

Sea trial results of a chaotic direct-sequence spread spectrum underwater communication system

S. Azou¹ and G. Burel¹

¹Laboratoire d'Electronique et Systèmes de
Télécommunications (UMR CNRS 6165)
6, Avenue Le Gorgeu, BP 809
29285 BREST Cedex, France

e-mail : {Stephane.Azou, Gilles.Burel}@univ-brest.fr

L. Le Duff², C. Pistre²

²Groupe d'Etudes Sous-Marines de l'Atlantique
(GESMA), BP 42
29240 BREST Armées, France
e-mail : {leduff, pistre}@gesma.fr

Abstract- Recent theoretical results show that use of chaotic dynamics can significantly increase privacy of digital communication signals. The purpose of this paper is to report sea trial results of a chaotic spread spectrum system. Due to its ability to simultaneously sharing the same frequency band for various users (through Code Division Multiple Access) and its robustness against channel imperfections, it is the Direct-Sequence scheme that we use in our system. This is done by using a chaotic dynamic for the spreading code generator.

Two receiver structures are discussed ; one is similar to the matched filter structure usually encountered in standard DS-SS systems ; the other, more original, is based on a state-space formulation to recover various parameters of the incoming chaotic signal.

Through these first sea trials, we aim to prove the feasibility of a chaos-based transmission for a single user that operates without any covertness constraint. Other tests will be conducted soon to evaluate the performances for a Signal-to-Noise Ratio below 0 dB.

I. INTRODUCTION

In the last few years, a great research effort has been devoted towards the development of efficient chaos-based modulation techniques [1][2]. This motivation originates from theoretical results of Pecora and Carroll about the synchronizing capability of two identical chaotic systems that start from different initial conditions [3]. Due to its random-like deterministic behavior, chaos not only spreads the spectrum of the information signal but also acts as an encryption key. Hence, covertness of transmissions can be ensured and due to intricate dynamics of the received signals, it will be extremely difficult for the unauthorized user aware of the transmission to access the information. Many approaches exist to take advantage of these features, among others Direct-Sequence or Frequency-Hopped Spread Spectrum Systems, Chaotic Masking or Chaos Shift Keying. To date, most of the results available in the literature have been derived through numerical simulations and few practical investigations are detailed.

Due to their non periodic nature and their extreme sensitivity, it is not so easy to exploit chaotic signals for an information transmission.

As Direct-Sequence Code Division Multiple Access scheme becomes a popular choice in shallow water applications, such as Underwater Acoustic Network [4], we will focus on such a scheme. By this time, DS-SS transmitters make intensive use of pseudo-noise (PN) codes such as maximal-length, Gold or Kasami and are no longer robust against interception, as pointed out recently [5][6], because of the periodic nature of the codes and their well known construction process. Chaotic codes aim to correct this deficiency while maintaining comparable Bit-Error-Rate and data rate performances. A recent paper [7] attempted to show the feasibility of Chaotic DS-SS (CD3S) transmissions through numerical simulations. The present paper now puts into practice the receiver schemes that was introduced in the previous study.

The first receiver, operating at the symbol rate, employs a conventional matched filter structure [8], with acquisition and tracking through delay-lock loop for synchronization and a coherent correlator based demodulation (use of a phase-locked loop), together with power control. The second solution, more original, relies on a state space formulation of the demodulation process, thanks to the Unscented Kalman (UK) estimator developed by Julier *et al.* in the robotics field [9]. In presence of nonlinear dynamics, the UK estimator is known to be more accurate than the standard Extended Kalman Filter with the same computational complexity and an easier implementation. A dual estimation structure is proposed here to find the symbol and residual phase of the incoming baseband CD3S signal, together with a power control feedback. Such a receiver scheme is more suited for nonstationary channels, as it can operate at the chip-rate. In a blind approach, the despreading code has to be reconstructed from the noisy received signal ; this general approach based on chaotic synchronization was proposed in [7]. Although this method works on multipath channels for high SNRs (> 15 dB), it is not yet finalized and additional

investigations are needed to improve the denoising process for the code at lower SNRs. In this paper, knowledge of the despreading code will then be assumed and a code delay estimation will be used to track the received CD3S symbols. For the two receivers, the signal is first acquired through search and verification stages with an adaptive threshold to reduce false alarm probability [10].

An experiment was performed at the bay of Brest (France) in december 2002, to confirm the viability of the previous receivers. Several data blocks containing up to 200 bits was transmitted with a SNR about 7-8 dB. No error was noticed for the received symbols, using various spreading gains between 63 and 127. Other experiments will be conducted soon to evaluate the performances in a covert transmission scenario (low SNR).

The paper is organized as follows. In section II we present principles of a CD3S transmitter. Then, in third section, we present the acquisition process and the two receivers schemes. Experimental results will be illustrated and discussed in section IV and finally we will draw some concluding remarks.

II. CHAOTIC DIRECT-SEQUENCE SPREAD SPECTRUM (CD3S) SIGNALS

Figure 1 illustrates the principles of a CD3S transmitter. At the moment, data have been modulated through BPSK. A differential encoding may be performed to eliminate the phase ambiguity at the reception. The spreading operation is done by multiplication of the data symbols with the chaotic signal, evolving at a rate $F_c \gg F_d$, F_d being the data rate. The choice of the processing gain $W = F_c / F_d$ results from a tradeoff between the available bandwidth of the channel, the desired data rate and bit error rate together with the existence of any covertness constraint.

In order to facilitate the receiver synchronization, the information to transmit is structured in frames; In this way, chaotic markers, whose length is identical to the processing gain, are regularly inserted after the spreading operation. This means that the receiver can reconstruct the markers in an autonomous way. A basic solution is to repeat the same marker for each new frame and to store the marker signal at the receiver side.

Then, an upsampling process by zeros inserting is accomplished and a square-root raised cosine shaping filter is applied, with a rolloff factor α of 0.3, before a carrier modulation at central frequency F_0 . To avoid aliasing, the signal has to be sampled at a minimum value of $2F_0 + (1 + \alpha)F_c$.

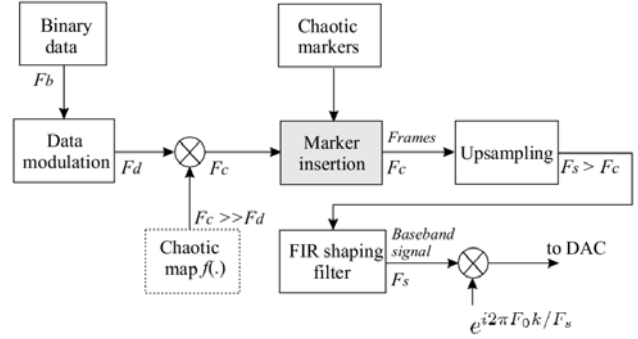


Figure 1 – Block diagram of a CD3S transmitter

As in [7], the logistic map is suggested as the spreading sequence generator, due to its favorable correlation properties. Hence, the wideband signal resulting from the spreading operation (before markers insertion) is given by

$$x_k = d_k(1 - 2x_{k-1}^2) \quad (1)$$

where x_k denotes the *state* of the dynamical system and where the *parameter* d_k is the data symbol (e.g. ± 1 for a BPSK encoding).

III. RECEIVER STRUCTURES FOR CD3S SIGNALS

The receivers that we describe in this paper both have to generate a perfect replica of the original spreading code, in a synchronous manner. This will require two steps: The role of the code acquisition will be to achieve a coarse time alignment between the received chaotic code and the locally generated code, whereas the tracking loop will have to maintain the receiver code offset below a fraction of chip duration and to track carrier phase (the Doppler will not be considered here) before any demodulation.

Although a chaotic generator exhibits an extreme sensitivity to its initial conditions and a stochastic-like behavior, the construction of a perfect replica of the original spreading code at the receiver side is not a problem, thanks to the deterministic nature of chaotic systems and the discrete-time implementation we chose.

A. Code Acquisition

As mentioned before, the objective of initial code acquisition is to achieve a coarse synchronization between the receiver despreading code and the transmitted signal. A popular approach to solve this problem is the serial search [8], which relies on a correlation between the received signal and the receiver code; the tracking is then started when a predefined threshold is crossed or for the maximum correlation value. In order to reduce the false alarm

probability, it is desirable to use search techniques in conjunction with a verification step (*double-dwell* system). To improve the performances, it is even possible to run the search and verification simultaneously, as it is proposed in [10]. Such an approach has been implemented in our CD3S system; It is summarized in the rest of this subsection.

A number M of preamble symbols will be devoted to acquisition. The same chaotic code (chaotic marker) can be chosen for each preamble symbols ; if a low probability of interception is needed, the marker will change for each new frame. If W denotes the spreading gain, that is the length of the chaotic code $c[k]$ for one symbol, and $r[k]$ is the received baseband signal, we compute the matched-filter output in the search block :

$$g[k] = \sum_{l=0}^{\Delta W-1} r[k-l]c[W-l] \quad (2)$$

where Δ is the number of samples per chip.

Then, we proceed to the comparison

$$|g[k]|^2 \geq \eta[k] \quad (3)$$

where $\eta[k]$ denotes an adaptive threshold, whose value starts from η_0 at $k=0$ or at time instants where a failure is declared by the verification process. Then, the threshold evolves in time as

$$\eta[k] = \max\{\eta_0, \eta[k-1], |g[k-1]|^2\} \quad (4)$$

A verification will be started as soon as

$$|g[k]|^2 > \eta[k] \quad (5)$$

and then search and verification processes operates simultaneously. The task of the verification is to verify that correlation peaks occur at time instants

$$k_{m+1} = k_1 + m\Delta W, \quad m = 1, 2, \dots, M \quad (6)$$

where k_1 denotes the instant where the verification have been started.

The verification will be considered successful, and then the tracking initiated, if

$$(1/M) \sum_{m=1}^M |g(k_m)|^2 > \rho \eta[k_1 + 1], \quad \rho = 0.8 \quad (7)$$

otherwise the acquisition continues in the search mode only, until initial threshold η_0 is crossed again. During the verification process, if a crossing is observed at a time instant $k \neq k_m$, then the verification is stopped to save on computational time.

The number M of preamble symbols required to proceed the acquisition have to be carefully chosen in practice. A greater M is needed as the SNR decreases in order to keep false alarm probability as low as possible.

B. Conventional Matched-filter approach

Figure 2 shows the block diagram of a typical DS-SS receiver structure (single user), which consists of a Delay Lock Loop (DLL) for code tracking and a Costas Loop for carrier tracking [8]. The acquired signal is first downconverted to the baseband using a locally generated In-phase and Quadrature-phase of the carrier. Then, after a low-pass filtering (I & Q arms), the signal is correlated with the prompt, early and late versions of the locally generated code (figure 2). The Early and Late I/Q-components are used to detect a code phase error; the code discriminator output is then used to control the code generator. The carrier discriminator, working at the symbol-rate, relies on the I/Q Prompt correlations values, the purpose being to keep the angle between the I-component and Q-component as small as possible. After the phase error has been filtered, it is fed back to the local oscillator of the receiver. Finally, transmitted symbols are recovered as the sign of the In-phase prompt correlation values (for a Binary Phase Shift Keying modulation). Such DS-SS receivers have been studied for application to the underwater acoustic channel for many years now; experimental results are discussed in recent papers such as [11][12]. As reported in [11], the PLL performance is dependent upon the signal amplitude. Hence, a power control has to be implemented to reach good phase tracking performances.

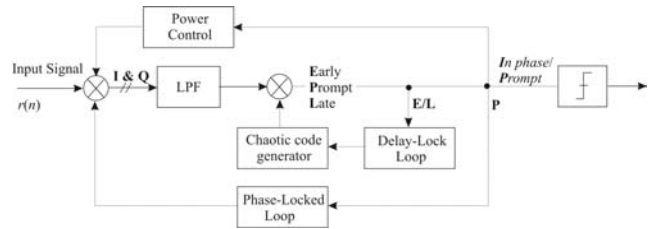


Figure 2 – Conventional Matched-Filter CD3S Receiver

We made use of the structure illustrated by figure 2 to receive chaotic DS-SS signals. The only difference of this receiver with respect to PN codes based DS-SS receivers is the way the code generator is controlled. This generator is a discrete-time chaotic system (*logistic* system); After the acquisition process, the receiver code starts from the same value as that used by the transmitter, hence ensuring a perfect replica of the original spreading code.

To implement the power control, we follow the method proposed by Freitag *et al.* in [11] : the input signal is normalized according to

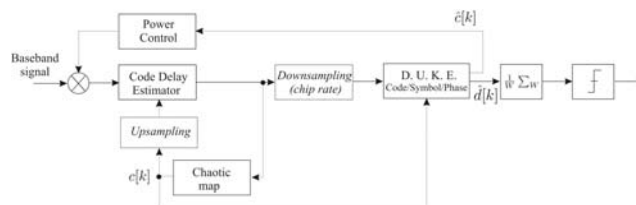
$$r'[n] = r[n] / \sqrt{P[n]} \quad (8)$$

where the power P is estimated at the symbol-rate as the following recursion :

C. *Dual Unscented Kalman Estimation (DUKE) approach*

recursion, these sample points are propagated through the true nonlinear functions of the model. Hence, posterior mean and covariance are captured accurately to the second order (Taylor series expansion), whatever the nonlinearity is. To the knowledge of the authors, such a tool has not been yet employed for synchronization of chaotic signals; also, it is the purpose of this paper to verify the reliability of the UK estimator on in-water data.

$$z[k] = d[k].c[k].e^{j\phi[k]} + n[k] \quad (10)$$



The block diagram of the proposed estimation scheme is shown at figure 4. Three UK filters operate simultaneously: two of these filters compute the symbol $\hat{d}[k]$ and the phase $\hat{\phi}[k]$ thanks to the exact spreading code $c[k]$, the noisy observations $z[k]$ and past outputs $\hat{\phi}[k-1] / \hat{d}[k-1]$ (for the UK symbol estimator/UK phase estimator respectively), while the third filter aims to reconstruct the original code owing to the estimated symbol and phase. This last filter is used for power control purpose only, by comparing the statistics (e.g. standard deviation) of the incoming code with respect to that of the estimated code $\hat{c}[k]$.

enable a better tracking capability. The reason is that many chips are required to derive the statistics of $\hat{c}[k]$.

Each UK estimator relies on a dynamic model that depends upon the underlying state that is searched. The models we used was as follows, for the code, symbol and phase respectively :

$$\begin{cases} c[k] = 1 - 2c^2[k-1] + v^c[k] \\ d[k] = d[k-1] + v^d[k] \\ \phi[k] = \phi[k-1] + v^\phi[k] \end{cases} \quad (11)$$

where $v^c[k]$, $v^d[k]$ and $v^\phi[k]$ denote zero mean WGN processes with variance Q^c , Q^d and Q^ϕ respectively ; these uncertainties about various dynamics act upon the adaptation rate of the receiver. The lower the variances will be, the less the receiver will be capable of tracking rapid varying channels. Also, it should be noted that a more sophisticated model for the phase can significantly increase the performances.

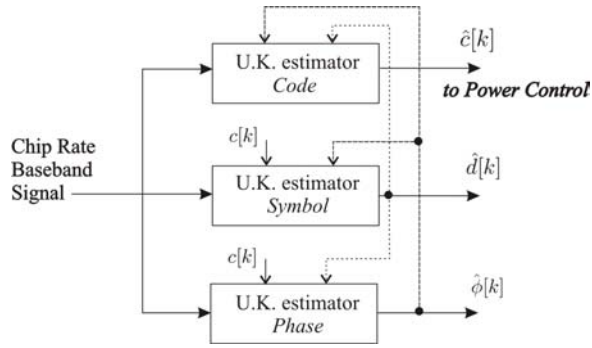


Figure 4 – Structure of the Dual Unscented Kalman Estimator

An interesting characteristic of this DUKE based receiver is its ability to cope with multipath propagation although the state space model implemented does not explicitly take into account the delayed versions of the transmitted signal. The reason is that in the observation model, the noise $n[k]$ reflects the uncertainty due to all channel imperfections : noise, interference, multipath... In practice, variance R of this noise has to be carefully tuned to get good performances; This can be achieved thanks to preamble symbols.

IV. EXPERIMENTAL RESULTS

A. Description of the Experiment

The two previously described CD3S receivers was tested on in-water data at the bay of Brest (France) in last december. This first experiment is intended to verify that chaos based transmissions can work in shallow water for moderate SNRs.

We report the following trial here : The transmission range was about 1 km, with the transmitter and receiver at a depth of 5 m and 10 m respectively, for a water 20 m deep. A frame of 200 bits, BPSK modulated, has been transmitted with a carrier frequency F_0 equal to 4410 Hz and a chip frequency F_c of 3150 Hz. The processing gain was 63 and no channel encoding is applied.

One hundred maximal-length sequences of length 127 has been sent prior to the frame transmission in order to measure the channel impulse response. The whole set of estimated impulse responses is drawn at figure 5 and figure 6 illustrates one impulse response.

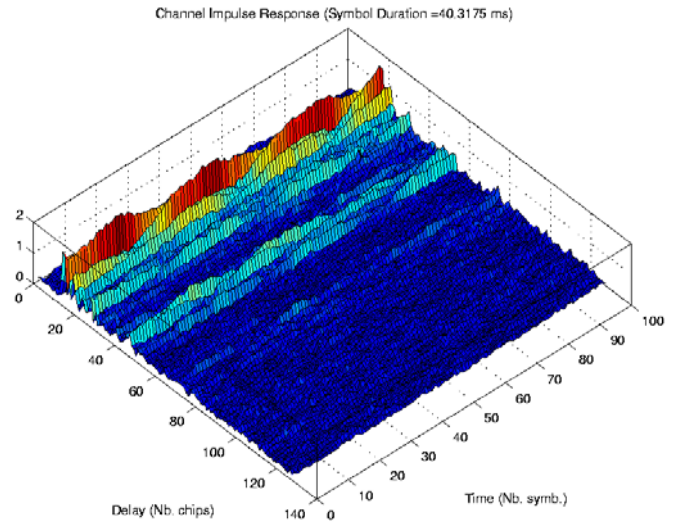


Figure 5 – Fluctuations of the channel impulse response (Bay of Brest, France, Dec. 02 2002)

A time spread less than 20 ms (value of the BPSK symbols period) is noticed on these figures. So the multipath propagation leads to negligible ISI.

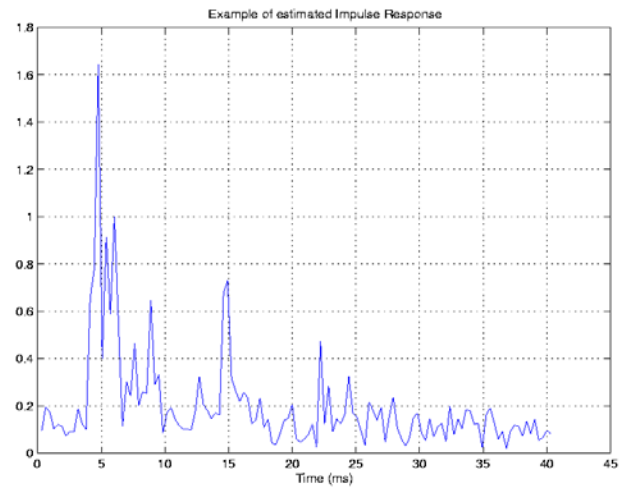


Figure 6 – An example of measured channel impulse response

The SNR value at the receiver input (in the Nyquist band) was about 7.5 dB. The Power Spectral Density (PSD) of the received signal, sampled at 22050 Hz, is illustrated at figure 7.

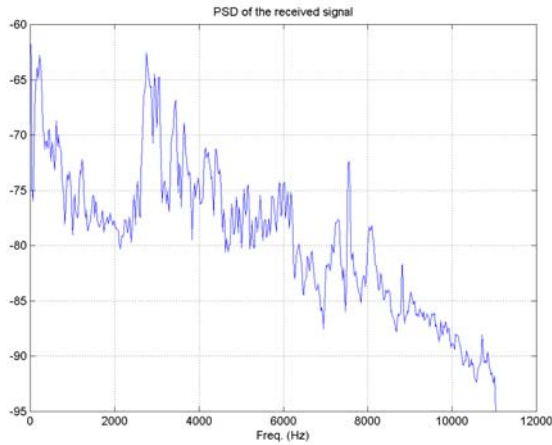


Figure 7 – Power Spectral Density of the received signal

B. Performance Comparison of two receivers

- Conventional Matched Filter receiver –

The results for the matched filter CD3S receiver are reported below. Due to the values of the processing gain and the data rate, this receiver does not significantly suffer from ISI and no additional RAKE processing is required to combat multipath propagation.

The DLL performance is illustrated by figure 8. As long as the E/L discriminator output stays in the interval $[0.8, 1.2]$, the receiver code was considered on-time. Hence, we can observe that the code delay is correctly tracked for the whole frame.

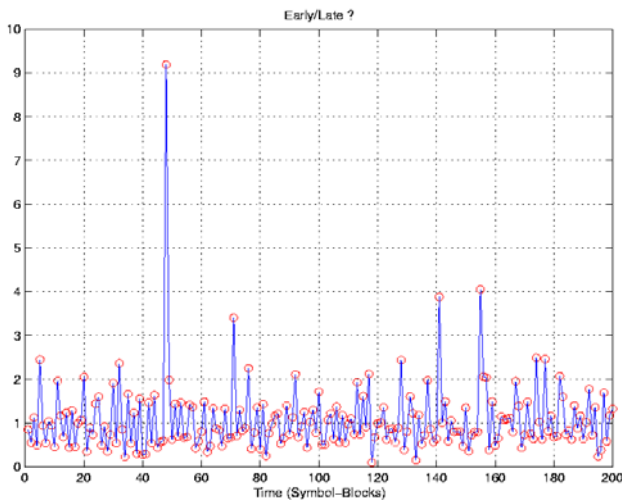


Figure 8 - Evolution of the Early/Late discriminator

Figure 9 shows the estimated phase. As a limited spreading gain and a sufficient value for the chip rate has been used in this test, a rather good phase tracking is noticed. Additional experiments with higher processing gains on the same channel did not yield better results. The dependance of phase tracking upon the symbol rate is a drawback of this receiver ; It will not particularly suited for more difficult channels.

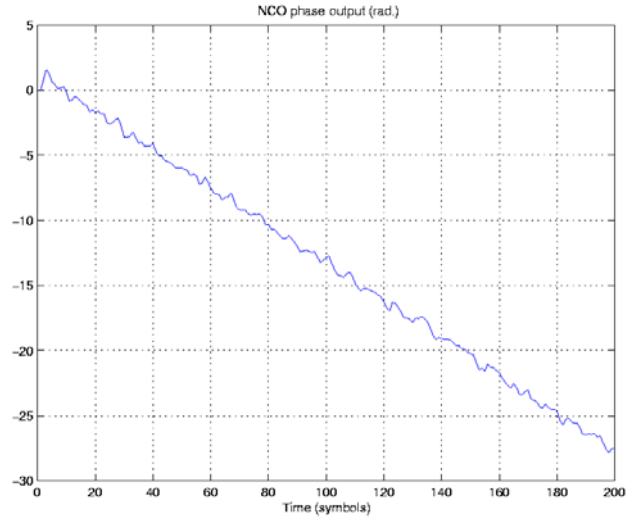


Figure 9 - Symbol rate estimated phase (Costas loop)

The gain control for a weighting factor α of 0.5 is illustrated by figure 10. This choice enables the receiver to correctly follow changes of signal power. However, as the estimation is performed at symbol rate only, more rapid changes would be difficult to track.

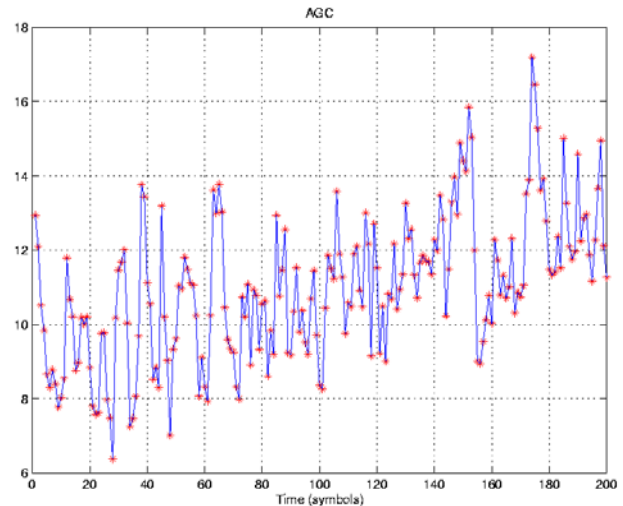


Figure 10 - Power control in the conventional CD3S receiver

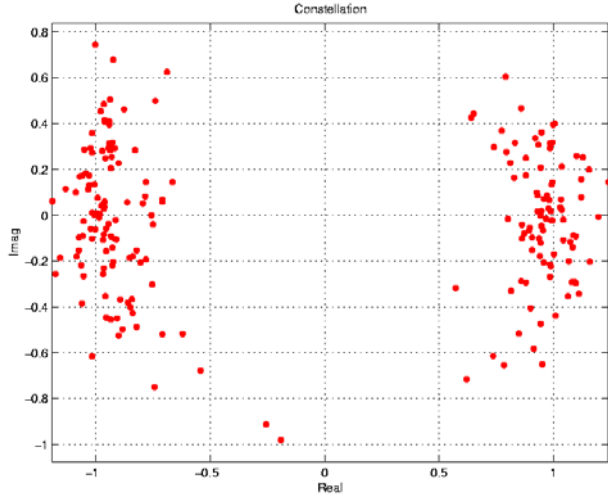


Figure 11 – Symbol scatter plot for the conventional CD3S receiver

Finally, figure 11 gives the symbol scatter plot for the transmitted frame. No error was noticed here, but we can observe the degradation due to low rate phase tracking.

- DUKE receiver -

Now we illustrate the behavior of the DUKE-based CD3S receiver. To initiate the demodulation process, various estimators employed in this receiver has first to be configured ; that is noise variances $\{Q^c, Q^d, Q^\phi, R\}$ together with initial points $\{\hat{d}[0], \hat{\phi}[0]\}$ in the state space must be chosen.

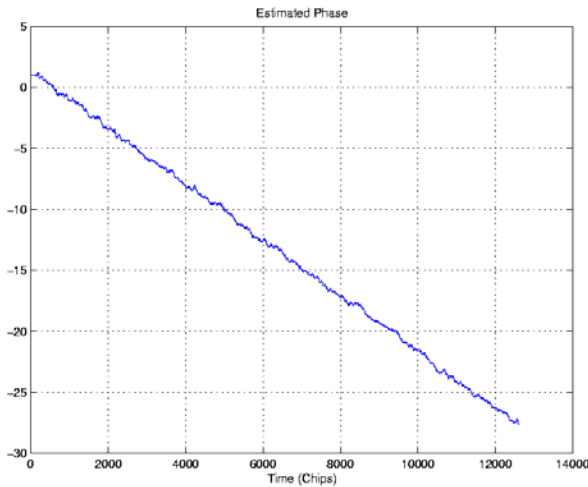


Figure 12 - Chip-rate phase tracking in the DUKE receiver

The following choice was made here : $Q^c = 10^{-1}$, $Q^d = 10^{-2}$, $Q^\phi = 10^{-3}$, $R=0.8$, $\hat{d}[0]=1$ (chosen

randomly) and $\hat{\phi}[0]=1$. The initial condition for the phase corresponds to the mean value of the correlation peaks obtained during the acquisition process.

Phase tracking is illustrated by figure 12 ; it is similar in appearance to that obtained through Costas lock loop for the conventional receiver, but the chip rate processing enables a more precise tracking.

Figure 13 illustrates the power control ; a symbol rate processing was carried out for this trial. It should be noted however that a higher tracking rate becomes possible for a larger processing gain. From figure 13 and a comparison with results obtained with first receiver, one can notice that the proposed gain control method works rather well in this case.

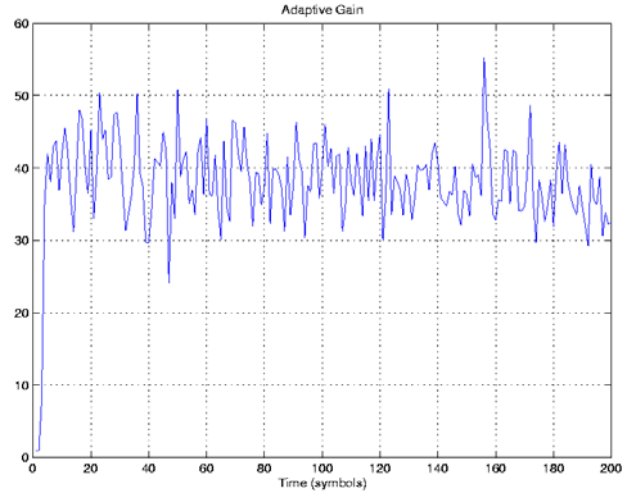


Figure 13 - Symbol-rate power control for the DUKE receiver

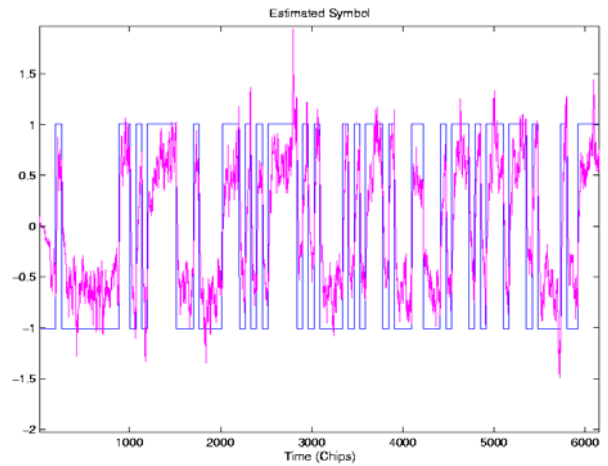


Figure 14 - Chip-rate symbol estimation for the DUKE receiver

Finally, figure 14 shows few transmitted BPSK symbols and estimated symbols at chip-rate using the DUKE receiver. It is seen that the demodulator is able to track perfectly symbol changes. No error was noticed for the

whole frame. Due to process and observation noises present in DUKE models and the symbol estimation at chip-rate, the receiver implicitly combats multipath fading.

V. CONCLUSIONS & FUTURE WORK

Many recent papers claimed that use of chaotic codes can significantly decrease probabilities of interception and detection of digital communication signals. At the moment, few practical investigations permitted to verify this benefit. The problem of receiver design in a Chaotic Direct-Sequence Spread Spectrum System (CD3S) has been considered in this paper. The aim is to report sea trial results of such a system in standard shallow water propagation conditions (single user, moderate SNR, low doppler...). This first step will be followed by other tests on in water data with more constraints such as covertness and/or multiple access.

Two receiver schemes has been described: the first receiver follows the conventional receiver structure frequently encountered in DS-SS systems based on PN periodic codes. There is just a change at the spreading code generator level (use of a chaotic dynamic instead of linear feedback shift registers). Good performances was obtained for this receiver, although it is not capable of tracking rapid varying channels. Its main advantage is its computational/implementation simplicity. An additionnal RAKE processing can be performed to increase the performances. The second receiver is more innovative; it is based on a state-space formulation of the symbol/phase estimation in baseband (no carrier PLL) thanks to Unscented Kalman filters. A dual estimation approach has been proposed to solve the demodulation process (DUKE structure). An additionnal UK filter is used for power control purpose. From sea trial results, one can conclude that this approach is viable for difficult channels, as the symbol and phase are tracked at chip-rate. Although this approach requires more complexity, the implementation remains simple.

Additionnal investigations is now necessary to succeed in using chaos for covertness transmission and/or in multiple access systems. The code delay synchronization will be examined in a different way of Early/Late DLL, together with effect of Doppler on the DUKE receiver.

REFERENCES

- [1] M. Hasler « Synchronization of chaotic systems and transmission of information », *Int. J. Bifurcation and Chaos*, Vol. 8, No 4, pp 647-659, 1998.
- [2] G. Kolumban, M. P. Kennedy, L. O. Chua, « The role of synchronization in digital communication using chaos – Part II : Chaotic modulation and chaotic synchronization », *IEEE Trans. Circuits Syst.*, Vol. 45, No 11, 1998.
- [3] L. Pecora, T. Carroll, « Synchronization in chaotic systems », *Phys. Rev. Lett.*, Vol. 64, pp. 821-823, 1990.

- [4] E. M. Sozer, M. Stojanovic, J. G. Proakis, « Underwater Acoustic Networks », *IEEE J. Oceanic Eng.*, Vol. 25, No 1, 2000.
- [5] G. Burel, C. Boudier, « Blind estimation of the pseudo-random sequence of a direct-sequence spread spectrum signal », *IEEE 21st Century Military Communications Conference* (IEEE-MILCOM'2000), October 22-25, 2000, Los Angeles, USA.
- [6] M. K. Tsatsanis, G. B. Proakis, « Blind estimation of direct sequence spread spectrum signals in multipath », *IEEE Trans. Signal Processing*, Vol. 45, No. 5, pp. 1241-1252, 1997.
- [7] S. Azou, C. Pistre, G. Burel, "A chaotic direct sequence spread-spectrum system for underwater communication", *IEEE-Oceans'02*, Biloxi, Mississippi, Oct. 2002.
- [8] J. G. Proakis, *Digital communications*, 3rd ed., Mac-Graw-Hill Int. Ed., 1995.
- [9] S. Julier, J. Uhlmann, H. F. Durrant-Whyte, « A new method for the nonlinear transformation of means and covariances in filters and estimators », *IEEE Trans. Automat. Contr.*, Vol. 45, No. 3, pp. 477-482, 2000.
- [10] H. S. Chang, Y. W. Park, Y. H. Lee, « DS-SS Code Acquisition Based on Simultaneous Search and Verification », *IEEE Trans. On Communications*, Vol. 48, No. 6, June 2000.
- [11] L. Freitag, M. Stojanovic, S. Singh, M. Johnson, « Analysis of Channel Effects on Direct-Sequence and Frequency-Hopped Spread-Spectrum Acoustic Communication », *IEEE J. Oceanic Eng.*, Vol. 26, No. 4, Oct. 2001.
- [12] E. M. Sozer *et al.*, "Direct Sequence Spread Spectrum Based Modem for Underwater Acoustic Communication and Channel Measurement", *Proc. IEEE OCEANS Conf.*, Seattle, USA, Sept. 1999.
- [13] M. Stojanovic, L. Freitag, "Hypothesis-Feedback Equalization for Direct-Sequence Spread-Spectrum Underwater Communications", *Proc. IEEE OCEANS Conf.*, 2000.
- [14] H. Leung, J. Lam, "Design of demodulator for the chaotic modulation communication", *IEEE Trans. Circuits Syst. I*, Vol. 44, 1997.
- [15] Y. Bar-Shalom, X.-R. Li, « Estimation and Tracking – Principles, Techniques and Software », Artech House, 1993.
- [16] E. A. Wan and R. van der Merwe, "Kalman Filtering and Neural Networks", chap. 7 : The Unscented Kalman Filter, *Wiley Publishing*, Eds. S. Haykin, 2001.