

A Chaotic Direct-Sequence Spread-Spectrum System for Underwater Communication

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

C. Pistre²

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

Abstract—The recent advances in acoustic modem technology have enabled the development of Underwater Acoustic Networks (UAN). Application interests include oceanographic information gathering, environmental monitoring or coastal defense. Due to its ability of simultaneously sharing the same frequency band for various users and the poor propagation conditions usually encountered in shallow water environment, the Code Division Multiple Access (CDMA) is a promising scheme for UAN.

Recent results show that a standard CDMA direct-sequence spread spectrum approach is not sufficient to ensure Low Probabilities of Detection (LPD) and/or Interception (LPI), that is an unauthorized observer may notice that a communication signal is present. For many applications, this drawback is not acceptable.

In this paper, the application of chaos to transmission of information is under investigation to achieve an LPI/LPD objective in an UAN context. Performance results of two receivers are shown for a single user through a realistic simulation scenario. An experiment at sea will be conducted by GESMA soon to confirm these first results.

I. INTRODUCTION

For many applications the data transmission has to be carried out at low Signal-to-Noise Ratio (SNR). For UAN [1], the minimization of the output power at each node is desirable to reduce the battery consumption (immersed autonomous transmitter). In a military context, the low SNR constraint comes from a discretion purpose (preventing the enemy to detect the transmission). Due to severe propagation conditions usually encountered in shallow water (limited bandwidth, time varying multipath, noise), resulting in Inter Symbol Interference (ISI) and Doppler effect, Spread Spectrum (SS) techniques are often used at low SNR. Two major spreading techniques are available [2] : Frequency Hopped (FH) or Direct-Sequence (DS) spreading. The two approaches allow multiple users to operate simultaneously in time over the same frequency band, by using pseudo-noise (PN) codes (Code Division Multiple Access). A FH-SS system changes the frequency of the carrier signal continuously, in a pattern obtained from a PN code. This scheme is able to combat great Doppler spread but is less efficient than DS-SS for low SNR.

In a standard DS-SS system, the data to be transmitted are multiplied by a PN sequence, generally produced by linear feedback shift registers (e.g. maximal length sequences, Gold sequences...). The resulting wideband signal modulates the carrier. The transmitted wave has then to be demodulated by the receiver : it is realized by correlating the received signal with a copy of the direct-sequence (periodic) used by the transmitter, in a synchronous manner.

As demonstrated in recent papers [3][4], a transmission by DS-SS is not secured, even if the SNR is below 0 dB, due to the periodic nature of the spreading code. Hence, a receiver unaware of the transmission on the channel will be able to determine that any signal is being sent (Interception). Then, the demodulation becomes possible if the construction process of the spreading code is well known (Detection). These remarks make the principal motivation for the study presented in this paper.

There has been significant interest in recent years in exploiting chaos in communication systems [5][6]. Due to its random-like behavior and its wideband characteristics, a chaotic dynamical system can be very helpful for discretion purposes. Chaos not only spreads the spectrum of the information signal but also acts as an encryption key. Thus, without knowledge of the type of nonlinearity on which the transmission is based (the chaotic dynamic), it is extremely difficult for the unauthorized user aware of the transmission to access the information. Furthermore, such signals are potentially robust against channel imperfections such as multipath propagation or jamming. As a result of their sensitive dependence on their initial conditions, chaotic systems are able to produce large sets of uncorrelated signals. This extreme sensitivity can be demonstrated by giving two very close initial states to a chaotic map ; After a few iterations, the two resulting sequences will look completely decorrelated. This can be observed even for very simple (one dimensional discrete-time) chaotic dynamical system. The large signal set generated is an attractive feature in a multiple access transmission context.

In this paper, it is proposed to replace the periodic PN-code used in standard DS-SS communication systems by a chaotic code and we propose a new and robust

demodulator based on dual Unscented Kalman Filters. The idea of a chaos based DS-SS system is not new [7][8]; however few results are available concerning experimental results or realistic scenarios at the moment.

A fundamental difference for a Chaotic DS-SS (CD3S) system in comparison with a classical DS-SS system is that each data symbol is multiplied by a different spreading code each time. Consequently, demodulation of CD3S signals will be more tricky than in the standard case (periodic sequence), especially if the SNR is low.

In this paper, the feasibility of a CD3S system is examined in shallow water environment, for a single user. Two new schemes of demodulation are proposed for the receiver, namely the Exact Spreading Sequence (ESS) demodulation and the Dual Unscented Kalman Filtering (UKF) demodulation. The first solution relies upon regeneration of an exact replica of the chaotic spreading code, applied at the transmitter side. The second solution, more general, is based on a dual estimation of the spreading code and the data symbols through the Unscented Kalman filtering approach proposed by Julier *et al.* [9] in the different context of nonlinear control.

The paper is organized as follows. Section II is devoted to general results about the logistic map, used here as the spreading code generator. The CD3S transmitter is explained in section III. Then, the design of CD3S receivers is mentioned in section IV. System performances are illustrated in section V. Finally, section VI summarizes the conclusions and gives an outline of future research directions in this area.

II. CHAOTIC SPREADING SEQUENCES AND THE LOGISTIC MAP

A chaotic dynamical system is one that is deterministic but appears not to be so, as a consequence to its extreme sensitivity to initial conditions. A chaotic system can be described by state space equations :

$$x_{k+1} = f(x_k) \quad , \quad k = 0,1,2,\dots$$

where $x_k \in \mathfrak{R}^n$ is called the state, and $f(\cdot)$ maps the state x_k to the next state x_{k+1} .

Given the same initial conditions, two chaotic systems with the same state parameters will result in exactly the same sequence of output samples. On the other hand, any minor difference between initial states will lead to an eventual divergence of the output streams from the two systems. Asymptotically, the output streams will be completely decorrelated.

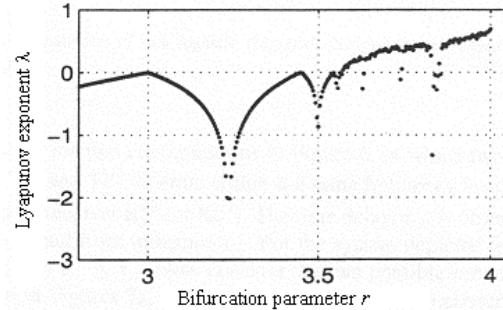


Fig. 1. Bifurcation diagram for the logistic map.

A chaotic map does not have to be very complicated. However, in a context of CDMA application, the map has to possess a δ -like autocorrelation function, for a proper signal detection, and a low cross-correlation function for proper signal separation. Moreover, a zero-mean symmetric sequence is desirable.

As in [7], the logistic map is chosen here as the spreading sequence generator :

$$x_{k+1} = rx_k(1 - x_k)$$

This system exhibits a great variety of dynamics, depending upon the value of the bifurcation parameter $r \in [1,4]$. To obtain a chaotic dynamic the bifurcation parameter must be chosen so that the Lyapunov exponent λ is strictly positive. Figure 1 shows the evolution of λ as a function of r . It is seen that for almost all $r \in [3.6,4]$ the system is chaotic. For the case $r=4$ the map generates intricate trajectories and some favorable analytical properties are available, as mentioned in [8]. In what follows we will refer to this particular case. In order to have symmetric zero-mean trajectories, the state equation is modified as

$$x_{k+1} = 1 - 2x_k^2$$

Figure 2 illustrates typical trajectories for the system. A low cross-correlation is clearly seen, although the initial states for the two sequences differ only by 10^{-5} .

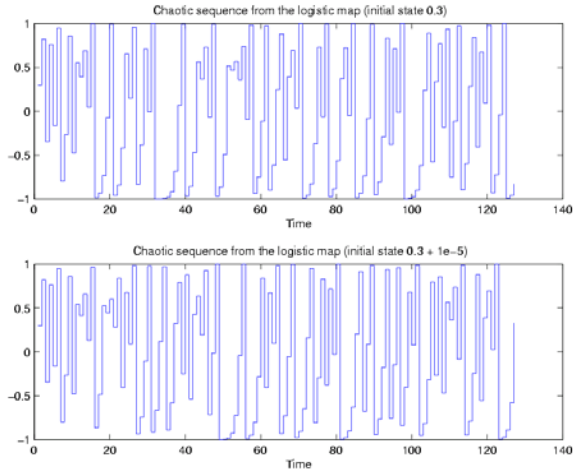


Fig. 2. Two spreading sequences generated by the logistic map (127 chips) ; The initial states differ only by 10^{-5} .

The overall performance of a DS-SS system is dependent upon the correlation properties of the spreading sequence. Asymptotically, the logistic map is able to produce an infinite set of orthogonal codes by choosing different initial states and/or changing the bifurcation parameter. That is, the autocorrelation tends towards a δ -function and the crosscorrelation is equal to zero. Nevertheless, in practice, it is not evident that we can take advantage of these properties : For finite length sequences, partial correlation appears and secondary peaks are noticed for the autocorrelation. As a consequence, the processing gain of a CD3S communication system will have to be designed with caution. As illustrated by figure 3, for a 63-length logistic sequence, the autocorrelation moves away from the perfect δ -function, but is still acceptable. Shorter sequences must be avoided. The correlation fluctuations is not the only reason for performance degradation ; The problem of bit energy fluctuations has also to be noticed. Figure 4 illustrates these fluctuations as a function of processing gain. It is clearly seen that very short sequences (length less than 63) are not suitable for a CDMA application.

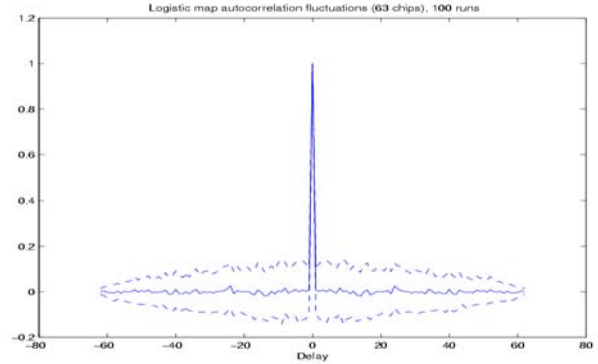


Fig. 3. Logistic map autocorrelation fluctuations averaged over 100 runs, for a sequence of length 63 ($m \pm \sigma$)

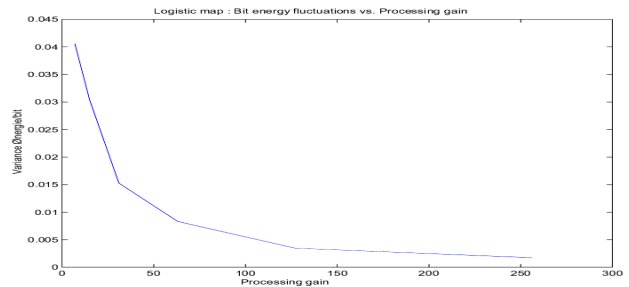


Fig. 4. Bit energy fluctuations vs. Processing gain for the logistic map

Finally, notice that no restriction exists for a chaotic sequence concerning its length. This is not the case for standard PN (maximal-length or Gold) codes which must have a length equal to $2^n - 1$.

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

At the transmitter, the information is structured in frames, as shown by figure 5. After spreading the data signal through use of the chaotic map (logistic), chaotic markers, whose length is identical to the processing gain (number of chips of the spreading sequence per data symbol), are regularly inserted in order to synchronize the receiver. This means that the receiver can reconstruct the markers in an autonomous way.

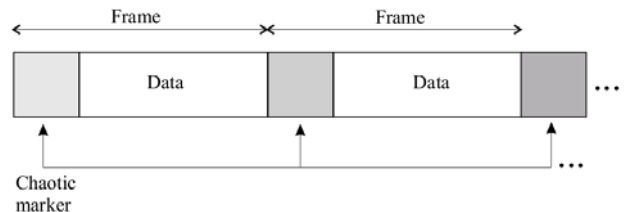


Fig. 5. Frame structure used at the CD3S transmitter.

A basic solution is to repeat the same chaotic marker for each new frame and to store the marker signal at the

receiver side. A more sophisticated approach is to use a secondary chaotic map (with the same or similar dynamic), whose initial condition is changed according to a reference clock. Then the receiver has to reconstruct the marker signals referring to a synchronized clock (the relative clock drift must be negligible).

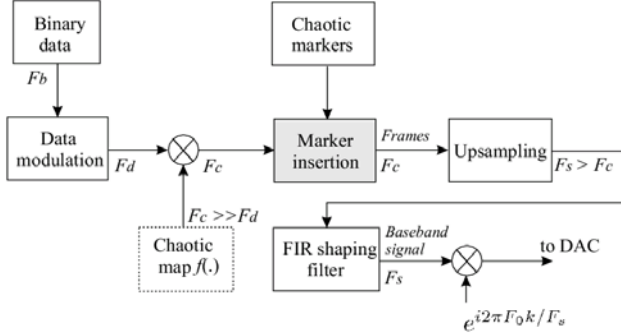


Fig. 6. Chaotic DS-SS (CD3S) modulator.

Figure 6 illustrates the principles of the CD3S modulator. 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 processing gain $W = F_c / F_d$ must be an integer. Its value depends on the bandwidth available for the propagation channel, notably. The chaotic markers, also sampled at a rate F_c , are inserted before an upsampling process by zeros inserting. Then a square-root raised cosine shaping filter is applied, with a rolloff factor α of 0.5, before a carrier modulation at central frequency F_0 . To avoid aliasing, the signal has to be sampled at a minimum value of $2F_0 + (1 + \alpha)F_c$.

IV. DEMODULATOR STRUCTURES FOR CD3S SIGNALS

In this section, we focus on the demodulator design for CD3S signals. Two schemes are investigated ; The first one, named Exact Spreading Sequence (ESS), relies on the knowledge of the original spreading sequence, that is the one that has been used by the transmitter to spread the spectrum of the information signal. The second scheme, called Dual Unscented Kalman Filtering, is based on a simultaneous estimation of the state of the noisy received chaotic signal and the data symbol. Due to strong nonlinearity of chaotic signals, such an estimation must be carried out with a robust state space adaptive filter. This problem has been solved here owing to the Unscented transformation recently developed by Julier et al. [9]. This method allows the calculation of the statistics of a

random variable which undergoes a non-linear transformation in an efficient manner.

A. Receiver preprocessing

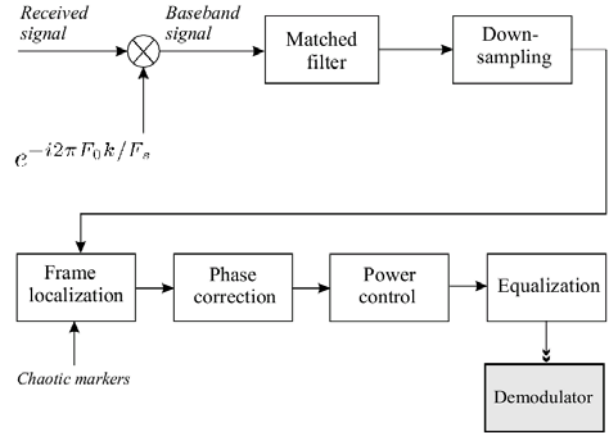


Fig. 7. CD3S receiver preprocessing

Figure 7 shows the preprocessing blocks at the receiver. The received signal, sampled at frequency F_s has first to be brought back to baseband and lowpass filtered (square root raised cosine filter) before any processing. Then, the frames are synchronized, by correlations, thanks to the set of chaotic markers that has been inserted by the transmitter. The carrier phase fluctuations, caused by clock drift and/or Doppler effect, must then be compensated. A basic solution is to exploit the markers to estimate the phase difference over current frame. A correction via linear interpolation is then possible. At this stage, the information is embodied in the real part of the signal only, for a binary data modulation (BPSK, DPSK). Before demodulation, it remains to adjust the signal power. An additional channel equalization is then performed. This problem, essential for a practical issue, is not addressed in the present paper.

B. Exact Spreading Sequence (ESS) Demodulator

This demodulator is outlined by figure 8. The ability of the receiver to reconstruct exactly, in a synchronous manner, the original spreading sequence, is of central importance in this approach. Assuming this objective is realizable, the symbol decision is just given as the sign of the output of a correlator, operating over symbol duration. A first solution, the simplest, could be to utilize the same initial state for the chaotic spreading sequence for each new transmission. Knowing this starting point and the chaotic dynamic, the receiver will be able to reproduce the whole sequence. Another way could be to reinitialize the sequence for each new frame, by choosing initial values in

a finite set, known by the receiver. By using approximately synchronized clocks (small relative drift), and the way the initial value is changed during the transmission, the receiver can retrieve the whole sequence.

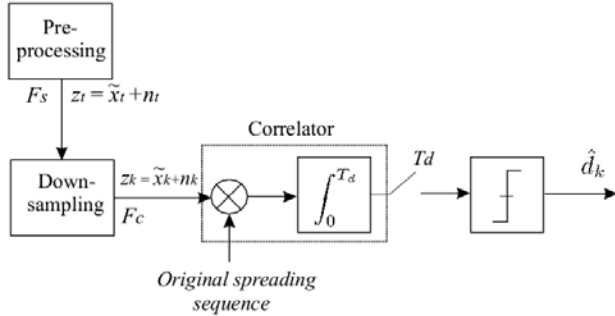


Fig.8. CD3S Exact Spreading Sequence demodulator.

C. Dual Unscented Kalman Filtering (UKF) Demodulator

Dual Unscented Kalman Filtering, shown at figure 9, is a more general approach to solve the problem of CD3S signals demodulation. Here, the exact knowledge of the chaotic spreading code is not available at the receiver side. Hence, it is necessary to estimate the sequence from the received noisy signals. As the underwater acoustic channel is a very hostile medium (multipath, Doppler spread, various noises), this approach becomes a very challenging task. The Unscented Kalman Filter (UKF), detailed in [9], is a particularly innovative solution to the problem a non-linear state space estimation. The algorithm, not detailed here, has a structure comparable to the usual Extended Kalman Filter (EKF) [10]. In presence of strong nonlinearity, EKF is known to have an unstable behaviour. Moreover, its implementation can be delicate. For these reasons, the UKF solution is recommended here, with a combined estimation scheme : One filter has to estimate the state of the noisy chaotic signal and the second filter searches the associated information symbol (unknown parameter). Each filter uses the last estimates of the other. The output of the second filter is continuous time. Then, a symbol decision is taken as the sign of the averaged output over symbol duration.

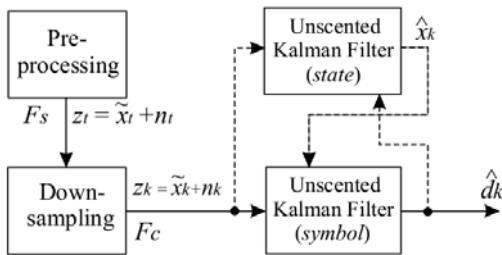


Fig. 9. CD3S Dual Unscented Kalman Filtering demodulator.

V. NUMERICAL RESULTS

A. Shallow Water Acoustic Channel Model & Transmission Scenario

Numerical simulations have been conducted to evaluate performances of our CD3S receivers. The transmission has been operated through use of an additional software module able to predict acoustic field using a ray method. Hence, important characteristics of the shallow water propagation channel have been taken into account, that is the range dependent nature of the medium, sorts of bottom profile, random air-sea boundary and ambient noise (Knudsen model).

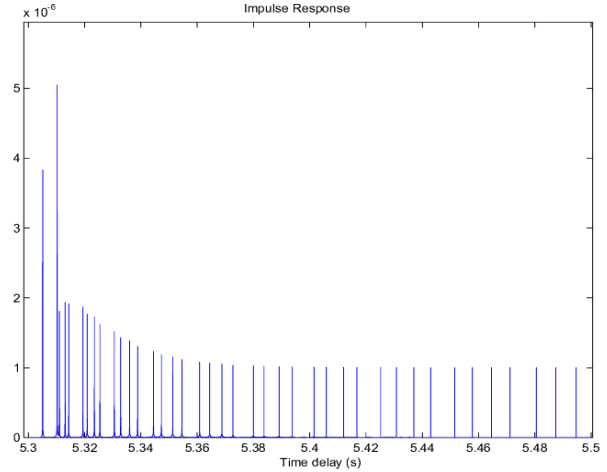


Fig. 10. Averaged impulse response for the shallow water acoustic channel

The transmission range was 8 km, with a transmitter placed to a depth of 20 m and a receiver to 40 m. The water depth was 90 m, and an averaged sound speed profile measured at $\varphi = 10^\circ 30' 00''$ latitude and $g = 16^\circ 30' 00''$ longitude has been used. The bottom, made of smudge, was flat and there was no wind. A frame of 200 bits, BPSK modulated, has been transmitted with a carrier frequency F_0 equal to 8820 Hz and a chip frequency F_c of 4410 Hz. The processing gain was 80. The SNR value was 0 dB at receiver input.

The averaged impulse response of the channel is shown by figure 10 (on this figure, the time-evolution of the impulse response, taken into account for simulations, is not shown). Figure 11 gives the acoustic loss field observed during transmission.

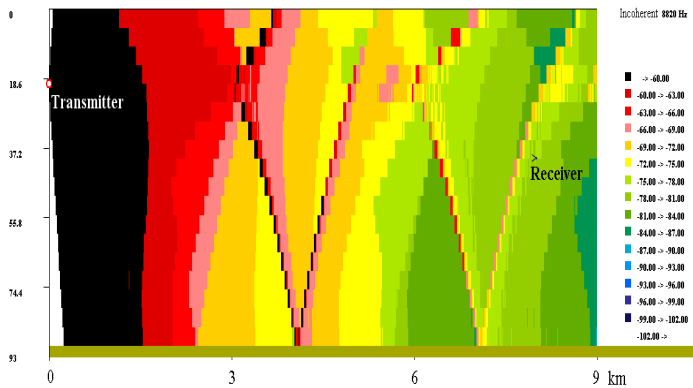


Fig. 11. Acoustic transmission loss field

B. ESS-based receiver performance

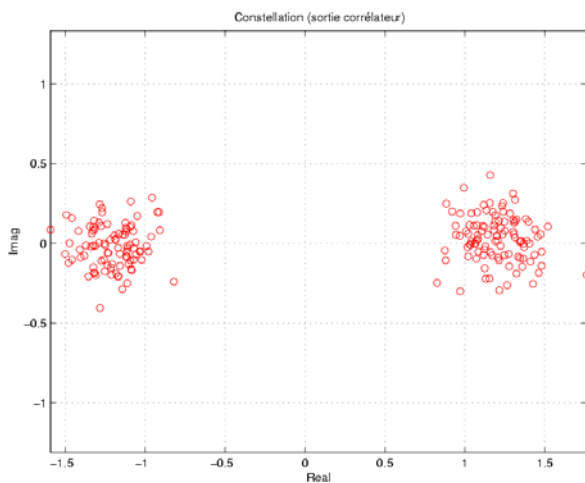


Fig. 12 – Correlator output for the ESS CD3S demodulator.

For this scenario, the ESS demodulator performs very well, as no decision error is noticed. Figure 12 shows the correlator output values. Indeed, in [7], for an additive white gaussian noise channel simulation, it has been mentioned that an approach similar to our ESS scheme has performances comparable to a standard DS-SS system, if the receiver synchronization is ensured. Hence, our results are no surprising.

C. Dual UKF-based receiver performance

This demodulator is more sensitive to channel imperfections, as it can be observed on figure 13. A Bit Error Rate (BER) of 5.5 % is noticed. Nevertheless, it should be emphasized that a basic implementation of the dual filtering scheme has been done (simple dynamic

model for signals at demodulator input, notably) and that we don't make use of an equalizer or channel encoding to reduce the BER. Finally, note the limited processing gain used.

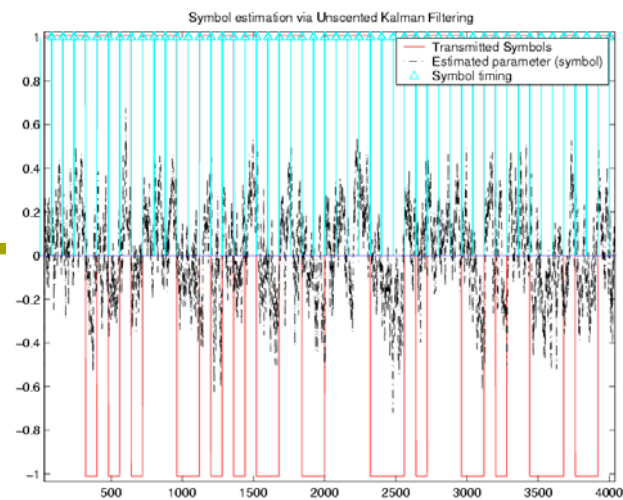


Fig. 13 – Dual Unscented Kalman Filtering CD3S demodulation (first 50 symbols).

VI. CONCLUSIONS & FUTURE WORK

Motivated by covertness deficiencies of standard spread spectrum systems, we have examined the feasibility of chaos based underwater communications. We have adopted a direct-sequence approach which is surely one of the most promising chaos based communication schemes. The aperiodicity of the spreading code, which plays a central role in such a system, has led us to develop specific demodulators. The first one, called Exact Spreading Sequence (ESS) demodulator, is comparable to the one previously mentioned in [7]. This solution, potentially excellent, applies only if the receiver is able to reproduce, in a synchronous way, the original spreading code. A robust reproduction strategy has then to be developed. The second solution is based on a dual state space adaptive filtering scheme (Unscented Kalman Filters), in order to estimate simultaneously the state of the received chaotic signal and the associated symbol. Then, the demodulator makes use of an approximate spreading sequence only. Despite this approximation, encouraging results have been observed.

Applications such as Underwater Acoustic Networks could take benefits of these results.

The multiuser capability of CD3S systems has not been discussed here; This problem is currently under investigation. To confirm our first conclusions, an experiment at sea will be performed soon with the help of

GESMA¹. To get a competitive system, it should be judicious to exploit the time-diversity that is present on the channel.

REFERENCES

- [1] E. M. Sozer, M. Stojanovic, J. G. Proakis, « Underwater Acoustic Networks », *IEEE J. Oceanic Eng.*, Vol. 25, No 1, 2000.
- [2] J. G. Proakis, Digital communications, 3rd ed., Mac-Graw-Hill Int. Ed., 1995.
- [3] 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.
- [4] 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.
- [5] L. M. Pecora, T. L. Carroll, « Synchronization in chaotic systems », *Phys. Rev. Lett.*, 64, pp. 821-824, 1990.
- [6] M. Hasler « Synchronization of chaotic systems and transmission of information », *Int. J. Bifurcation and Chaos*, Vol. 8, No 4, pp 647-659, 1998.
- [7] G. Heidari-Bateni, C. D. McGillem, « A chaotic direct-sequence spread spectrum communication system », *IEEE Trans. Comm.*, Vol. 42, No. 2, pp. 1524-1527, 1994.
- [8] V. Milanovic, K. M. Syed, M. E. Zaghoul, « Combating noise and other channel distortions in chaotic communications », *Int. J. Bifurcation and Chaos*, Vol. 7, No. 1, pp. 215-225, 1997.
- [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] Y. Bar-Shalom, X.-R. Li, « Estimation and Tracking – Principles, Techniques and Software », Artech House, 1993.

¹ Groupe d'Etudes Sous-Marines de l'Atlantique, Brest, France.