A New Receiver for Chaotic Digital Transmissions: The Symbolic Matching Approach

Gilles BUREL and Stéphane AZOU
LEST, Université de Bretagne Occidentale
CS 93837, 29238 BREST cedex 3, France

Abstract : — Chaotic digital transmissions have recently emerged as a way to improve the security and privacy of digital transmissions. In this paper, we propose a new approach to estimate the transmitted symbols on the receiver side. This approach, that we call "Symbolic Matching", consists in matching vectors built from the received signal with a symbolic model of the chaotic oscillator trajectories. Simulation results are also provided and they show that low error rates are obtained.

Key-Words : — Chaos, Digital Transmissions, Communications, Receiver, Symbolic Matching

1 Introduction

In the last few years, chaos-based modulation techniques have emerged as an interesting alternative to standard spread spectrum techniques [5][7][9]. Indeed, chaotic transmissions provide many advantages, among which we can mention:

- Their wideband nature which provides robustness against frequency selective fading in multipath channels and against narrowband interference.
- The intricate dynamic of chaos which significantly increases the privacy of communications in comparison with standard pseudo-noise codes used in spread-spectrum. Without knowledge about the chaotic oscillator on which the transmission is based, it is extremely difficult for the unauthorized user aware of the transmission to access the information.

Indeed, standard spread spectrum transmissions are not so secure. For instance, in [3][4] we proposed approaches for interception of standard spread spectrum transmissions. On the contrary, no efficient approach is known today for interception of chaotic signals.

Chaos can be used in multiple ways in a digital communication system. In this paper we will focus on one of the most efficient technique, which is called CD3S (Chaotic Direct-Sequence Spread Spectrum) [6]. In order to get reliable communication for realistic propagation conditions, a robust synchronization procedure and gain control has to be developed at the receiver side. Readers interested by these aspects can refer to our previous papers[1][2], in which we report experiments on real-world application and signals in the context of a chaotic underwater acoustic network.

In this paper, we assume synchronization and gain control done and we focus on the estimation of the transmitted symbols. A simple and efficient approach was proposed by Milanovic et al. [8]. In the present paper, we propose a new approach, which we call "Symbolic Matching". From the received signal, we build N-dimensional vectors composed of N successive received samples, and we match these vectors with a symbolic model. A criterion, based on the result of the matching, is then used to estimate the transmitted symbols. Simulation results show that this approach provides a lower error rate than the approach described in [8].

The paper is organized as follows. In Section 2, we recall the principle of CD3S chaotic digital transmissions. Then, in Section 3, the approach described in [8] is summarized. Our "Symbolic Matching" method is explained in Section 4, and illustrated by simulation results in Section 5. Finally, a conclusion is drawn in Section 6.

2 Principle of CD3S chaotic digital transmissions

2.1 Overview

A chaotic oscillator is a system which is extremely dependent on the initial conditions. If we consider two identical chaotic oscillators, an extremely small difference of their initial state causes the signals they gener-

ate to quickly diverge. A chaotic signal is therefore unpredictable in the long term. An n-dimensional chaotic system can be described by state space equations:

$$c_k = g\left(c_{k-1}\right) \tag{1}$$

where $c_k \in \mathbb{R}^m$ is called the state, and nonlinear function g maps state c_{k-1} to the next state c_k.

A chaotic dynamical system is one that is deterministic but appears not to be so, as a consequence to its extreme sensitivity to initial conditions. This can be observed even for very simple (one dimensional discrete time) chaotic dynamical system. In this paper, for clarity purpose, we will focus on one dimensional discrete time chaotic dynamical system (another reason is that most chaotic oscillators in use in actual transmission applications are one dimensional).

In most chaotic transmission systems, a BPSK (Binary Phase Shift Keying) is used, hence the symbols a_n belong to $\{-1, +1\}$. If we note P the spreading factor (i.e. the number of chaotic samples per symbol), the transmitted signal is:

$$x_k = a_{\lfloor k/P \rfloor} c_k \tag{2}$$

where $\lfloor k/P \rfloor$ stands for k/P rounded to the nearest integer towards minus infinity. The received signal is then:

$$y_k = x_k + n_k \tag{3}$$

where n_k stands for the noise. Usually, the nonlinear function g is such that:

$$g\left(-x\right) = g\left(x\right) \tag{4}$$

Let us note $g_a\left(x\right) = ag(x)$. We can write:

$$\begin{aligned} x_k &= a_{\lfloor k/P \rfloor} c_k && (5)\\ &= a_{\lfloor k/P \rfloor} g\left(c_{k-1}\right) && (6)\\ &= a_{\lfloor k/P \rfloor} g\left(a_{\lfloor k/P \rfloor} c_{k-1}\right) && (7)\\ &= a_{\lfloor k/P \rfloor} g\left(x_{k-1}\right) && (8)\\ &= g_{a_{\lfloor k/P \rfloor}}\left(x_{k-1}\right) && (9) \end{aligned}$$

This result will be used for estimation of the symbol.

2.2 A simple example of chaotic oscillator

Let us consider the nonlinear function below:

$$g\left(x\right) = 1 - 2x^2 \tag{10}$$

This map generates intricate chaotic trajectories. The corresponding state equation is:

$$c_k = 1 - 2c_{k-1}^2 \tag{11}$$

Figure 1 illustrates two chaotic sequences: a low cross-correlation is clearly seen, although the initial states for the two sequences differ only by 10^{-3}.

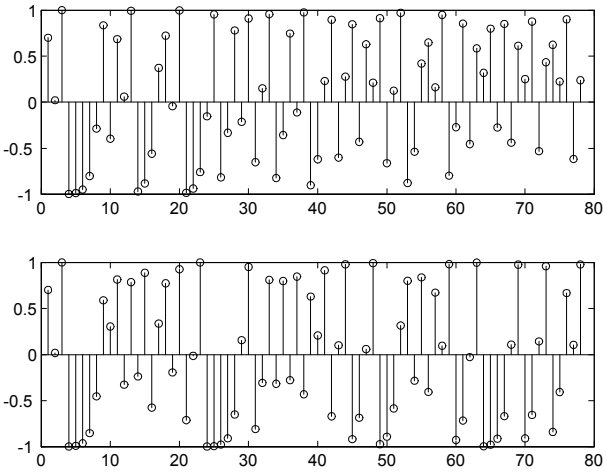

Figure 1: Two chaotic sequences generated by the map $g(x) = 1 - x^2$. The initial states differ only by 10^{-3}.

3 Milanovic receiver

3.1 Principle

In [8], Milanovic et al. proposed a simple and efficient chaotic receiver. Synchronization is assumed, hence we know where begins and ends each block of P samples corresponding to a symbol. For simplicity, let us explain the approach for the estimation of the first symbol (generalization to other symbols is trivial, since it only requires an offset on index k). The index $\lfloor k/P \rfloor$ of $a_{\lfloor k/P \rfloor}$ is also omitted.

First, from the received samples $\{y_k\}$, the values below are computed:

$$\widehat{y}_k = g\left(y_{k-1}\right) \tag{12}$$

for $k \in \{1, 2, \ldots, P-1\}$. Then, the following criterion is computed:

$$C = \sum_{k=1}^{P-1} \widehat{y}_k y_k \tag{13}$$

If $C < 0$ then the estimated symbol is $\widehat{a} = -1$ else it is $\widehat{a} = +1$.

3.2 Justification

If there is no noise, we have $y_k = x_k$ and

$$\widehat{y}_k = g\left(y_{k-1}\right) \tag{14}$$
$$= g\left(x_{k-1}\right) \tag{15}$$

Therefore:

$$C = \sum_{k=1}^{P-1} \widehat{y}_k y_k \tag{16}$$
$$= \sum_{k=1}^{P-1} g\left(x_{k-1}\right) x_k \tag{17}$$
$$= \sum_{k=1}^{P-1} g\left(x_{k-1}\right) a g\left(x_{k-1}\right) \tag{18}$$
$$= a \sum_{k=1}^{P-1} g^2\left(x_{k-1}\right) \tag{19}$$

Since the sum is positive, the sign of C is equal to the sign of the transmitted symbol a.

4 Proposed "Symbolic Matching" receiver

4.1 Overview

Let us consider P successive received samples corresponding to a symbol. For simplicity, as in the previous Section, let us explain the approach for the estimation of the first symbol (generalization to other symbols is trivial, since it only requires an offset on index k). The index $\lfloor k/P \rfloor$ of $a_{\lfloor k/P \rfloor}$ is also omitted.

Let us consider N successive received samples ($N \ll P$) and note:

$$\mathbf{y}_k = \left[y_k, y_{k+1}, ..., y_{k+N-1}\right]^T \tag{20}$$

and define a symbolic vector $\mathbf{z}_a(x)$:

$$\mathbf{z}_a(x) = \left[x, g_a(x), g_a^{(2)}(x), \ldots, g_a^{(N-1)}(x)\right]^T \tag{21}$$

where x is a symbolic variable, $a \in \{-1, +1\}$, and $g^{(n)}(x)$ is defined as:

$$g^{(n)}(x) = \underbrace{g(g(\ldots(g}_{n\ times}(x))) \tag{22}$$

$\mathbf{z}_a(x)$ is a symbolic model of chaotic trajectories. When x varies, $\mathbf{z}_a(x)$ moves along a one-dimensional curve into an N-dimensional vector space.

Let us compute:

$$\widehat{x}_{a,k} = \arg\min_x \left\|\mathbf{y}_k - \mathbf{z}_a(x)\right\|^2 \tag{23}$$

$\widehat{x}_{a,k}$ is the value of x which moves $\mathbf{z}_a(x)$ as close as possible to y_k (hence, which provides the best correspondence between the symbolic model and the actual received data). Details about this computation are given in next subsection.

Then, compute the vector below:

$$\widehat{\mathbf{x}}_{a,k} = \mathbf{z}_a\left(\widehat{x}_{a,k}\right) \tag{24}$$

that is:

$$\widehat{\mathbf{x}}_{a,k} = \left[\widehat{x}_{a,k}, g_a(\widehat{x}_{a,k}), g_a^{(2)}(\widehat{x}_{a,k}), \ldots, g_a^{(N-1)}(\widehat{x}_{a,k})\right]^T \tag{25}$$

The criterion below is computed for $a \in \{-1, +1\}$:

$$C_a = \sum_{k=0}^{P-N} \left\|\mathbf{y}_k - \widehat{\mathbf{x}}_{a,k}\right\|^2 \tag{26}$$

This criterion represents the sum of the distances between vectors $\mathbf{y}_k$ built from the received signal and their closest neighbors on the symbolic model.

Finally, if $C_{-1} < C_{+1}$ then the estimated symbol is $\widehat{a} = -1$ else it is $\widehat{a} = +1$. The reason is obvious: if $C_{-1} < C_{+1}$, this means that the symbolic model corresponding to $a = -1$ is closer to the received signal than the symbolic model corresponding to $a = +1$.

4.2 Computation of $\widehat{x}_{a,k}$

Since the problem is similar whichever the values of k and a are, these indexes are omitted below. We have:

$$\widehat{x} = \arg\min_x \left\|\mathbf{y} - \mathbf{z}(x)\right\|^2 \tag{27}$$
$$= \arg\min_x \sum_{n=0}^{N-1} \left(y_n - g^{(n)}(x)\right)^2 \tag{28}$$

Let us note

$$d(x) = \left\|\mathbf{y} - \mathbf{z}(x)\right\|^2 \tag{29}$$
$$= \sum_{n=0}^{N-1} \left(y_n - g^{(n)}(x)\right)^2 \tag{30}$$

Its derivative is:

$$d'(x) = 2 \sum_{n=0}^{N-1} \left(g^{(n)}(x) - y_n\right) \frac{\partial g^{(n)}}{\partial x}(x) \tag{31}$$

Functions $d(x)$ and $d'(x)$ can be easily precomputed using symbolic computation software, such as Maple or Matlab symbolic toolbox. For instance, when $g(x) = 1 - 2x^2$, $d(x)$ and $d'(x)$ are polynomials.

The numerical value of x is then obtained by solving

$$d'(x) = 0 \tag{32}$$

and keeping the solution which produces the lowest value of $d(x)$ when there is more than one root. This solution is $\widehat{x}_{a,k}$.

5 Simulation Results

In this section, we show simulation results obtained with the map $g(x) = 1 - 2x^2$.

Let us take $N = 3$ and consider a signal to noise ratio equal to $15dB$ on the receiver side. Figure 2 shows the symbolic models $\mathbf{z}_{+1}(x)$ and $\mathbf{z}_{-1}(x)$, which are 1D curves in the 3D space. Vectors $\mathbf{y}_k = \left[y_k, y_{k+1}, y_{k+2}\right]^T$, represented by symbols "+", and built from a block of the received signal corresponding to a transmitted symbol $a = +1$, are shown. It is clear that these vectors are (on average) closer to the symbolic model $\mathbf{z}_{+1}(x)$ than to $\mathbf{z}_{-1}(x)$. Hence, since criterion C_a represents the sum of the distances between the vectors $\mathbf{y}_k$ and the symbolic model $\mathbf{z}_a(x)$, we will have $C_{+1} < C_{-1}$ and the receiver will (correctly) estimate that the transmitted symbol is $+1$.

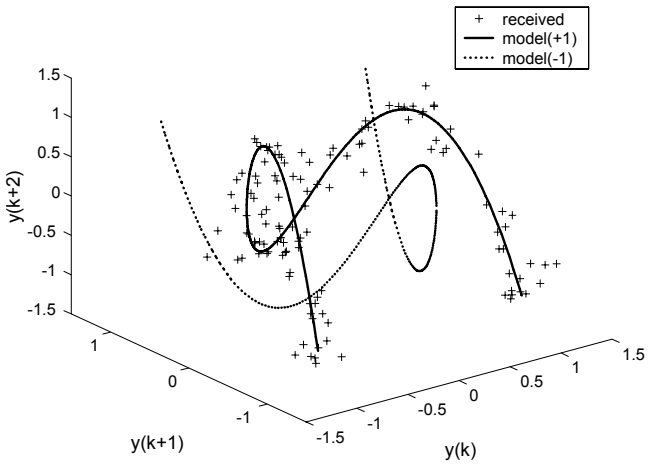

Figure 2: Representation of vectors $\mathbf{y}_k$ and symbolic models $\mathbf{z}_{+1}(x)$ and $\mathbf{z}_{-1}(x)$ in a 3-dimensional space ($N = 3$). The map is $g(x) = 1 - 2x^2$ and the signal to noise ratio is $SNR = 15dB$.

If the signal to noise ratio on the receiver side is only $3dB$, things are less obvious, as shown on figure 3, and estimation errors may occur. However, on average, vectors $\mathbf{y}_k$ are closer to the right model than to the wrong one.

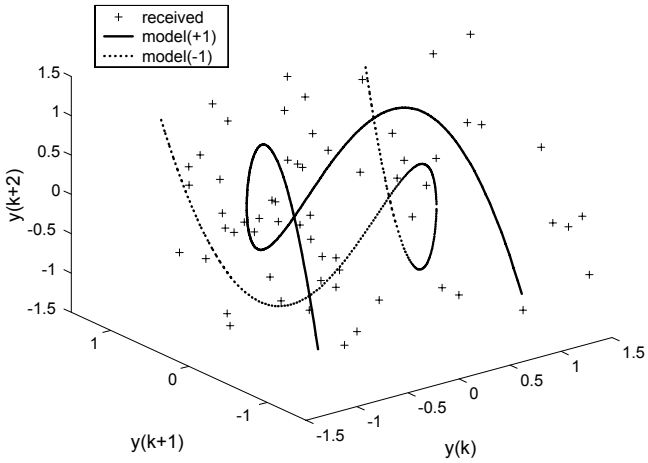

Figure 3: Representation of vectors $\mathbf{y}_k$ and symbolic models $\mathbf{z}_{+1}(x)$ and $\mathbf{z}_{-1}(x)$ in a 3-dimensional space ($N = 3$). The map is $g(x) = 1 - 2x^2$ and the signal to noise ratio is $SNR = 3dB$.

The table below shows simulation results using a CD3S transmission system with a spreading factor $P = 32$. On the receiver side, the signal to noise ratio was $SNR = 3dB$ and 10^4 symbols were transmitted (i.e. 32×10^4 signal samples were received). The table shows the number of symbol errors with respect to the method used for symbol estimation.

method	nb. errors
Milanovic et al.	290
Symbolic Matching ($N = 2$)	179
Symbolic Matching ($N = 3$)	151
Symbolic Matching ($N = 4$)	148

The table shows that Symbolic Matching provides a lower error rate than Milanovic et al. approach. However, except for $N = 2$, the Symbolic Matching requires more computational power. Hence, due to its simplicity, Milanovic et al. approach is a very interesting method when low computational power is available, while when reasonable computational power is available Symbolic Matching may be preferred.

6 Conclusion

In this paper, we have proposed a new approach for symbol estimation in a digital chaotic transmission receiver. The originality of the approach is to match

vectors built from the received signal with a symbolic model of the chaotic oscillator trajectories. Experimental results show that good error rates are obtained. Further work will include a more theoretical study of the performances of this receiver.

References

[1] S. Azou, C. Pistre, G. Burel, A chaotic direct sequence spread-spectrum system for underwater communication, *MTS/IEEE-Oceans'02*, Biloxi, Mississippi, USA, Oct. 29-31, 2002

[2] S. Azou, C. Pistre, L. Le Duff, G. Burel, Sea trial results of a chaotic direct sequence spread spectrum underwater communication system, *MTS/IEEE Oceans'2003*, San Diego, USA, Sept. 22-26, 2003, accepted

[3] G. Burel, Detection of Spread Spectrum Transmissions using fluctuations of correlation estimators, *IEEE Int. Symp. on Intelligent Signal Processing and Communication Systems (ISPACS2000)*, Honolulu, Hawaii, USA, Nov. 5-8, 2000

[4] G. Burel, C. Bouder, Blind estimation of the pseudo-random sequence of a direct-sequence spread spectrum signal , *IEEE 21st Century Military Communications Conference (IEEE-MILCOM2000)*, Los Angeles, USA, Oct. 22-25, 2000

[5] M. Hasler, Synchronization of chaotic systems and transmission of information, *Int. J. Bifurcation and Chaos*, Vol. 8, No 4, pp 647-659, 1998

[6] G. Heidari-Bateni, C. D. McGilleme, A chaotic direct-sequence spread spectrum system, *IEEE Trans. on Communications*, Vol. 42, No. 2/3/4, Feb./March/April 1994, pp. 1524-1527

[7] 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. on Circuits and Systems*, Vol. 45, No 11, 1998.

[8] 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

[9] N.F. Rulkov, L. Illing, and M.A. Vorontsov, *Chaos-based Communication over Turbulent Channel*, IASTED Int. Conf. on Communications, Internet and Information Technology, St. Thomas, US Virgin Islands, Nov. 18-20, 2002