# Secure Communications Using OFDM with Chaotic Modulation in the Subcarriers

David Luengo
Dep. Teoría de la Señal y Comunicaciones
Universidad Carlos III de Madi
Leganés, Madrid 28911 (Spain)
Email: luengod@ieee.org

Ignacio Santamaría
Dep. Ingeniería de Comunicaciones
Universidad de Cantabria
Santander, Cantabria 39005 (Spain)
Email: nacho@gtas.dicom.unican.es

*Abstract*— **Chaotic sequences may be advantageous for secure communications. Although many chaotic communications systems have been proposed, most of them show a poor performance under realistic channel conditions (i.e. noise and multipath fading). In this paper, we propose a novel chaotic modulation scheme based on the symbolic sequence associated to the chaotic map and backward iteration. These chaotically modulated signals are then sent in each sub-carrier of a conventional OFDM system instead of the usual BPSK or QAM ones. In the receiver, equalization is performed in the frequency domain, and the Viterbi algorithm is used to estimate the transmitted sequence. Computer simulations confirm the good performance of the proposed approach.**

## I. Introduction

Chaotic systems generate signals which are purely deterministic, although they show features typical of random signals due to the numerical instability of the system (i.e. sensitivity to initial conditions). In a signal processing context, chaotic signals and systems have been proposed for a wide range of applications: communications, watermarking, cryptography, time series modeling, etc. (see for example [1]).

Many different chaotic communications systems have been proposed: chaotic modulation, chaotic masking, chaos shift keying (CSK) and its variants, spread spectrum techniques, etc. (see [2], [3] for a review). In this paper, we focus on chaotic modulation techniques (i.e. using chaotic signals as basis functions instead of sinusoids), and propose a novel chaotic modulation scheme based on the symbolic sequence associated to the chaotic map and backward iteration.

This modulation technique shows good performance under noisy conditions, but can suffer severe degradation in channels with multipath distortion and selective fading. In order to avoid this problem, we consider an OFDM communications system which sends the chaotically modulated signals in each subcarrier, instead of the usual PSK or QAM signals. Although a conventional modulation achieves a better performance in terms of bit error rate (BER), the proposed chaos-based scheme is advantageous in terms of secure communications: the BER of an eavesdropper without a perfect knowledge of the parameters of the chaotic system is highly deteriorated. Moreover, we explore a class of chaotic maps with a control parameter which allows us to trade performance (i.e. BER) and security (i.e. chaotic behaviour) in a natural way.

The key element of the system is the implementation of the receiver. Maximum Likelihood (ML) and Bayesian (Maximum A Posteriori (MAP) and Minimum Mean Square Error (MMSE or MS)) estimators have been developed for chaotic sequences in [4] and [5] respectively. However, their computational cost grows exponentially with the length of the sequence, rendering them impractical even for signals of moderate length.

Although many suboptimal algorithms have been proposed (see for example [6]–[9]), their performance is far from that of ML and Bayesian estimators, specially when the signal to noise ratio (SNR) is low. In this paper, we use the Viterbi decoding algorithm to detect the transmitted sequence. In spite of being a suboptimal method in this case, the Viterbi algorithm shows a performance which is close to the exact ML estimator with a fraction of its computational cost.

Note that the use of the Viterbi algorithm for estimating chaotic sequences has already been proposed by Ciftci and Williams in [10] and [11]. However, their approach relies on a linear filter representation of the chaotic system which is not always possible, requires delay and truncation (thus generating pseudochaotic signals, which may lose some of the interesting characteristics of chaotic signals) and a trellis with a large number of states. On the other hand, our approach is able to generate truly chaotic signals, since it is based on backward iteration of the system, is valid for any chaotic map, and uses a trellis with a reduced number of states.

The remainder of the paper is organised as follows. The class of chaotic maps used is presented in Section II, altogether with an introduction to symbolic dynamics. Then, in Section III, the structure of the chaotic modulator and demodulator is described, followed by the block diagram and details of the proposed novel OFDM system, shown in Section IV. Finally, simulation results are given in Section V, and concluding remarks close the paper in Section VI.

## II. Chaotic Maps and Symbolic Dynamics

In this work we consider sequences generated by unidimensional chaotic maps. The $n$-th sample of the sequence is obtained iterating a known initial condition, $x[0]$, according to

$$x[n] = f(x[n-1]) = f^2(x[n-2]) = \ldots = f^n(x[0]), \quad (1)$$

0-7803-8887-9/05/$20.00 (c)2005 IEEE

where $f(x)$ is any suitable nonlinear and noninvertible function, $f^k(x)$ denotes the $k$-th functional composition of $f(x)$, and $1 \leq n \leq N$. Although the modulation technique proposed in the sequel can be put into practice with any nonlinear function, in this paper we use the following chaotic map:

$$f(x) = \begin{cases} \frac{2x+(1+p)}{1-p}, & -1 \leq x \leq -p; \\ \frac{x}{p}, & -p < x < p; \\ \frac{2x-(1+p)}{1-p}, & p \leq x \leq 1. \end{cases} \quad (2)$$

Being $p$ a control parameter of the map, $0 \leq p < 1$. Fig. 1 shows the chaotic map for $p = 0.1$. The parameter $p$ controls the width of the middle region of the map, which in turn determines the slope in each interval, and ultimately the chaotic behaviour of the sequences generated.

The reason for using the chaotic map given by (2) is that it offers an adjustable guard region, which allows us to trade performance for security. This guard band appears because the proposed communications system shown in Section III uses only the two external intervals of the map (i.e. $p \leq |x| \leq 1$). Hence, as $p$ increases the allowed signal range decreases, and the distance between the permitted intervals grows. Thus it becomes easier to distinguish samples that belong to $E_1$ from samples that belong to $E_3$, even in noisy conditions. Overall this leads to a better performance of the system shown in the next section, but also to a lower level of security.

It is not easy to guarantee that a chaotic sequence does not belong to the inner interval when it is generated using (2) according to (1). We need to know beforehand the length of the sequence, $N$, to ensure that none of the iterations of $x[0]$ falls within $(-p, p)$. This restriction is better achieved using backward iteration, i.e. generating the chaotic signal starting from a final condition, $x[N]$, instead of an initial condition, $x[0]$. Unidimensional chaotic maps are never invertible, but they always have a finite number of preimages, which allows us to define an inverse map.

A necessary tool for defining the inverse function is *symbolic dynamics*. For any function we can define a partition of its phase space into a set of nonoverlapping intervals where it is continuous and monotonous in such a way that they cover its whole phase space. This partition is never unique, but we can always find the simplest possible partition, which is called the *natural* or *generating partition* of the map. For (2) it is obvious that $M = 3$, $E_1 = [-1, \ -p]$, $E_2 = (-p, \ p)$, and $E_3 = [p, \ 1]$. Now, it is possible to define the *symbolic sequence* or *itinerary* of the map as the sequence of regions of the generating partition that the chaotic signal visits during its time evolution:

$$s[n] = i \Leftrightarrow x[n] \in E_i, \qquad n = 0, \ \ldots, \ N. \quad (3)$$

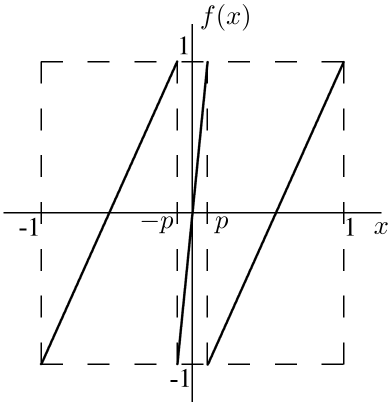

Fig. 1. Nonlinear map used to generate the chaotic sequences ($p = 0.1$).

For piecewise linear (PWL) maps, such as (2), it can be easily shown that each point in their phase space has a unique symbolic sequence of length $N$ associated, and that an itinerary of infinite length defines a single initial condition [12]. Therefore, the symbolic sequence provides the means of generating the chaotic signal iterating backwards:

$$x[n] = f^{-1}_{s[n]}(x[n+1]) = \ldots = f^{-(N-n)}_{s[n], \ \ldots, \ s[N-1]}(x[N]). \quad (4)$$

Where $f^{-1}_{s[n]}$ denotes the inverse map, and $f^{-(N-n)}_{s[n], \ \ldots, \ s[N-1]}$ denotes the functional composition of $f^{-1}$ with itself $N - n$ times. For the map given in (2) the inverse map is

$$f^{-1}_s(x) = \begin{cases} \frac{(1-p)x-(1+p)}{2}, & s = 1; \\ px, & s = 2; \\ \frac{(1-p)x+(1+p)}{2}, & s = 3. \end{cases} \quad (5)$$

Generating the samples of the chaotic sequence iterating backwards from a known $x[N]$ according to (4) using (5) allows us to easily restrict them not to belong to $E_2$ (simply not using $s[n] = 2$), avoids some of the problems associated to the numerical instability characteristic of chaotic sequences (error amplification and precision truncation of direct forward iteration), and suggests the structure of the chaotic modulator described in the next section.

## III. Chaotic Communications System

The structure of the whole chaotic communications system considered is shown in Fig. 2. The input bits are fed into a chaotic modulator with pre-assigned parameters $p$ and $x[N]$, which generates the baseband transmitted signal, $\tilde{x}[n]$. This chaotic sequence then passes through the channel, composed of a linear time-invariant (LTI) filter and additive white Gaussian noise (AWGN), resulting in a received signal $\tilde{y}[n]$. Finally, the chaotic demodulator tries to obtain the best estimate (i.e. the one with the minimum probability of error) of the transmitted bits. In this section we show an efficient implementation of the modulator and the demodulator.

### A. Chaotic Modulator

Suppose that we have a sequence of input bits, $\mathbf{b} = [b[1], \ \ldots, \ b[N]]^T$, that we want to transmit using a chaotic signal. The main idea of the proposed chaotic modulator is to iterate backwards from a known final condition, $x[N]$, using the input bits to construct the symbolic sequence as

$$\tilde{s}[n] = s[N-n] = 1 + 2b[n], \qquad 1 \leq n \leq N. \quad (6)$$

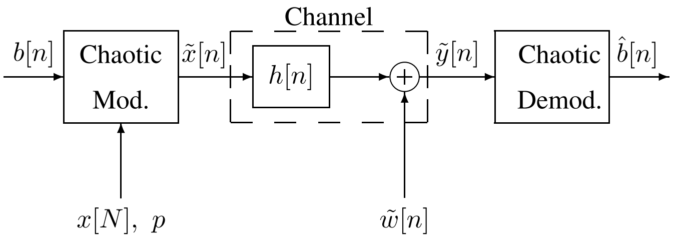

Fig. 2. Baseband chaotic communications system: modulator, channel, and demodulator.

Consequently, the signals generated can only belong to the external regions, $E_1$ and $E_3$, and the inner region, $E_2$, is used as a guard interval to ensure a minimun distance between the waveforms associated to a zero and a one. This itinerary is used to construct the chaotic signal according to (4), using (5), resulting in a transmitted baseband sequence

$$\tilde{x}[n] = x[N-n] = f^{-1}_{\tilde{s}[n]}(\tilde{x}[n-1]), \qquad (7)$$

for $n = 1, \ldots, N$. This baseband chaotic signal can then be moved to any desired frequency band for passband transmission. Fig. 3 shows the structure of the baseband chaotic modulator, and Fig. 4 shows a typical output sequence altogether with the input bits and the auxiliar symbolic sequence.

### B. Chaotic Demodulator: Problem Statement

The received signal is

$$\tilde{y}[n] = \tilde{x}[n] * h[n] + \tilde{w}[n], \qquad 1 \leq n \leq N; \qquad (8)$$

where $\tilde{w}[n]$ is stationary, zero-mean, additive white Gaussian noise (AWGN) with variance $\sigma^2$, and '*' denotes the aperiodic discrete-time convolution operator.

Hence, the first step in the receiver consists of equalizing the channel (i.e. undoing the effects of the channel's impulse response to obtain a sequence free of the multipath distortion). Let us assume that the output of the equalizer is

$$\tilde{z}[n] = \tilde{x}[n] + \tilde{v}[n], \qquad (9)$$

where $\tilde{v}[n]$ is the filtered Gaussian noise, and $1 \leq n \leq N$. Now, the demodulator seeks the sequence of input bits (i.e. the symbolic sequence) which minimizes the probability of error. In the Gaussian case, and for equiprobable input bits, this is achieved by the maximum likelihood (ML) estimator:

$$\hat{\mathbf{b}}_{\text{ML}} = \arg\min_{\mathbf{b}} \ J(\mathbf{z}; x[N], \mathbf{b}), \qquad (10)$$

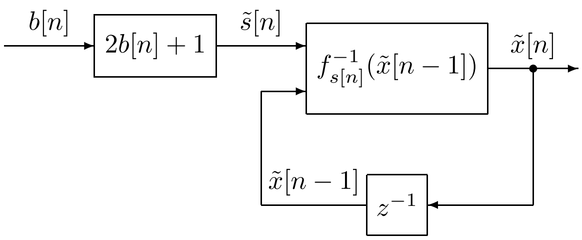

Fig. 3. Block diagram for the proposed chaotic modulator for a generic map.

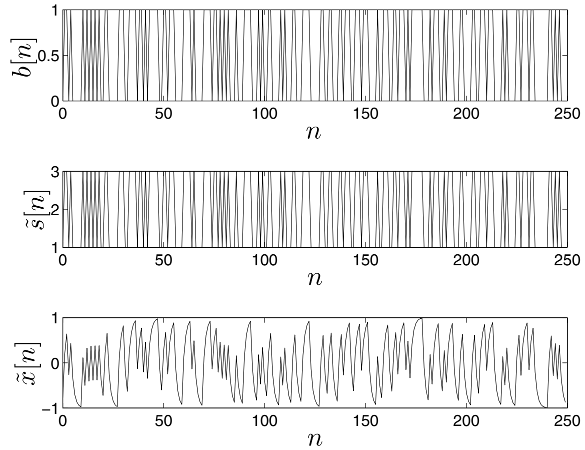

Fig. 4. Example of typical input bits sequence, $b[n]$, constructed symbolic sequence, $\tilde{s}[n]$, and baseband chaotic communications signal, $\tilde{x}[n]$.

where $\mathbf{z} = [\tilde{z}[1], \ \ldots, \ \tilde{z}[N]]^T$ is the equalized observations vector, $J(\mathbf{z}; x[N], \mathbf{b})$ is a quadratic cost function,

$$J(\mathbf{z}; x[N], \mathbf{b}) = (\mathbf{z} - \mathbf{x})^T \mathbf{C}_z^{-1} (\mathbf{z} - \mathbf{x}), \qquad (11)$$

$\mathbf{x} = [\tilde{x}[1], \ \ldots, \ \tilde{x}[N]]^T = [f^{-1}_{\tilde{s}[1]}(\tilde{x}[0]), \ \ldots, \ f^{-1}_{\tilde{s}[N]}(\tilde{x}[N-1])]^T = [f^{-1}_{\tilde{s}[1]}(\tilde{x}[0]), \ \ldots, \ f^{-1}_{\tilde{s}[1],\ldots,\tilde{s}[N]}(\tilde{x}[0])]^T$ is the transmitted vector, and $\mathbf{C}_z$ is the autocorrelation matrix of $\mathbf{z}$, which does not depend on the itinerary, and whose $(m, n)$ element is given by

$$[\mathbf{C}_z]_{m,n} = \mathrm{E}\{\tilde{z}[m]\tilde{z}[n]\}. \qquad (12)$$

Unfortunately, we cannot take the derivative of (11) with respect to each $b[n]$ to obtain their ML estimates, because $J(\mathbf{z}; x[N], \mathbf{b})$ is a discontinuous function of the itinerary, and consequently of $\mathbf{b}$. Nevertheless, since the number of possible symbolic sequences (i.e. bit sequences) is finite, a "brute force" approach is possible: test all the valid sequences and select the best one. This is the same approach that was used in [4], [5] to estimate the initial condition of the map, and in fact it is the only known way to implement exactly the ML estimator for most chaotic maps such as (2).

The ML estimator provides good results, achieving an optimum performance asymptotically as SNR → ∞ [4], [5]. However, it requires testing $2^N$ sequences, and thus becomes impractical even for moderate-sized data records. Many suboptimal algorithms have been proposed, but they typically present a poor performance in medium/low SNR range. In the next section we propose a demodulation technique based on the Viterbi algorithm which achieves a quasi-optimal performance with a reduced computational cost.

### C. Demodulation using the Viterbi Decoding Algorithm

As an efficient solution for the demodulation problem, in this paper we propose to use the Viterbi decoding algorithm (VDA) to estimate the itinerary of the chaotic sequence. It is clear that a symbolic sequence of finite length, $N$, has an exact trellis representation. However, this trellis requires $2^N$

states, since $\tilde{x}[N]$ depends on the whole symbolic sequence, and hence can take $2^N$ different values.

Therefore, using the VDA to solve exactly the problem requires a computational cost similar to the ML estimator of the previous section. As a cost-effective alternative, we propose to use a trellis with only two states and apply the VDA. Obviously this is a suboptimal method, but it provides a performance close to the optimal because previous bits become less and less important in the estimation of future ones.

As an example, consider two different samples, $\tilde{x}_1[n]$ and $\tilde{x}_2[n]$ $(0 \leq n < N)$, which share the itinerary for $k > n$ (i.e. $\tilde{s}_1[k] = \tilde{s}_2[k] = \tilde{s}[k]$ for $n+1 \leq k \leq N$). The next sample generated for $\tilde{x}_1[n]$ and $\tilde{x}_2[n]$ is given by

$$\tilde{x}_1[n+1] = \frac{(1-p)\tilde{x}_1[n] + (\tilde{s}[n+1]-2)(1+p)}{2}, \quad (13)$$

$$\tilde{x}_2[n+1] = \frac{(1-p)\tilde{x}_2[n] + (\tilde{s}[n+1]-2)(1+p)}{2}. \quad (14)$$

Now, if we define the distance between the two original samples as $d[n] = |\tilde{x}_2[n] - \tilde{x}_1[n]|$, then

$$d[n+1] = |\tilde{x}_2[n+1] - \tilde{x}_1[n+1]| = \frac{1-p}{2} d[n] < d[n]. \quad (15)$$

Hence, the distance between the original samples has decreased after one iteration, independently of their position. In fact, it can be shown by induction that the distance between both sequences decreases by a factor $(1-p)/2$ after each iteration of the map:

$$d[n+k] = \left(\frac{1-p}{2}\right)^k d[n] < d[n+k-1] < \cdots < d[n]. \quad (16)$$

This means that far away input bits have little importance in determining the current state of the system (i.e. the chaotic sequence gradually forgets its past), and that it makes sense to use a trellis diagram with a reduced set of states.

The basic butterfly of the trellis diagram is shown in Fig. 5. Assuming equiprobable symbols, the branch metrics are

$$c_{ij}[n] = |\tilde{z}[n+1] - f_j^{-1}(\hat{x}_i[n])|, \quad (17)$$

where $c_{ij}[n]$ is the cost of taking the $j$-th branch starting from the $i$-th node $(1 \leq i, j \leq 2)$ at the $n$-th time instant $(1 \leq n \leq N)$, and $\hat{x}_i[n]$ $(i \in \{1, 2\})$ is the sample obtained iterating backwards $N-n$ times from $x[N]$ using the best sequence which ends in the $i$-th node (state) at time $n$. The cost of the $i$-th node at the $(n+1)$-th instant can be obtained as usual from that of all the nodes at time $n$ as

$$C_i[n+1] = \min_{j=1,2} \{C_j[n] + c_{ji}[n]\}.$$

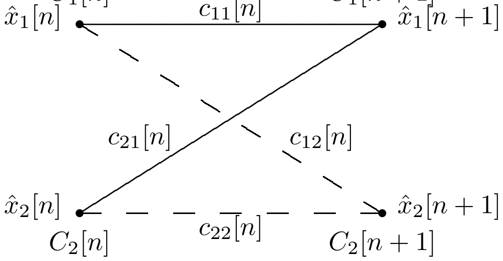

Fig. 5. Basic butterfly for the Viterbi algorithm using only two states per iteration of the chaotic sequence.

## IV. OFDM Communications System with Chaotic Modulation in the Sub-Carriers

The chaotic modulation system proposed in Section III has a good performance for the AWGN channel, i.e. flat channel's frequency response. However, it suffers from severe degradation in a multipath environment, just as most conventional and chaotic communications systems. To avoid this distortion, we combine the chaotically modulated signals with a modulation scheme which is robust against multipath interference: OFDM.

We propose to construct an OFDM system where the signals sent in each sub-carrier are chaotically modulated instead of using a conventional modulation such as PSK or QAM. The structure of the transmitter is shown in Fig. 6. The input bits are used to obtain the chaotic signal as in Fig. 3. Then, a serial to parallel conversion is performed to generate the signal corresponding to each sub-carrier, pilots and guard symbols (zeros) are inserted, and an IFFT is performed. A cyclic prefix is finally added to counter the effect of intersymbol interference (ISI), and the signal is transmitted through the channel. The receiver is simply the dual of the transmitter: removing first the cyclic prefix, performing then an FFT, equalizing the channel in the frequency domain, and estimating the transmitted bits using the VDA.

## V. Simulation Results

The performance of the chaotic OFDM system has been tested by Monte Carlo simulations in two different cases: AWGN channel and multipath channel. In both cases the system has been analyzed using the basic parameters of the HIPERLAN 2 standard: 64 carriers composed of 48 data carriers, 4 pilots and 12 guard symbols (zeros) [13], [14].

Fig. 7 shows the results for the AWGN channel and four different values of $p$, with the OFDM+BPSK system used for comparison. As $p$ is increased towards one the performance of the system approaches that of the conventional OFDM+BPSK modulation scheme. When $p$ is decreased the BER increases, but we achieve an improvement in the level of security: since the amplitude for each symbol becomes more irregular and unpredictable, an unintended user who does not know exactly the parameters of the system will see his detection capability heavily impaired. Hence, $p$ is a design parameter which allows us to balance performance and security.

In order to evaluate the performance in a multipath environment, we consider two channels: $\mathbf{h}_1 = [1,\ -0.5]^T$, and $\mathbf{h}_2 = [0,\ -0.3,\ 0.7,\ 0.4,\ 0.1]^T$. The results are shown in Fig. 8. For all the simulations we assume that the channel's frequency response has been perfectly estimated, and simply divide each subcarrier by $H(\omega)$ to equalize the received signal. For both channels the performance deteriorates slightly and similarly for both the conventional modulation scheme and the chaotic one.

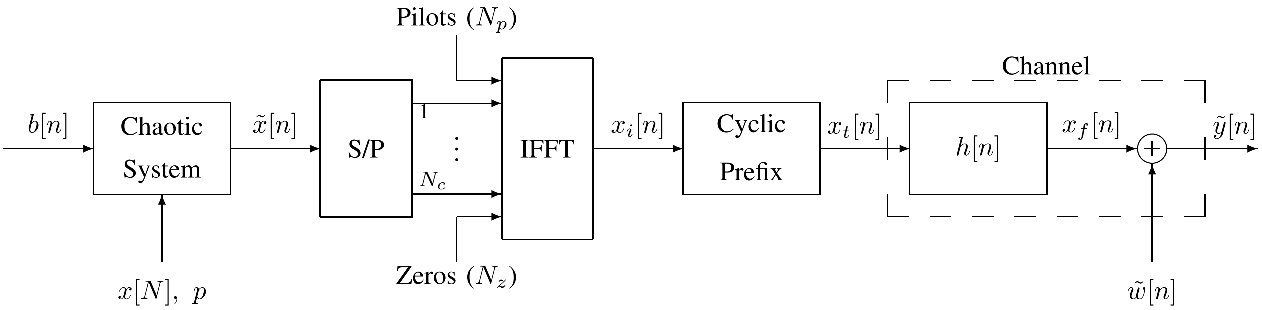

Fig. 6. Block diagram for the proposed OFDM communications system with chaotically modulated signals in each sub-carrier.

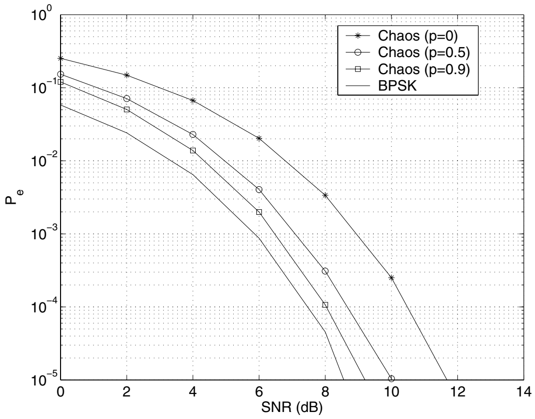

Fig. 7. BER for the OFDM system and AWGN channel.

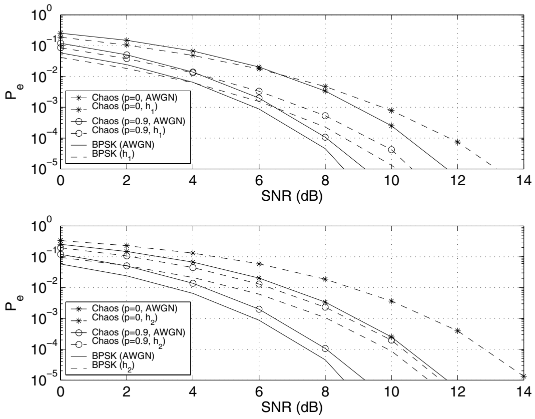

Fig. 8. BER for the OFDM system and multipath channels.

## VI. Conclusions

In this paper we have proposed a novel OFDM communications system with chaotically modulated signals sent in each sub-carrier. This system is robust against multipath interference thanks to the use of OFDM, and provides protection against interception thanks to the use of chaotic signals. Moreover, the map considered has a parameter which allows us to trade security for performance. In the receiver, equalization in the frequency domain is performed, and the Viterbi decoding algorithm is used as an efficient and quasi-optimal method for detecting the transmitted bits. Monte Carlo simulations show that the system is able to operate under realistic channel conditions (i.e. noise and multipath distortion) with similar performance as a conventional communications system.

Future lines of research include considering more efficient chaotic modulation schemes using PWL maps with $M$ intervals, obtaining closed formulas for the performance of the system and developing bit loading strategies, and studying the security offered by the proposed system.

## Acknowledgment

This work has been partially supported by MCYT (Ministerio de Ciencia y Tecnología) under grants TIC2001-0751-C04-03 and TEC2004-06451-C05-02.

## References

[1] *Special Issue on Applications of Nonlinear Dynamics to Electronic and Information Engineering*. Proceedings of the IEEE, May 2002, vol. 90, no. 5.

[2] M. P. Kennedy, R. Rovatti, and G. Setti, Eds., *Chaotic Electronics in Telecommunications*. CRC Press, 2000.

[3] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*. Berlin: Springer-Verlag, 2003.

[4] C. Pantaleón, D. Luengo, and I. Santamaría, "Optimal estimation of chaotic signals generated by piecewise-linear maps," *IEEE Signal Processing Letters*, vol. 7, no. 8, pp. 235–237, Aug. 2000.

[5] C. Pantaleón, L. Vielva, D. Luengo, and I. Santamaría, "Bayesian estimation of chaotic signals generated by piecewise-linear maps," *Signal Processing*, vol. 83, pp. 659–664, Mar. 2003.

[6] S. M. Kay and V. Nagesha, "Methods for chaotic signal estimation," *IEEE Trans. on Signal Processing*, vol. 43, no. 8, pp. 2013–2016, Aug. 1995.

[7] L. Cong, W. Xiaofu, and S. Songgeng, "A general efficient method for chaotic signal estimation," *IEEE Trans. on Signal Processing*, vol. 47, no. 5, pp. 1424–1428, May 1999.

[8] S. Wang, P. C. Yip, and H. Leung, "Estimating initial conditions of noisy chaotic signals generated by piece-wise linear Markov maps using itineraries," *IEEE Trans. on Signal Processing*, vol. 47, no. 12, pp. 3289–3302, Dec. 1999.

[9] C. Pantaleón, D. Luengo, and I. Santamaría, "Optimal estimation of a class of chaotic signals," in *Proc. 16th World Computer and Communications Conf. - Int. Conf. on Signal Processing (WCCC-ICSP)*, vol. 1, 2000, pp. 276–280.

[10] M. Ciftci and D. B. Williams, "Optimal estimation for chaotic sequences using the viterbi algorithm," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2001, pp. 1094–1097.

[11] ——, "Optimal estimation and sequential channel equalization algorithms for chaotic communications systems," *EURASIP Journal on Applied Signal Processing*, vol. 4, pp. 249–256, 2001.

[12] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*. Reading, MA (USA): Perseus Books, 1989.

[13] ETSI TS 101 475 V1.1.1, *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Physical (PHY) Layer*, ETSI, Apr. 2000.

[14] J. Khun-Jush, P. Schramm, G. Malmgren, and J. Torsner, "Hiperlan2: Broadband wireless communications at 5 ghz," *IEEE Communications Mag.*, vol. 40, no. 6, pp. 130–136, June 2002.