Available online at www.sciencedirect.com
SCIENCE DIRECT®
PERGAMON
Chaos, Solitons and Fractals 18 (2003) 141–148
CHAOS
SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

An adaptive chaos synchronization scheme applied to secure communication

Moez Feki *

Département EEA, UFR Sciences Exactes, Université de Reims Champagne Ardenne, Moulin de la Housse, BP 1039, 51687 Reims cedex 2, France

Accepted 25 November 2002

Abstract

This paper deals with the problem of synchronization of a class of continuous-time chaotic systems using the drive-response concept. An adaptive observer-based response system is designed to synchronize with a given chaotic drive system whose dynamical model is subjected to unknown parameters. Using the Lyapunov stability theory an adaptation law is derived to estimate the unknown parameters. We show that synchronization is achieved asymptotically. The approach is next applied to chaos-based secure communication. To demonstrate the efficiency of the proposed scheme numerical simulations are presented.

1. Introduction

In recent years, there has been increasing interest in the study of synchronizing chaotic systems [1–4]. In their seminal paper, Pecora and Carroll [5] addressed the synchronization of chaotic systems using a drive-response conception. The idea is to use the output of the drive system to control the response system so that they oscillate in a synchronized manner. Since then, several other synchronization schemes have been developed, such as mutual coupling by Chua et al. [6] and inverse system approach by Hasler and coworkers [7,8]. More recently, the synchronization has been regarded as a special case of observer design problem [9–12]. In most of the research done on synchronizing chaotic system, perfect knowledge of these systems was assumed, yet such perfection is not realistic. Actually a few attempts to synchronize uncertain chaotic systems have been proposed. In [13] we have considered the presence of unknown disturbances and achieved synchronization using a reduced-order observer. In [14] a robust sliding observer was suggested to overcome the effect of parameter uncertainties. In [15,16] adaptive observers were used to synchronize Lur'e type chaotic systems (i.e., where the nonlinearity is a function of the output).

In this work we suggest an adaptive observer for a larger class of chaotic systems. We use the Lyapunov approach to derive an updating law for the estimation of the unknown parameters. We show that under mild conditions, synchronization is asymptotically achieved and the parameters are correctly estimated. We also show that this method can be applied to secure message transmission using parameter modulation. The outline of this paper is as follows. In Section 2 we present the adaptive observer-based response system design and we prove its synchronization. In Section 3 we present some illustrative examples. In Section 4 we explain how can the proposed synchronization scheme be used for secure digital message transmission and we give some simulation results. Finally in Section 5 we include some concluding remarks.

* Tel.: +33-3-2691-8579; fax: +33-3-2691-3106.
E-mail address: moez.feki@univ-reims.fr (M. Feki).

0960-0779/03/$ - see front matter
doi:10.1016/S0960-0779(02)00585-4

2. Adaptive synchronization

Chaotic systems are generally described by a set of nonlinear differential equations. It is very common, however, to be able to separate the dynamics into linear and nonlinear parts. If we furthermore consider that the chaotic system is subjected to unknown parameters, the chaotic dynamics can therefore be described by the following equations:

$$\dot{x} = Ax + f(x) + B\Phi(x)\theta \tag{1a}$$

$$y = Cx \tag{1b}$$

where $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^m$ are respectively the state vector and the output of the drive system. $\theta \in \mathbb{R}^p$ represents a constant vector of unknown parameter. A and C are two constant matrices of appropriate dimensions and $B \in \mathbb{R}^{n\times q}$ is the injection map of the unknown dynamics. $f : \mathbb{R}^n \to \mathbb{R}^n$ and $\Phi : \mathbb{R}^n \to \mathbb{R}^{q\times p}$ are smooth vector fields. We assume that the following hypotheses are pertaining to the drive system (1).

($\mathscr{H}1$) f (respectively Φ) is Lipschitz in x, with Lipschitz constant k_f (respectively k_Φ) i.e., for all $x, \hat{x} \in \mathbb{R}^n$

$$\|f(x) - f(\hat{x})\| \leqslant k_f \|x - \hat{x}\|$$

$$\|\Phi(x) - \Phi(\hat{x})\| \leqslant k_\Phi \|x - \hat{x}\|$$

($\mathscr{H}2$) We can choose a gain matrix L and two positive definite matrices P and Q satisfying

$$(A - LC)^{\mathrm{T}}P + P(A - LC) = -Q \tag{2}$$

$$k_f + k_\Phi\|\theta\|\|B\| < \frac{\lambda_{\min}(Q)}{2\lambda_{\max}(P)} \tag{3}$$

$$B^{\mathrm{T}}P = HC \tag{4}$$

for some matrix H. Note that the last equality implies that the span of rows of $B^{\mathrm{T}}P$ belongs to the span of rows of C.

Remark 1. Finding a gain matrix L satisfying ($\mathscr{H}2$) is not a trivial task. However, it was shown in [17] using the Kalman–Yakubovich–Popov lemma that if a matrix L can be chosen such that the transfer function matrix $G(s) = C(sI - (A - LC))^{-1}B$ is strictly positive real, then there exist matrices P and Q such that (2) and (4) are satisfied with $H = I$.

Similarly to many different synchronization schemes, the response system is merely a duplicate of the drive system with the addition of a crucial term depending on the synchronizing signal of the drive system. Herein, we propose an adaptive observer-based response system in the following form:

$$\dot{\hat{x}} = A\hat{x} + f(\hat{x}) + B\Phi(\hat{x})\hat{\theta} + L(y - C\hat{x}) \tag{5}$$

where $\hat{\theta}$ is the solution of an adaptation law to be determined in the sequel.

Let $e = x - \hat{x}$ be the synchronization error. Then from (1) and (5) the error dynamics are

$$\dot{e} = (A - LC)e + f(x) - f(\hat{x}) + B\Phi(x)\theta - B\Phi(\hat{x})\hat{\theta} \tag{6}$$

The synchronization problem is now reduced to the stability of system (6). Consider the Lyapunov function candidate

$$V = e^{\mathrm{T}}Pe + \frac{1}{\gamma}(\theta - \hat{\theta})^{\mathrm{T}}(\theta - \hat{\theta}), \quad \gamma > 0 \tag{7}$$

The derivative of V along the trajectories of (6) is given by

$$\begin{aligned}
\dot{V} &= e^{\mathrm{T}}\Big((A - LC)^{\mathrm{T}}P + P(A - LC)\Big)e + 2e^{\mathrm{T}}P\Big(f(x) - f(\hat{x})\Big) + 2\Big(B\Phi(x)\theta - B\Phi(\hat{x})\hat{\theta}\Big)^{\mathrm{T}}Pe - \frac{2}{\gamma}(\theta - \hat{\theta})^{\mathrm{T}}\dot{\hat{\theta}} \\
&\leqslant -e^{\mathrm{T}}Qe + 2k_f\lambda_{\max}(P)e^{\mathrm{T}}e + 2\Big(B\Phi(x)\theta - B\Phi(\hat{x})\theta\Big)^{\mathrm{T}}Pe + 2\Big(B\Phi(\hat{x})(\theta - \hat{\theta})\Big)^{\mathrm{T}}Pe - \frac{2}{\gamma}(\theta - \hat{\theta})^{\mathrm{T}}\dot{\hat{\theta}} \\
&\leqslant -\lambda_{\min}(Q)\|e\|^2 + 2k_f\lambda_{\max}(P)\|e\|^2 + 2\|B\|k_\Phi\|\theta\|\lambda_{\max}(P)\|e\|^2 + 2(\theta - \hat{\theta})^{\mathrm{T}}\left(\Phi(\hat{x})^{\mathrm{T}}B^{\mathrm{T}}Pe - \frac{1}{\gamma}\dot{\hat{\theta}}\right) \\
&\leqslant -\big(\lambda_{\min}(Q) - 2k_f\lambda_{\max}(P) - 2\|B\|k_\Phi\|\theta\|\lambda_{\max}(P)\big)\|e\|^2 + 2(\theta - \hat{\theta})^{\mathrm{T}}\left(\Phi(\hat{x})^{\mathrm{T}}HCe - \frac{1}{\gamma}\dot{\hat{\theta}}\right)
\end{aligned}$$

Should we choose the following adaptation law

$$\dot{\hat{\theta}} = \gamma \Phi(\hat{x})^{\mathrm{T}} H(y - C\hat{x}) \tag{8}$$

then

$$\dot{V} \leqslant -\mu \|e\|^2 \tag{9}$$

where

$$\mu = \lambda_{\min}(Q) - 2k_f \lambda_{\max}(P) - 2\|B\|k_\Phi\|\theta\|\lambda_{\max}(P) > 0$$

as far as ($\mathscr{H}2$) is satisfied. And so the system is Lyapunov stable, whence $e \in L_\infty$ and $(\theta - \hat{\theta}) \in L_\infty$. Therefore using (6) and (7) we have $V(t) \in L_\infty$ and $\dot{e} \in L_\infty$.

Integrating (9) we obtain

$$\int_0^t \|e\|^2 \,\mathrm{d}t \leqslant \frac{V(0) - V(t)}{\mu}$$

since $V(0)$ is finite it follows that $e \in L_2$. Hence using Barbalat's lemma [18] and the fact that $e \in L_\infty$, $\dot{e} \in L_\infty$ and $e \in L_2$ it results that $\lim_{t\to\infty} e(t) = 0$.

Moreover, since f and Φ are Lipschitz, then $\dot{e}$ is uniformly continuous and the integral

$$\int_0^\infty \dot{e}\,\mathrm{d}t = -e(0)$$

is finite. Thus by Barbalat's lemma $\lim_{t\to\infty} \dot{e}(t) = 0$. Therefore using (6) we obtain $\lim_{t\to\infty}(B\Phi(x)\theta - B\Phi(\hat{x})\hat{\theta}) = 0$.

We can now summarize our result in the following theorem

Theorem 1. *Consider the drive chaotic system* (1) *satisfying hypotheses* ($\mathscr{H}1$) *and* ($\mathscr{H}2$). *The observer-based response system* (5) *associated with the adaptation law* (8) *globally asymptotically synchronizes with the drive system i.e.*, $\|e(t)\| = \|x(t) - \hat{x}(t)\| \to 0$ *as* $t \to 0$.

Remark 2. We note that if $\mathrm{d}\Phi(x(t))/\mathrm{d}t$ is bounded and $\Phi(x)$ satisfy

$$\int_t^{t+T_0} \Phi(x(\tau))^{\mathrm{T}} \Phi(x(\tau))\,\mathrm{d}\tau \geqslant \alpha I$$

for some T_0, $\alpha > 0$ and any $t \geqslant 0$, then $\lim_{t\to\infty} \|\theta - \hat{\theta}\| = 0$, [19].

Remark 3. If the drive chaotic system is described by the following equations

$$\dot{x} = Ax + f(x) + B\Phi(y)\theta \tag{10a}$$

$$y = Cx \tag{10b}$$

then ($\mathscr{H}1$) and ($\mathscr{H}2$) are substituted by

($\mathscr{H}1'$) f is Lipschitz in x with Lipschitz constant k_f.
($\mathscr{H}2'$) We can choose matrices L, P and Q such that

$$(A - LC)^{\mathrm{T}}P + P(A - LC) = -Q$$

$$k_f < \frac{\lambda_{\min}(Q)}{2\lambda_{\max}(P)}$$

$$B^{\mathrm{T}}P = HC$$

Remark 4. If the drive chaotic system is described by the following equations

$$\dot{x} = Ax + f(y) + B\Phi(y)\theta$$

$$y = Cx$$

then the system reduces to that studied in [15,16].

3. Illustrative examples

In this section, we consider two well-known chaotic systems to which we apply the chaotic synchronization scheme proposed in the foregoing section.

3.1. Chua's circuit

Chua's circuit is a simple electronic circuit that exhibits chaotic behavior for some specified components values. The circuit dynamics can be described by three differential equations, which in dimensionless form are as follows (see Ref. [20])

$$\dot{x}_1 = \alpha(-x_1 + x_2 - f_1(x_1))$$

$$\dot{x}_2 = x_1 - x_2 + x_3$$

$$\dot{x}_3 = -\beta x_2$$

where $f_1(x_1) = bx_1 + 0.5(a-b)(|x_1+1| - |x_1-1|)$. Typical values of the parameters are $(\alpha, \beta, a, b) = (10, 18, -4/3, -3/4)$. β depends on the inductance value which has an uncertainty resulting in $\theta = \Delta\beta = 1.25$ that is supposed unknown to the response system. We consider that the current through the inductor is being measured and sent to the response system to synchronize it. Then the uncertain system in a compact form can be written

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\end{bmatrix} = \begin{bmatrix}-10 & 10 & 0\\ 1 & -1 & 1\\ 0 & -18 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} + \begin{pmatrix}f_1(x_1)\\ 0\\ 0\end{pmatrix} + \begin{bmatrix}0\\ 0\\ 1\end{bmatrix}x_2\theta \tag{11}$$

$$y = [\,0 \quad 0 \quad 1\,]x = x_3 \tag{12}$$

The above system is in the form of (1). By choosing

$$L = \begin{bmatrix}0.5\\ -29\\ 25\end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix}0.1 & 0.05 & 0\\ 0.05 & 0.1 & 0\\ 0 & 0 & 0.1\end{bmatrix} \quad \text{then } Q = \begin{bmatrix}2 & -1.1 & 0\\ -1.1 & 2 & 0.1\\ 0 & 0.1 & 2\end{bmatrix}$$

we find that $B^{\mathrm{T}}P = 0.1C$ and

$$2.58 = 1.33 + 1 \times 1.25 \times 1 = k_f + k_\Phi\|\theta\|\|B\| < \frac{\lambda_{\min}(Q)}{2\lambda_{\max}(P)} = 2.985$$

thus ($\mathscr{H}1$) and ($\mathscr{H}2$) are satisfied and therefore an observer-based response system can be designed as follows

$$\begin{bmatrix}\dot{\hat{x}}_1\\ \dot{\hat{x}}_2\\ \dot{\hat{x}}_3\end{bmatrix} = \begin{bmatrix}-10 & 10 & 0\\ 1 & -1 & 1\\ 0 & -18 & 0\end{bmatrix}\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\end{bmatrix} + \begin{pmatrix}f_1(\hat{x}_1)\\ 0\\ 0\end{pmatrix} + LC(x_3 - \hat{x}_3) \tag{13}$$

$$\dot{\hat{\theta}} = 2.5\hat{x}_2(x_3 - \hat{x}_3) \tag{14}$$

The above systems were simulated using a fourth order Runge-Kutta integration algorithm of MATLAB 6 with the following initial conditions $(x_1(0), x_2(0), x_3(0)) = (2, -0.5, -2)$ and $(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0), \hat{\theta}(0)) = (0, 0, 0, 0)$. Fig. 1 delineates the synchronization of the drive and the response system and the estimation of the uncertainty.

3.2. Lorenz system

Lorenz system is another typical chaotic system that has been thoroughly studied. It is described by the following equations

$$\dot{x}_1 = -\sigma_1 x_1 + \sigma_2 x_2$$

$$\dot{x}_2 = rx_1 - x_2 - x_1x_3$$

$$\dot{x}_3 = x_1x_2 - bx_3$$

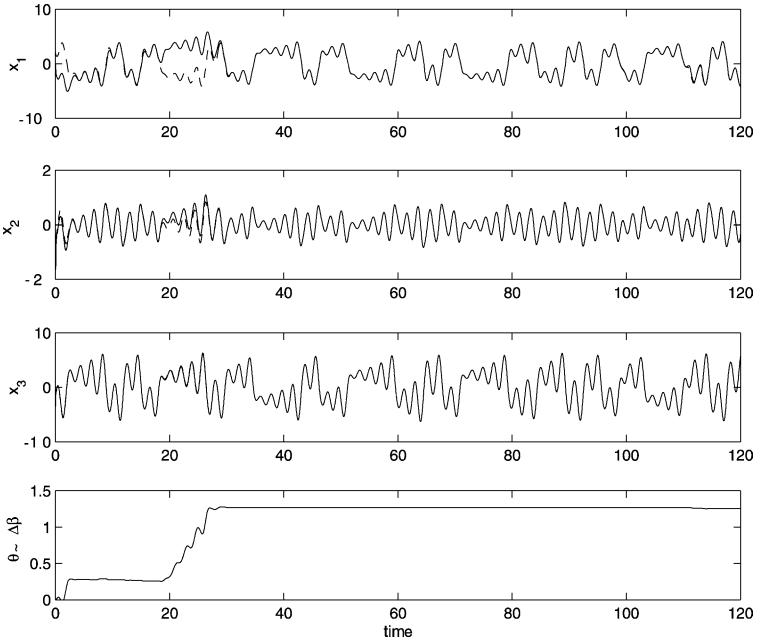

Fig. 1. Adaptive observer-based synchronization of Chua's circuit.

It is well known that the system exhibits chaotic behavior with the following parameters, $(\sigma_1, \sigma_2, r, b) = (10, 10, 28, 8/3)$. We suppose that σ_1 is known with an uncertainty $\theta = \Delta\sigma_1 = 2.5$. Next, we consider that x_1 is the signal used for synchronization. The uncertain system in a compact form can be written

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -\frac{8}{3} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{pmatrix} 0 \\ -x_1x_3 \\ x_1x_2 \end{pmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} (-y)\theta \tag{15}$$

$$y = [1 \quad 0 \quad 0]x = x_1 \tag{16}$$

The above system is in the form of (10). Let us choose

$$L = \begin{bmatrix} 0 \\ 38 \\ 0 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix} \quad \text{then} \quad Q = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0.2 & 0 \\ 0 & 0 & 0.53 \end{bmatrix}$$

we can check that $(\mathscr{H}1')$ and $(\mathscr{H}2')$ are satisfied and therefore an observer-based response system can be designed as follows

$$\begin{bmatrix} \dot{\hat{x}}_1 \\ \dot{\hat{x}}_2 \\ \dot{\hat{x}}_3 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & \frac{8}{3} \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \end{bmatrix} + \begin{pmatrix} 0 \\ -\hat{x}_1\hat{x}_3 \\ \hat{x}_1\hat{x}_2 \end{pmatrix} + LC(x_1 - \hat{x}_1) \tag{17}$$

$$\dot{\hat{\theta}} = -5y(x_1 - \hat{x}_1) \tag{18}$$

The above systems were simulated using a fourth order Runge-Kutta integration algorithm of MATLAB 6 with the following initial conditions $(x_1(0), x_2(0), x_3(0)) = (10, 15, 10)$ and $(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0), \hat{\theta}(0)) = (0, 0, 0, 0)$. Fig. 2 delineates the synchronization of the drive and the response system and the estimation of the uncertainty. We note that the synchronization is rapidly achieved despite the very different initial conditions, and the unknown uncertainty is also quickly estimated to the right value.

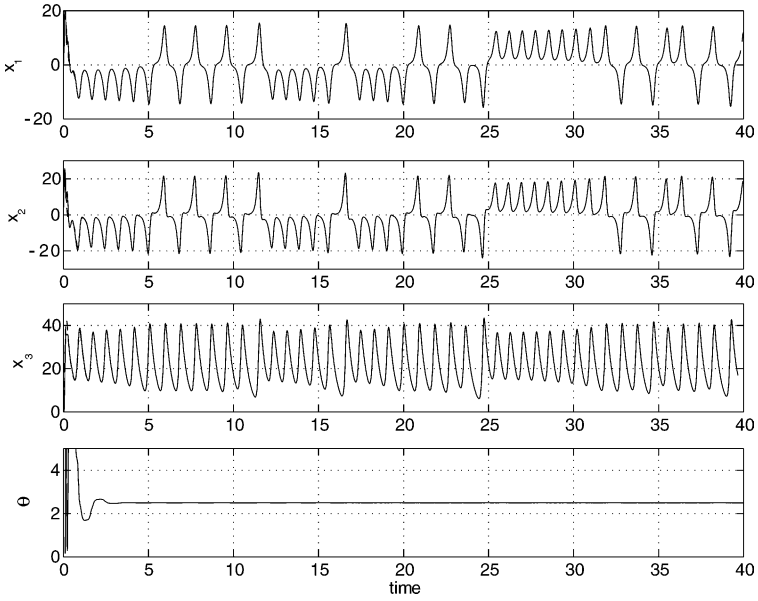

Fig. 2. Adaptive observer-based synchronization of Lorenz system.

4. Secure communication using parameter modulation

Secure communication has been an interesting field of application of chaotic synchronization since the last decade [21–23]. Due to their unpredictability and broad band spectrum, chaotic signals have been used to encode information by simple masking (addition) or using modulation. As a matter of fact, since the synchronization scheme proposed in the previous section can correctly estimate the unknown constant uncertainty of the drive system parameter, one can expect that it can also estimate slow varying changes such that $\dot{\theta} \approx 0$ or piecewise constant uncertainty such that $\dot{\theta} = 0$

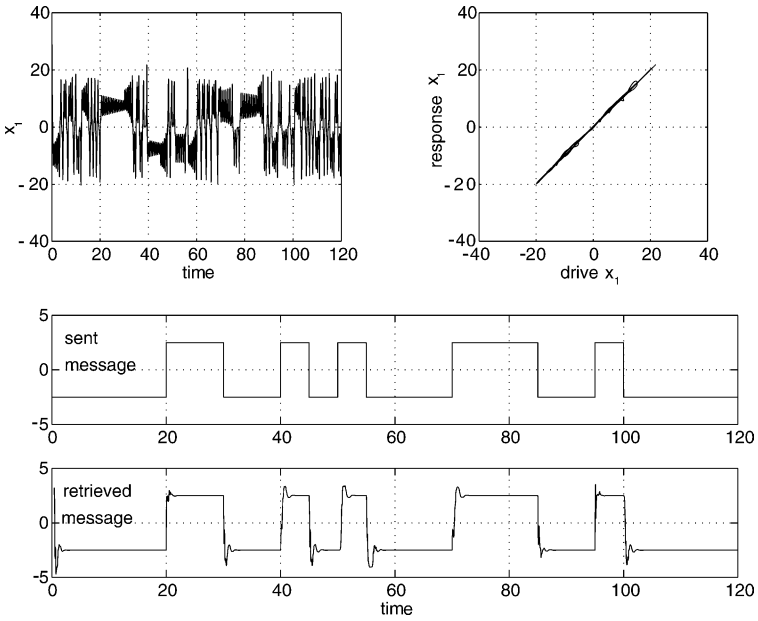

Fig. 3. Secure communication using Lorenz system via noiseless channel.

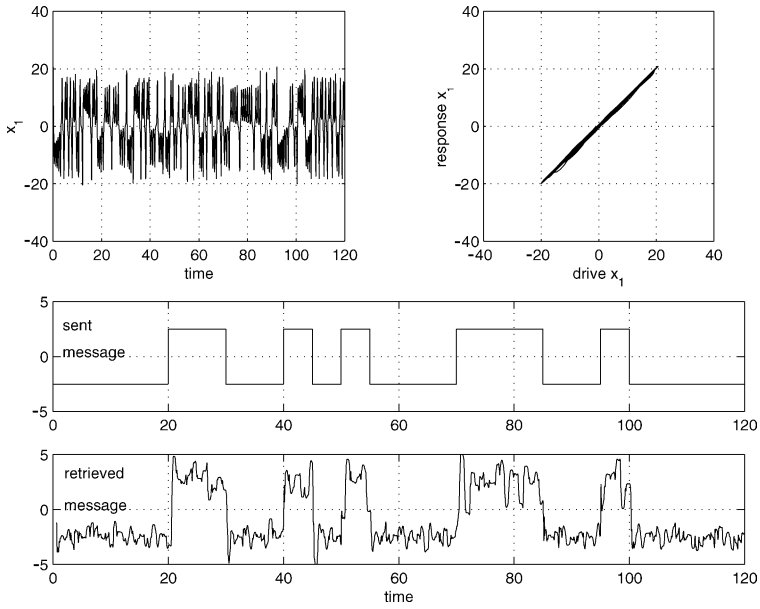

Fig. 4. Secure communication using Lorenz system via noisy channel.

everywhere except at some discrete instants of time. Therefore if a drive system parameter changes its value from the nominal one according to the level of a digital information signal, the response system can estimate these variations and hence the modulating information signal. As an example, we present the Lorenz system with σ_1 being modulated by a digital information signal, so that we have $\sigma_1 = \sigma_1^n + 2.5$ if the modulating bit is "1" and $\sigma_1 = \sigma_1^n - 2.5$ if the modulating bit is "0". It is important that the bit duration T_b be much larger than the convergence time of the adaptation law, hence the unknown uncertainty can be assumed to be piecewise constant. Fig. 3 shows that the information is not perceived in the sent signal x_1. The drive-response synchronization is well obtained and the sent message is retrieved with a good quality. Moreover, since the synchronization is asymptotically achieved, we can expect to have some robustness with respect to low noise level. The same simulations were carried with a zero mean channel noise representing 2.5% of the sent signal level. The obtained results are depicted in Fig. 4. It is shown that synchronization is obtained and the retrieved message can be filtered using a threshold detector set at zero.

5. Conclusion

In this paper we showed that given a single driving signal of a drive chaotic system, we can concurrently obtain synchronization and estimation of a constant unknown parameter at the response system side. The result is obtained using an adaptive observer. We demonstrated that information about the parameters of a chaotic system is embedded in the time series data of a state variable and can be extracted under mild conditions. Consequently, a parameter of the drive system can be stirred to vary in a piecewise constant manner according to an information modulating signal. The estimation of the parameter variations leads to information reconstruction at the response system side. Hence the drive-response systems are used as transmitter–receiver systems for secure communication.

References

[1] Pecora LM, Carroll TL. Driving systems with chaotic signals. Phys Rev A 1991;44(4):2374–83.
[2] Ogorzalek M. Taming chaos—Part-I: Synchronization. IEEE Trans Circ Syst I 1993;40(10):693–9.
[3] Morgül Ö, Feki M. On the synchronization of chaotic systems by using occasional coupling. Phys Rev E 1997;55(5):5004–9.
[4] Boccaletti S, Kurths J, Osipov G, Valladares D, Zhou C. The synchronization of chaotic systems. Phys Rep 2002;366:1–101.
[5] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64(8):821–4.
[6] Chua L, Itoh M, Kocarev L, Eckert K. Chaos synchronization in Chua's circuit. J Circ Syst Comput 1993;3(1):93–108.

[7] Hasler M. Synchronization principles and applications. In: IEEE Int. Symp. Circuits and Systems, New York, 1994. p. 314–27 [Chapter 6.2].
[8] Feldmann U, Hasler M, Schwarz W. Communication by chaotic signals: the inverse system approach. In: IEEE Int Symp Circuits and Systems, Vol. 1. Seattle, 1995. p. 3–6.
[9] Morgül Ö, Solak E. Observer based synchronization of chaotic signals. Phys Rev E 1996;54(5):4803–11.
[10] Morgül Ö, Solak E. On the synchronization of chaotic systems by using state observers. Int J Bifurcat Chaos 1997;7(6):1307–22.
[11] Nijmeijer H, Mareels IM. An observer looks at synchronization. IEEE Trans Circ Syst I 1997;44(10):882–90.
[12] Feng L, Yong R, Shan X, Qiu Z. A linear feedback synchronization theorem for a class of chaotic systems. Chaos, Solitons & Fractals 2002;13(4):723–30.
[13] Feki M, Robert B. Observer-based chaotic synchronization in the presence of unknown inputs. Chaos, Solitons & Fractals 2003;15:831–40.
[14] Feki M. Observer-based exact synchronization of ideal and mismatched chaotic systems. Phys Lett A, submitted for publication.
[15] Liao T-L, Tsai S-H. Adaptive synchronization of chaotic systems and its application to secure communications. Chaos, Solitons & Fractals 2000;11(9):1387–96.
[16] Andrievsky B. Adaptive synchronization methods for signal transmission on chaotic carrier. Math Comput Simul 2002;58:285–93.
[17] Marino R, Tomei P. Nonlinear control design—geometric, adaptive, robust. Englewood Cliffs, NJ: Prentice-Hall; 1995.
[18] Khalil HK. Nonlinear systems. New York: Macmillan; 1992.
[19] Besançon G. Remarks on nonlinear adaptive observer design. Syst Control Lett 2000;41:271–80.
[20] Kennedy MP. Bifurcation and chaos. In: Chen WK, editor. The circuits and filters handbook. USA: IEEE Press; 1995. p. 1089–163 [Chapter VII-38].
[21] Cuomo KM, Oppenheim AV, Strogatz SH. Synchronization of Lorenzed-based chaotic circuits with applications to communications. IEEE Trans Circ Syst II 1993;40(10):626–33.
[22] Dedieu H, Kennedy MP, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit. IEEE Trans Circ Syst II 1993;40(10):634–42.
[23] Morgül Ö, Feki M. A chaotic masking scheme by using synchronized chaotic systems. Phys Lett A 1999;251(3):169–76.