Breaking Two Secure Communication Systems Based on Chaotic Masking

G. Álvarez, F. Montoya, M. Romera, and G. Pastor

***Abstract*—This paper describes the security weakness of two generalized nonlinear state-space observers-based approaches for both chaos synchronization and secure communication, using chaotic masking and chaotic modulation of a Lorenz system. We show that the security is compromised without any knowledge of the chaotic system parameter values and even without knowing the transmitter structure.**

***Index Terms*—Chaos, cryptography, nonlinear systems, security of data, state-space methods, telecommunication.**

I. Introduction

The possibility of synchronization of two coupled chaotic systems was first shown by Pecora and Carrol [1]. This discovery soon aroused great interest as a potential means for secure communications [2], [3]. Accordingly, a great number of cryptosystems based on chaos have been proposed [4]–[6]; some of them fundamentally flawed by a lack of robustness and security [7]–[10].

Lately, the synchronization has been regarded as a special case of a state observer design problem [11]. In [12], the authors propose a secure communication system based on state-space observers for chaotic synchronization. The transmitter is a chaotic oscillator in which the plaintext is introduced either in linear or nonlinear form. The receiver is a chaotic system synchronized by means of an adaptive observer. This work may be seen as a generalization of the approach developed by Liao *et al.* in [13].

In [12, Sect. IV], two cases are considered. In Case 1, the information is linearly introduced into the model, exactly reproducing the example number 3 of [13, Sect. V], while in Case 2 the information is nonlinearly introduced into the model. Both cases are illustrated by applying this approach to the Lorenz attractor as an example.

A. Linearly Introduced Information Into the Model

In [12, Sect. IV, Case 1] and [13, Sect. V, Example 3] the Lorenz system is implemented with the following parameter values: $(\sigma_1, \sigma_2, r, b) = (10, 10, 28, 8/3)$. The plaintext is the signal $s(t) = 0.05\ \sin(60\pi t)$.

The encryption process is defined by adding the plaintext $s(t)$ and the variable x_1 to form the system output y. The system can be written in a compact form as

$$\dot{x} = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} x + \begin{pmatrix} 0 \\ -yx_3 \\ yx_2 \end{pmatrix} + Bs \qquad (1)$$

where $B = [30\ 28\ 0]^T$ and $y = [1\ 0\ 0]\, x + s$.

B. Nonlinearly Introduced Information Into the Model

In [12, Sect. IV, Case 2], the same state observer and system parameter values of case Case 1 are used, but the plaintext is now a large magnitude signal $s(t) = 0.5\ \sin(60\pi t)$ and the information is nonlinearly introduced into the model.

$$\dot{x}_1 = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} x + \begin{pmatrix} ys \\ -yx_3 - ys \\ yx_2 + ys \end{pmatrix} + Bs \qquad (2)$$

where $B = [30\ 28\ 0]^T$ and $y = [1\ 0\ 0]\, x + s$.

II. Ciphertext Filtering Attack

Although the authors of [12] and [13, Sect. V, Example 3] seemed to base the security of both described cryptosystems on the chaotic behavior of the output of the Lorenz nonlinear system, no analysis of security was included.

It is supposed that chaotic modulation is an adequate means for secure transmission, because chaotic maps present some properties as sensitive dependence on parameters and initial conditions, ergodicity, mixing, and dense periodic points. These properties make them similar to pseudorandom noise [14], which has been used traditionally as a masking signal for cryptographic purposes.

A fundamental requirement of the pseudorandom noise used in cryptography is that its spectrum should be infinitely broad, flat, and of higher power density than the signal to be concealed with. In other words, the plaintext power spectrum should be buried into the pseudorandom noise power spectrum.

The cryptosystems proposed in [12] and [13, Sect. V, Example 3] do not satisfy this condition. On the contrary, the spectrum of the signal generated by the Lorenz oscillator is narrow-band, decaying very fast with increasing frequency, showing a power density much lower than the plaintext at plaintext frequencies.

In Fig. 1, the ciphertext logarithmic power spectra of the cryptosystem described in [12, Sect. IV, Case 1] and [12, Sect. IV, Case 2] are illustrated. Both cases exhibit similar power spectra. It can be seen that plaintext signals clearly emerge at 30 Hz over the background noise created by the Lorenz oscillator, with a

Manuscript received February 10, 2004; revised March 16, 2004. This work was supported by the MCYT of Spain under Grant TIC2001-0586 and Grant SEG2004-02418. This paper was receommended by Associate Editor C. W. Wu.

The authors are with the Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain (e-mail: gonzalo@iec.csic.es).

Digital Object Identifier 10.1109/TCSII.2004.836047

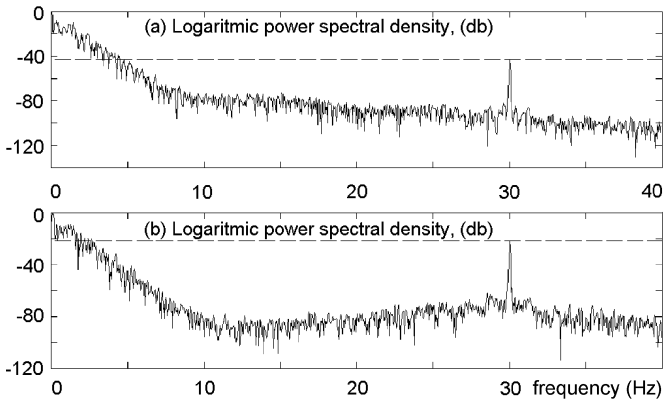

Fig. 1. Power spectral density analysis of the ciphertext signal: (a) spectrum corresponding to [12, Sect. IV, Case 1]; spectrum corresponding to [12, Sect. IV, Case 2]. The peaks at 30 Hz correspond to the plaintext frequency.

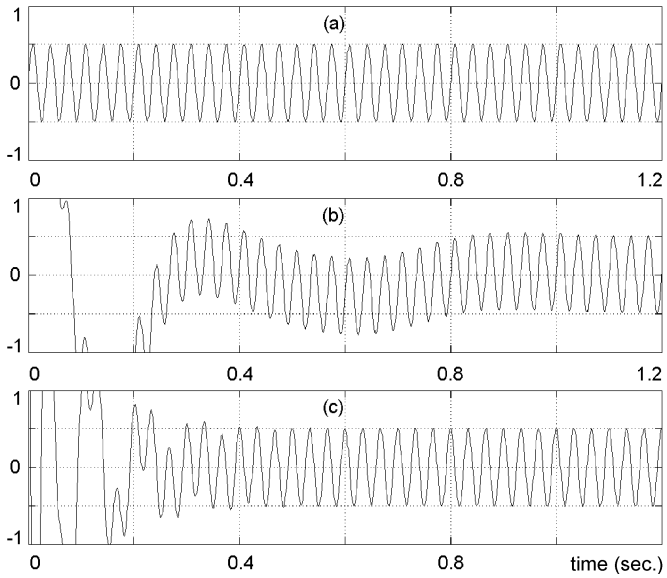

Fig. 2. Plaintext recovery with ciphertext filtering attack. Time histories of: (a) plaintext, (b) recovered plaintext with the authorized receiver, and (c) recovered plaintext with a high-pass filter.

power -44 dB and -24 dB, respectively, relative to the maximum power of the ciphertext spectrum, while the power density of the ciphertext, for the same frequency, falls below -70 dB.

To break the system, the transmitters of the examples have been simulated with the same parameter values. A fourth-order Runge–Kutta integration algorithm in MATLAB 6 was used.

To recover the plaintext, we used no chaotic receiver; instead, the ciphertext was high-pass filtered. The procedure is illustrated in Fig. 2 for [12, Sect. IV, Case 1], which is the harder case. The high-pass filter employed was an eight-pole Butterworth with a frequency cutoff of 5 Hz. The result is a perfect estimation of the plaintext, with a transient error of shorter duration than that obtained with the authorized receiver.

Retrieving the plaintext in [12, Sect. IV, Case 2] is easier, because its amplitude is stronger, so a simpler filter may be used. The plaintext presence in the ciphertext is so evident that it can be appreciated even with the naked eye, as shown in Fig. 3.

Our method works only for plaintext frequencies higher than the cut-off frequency of the employed high-pass filter, i.e., for frequencies from 5 Hz to infinity. For lower frequencies, the noise created by the Lorenz oscillator effectively masks the plaintext, preventing its retrieval by nonauthorized means.

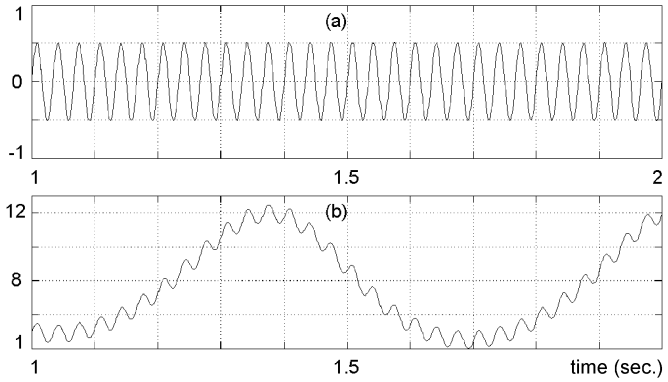

Fig. 3. Direct observation of plaintext looking at the ciphertext: (a) plaintext and (b) ciphertext.

III. Conclusion

The proposed cryptosystem is rather weak, since it can be broken without knowing its parameter values and even without knowing the transmitter structure. There is no mention about what the key is, nor which is the key space and how it would be managed, a fundamental aspect in every secure communication system that should not be neglected. The total lack of security discourages the use of this algorithm for secure applications.

References

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, Feb. 1990.

[2] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of chaotic carrier using self-synchronizing Chuass circuits," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634–642, Oct. 1993.

[3] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.*, vol. 74, no. June, pp. 5028–5031, 1995.

[4] K. M. Cuomo, A. V. Oppenheim, and H. Strogatz, "Synchronization of lorenzbased chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II*, vol. 40, no. Oct, pp. 626–633, 1993.

[5] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurc. Chaos*, vol. 3, pp. 1619–1627, June 1993.

[6] T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comp. Cognition*, vol. 2, pp. 81–130, June 2004.

[7] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurc. Chaos*, vol. 4, pp. 959–977, Apr. 1994.

[8] H. Zhou and X. Ling, "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 268–271, Mar. 1997.

[9] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst I*, vol. 45, pp. 1062–1067, Oct. 1998.

[10] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a chaotic secure communication system," *Phys. Lett. A*, vol. 306, pp. 200–205, Jan. 2003.

[11] Ö Morgül and E. Solak, "Observer based synchronization of chaotic signals," *Phys. Rev. E*, vol. 54, pp. 4803–4811, Nov. 1996.

[12] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized state-space observers for chaotic syncronization and secure communication," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 345–349, Mar. 2002.

[13] T. L. Liao and N. S. Huang, "An observer based approach for chaotic synchronization with application to secure communications," *IEEE Trans. Circuits Syst. I*, vol. 46, pp. 1144–1150, Sept. 1999.

[14] R. L. Devaney, *A First Course in Chaotic Dynamical Systems*. Reading, MA: Addison-Wesley, 1992.