NONLINEAR DYNAMICS RECONSTRUCTION WITH NEURAL NETWORKS OF CHAOTIC TIME-DELAY COMMUNICATION SYSTEMS

S. Ortín[1,2], L.Pesquera[1], J.M. Gutiérrez[3], A. Valle[1], and A. Cofino[3]

(1) Instituto de Física de Cantabria (CSIC-UC), Avenida de los Castros s/n, E-39005, Santander, Spain
(2)Dpt. de Física Moderna (Universidad de Cantabria)
(3)Dpt. de Matemática Aplicada y Ciencias de la Computación (UC)

In the last decade secure communication by applying chaos synchronization has attracted a great deal of interest (A. Argyris et al. NATURE **438**, 343, 2005). An important issue is the security level of these systems. Since the dynamics generated by delay systems can be high dimensional, many optical chaotic cryptosystems are based on delayed optoelectronic feedback (J.P. Goedgebuer et al. Phys. Rev. Lett. **80**, 2249, 1998). The dynamics of these systems can be modeled by $\dot{x}(t) = -x(t) + \beta \sin^2(x(t-\tau) + \phi)$. In this work we show that chaos encryption based on these systems can be broken. A new type of modular neural networks (NN) is used to reconstruct the nonlinear dynamics from time series (S. Ortin et al. Physica A **351**, 133, 2005). The modular NN has two modules, one for non-feedback part with input data delayed by the embedding time, and a second one for the feedback part with input data delayed by the feedback times. When a small training error is achieved, the nonlinear model obtained in this way is used to extract the message from the chaotic transmitted signal.

It is found that the complexity of the NN required to reconstruct the nonlinear dynamics with a given accuracy level increases with the feedback strength β, but not with the delay time τ. When β is increased by a factor of 3 the complexity of the NN, given by the number of parameters, increases almost a 50%. Then the confidentiality level of the system increases with β.

It has been recently proposed to enhance chaos encryption by using several delays (M. W. Lee et al Opt. Lett. **29**, 325, 2004). Our results show that for some configurations delay identification is more difficult for these systems. We have also found that the complexity of the NN required to break the system is greater than for one delay systems. For example, in one of the configurations, when β is increased by a factor of 3 the complexity of the NN increases almost a 200%. Then the number of parameters of the NN required to obtain the same accuracy increases in a factor of 4 with respect to one delay systems. Results for more efficient NN models adapted to the specific configuration of the system with several delays will be also reported.