Pseudo-blind demodulation of chaotic DS-SS signals through Exact Kalman Filtering

Mihai Bogdan Luca, Stéphane Azou, Emanuel Hodina, Alexandru Serbanescu, Gilles Burel

Pseudo-blind demodulation of chaotic DS-SS signals through Exact Kalman Filtering

M. B. Luca[1,2], S. Azou[1], E. Hodina[2], A. Serbanescu[2] and G. Burel[1]

[1]Laboratoire d'Electronique et des Systèmes de Télécommunications (UMR CNRS 6165), Brest, France

[2]Military Technical Academy, Bucharest, Romania

***Abstract*— This paper adresses the problem of symbol estimation in the case of a spread spectrum based system where the receiver has only the information about the nonlinear function used to generate the spreading sequence. We propose two methods to achieve this, first based on the already considered DUAL form and a correlator second based one. For the DUAL form we consider multiple Kalman filter implementations suited to the case of nonlinear estimation methods among them Unscented Kalman Filter (UKF) and Exact Polynomial Kalman Filter (ExPKF). Finaly to provide a perfomance evaluation on the proposed methods we obtain throughout Monte-Carlo simulations the *Bit Error Rate* (BER) characteristics with respect to *Signal to Noise Ratio* (SNR).**

I. Introduction

The first nonlinear Kalman filtering method represented by the Extended variant (EKF) has been for many years the only method implemented to cope with the nonlinear model characteristics. Some attractive nonlinear Kalman filtering methods have recently been proposed to avoid previous limitations of the EKF without any significant additional computation cost. The UKF, first introduced by Julier *et al.* [6] in the context of nonlinear control addresses the approximation issues of the EKF. The state distribution is considered to be a Gaussian random variable, but is now specified using a minimal set of carefully chosen sample points (the *sigma points*). At each step of the recursion, these sample points are propagated through the true nonlinear functions of the model (*Unscented* Transformation), hence avoiding Jacobians computation. Following this approach, posterior mean and covariance are captured up to the third or second order terms of the Taylor series expansion, whatever the nonlinearity is.

Another newly introduced method is the Exact polynomial transform that performs the closed-form calculus for the posterior mean and covariance without any constraints on the anterior distribution. Actually as it is briefly presented in the second section, and largely exposed in [11], for the particular case of monodimensional polynomial functions we can obtain general matrix formulation for the first two *a posteriori* moments. It is unfortunate that we can not benefit completly from the closed form calculus, as the recursive implementation using a Kalman algorithm will calculate the first two moments and we are forced to express the next statistical distribution of the state using these two moments, meaning that we still work with Gaussian hypothesis. To show the significance of this filtering scheme we consider a direct application to synchronization of chaotic signals [1] generated through Chebyshev maps [9].

There has been significant interest in recent years in exploiting chaos in communication systems [2], [3]. Due to its random-like behavior and its wideband characteristics, a chaotic dynamical system can be very helpful to secure or encrypt a transmission. Leung and Zhu [4] have recently derived important results about chaos synchronization through Extended Kalman Filtering (EKF); the authors showed that the EKF-based technique is a generalization of two conventional schemes (unidirectionally coupled and drive-response methods). It is also shown that the EKF-based synchronization approaches the averaged Cramer-Rao Lower Bound at high SNR. In [11] the authors apply the Exact Polynomial Filtering (ExPKF) to the same problem of chaos synchronization and observe through analitical and simulation that this approach can offer a better solution to high nonlinearity models, keeping a low computational cost.

To apply the ExPKF to some data demodulation scheme we consider the DUAL approach presented in papers [7], [8] and compare it with a newly introduced correlator approach.

The paper is organized as follows. In section II, we shortly present the general matrix formulas giving the second-order statistics of any random variable which has been transformed through a polynomial function. Then, in section III, an Exact Kalman Filter relying on these analytical results is applied to a chaos synchronization model. A short presentation of the DUAL demodulation scheme is considered in section IV. In section V we present a new method of retriving the data transmitted through a direct spread spectrum modulation, using only the generator nonlinearity. Finally, before the conclusions, some numerical results are presented comparing the different methods for different Chebyshev polynomials and process gains.

II. Exact polynomial transformation

As the name of the section suggests, the goal of the transformation, and as the ulterior application to the general Kalman filtering algortihm requires, is to exactly calculate the first two moments of the random variable transformed distribution y, with the complete knowledge of the initial distribution x, and of the polynomial transform function $y = f(x)$. The general form of the monodimensional polynomial transformation can be expressed as:

$$f(x) = \sum_{n=0}^{N} a_n x^n \tag{1}$$

The first two moments expression calculated below supposes no restrictions about the initial probability density functions,

but later when the transformation will be employed for a Kalman filter model the gaussianity restriction over the a priori distribution will be considered.

In general, we can write the first two moments of the transformed distribution of the random variable y using the Taylor series expansion. So we consider the initial distribution written as $x = \bar{x} + \Delta x$, where Δx is a random variable having a zero mean distribution. Now we can write the Taylor expansion for y as

$$y = f(\bar{x}) + \sum_{n=1}^{N} \frac{(\Delta x)^n}{n!} \frac{d^n f}{dx^n}\bigg|_{x=\bar{x}} \tag{2}$$

and we can determine the first moment:

$$\begin{aligned} \bar{y} &= E[y] \\ &= f(\bar{x}) + \sum_{n=2}^{N} \frac{m_n}{n!} \frac{d^n f}{dx^n}\bigg|_{x=\bar{x}} \end{aligned} \tag{3}$$

where m_n denotes the n^{th}- order moment of the random variable Δx.

Using the developpement of the derivatives we can obtain a general matricial expression of the first order moment as presented in [11]:

$$\bar{y} = \mathbf{a}_{0:N}^T \mathbf{C}^{\bar{x}} \mathbf{m}_{0:N}^x \tag{4}$$

where $\mathbf{a}_{i:j}$ stands for $[a_i, a_{i+1}, ..., a_j]^T$, $\mathbf{m}_{i:j}^x = [m_i, m_{i+1}, ..., m_j]^T$ and $\mathbf{C}^{\bar{x}}$ denoting a lower triangular matrix where entries are powers of $\bar{x}$ and some binomial coefficients.

Considering again the Taylor series expansion, the second order centered moment σ_y^2 can be computed following a similar approach:

$$\sigma_y^2 = \mathbf{1}_N^T \left(\mathcal{M}^x \boxdot \mathcal{C}^{\bar{x}}\right) \mathbf{1}_N - \left(\mathbf{m}_{1:N}^x\right)^T \mathcal{C}^{\bar{x}} \mathbf{m}_{1:N}^x \tag{5}$$

where the matrix $\mathcal{C}^{\bar{x}}$ has entries: $\bar{x}$, the binomial coefficients and the polynomial coefficients vectors $\mathbf{a}_{i:j}$; Similarly $\mathcal{M}^x$ is computed only from the centered moments vector of the initial distribution x. From the operator point of view $\boxdot$ denotes the Hadamard product and $\mathbf{1}_N$ stands for a column vector of size N whose entries are all one.

Our objective being to derive a Kalman filter relying on the previous relations, it remains to express the transition covariance P_{xy} between the variables x and y:

$$P_{xy} = E[(x - \bar{x})(y - \bar{y})] \tag{6}$$

Once again we can put the relation in matrix form:

$$P_{xy} = \mathbf{a}_{0:N}^T \mathbf{C}^{\bar{x}} \mathbf{m}_{1:N+1}^x \tag{7}$$

We would like to point out that the relations (4), (5) and (7) are given for any initial random variable x for which we know the centered moments, and for any polynomial form of the function $f(\cdot)$. It doesn't mean that these relations minimize the computationnal cost but in exchange offer a general formula to calculate exactly the first two moments $\left(\bar{y}, \sigma_y^2\right)$.

We will present in the next section a particular approach, for a 2^{nd}- order Chebyshev polynomial function, where the general matricial equations of the moments can be reduced to a much simpler form.

III. The application of the ExPKF to chaos synchronization

We will apply the nonlinear transformation presented above to the problem of chaos synchronization, where the characteristic non-linear function is chosen to be polynomial.

The general model of synchronization for a mono-dimensional chaotic polynomial map, can be expressed as:

$$\begin{aligned} x_{k+1} &= f(x_k) + v_k \\ y_k &= x_k + n_k \end{aligned} \tag{8}$$

which will allow us to write the equations of the proposed ExPKF algorithm using the analytical formulas of $\left\{\bar{y}, \sigma_y^2\right\}$. As an example, for a second order Chebyshev sequence synchronization $f(x_k) = 2x_k^2 - 1$; The filter is implemented as follows, once the second order statistics have been computed analytically.

The time-update equations are:

$$\hat{x}_{k+1|k} = E[f(x_k)] = 2P_k + 2\hat{x}_k^2 - 1 \tag{9}$$

$$P_{k+1|k} = E\left[\left(x_{k+1|k} - \hat{x}_{k+1|k}\right)^2\right] = 8P_k^2 + 16P_k\hat{x}_k^2 + Q \tag{10}$$

Also, considering the observation function linearity and the independence of the model and observation noises between them and with the states, the measurement-update equations become:

$$\hat{y}_{k+1|k} = E\left[h\left(x_{k+1|k}\right)\right] = \hat{x}_{k+1|k} \tag{11}$$

$$\begin{aligned} P_{x_{k+1|k}y_{k+1|k}} &= E\left[\left(x_{k+1|k} - \hat{x}_{k+1|k}\right)\left(y_{k+1|k} - \hat{y}_{k+1|k}\right)\right] \\ &= P_{k+1|k} \end{aligned} \tag{12}$$

$$\begin{aligned} P_{y_{k+1|k}y_{k+1|k}} &= E\left[\left(y_{k+1|k} - \hat{y}_{k+1|k}\right)\left(y_{k+1|k} - \hat{y}_{k+1|k}\right)\right] \\ &= P_{k+1|k} + R \end{aligned} \tag{13}$$

$$K_{k+1} = \frac{P_{k+1|k}}{P_{k+1|k} + R} \tag{14}$$

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}\left(y_{k+1} - \hat{x}_{k+1|k}\right) \tag{15}$$

$$P_{k+1} = P_{k+1|k} - K_{k+1}^2 P_{y_{k+1|k}y_{k+1|k}} = \frac{P_{k+1|k}R}{P_{k+1|k} + R} = K_{k+1}R \tag{16}$$

As can be seen by the relations (11) - (16), the ExPKF algorithm applied to the chaos synchronization of a second order Chebyshev polynomial model, offers if not the best, one of the most cost-effective solutions. So complementary with the general matrix form, for particular system models, some low computational cost implementations with very good performances can be expressed, as it will be confirmed by the numerical results presented in the next section.

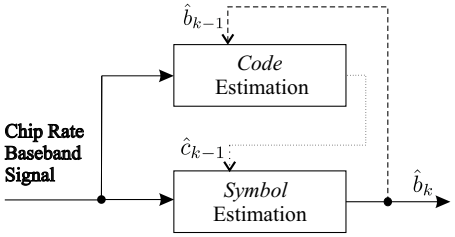

Fig. 1. Code/Symbol Dual Estimation Block

IV. The demodulation via dual estimation

We have considered the CD3S receiver relying on EKF or UKF dual estimations, reported into [7], [8]. If the cited papers consider only the Unscented implementation but deal with gain control methods, carrier recovery options and even multipath channel supposition, in this article we will consider only the base band signal affected by a gaussian noise, the goal beeing to see how the new filter approach can cope with the non-linearity of the models.

As shown by figure 1, the dual Kalman filtering scheme enables the estimation, at chip rate F_c, of the original chaotic spreading code c_k together with the data symbol b_k from noisy observations y_k. Each of the two filters uses last estimate of the other as a parameter, the general model being presented by equation (17). The dynamical model and the observation model used for code estimation take the following form:

$$\begin{cases} c_{k+1} &= f(c_k) + v_k^c \\ y_{k+1} &= sgn\left(\hat{b}_k\right) c_{k+1} + n_{k+1} \end{cases} \tag{17}$$

where $f(\cdot)$ stands for the nonlinear chaotic function, and where the noise sequence $v_k^c \sim N(0, Q^c)$, independent of the past and current state c_k, reflects the model uncertainty due to channel imperfections; the noise term $n_k \sim N(0, R)$ in the observation model will be mainly dependent upon the SNR at the receiver input.

Similarly, the symbol will be estimated at chip rate through the following model:

$$\begin{cases} b_{k+1} &= b_k + v_k^b \\ y_{k+1} &= b_{k+1} f(\hat{c}_k) + n_{k+1} \end{cases} \tag{18}$$

where the gaussian noise sequence $v_k^b \sim \mathcal{N}\left(0, Q^b\right)$, independent of the past and current state b_k, will influence the adaptability of the symbol filter; a low value Q^b will result in slow changes whereas a larger value will result in rapid variations of the symbol estimates.

V. Correlator based receiver using the chaotic dynamic

The simplest way to retrieve the information signal spreaded by some chaotic sequence is to use a correlator implementation. In general the correlator based receiver is also the optimal one with the condition of complete knowledge of the spreading sequence. If the spreading sequence is not known we will prove in this section that the information signal can still be retrieved by a correlator based scheme with only the knowledge of the chaotic generator dynamics. Actually we will prove that under the hypothesis of some odd generating function and BPSK data modulation, the current spreading chip can be obtained by just propagating the previous observation, with the consequence of some channel noise amplification. For example in the case of the 2^{nd}-order Chebyshev polynomial we obtain:

$$\begin{aligned} f(y_k) &= f(b_k c_k + n_k) \\ &= 2(b_k c_k + n_k)^2 - 1 \\ &= f(c_k) + 4 b_k c_k n_k + 2 n_k^2 \\ &= c_{k+1} + n_k^r \end{aligned} \tag{19}$$

where $n_k^r = 4 b_k c_k n_k + 2 n_k^2$ is the noise resulting from the observed chip propagation. We can qualitatively affirm that this noise term is 2^{nd}- degree dependent with the noise present in the channel and in a low SNR scenario the effect of the propagation will decrease a lot the performances of the method. With a 4^{th}- order Chebyshev generator the problem will be more critical as the greatest coefficient of the recursive noise term will be 4^{th}- order dependent with the noise present in the channel, and as a consequence a larger performance decrease will occur as shown in the next section.

Finally the decision over the current informational symbol is done by correlating the supposed propagated sequence with the received one over the symbol length, and in our BPSK modulation case a regular $sign$ operator it is used.

VI. Numerical results

One of most important performance criteria for any communication scheme is the BER achieved by the selected method with respect to some noise coefficient factor. As our case considers a binary data modulation, the SNR is the most pertinent one. To exemplify the performances achieved by the methods presented above we will consider two principal cases: 2^{nd} and 4^{th}-orders Chebyshev polynomials as generating the spreading sequence.

The goal is to identify how the methods can cope with the increased nonlinearity presented by the generator, the spreading gain and the noise present in the channel. In figures 2, 3 we have considered the case of the 2^{nd}-order polynomial for spreading gains of 31, respectively 63. We observed that in both cases the correlator based method has the best performances, but increasing the gain, the difference with the dual estimation based receiver diminishes. The scaled-UKF has a small uphold over the ExPKF implementation as the moments calculation has been modified to cope with some divergence of the error covariance. At this order we do not observe an important difference betwwen the ExPKF and the UKF implementations as the UKF assures the correct expression of the moments for this order.

Considering now the 4^{th}-order polynomial we observe in figures 4 and 5, a general decrease of performances for all the methods. As it was supposed to happen, the correlator based can not cope with the noise present in the channel, and this time the chaos synchronization based methods have the lead with ExPKF and standard UKF implementations surpassing the scaled-UKF method. We put this slight performance decrease of the scaled-UKF on the adaptation of the method to perform well with relatively low non-linear charateristics. A last observation

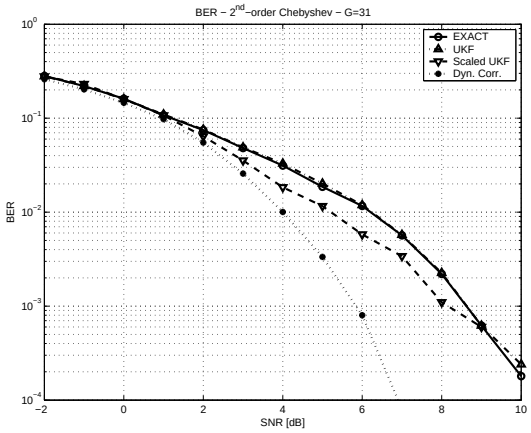

Fig. 2. BER estimated for the 2^{nd}-order Chebyshev spreading sequence with a 31 spreading gain

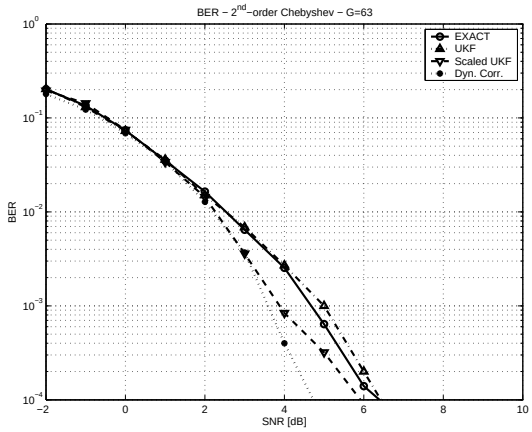

Fig. 3. BER estimated for the 2^{nd}-order Chebyshev spreading sequence with a 63 spreading gain

can be done over the calculus burden in which the ExPKF implementation excels as there is no point propagation method and the expression of the moments is calculated directly, in opposition with the UKF filtering methods.

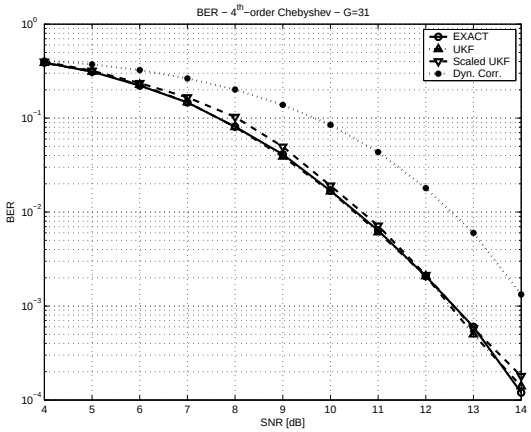

Fig. 4. BER estimated for the 4^{th}-order Chebyshev spreading sequence with a 31 spreading gain

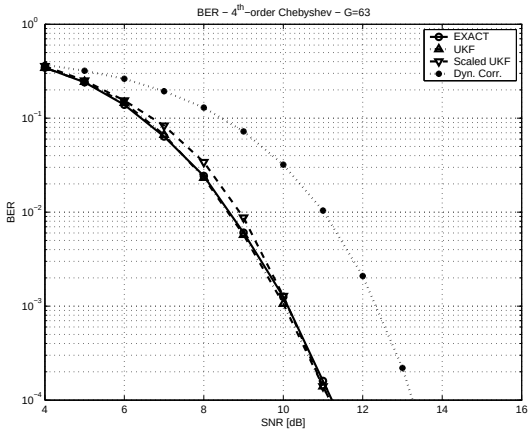

Fig. 5. BER estimated for the 4^{th}-order Chebyshev spreading sequence with a 63 spreading gain

VII. Conclusions

An Exact Polynomial (ExP) transformation has been applied to the problem of dual code/symbol estimation in chaotic DS-SS receivers. The analytical computations of the moments in the proposed ExP Kalman Filter leads to better performances in presence of strong code nonlinearity and a very limited computational cost. An alternative approach, based on direct propagation through the code nonlinear function, enables symbol detection by correlation. Due to channel noise amplification, good performances are obtained for weak nonlinearity only. The compared BER show that the proposed ExPKF is a pertinent approach for pseudo-blind demodulation of chaotic DS-SS signals.

References

[1] L. Pecora and T. Caroll, " Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 2, pp. 821-823, 1990.

[2] M. Hasler " Synchronization of chaotic systems and transmission of information," *Int. J. Bifurcation and Chaos*, vol. 8, no. 4, pp. 647-659, 1998.

[3] T. Yang, " A Survey of Chaotic Secure Communication Systems," *Int. Journal of Computational Cognition*, vol. 2, no. 2, June 2004.

[4] H. Leung and Z. Zhu, " Performance evaluation of EKF-based chaotic synchronization," *IEEE Trans. Circuits Syst. I*, vol. 48, no. 9, pp.1118-1125, Sept. 2001.

[5] Y. Bar-Shalom and X.-R. Li, *Estimation and Tracking: Principles, Techniques and Software.* Artech House, Boston, 1993.

[6] S. Julier, J. Uhlmann and 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.

[7] S. Azou, M. B. Luca, G. Burel, and A. Serbanescu "The problem of gain control in a Kalman filter based synchronization chaotic receiver," *IEEE-Communications 2004*, June 3-5, 2004, Bucharest, Romania.

[8] M. B. Luca, S. Azou, G. Burel and A. Serbanescu, "A Complete Receiver Solution for a Chaotic Direct Sequence Spread Spectrum Communication System," *Proc. IEEE ISCAS '05*, Kobe, Japan, May 2005.

[9] T. J. Rivlin, *Chebyshev Polynomials*. New York: Wiley, 1990.

[10] F.C.M. Lau, C.K. Tse, M. Ye and S.F. Hau, " Co-existence of Chaos-Based and Conventional Communication Systems of Equal Bit Rate," *IEEE Trans. Circuit Syst. I*, vol. 51, no. 2, pp.391-408, Feb. 2004.

[11] M. B. Luca, S. Azou, G. Burel and A. Serbanescu, " On Exact Kalman Filtering of Polynomial Systems," *IEEE Trans. Circuits and Syst. I, accepted oct. 2005*