Use of Chebyshev Polynomial Kalman Filter for pseudo-blind demodulation of CD3S signals

Moussa Yahia, Davide Radi, Laura Gardini and Valerio Freschi

Abstract: Chaos based communication represents an attractive solution in order to design secure multiple access digital communication systems. In this paper we investigate the use of piecewise linear chaotic maps as chaotic generators combined, on the receiver side, with Chebyshev Polynomial Kalman Filters in a dual scheme configuration for demodulation purpose. Piecewise linear maps results into enhanced robustness properties of the spreading chaotic sequence, while approximation of nonlinear systems through Chebyshev polynomial series allows closed form estimation of mean and variance. Therefore, statistical moments can be computed by means of simple algebraic operations on matrices in compact form. In this work we extend these concepts to a dual Chebyshev Polynomial Kalman Filter scheme, suitable for signal recovery in chaos based spread spectrum systems. Numerical simulations show that the proposed method achieves lower error levels on a wide range of the bit-energy-to-noise-power-spectral-density ratio with respect to a state-of-the-art method based on unscented Kalman filters.

Keywords: Kalman filter, chaotic direct sequence spread spectrum communication, Chebyshev polynomials, nonpolynomial maps, estimation.

---

1. INTRODUCTION

Estimating the current state variables of nonlinear systems affected by Gaussian or non-Gaussian noise is of fundamental importance in a wide range of fields such as signal processing, robotics, localization and economics.

Indeed, it is quite common that in real situations the required information is not directly available, but must be retrieved posteriorly once evidences are acquired through measurements. To cope with the issue, some interesting Kalman filtering methods have been introduced. Notably, filtering methods have been applied to different but related problems, (e.g. inverse modeling of discrete-time nonlinear systems) without requiring any prior knowledge of noise statistics [1, 2].

For what concerns Kalman filtering methods, the most known are the Unscented Kalman Filter (UKF) and the Exact Polynomial Kalman Filter (ExPKF). The first one was introduced in [3]. It can deal with any type of nonlinearity and it is based on a deterministic sampling technique, known as the unscented transform, used to select a minimal set of sample points around the mean (the *sigma points*). At each step of the recursion, these sample points are propagated through the nonlinear function of the model, from which the posterior mean and variance are recovered. The technique is based on a rather coarse approximation as only a small set of sigma points is usually employed. Moreover, as only a point representation is propagated instead of the entire Gaussian distribution, it does not allow to capture higher-order information of the prior density of the nonlinear functions.

Differently, the ExPKF, introduced in [4], is a closed-form estimator for polynomial nonlinear systems. The main drawbacks are the computational cost and the impossibility to work with nonlinear non polynomial functions, such as piecewise linear functions. In order to overcome both problems, recently [5] and [6] reformulated the ExPKF algorithm. The reformulation is based on the Chebyshev series approximation of the original model which allows to exploit the Chebyshev polynomial properties to derive and express in vector-matrix notation the closed-form solutions for the moment propagation ensuring a computationally efficient implementation. This new method is named Chebyshev Polynomial Kalman Filter (CPKF). As shown in [6], the computational performance of CPKF is comparable to that of UKF.

The CPKF and the UKF schemes can both be used in the demodulation of signals generated by a Chaotic Direct Sequence Spread Spectrum (CD3S) communication system. This communication system makes use of a chaotic sequence, generated by means of a chaotic map, to secure information signals sent on a channel. In order to ensure security, the chaotic sequence generated by the chaotic

The first author acknowledges the University of Jijel, Algeria, for financial support.

Moussa Yahia is with the Department of Electronics, University of Jijel, Jijel, Algeria (e-mail: yahiamos@yahoo.fr).

Davide Radi is with the Department of Management, Universitá Politecnica delle Marche, Ancona, Italy (e-mail: d.radi@univpm.it).

Laura Gardini is with the DESP, University of Urbino, Urbino, Italy (e-mail: laura.gardini@uniurb.it).

Valerio Freschi (corresponding author) is with DiSBeF, University of Urbino, Urbino, Italy (e-mail: valerio.freschi@uniurb.it).

map has to be robust, i.e. persistent under parameter perturbations, which means that there must exist a neighborhood in the parameter space of the map with no periodic attractors. As it is well known that smooth maps cannot generate robust chaos, see e.g. [7], we are forced to use a piecewise-smooth map, and so a non-polynomial map, such as the skew tent map, to generate the chaotic sequence required in the CD3S communication system. Employing a non-polynomial map to generate a robust chaotic sequence prevents the use of the ExPKF to demodulate the signals and requires the use of the CPKF scheme, i.e. it requires to fit with a Chebyshev polynomial of a suitable order a piecewise-smooth map. The properties of the Chebyshev polynomials allow to compute the moments required by the Kalman estimator in closed and compact vector-matrix form. This ensures precision and speed of execution. On the contrary, the UKF does not allow to capture higher-order information of the prior density of the nonlinear function and this could cause a loss of precision.

In this paper, we propose to extend the CPKF method to a dual Kalman filtering scheme in order to pseudo-blindly demodulate a signal generated through a CD3S communication system. We derive analytical closed form expression of appriximated statistical moments and provide simulation results for evaluating the effectiveness of the proposed approach. A numerical comparison between the CPKF and the UKF, based on Monte Carlo simulations, shows the improved performance of the CPKF in term of Bit-Error-Rate (BER), in particular for low levels of the bit-energy-to-noise-power-spectral-density ratio (Eb/No).

The paper is organized as follows. The Chebyshev approximation and the related moments computation procedure in matrix form required by the CPKF scheme is described in section 2. The principles of the CD3S transmitter are shortly summarized in section 3. Section 3 contains the Kalman estimation scheme implemented for demodulating the signal produced by a CD3S communication system and a short description of the chaotic map used to generate the chaotic sequence of the spreading system. The numerical results are summarized and commented in section 4. Section 5 concludes.

2. APPROXIMATION VIA CHEBYSHEV POLYNOMIALS AND COMPUTATION OF MOMENTS

In this section we recap shortly the algebraic procedure required to implement the Chebyshev Polynomial Kalman Filter (we refer to [5] for more details). For a nonlinear non-polynomial transformation of a random variable $\mathbf{x}$, say $f(x) := \Omega \to \Omega$, where $\Omega = [-1,1]$ (it is worth to point out that the same hold true for a nonlinear non-polynomial transformation $f(x) := [a,b] \to [a,b]$ with $a,b \in \mathbb{R}$, see for instance [6]), it is not possible to apply the Exact Polynomial Kalman Filter introduced in [4] as it works only for polynomial systems. To overcome the problem, in [5] the authors proposed first to exploit the orthogonality properties of Chebyshev polynomials to fit a polynomial $g(x)$ to the nonlinear and non-polynomial function $f(x)$, and then to use the ExPKF on the polynomial $g(x)$ to estimate the original signal. The technique is summarized in the following. Let us start recalling that the Nth-order Chebyshev polynomial of the first kind is defined as

$$T_N(x) = \cos(N \arccos(x)), \quad N = 0,1,2,... \tag{1}$$

which, given the initial conditions $T_0(x) = 1$ and $T_1(x) = x$, can also be rewritten in a recursive way as

$$T_N(x) = 2xT_{N-1}(x) - T_{N-2}(x), \quad N = 2,3,...$$

A first important property of the Chebyshev polynomial $T_N(x)$ is that all its zeros for $x \in [-1,1]$ are located at

$$x_k = \cos\left(\frac{\left(k-\frac{1}{2}\right)\pi}{N}\right) \quad k = 1,2,...,N \tag{2}$$

and a second one is the orthogonality property of the Chebyshev polynomials T_i, $i = 0,1,...,N$ over the zeros x_k of $T_{N+1}(x)$, i.e.,

$$\sum_{k=1}^{N+1} T_i(x_k) T_j(x_k) = \begin{cases} 0 & i \neq j \\ \frac{N}{2} & i = j \neq 0 \\ N & i = j = 0 \end{cases} \tag{3}$$

for $0 \le i, j \le N$.

Exploiting the above-mentioned properties of the Chebyshev polynomials, it is easy to combine equations (1), (2) and (3) to prove that if $f(x)$ is an arbitrary function defined in the interval $\Omega = [-1,1]$, and if $N+1$ coefficients c_j, $j = 0,1,...,N$ are defined as:

$$\begin{aligned} c_j &= \tfrac{2}{N+1} \textstyle\sum_{k=1}^{N+1} f(x_k) T_j(x_k) \\ &= \tfrac{2}{N+1} \textstyle\sum_{k=1}^{N+1} f\left[\cos\left(\frac{\left(k-\frac{1}{2}\right)\pi}{N+1}\right)\right] \cos\left(\frac{j\left(k-\frac{1}{2}\right)\pi}{N+1}\right) \end{aligned} \tag{4}$$

then the approximation formula

$$f(x) \approx g(x) = \left[\sum_{j=0}^{N} c_j T_j(x)\right] - \frac{1}{2}c_0 \tag{5}$$

is exact for x equal to all of the $N+1$ zeros of $T_{N+1}(x)$. The numerical calculation (4) of the series coefficients is an important aspect as it allows a polynomial representation, i.e. (5), of a given nonlinear function $f(x)$.

As ExPKF demands closed-form calculations of the mean μ_y and the variance σ_y^2 of a one-dimensional random variable $\mathbf{y} = f(\mathbf{x})$, using the Chebyshev series to fit a polynomial $g(x)$ to $f(x)$, it is possible to satisfy the requirements. The whole process of moment calculation is summarized in the following. First of all, we have

$$\mathbf{y} = f(\mathbf{x}) \approx g(\mathbf{x}) = \sum_{n=0}^{N} a_n \mathbf{x}^n \tag{6}$$

where $a_n = c_{0:N} A_N^n$ and $c_{0:N} = [c_0, c_1, ..., c_N]$ is the vector of series coefficients obtained as in (4), while A_N^n is the n-th column of the matrix A_N of Chebyshev coefficients defined by

$$A_N = \left[\alpha_{0:N}^0, \alpha_{0:N}^1, ..., \alpha_{0:N}^N\right]^T \tag{7}$$

so that $\alpha_{0:N}^n = \left[\alpha_0^n, \alpha_1^n, ..., \alpha_N^n\right]^T$ comprises all coefficients of the n-th Chebyshev polynomial up to and including the N-th monomial. Then, given that $\mathbf{x} \sim \mathcal{N}\left(\overline{x}, \sigma_x^2\right)$, it can be written as $\mathbf{x} = \overline{x} + \Delta\mathbf{x}$, where $\Delta\mathbf{x} \sim \mathcal{N}\left(0, \sigma_x^2\right)$ is a zero mean Gaussian random variable, and by means of Pascal's triangle rule, the terms $\mathbf{x}^n$ can be expanded as:

$$\mathbf{x}^n = (\overline{x} + \Delta\mathbf{x})^n = \sum_{i=0}^{n} c_n^i (\overline{x})^{n-i} (\Delta\mathbf{x})^i$$

where $c_n^i = \frac{n!}{i!(n-i)!}$ is a binomial coefficient. Consequently, the expression (6) becomes

$$\mathbf{y} \approx \sum_{n=0}^{N} a_n \sum_{i=0}^{n} c_n^i (\overline{x})^{n-i} (\Delta\mathbf{x})^i$$

The mean of the random variable $\mathbf{y}$, i.e. $\overline{y} = E[\mathbf{y}] \approx E[g(\mathbf{x})]$, can then be expressed as

$$\overline{y} \approx \sum_{n=0}^{N} a_n \sum_{i=0}^{n} c_n^i (\overline{x})^{n-i} m_i \tag{8}$$

where m_i denotes the ith-order moment of the random variable $\Delta\mathbf{x}$. Given that $a_{0:N} = [a_0, a_1, ..., a_N] = c_{0:N} A_N$, equation (8) can be written in matrix notation as:

$$\overline{y} \approx a_{0:N} C_N^{\overline{x}} m_{0:N}^x \tag{9}$$

where $m_{0:N}^x$ stands for $[1, 0, m_2, ..., m_N]^T$ and $C_N^{\overline{x}}$ denotes a lower triangular matrix that, in order to reduce the computation cost, we write as $C_N^{\overline{x}} = M_N^c \odot M_N^{\overline{x}}$, where

$$M_N^c = \begin{bmatrix} c_0^0 & 0 & 0 & \cdots & 0 \\ c_1^0 & c_1^1 & 0 & \cdots & 0 \\ c_2^0 & c_2^1 & c_2^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_N^0 & c_N^1 & c_N^2 & \cdots & c_N^N \end{bmatrix},$$

$$M_N^{\overline{x}} = \begin{bmatrix} \overline{x}^0 & 0 & 0 & \cdots & 0 \\ \overline{x}^1 & \overline{x}^0 & 0 & \cdots & 0 \\ \overline{x}^2 & \overline{x}^1 & \overline{x}^0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \overline{x}^N & \overline{x}^{N-1} & \overline{x}^{N-2} & \cdots & \overline{x}^0 \end{bmatrix}$$

and $\odot$ is the Hadamard product form.

In this way, we can reduce computational burden as M_N^c is a constant matrix and for $M_N^{\overline{x}}$, we only build its $(N+1)$th-row : $R_N = \left[\overline{x}^N, \overline{x}^{N-1}, ..., \overline{x}^0\right]$ and then we truncate this vector to obtain the other rows of matrix $M_N^{\overline{x}}$.

The term $(\mathbf{y} - \overline{y})$ can also be approximated by a polynomial function whose vector of polynomial coefficients is: $b_{0:N} = [a_0 - \overline{y}, a_1, a_2, ..., a_N]$, so that, for $n > 1$, the nth-order approximated central moment of the transformed variable $\mathbf{y}$, i.e. $E[(\mathbf{y} - \overline{y})^n]$, is expressed by the expected value of the polynomial approximating $(\mathbf{y} - \overline{y})^n$:

$$E[(\mathbf{y} - \overline{y})^n] \approx E\left[\left(g(\mathbf{x}) - \overline{g(x)}\right)^n\right] = V_{0:nN}\left(M_{nN}^c \odot M_{nN}^{\overline{x}}\right) m_{0:nN}^x \tag{10}$$

whose coefficients vector noted $V_{0:nN}$ is obtained by means of Algorithm 1:

Algorithm 1:
$V_{0:nN} = b_{0:N}$
for $i = 1$ to $n-1$ do
    $V_{0:nN} = Conv(V_{0:nN}, b_{0:N})$
end for

where *Conv* stands for convolution (i.e. polynomial multiplication). Algorithm 1 has to be used to find the vector $V_{0:nN}$ needed to calculate the variance $P_{yy} \approx E\left[(\mathbf{y} - \overline{y})^2\right]$. Thus, from (10) we have

$$P_{yy} = V_{0:2N}\left(M_{2N}^c \odot M_{2N}^{\overline{x}}\right) m_{0:2N}$$

Moreover, as it is easy to observe that the term $(\mathbf{x} - \overline{x})(\mathbf{y} - \overline{y})$ is an $(N+1)$-order polynomial function, it is sufficient only to find its coefficient vector to calculate the covariance P_{xy}. As we have shown, closed-form solutions for moment propagation can be derived and expressed in vector-matrix notation, given a Chebyshev series expansion of a system, which allows a computationally efficient implementation. In the next section we employ these moments propagation expressions in a Kalman filter framework in order to (demodulating the signal of a CD3S) obtain a Gaussian estimator of a CD3S system.

Before moving to the next section, let us just recall the basic philosophy of the CPKF. Let us consider the following nonlinear non polynomial model:

$$\begin{cases} x_{k+1} &= f(x_k) + \eta_{k+1} \\ y_k &= h(x_k) + \mu_k \end{cases} \tag{11}$$

where $f(\cdot)$ is a nonlinear non-polynomial function, which is approximated with Chebyshev polynomials of a suitable order N (see eq. (5)) in case of CPKF, and $h(\cdot)$ is the measurement function. Moreover, the dynamical noise η_{k+1} and measurement noise μ_k are independent Gaussian random variables with probability density function, $\mathcal{N}(0, Q)$ and $\mathcal{N}(0, R)$, respectively (in the previous part of this paper random variables were indicated in bold, while in the following part we avoid to use bold face to denote random variables since we specify the related probability density function and there is no risk of confusion).

Known the value y_k at the receiver, the Kalman Filter (KF, for short) constructs a *posterior* state estimate $\widehat{x}_{k+1/k+1}$ of the original signal x_{k+1}. The structure of the

Kalman observer needs to estimate the mean, the variance and the covariance of the stochastic variables. Thus, according to the nonlinear non-polynomial model (11), the equations of the recursive KF are derived as:

$$\begin{cases} \widehat{x}_{k+1/k+1} &= \widehat{x}_{k+1/k} + K_{x_{k+1}} \left(y_{k+1} - \widehat{y}_{k+1/k} \right) \\ P_{x_{k+1/k+1}} &= P_{x_{k+1/k}} - K^2_{x_{k+1}} P_{y_{k+1/k}} \\ K_{x_{k+1}} &= \frac{P_{x_{k+1/k} y_{k+1/k}}}{P_{y_{k+1/k}}} \end{cases} \quad (12)$$

where

$$\widehat{x}_{k+1/k} = E\left[f(x_k) + \eta_{k+1} \right] \quad (13)$$

$$\widehat{y}_{k+1/k} = E\left[h\left(\widehat{x}_{k+1/k} \right) + \mu_{k+1} \right] \quad (14)$$

$$P_{y_{k+1/k}} = E\left[\left(y_{k+1} - \widehat{y}_{k+1/k} \right)^2 \right] \quad (15)$$

$$P_{x_{k+1/k}} = E\left[\left(x_{k+1} - \widehat{x}_{k+1/k} \right)^2 \right] \quad (16)$$

$$P_{x_{k+1/k}, y_{k+1/k}} = E\left[\left(x_{k+1/k} - \widehat{x}_{k+1/k} \right) \left(y_{k+1} - \widehat{y}_{k+1/k} \right) \right] \quad (17)$$

3. CD3S COMMUNICATION SYSTEMS

The design of communication systems based on chaos is an increasingly active area of research. Indeed, several interesting features of chaos signals (namely, sensitivity to initial conditions, uncorrelation, aperiodicity) make them valuable candidates as building blocks for secure and reliable communications. In particular, the large band characteristics of chaotic signals can be exploited in order to modulate baseband signals to be transmitted into spread spectrum ones, which constitute a key component of many digital communication systems [8]. A widely adopted approach to chaos based communication is represented by the so called CD3S systems, where chaos based sequences are directly multiplied to the information signals to be transmitted on the channel. On the receiver side, the knowledge (to some degree) of the structure of the transmitter enables to recover, through proper demodulation, the original signal. In general, the adoption of chaos based signals is considered as a valuable alternative to the use of pseudo-noise sequences in direct sequence spread spectrum communications, sharing with the latter some properties useful for enabling spread spectrum techniques, while providing higher security levels, such as low probability of intercept [9].

According to the scientific literature, the use of chaotic sequences in digital communication can be traced back to the work of Pecora and Carrol in 1990, who demonstrated the synchronization of two coupled chaotic systems [7]. Since then, a huge body of research has flourished aimed at investigating both theoretical and practical issues towards the direction of designing chaos based digital systems. For instance, [10] introduced a CD3S system for underwater communication. In this work a solution for demodulating the signal without exact knowledge of the chaotic spreading sequence (also termed code) was proposed by means of a dual UKF formulation which enables the simultaneous estimation of spreading sequence and original transmitted symbols. Luca *et al.* studied how to exploit UKF to deal with carrier phase recovery in CD3S systems [11] while the performances achieved by UKF have been further explored by comparing it with an exact Kalman filter approach [12]. A related issue regards security in chaos based communication systems. In fact, several works have been proposed with the aim of investigating the security levels guaranteed by these schemes. For instance, methods for breaking CD3S communications with different knowledge of the transmitter/receiver structure were introduced in recent years [13, 14].

Figure 1 reports an example of three signals at different levels of a typical CD3S system. In particular, Figure 1 (a) refers to a message to be transmitted (i.e. a sequence of binary symbols), Figure 1 (b) represents a chaotic sequence (also denoted as code) generated by a chaotic map (namely a piecewise linear map as detailed below) and Figure 1 (c) is the product of the first two signals.

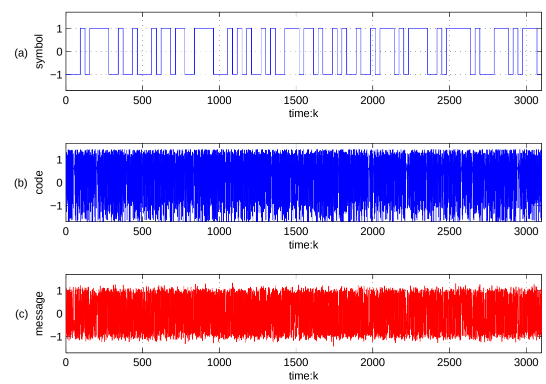

Fig 1: CD3S communication signals, (a) binary information symbols, (b) chaotic spreading sequence, (c) the transmitted CD3S signals.

As already remarked, we need a function defined in a compact interval, with chaotic dynamics. It is well known that in other works several authors use the logistic function $F(x) = \mu x(1-x)$, however, in the logistic map the sequences are chaotic in one interval or cyclical intervals only at particular values of the parameter μ, corresponding to homoclinic bifurcations, which (although of positive measure in the interval $[3.5, 4]$) are not structurally stable, and destroyed under parameter variation. Instead, we consider the one-dimensional piecewise linear map f given by two linear functions and defined as:

$$f : x \mapsto f(x) = \begin{cases} f_L(x) = s_L x + b, & x \leq 0 \\ f_R(x) = -s_R x + b, & x \geq 0 \end{cases} \quad (18)$$

where s_L and s_R are positive parameters associated with the slopes of the linear branches of the function which is the so-called skew-tent map. The rich dynamics of this map has already been studied by many authors (see, e.g., [15], [16], [17], [18], [19]). The case here considered, increasing/decreasing with maximum in b, is topologically conjugate to the case decreasing/increasing with minimum in $-b$, which also can be equivalently considered. The particular case with $s_L = s_R$ is the well known tent map. As we are interested to the cases in which the map is chaotic, we consider the ranges $s_L > 1$ and $s_R > 1$. The peculiarity of this map is that the chaotic regime is structurally stable, or robust, following the definition given in [20]. That is, the chaotic sequences are persistent under parameter perturbation, which is a useful property required for transmission security. In our simulations we consider the map f defined in (18) assuming the slopes as follows:

$$s_R = 2 \text{ and } s_L \in [1,2]$$

in order to have chaotic dynamics bounded in the interval $[-b, b]$. In particular, to obtain the results shown in Fig. 3 we have fixed $s_L = 2$ and $b = 1$.

It is worth to note that this choice is the result of a deep investigation. In fact, we also tried to use a piecewise smooth function linear-logistic, and also a bimodal function with chaotic dynamics and others. However, all the alternatives have the same disadvantage of the logistic function $F(x)$. That is, as described above, with these functions the chaotic sequences are not robust, and their performance in our system is worse with respect to the one obtained with map f defined in (18).

3.1. Dual estimation approach using CPKF

The dual Kalman filtering scheme requires only the noisy observation y_{k+1} as input to activate the two Kalman filters involved and it allows to estimate simultaneously, at chip frequency (or chip rate) f_s, the original chaotic spreading sequence (or code) s_k and the data symbol b_k. In particular, the filter that estimates s_{k+1} requires and treats the last estimated $\widehat{b}_k$ as a parameter, while the filter that estimates b_{k+1} requires and considers $\widehat{s}_k$ as a parameter, where $\widehat{s}_k$ and $\widehat{b}_k$ are estimated from the observed state y_k, see fig. 2. Then, the dynamical model and the observation model used for code estimation are given by the following equations:

$$\begin{cases} s_{k+1} &= f(s_k) + \upsilon^s_{k+1} \\ y_{k+1} &= sgn(\widehat{b}_k) s_{k+1} + \eta_{k+1} \end{cases} \tag{19}$$

where $f(\cdot)$ denotes the chaotic function given in equation (18), $\upsilon^s_{k+1} \sim \mathcal{N}(0, Q_s)$ indicates the Gaussian system noise which is independent of the past and current state s_k and reflects the model uncertainty due to channel imperfections, and $\eta_{k+1} \sim \mathcal{N}(0, R)$ represents the Gaussian measurement noise at time point $k+1$ and it depends upon the signal and noise levels at the receiver input.

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

$$\begin{cases} b_{k+1} &= b_k + \upsilon^b_{k+1} \\ y_{k+1} &= b_{k+1} f(\widehat{s}_k) + \eta_{k+1} \end{cases} \tag{20}$$

where $\upsilon^b_{k+1} \sim \mathcal{N}(0, Q_b)$ is the Gaussian system noise which is independent of the past and current state b_k. This noise influences the adaptability of the filter of the symbol. In particular, a low value of Q_b will result in slow changes whereas a large value will result in rapid variations of the symbol estimates. It is worth noticing that we assume $E[\eta_{k+1} s_{k+1}] = E[\eta_{k+1} b_{k+1}] = 0$.

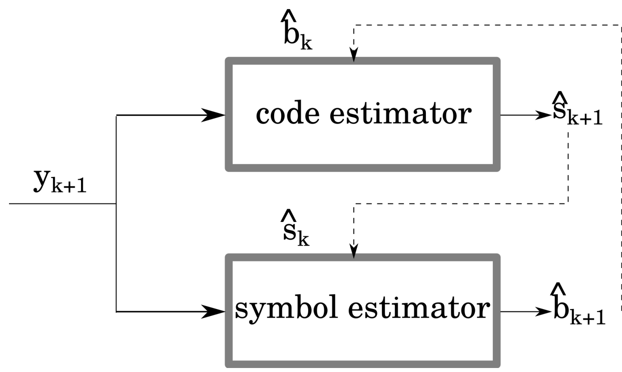

Fig 2: Code/Symbol Dual Estimation Block for the Chebyshev Polynomial Kalman Filter.

Given the model represented by systems (19) and (20) and the observation y_{k+1}, the KF constructs an estimated state $\hat{s}_{k+1/k+1}$ and $\hat{b}_{k+1/k+1}$ at the receiver. In doing so, it requires to estimate the mean, the variance and the covariance of the stochastic variables s_{k+1} and y_{k+1}. Then, in order to have a closed-form KF, first the function $f(\cdot)$ must be approximated with Chebyshev polynomials as described in the previous section (it is worth to point out that in the numerical simulation of the next section Chebyshev polynomials up to order 10 are used in fitting $f(\cdot)$).

Thus, according to the nonlinear non polynomial model (19), the equations of the recursive KF are as follows

$$\begin{cases} \widehat{s}_{k+1/k+1} &= \widehat{s}_{k+1/k} + K_{s_{k+1}} \left(y_{k+1} - \widehat{y}_{k+1/k} \right) \\ P_{s_{k+1/k+1}} &= P_{s_{k+1/k}} - K^2_{s_{k+1}} P_{y_{k+1/k}} \\ K_{s_{k+1}} &= \frac{P_{s_{k+1/k} y_{k+1/k}}}{P_{y_{k+1/k}}} \end{cases} \tag{21}$$

where (noting that b_k is considered as a parameter and following the algebraic manipulation as indicated in (9) of the previous section),

$$\begin{aligned}
\widehat{s}_{k+1/k} &= E\left[f(s_k)+\upsilon^s_{k+1}\right] = E\left[f(s_k)\right] \\
&\approx E\left[\sum_{j=0}^{N} c_j T_j(s_k) - \frac{1}{2}c_0\right] \\
&= a_{0:N}\left(M^c_N \odot M^{\widehat{s}}_N\right) m^s_{0:N} \qquad (22) \\
\widehat{y}_{k+1/k} &= E\left[sign\left(\widehat{b}_k\right) s_{k+1} + \eta_{k+1}\right] \\
&= sign\left(\widehat{b}_k\right) E\left[s_{k+1}\right] \\
&= sign\left(\widehat{b}_k\right) \widehat{s}_{k+1/k} \qquad (23) \\
P_{s_{k+1/k}} &= E\left[\left(s_{k+1}-\widehat{s}_{k+1/k}\right)^2\right] \\
&= conv\left(b_{0:N}, b_{0:N}\right)\left(M^c_{2N}\odot M^{\widehat{s}}_{2N}\right) m^s_{0:2N} + Q_s \qquad (24)
\end{aligned}$$

with

$$b_{0:N} = a_{0:N} - \widehat{s}_{k+1/k}\left[1,0,...,0\right]_{0:N} \qquad (25)$$

and

$$\begin{aligned}
P_{s_{k+1/k}y_{k+1/k}} &= E\left[\left(s_{k+1}-\widehat{s}_{k+1/k}\right)\left(y_{k+1}-\widehat{y}_{k+1/k}\right)\right] \\
&= E\left[\left(s_{k+1}-\widehat{s}_{k+1/k}\right) sign\left(\widehat{b}_k\right)\left(s_{k+1}-\widehat{s}_{k+1/k}\right)\right] \\
&= sign\left(\widehat{b}_k\right) P_{s_{k+1/k}} \qquad (26) \\
P_{y_{k+1/k}} &= E\left[\left(y_{k+1}-\widehat{y}_{k+1/k}\right)^2\right] \\
&= sign\left(\widehat{b}_k\right)^2 E\left[\left(s_{k+1}-\widehat{s}_{k+1/k}\right)^2\right] + E\left[\left(\eta_{k+1}\right)^2\right] \\
&= sign\left(\widehat{b}_k\right)^2 P_{s_{k+1/k}} + R \qquad (27)
\end{aligned}$$

In the algebraic manipulations we have used the property $E\left[\eta_{k+1}s_{k+1}\right] = 0$.

Moreover, to estimate the binary information symbol b_{k+1} one has the model described by equation (20). In this case, $\widehat{s}_k$ is considered as a parameter, so no approximation of the piecewise linear function $f(\cdot)$ is required. The model is linear and the equations of the recursive KF are as follows:

$$\left\{\begin{array}{lcl}
\widehat{b}_{k+1/k+1} &=& \widehat{b}_{k+1/k} + K_{b_{k+1}}\left(y_{k+1}-\widehat{y}_{k+1/k}\right) \\
P_{b_{k+1/k+1}} &=& P_{b_{k+1/k}} - K^2_{b_{k+1}} P_{y_{k+1/k}} \\
K_{b_{k+1}} &=& \frac{P_{b_{k+1/k}y_{k+1/k}}}{P_{y_{k+1/k}}}
\end{array}\right. \qquad (28)$$

where

$$\begin{aligned}
\widehat{b}_{k+1/k} &= E\left[b_k + \upsilon^b_{k+1}\right] = \widehat{b}_{k/k} \qquad (29) \\
\widehat{y}_{k+1/k} &= E\left[b_{k+1}f(\widehat{s}_k)+\eta_{k+1}\right] = f(\widehat{s}_k)\,\widehat{b}_{k+1/k} \qquad (30) \\
P_{b_{k+1/k}} &= E\left[\left(b_{k+1}-\widehat{b}_{k+1/k}\right)^2\right] = P_{b_{k/k}} + Q_b \qquad (31) \\
P_{b_{k+1/k}y_{k+1/k}} &= E\left[\left(b_{k+1}-\widehat{b}_{k+1/k}\right)\left(y_{k+1}-\widehat{y}_{k+1/k}\right)\right] \\
&= f(\widehat{s}_k)\,E\left[\left(b_{k+1}-\widehat{b}_{k+1/k}\right)^2\right] = f(\widehat{s}_k)\,P_{b_{k+1/k}} \qquad (32) \\
P_{y_{k+1/k}} &= E\left[\left(y_{k+1}-\widehat{y}_{k+1/k}\right)^2\right] = \left(f(\widehat{s}_k)\right)^2 P_{b_{k+1/k}} + R \qquad (33)
\end{aligned}$$

In the algebraic manipulations we have used the property $E\left[\eta_{k+1}b_{k+1}\right] = 0$.

3.2. Numerical simulations

In this section we describe the numerical simulations we used for evaluating the proposed approach based on CPKF when applied to a CD3S system. We compared the CPKF demodulation algorithm with the UKF-based solution under different values of the Eb/N0 ratio, taking the BER as a comparison metric. This benchmarking is commonly adopted in order to evaluate the performance of a communication system.

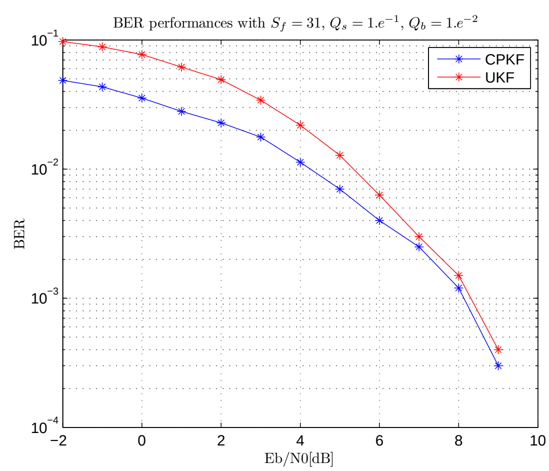

Fig 3: BER (bit-error-rate) performances for Unscented Kalman Filter (UKF) and Chebyshev Polynomial Kalman Filter (CPKF).

In particular, we generated a pseudo-random sequence of N bits, representing the symbols to be transmitted. This message was then multiplied with a chaotic carrier generated by means of the piecewise linear map with a given spreading factor S_f. After adding system noise $\mathcal{N}(0,Q_s)$ and measurement noise $\mathcal{N}(0,Q_b)$, the resulting signal was properly demodulated and the number of correctly recovered bits counted. The whole process has been repeated for values of Eb/N0 ranging from -2dB to 9dB, with increasing unitary step. Figure 3 reports the obtained BER curves for both the compared approaches. Each point is the average of 5 independent runs. Experiments have been done with the following parameters: $N = 10^5$, $Q_b = 10^{-2}$, $Q_s = 10^{-1}$, $S_f = 31$. The lower error level of the proposed CPKF method is apparent over the whole range of Eb/N0. In particular, CPKF shows higher accuracy for low Eb/N0 levels, while the different between the two methods becomes less marked for $Eb/N0 \geq 6$dB.

4. CONCLUSION

In this paper, we used the Chebyshev Polynomial Kalman Filter method proposed in [5] and [6] in the dual Kalman filtering scheme to achieve pseudo blind demodulation of the signal generated through a CD3S communication system. The performance of this new method in terms of BER has been compared to traditional and popular Unscented Kalman Filter for different values of Eb/N0. The Monte Carlo simulations show a significant reduction in the BER when we retrieve the signal generated by a CD3S communication systems using a dual Kalman filter based on the Chebyshev Polynomial Kalman Filter method. In particular, the numerical analysis reveals that the Chebyshev Polynomial Kalman Filter is particular efficient in reducing the BER when the Eb/N0 ratio is relatively small, i.e. when the noise is preponderant respect to the signal. This gives a clear indication of the suitability of the method for demodulating signals in CD3S applications.

ACKNOWLEDGMENTS

The authors are grateful to Prof. Federico Bizzarri (Politecnico di Milano) for his valuable advices during the preparation of this article and for his helpful comments on early drafts of it.

REFERENCES

[1] Z. Wu, H. Su, and J. Chu, "Delay-dependent filtering for singular markovian jump time-delay systems," *Signal Processing*, vol. 90, no. 6, pp. 1815 – 1824, 2010.

[2] Z. Wu, P. Shi, H. Su, and J. Chu, "Asynchronous filtering for discrete-time stochastic markov jump systems with randomly occurred sensor nonlinearities," *Automatica*, vol. 50, no. 1, pp. 180 – 186, 2014.

[3] S. Julier, J. Uhlmann, and H. F. Durrant-Whyte, "A new method for the nonlinear transformation of means and covariances in filters and estimations," *IEEE Transactions and Automatic Controls*, vol. 45, no. 3, pp. 477–482, 2000.

[4] M. Luca, G. B. S. Azou, and A. Serbanescu, "On exact kalman filtering of polynomial systems," *IEEE Transactions on Circuits and Systems I*, vol. 53, no. 6, pp. 1329–1340, 2006.

[5] M. Yahia, P. Acco, and M. Benslama, "Estimation of nonlinear systems via a chebyshev approximation approach," *International Journal of Control, Automation, and Systems*, vol. 9, no. 6, pp. 1021–1027, 2011.

[6] M. F. Huber, "Chebyshev polynomial kalman filter," *Digital Signal Processing*, vol. 23, no. 5, pp. 1620–1629, 2013.

[7] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[8] F. C. M. Lau and K. T. Chi, *Chaos-based digital communication systems: Operating principles, analysis methods, and performance evaluation*. Springer, 2003.

[9] J. Yu and Y. D. Yao, "Detection performance of chaotic spreading lpi waveforms," *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 390–396, 2005.

[10] S. Azou, G. Burel, and C. Pistre, "A chaotic direct-sequence spread-spectrum system for underwater communication," *Proc. of MTS/IEEE OCEANS '02*, vol. 4, pp. 2409–2415, 2002.

[11] M. B. Luca, S. Azou, G. Burel, and A. Serbanescu, "A complete receiver solution for a chaotic direct-sequence spread spectrum communication system," *Proc. of IEEE International Symposium on Circuits and Systems (ISCAS 2005)*, pp. 3813–3816, 2005.

[12] M. B. Luca, S. Azou, E. Hodina, A. Serbanescu, and G. Burel, "Pseudo-blind demodulation of chaotic ds-ss signals through exact kalman filtering," *Proc. of IEEE-Communications 2006*, pp. 1–4, 2006.

[13] H. JinFeng and G. JingBo, "Breaking a chaotic secure communication scheme," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 1, p. 013121, 2008.

[14] G. Lu and X. Bo, "Breaking a chaotic direct sequence spread spectrum communication system using interacting multiple model-unscented kalman filter," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 22, no. 4, p. 043122, 2012.

[15] S. Ito, S. Tanaka, and H. Nakada, "On unimodal transformations and chaos II," *Tokyo Journal of Mathematics*, vol. 2, pp. 241–259, 1979.

[16] F. Takens, *Transitions from periodic to strange attractors in constrained equations, In Dynamical Systems and Bifurcation Theory, Camacho M I, Pacifico MJ and Takens F, Research Notes in Mathematis Series. 160.* Pitman: Longman Scientific and Techical, 1987.

[17] V. M. Y.L. Maistrenko and L. Chua, "Cycles of chaotic intervals in a time-delayed chua's circuit," *International Journal of Bifurcation and Chaos*, vol. 3, pp. 1557–1572, 1993.

[18] H. E. Nusse and J. A. Yorke, "Border-collision bifurcations for piecewise smooth one-dimensional maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 5, no. 1, pp. 189–207, 1995.

[19] I. Sushko and L. Gardini, "Degenerate bifurcations and border collisions in piecewise smooth 1d and 2d maps," *International Journal of Bifurcation and Chaos*, vol. 20, pp. 2045–2070, 2010.

[20] S. Banerjee, J. Yorke, and C. Grebogi, "Robust chaos," *Phys Rev Lett*, vol. 80, pp. 3049–3052, 1998.

Moussa Yahia was born in Fej-M'zala, Jijel, Algeria. He received his Ph.D. degree in Electronics from the University of Constantine 1, Algeria. Currently, he is an Assistant professor in Department of Electronics, University of Jijel, Algeria. His research activities concern nonlinear signal processing, secure communications relying on chaotic dynamics.

Davide Radi received the B.S. degree in information technology management for business and the M.Sc. degree in economics from the University of Urbino Carlo Bo, Urbino, Italy, in 2007 and 2010, respectively, and the D.Phil. degree in economics, applied mathematics and operational research from the University of Bergamo, Bergamo, Italy, in 2014. His current position is with Marche Polytechnic University, Ancona, Italy. His research interests include nonlinear dynamical systems and their applications.

Laura Gardini. Born in Ravenna, Italy, in 1952, she graduated in mathematics in 1975 at the University of Bologna. She worked as a researcher for the ENI group, and became a Universitary Resercher in 1988. Full professor of Mathematics for Economics and Social Sciences since 1994, she now lives and works in Urbino. Her research interests are Discrete Dynamical Systems and their applications to the modeling of Economic, Financial, Social, Biological, Engineering and Physical systems. The main results have been obtained in the global properties of noninvertible maps, homoclinic bifurcations, dynamics and bifurcations of piecewise-smooth and discontinuous systems.

Valerio Freschi graduated in Electrical Engineering at University of Ancona (Italy) in 1999 and received the PhD in Computer Science Engineering from University of Ferrara (Italy) in 2006. Since 2009 he is Assistant Professor in the Department of Basic Sciences and Foundations (DiSBeF) at University of Urbino, Italy. His research interests include wireless embedded systems, sensor networks, graph algorithms, bioinformatics, optimization.