Design of a chaos-based spread-spectrum communication system using dual Unscented Kalman Filters

S. Azou[1] and G. Burel[2]

[1] L.E.S.T. - UMR CNRS 6165, Pôle Universitaire Per Jakez Helias, Creac'h Gwen, 29000 QUIMPER, France
[2] L.E.S.T. - UMR CNRS 6165, Université de Bretagne Occidentale, BP 809, 29285 BREST cedex, France
e-mail : {Stephane.Azou, Gilles.Burel}@univ-brest.fr

Abstract - *It has been demonstrated recently than use of chaotic spreading codes can significantly increase transmission privacy for direct-sequence spread spectrum systems. In this note, we consider the problem of receiver synchronization as a dual estimation of the clean state and the underlying model parameters from the observed noisy chaotic signal. An efficient implementation of the demodulator is investigated owing to the Unscented Kalman Filter, a recent alternative to the Extended Kalman Filter, providing superior performance at an equivalent computational complexity. Numerical simulations show the performance of this novel demodulator against noise for a single user on Gaussian channels.*

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]. The motivation to use chaos for transmission is mainly due to its wideband nature and its noise-like appearance. Hence, as for common spread-spectrum techniques, chaotic signals provide robustness against frequency selective fading in multipath channels and narrowband interference. Owing to the intricate dynamic of chaos, the privacy of communications can be significantly increased in comparison with standard pseudo-noise codes used in spread-spectrum [3]. Without knowledge of the type of nonlinearity on which the transmission is based, it will be extremely difficult for the unauthorized user aware of the transmission to access the information. Many other potential benefits have to be noticed, among others the reduced complexity of transmission devices and a sharing of channel resources via Code Division Multiple Access (CDMA). Chaos can be used in multiple ways in a digital communication system [4]. As in conventional communication systems, the transmitted symbols can be recognized at the receiver using either *coherent* or *noncoherent* demodulation techniques. Whereas a noncoherent receiver relies only on some statistics of the received signal, a coherent receiver requires a complete knowledge about the transmitter to recover the original chaotic spreading code, by a synchronization process. Although the latter approach suffers from sensitivity to parameter mismatches between the transmitter and the receiver, and also from signal distortion induced by the channel, the probability of interception is reduced in this way.

This paper deals with demodulator design in a Chaotic Direct-Sequence Spread Spectrum system [5]. As in previous papers, the logistic map is recommended here as the spreading code generator, due to its favorable correlation properties. In order to get reliable communication for realistic propagation conditions, a robust synchronization procedure has to be developed at the receiver side. A recursive nonlinear estimation scheme is preferred here to the standard master-slave configuration, initially proposed by Pecora and Caroll [6]. The idea of using state-space adaptive filtering to perform chaotic synchronization is not new ; Cuomo et al. [7] have previously mentioned the interest of the Extended Kalman Filter in such a context, for a Lorenz system. More recently, a method of synchronizing two chaotic Duffing systems is described in [8] by implementing an EKF for continuous-time systems. In this work, communication is achieved by modulating a parameter within the transmitter and augmenting the model order within the EKF to estimate that parameter. In [9][10], similar results are reported using a discrete-time formalism.

Given a stochastic linear discrete-time model in state-space, the Kalman filtering problem [11] is to produce an estimate $\hat{x}_k$ of the true state x_k, given a sequence of noisy observations up to time k. In the linear case, the Kalman filter yields the optimal estimate in the minimum mean-squared error (MMSE) sense. For application to nonlinear models, the so-called Extended Kalman Filter is often used in practice. In the EKF, the state distribution is approximated by a Gaussian random variable, which is propagated analytically through a first-order linearization of the nonlinear system. As a consequence of these successive approximations, large errors in the true posterior mean and covariance of the transformed random variable can occur, which may lead to sub-optimal performance and sometimes divergence of the filter.

Motivated by the deficiencies of the EKF, we propose to use the more robust Unscented Kalman Filter (UKF) to perform the synchronization in a CD3S receiver. The UKF, recently proposed by Julier et al. in the context of nonlinear control [12], addresses the approximation issues of the EKF. The state distribution is again represented by a Gaussian random variable, but is now specified using a minimal set of carefully chosen sample points. At each step of the 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 [13].

Spreading the spectrum of the information signal by direct-sequence can be considered as a special case of switching the parameter of a dynamic model for communicating with chaos. It follows from this observation that CD3S signals can be demodulated through a dual estimation scheme. This process will be implemented in an original manner here owing to the UKF.

The paper is organized as follows. In section II we present principles of a CD3S transmitter and the pre-processing that have to be done at the receiver before demodulation. The dual estimation scheme for receiver synchronization and implementation details using UKF are treated in section III. The *unscented transform*, playing a central role in the UKF, is overviewed in section IV. Then, in section V, the method is illustrated and some performances for Gaussian channels are given. Finally, in section VI we draw some concluding remarks.

II. Chaotic Direct-Sequence Spread Spectrum (CD3S) Signals

Figure 1 illustrates the principles of a 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 $Fc \gg Fd$, F_d being the data rate. The processing gain $W = Fc / Fd$ must be an integer. Its value depends on the bandwidth available for the propagation channel, notably.

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 0.5, before a carrier modulation at central frequency F_0. To avoid aliasing, the signal has to be sampled at a minimum value of $2F_0 + (1+\alpha)F_c$.

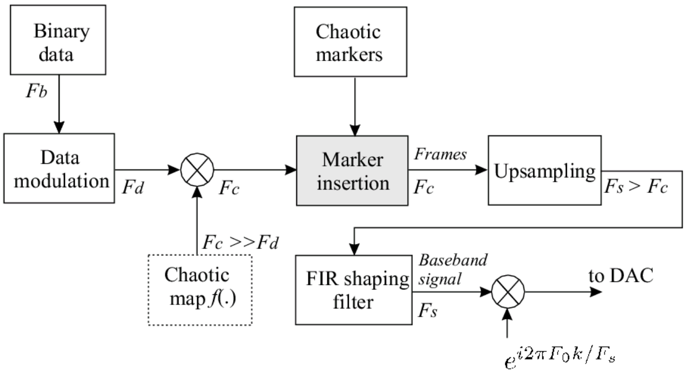

Fig. 1 – Block diagram of a CD3S transmitter.

As in [14], 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

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

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. A dual estimation scheme for CD3S demodulation

In this section, we focus on the demodulator design for CD3S signals. A simultaneous estimation of the state of the noisy received chaotic signal and the data symbol is proposed to recover the information. As illustrated by figure 2, this dual estimation problem is solved owing to Unscented Kalman Filters, due to their moderate computational cost and their robustness in the presence of strongly nonlinear signals.

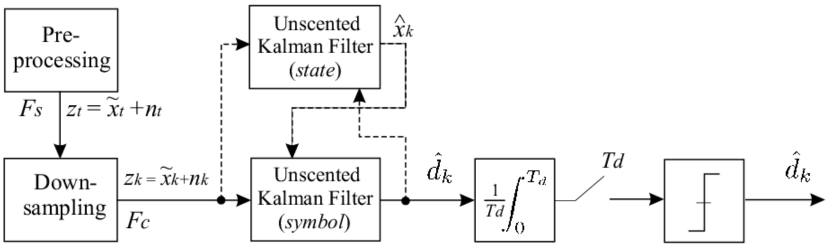

Fig. 2 – Dual estimation scheme for CD3S demodulation.

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. Also, the carrier phase and the signal power fluctuations have to be adjusted before the demodulation process. In what follows, a binary data modulation (e.g. BPSK) is assumed ; In this case, the information is embodied in the real part of the signal only at the output of the pre-processing block.

The received downsampled signal is assumed to evolve according to the following system model :

$$x_k = f(x_{k-1}) + v_k = d_k(1 - 2x_{k-1}^2) + v_{k-1}$$

where x_k and d_k are the clean chaotic signal state and true symbol respectively, and where v_k is a zero mean, White Gaussian Noise (WGN) sequence with variance Q, independent of the past and current state. This model uncertainty is necessary to take into account the distortions resulting from transmitter/receiver filters, the analog-digital conversions and the channel multipath.
The available observations are modelled as

$$z_k = h(x_k) + n_k = x_k + n_k$$

where x_k is the true state and where n_k is a WGN whose variance R depends upon signal-to-noise ratio (SNR).
As the information symbol d_k is constant over $W = F_c / F_d$ consecutive samples, it is assumed to evolve as

$$d_k = f^p(d_{k-1}) + w_{k-1} = d_{k-1} + w_{k-1}$$

The additional term w_k is a WGN. Its variance Q^p will influence the adaptability of the symbol filter ; A low value will result in slow changes whereas a larger value will result in rapid variations of the symbol estimates.
Finally, the true symbol is observed according to the model

$$z_k = h^p(d_k) + n_k = d_k(1 - 2x_{k-1}^2) + n_k$$

The implementation of the dual estimation procedure is outlined at figure 3.

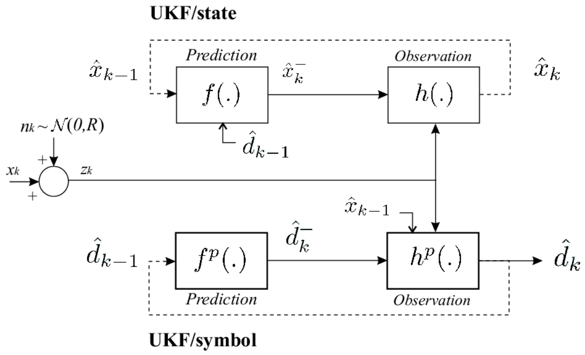

Fig. 3 – Implementation of the demodulator using Unscented Kalman Filters.

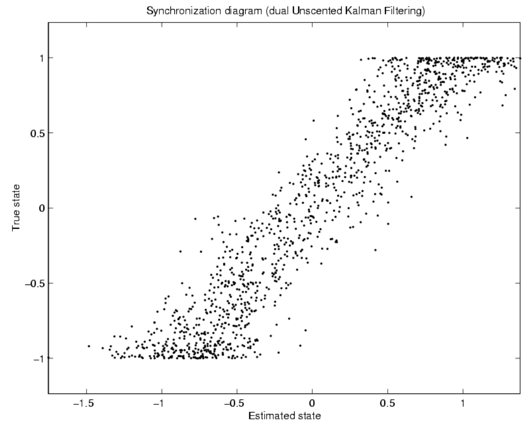

Fig. 4 –True state vs. Estimated state for a dual UKF synchronization of a CD3S receiver.

IV. Overview of the Unscented Kalman Filter (UKF)

The UKF, developed by Julier et al. [12], addresses the approximation issues of the EKF. The reader is referred to [11] for a detailed explanation of the EKF.

The state distribution is represented by a Gaussian random variable $\boldsymbol{x}$, but is specified using a minimal set of carefully sample points. These points completely capture the mean and covariance of the random variable $\boldsymbol{x}$. Then, owing to the Unscented Transformation (UT), it is possible to capture precisely the statistics of the random variable $\boldsymbol{y}$ resulting from a nonlinear transformation.

The general problem of approximating nonlinear transformations of probability distributions can be stated as follows : given a r.v. $\boldsymbol{x} \in \Re^n$ with mean $\bar{\boldsymbol{x}}$ and covariance $\boldsymbol{P}_{xx}$, we would like to predict the mean $\bar{\boldsymbol{y}}$ and covariance $\boldsymbol{P}_{yy}$ of a r.v. $\boldsymbol{y} \in \Re^m$, where $\boldsymbol{y}$ is related to $\boldsymbol{x}$ by the nonlinear transformation $\boldsymbol{y} = \boldsymbol{f(x)}$. To solve this problem, Julier had an intuition that *with a fixed number of parameters it should be easier to approximate a Gaussian* *distribution than it is to approximate an arbitrary non linear transformation*. The procedure can be summarized as follows :

1. A set of weighted points $\{\chi_i\}_{i=1,\ldots,2n+1}$ is chosen to approximate the r.v. $\boldsymbol{x}$:

$$\begin{aligned} \chi_0 &= \bar{\boldsymbol{x}} & W_0 &= \kappa/(n+\kappa) \\ \chi_l &= \bar{\boldsymbol{x}} + \left(\sqrt{(n+\kappa)\boldsymbol{P}_{xx}}\right)_l & W_l &= 1/2(n+\kappa) \\ \chi_{l+n} &= \bar{\boldsymbol{x}} - \left(\sqrt{(n+\kappa)\boldsymbol{P}_{xx}}\right)_l & W_{l+n} &= 1/2(n+\kappa)\ ,\ l = 1,\ldots,n \end{aligned}$$

where $\kappa \in \Re$;

2. Each point is then transformed as $\boldsymbol{\mathcal{Y}}_i = \boldsymbol{f}(\chi_i)$;

3. The mean $\bar{\boldsymbol{y}}$ is given by the weighted average of the transformed points : $\bar{\boldsymbol{y}} = \sum_{i=0}^{2n} W_i \boldsymbol{\mathcal{Y}}_i$;

4. The predicted covariance $\boldsymbol{P}_{yy}$ is computed as : $\boldsymbol{P}_{yy} = \sum_{i=0}^{2n} W_i \{\boldsymbol{\mathcal{Y}}_i - \bar{\boldsymbol{y}}\}\{\boldsymbol{\mathcal{Y}}_i - \bar{\boldsymbol{y}}\}^T$.

In comparison with Monte Carlo techniques, the fundamental difference is that the samples are not drawn at random but according to a deterministic algorithm. A very small number of samples is then required to approximate the probability distribution. This method has many others advantages : owing to the parameter κ the scaling of the fourth and higher order moments can be influenced; the function *f*, which may be implicit, is not approximated through a truncation of its series expansion and the implementation is very easy since no evaluation of Jacobians is needed. It is shown that the mean and covariance of $\boldsymbol{y}$ are captured accurately to the second order (Taylor series expansion) for any nonlinearity. The Unscented Kalman Filter is an extension of the UT to the recursive estimation scheme of a Kalman filter. More details about this subject can be found in [13].

V. Illustrations and Performance evaluation for Gaussian channels

Numerical simulations have been conducted to evaluate performances of the proposed CD3S receiver. In this section, results for a single user on a Gaussian channel are described only. Performances in a realistic context of transmission underwater are reported in [15]. Figures 4 & 5 illustrate the receiver behaviour for an additive white Gaussian noise with SNR equal to 8 dB and a processing gain of 63. The UKF configuration was chosen as : $Q = 0.1$, $R = 0.5$ and $Q^p = 0.02$. As shown by figure 4, the chaotic synchronization performs well at this noise level. Figure 5 shows few transmitted symbols and their estimates ; A good adaptativity of the UKF is noticed on this figure. Monte Carlo simulations have been conducted to evaluate the Bit Errror Rate for larger noise levels. The results are given in figure 6. It should be noticed that the variance R was adjusted for each SNR, in order to get the upper bound of the performances. Nevertheless, it has been observed that a rough estimation of the noise level is sufficient to approach this bound. The proposed UKF demodulator has a good allowance concerning its configuration (choice of Q, Q^p, R).

VI. Conclusion

A novel demodulator has been investigated for Chaotic Direct-Sequence Spread Spectrum (CD3S) signals. This demodulator relies on a dual estimation of the state of the received chaotic signal and the associated data symbol (parameter of the system model). An implementation based on Unscented Kalman Filters is proposed. In this way, a good robustness against noise is achieved at a limited computational cost. The BER performance has been evaluated via Monte Carlo simulations, for a single user on a Gaussian channel.

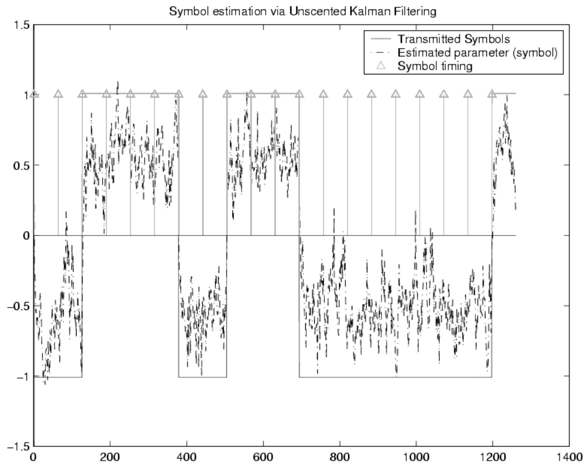

Fig. 5 – Estimated and. True symbol for a dual UKF synchronization of a CD3S receiver.

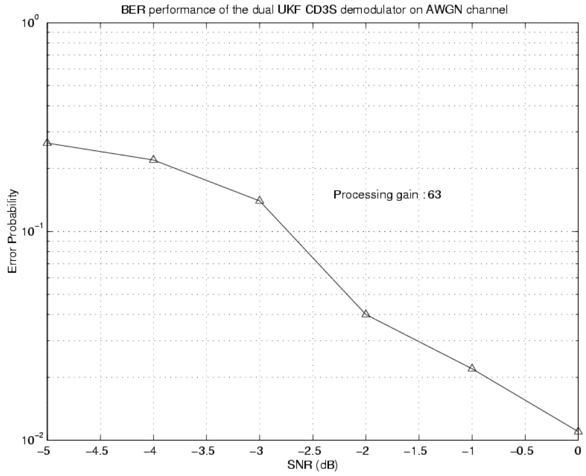

Fig. 6 – BER performance of a CD3S receiver based on dual Unscented Kalman Filters (logistic map, processing gain of 63)

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, pp. 1129-1140, 1998.

[3] G. Burel, A. Quinquis, S. Azou, « Interception and Furtivity of Digital Transmissions», *IEEE Communications Conf.*, Dec. 2002, Bucarest, Romania.

[4] A. Serbanescu, « Sisteme de Transmisiuni Integrate Vol. I ; Communicatii de Bande Larga folosind Sisteme Dinamice Haotice », Editura Academiei Tehnice Militare, Bucuresti, Romania, 2000.

[5] G. Heidari-Bateni, C. D. McGilleme, « A chaotic direct-sequence spread spectrum system », IEEE Trans. On Communications, Vol. 422, No. 2, pp. 1524-1527, 1994.

[6] L. Pecora, T. Caroll, « Synchronization in chaotic systems », Phys. Rev. Lett., Vol. 64, pp. 821-823, 1990.

[7] K. M. Cuomo, A. V. Oppenheim, S. H. Strogratz, « Synchronization of Lorenz-based chaotic circuits with application to communication », IEEE Trans. Circuits Syst. II, Vol. 40, No. 10, pp. 626-633, 1993.

[8] D. J. Sobiski, J. S. Thorp, « PDMA-1 : Chaotic Communication via the Extended Kalman Filter », IEEE Trans. Circ. Systems I, Vol. 45, No. 2, pp. 194-197, 1998.

[9] C. Cruz, H. Nijmeijer, « Synchronization through filtering », Int. J. Bifurcation and Chaos, Vol. 10, No. 4, pp. 763-775, 2000.

[10] H. Leung, J. Lam, « Design of demodulator for the chaotic modulation communication », IEEE Trans. Circuits Syst. I, Vol. 44, pp. 262-267, 1997.

[11] Y. Bar-Shalom, X.-R. Li, « Estimation and Tracking – Principles, Techniques ans Software », Artech House, 1993.

[12] 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.

[13] E. A. Wan, R. van der Merwe, "Kalman Filtering and Neural Networks", chap. 7 : The Unscented Kalman Filter, published by *Wiley Publishing* (editors S. Haykin), 2001.

[14] V. Milanovic, K. M. Syed, M. E. Zaghloul, « Combating noise and other channel distorsions in chaotic communications », *Int. J. Bifurcation and Chaos*, Vol. 7, No. 1, pp. 215-225, 1997.

[15] S. Azou, C. Pistre, G. Burel, "A chaotic direct sequence spread-spectrum system for underwater communication", IEEE Oceans Conf., Biloxi, Mississippi, October 29-31, 2002.