, where the correlation level is defined as

$$\text{correlation level} = 20\log_{10}\frac{|\tilde{r}_p|}{P}\text{dB}, \quad p=0,1,\ldots,P-1, \tag{19}$$

and $\tilde{r}_p$ has been given in (9). Note that the CA and WeCAN waveforms in Figs. 2(c) and 2(d), respectively, are generated using the random phase waveform in Fig. 2(b) to initialize the algorithms. By considering the simulated time-invariant frequency-selective channel shown in Fig. 3 with $R=20$ resolved taps, we are particularly interested in suppressing the correlation levels over the lags $[-62,-44]\cup[-19,-1]\cup[1,19]\cup[44,62]$ (indicated with the vertical dash-dot lines in Fig. 2). Overall, the WeCAN waveform gives the lowest correlation levels over the lag ranges of interest, while the random phase waveform exhibits the highest.

Next, we proceed with the evaluation of the BER performance. The selected information sequence consists of 1000 QPSK payload symbols and each symbol is spread by a common spreading waveform. The transmitted signal propagates through the frequency-selective channel shown in Fig. 3, followed by the coherent RAKE receiver outlined in Fig. 1. The incoming measurements are constructed according to (1). 50 different random phase waveforms are used in this

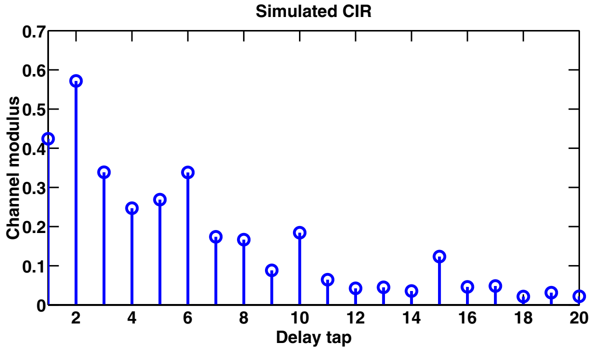


FIG. 3. (Color online) The modulus of the simulated CIR where $R=20$ channel taps are considered.

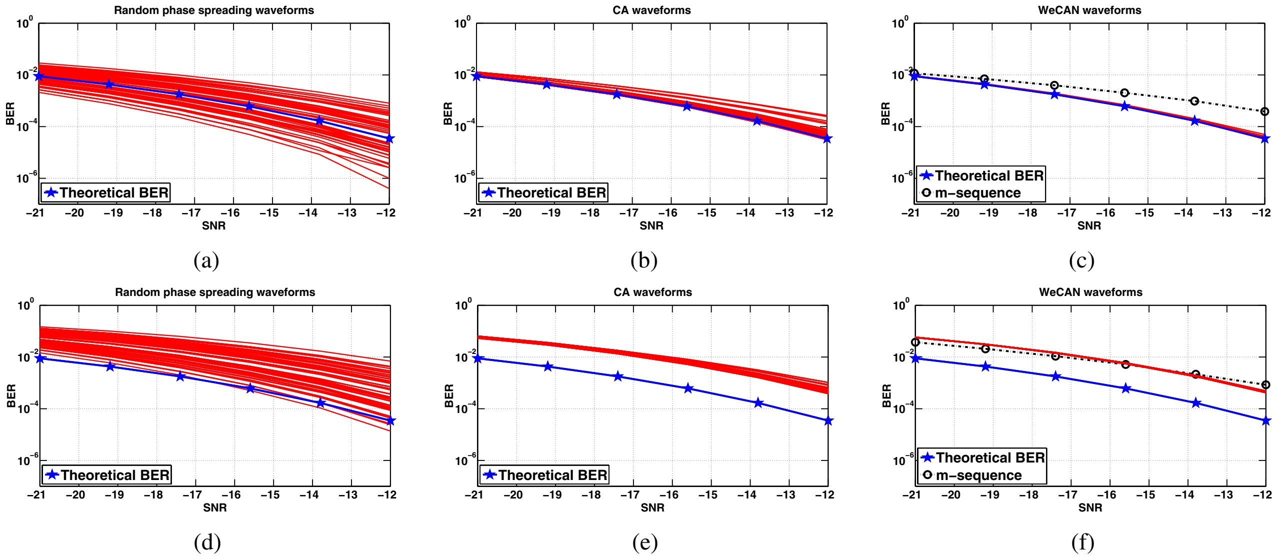


FIG. 4. (Color online) The 50 empirical BER curves of different types of spreading waveforms with $P=63$, along with the theoretical BER values. Each point is averaged over 5000 Monte-Carlo runs. [(a)–(c)] The receiver has perfect channel characteristics as prior knowledge. [(d)–(f)] The receiver estimates the CIR using 5 QPSK pilot symbols. [(a) and (d)] Random phase waveforms. [(b) and (e)] CA waveforms. [(c) and (f)] WeCAN waveforms and m-sequence. Note that the 50 CA and 50 WeCAN waveforms considered are generated by using the 50 random phase waveforms in (a) to initialize the algorithms.

example and they are obtained as follows. We first generate 1000 independent random phase waveforms, calculate the peak sidelobe level (PSL) of each waveform and then keep the waveforms corresponding to the 50 lowest PSL values among the 1000 candidates. [The lowest PSL of the 1000 candidates is −19.02 dB, which is shown in Fig. 2(b).] These 50 selected random phase waveforms are used to initialize the CA and WeCAN algorithms to synthesize 50 CA waveforms and 50 WeCAN waveforms.

We first assume that the receiver has perfect channel characteristics as prior knowledge. The resulting empirical BER curves for the different types of waveforms are shown superimposed in Figs. 4(a)–4(c), along with the theoretical BER given by (18). Each point here is averaged over 5 K Monte-Carlo trials. The information sequence and the noise pattern vary independently for each trial. From Fig. 4(a), the theoretical BER curve can be reasonably regarded as an average detection performance of the 50 selected random phase waveforms. The random phase waveform, however, exhibits significant variations in BER performance. For example, at SNR=−12 dB, the span of the 50 empirical BER values exceeds 3 orders of magnitude. The performance variations of the 50 related CA waveforms, on the other hand, are considerably reduced [see Fig. 4(b)] owing to the suppressed correlation levels. The rather low correlation levels at the lags of interest of the WeCAN waveforms translate into the remarkable similarity between the theoretical BER curve and the empirical values, see Fig. 4(c). The BER curve derived by adopting the m-sequence in Fig. 2(a) is also plotted in Fig. 4(c). By comparing Fig. 2 and Figs. 4(a)–4(c), we note that the conformity to the theoretical values, to some extent, reflects the goodness of the correlation levels.

Next, we proceed to assess the detection performance when the receiver does not possess perfect channel information and has to estimate it in the training-directed mode. To this end, 5 QPSK pilot symbols are added before the 1000 QPSK payload symbols and these 5 pilot symbols (or 500 chips after spreading) are used to conduct the training-directed channel estimate. The channel estimation algorithm is implemented by sparse learning via iterative minimization (SLIM).[20] For a simulated time-invariant channel, the initial CIR estimate is then treated as constant when detecting the payload symbols. By performing RAKE detection using the estimated CIR, the resulting empirical BER performance is shown in Figs. 4(d)–4(f) for the different waveforms, along with the theoretical BER obtained with perfect spreading waveform and perfect CIR information. Each point is averaged over 5 K Monte-Carlo trials, and the information sequence (including the 5 QPSK pilot symbols) and the noise vary independently for one trial to another. By comparing Figs. 4(a)–4(f), one observes that the presence of the CIR estimate error shifts the empirical BER curves upward by approximately one order of magnitude. For a time-invariant channel, the gap between the theoretical and empirical BER curves for CA and WeCAN waveforms would diminish had more pilot symbols been used to conduct training-directed channel estimation.

Although random phase spreading waveforms help ensure LPI communications, their large variations in detection performance make them rather unappealing for covert communications [since it is hard to predict the resulting performance of a specific realization of a random phase waveform, as evidenced in Figs. 4(a) and 4(d)]. On the other hand, the optimized correlation levels possessed by WeCAN and CA waveforms lead to very consistent performance [in particular, when the receiver has perfect CIR information, one would expect reasonable agreement between the empirical and theoretical BER values, as shown in Figs. 4(b) and 4(c)], making them preferable over their random phase counterpart.

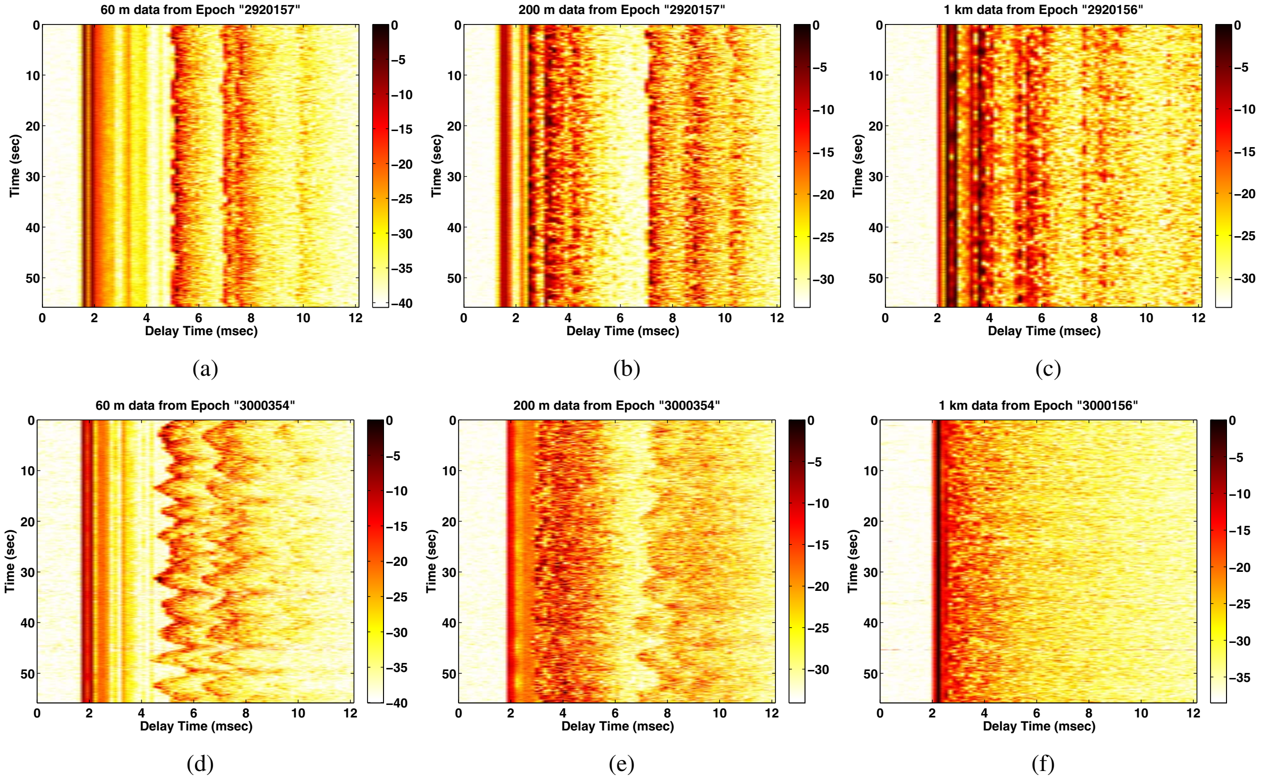


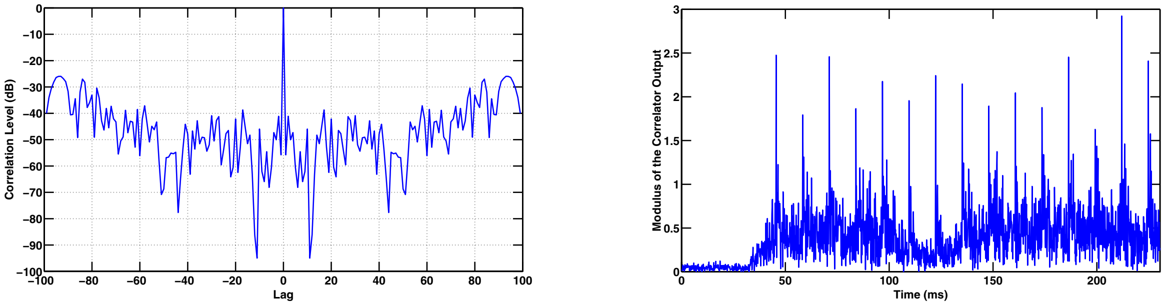
FIG. 5. (Color online) Normalized CIR evolution over approximately a 1 min period. The modulus of the channel tap is shown in dB. CIR is estimated using m-sequences. The CIR taps have been manually shifted so that the principal arrival occurs at about 2 ms. [(a) and (d)] Benign and severe channel conditions at 60 m. [(b) and (e)] Benign and severe channel conditions at 200 m. [(c) and (f)] Benign and severe channel conditions at 1 km. [(a)–(c)] Measurements recorded on Julian date 292. [(d)–(f)] Measurements recorded on Julian date 300.

B. SPACE'08 in-water experimentation results

(1) The experiment: The SPACE'08 in-water experiment was conducted by WHOI at the Air-Sea Interaction Tower, 2 miles south to the coast of Martha's Vineyard, MA, at a water depth of 15 m. The system was equipped with 4 transmit transducers. The primary transducer was located approximately 4 m above the ocean floor using a stationary tripod. Below the primary transducer, a source array consisting of 3 transducers was deployed vertically with a spacing of 0.5 m between the elements. The top element of the source array was 3 m above the ocean floor. The carrier frequency and bandwidth used in the experiments were 13 KHz and 10 KHz, respectively.

We consider three separate receiver configurations deployed respectively at a horizontal distance of 60 m, 200 m and 1 km. The experimental measurements analyzed in this section were recorded on Julian dates 292 (October 18, 2008) and 300 (October 26, 2008) sampled at one sample per symbol. SPACE'08 meteorological data indicates that the average wave height were approximately 0.4 m and 2.75 m on Julian dates 292 and 300, respectively,[20] and these two dates are purposely selected to assess the impact of different channel conditions (i.e., benign channel conditions on Julian date 292 and severe conditions on 300) on the performance of covert UWA communications. In this way, we are interested in 6 different scenarios as there are 3 receiver configurations and 2 channel conditions. Fig. 5 shows the evolution of the normalized CIR between the primary transducer and the receiving hydrophone pair over time for these 6 scenarios. In these plots, a single transducer continually transmitted an m-sequence, while the other transducers were inactive. One observes that the channel taps experience significant variations over time as the wave height increases.

For covert UWA communications, the covert signal was sent by the primary transducer only. To form a strong noise background, the other 3 transducers simultaneously transmitted independent constant modulus co-channel interferences. These co-channel interferences, collectively with the ambient sea noise, formed the strong noise $\mathbf{e}_n$ in (1) (henceforth, we do not distinguish the co-channel interferences from the sea noise, and therefore we only consider SNR instead of the signal-to-interference-plus-noise ratio). The transmitted covert signal consisted of 2 K QPSK payload symbols $\{s_n\}_{n=1}^{2000}$. The common spreading waveform used in the experiments was synthesized by the CA algorithm with $P=100$ chips. The correlation levels of the waveform versus lag are shown in Fig. 6(a). A transmit bandwidth of 7.8125 K chips per second leads to a payload data rate of 156.25 bps and a symbol duration of 12.8 ms. When a single receiving hydrophone is used to detect the transmitted symbols, Table I lists the estimated received SNR. To obtain these SNR values, the entire 2000 payload symbols $\{s_n\}_{n=1}^{2000}$ are divided into 400 groups, each containing 5 symbols, and these 2000 payload symbols are assumed to be perfectly known at the receiver side as if in the training-directed mode. For each group the SLIM algorithm is employed to estimate the CIR between the primary transducer (which transmitted the covert signal) and the receiving hydrophone. Once the CIR estimate is avail-



(a) (b)

FIG. 6. (Color online) (a) The correlation levels of the CA spreading waveform employed in SPACE'08 in-water experiment. (b) The modulus of the correlation output over the first 230 ms.

able, the received covert signal is re-constructed by performing convolution of the CIR estimate and the transmitted waveform chips. After subtracting out the so-obtained covert signal from the received measurements, the noise power is estimated as the variance of the residual measurements with the contribution from the covert signal removed. Repeating the above procedure for each group gives 400 CIR estimates and 400 noise power estimates, and the signal power and noise power listed in Table I are determined respectively as the average channel power and the average noise power over the 400 groups. The ratio of the signal power to the noise power gives the SNR value in Table I. One observes from Table I that as the channel conditions become worse, the SNR value decreases at 60 m and 200 m range, while it increases in the 1 km case (probably due to the fact that the hydrophones at 1 km range were deployed beneath the thermocline). Without artificially injecting more ambient noise into the measured data, these SNR values only allow for an investigation of the LPI properties.[6]

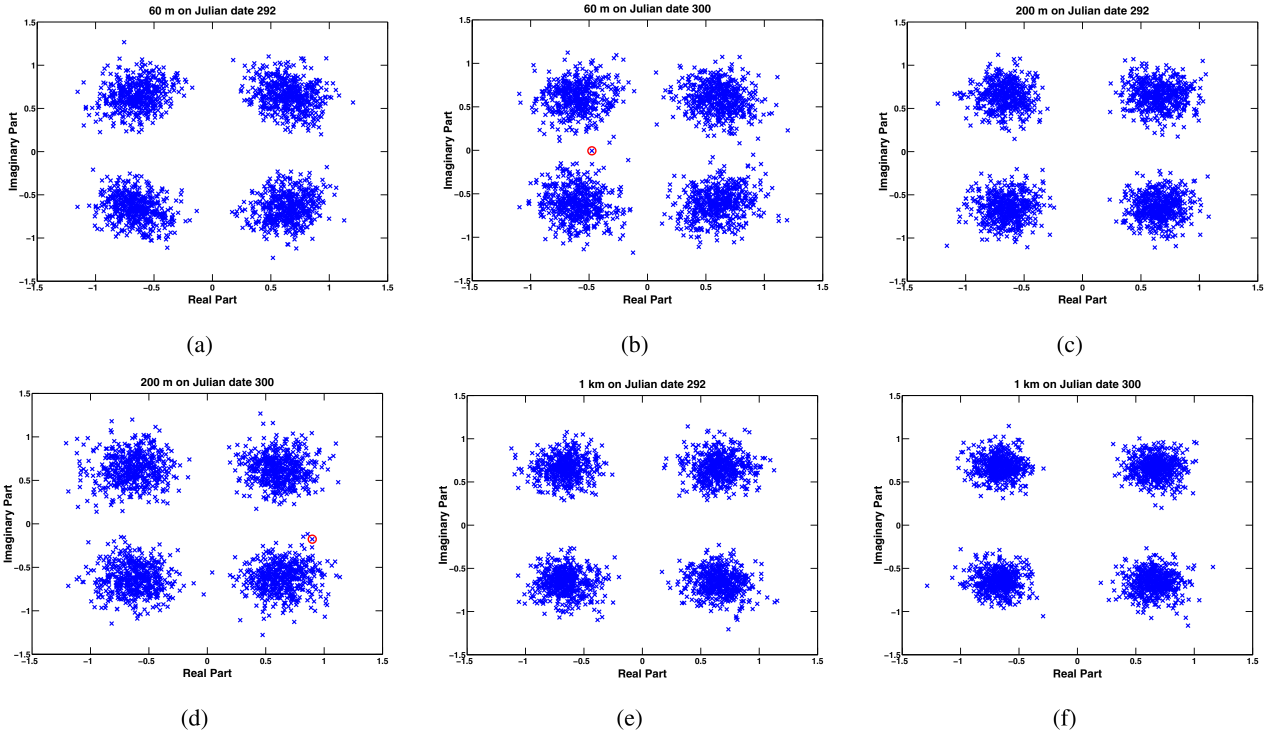
(2) LPI Properties: As mentioned, the LPI properties of a spreading waveform are important for scenarios that lack a sufficiently low SNR. We will now investigate the BER performance of the intended receiver for the 6 scenarios considered, followed by a discussion of the LPI properties of the CA spreading waveforms.

Intended receivers are identified as those having perfect knowledge on the modulation scheme (see the elaboration in Section II) and the spreading waveform $\mathbf{x}$. Before discussing detection performance, we analyze the 1 km measurements acquired on Julian date 300 to show how synchronization is achieved (synchronization procedure for other scenarios, for both LPI and LPD, is performed in a similar manner). By correlating (or matched filtering) the received measurements with the common CA spreading waveform $\mathbf{x}$, the modulus of the correlator output over the first 230 ms is shown in Fig. 6(b). One observes that although the covert signal is contaminated by strong co-channel interferences, the correlator output exhibits a series of conspicuous peaks every 12.8 ms (i.e., every symbol period). Synchronization is achieved by mapping the first element of $\mathbf{y}_1$ [see (2)] to the location of the initial peak.

Although multiple receiving hydrophones were deployed for all the three receiver configurations, for the time being, we only focus on one single hydrophone to make the symbol detection problem more difficult. The number of the channel taps is fixed at $R=80$ for all the 6 scenarios considered. At the channel estimation stage, it is obviously beneficial to increase the training length for estimating the channel more accurately. However, the training length cannot be too long; otherwise the stationarity assumption of the UWA channel will be easily violated. As a tradeoff, we use the leading 5 QPSK symbols $\{s_n\}_{n=1}^{5}$ as pilots to obtain the training-directed channel estimate. The so-obtained initial channel estimate is used to detect s_6 as in (14). When $\hat{s}_6$ is available, the channel is tracked in decision-directed mode using 5 symbols (containing the most recently detected symbol, and a portion of the training symbols as well), namely $\{s_n\}_{n=2}^{5}$ and $\hat{s}_6$. The updated channel estimate is then used to detect s_7, and so on. The channel estimation algorithm, in both training- and decision-directed modes, is implemented by SLIM.[20] Note that this detection scheme implicitly assumes that the channel remains stationary over at least 6 symbol periods. Using the measurements from one single receiving hydrophone, Fig. 7 shows the constellation plot of $\{\bar{s}_n\}_{n=6}^{2000}$ (the quantities before slicing) for all the 6 scenario considered. By comparing the SNR values listed in Table I and the constellation plots shown in Fig. 7, one observes that a larger (smaller) SNR value in general translates into more concentrated (smeared) constellation clusters. In particular, the low SNR values at 60 m and 200 m distance on Julian date 300 lead to one wrongly estimated payload symbol, which is marked by a circle in Figs. 7(b) and 7(d). To en-

TABLE I. Estimated SNR for the 6 scenarios considered.

	60 m		200 m		1000 m	
	Julian date 292	Julian date 300	Julian date 292	Julian date 300	Julian date 292	Julian date 300
Signal power, noise power	0.3124, 0.9213	0.7909, 2.5607	0.0860, 0.2800	0.2600, 0.9301	0.0021, 0.0054	0.0010, 0.0023
SNR (dB)	−4.6968	−5.1023	−5.1254	−5.5353	−4.0797	−3.6097

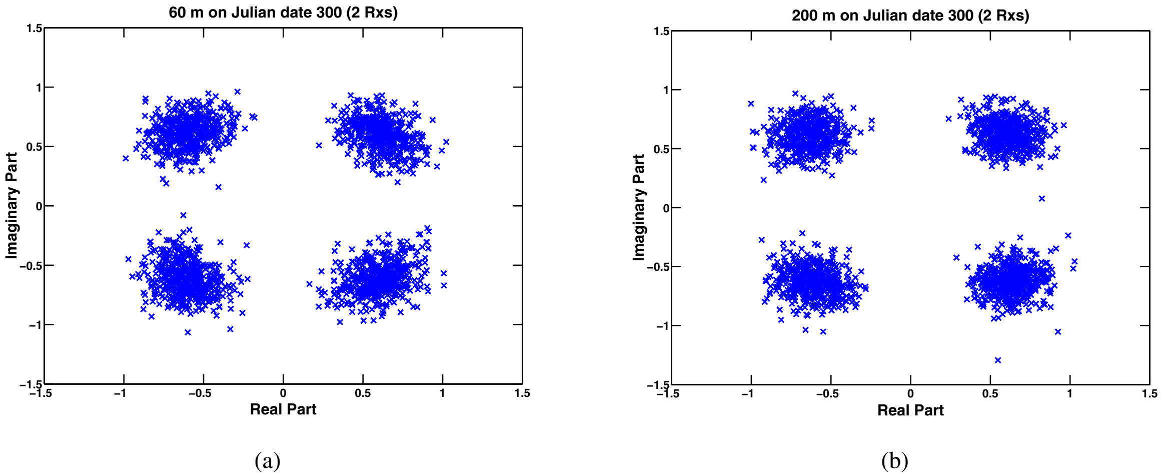


(a) (b) (c) (d) (e) (f)

FIG. 7. (Color online) Constellation plot of $\{\bar{s}_n\}_{n=6}^{2000}$. [(a) and (b)] Benign and severe channel conditions at 60 m. [(c) and (d)] Benign and severe channel conditions at 200 m. [(e) and (f)] Benign and severe channel conditions at 1 km. [(a), (c), and (e)] Under benign channel conditions. [(b), (d), and (f)] Under severe channel conditions.

hance the detection performance in these two challenging scenarios, we now use two receiving hydrophones by exploiting the receive diversity and the resulting constellations are shown in Fig. 8. By comparing Fig. 8 and Figs. 7(b)7(d), one observes that using two hydrophones effectively concentrates the constellation clusters by boosting the received SNR value, which leads to error-free detection performance for both cases.

The detection scheme developed previously is based on a frequency-selective channel assumption (recall that $R = 80$). Noting that the channel at 1 km under severe channel conditions shown in Fig. 5(f) can be reasonably modeled as a flat-fading channel with one single dominant channel tap representing the principal arrival (direct path), we proceed to assess the detection performance with a flat-fading channel model by analyzing the 1 km measurements. Since the periodic correlation peaks in Fig. 6(b), per the discussions in Section II, are nothing but the RAKE finger outputs $\{d_n^{(1)}\}_{n=1}^{2000}$. For notational simplicity, when analyzing 1 km data under a flat-fading channel assumption, finger output $d_n^{(1)}$ and the channel tap $h(n,1)$ are replaced, respectively, with d_n and h_n for $n = 1, \ldots, 2000$ without causing any confusion. By applying PSK modulation and assuming a flat-fading channel model, only the phase of the single tap, denoted as $\angle h_n$, is of interest. The modulus $|h_n|$ does not affect



(a) (b)

FIG. 8. (Color online) Constellation plot of $\{\bar{s}_n\}_{n=6}^{2000}$ by incorporating two receiving hydrophones. (a) Severe channel conditions at 60 m. (b) Severe channel conditions at 200 m.

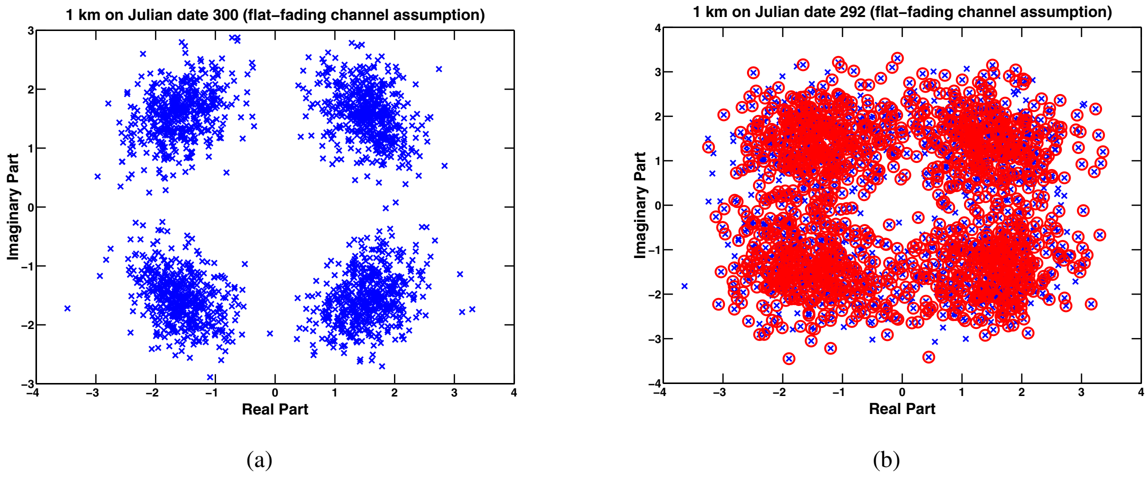


FIG. 9. (Color online) (a) Constellation plot of $\{\bar{s}_n\}_{n=2}^{2000}$ for 1 km measurements using flat-fading channel model. (a) On Julian date 300. (b) On Julian date 292.

the hard decision on s_n. Based on this observation and by addressing the time-varying nature of the UWA medium, $\angle h_1$ is first estimated in the training-directed mode as the difference in phase between the finger output d_1 and the symbol truth s_1 (i.e., $\angle\hat{h}_1 = \angle d_1 - \angle s_1$). This operation is performed by assuming that s_1 has been known to the receiver a priori for training purposes. The so-obtained channel phase $\angle\hat{h}_1$ is used to compensate for the phase of d_2 when detecting s_2 (i.e., $\hat{s}_2$ is determined by slicing $\bar{s}_2 = d_2 e^{-j\angle\hat{h}_1}$). Then $\angle\hat{h}_2$ can be calculated as $\angle\hat{h}_2 = \angle d_2 - \angle\hat{s}_2$ in the decision-directed mode, and $\angle\hat{h}_2$ will be used to compensate for the phase of d_3. This procedure is repeated until all the payload symbols have been detected. Note that this detection scheme implicitly assumes that the channel is stationary over two successive symbol periods, which allows for treating $\angle\hat{h}_{n-1}$ as constant when detecting s_n. Fig. 9(a) shows the constellation plot of $\bar{s}_n = d_n e^{-j\angle\hat{h}_{n-1}}$ following this detection scheme, where four clustered groups can be observed. Although this detection scheme leads to an error-free BER result, the corresponding constellation plot, by comparing Fig. 9(a) with Fig. 7(f), is more smeared than that obtained with a frequency-selective model. This is expected since under the flat-fading channel assumption, the taps other than the dominant tap in Fig. 5(f) contribute to additional noise, and the true SNR is actually lower than −3.61 dB as listed in Table I. The same detection procedure is repeated for 1 km measurements acquired on Julian date 292, and the resulting empirical constellation plot is shown in Fig. 9(b). More detection errors occur in this example (final BER is 0.4717) due to the modeling error: it is obviously wrong to treat a 1 km benign channel [see Fig. 5(c)] as a flat-fading one.

Finally, the LPI properties of the CA spreading waveform are investigated under a relaxed assumption. We consider the measurements at 1 km range recorded on Julian date 300 with flat-fading channel model (the analysis of other data sets, whether the channel is assumed to be flat-fading or frequency-selective, leads to similar observations) and assume that except for the random sequence used to initialize the CA algorithm, an eavesdropper has the same information about the communication details as an intended receiver, such as the value of $P=100$, the index mapping for synchronization, the package structure and modulation scheme, etc. (Actually, the above assumption is idealistic since, in the absence of the knowledge on the actual spreading waveform, even the synchronization would be very hard to achieve.) We generate 500 independent initial random phase sequences, and perform the detection by using the resulting 500 CA waveforms as the assumed spreading waveforms (the actual spreading waveform was fixed and different from the 500 assumed ones). The so-obtained BER results are shown in Fig. 10. Since different CA waveforms obtained from different initial random sequences are almost uncorrelated to one another,[21] the detection performance by generating spreading waveforms in a random manner is, on average, the same as that of an uninformed guess. This is evidenced by an average BER of 0.5, see Fig. 10. Consequently, the CA waveform possesses desirable LPI properties. For m-sequences with length P, on the other hand, the eavesdropper can easily exhaustively attempt all waveforms.

(3) LPD Properties: In practice, LPD UWA communications are generally referred to as those with SNR$<$ −8 dB.[6] The LPD properties, discussed below, are evaluated using synthetic data by adding simulated noise to the in-water experimental measurements. We model the sea ambient noise as a circularly symmetric complex-valued zero-

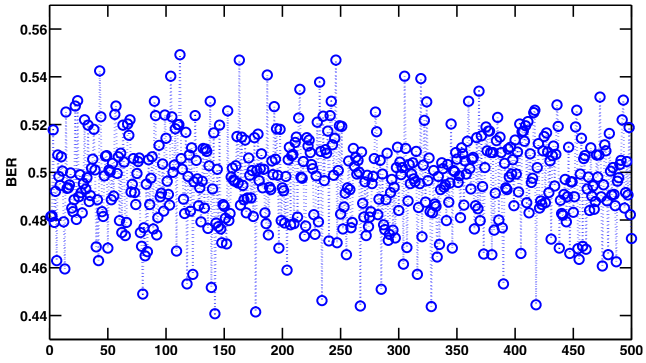
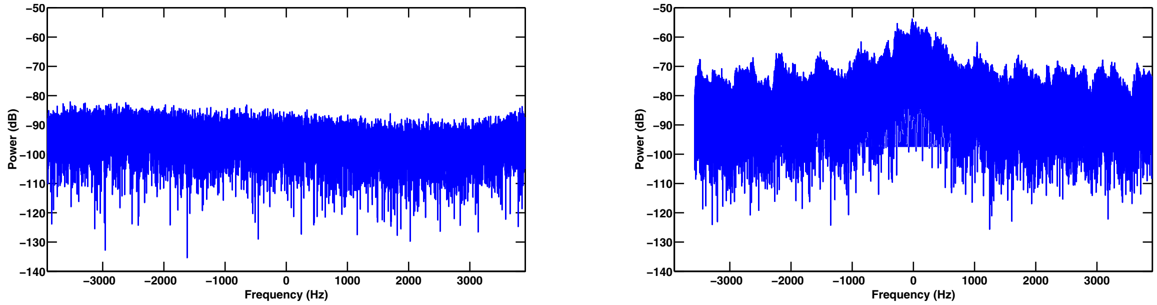


FIG. 10. (Color online) BER performance achieved by generating 500 CA waveforms in a random manner. The BER is 0.5 on average, implying the desired LPI features offered by the CA spreading waveforms.



(a)

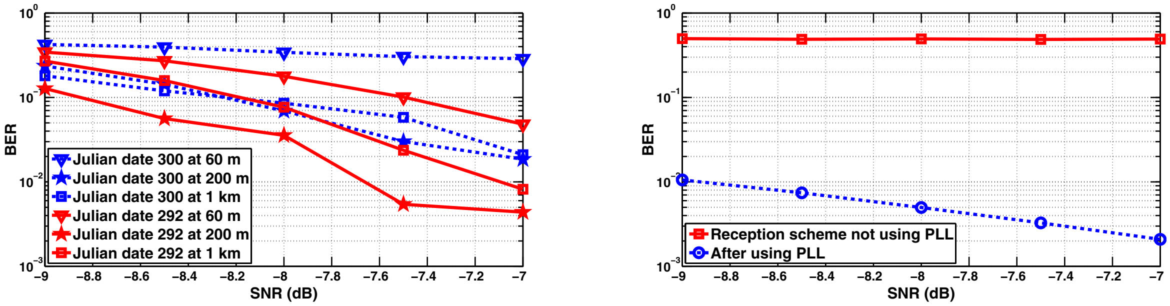
(b)

FIG. 11. (Color online) Spectral estimation of the received measurement at 1 km distance on Julian date 300. (a) The ambient sea noise. (b) The covert signal in conjunction with the co-channel interferences and sea noise.

mean white Gaussian random process. To verify the practical validity of this assumption, Fig. 11 shows the spectral estimate of 1 km measurements acquired on Julian date 300. Fig. 11(a) is obtained from 10 K complex-valued samples of in-water ambient noise, while Fig. 11(b) is during the covert transmission in the presence of strong co-channel interferences. Recalling that the data rate employed in SPACE'08 in-water experiment was 7.8125 K chips per second, the frequency range shown in Fig. 11 is confined to $[-3900\ 3900]$ Hz due to Nyquist sampling theory. The flat power spectrum shown in Fig. 11(a) indicates that it is reasonable to approximate the ocean noise as a white Gaussian process and further verifies that the simulation provided herein resembles the in-water environments. Analogous to the methodologies developed in the previous section, the LPD performance under both frequency-selective and flat-fading channel assumptions are discussed next.

To effectively reduce the SNR, computer-generated complex-valued white Gaussian noise is injected into the in-water received measurements. Based on the estimated SNR listed in Table I, the power of the synthetic Gaussian noise is adjusted so that the resulting SNR lies between -9 and -7 dB. We start with a frequency-selective channel assumption and the detection scheme discussed in the previous section that leads to Fig. 7 is still used here. The channel tap number is fixed at $R=80$ for all the 6 scenarios considered and the SLIM algorithm is used for both training- and decision-directed channel estimation. By analyzing the measurements from one single receiving hydrophone, the empirical BER curves for the 6 scenarios are shown in Fig. 12(a). Each point here is averaged over 500 Monte-Carlo trials, and the injected noise varies independently for one trial to another. One observes that for a fixed transmission distance, the LPD performance degrades as the channel conditions become worse, while for fixed channel conditions, 200 m data yields the best LPD performance in general.

Next, we proceed with the investigation of the LPD with flat-fading channel assumption and focus on the 1 km data on Julian date 300 only. Empirical experience dictates that the reception scheme used in the previous section that leads to Fig. 9(a) fails in this SNR range due to severe error propagation, as shown in Fig. 12(b). To alleviate the problem, we consider a second-order phase lock loop (PLL).[2] The pseudo code of the PLL-based reception scheme is listed in Table II. One observes that the algorithm involves two layers of phase compensation. The first layer serves to compensate all the 2 K RAKE finger outputs $\{d_n\}$ in phase by the training-directed phase estimate $\angle \hat{h}_1$ (recall that s_1 is a pilot symbol), and the second layer is implemented by a second-order PLL module conducted on a group basis (with each group consisting of 10 symbols). The quantities K_1 and K_2, which represent the proportional and integral tracking constants, are determined following the guideline provided by Stojanovic *et al.*[2] By assuming that perfect synchronization has been achieved, the BER results after incorporating the PLL module are shown in Fig. 12(b). Each point here is obtained by averaging over 500 Monte-Carlo trials. The injected noise varies indepen-



(a)

(b)

FIG. 12. (Color online) (a) The comparison of the detection scheme for the 6 scenarios considered under the frequency-selective channel assumption. (b) The comparison of the detection scheme presented in the previous section and the second-order PLL in term of BER. The BER curves are obtained by analyzing the measurements at 1 km on Julian date 300 (with injected noise) under the flat-fading channel assumption.

TABLE II. The reception scheme based on the second-order PLL.

```
Initialize
$\Phi_1=0$, $i=1$, $\angle\hat{h}_1=\angle d_1-\angle s_1$, $K_1=0.1$, $K_2=0.1$ and
denote $\tilde{d}_n=e^{-j\angle\hat{h}_1}d_n$ for $n=1,\ldots,2000$
Repeat
    Let $\bar{s}_n=e^{-j\Phi_i}\tilde{d}_n$ for $n=10i-9,\ldots,10i$, and slice $\{\bar{s}_n\}_{10i-9}^{10i}$
    to obtain $\{\hat{s}_n\}_{10i-9}^{10i}$
    $\phi_i=\frac{1}{10}\Sigma_{n=10i-9}^{10i}(\angle\bar{s}_n-\angle\hat{s}_n)$
    $\Phi_{i+1}=K_1\phi_i+K_2\Sigma_{j=1}^{i}\phi_j$
    $i=i+1$
Until $(i=201)$
```

dently from one trial to another. We observe that the PLL module effectively suppresses the BER to 5×10^{-3} at SNR $=-8$ dB, as compared to 8.56×10^{-2} with a frequency-selective channel model as shown in Fig. 12(a).

V. CONCLUSIONS

We have considered covert UWA communication schemes that adopt a DSSS-based modulation technique and a coherent RAKE reception. The covertness is evaluated in terms of the LPD and LPI properties. We have shown that WeCAN and CA are two viable algorithms to synthesize spreading waveforms. The so-obtained waveforms not only possess good correlation levels that account for the RAKE structure and frequency-selective nature of the UWA channel, but also show remarkable covert properties that serve to protect the privacy of the transmitted information. We have demonstrated the effectiveness of so-synthesized spreading waveforms in UWA covert communications using both simulated and the SPACE'08 in-water experimentation data.

ACKNOWLEDGMENTS

This work was supported in part by the SMART Fellowship Program, the Office of Naval Research (ONR) under Grant No. N00014-10-1-0054 and N00014-09-1-0211, the National Science Foundation (NSF) under Grant No. ECS-0621879, the U.S. Army Research Laboratory and the U.S. Army Research Office under contract/grant No. W911NF-07-1-0450, the Swedish Research Council (VR), and the European Research Council (ERC).

[1] D. Kilfoyle and A. Baggeroer, "The state of the art in underwater acoustic telemetry," IEEE J. Ocean. Eng. **25**, 4–27 (2000).

[2] M. Stojanovic, J. Catipovic, and J. Proakis, "Phase-coherent digital communications for underwater acoustic channels," IEEE J. Ocean. Eng. **19**, 100–111 (1994).

[3] M. Palmese, G. Bertolotto, A. Pescetto, and A. Trucco, "Spread spectrum modulation for acoustic communication in shallow water channel," in Proceedings of MTS/IEEE OCEANS (2007), pp. 1–4.

[4] M. Stojanovic, J. G. Proakis, J. A. Rice, and M. D. Green, "Spread spectrum underwater acoustic telemetry," Proceedings of MTS/IEEE OCEANS (1998), pp. 650–654.

[5] P. Hursky, M. B. Porter, and M. Siderius, "Point-to-point underwater acoustic communications using spread-spectrum passive phase conjugation," J. Acoust. Soc. Am. **120**, 247–257 (2006).

[6] T. C. Yang and W.-B. Yang, "Performance analysis of direct-sequence spread-spectrum underwater acoustic communications with low signal-to-noise-ratio input signals," J. Acoust. Soc. Am. **123**, 842–855 (2008).

[7] M. Stojanovic and L. Freitag, "Hypothesis-feedback equalization for direct-sequence spread-spectrum underwater communications," in Proceedings of MTS/IEEE OCEANS (2000), pp. 123–128.

[8] F. Blackmon, E. Sozer, M. Stojanovic, and J. Proakis, "Performance comparison of RAKE and hypothesis feedback direct sequence spread spectrum techniques for underwater communication applications," in Proceedings of MTS/IEEE OCEANS (2002), pp. 594–603.

[9] J. A. Ritcey and K. R. Griep, "Code shift keyed spread spectrum for ocean acoustic telemetry," in Proceedings of MTS/IEEE OCEANS (1995), pp. 1386–1391.

[10] M. Stojanovic and L. Freitag, "MMSE acquisition of DSSS acoustic communications signals," in Proceedings of MTS/IEEE OCEANS (2004), pp. 14–19.

[11] E. M. Sozer, J. G. Proakis, M. Stojanovic, J. A. Rice, A. Benson, and M. Hatch, "Direct sequence spread spectrum based modem for under water acoustic communication and channel measurements," in Proceedings of MTS/IEEE OCEANS (1999), pp. 228–233.

[12] C. C. Tsimenidis, O. R. Hinton, A. E. Adams, and B. S. Sharif, "Underwater acoustic receiver employing direct-sequence spread spectrum and spatial diversity combining for shallow-water multiaccess networking," IEEE J. Ocean. Eng. **26**, 594–603 (2001).

[13] R. A. Iltis and A. W. Fuxjaeger, "A digital DS spread-spectrum receiver with joint channel and Doppler shift estimation," IEEE Trans. Commun. **39**, 1255–1267 (1991).

[14] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication* (Cambridge University Press, New York, 2005), pp. 105–109.

[15] J. Ling, T. Yardibi, X. Su, H. He, and J. Li, "Enhanced channel estimation and symbol detection for high speed MIMO underwater acoustic communications," J. Acoust. Soc. Am. **125**, 3067–3078 (2009).

[16] G. Weeks, J. Townsend, and J. Freebersyser, "A method and metric for quantitatively defining low probability of detection," in Proceedings of IEEE Military Communications Conference (1998), Vol. **3**, pp. 821–826.

[17] P. Stoica, H. He, and J. Li, "New algorithms for designing unimodular sequences with good correlation properties," IEEE Trans. Signal Process. **57**, 1415–1425 (2009).

[18] J. Li, P. Stoica, and X. Zheng, "Signal synthesis and receiver design for MIMO radar imaging," IEEE Trans. Signal Process. **56**, 3959–3968 (2008).

[19] J. G. Proakis, *Digital Communications*, 4th ed. (McGraw-Hill, New York, 2001), pp. 254–272.

[20] J. Ling, X. Tan, T. Yardibi, J. Li, M. L. Nordenvaad, and H. He, "Enhanced channel estimation and efficient symbol detection in MIMO underwater acoustic communications," in Proceedings of the 43rd Annual Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA (2009), pp. 600–604.

[21] P. Stoica, H. He, and J. Li, "On designing sequences with impulse-like periodic correlation," IEEE Signal Process. Lett. **16**, 703–706 (2009).