Chapter 17
Unmasking Optical Chaotic Cryptosystems Based on Delayed Optoelectronic Feedback

Silvia Ortín
Instituto de Física de Cantabria (CSIC-Universidad de Cantabria), Spain

Luis Pesquera
Instituto de Física de Cantabria (CSIC-Universidad de Cantabria), Spain

ABSTRACT

The authors analyze the security of optical chaotic communication systems. The chaotic carrier is generated by a laser diode subject to delayed optoelectronic feedback. Transmitters with one and two fixed delay times are considered. A new type of neural networks, modular neural networks, is used to reconstruct the nonlinear dynamics of the transmitter from experimental time series in the single-delay case, and from numerical simulations in single and two-delay cases. The authors show that the complexity of the model does not increase when the delay time is increased, in spite of the very high dimension of the chaotic attractor. However, it is found that nonlinear dynamics reconstruction is more difficult when the feedback strength is increased. The extracted model is used as an unauthorized receiver to recover the message. Therefore, the authors conclude that optical chaotic cryptosystems based on optoelectronic feedback systems with several fixed time delays are vulnerable.

INTRODUCTION

Chaotic signals typically have broadband spectrum. This property is desirable for applications that require robustness against interference, jamming and low detection probability. Those issues have been addressed by traditional communication systems by using spread spectrum and frequency hopping modulations. In chaos-based communications the broadband chaotic signal is generated at the physical layer instead of algorithmically. Additionally, chaotic carriers offer a certain degree of intrinsic privacy in the data

DOI: 10.4018/978-1-61520-737-4.ch017

transmission. In chaotic communication systems (Cuomo et al., 1993b; Colet & Roy, 1994) the masking of the message is performed at the physical layer by embedding the signal within a chaotic carrier in the emitter. The recovery of the message is based on the synchronization phenomenon (Ashwin, 2003) by which a receiver, quite similar to the transmitter, is able to reproduce the chaotic part of the transmitted signal. After synchronization occurs, the decoding of the message is straightforward by comparing the input and output of the receiver. Privacy in chaotic communication systems results from the fact that the eavesdropper must have the proper hardware and parameter settings in order to recover the message. The suitability of chaos-based optical communication systems for encrypting gigabit signals has been recently demonstrated in an installed optical network infrastructure of approximately 120 km that covers the metropolitan area of Athens (Argyris et al., 2005). However, the security of these systems remains the key issue to be addressed.

In conventional encryption techniques a key is used to alter the information symbols. The transmitter and the receiver share the key so that the information can be recovered. In a chaotic communication system the transmitter generates a time-evolving chaotic waveform that is used to mask the message. The cryptographic key relies on structural characteristics of the hardware as well as on the set of operating parameters chosen for the system. The message can be recovered with a receiver such that its configuration and parameter settings are matched to those of the transmitter. Encryption is achieved by encoding at the physical layer, providing full compatibility to conventional software encryption techniques. Dynamical encoding with a chaotic waveform can then be considered as an additional layer of encryption.

Chaos cryptography is a recent encryption technique (the idea was proposed in the early 90s), and it will take some time for its security analysis to mature. Some rules have been suggested to achieve a reasonable degree of security (Alvarez & Li, 2006). Methods to quantify the cryptanalysis of chaotic encryption schemes have been also proposed (Tenny & Tsimring, 2004). However, more research needs to be done to develop a systematic cryptographic approach for the analysis of the security of different chaotic communication systems. Many chaos-based encryption schemes have been proposed, and many of those schemes have been broken later on.

Some chaotic encryption systems were broken even without reconstructing the transmitter's chaotic dynamics, that is, without searching for the secret key that was used to encrypt the message. This kind of attack is usually applicable if the statistical properties of the ciphertext change as a result of changing the transmitted plaintext. Return maps (Perez & Cerdeira, 1995) and spectral analysis (Yang et al., 1998a) of the transmitted ciphertext have been used to decode the message eliminating the need to reconstruct the secret dynamics.

Another type of attacks relies on partial knowledge of the chaotic dynamics. If the unauthorized receiver knows the type of attractor used for the transmission and reception, but ignores the precise value of the parameters, generalized synchronization (Rulkov et al., 1995) can be used to extract the message (Yang et al., 1998b). In this case a generalized synchronization between transmitter and unauthorized receiver with a different set of parameters occurs, and the message is decoded using variations in the synchronization error. In another case the unauthorized receiver knows that the transmitter is an erbium-doped fiber-ring laser with two delay loops (Geddes et al., 1999). The dynamics of this chaotic transmitter is high dimensional (dimension greater than 10). However, using a simplified lower dimensional model with four parameters, the message can be decoded by estimating the model parameters. In this case the laser dynamics was governed almost entirely by the modulation signal, which echoed in the two loops, and nonlinear effects could be neglected to a good approximation.