Nonlinear Analysis 71 (2009) e21–e31

Contents lists available at ScienceDirect

Nonlinear Analysis

journal homepage: www.elsevier.com/locate/na

Review

Nonlinear electronic circuit, Part II: synchronization in a chaotic MODEM scheme

A.N. Miliou [a,*], S.G. Stavrinides [b], A.P. Valaristos [a], A.N. Anagnostopoulos [b]

[a] Department of Informatics, Aristotle University of Thessaloniki, GR 54124, Thessaloniki, Greece

[b] Physics Department, Aristotle University of Thessaloniki, GR 54124, Thessaloniki, Greece

ARTICLE INFO

Keywords:
Chaos
Nonlinear circuits
Routes to chaos
Synchronization
Communication system security

ABSTRACT

In this work we present a thorough investigation of the effect of noise (internal or external) on the synchronization of a drive–response configuration system (unidirectional coupling between two identical systems). Moreover, since in every practical implementation of a communication system, the transmitter and receiver circuits (although identical) operate under slightly different conditions it is essential to consider the case of the mismatch between the parameters of the transmitter and the receiver. In our work we consider the non-autonomous 2nd order nonlinear oscillator system presented in [G. Mycolaitis, A. Tamasevicious, A. Cenys, A. Namajunas, K. Navionis, A. N. Anagnostopoulos, Globally synchronizable non-autonomous chaotic oscillator, in: Proc. of 7th International Workshop on Nonlinear Dynamics of Electronic Systems, Denmark, July 1999, pp. 277–280] which is particularly suitable for digital communications.

Furthermore, we modified the previous chaotic communication system in order to exhibit enhanced security features. The enhancement in the security of the system is achieved by introducing a set of parameters used in the encoding and decoding of the message signal. We also introduce a time delay parameter in the dynamical system which on the one hand improves the chaotic behavior of the system and on the other hand, adds further security in the encoding–decoding scheme.

Contents

1. Introduction

The significance of private and secure communications is very clear in a world, which increasingly relies on rapid transmission of large amounts of information. The current solutions for secure communications are the public key cryptosystems using software techniques to achieve computational complexity while quantum cryptography has the

* Corresponding author. Tel.: +30 2310 998407; fax: +30 2310 998419.
E-mail address: amiliou@csd.auth.gr (A.N. Miliou).

0362-546X/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.na.2009.05.076

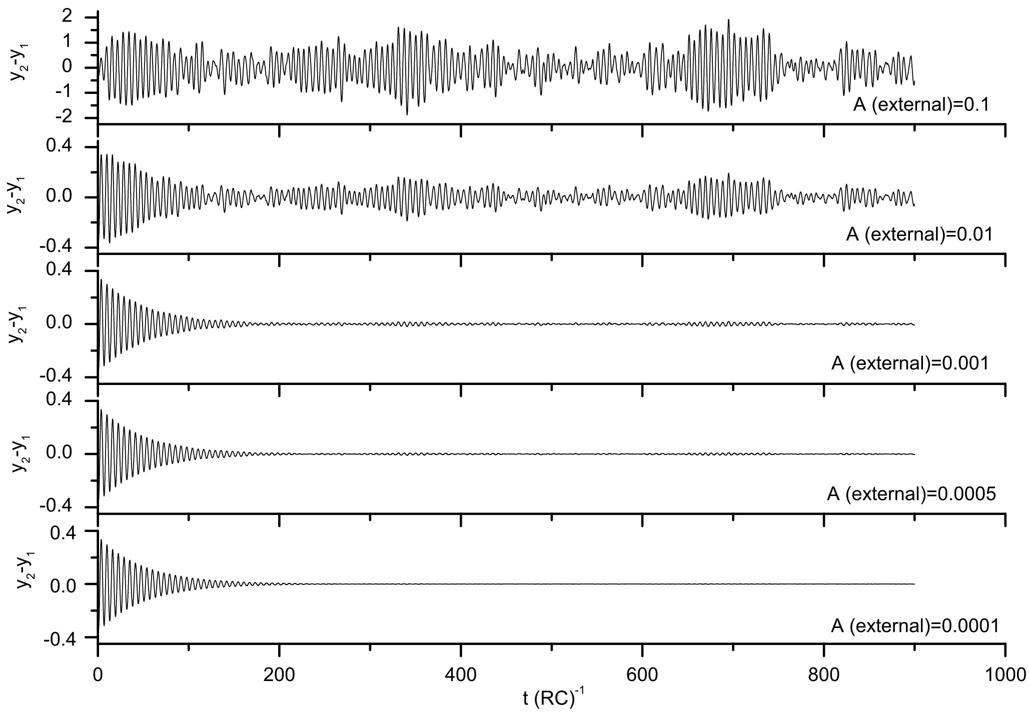

Fig. 1. Synchronization with the application of external noise (channel).

potential to render such techniques obsolete. However, another method of increasing security in communications is to use hardware complexity to hide or mask the message on a chaotic carrier [1–8].

With chaos-based communication systems, the key fact is that the procedure used by the transmitter to generate the chaotic waveform is deterministic; the knowledge of this procedure by an authorized receiver allows him to replicate, or synchronize, the chaotic waveform, and then to recover the message by subtracting the chaotic carrier [3–9]. The confidentiality of the encryption technique is based on the difficulty to reproduce the chaotic carrier signal if an intruder does not know the particular dynamical system used.

In this paper, we investigate the synchronization of the system (transmitter + receiver) under noisy channel conditions as well as the case where different noise levels are added in the transmitter and the receiver (internal noise) due to electronics. Moreover, we study the robustness of the system and relate it to the desired security, proposing a more sophisticated approach, combining the simplicity in the implementation of a chaotic system with an enhanced encoding scheme that will overall increase security.

2. The effect of noise and parameter mismatch in the system

The general set-up and the set of equations governing the communication system were presented in Part I.

The use of synchronized chaotic systems for communications usually relies on the robustness of the synchronization within the transmitter and receiver pair [2,4–10]. However, if the communication channel is imperfect and/or there is internal noise at the electronic circuitry the distorted signal at the receiver input might cause considerable synchronization mismatch between the transmitter–receiver pair [11–15].

Figs. 1 and 2 depict the synchronization with the application of external and internal noise respectively. The external noise is applied on the communication channel and in our simulation is represented by white noise added on $F(y_1, t)$, where frequencies greater than RC were cutoff. The internal noise is due to the electronics circuitry and is again applied both on the transmitter and the receiver (added on x_1, y_1 and x_2, y_2 variables). Once again frequencies higher than RC are cutoff.

Different noise amplitudes A, have been utilized ranging from 0.01% to 50% of the mean signal amplitude. As the noise amplitude A is increased, the synchronization of the system continuously deteriorates and is practically destroyed in both cases (external and internal noise) above a certain noise level.

The artificial noise added at the simulation was produced as follows: A pseudorandom number generator produces an array of random numbers in the interval [0, 1]. The random numbers are equal to the total number of simulation steps. Then the Fourier transform of this series is obtained by standard procedures and amplitudes for frequencies larger than a particular cutoff value are zeroed. The inverse Fourier transform is taken in order to produce the noise series to be used in the subsequent simulation. In our simulation we cutoff frequencies larger than the characteristic frequency of the system RC. By this "noise filtering" procedure we avoid the dependence of the generated noise on the simulation step. Noise was