Covert Underwater Acoustic Communications: Transceiver Structures, Waveform Designs and Associated Performances

Jun Ling, Hao He, Jian Li and William Roberts
Department of Electrical and Computer Engineering
University of Florida, Gainesville, FL

Petre Stoica
Department of Information Technology
Uppsala University, Uppsala, Sweden

***Abstract*—Covert communications are conducted at a low received signal-to-noise ratio (SNR) to prevent interception or detection by an eavesdropper, and successful detection in this particular area heavily relies on the processing gain achieved by employing the direct-sequence spread-spectrum (DSSS) technique. If covert communications take place in underwater acoustic (UWA) environments, then additional challenges are present. UWA channels are time-varying in nature, which could preclude an accurate channel estimation at low SNR. Furthermore, UWA environments are frequency-selective with long-memory channels, which imposes challenges to the design of the spreading waveform. In this paper, we investigate covert UWA communications from a noncoherent perspective. Two modulation schemes are addressed, namely, binary orthogonal modulation and binary differential phase-shift keying (DPSK). Both schemes are coupled with the DSSS technique and a RAKE receiver. The employed spreading waveforms not only account for the transceiver structure and frequency-selective nature of the UWA channel, but also serve to protect the privacy of the transmitted information. The effectiveness of the proposed methods is verified by numerical examples.**

I. Introduction

Achieving reliable communications 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 and frequency domains [1]. Delay and Doppler spreadings are 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 a direct-sequence spread-spectrum (DSSS) based modulation technique [3], in which a symbol of information is spread by a waveform with long chip length before transmission, are conventionally referred to as operating at a low data rate. Previous investigations in the literature regarding low data rate UWA communications include [4]–[9]. DSSS technique exploits frequency diversity in a frequency-selective UWA channel and benefits from the spreading gain to allow many active users to share a channel [3]. At the receiver side, feasible decentralized reception schemes (which detect the signal from a particular user in a multi-access scenario using knowledge of the user's particular waveforms, see [7]) encompass nonlinear equalization, like hypothesis-feedback equalization [7], and linear equalization, like RAKE receivers [10]. Performance comparisons of these two reception schemes are presented in [8]. Note that a DSSS-based modulation scheme still allows successful detection even at low chip SNR, which serves to protect the privacy of the transmitted information and to prevent its interception in hostile environments [6]. Consequently, DSSS is a preferred approach when low probability of interception (LPI) or low probability of detection (LPD) is of concern.

Low chip SNR communication over a time-varying UWA channel precludes an accurate channel estimate, and makes various otherwise promising coherent detection schemes ineffective [6]. Consequently, noncoherent schemes become appropriate approaches in this challenging field. In the present paper, we consider a single user case, and two types of noncoherent transceiver design are addressed: namely, orthogonal modulation [11] and differential phase-shift keying (DPSK) [11], both coupled with a DSSS technique and a noncoherent RAKE reception via equal gain combining (EGC) [12]. Although only binary information sequences are considered here, the derivations can be easily extended to a general M-ary case. Various issues arising herein, such as the transceiver structure, the waveform design and the performance analysis, form the focus of this paper. Doppler spread is not addressed in our discussions; investigation of covert UWA communications that accounts for Doppler spreading will be the subject of future work.

At the transmitter side, waveform design should account for the delay spread of the UWA channel [13], as well as the concerns on LPI/LPD. For orthogonal modulation, Hadamard sequences [14] can be used effectively in a flat fading channel, as would be the case in radio communication [3]. In realistic UWA channels, on the other hand, the multipath delay spread ranges up to tens of chip intervals, leading to severe intra- and inter-symbol interferences [1]. In these cases, Hadamard sequences are no longer the optimal choice. Instead, spreading waveforms with good auto- and cross-correlation properties are preferred, such as Gold sequences [15]. For DPSK modulation, a common spreading waveform is phase-modulated by the encoded symbols before transmission [16]. Adopting the cyclic prefix design widely-used in the orthogonal fre-

quency division multiplexing (OFDM) regime, the receiver can eliminate the inter-symbol interference by simply ignoring the prefix chips before proceeding with symbol detection [3]. Consequently, a single waveform with zero periodic correlations over certain lags is desired. These types of sequences are usually named ZCZ (zero-correlation zone) sequences and the relevant literature is extensive, e.g., [17]–[19]. The Frank sequence proposed in [20] is one of the most famous. All of the aforementioned waveforms, namely Hadamard, Gold and Frank sequences, belong to the class of unimodular polyphase sequences, in which the phase value of each chip is drawn from a predefined set with finite elements [21] (to be exact, Hadamard and Gold sequences are binary, with chip either 1 or -1). Gold and Frank sequences are normally chosen for UWA communications at low data rates (see, for example, [4] [5] [9]). These sequences, however, are constructed in a systematic manner with strict constraints on the chip length. Length-constrained polyphase (especially binary) sequences have a significant probability of interception or detection by a brute force exhaustive search, and therefore these sequences have undesirable LPI/LPD properties.

In this paper, algorithms are reviewed to synthesize waveforms whose phase values lie between 0 and 2π and which are computationally trackable. The resultant waveforms not only have enhanced LPI/LPD properties, but also allow for a flexible chip length that can be adjusted to best suit the system requirements. It is worth pointing out that the waveform design and the reception scheme are coupled [13]. Being a linear equalizer, the RAKE receiver cannot effectively combat the severe inter-symbol interference in a frequency-selective UWA channel [8]. This, however, does not imply that the interference cannot be suppressed. Indeed, the adverse effects of the interference can be alleviated by carefully designing the spreading waveforms [13]. 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). We maintain that the simplicity, both in implementation and computation, enjoyed at the receiver side completely justifies the efforts devoted to the waveform design stage. By adopting the two transceiver structures considered here, the corresponding detection performance, in terms of the bit error rate (BER), matches the theoretical values provided in [11].

Many channels, including UWA and wireless, are appropriately modeled as sparse channels, which consist of a few dominant delay and Doppler taps [22]. Incorporating this sparsity characteristic, the RAKE performance can be further improved by discarding the finger outputs associated with the nulls in the channel spectrum and instead combining only those with higher SNR [11]. To address this, a threshold module is cascaded after the finger outputs: an output whose energy is below the threshold is discarded [8] [5]. The resulting performance becomes sensitive to the threshold value, whose selection, to obtain optimal performance, can be rather hard. As an alternative method to this threshold-based RAKE reception, we consider an approach that uses partial channel information by identifying the channel tap with the strongest power (also called the principal arrival, see [23]), and the RAKE receiver is modified to only use the finger output along this dominant tap that enjoys the highest SNR.

This paper is organized as follow. Section II elaborates on various issues that arise when adopting binary orthogonal modulation, coupled with the DSSS methodology and a non-coherent RAKE energy-based detector, such as the modulation scheme and spreading waveform design. A performance evaluation of the detection scheme is also presented. In Section III, these issues are re-considered by shifting our focus to the DPSK modulation regime. Section IV assesses the impact of the processing gain and the frequency-selective channel on the BER performance. The analysis motivates us to modify the RAKE receiver to enhance performance by using only the finger output along the principal arrival. Section V presents numerical examples to verify the effectiveness of the proposed methods. Conclusions are drawn in Section VI.

Notations: Matrices and column vectors are denoted, respectively, by boldface uppercase and lowercase letters. $(\cdot)^T$ refers to the transpose and $(\cdot)^*$ refers to the conjugate transpose of vectors and matrices (or 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 $\binom{a}{b} = \frac{a!}{b!(a-b)!}$ denotes, in statistical jargon, "a choose b". $\mathrm{Re}(\cdot)$ is the real part of a complex value, and $\mathrm{sign}(\alpha) = 1$ if α is positive and -1 otherwise.

II. RAKE Energy-Based Detection of Orthogonal Signals

A. System Outline

Suppose a transmitter maps each symbol (bit) in a binary information sequence to one of two orthogonal spreading waveforms $\{\mathbf{x}_i\}_{i=1}^2$ ($\mathbf{x}_1^*\mathbf{x}_2 = 0$). Each spreading waveform consists of P unimodular chips (i.e., $\mathbf{x}_i = [x_i(1) \ \ldots \ x_i(P)]^T$ where $i \in \{1, 2\}$) and the information is conveyed by choosing one out of the two candidate spreading waveforms. The mapped waveform chips are then up-converted to the carrier frequency and transmitted over a UWA channel in a strong noise background for covert communication. The UWA channel is frequency-selective with R resolved taps. We do not go into the details of the sampling and synchronization procedures, as we assume that such operations have already been employed and that the sampled complex baseband signals are available at the receiver.

Let us assume that the spreading waveform $\mathbf{x}_1$ is transmitted over one symbol (bit) interval. We confine our focus on detecting this waveform (the discussion for $\mathbf{x}_2$ is similar). The problem can then be formulated as:

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

where $\mathbf{y} = [y(1), \ldots, y(P+R-1)]^T$ and $\mathbf{e} = [e(1), \ldots, e(P+R-1)]^T$ represent, respectively, the vectors of the incoming measurements and the noise terms. We assume the noise to be a complex-valued white Gaussian random process with zero

mean and variance σ^2, denoted as $\mathbf{e} \sim \mathcal{CN}(0, \sigma^2\mathbf{I})$. The channel impulse response (CIR) vector is $\mathbf{h} = [h(1), \ldots, h(R)]^T$. The matrix $\mathbf{X} \in \mathcal{C}^{(P+R-1)\times R}$ contains multiple shifted replicas of the transmitted chips, given by:

$$\mathbf{X} = \begin{bmatrix} x_1(1) & x_i(P) & \ldots & x_i(P-R+2) \\ \vdots & x_1(1) & & x_i(P-R+3) \\ x_1(P) & \vdots & \ddots & \vdots \\ x_j(1) & x_1(P) & & x_i(P) \\ \vdots & x_j(1) & \ddots & x_1(1) \\ x_j(R-2) & \vdots & \ddots & \vdots \\ x_j(R-1) & x_j(R-2) & & x_1(P) \end{bmatrix}, \quad (2)$$

where $\mathbf{x}_i$ and $\mathbf{x}_j$ denote the waveforms transmitted before and after the current waveform, respectively. Subscripts $i, j \in \{1, 2\}$, but their specific values cannot be determined due to the randomness nature of the original bit sequence.

Expressing the received measurements as in (1), the problem of interest reduces to determining which waveform out of two candidates is transmitted ($\mathbf{x}_1$ in this example) given the measurements $\mathbf{y}$. Covert communication with low chip SNR over a time-varying UWA channel basically constrains the feasible detection methodologies to the noncoherent domain. Consequently, knowledge of $\mathbf{h}$ is not incorporated into the detection procedure.

Herein, we explore the key characteristics of the two spreading waveforms that facilitate noncoherent RAKE reception. To pursue this idea, it is instructive to assess the impact of the auto- and cross-correlation properties of the spreading waveforms on the outputs of each finger used in the RAKE receiver. An interesting analysis follows from the decomposition of the matrix $\mathbf{X}$ in (2) to isolate the spreading waveform of interest $\mathbf{x}_1$ from its adjacent waveforms (i.e., $\mathbf{x}_i$ and $\mathbf{x}_j$). We can rewrite the matrix $\mathbf{X}$ as:

$$\mathbf{X} = \mathbf{X}_1 + \mathbf{A}_{ij}, \quad (3)$$

where the dimensions of $\mathbf{X}_1$ and $\mathbf{A}_{ij}$ conform with those of $\mathbf{X}$. The matrix $\mathbf{X}_1$ contains only the shifted replicas of $\mathbf{x}_1$:

$$\mathbf{X}_1 = \begin{bmatrix} x_1(1) & & \mathbf{0} \\ \vdots & \ddots & \\ x_1(P) & & x_1(1) \\ & \ddots & \vdots \\ \mathbf{0} & & x_1(P) \end{bmatrix}, \quad (4)$$

while $\mathbf{A}_{ij} = \mathbf{X} - \mathbf{X}_1$ is composed of the chips of the adjacent waveforms $\mathbf{x}_i$ and $\mathbf{x}_j$.

The structure of an energy-based RAKE detector for binary orthogonal waveforms is shown in Fig. 1. This structure can be roughly divided into two stages. The first stage projects the incoming measurements $\mathbf{y}$ onto vector $\mathbf{x}_m^{(r)} \in \mathcal{C}^{(P+R-1)\times 1}$, which is a shifted version of the waveform $\mathbf{x}_m$ associated

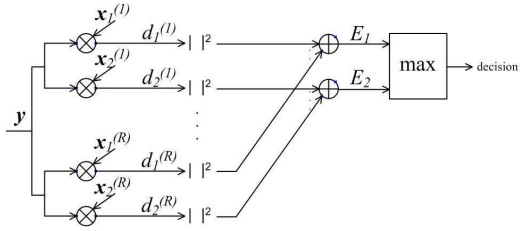


Fig. 1. Structure of an energy-based RAKE detector for binary orthogonal waveforms.

with the r^{th} channel tap (i.e., the path represented by $h(r)$). The vector $\mathbf{x}_m^{(r)}$ is constructed by padding, respectively, $r-1$ and $R-r$ zeros before and after the spreading waveform $\mathbf{x}_m$:

$$\mathbf{x}_m^{(r)} = [\ \underbrace{0\ \ldots\ 0}_{r-1}\ x_m(1)\ x_m(2)\ \ldots\ x_m(P)\ \underbrace{0\ \ldots\ 0}_{R-r}\ ]^T, \quad (5)$$

where $m = 1, 2$ and $r = 1, \ldots, R$. We define the correlation function as:

$$r_{\tilde{i}\tilde{j}}(k) = \sum_{n=k+1}^{P} x_{\tilde{i}}(n) x_{\tilde{j}}^*(n-k), \quad (6)$$

where $\tilde{i}, \tilde{j} = 1, 2$ and $k = 0, \ldots, P-1$. When $\tilde{i}$ equals $\tilde{j}$, the quantity $r_{\tilde{i}\tilde{i}}(k)$ reflects the auto-correlation property of the waveform $\mathbf{x}_{\tilde{i}}$; otherwise, $r_{\tilde{i}\tilde{j}}(k)$ shows the cross-correlation property between the waveforms $\mathbf{x}_{\tilde{i}}$ and $\mathbf{x}_{\tilde{j}}$.

By using these notations, it can be easily verified that:

$$\begin{aligned} \mathbf{x}_m^{(r)*}\mathbf{X}_1 &= [r_{1m}(r-1)\ \ldots\ r_{1m}(1)\ r_{1m}(0) \\ &\quad\ r_{m1}^*(1)\ \ldots\ r_{m1}^*(R-r)], \quad (7) \\ \mathbf{x}_m^{(r)*}\mathbf{A}_{ij} &= [r_{mj}^*(P-r+1)\ \ldots\ r_{mj}^*(P-1)\ 0 \\ &\quad\ r_{im}(P-1)\ \ldots\ r_{im}(P-R+r)]. \quad (8) \end{aligned}$$

Based on (7) and (8), we can express the output of a RAKE finger $d_m^{(r)}$, i.e., the projection of $\mathbf{y}$ onto $\mathbf{x}_m^{(r)}$, as:

$$\begin{aligned} d_m^{(r)} &= \frac{\mathbf{x}_m^{(r)*}\mathbf{y}}{||\mathbf{x}_m||} \\ &= e_m^{(r)} + \frac{1}{||\mathbf{x}_m||}\left\{ \sum_{q=1}^{r-1} \left[r_{1m}(r-q) + r_{mj}^*(P-r+q)\right] h(q) + \right. \\ &\left. \sum_{q=r+1}^{R} \left[r_{m1}^*(q-r) + r_{im}(P-q+r)\right] h(q) + r_{1m}(0)h(r) \right\}, \quad (9) \end{aligned}$$

where $i, j, m = 1, 2$, $r = 1, 2, \ldots, R$, and $e_m^{(r)} = \frac{\mathbf{x}_m^{(r)*}\mathbf{e}}{||\mathbf{x}_m||}$. The factor $\frac{1}{||\mathbf{x}_m||}$ is for normalization such that $e_m^{(r)} \sim \mathcal{CN}(0, \sigma^2)$ given that $\mathbf{e} \sim \mathcal{CN}(0, \sigma^2\mathbf{I})$.

A frequency-selective channel scatters the signal power over R resolved channel paths, and the second stage of the RAKE receiver combines the scattered energy along each candidate vector by performing EGC [3] [12]:

$$E_m = \sum_{r=1}^{R} \left| d_m^{(r)} \right|^2, \qquad m = 1, 2. \quad (10)$$

By comparing E_1 and E_2, a final decision is made in favor of the one with larger power. Since we assume that $\mathbf{x}_1$ is transmitted, a wrong decision occurs if $E_1 < E_2$.

Note that (9) includes a flat-fading channel as a special case by fixing $R = 1$. In this way, $\mathbf{X} = \mathbf{X}_1$ shrinks to a

column vector (indicating no intra-symbol interference), and $\mathbf{A}_{ij}$ reduces to a zero column vector (indicating no inter-symbol interference). Consequently, (9) is simplified as:

$$d_m = \frac{r_{1m}(0)h(1)}{||\mathbf{x}_m||} + e_m, \qquad m = 1, 2. \tag{11}$$

A flat-fading channel is represented by a single tap $h(1)$, therefore the r index is suppressed in (11) without introducing any ambiguity. We observe that the quantities $\{r_{1m}(0)\}_{m=1}^{2}$ involved in (11) are concerned only with the in-phase case (i.e., with 0 delay lag). Consequently, for a flat-fading channel, the Hadamard waveforms [14] [24] are optimal choices in the sense of nulling the in-phase cross-correlation functions, which can be stated as:

$$\begin{cases} r_{11}(0) = r_{22}(0) = P, \\ r_{12}(0) = r_{21}(0) = 0. \end{cases} \tag{12}$$

On the other hand, for a general frequency-selective channel with $R > 1$, correlation functions other than $\{r_{1m}(0)\}_{m=1}^{2}$ appear in (9). Consequently, the Hadamard sequences are no longer optimal. Instead, the Gold sequences [15] are widely used due to their superior auto- and cross-correlation properties. A key aspect relevant to the Hadamard and Gold sequences is that the chip length P is constrained to 2^k and to $2^k - 1$ (where k is some integer), respectively. In the next subsection, we consider how to design two spreading waveforms with flexible length while still achieving good auto- and cross-correlation properties.

B. Spreading Waveform Design

By expressing the finger outputs in terms of the auto- and cross-correlation functions, (9) offers insights into formulating the design criteria for the spreading waveforms. The contributions of the auto- and cross-correlation functions are carried over into the finger output $d_m^{(r)}$ through a weighted sum, with the channel taps being the weights. In the absence of prior information on $\mathbf{h}$, the best we can do is to design two spreading waveforms such that, other than the quantities $\{r_{ii}(0)\}_{i=1}^{2}$ (which equal P by definition), all the other correlation functions involved in (9) are 0. Mathematically, we want

$$\begin{cases} r_{11}(k) = r_{22}(k) = 0, \quad k \in \mathcal{A}_1, \\ r_{12}(k) = r_{21}(k) = 0, \quad k \in \mathcal{A}_2, \end{cases} \tag{13}$$

where $\mathcal{A}_1 = \{1, \ldots, R-1\} \cup \{P-R+1, \ldots, P-1\}$ and $\mathcal{A}_2 = \{0, \ldots, R-1\} \cup \{P-R+1, \ldots, P-1\}$. We assume that $P > 2R-2$.

Inserting (13) into (9) and recalling that $r_{11}(0) = r_{22}(0) = P$, we have:

$$d_m^{(r)} = \begin{cases} \sqrt{P}h(r) + e_1^{(r)}, & m = 1, \\ e_2^{(r)}, & m = 2. \end{cases} \tag{14}$$

Thus two waveforms that perfectly satisfy (13) decompose the original multipath problem into R independent flat-fading channels that do not interfere with each other. In this ideal case, the matched filter based RAKE finger is optimal in the sense of maximizing the output SNR.

In the literature of waveform design, the WeCAN algorithm proposed in [25] is viable to synthesize two waveforms that approximately satisfy (13).

C. Performance Evaluation

With the two waveforms synthesized by the algorithm presented in the previous subsection, we proceed here to evaluate the BER performance by using the reception structure shown in Fig. 1. In a strict sense, the two synthesized spreading waveforms are not perfect (consider the *Remark* at the end of the last subsection). The imperfection of the waveforms, combined with the random channel condition, can be interpreted as a small perturbation to the quantities shown in (14). The following performance evaluation ignores this perturbation, i.e., we assume that the two waveforms satisfy (13) perfectly.

Let $\mathbf{SNR} = ||\mathbf{h}||^2/\sigma^2$ be the received chip SNR before RAKE processing; this notation will be used throughout the rest of the paper unless stated otherwise. By using **SNR**, the BER performance can be expressed as [26]:

$$P_{\text{BER}} = \frac{e^{-\lambda}}{2^{2R-1}} \sum_{k=0}^{R-1} \left[\frac{1}{k!} \sum_{n=1}^{R-1-k} \binom{2R-1}{n} \right] \lambda^k, \tag{15}$$

where $\lambda = \frac{P}{2}\mathbf{SNR}$.

III. RAKE Demodulator for DPSK signals

A. System Outline

DPSK is a widely-used encoding scheme, in which a transmitted symbol of information is conveyed in the phase difference between two successive encoded symbols. Depending on the channel conditions, a DPSK detection scheme can be conducted either coherently (predetection MRC) or noncoherently (postdetection EGC) [27]. In general, a noncoherent approach is preferred for covert communication applications, in which the reliability of the communication heavily depends on the processing gain achieved by adopting a DSSS technique and the assumption that the channel fades slowly (so that the channel taps remain stable over at least two successive symbol periods) [11] [6].

Denote $\{b_i\}$ and $\{a_i\}$ as the original information symbols and the DPSK encoded symbols, respectively. For expositional simplicity, we consider binary symbols with the entries of $\{b_i\}$ and $\{a_i\}$ either 1 or -1. The results developed in this section, however, can be extended to a general M-ary symbol scenario, through some relatively involved calculations [11].

Given a binary information sequence $\{b_i\}$, $\{a_i\}$ is constructed recursively as:

$$a_i = b_i a_{i-1}, \qquad i = 1, 2, \ldots, \tag{16}$$

with symbol a_0 initialized to be either -1 or 1. In typical DSSS applications, encoded DPSK symbols (bits) $\{a_i\}$ phase-modulate (or, multiply) a common waveform, say $\tilde{\mathbf{x}}$, before transmission over a UWA channel.

Fig. 2 shows a phase-modulated spreading waveform $a_i\tilde{\mathbf{x}}$ propagating over R resolved paths. The multipath effects are reflected by the shifted replicas of $a_i\tilde{\mathbf{x}}$, where $\tilde{\mathbf{x}}$ has chip length $R + P - 1$ and is phase-modulated by encoded symbol a_i. Due to the delay spreading, for a frequency-selective channel with R resolved paths, the inter-symbol interference from the waveform $a_{i-1}\tilde{\mathbf{x}}$ in the previous symbol period extends over the first $R-1$ chips of $a_i\tilde{\mathbf{x}}$. The receiver can simply ignore

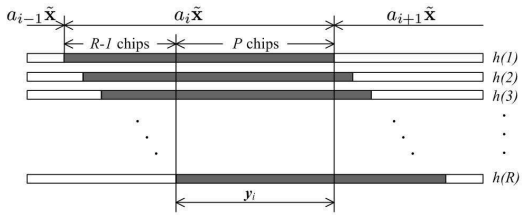


Fig. 2. Phase-modulated spreading waveforms propagate over a frequency-selective channel with R resolved paths.

this inter-symbol interference by considering only the output $\mathbf{y}_i$ over the remaining P chips, where the effects of $a_{i-1}\tilde{\mathbf{x}}$ have died out. By considering $\mathbf{y}_i$, the intra-symbol interference becomes the only possible source of interference.

Reminiscent of the cyclic prefix adopted in OFDM [3], the common waveform $\tilde{\mathbf{x}}$ can be mathematically expressed as:

$$\tilde{\mathbf{x}} = [\underbrace{x(P-R+2)\ \ldots\ x(P)}_{R-1 \text{ prefix chips}}\ x(1)\ x(2)\ \ldots\ x(P)], \quad (17)$$

where the first $R-1$ elements are the prefix chips, and they are a copy of the last $R-1$ chips of $\tilde{\mathbf{x}}$. This way, based on Fig. 2, the incoming measurements $\mathbf{y}_i \in \mathcal{C}^{P\times 1}$ can be represented as:

$$\mathbf{y}_i = a_i\mathbf{X}\mathbf{h} + \mathbf{e}_i, \qquad i = 1, 2, \ldots, \quad (18)$$

where

$$\mathbf{X} = \begin{bmatrix} x(1) & x(P) & \ldots & x(P-R+2) \\ x(2) & x(1) & \ldots & x(P-R+3) \\ \vdots & \vdots & \ddots & \vdots \\ x(P) & x(P-1) & \ldots & x(P-R+1) \end{bmatrix}_{P\times R}, \quad (19)$$

the CIR vector $\mathbf{h}$ has the same definition as in (1), and $\mathbf{e}_i \in \mathcal{C}^{P\times 1}$ is the noise vector in the ith symbol period, which follows the distribution $\mathcal{CN}(0, \sigma^2\mathbf{I})$. Note that $\mathbf{X}$ and $\mathbf{h}$ are independent of the symbol period i. By investigating (19), we can see that the cyclic prefix scheme entrusts $\mathbf{X}$ with a cyclic shift property. That is, the rth column of $\mathbf{X}$, say $\mathbf{x}_r$, is derived by cyclically rotating the first column $\mathbf{x}_1$ by $r-1$ chips, where $r = 2, \ldots, R$.

A noncoherent RAKE receiver structure corresponding to the considered modulation scheme is illustrated in Fig. 3. The receiver first removes the $R-1$ prefix chips, followed by an array of R RAKE fingers designed to combine multipath arrivals. During the ith symbol period, the rth finger projects $\mathbf{y}_i$ onto vector $\mathbf{x}_r$ (i.e., the rth column of $\mathbf{X}$, see (19)), generating:

$$d_i^{(r)} = \mathbf{x}_r^*\mathbf{y}_i, \qquad r = 1, \ldots, R. \quad (20)$$

Each RAKE finger is followed by a differential phase decoder, which correlates $d_i^{(r)}$ with $d_{i-1}^{(r)}$. The quantity $d_{i-1}^{(r)}$ is similarly derived to (20), but in the preceding signaling interval. Denote the output of this correlation as $c_i^{(r)}$, where

$$c_i^{(r)} = d_{i-1}^{(r)*}d_i^{(r)}, \qquad r = 1, \ldots, R. \quad (21)$$

The EGC sums the quantities $\{c_i^{(r)}\}_{r=1}^R$ to generate a sufficient statistic for estimating the information bit b_i [11].

We can see that if the columns of $\mathbf{X}$ are orthogonal to each other, (20) equals

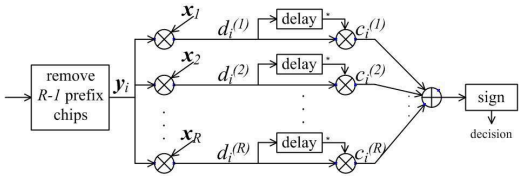


Fig. 3. Noncoherent RAKE demodulator for binary DPSK signals.

$$d_i^{(r)} = a_iPh(r) + \mathbf{x}_r^*\mathbf{e}_i, \qquad r = 1, \ldots, R, \quad (22)$$

which means that the finger outputs are not contaminated by any intra-symbol inference. Consequently, we are particularly interested in designing a waveform with P chips such that its cyclically rotated versions (which appear in the $\mathbf{X}$ matrix) are orthogonal to each other. This requirement is equivalent to designing a ZCZ waveform with

$$\hat{r}_k = 0, \quad k = 1, \ldots, R-1, \quad (23)$$

where $\{\hat{r}_k\}$ is the so-called periodic (auto) correlation function, defined as:

$$\hat{r}_k = \sum_{n=1}^{P} x^*(n)x((n+k) \bmod P), \quad (24)$$

where $k = -(P-1), \ldots, 0, \ldots, (P-1)$.

Before we end this subsection, it is worth emphasizing that an apparent disadvantage of the cyclic prefix scheme is that the data rate is reduced by a factor of $\frac{R-1}{P+R-1}$, since the receiver discards the $R-1$ prefix chips [3].

B. Waveform Design

As mentioned in the Section I, there exist several types of sequences with zero periodic correlation functions over certain lag intervals. Consider, for example, the Frank sequence [20] given by:

$$x((n-1)q + k) = e^{j2\pi nk/q}, \qquad n, k = 1, 2, \ldots, q, \quad (25)$$

which exhibits zero periodic correlations over the entire lag range (i.e., $1, 2, \ldots, P-1$), not only over the support shown in (23). However, the chip length P of a Frank sequence must be a perfect square, i.e., $P = q^2$. Other sequences with zero periodic correlation functions previously suggested in the literature (e.g., [17]–[19] and the references therein) have either length constraints or are constructed such that the number of candidate waveforms is limited. Consequently, these ZCZ waveforms exhibit undesirable LPI/LPD properties. Furthermore, a flexible system should allow the designer to freely choose the chip length to best suit the system needs. To this end, we suggest the PeCAN algorithm [28], which is similar to the CAN algorithm proposed in [29], and which can be used to generate many waveforms with flexible length and with zero periodic correlations over the entire lag interval.

C. Performance Evaluation

With the waveform synthesized by the PeCAN algorithm, we proceed to evaluate the BER performance. Assume that the PeCAN waveform satisfies (23) (almost) exactly (which will be verified shortly by means of numerical examples). Under this condition, the RAKE finger output is given by (22), and correspondingly, $c_i^{(r)}$ can be expressed as:

$$c_i^{(r)} = a_{i-1}^*a_i|h(r)|^2P^2 + \Delta e, \quad (26)$$

where $\Delta e = Ph(r)^* a_{i-1}^* \mathbf{x}_r^* \mathbf{e}_i + Ph(r) a_i \mathbf{e}_{i-1}^* \mathbf{x}_r + \mathbf{e}_{i-1}^* \mathbf{x}_r \mathbf{x}_r^* \mathbf{e}_i$.

In a flat-fading channel with $R = 1$, the detection is based on the sign of the sufficient statistic $\mathrm{Re}\left(c_i^{(1)}\right)$ [11]

$$\hat{x}_i = \mathrm{sign}\left[\mathrm{Re}\left(c_i^{(1)}\right)\right]. \tag{27}$$

For a frequency-selective channel with $R > 1$, on the other hand, the sufficient statistic becomes $\mathrm{Re}\left(\sum_{r=1}^{R} c_i^{(r)}\right)$. Similar to (27), the detection is based on (see Fig. 3) [11]:

$$\hat{x}_i = \mathrm{sign}\left[\mathrm{Re}\left(\sum_{r=1}^{R} c_i^{(r)}\right)\right]. \tag{28}$$

The BER performance of this detection scheme follows from [11] [26]:

$$P_{\mathrm{BER}} = \frac{e^{-\tilde{\lambda}}}{2^{2R-1}} \sum_{k=0}^{R-1} \left[\frac{1}{k!} \sum_{n=1}^{R-1-k} \binom{2R-1}{n}\right] \tilde{\lambda}^k, \tag{29}$$

where $\tilde{\lambda} = P\mathbf{SNR}$.

IV. The Impact of P and R on Performance and an Enhanced RAKE Scheme

In this section, we proceed to investigate the impact of P and R on the BER performance. The numerical analysis leads to the discouraging conclusion that the reliability of the communication schemes is questionable, since the UWA frequency-selective channel requires a large R value, which leads to severe degradation in the BER performance. This degradation can be compensated for, to some extent, by using a longer spreading waveform(s) (i.e., a larger P). The time-varying nature of the UWA channel, however, constrains the largest P value that we can use. This dilemma leads us to the idea of exploiting the sparse nature of the UWA channel: we identify the path corresponding to the principal arrival that enjoys the highest SNR, and use only the output from this RAKE finger to make decisions.

A. Impact of P and R on the BER performance

The **SNR** defined above (15) is an important metric for evaluating the covertness of communications. For example, a received signal transmitted at a level of **SNR** < -8 dB within the signal band is hard to detect by an unalerted eavesdropper [6]. By comparing (15) and (29), we can see that for binary orthogonal modulation, **SNR** should be doubled to achieve the same BER as DPSK. Fig. 4 therefore gives several BER curves with different values of P and R only for DPSK modulation. Note once again that these curves are derived by assuming perfect spreading waveform(s).

We observe from Fig. 4 that for a fixed processing gain P, a flat-fading channel with $R = 1$ gives the best BER performance, and that the larger the value of R, the more severe degradation the BER performance suffers (see also [11]). In UWA applications, the R value is determined by several factors, such as the acoustic conditions, the chip rate, the sampling scheme at the receiver side and the communication

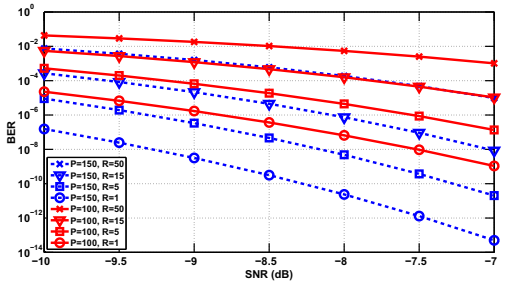


Fig. 4. BER curves for the DPSK modulation with different values of P and R.

range. For a typical frequency-selective UWA channel, a value of 50 or more for R is quite normal. For $R = 50$, we can see that for DPSK, using a spreading waveform with $P = 100$, the BER equals 5.4×10^{-3} at an **SNR** of -8 dB.

Theoretically, the performance degradation that results from a larger R can be compensated for by adopting a spreading waveform with a larger P, as is also verified by Fig. 4. A larger P, however, further decreases the data rate for both the orthogonal and DPSK modulation schemes. Also, the time-varying nature of the UWA channel constrains the maximum P value that we can use. This constraint leads us to considering a performance enhancement method that does not require increasing P.

B. RAKE Reception Based on the Principal Arrival

Many channels, including UWA communication channels, can be considered to be sparse, as they consist of only a few dominant delay and Doppler taps [22]. This sparsity feature, however, has not been addressed in our discussion so far. In UWA communication over a sparse frequency-selective channel, the channel paths associated with the nulls in the channel spectrum contain no information about the transmitted signal, and the finger outputs on these paths comprise only noise. The EGC stage of the RAKE receiver does not distinguish these defective paths from those carrying the signal power. Indeed, the finger outputs are equally weighted and summed. Consequently, after EGC, the noise contaminates also the reliable finger outputs with higher SNR, and a poor BER performance is expected.

A natural way to alleviate this problem is to discard the finger outputs associated with the nulls in the channel spectrum and instead combine only those outputs with higher SNR [11]. In [5] [8], a threshold module is cascaded after each finger output, and an output whose energy is below that threshold is not included when performing EGC. However, the resulting performance becomes sensitive to the threshold value whose selection, to obtain optimal performance, is not easy.

An alternative method to the threshold-RAKE reception is to instead make a decision by using only the finger output along the principal arrival (i.e., the tap with the strongest power, see [23]) that enjoys the highest SNR. The feasibility of this idea is demonstrated by the fact that, in general, a dominant channel tap can be associated in relatively benign shallow water environments with the principal arrival [23]

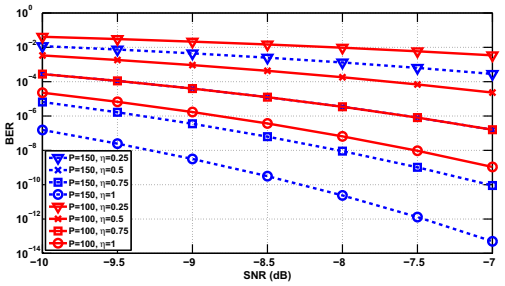


Fig. 5. BER curves with different values of P and η formed by using only the principal arrival for the DPSK modulation.

[6]. The key problem then is how to identify this principal arrival. In a strict sense, the attempt to identify the principal arrival incorporates partial channel information, which basically violates the noncoherent nature. On the other hand, this is not coherent reception either, since the receiver does not undo the phase shift introduced by the UWA channel during propagation. We will show shortly that the BER performance of this hybrid reception scheme is considerably enhanced as long as the principal arrival is successfully identified and its corresponding path sufficiently dominates the channel power.

Identification of the principal arrival requires that a known probing sequence be first transmitted. The probing sequence helps not only to synchronize the transmitted information, but also to identify the principal arrival. With binary DPSK modulation for example, a probing sequence can be constructed by repeating $\tilde{\mathbf{x}}$, say α times, where $\tilde{\mathbf{x}}$ is constructed by prefixing the PeCAN waveform, as in (17). We still use the receiver structure in Fig. 3, but only the finger outputs $\{d_i^{(r)}\}_{r=1}^{R}$ $(i = 1, \ldots, \alpha)$ are of interest in the probing mode. Based on (22), the sample mean along the rth RAKE finger, i.e., $\frac{1}{\alpha}\sum_{i=1}^{\alpha} d_i^{(r)}$, has a $\mathcal{CN}(Ph(r), \frac{P\sigma^2}{\alpha})$ distribution, where $r = 1, \ldots, R$. Statistically, a larger α decreases the variance of the sample mean, and centralizes the sample mean to $Ph(r)$. Consequently, a larger α favors the identification of the principal arrival: we simply pick up the finger path that generates the largest norm of the sample mean. However, a larger α decreases the net data rate. This method can also be applied to the orthogonal modulation case by sending $\mathbf{x}_1$ α times and, during the probing mode, projecting the received information onto only $\mathbf{x}_1$. Note that if the channel were time-invariant, a single long WeCAN or PeCAN waveform would have been used as the probing waveform. To address the piecewise time-invariant assumption, several shorter waveforms could be cascaded to avoid using a single probing waveform.

We can now derive the BER expressions when the RAKE receiver only uses the finger output along the principal arrival. For binary orthogonal modulation, by setting $R = 1$, (15) reduces to:

$$P_{\text{BER}} = \frac{1}{2}\exp\left(-\frac{\eta P \mathbf{SNR}}{2}\right), \tag{30}$$

where $\eta = \frac{|h(r)|^2}{||\mathbf{h}||^2} \in [0, 1]$ is the ratio of the power of the principal arrival to the total channel power. Similarly, for

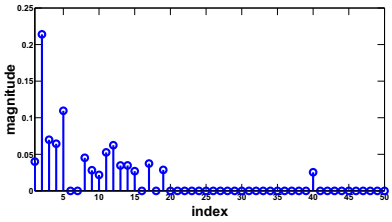
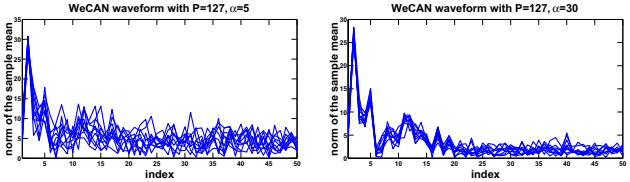


Fig. 6. The magnitude of the simulated CIR. Among the $R = 50$ taps, 34 are nulls. The dominant tap is $h(2)$ with $\eta = 54.27\%$.



(a) (b)

Fig. 7. Principal arrival identification using a probing sequence with **SNR** $= -10$ dB. 10 Monte-Carlo trials are shown. (a) $\alpha = 5$ and (b) $\alpha = 30$.

DPSK modulation, by setting $R = 1$, (29) reduces to:

$$P_{\text{BER}} = \frac{1}{2}\exp\left(-\eta P \mathbf{SNR}\right). \tag{31}$$

Note that in either case, a factor of $1-\eta$ of the signal power is lost by using the principal arrival only. By comparing (30) and (31), we can see, once again, that to achieve the same BER performance, orthogonal modulation requires twice the **SNR** as DPSK does. The BER curves versus **SNR** for different η and P values are plotted in Fig. 5 for the DPSK scenario only. As evidenced, if the principal arrival occupies only $\eta = 0.25$ of the total channel power, the resultant BER performance for $P = 100$ is comparable to that shown in Fig. 4 with $R = 50$. In general, however, a principal arrival with $\eta = 0.25$ is quite a conservative assumption, and larger values of η promising better BER performance (see Fig. 5) occur in applications.

V. Numerical Examples

The main purpose of this section is to assess the BER performance achieved by using the WeCAN and PeCAN waveforms. The covertness of the communication is also addressed. We start by considering binary orthogonal modulation, and then we consider the binary DPSK model.

A. Binary Orthogonal Modulation

Consider a simulated time-invariant frequency-selective channel represented by $R = 50$ resolved taps, as shown in Fig. 6. To address sparsity, 34 out of 50 taps are nulls. The second tap $h(2)$ is the principal arrival with $\eta = 54.27\%$. Two WeCAN spreading waveforms $\{\mathbf{x}_i\}_{i=1}^{2}$, each with a chip length $P = 127$, are used to spread the information symbols (bits). The P value for the WeCAN spreading waveforms can be arbitrary but is chosen as 127 to meet the length constraint imposed on the Gold sequence (to ensure a proper comparison in the forthcoming analysis).

Using the available WeCAN spreading waveforms, we first investigate the performance of the principal arrival identification by transmitting a probing sequence over the simulated

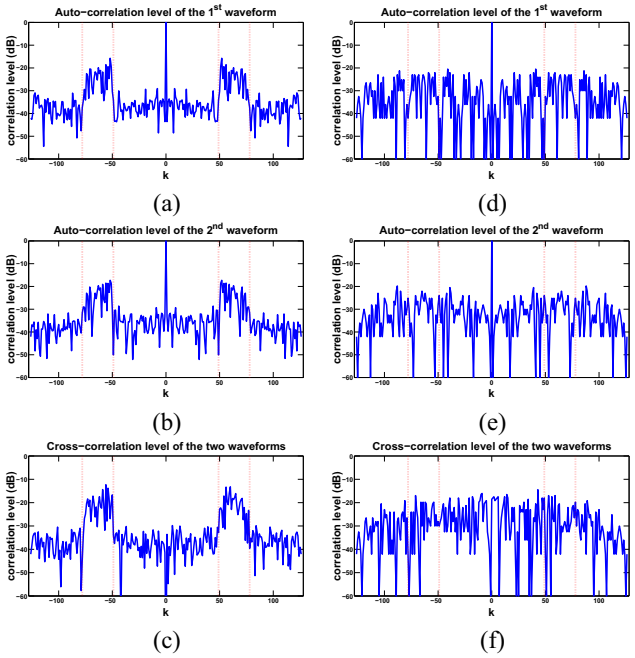


Fig. 8. Correlation levels of the WeCAN sequences and Gold sequences with $P = 127$. (a)-(c) WeCAN sequences and (d)-(f) Gold sequences. Zero correlation levels of Gold sequences are represented by -60 dB. The vertical dashed lines indicate the lag intervals $[-126, -78] \cup [-49, 49] \cup [78, 126]$, over which we want to suppress the correlation levels.

channel represented by the CIR shown in Fig. 6. Note that this simulated channel is time-invariant. Consequently, a single long probing sequence could be employed. To be consistent with the approach developed in the previous section, we will apply a probing sequence constructed via repeating $\mathbf{x}_1$ α times. At the receiver side, the incoming measurements are projected onto $\{\mathbf{x}_1^{(r)}\}_{r=1}^{50}$ (see Fig. 1). The norms of the sample mean along each RAKE finger are plotted in Fig. 7 using 10 Monte-Carlo trials. We fix $\mathbf{SNR} = -10$ dB and use two different α values 5 and 30. We can see that by using a larger α value, the curves in Fig. 7(b) show less variance than (a), which favors the identification of the principal arrival, and this observation is in line with the remark made in the previous section. In both cases, the principal arrival $h(2)$ is successfully identified.

We are interested in comparing the BER performance by using WeCAN waveforms and Gold waveforms. To be exact, since only two waveforms are required, Gold waveforms in this case reduce to a preferred pair of m-sequences [15]. The preferred generator polynomials are [7 3 0] and [7 3 2 1 0], respectively. We investigate the correlation levels of the two types of waveforms before proceeding with the evaluation of the BER performance. The auto- and cross-correlation level of the WeCAN waveforms and of the Gold waveforms are plotted in Fig. 8, where the correlation level is defined as:

$$\text{correlation level} = 20\log_{10}\left|\frac{r_{\tilde{i}\tilde{j}}(k)}{P}\right| \text{ dB}, \qquad (32)$$
$$\tilde{i}, \tilde{j} = 1, 2, \qquad k = 0, 1, \ldots, P-1,$$

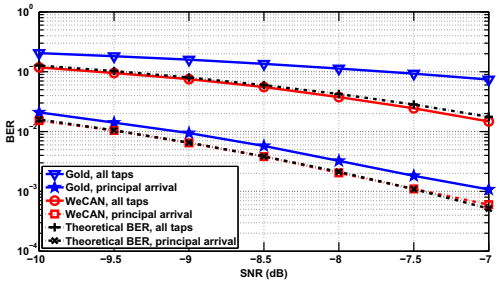


Fig. 9. The empirical BER curves corresponding to WeCAN sequences and Gold sequences with $P = 127$, the theoretical values are plotted alongside. Two reception schemes are considered: one uses EGC over all the $R = 50$ finger outputs, and the other uses the principal arrival only.

and $r_{\tilde{i}\tilde{j}}(k)$ is defined in (6). Note that the correlation levels of Gold sequences are zero at certain lags, and these points are represented by -60 dB in Fig. 8 (d)$\sim$(f). We observe that overall the WeCAN waveforms give lower correlation levels over the lag ranges of interest than the Gold sequences.

Next, the BER performance is evaluated. The selected information sequence consists of 1000 symbols (bits), and each symbol is mapped to one of the waveforms. The incoming measurements are constructed according to Equation (1), with the noise vector $\mathbf{e} \sim \mathcal{CN}(0, \sigma^2\mathbf{I})$. The frequency-selective channel, as shown in Fig. 6, is considered here. We address two reception schemes. The first scheme implements an EGC over $R = 50$ RAKE fingers, as shown in Fig. 1, and the other relies on the principal arrival only, which we assume has been successfully identified in the probing mode. The resulting empirical BER curves are shown in Fig. 9, along with the theoretical BER given by (15) and (30). Each point is averaged over 1000 independent Monte-Carlo runs. Since the principal arrival occupies $\eta = 54.27\%$ of the total channel power, a considerable BER improvement by using the RAKE finger along this path only is achieved. Note the good agreement between the theoretical BER curves and those derived by adopting WeCAN waveforms. This can be explained by the quite low correlation levels at the lags of interest for the WeCAN waveforms. On the other hand, in this particular example, the BER curves of the Gold waveforms deviate from the theoretical curves due to their higher sidelobe levels within the lag ranges of interest. To enhance the BER performance, we can either apply sophisticated channel coding scheme, which comes at the price of a further reduced data rate, or increase P value if the channel permits.

Finally, we consider the covertness of the communication scheme. We assume that, except for precise knowledge of the spreading waveforms $\{\mathbf{x}_i\}_{i=1}^2$, an eavesdropper has the same information about the communication details as an intended receiver, such as the value of $P = 127$, the location of the principal arrival, the package structure and modulation scheme, etc. The eavesdropper tries to detect the transmitted information by generating a pair of spreading waveforms, whose chips have independently and randomly generated phase values. The resulting BER performance is plotted in Fig. 10 by conducting 1000 independent Monte-Carlo runs.

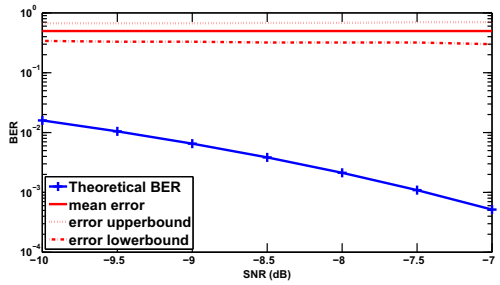
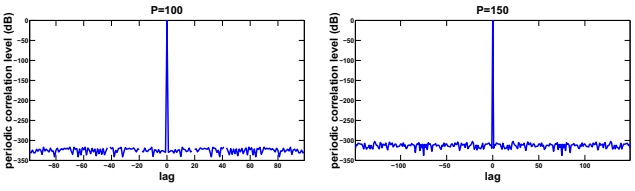
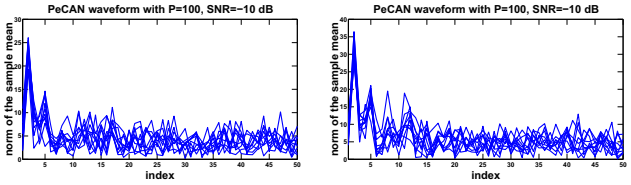


Fig. 10. BER performance achieved by generating the unimodular waveforms in a random manner. The BER is 0.5 on average, implying desired LPI/LPD properties for the WeCAN waveforms.



(a) (b)

Fig. 11. The periodic correlation levels of the PeCAN waveform. (a) $P = 100$ and (b) $P = 150$.



(a) (b)

Fig. 12. Principal arrival identification using probing waveforms with **SNR** $= -10$ dB. 10 Monte-Carlo trials are shown. (a) $P = 100$ and (b) $P = 150$.

We can see that the BER is 0.5 on average. The error lowerbound or upperbound is not produced by a specific trial. Instead, they are the minimum and maximum values over the entire 1000 trials. From Fig. 10, we can see that the detection performance by generating spreading waveforms in a random manner is on the average the same as that of a uninformed guess. Consequently, the WeCAN waveforms have desirable LPI/LPD properties. For Gold sequences with length P, on the other hand, the eavesdropper can exhaust all pairs of Gold waveforms by using all the possible preferred pairs of P-length m-sequences.

B. DPSK Modulation

Now we shift our focus to the DPSK modulation. We start by investigating the periodic correlation property of the PeCAN waveform.

Fig. 11 shows the periodic correlation levels of two different PeCAN waveforms with P being 100 and 150. The two PeCAN waveforms have practically 0 correlation sidelobes over the non-zero lags. The sidelobe level shown in Fig. 11 is about -320 dB, i.e., 10^{-16}, which is the smallest number that can be properly handled in MATLAB and can thus be considered as "zero".

Next we consider the performance of the principal arrival

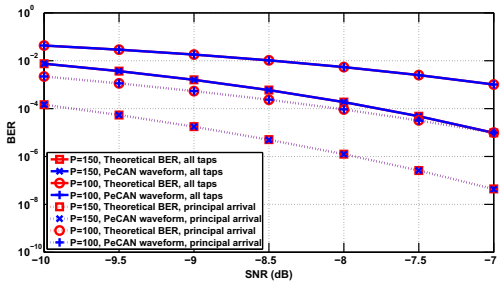


Fig. 13. The empirical BER curves corresponding to two different PeCAN waveforms with $P = 100$ and 150, the theoretical values are plotted alongside. Two reception schemes are considered: one uses EGC over all the $R = 50$ finger outputs, and the other uses the principal arrival only. Each point is averaged over 2×10^6 independent Monte-Carlo trials.

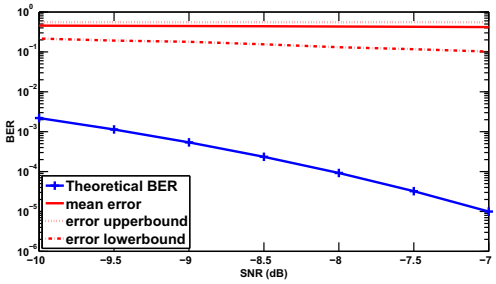


Fig. 14. BER performance achieved by generating the unimodular waveform chips in a random manner. The BER is 0.5 on average, implying desired LPI/LPD properties for the PeCAN waveform.

identification. The simulated CIR shown in Fig. 6 is also used here. We fix **SNR** $= -10$ dB, and the probing sequence is constructed by repeating 5 times the spreading waveform $\tilde{\mathbf{x}}$, with a chip length equal to $P + 49$. At the receiver side, after removing the 49 prefix chips from each $\tilde{\mathbf{x}}$, the norms of the sample mean along each RAKE finger are shown in Fig. 12 from 10 independent Monte-Carlo trials. In both scenarios, the principal arrival $h(2)$ is successfully identified.

The original information sequence contains 1000 binary symbols $\{b_i\}_{i=1}^{1000}$, and the corresponding encoded symbols $\{a_i\}_{i=0}^{1000}$ are constructed based on (16). The encoded symbols then phase-modulate $\tilde{\mathbf{x}}$ before being transmitted over a frequency-selective channel represented by $R = 50$ resolved taps, as shown in Fig. 6. Again, two reception schemes are considered. The first uses a conventional EGC approach as shown in Fig. 2, and the other is based on the principal arrival only, which is assumed to be correctly identified in the probing mode. The resulting empirical BER performance, along with the theoretical values, are shown in Fig. 13. Each point in the figure is averaged over 2×10^6 independent Monte-Carlo runs. We can see that due to the (almost) zero periodic correlation sidelobes of the PeCAN waveform, the empirical BER curves show perfect agreement with the theoretical values. Due to the same reason, the average performance of a Frank sequence with $P = 100$ also coincides with the theoretical BER value for $P = 100$, and therefore the corresponding curve is not included in the figure. Note that there is no Frank sequence corresponding to length $P = 150$, and Frank sequence can be guessed once kowning P.

Finally, we consider the covertness of the communication scheme. We assume that, except for precise knowledge of the spreading waveforms, an eavesdropper has the same information about the communication details as an intended receiver. The resulting BER performance is plotted in Fig. 14 obtained by conducting 1000 independent Monte-Carlo runs. The observations made from Fig. 10 are equally applicable in this case.

We now relax the assumptions by allowing the eavesdropper to use even the PeCAN algorithm for waveform generation. Consequently, the initial sequence (see Step 0 in Table II) becomes the only information that the eavesdropper does not have. Again we conduct 1000 independent Monte-Carlo runs by randomly generating initial sequences, and we perform the detection by using the resulting PeCAN spreading waveforms. Interestingly, the so-obtained BER results are almost identical with those given in Fig. 14. This fact suggests that the different PeCAN waveforms obtained by using different initial random sequences are almost uncorrelated to one another, which is a desired feature from a LPI/LPD point of view. Note that, we could have conducted a similar simulation for the WeCAN waveforms by initializing the algorithm with an independent waveform, and then running the WeCAN algorithm to generate eavesdropper's waveforms. However, for the WeCAN algorithm, such an experiment turns out to be too time consuming.

VI. Conclusions

We have considered covert UWA communication schemes that possess good LPI/LPD properties, which are achieved by maintaining communication at a low SNR level, and by synthesizing spreading waveforms that prevent detection in hostile environments. For the binary orthogonal modulation scheme, the WeCAN algorithm can be used to synthesize two spreading waveforms that have good auto- and cross-correlation properties over a certain lag range. For the binary DPSK scheme, by using a cyclic prefix, the waveform generated by the PeCAN algorithm possesses the desired ZCZ properties. To enhance the BER performance, the RAKE reception was modified to rely on the principal arrival only by identifying the dominant channel tap.

Acknowledgments

This work was supported in part by the Office of Naval Research (ONR) under Grant No. N00014-10-1-0054, the National Science Foundation (NSF) under Grant No. ECS-0621879, the Army Research Office (ARO) under Grant No. W911NF-07-1-0450, the Swedish Research Council (VR), and the European Research Council (ERC).

References

[1] J. Catipovic, "Performance limitations in underwater acoustic telemetry," *IEEE Journal of Oceanic Engineering*, vol. 15, pp. 205–216, July 1990.

[2] D. Kilfoyle and A. Baggeroer, "The state of the art in underwater acoustic telemetry," *IEEE Journal of Oceanic Engineering*, vol. 25, pp. 4–27, January 2000.

[3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY: Cambridge University Press, 2005.

[4] M.Palmese, G. Bertolotto, A. Pescetto, and A. Trucco, "Spread spectrum modulation for acoustic communication in shallow water channel," *OCEANS'07* Europe, pp. 1–4, June 2007.

[5] P. Hursky, M. B. Porter, and M. Siderius, "Point-to-point underwater acoustic communications using spread-spectrum passive phase conjugation," *Journal of the Acoustical Society of America*, vol. 120, pp. 247–256, July 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," *Journal of the Acoustical Society of America*, vol. 123, pp. 842–855, February 2008.

[7] M. Stojanovic and L. Freitag, "Hypothesis-feedback equalization for direct-sequence spread-spectrum underwater communications," *Proc. of MTS/IEEE OCEANS '00*, pp. 123–129, 2000.

[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," *Proc. of MTS/IEEE OCEANS '02*, pp. 594–603, 2002.

[9] J. A. Ritcey and K. R. Griep, "Coded shift keyed spread spectrum for ocean acoustic telemetry," *Proc. of MTS/IEEE OCEANS'95*, pp. 1386–1391, 1995.

[10] P. Price and P. Green, "A communication technique for multipath channels," *Proc. IEEE*, pp. 555–570, March 1958.

[11] J. G. Proakis, *Digital Communications*. New York, NY: McGraw-Hill Inc., Third edition, 1995.

[12] D. Brennan, "Linear diversity combining techniques," *Proc. IRE*, pp. 1075–1102, June 1959.

[13] J. Ling, T. Yardibi, X. Su, H. He, and J. Li, "Enhanced channel estimation and symbol detection for high speed MIMO underwater acoustic communications," *IEEE 13th DSP Workshop and 5th SPE Workshop,* Marco Island, FL, USA, January 2009.

[14] H. Ryser, *Combinatorial Mathematics*. John Wiley and Sons, 1963.

[15] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Infor. Theory*, pp. 154–156, 1968.

[16] M. B. Pursley, "Performance evaluation for phase-coded spread-spectrum multiple-access communication–Part I: System analysis," *IEEE Trans. Commun.*, vol. 25, pp. 795–799, August 1977.

[17] N. Suehiro, "A signal design without co-channel interference for approximately synchronized CDMA systems," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 837–841, Jun 1994.

[18] P. Fan, N. Suehiro, N. Kuroyanagi, and X. Deng, "Class of binary sequences with zero correlation zone," *Electronics Letters*, vol. 35, pp. 777–779, May 1999.

[19] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Transactions on Information Theory*, vol. 50, pp. 559–565, March 2004.

[20] R. Frank, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Infor. Theory,* IT-8, October 1962.

[21] R. L. Frank, "Polyphase codes with good nonperiodic correlation properties," *IEEE Transactions on Information Theory*, pp. 43–45, January 1963.

[22] C. Carbonelli, S. Vedantam, and U. Mitra, "Sparse channel estimation with zero tap detection," *2004 IEEE International Conference on Communications*, vol. 6, pp. 3173–3177, June 2004.

[23] M. Stojanovic, J. Catipovic, and J. Proakis, "Phase coherent digital communications for underwater acoustic channels," *IEEE Journal of Oceanic Engineering*, vol. 19, pp. 100–111, January 1994.

[24] W. Pratt, *Digital Signal Processing*. John Wiley and Sons, 1978.

[25] H. He, P. Stoica, and J. Li, "Designing unimodular sequence sets with good correlations - Including an application to MIMO radar," *IEEE Transactions on Signal Processing*, vol. 57, pp. 4391–4405, November 2009.

[26] M. Simon and M. Alouini, "A unified approach to the performance analysis of digital communication over generalized fading channels," *Proceedings of the IEEE*, vol. 86, pp. 1860–1877, September 1998.

[27] J. Wang and M. Moeneclaey, "DS-SSMA star network over indoor radio multipath Rician fading channels," *Military Communications Conference*, vol. 3, pp. 841–845, October 1992.

[28] P. Stoica, H. He, and J. Li, "On designing sequences with impulse-like periodic correlation," *IEEE Signal Processing Letters*, vol. 16, pp. 703–706, August 2009.

[29] P. Stoica, H. He, and J. Li, "New algorithms for designing unimodular sequences with good correlation properties," *IEEE Transactions on Signal Processing*, vol. 57, pp. 1415–1425, April 2009.