International Journal of Bifurcation and Chaos, Vol. 13, No. 4 (2003) 1003–1017

OBSERVER BASED CHAOTIC MESSAGE TRANSMISSION

ÖMER MORGÜL*, ERCAN SOLAK and MURAT AKGÜL
Department of Electrical and Electronics Engineering, Bilkent University, 06533, Bilkent, Ankara, Turkey
**morgul@ee.bilkent.edu.tr*

Received June 1, 2001; Revised March 25, 2002

We consider observer based synchronization of continuous-time chaotic systems. We present two message transmission schemes for such systems. The first one is based on chaotic masking and modulation, and the second one is based on only chaotic modulation. We show that in these schemes, the message may be recovered under certain conditions. We show that the proposed schemes are robust with respect to noise and parameter mismatch. We also present some simulation results.

Keywords: Chaotic systems; chaos synchronization; message chaotic communication.

1. Introduction

After the seminal works of Pecora and Carrol [1990, 1991], the idea of synchronization and control of chaotic systems has received a great deal of interest among researchers from various fields. Many scientific journals in fact devoted special issues on these and related subjects, see e.g. *IEEE Trans. Circuits Syst., Part 1*, October 1997 and December 2000, *Int. J. Bifurcation and Chaos*, March and April 2000 issues. For more information on this subject and for more references, see [Chen & Dong, 1998; Boccaletti *et al.*, 2000]. While the synchronization of two chaotic systems is an interesting subject on its own, one of the main motivations for the research in this area is the possibility of using chaotic signals for secure communication, see [Cuomo & Oppenheim, 1993; Kocarev & Parlitz, 1995; Okşaşoğlu & Akgül, 1995; Hasler, 1995]. Use of chaos may also increase the performance of communication systems, see e.g. [Kolumbán *et al.*, 1997]. Most of the synchronization schemes consist of two parts: a generator of chaotic signals, which is called the drive system, and a receiver, which is also called a response system. A signal generated by the drive system may be used as an input to the receiver to achieve synchronization. An extensive list of references for various aspects of chaotic systems may be found in [Chen, 1997].

Chaotic systems may be used in message transmission in various ways, see e.g. [Hasler, 1995; Kolumbán *et al.*, 1997]. One of the widely used techniques is called chaotic masking, and in this scheme the message is added to the chaotic signal used for synchronization, and this signal is sent to the receiver. Under certain conditions the message may be recovered at the receiver, see [Cuomo & Oppenheim, 1993; Kocarev & Parlitz, 1995; Kocarev *et al.*, 1992; Liao & Huang, 1999; Okşaşoğlu & Akgül, 1995]. Another possibility is to use the message as an appropriate input to the drive system, and send the synchronization signal to the receiver. This scheme may be called as chaotic modulation, and as in chaotic masking scheme, the message may be recovered in the receiver under certain conditions.

In this paper, we will consider continuous-time chaotic systems. For the synchronization of such systems various methods are available, and we choose the method based on observers, see [Morgül & Solak, 1996, 1997; Morgül, 1999]. For the message transmission, we propose two schemes.

The first one is based on chaotic modulation and masking, and is a slight modification of the scheme proposed in [Liao & Huang, 1999]. The second scheme is based only on chaotic modulation. We will show that in these schemes, under certain conditions the message may be recovered in the receiver.

This paper is organized as follows. In Sec. 2, we will briefly outline the observer based synchronization scheme. In Sec. 3, we will propose a chaotic masking scheme, which is similar to the scheme proposed in [Liao & Huang, 1999]. In the following section we show that the proposed scheme is robust with respect to noise and parameter mismatch under certain conditions. This method may have some disadvantages, and to eliminate these, we propose a chaotic modulation scheme in Sec. 5. We also give a robustness result for this scheme as well. We will present some simulation results in Sec. 6, and finally we will give some concluding remarks.

2. Observer Based Synchronization

Let a chaotic (drive) system be given as:

$$\dot{u} = f(u)\,, \quad o = c(u)\,, \tag{1}$$

where $u \in \mathbf{R}^n$, f: $\mathbf{R}^n \to \mathbf{R}^n$ and c: $\mathbf{R}^n \to \mathbf{R}^m$ are differentiable functions, and o is the synchronization signal to be sent to the response system. Later, for simplicity, we will choose $m = 1$, i.e. a scalar synchronization signal. An observer for (1) is another system of the form

$$\dot{v} = g(v, o)\,, \quad u_r = k(v, o)\,, \tag{2}$$

where $v \in \mathbf{R}^l$, g: $\mathbf{R}^l \times \mathbf{R}^m \to \mathbf{R}^l$ and k: $\mathbf{R}^l \times \mathbf{R}^m \to \mathbf{R}^n$ are differentiable functions. Let the error signal be defined as $e = u - u_r$. The system (2) is called a local observer for (1) if $e(t) \to 0$ as $t \to \infty$ for all sufficiently small $e(0)$, i.e. when $\|e(0)\| < \gamma$ for some $\gamma > 0$. If $\gamma = \infty$, then the observer is global. As noted in [Morgül, 1999], many synchronization schemes proposed in the literature are in fact observer based schemes.

In this paper, we will assume the following form for the chaotic drive system:

$$\dot{u} = Au + f(u) + h(t)\,, \quad o = Cu\,, \tag{3}$$

where $A \in \mathbf{R}^{n\times n}$ and $C \in \mathbf{R}^{1\times n}$ are constant matrices, f: $\mathbf{R}^n \to \mathbf{R}^n$ is a smooth function, and h: $\mathbf{R} \to \mathbf{R}^n$ is a known forcing function. (Note that certain chaotic systems, such as Duffing oscillator, contains such a known forcing function, and with the inclusion of such a term in (3), we will be able to cover such systems as well.) For the response system, we use the following observer

$$\dot{\hat{u}} = A\hat{u} + f(\hat{u}) + h(t) + K(o - \hat{o})\,, \quad \hat{o} = C\hat{u}\,, \tag{4}$$

where $K \in \mathbf{R}^n$ is a gain vector to be selected. Note that (4) is in the form given by (2), where we have $u_r = \hat{u}$. By defining the error as $e = u - \hat{u}$, and using (3) and (4), we obtain the following error dynamics:

$$\dot{e} = (A - KC)e + f(u) - f(\hat{u})\,. \tag{5}$$

Obviously, if $\|e(t)\| \to 0$ as $t \to \infty$, then synchronization is achieved. Moreover, if the following holds for some $M > 0$, $\delta > 0$

$$\|e(t)\| \le Me^{-\delta t}\|e(0)\|\,, \tag{6}$$

then we say that the synchronization is exponential. Local and global exponential synchronization may be defined similarly. We note that the norm $\|\cdot\|$ may be any norm on $\mathbf{R}^n$. If the pair (A, C) is observable, then we can always find gain vectors K such that the matrix $A - KC$ is stable, i.e. all eigenvalues have negative real parts, see e.g. [Morgül & Solak, 1996, 1997]. A related condition, which is called detectability, is a necessary condition for synchronization in certain cases, see [Morgül, 1999]. On the other hand, observability is a sufficient condition for exponential synchronization in many cases, see e.g. [Grassi & Mascolo, 1997; Morgül & Solak, 1996, 1997; Nijmeijer & Mareels, 1997]. These cases include the following.

(i) Assume that f is Lipschitz, i.e. the following is satisfied for some $\gamma > 0$:

$$\|f(u) - f(\hat{u})\| \le \gamma\|u - \hat{u}\|\,. \tag{7}$$

If γ is sufficiently small, then one can always choose a gain vector K such that (6) holds, see [Morgül & Solak, 1996, 1997].

(ii) When the system given by (3) is in Brunowsky canonical form and (7) holds, then for any $\gamma > 0$ one can always choose a gain vector K such that (6) holds, see [Morgül & Solak, 1996, 1997]. Note that many systems are already in this form, or can be transformed into this form, e.g. Rössler system, almost all forced chaotic oscillators, etc.

(iii) Assume that the nonlinearity f in (3) depends only on the measured signal o, i.e. the following holds:

$$f(u) = g(o)\,, \tag{8}$$

for some g: $\mathbf{R} \to \mathbf{R}^n$. In this case, the observer (4) could be selected as:

$$\dot{\hat{u}} = A\hat{u} + g(o) + h(t) + K(o - \hat{o})\,, \quad \hat{o} = C\hat{u}\,. \tag{9}$$

The error dynamics (5) now becomes:

$$\dot{e} = (A - KC)e\,. \tag{10}$$

Hence, one can choose a gain vector K such that (6) holds, see [Morgül & Solak, 1996, 1997]. We note that some chaotic systems, e.g. Lur'e systems, are already in this form, and some chaotic systems, e.g. such as Duffing oscillator, and most of the electronic chaotic oscillators such as Chua's circuit, can be transformed into this form.

3. A Chaotic Modulation and Masking Scheme

Let us assume that for the chaotic drive system given by (3), by using either of the observers given by (4) or (9), and with an appropriate choice of the gain vector K, exponential synchronization is achieved, i.e. (6) holds. Let $m(t)$ denote the message to be sent. We will use the synchronization signal $o(t)$ given by (3) to mask the message, hence we assume that both signals have the same dimension. If we use (4) as the observer, we will modify the drive system as follows:

$$\dot{u} = Au + f(u) + h(t) + Km\,, \quad o = Cu + m\,. \tag{11}$$

Note that in this case the signal o sent to the receiver is the masked message. Obviously, the message m should be sufficiently small so that (11) still generates chaotic signals. This might reduce the magnitude of m considerably if the gain K required for synchronization is too high. Note that in this case the error dynamics given by (5) is still valid, hence (6) still holds. Therefore if we define the recovered message m_r as:

$$m_r(t) = o(t) - \hat{o}(t) = Ce(t) + m(t)\,, \tag{12}$$

it follows from (6) that $m_r(t) \to m(t)$ as $t \to \infty$. Moreover, in most of the cases the decay rate δ could be adjusted by using the gain K, hence we may have arbitrary fast recovery of the message. We note that this scheme is quite similar to the one proposed in [Liao & Huang, 1999]. The only difference is in the assumed form of the nonlinearity $f(\cdot)$. In [Liao & Huang, 1999], the nonlinearity is assumed to depend on the synchronization signal o as well, i.e. f has the form $f(u, o)$, and this form is used in (4) and (11). Hence, in [Liao & Huang, 1999], the message is not only injected into (3) as a linear term (i.e. Km), but is also injected into the nonlinearity, whereas in our case, the message is only injected into the chaotic drive system as a linear term.

If the nonlinearity f has the form given by (8) and the observer is given by (9), we modify the drive system given by (3) as

$$\dot{u} = Au + g(o) + h(t) + Km\,, \quad o = Cu + m\,. \tag{13}$$

For the receiver system, we use the observer given by (9). Consequently, (10) and hence (6) are valid, and the message can be recovered by using (12). In this case, the decay rate δ could be adjusted arbitrarily by using appropriate K.

4. Robustness of the Proposed Scheme

To analyze the robustness of the proposed scheme with respect to noise and parameter mismatch, let us rewrite the drive and the response systems as follows:

$$\begin{aligned} &\dot{u} = A(\mu)u + f(u, \mu) + h(t) + Km\,, \\ &o = Cu + m\,, \end{aligned} \tag{14}$$

$$\begin{aligned} &\dot{\hat{u}} = A(\hat{\mu}) + f(\hat{u}, \hat{\mu}) + \hat{h}(t) + \hat{K}(o + n - \hat{o})\,, \\ &\hat{o} = C\hat{u}\,, \end{aligned} \tag{15}$$

where a hat denotes the variables and parameters which are used in the response system, μ, $\hat{\mu} \in \mathbf{R}^p$ are the parameter vectors used in the drive and the response systems, respectively, and n is the noise. In the ideal case, obviously we have $\mu = \hat{\mu}$, $h(t) = \hat{h}(t)$, $K = \hat{K}$, $n = 0$, and in this case we assume that the exponential synchronization holds, e.g. see (6). For robustness, we will assume that both $A(\cdot)$ and $f(u, \cdot)$ satisfy the following Lipschitz properties

$$\begin{aligned} &\|A(\mu_1) - A(\mu_2)\| \le k_a \|\mu_1 - \mu_2\|\,, \\ &\forall\, \mu_1, \mu_2 \in \mathbf{R}^p\,, \end{aligned} \tag{16}$$

$$\|f(u,\mu_1) - f(u,\mu_2)\| \le k_\mu \|\mu_1 - \mu_2\|\,,$$
$$\forall\, u \in \mathbf{R}^n, \forall\, \mu_1, \mu_2 \in \mathbf{R}^p\,, \tag{17}$$

where k_a and k_μ are appropriate positive constants. We note that the Lipschitz properties are satisfied locally if both $A(\cdot)$ and $f(u,\cdot)$ are differentiable with respect to μ. Let $\mathcal{U} \subset \mathbf{R}^n$ be a region which contains the chaotic attractor of (14) and let $\mathcal{M} \subset \mathbf{R}^p$ be a region containing the relevant parameter values for which (14) exhibits chaotic behavior. The following analysis will remain valid if (16) and (17) are satisfied locally for $u \in \mathcal{U}$ and $\mu_1, \mu_2 \in \mathcal{M}$.

Let us define the error as $e = u - \hat{u}$. By adding and subtracting likewise terms, we obtain the following error equation

$$\begin{aligned}\dot{e} = {} & [(A(\mu) - KC)e + f(u,\mu) - f(\hat{u},\mu)] \\ & + [A(\mu) - A(\hat{\mu})]\hat{u} + [f(\hat{u},\mu) - f(\hat{u},\hat{\mu})] \\ & + [K - \hat{K}]Ce + [h(t) - \hat{h}(t)] \\ & + [K - \hat{K}]m - \hat{K}n\,. \end{aligned} \tag{18}$$

Note that the first bracketed term in (18) is the same as the right side of (5); the remaining terms are the contributions of parameter mismatch and noise to the error equation. Let $u(t)$ and $\hat{u}(t)$ be the solutions of (14) and (15), respectively, and define $F(e,t) = (A(\mu) - KC)e + f(u,\mu) - f(\hat{u},\mu)$. Hence, in the ideal case (18) reduces to $\dot{e} = F(e,t)$. Since this dynamics is exponentially stable by assumption, by a well-known result in Lyapunov stability theory, there exists a Lyapunov function $V : \mathbf{R} \times \mathbf{R}^n \to \mathbf{R}$ which satisfies the following:

$$c_1\|e\|^2 \le V(t,e) \le c_2\|e\|^2\,, \tag{19}$$

$$\dot{V} = \frac{\partial V}{\partial t} + \frac{\partial V}{\partial e}F \le -c_3\|e\|^2\,, \tag{20}$$

$$\left\| \frac{\partial V}{\partial e} \right\| \le c_4\|e\|\,, \tag{21}$$

for some positive constants c_1, c_2, c_3, c_4. Note that the existence of such a Lyapunov function is both necessary and sufficient for the exponential stability of the error dynamics, see e.g. [Khalil, 2002, p. 162]. Moreover, the constants in (6) can be given as $M = \sqrt{c_2/c_1}$, $\delta = c_3/2c_2$.

Let us consider the nonideal case. By using the Lyapunov function V given above and by using (18), we obtain:

$$\begin{aligned}\dot{V} = {} & \frac{\partial V}{\partial t} + \frac{\partial V}{\partial e}F + \frac{\partial V}{\partial e}[A(\mu) - A(\hat{\mu})]\hat{u} \\ & + \frac{\partial V}{\partial e}[f(\hat{u},\mu) - f(\hat{u},\hat{\mu})] + \frac{\partial V}{\partial e}[K - \hat{K}]Ce \\ & + \frac{\partial V}{\partial e}[h(t) - \hat{h}(t)] + \frac{\partial V}{\partial e}[K - \hat{K}]m \\ & - \frac{\partial V}{\partial e}\hat{K}n\,. \end{aligned} \tag{22}$$

Let the noise n and the message m satisfy $|n(t)| \le n_m$ and $|m(t)| \le \overline{m}$ for some $n_m > 0$ and $\overline{m} > 0$, respectively. Moreover, let $\|h(t) - \hat{h}(t)\| \le \Delta h_m$ and $\|\hat{u}\| \le \hat{u}_m$ be satisfied for some $\Delta h_m > 0$ and $\hat{u}_m > 0$, respectively. Let us define $\Delta\mu = \|\mu - \hat{\mu}\|$ and $\Delta K = \|K - \hat{K}\|$. By using (16), (17) and (19)–(21), we obtain

$$\begin{aligned}\dot{V} \le -c_3\|e\| \Bigg\{ & \left(1 - \frac{c_4}{c_3}\Delta K\|C\|\right)\|e\| \\ & - \frac{c_4}{c_3}(k_a\hat{u}_m + k_\mu)\Delta\mu \\ & - \frac{c_4}{c_3}(\Delta h_m + \|\hat{K}\|n_m + \overline{m}\Delta K)\Bigg\}\,. \end{aligned} \tag{23}$$

Let us define $D = 1 - c_4/c_3\Delta K\|C\|$, $K_1 = c_4/c_3(k_a\hat{u}_m + k_\mu)$, $K_2 = c_4/c_3$, $K_3 = c_4/c_3\|\hat{K}\|$, $K_4 = (c_4/c_3)\overline{m}$. Let us assume that ΔK is sufficiently small so that $D > 0$. From (23) it follows that if $\|e\| > (K_1\Delta\mu + K_2\Delta h_m + K_3 n_m + K_4\Delta K)/D$, then $\dot{V} < 0$, hence V decreases, which implies that $\|e\|$ decreases as well, see (19). It then follows from the standard invariance arguments that asymptotically the error satisfies the following bound:

$$\|e\| \le C_1\Delta\mu + C_2\Delta h_m + C_3 n_m + C_4\Delta K\,, \tag{24}$$

where $C_i \ge K_i/D$, $i = 1,2,3,4$, see e.g. [Khalil, 2002, p. 323]. If we define the error in message recovery e_m as $e_m = m_r - m$, then from (12) we obtain $e_m = Ce$. By combining this result with (24) we see that a similar asymptotic bound for e_m is also valid, see Remark 2.

Remark 1. From (24) it follows that the asymptotic error depends linearly on the nonidealities $\Delta\mu$, Δh_m, and n_m. Hence, if these terms are small, the resulting error will be small as well. The dependence of the error on ΔK deserves special attention. Note that we have $D = 1 - (c_4/c_3)\Delta K\|C\|$

and $C_i \geq K_i/D$, $i = 1, 2, 3, 4$. Hence, as ΔK increases, D will decrease and consequently C_i will increase, which also increases the asymptotic error bound. For $D < 0$, the estimate given by (24) is not valid, hence ΔK cannot be made arbitrarily large. This argument shows that with the proposed method, ΔK should be made as small as possible.

Remark 2. Let us consider the recovered message $m_r(t)$ as given in (12) and define the error in message recovery e_m as $e_m = m_r - m$. From (12) we have $e_m = Ce$, where e denotes the synchronization error. If the error decay is exponential, then by using (6) we obtain:

$$\|e_m(t)\| \leq M\|C\|e^{-\delta t}\|e(0)\|\,. \tag{25}$$

Clearly, as $t \to \infty$, we have $e_m(t) \to 0$, hence $m_r(t) \to m(t)$, i.e. the message is recovered asymptotically. This property, together with the robustness result indicated above shows the importance of exponential synchronization. To elaborate further, let $\varepsilon_p > 0$ be a given precision level on the message error, i.e. we can recover the message successfully if $\|e_m(t)\| \leq \varepsilon_p$. (In this sense, the errors satisfying this bound may be called as acceptable errors.) Let us assume that $\|e(0)\| \leq R$ for some $R > 0$. (Note that if the chaotic attractor of (11) is inside of a ball in $\mathbf{R}^n$ whose radius is R_a, and if we choose $\hat{u}(0) = 0$, then we may choose $R = R_a$; if $\hat{u}(0)$ is also arbitrary in the same ball, then we may choose $R = 2R_a$.) Under these assumptions, from (25) it easily follows that we have $\|e_m(t)\| \leq \varepsilon_p$ for $t \geq T_p$ where

$$T_p = \frac{1}{\delta}\,\ln\frac{\varepsilon_p}{MR\|C\|}\,. \tag{26}$$

Hence, to guarantee successful message transmission, we may choose to apply the message for $t \geq T_p$, (e.g. use $m = 0$ in (11) for $t < T_p$).

The chaotic masking scheme presented in Sec. 3 yields exponential recovery of the message, hence is very efficient. However, the following points may be considered as possible drawbacks of this scheme.

(i) In some cases, the gain K which guarantees the exponential synchronization could be quite high, see e.g. [Solak, 1996]. On the other hand, the term Km used in (11) should not be too big to guarantee the chaotic solutions. Hence in case of high gain, we may be forced to send messages with small magnitudes. This may pose problems if the synchronization message is corrupted with noise.

(ii) The gain K may have arbitrary nonzero entries, hence the message need to be injected into (3) at more than one point. However, for some systems this may not be suitable and/or not possible (see e.g. the first simulation example).

(iii) Injection of the message into the nonlinearity may not be possible for some systems.

(iv) The gain K is a parameter used in the receiver end. However, in this scheme this parameter should also be known for the driver system as well. In some cases, it may be desirable to change the gains in the receiver, e.g. to improve the performance, and such a change will affect the driver system as well. This may require a communication between the driver and receiver systems, other than the transmission of the message, and it may not be suitable and/or desirable. See also Remark 1 to see the effect of this mismatch on the robustness of the proposed scheme.

To eliminate these problems, in the sequel we will propose a new message transmission scheme.

5. A Chaotic Modulation Scheme

Let us assume that the nonlinearity f in (3) is in the form given by (8) and let m be the message to be transmitted. We modify the chaotic drive system (3) as follows:

$$\dot{u} = Au + g(o) + h(t) + bm\,, \quad o = Cu\,, \tag{27}$$

where $b \in \mathbf{R}^n$ is a constant vector. We can choose the entries of b as 1 or 0, with nonzero entries denoting the possible entries of (3) to which the message can be injected. As for (11), we assume that the message magnitude is sufficiently small so that (27) has chaotic solutions. Note that in (11), the gain vector K may be too big, hence we may use messages with larger magnitudes in (27) as compared to (11). For the receiver system, we use the observer given by (9). The error equation (10) now becomes:

$$\dot{e} = (A - KC)e + bm\,. \tag{28}$$

Since the signal o is available at the receiver, we can measure $e_m = o - \hat{o} = Ce$. By using the Laplace transform in (28), we may relate the signals e_m and m. Let s denote the Laplace variable, and let the variables with capital letters such as

$E_m(s)$, $M(s)$, etc., denote the Laplace transform of the corresponding variables. From (28), we obtain:

$$E_m(s) = G(s)M(s)\,,$$
$$G(s) = C(sI - A + KC)^{-1}b\,. \tag{29}$$

Hence $e_m(t)$ is a *filtered* version of the message $m(t)$. Consequently, in some cases we may recover the message from e_m. These cases include the following.

Case 1. Let the message m be a *band-limited* signal, whose frequency spectrum is in the range $[0, \Omega]$. If $G(s)$ given by (29) is a low-pass filter whose cut-off frequency ω_c satisfies $\omega_c \gg \Omega$, then we can recover m. In most cases, by selecting the gain K appropriately, we can design such a $G(s)$. Moreover, since e_m is available, we may use another filter $G_1(s)$ to obtain another signal e_f as follows:

$$E_f(s) = G_1(s)E_m(s) = G_1(s)G(s)M(s)\,. \tag{30}$$

If we can choose G_1 and G such that $|1 - G_1(j\omega)G(j\omega)|$ is sufficiently small for $\omega \in [0, \Omega]$, then we may use $e_f(t)$ as the recovered message. We note that while in the masking scheme presented in the previous section we have asymptotic recovery of the message, in the present case there will always be error in the recovery, however this error may be made arbitrarily small by carefully selecting the gain K.

Case 2. Let the message m be a discrete signal, e.g. $m(t) \in \{0, 1\}$. In this case, it is possible to recover the message without error. To see this, we set $G(s) = n(s)/d(s)$ where $n(s)$ and $d(s)$ are polynomials as given below

$$n(s) = a_{n-1}s^{n-1} + \cdots + a_1 s + a_0\,,$$
$$d(s) = s^n + b_{n-1}s^{m-1} + \cdots + b_1 s + b_0\,, \tag{31}$$

where a_i and b_i are various constants, $i = 0, 1, \ldots, n-1$. We note that we may choose K appropriately so that $d(s)$ becomes a stable polynomial, i.e. all of its roots have negative real parts, moreover these roots may be selected arbitrarily, see [Morgül & Solak, 1996, 1997]. Let $\tilde{m}$ denote 0 or 1. After the transients, $e_m(t)$ will converge to $a_0\tilde{m}/b_0$. As for the transients, let T denote the interval length in which $m = 0$ or $m = 1$, and let s_i, $i = 1, 2, \ldots, n$ denote the roots of $d(s) = 0$. Since the transients contain the terms $e^{s_i t}$, these terms will become negligible within the interval T if $-\Re\{s_i\} \gg 1/T$, $i = 1, 2, \ldots, n$. Hence, the recovered message m_r may be given as

$$m_r(t) = \frac{b_0}{a_0} e_m(t)\,, \tag{32}$$

provided that $a_0 \neq 0$. We note that the roots s_i of $d(s)$ may be selected arbitrarily when A, C are an observable pair, see [Morgül & Solak, 1996, 1997], hence arbitrary fast decay of transient is possible. Furthermore, since m is discrete, we may even reconstruct the signal by comparing m_r with a threshold. Such a reconstructed signal m_c may be given as

$$m_c(t) = \begin{cases} 1 & \text{if} \quad m_r(t) > 0.5 \\ 0 & \text{if} \quad m_r(t) < 0.5 \end{cases}. \tag{33}$$

Obviously, this idea could be applied to any discrete message, i.e. when $m(t) \in \{a_1, \ldots, a_l\}$.

Case 3. In (27), instead of using the message directly, we may use a signal related to the message. Let $r(t)$ denote the message to be sent and let us choose the signal m used in (27) as follows:

$$M(s) = \frac{k}{G_p(s)}\, R(s)\,, \tag{34}$$

where k is a scaling constant, $G_p(s)$ is a new transfer function, M and R denote the Laplace transform of m and r, respectively. Let $G_p(s)$ be given as $G_p(s) = n_p(s)/d_p(s)$, where $n_p(s)$ and $d_p(s)$ are polynomials in s, see (31). Obviously, the polynomial $n_p(s)$ given by (31) should be stable to have bounded $m(t)$. Let, for any polynomial $q(s)$, $\deg(q)$ denote the degree of $q(s)$. In general, $\deg(n_p) \leq \deg(d_p)$, see (31), hence the derivatives of r should be available to generate m. Under these conditions, from (29) and (34) it follows that

$$R(s) = \frac{G_p(s)}{kG(s)}\, E_m(s)\,. \tag{35}$$

Note that $e_m(t)$ is available, hence to recover $r(t)$, the overall transfer function in (35) should be realizable. For this, (i) $n(s)$ in (31) should be a stable polynomial, and (ii) $\deg(d) + \deg(n_p) \leq \deg(n) + \deg(d_p)$ should hold. This is always satisfied if, e.g. we have $n_p(s) = 1$, and $\deg(d_p) = \deg(d)$. Under these conditions, the transfer overall function in (35) is realizable, hence we can recover $r(t)$. A special case is to choose $G_p(s) = G(s)$. In this case (35) becomes $R(s) = E_m/k$, hence we have

$r(t) \to e_m(t)/k$ as $t \to \infty$. However, note that in this case to generate $m(t)$ in the driver, we need to know the gain K of the receiver, cf. (29) and (34).

The scheme presented above was applied to a special class of chaotic systems, see (27). The same methodology may be used without this restriction in some cases. Assume that the chaotic drive system is given by (3). For the response system we will use the observer given by (4) and assume that with an appropriate choice of gain vector K, the error dynamics given by (5) is exponentially stable, i.e. (6) holds. Following (27), we first modify (3) as follows:

$$\dot{u} = Au + f(u) + h(t) + bm\,, \tag{36}$$

where m is the message to be transmitted, and $b \in \mathbf{R}^n$ is a constant vector as in (27). The error dynamics (5) now becomes:

$$\dot{e} = (A - KC)e + f(u) - f(\hat{u}) + bm\,. \tag{37}$$

If we compare (37) with (28) we see that they both contain the message as a linear addition to an exponentially stable error equation. However, the recovery of m from (37) may not be simple. If $f(\cdot)$ satisfies (7), then by choosing sufficiently high gain K, we may make the linear term dominant in (37). If the nonlinear terms in (37) have negligible effect, then the solution of (37) is similar to that of (28), hence we may use the techniques presented above. To elaborate further, let us assume that the message is discrete, e.g. $m(t) = \{0, \overline{m}\}$, and let T denote the interval length in which $m(t) = 0$ or $m(t) = \overline{m}$. When $m(t) = 0$, (37) reduces to (5). Since we assume that (6) holds in this case, we have $e_m(t) \to 0$, hence $e_m(t) \to m(t)$ for the period in which $m(t) = 0$. For the periods in which $m(t) = \overline{m}$, note that the term bm represents a perturbation to an exponentially stable dynamics given by (5), hence if $\overline{m}$ is small, e is also small. As before, let $e_m = Ce$ denote the measured error. If

$$\|C(A - KC)^{-1}(f(u) - f(\hat{u}))\| \ll 1\,, \tag{38}$$

then the effect of the nonlinear term in (37) on e_m may be neglected. For some cases, this may be possible by choosing K sufficiently big. If this is possible, then we may recover the message by using the techniques given above, see (32). Note that, due to the nonlinear terms, e_m may contain high frequency terms. These terms may be eliminated by further passing the signal e_m through a low pass filter, hence the recovered message may be improved. This approach may also be used when m is a band-limited signal.

Remark 3. We note that the scheme proposed above is also robust with respect to noise and parameter mismatch. This result could be proven by using the approach given in Sec. 4. Here we will present an alternative approach to the same problem. To be specific, let us consider the chaotic drive and the response systems given by (27) and (9), respectively, as follows:

$$\begin{aligned} \dot{u} &= A(\mu)u + g(o, \mu) + h(t) + bm\,, \\ o &= Cu\,, \end{aligned} \tag{39}$$

$$\begin{aligned} \dot{\hat{u}} &= A(\hat{\mu})\hat{u} + g(o + n, \hat{\mu}) + \hat{h}(t) + K(o + n - \hat{o})\,, \\ \hat{o} &= C\hat{u}\,, \end{aligned} \tag{40}$$

where μ, $\hat{\mu} \in \mathbf{R}^p$ are the parameter vectors, n is the channel noise, which is added to the transmitted signal o at the response system. Let us define the synchronization error as $e = u - \hat{u}$. By using (39) and (40), and by adding and subtracting likewise terms, we obtain:

$$\begin{aligned} \dot{e} = {} & (A(\mu) - KC)e + bm + [A(\mu) - A(\hat{\mu})]\hat{u} \\ & + [h(t) - \hat{h}(t)] + [g(o + n, \mu) - g(o + n, \hat{\mu})] \\ & + [g(o, \mu) - g(o + n, \mu)] - Kn\,. \end{aligned} \tag{41}$$

Note that the first two terms on the right-hand side of (41) are the same as (28), whereas the rest of the terms are due to parameter mismatch and noise, cf. (18). Since the gain K is only used in the response system, the term ΔK in (18) does not appear in (41). Similar to (16) and (17), we assume the following Lipschitz conditions:

$$\|A(\mu) - A(\hat{\mu})\| \le k_a\|\mu - \hat{\mu}\|\,, \quad \forall\, \mu, \hat{\mu} \in \mathbf{R}^p\,, \tag{42}$$

$$\begin{gathered} \|g(o, \mu) - g(o, \hat{\mu})\| \le k_\mu\|\mu - \hat{\mu}\|\,, \\ \forall\, o \in \mathbf{R}, \forall\, \mu, \hat{\mu} \in \mathbf{R}^p\,, \end{gathered} \tag{43}$$

$$\begin{gathered} \|g(o_1, \mu) - g(o_2, \mu)\| \le k_o\|o_1 - o_2\|\,, \\ \forall\, o_1, o_2 \in \mathbf{R}, \forall\, \mu \in \mathbf{R}^p\,. \end{gathered} \tag{44}$$

Since $A_c = A(\mu) - KC$ is stable by a proper choice of K, the exponential operator $e^{A_c t}$ is exponentially

stable, i.e. the following holds for some $M > 0$ and $\delta > 0$

$$\|e^{A_c t}\| \leq M e^{-\delta t}\,. \tag{45}$$

The solution of (41) can be given in the following form

$$\begin{aligned} e(t) = e^{A_c t}e(0) &+ \int_0^t e^{A_c(t-\tau)}bm(\tau)d\tau \\ &+ \int_0^t e^{A_c(t-\tau)}[h(\tau) - \hat{h}(\tau)]d\tau \\ &+ \int_0^t e^{A_c(t-\tau)}[A(\mu) - A(\hat{\mu})]\hat{u}(\tau)d\tau \\ &+ \int_0^t e^{A_c(t-\tau)}[g(o+n,\mu) - g(o+n,\hat{\mu})]d\tau \\ &+ \int_0^t e^{A_c(t-\tau)}[g(o,\mu) - g(o+n,\mu)]d\tau \\ &- \int_0^t e^{A_c(t-\tau)}Kn(\tau)d\tau\,. \end{aligned} \tag{46}$$

As before, assume that $|n(t)| \leq n_m$, $\|\hat{u}(t)\| \leq \hat{u}_m$ and $\|h(t) - \hat{h}(t)\| \leq \Delta h_m$ for some $n_m > 0$, $\hat{u}_m > 0$, and Δh_m, and let $\Delta\mu = \|\mu - \hat{\mu}\|$. By taking norms, using (45) and after simple integration we obtain:

$$\begin{aligned} \|e(t)\| \leq \|e^{A_c t}e(0) &+ \int_0^t e^{A_c(t-\tau)}bm(\tau)d\tau\| \\ &+ (1 - e^{-\delta t})(C_1\Delta\mu + C_2 n_m \\ &+ C_3\Delta h_m)\,, \end{aligned} \tag{47}$$

where $C_1 = M(k_a\hat{u}_m + k_\mu)/\delta$, $C_2 = M(k_o\|C\| + \|K\|)/\delta$, and $C_3 = M/\delta$. Here, the first term on the right-hand side of (47) is precisely the error obtained from (28). The rest of the terms give an upper bound for the contribution of the parameter mismatch and noise on the error. As can be seen, the contributions of these terms on the error is asymptotically bounded by the term $C_1\Delta\mu + C_2 n_m + C_3\Delta h_m$. Hence, for small $\Delta\mu$, Δh_m and n_m, this additional error will be small as well. Consequently, the effect of this small error on the message recovery will be small as well.

6. Simulation Results

In this section, we will give some simulation results. First, we consider the well-known forced Duffing equation. In this case, the chaotic drive system is given as:

$$\ddot{x} + 0.25x + x^3 = 11\cos t + m(t)\,, \tag{48}$$

where m is the message to be transmitted. It is known that this system exhibits chaotic behavior when $m(t) = 0$, see e.g. [Thompson, 1986]. We will use the solution x of (48) as the signal to be transmitted to the receiver, i.e. $o = x$. By using $x_1 = x$, $x_2 = \dot{x}$, we may rewrite (48) as follows:

$$\dot{x}_1 = x_2\,, \tag{49}$$

$$\begin{aligned} \dot{x}_2 &= -0.25x_1 - x_1^3 + 11\cos t + m(t)\,, \\ o &= x_1\,. \end{aligned} \tag{50}$$

This system is obviously in the form given by (27) with $C = (1\ \ 0)$, $b = (0\ \ 1)^T$ and $h(t) = 11\cos t$, where the superscript T denotes the transpose. For the receiver, we use the observer given by (9)

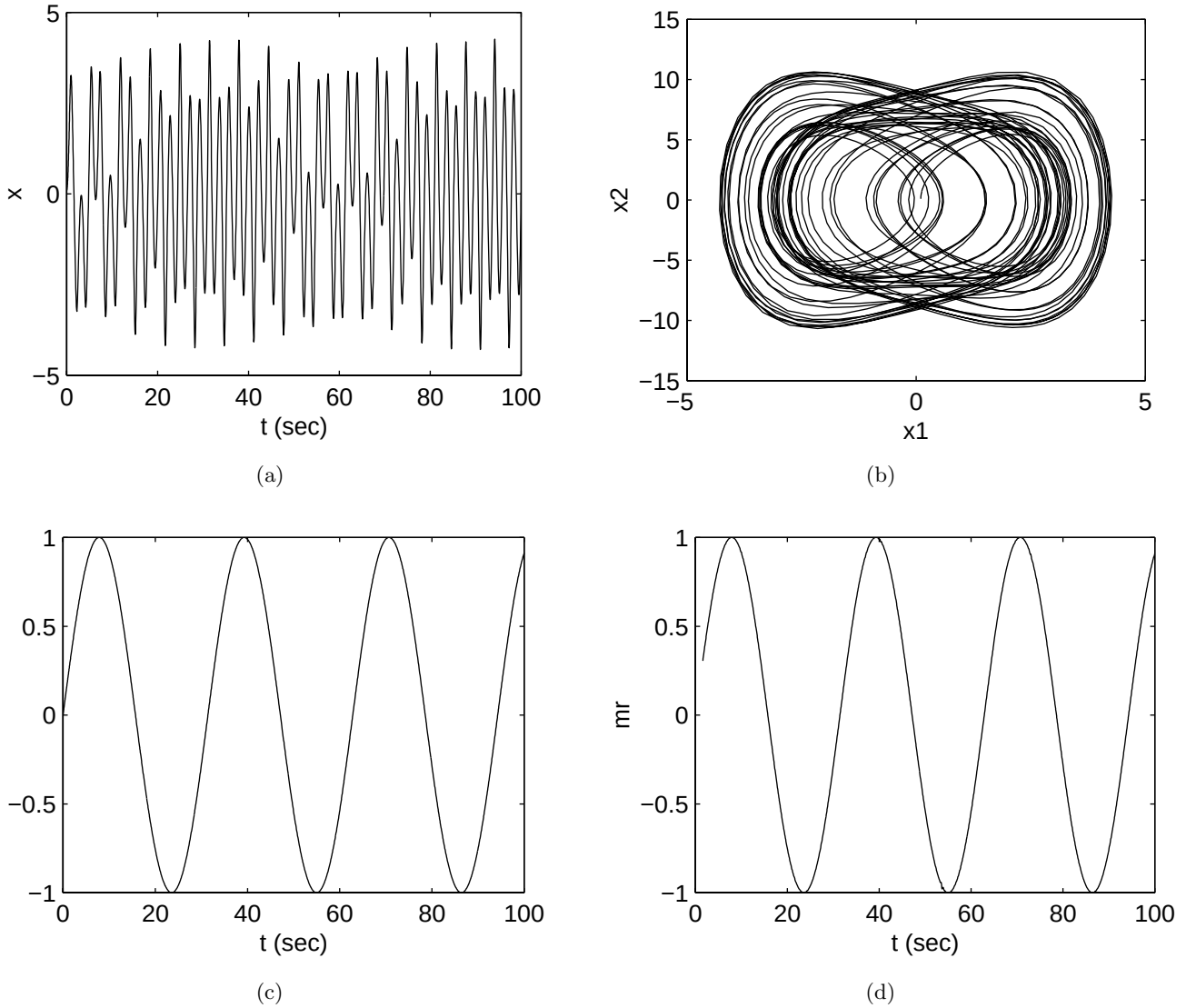
$$\dot{\hat{x}}_1 = \hat{x}_2 + k_1(x_1 - \hat{x}_1)\,, \tag{51}$$

$$\dot{\hat{x}}_2 = -0.25\hat{x}_1 - x_1^3 + 11\cos t + k_2(x_1 - \hat{x}_1)\,, \tag{52}$$

where k_1, k_2 are observer gains. Note that in this case, the message may only be injected into the equation of x_2, see (48), (50), hence for $k_1 \neq 0$, the scheme given by (11) is not appropriate. For this system, we performed the following two simulations.

Case i. We choose the message as $m(t) = \sin 0.2t$. Observer gains are chosen as $k_1 = 8$, $k_2 = 199.75$. In this case, $G(s)$ given by (29) is computed as $G(s) = 1/(s^2 + 8s + 200)$, and by choosing $G_1 = 200$, we have $|1 - G_1 G(j\omega)| = 0.008$ for $\omega = 0.2$. Hence, we may use $e_f = 200e_m$ as the recovered message, see (30). The results of this simulation is shown in Fig. 1. Here, Fig. 1(a) shows the transmitted message x, and Fig. 1(b) shows x versus $\dot{x}$. As can be seen, the solutions are chaotic. Figure 1(c) shows the message, and Fig. 1(d) shows the recovered message. As can be seen, the message is recovered with reasonable accuracy. Also note that, the message magnitude is comparable with the transmitted signal, see Figs. 1(a) and 1(c).

Case ii. We choose the message as the sum of three sinusoids as $r(t) = 0.5\sin t + 0.5\cos 0.5t + 0.5\sin 0.3t$. We choose the observer gains as $k_1 = 8$, $k_2 = 14.75$. In this case, $G(s)$ given by (29) is computed as $G(s) = 1/(s^2 + 8s + 15)$. In this case, we choose the signal m to be used in (50) as



(a) (b) (c) (d)

Fig. 1. Simulation result for Duffing system, case i (a) Transmitted signal x, (b) $x_1 = x$ versus $x_2 = \dot{x}$, (c) message, (d) recovered message m_r.

$m = (\ddot{r} + 8\dot{r} + 20r)/20$, hence (34) is satisfied with $k = 1/20$. Consequently, we have $20e_m(t) \to r(t)$. The results of this simulation are shown in Fig. 2. Here, Fig. 2(a) shows the transmitted message x, and Fig. 2(b) shows x versus $\dot{x}$. As can be seen, the solutions are chaotic. Figure 2(c) shows the message, and Fig. 2(d) shows the recovered message (as solid line), and the error in message recovery (dotted line). Also note that, the message magnitude is comparable with the transmitted signal, see Figs. 2(a) and 2(c).

Case iii. In this case, we choose the Lorenz system as the chaotic drive system:

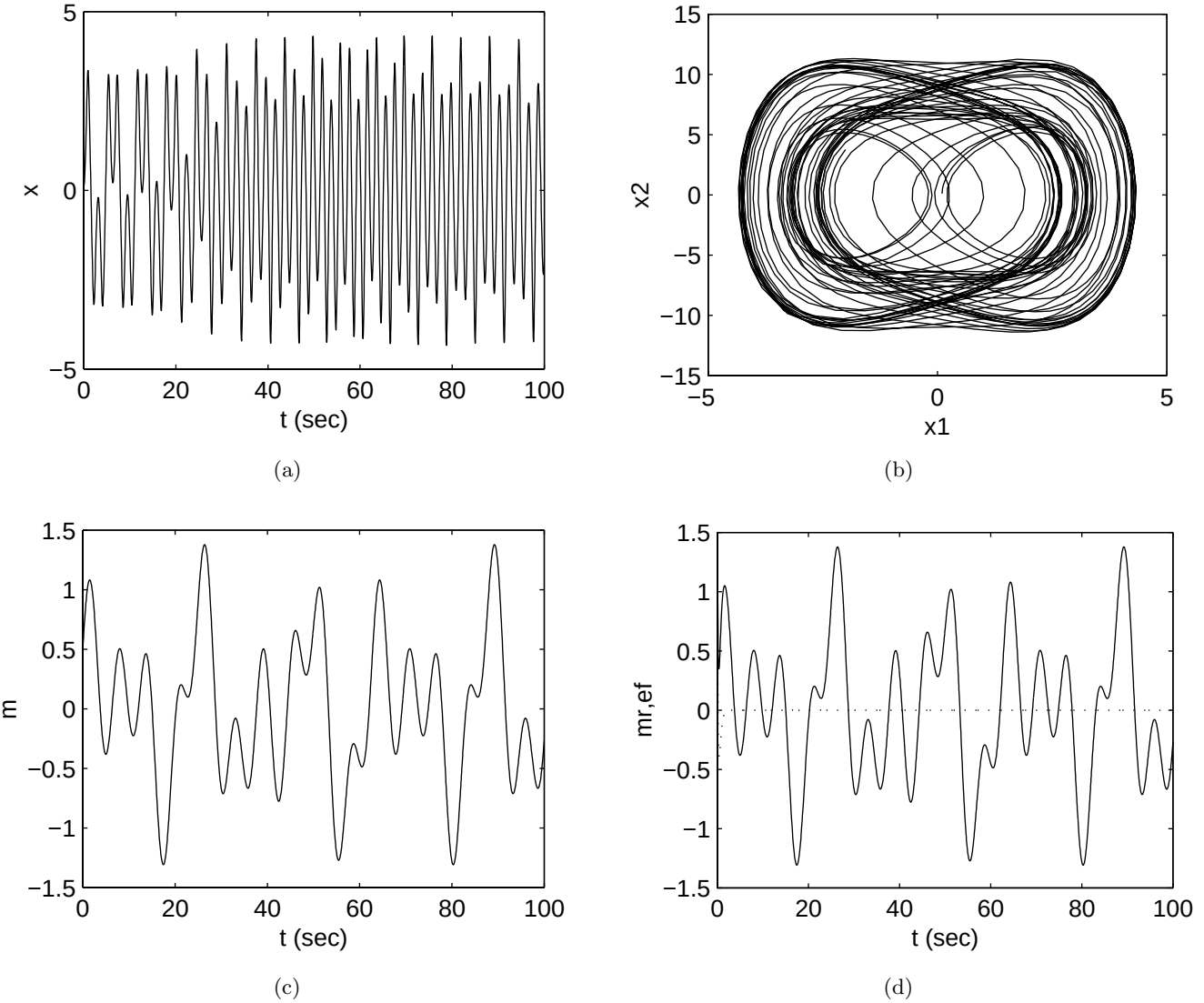
$$\dot{x} = -10x + 10y + m(t)\,, \tag{53}$$

$$\dot{y} = 28x - y - xz\,, \tag{54}$$

$$\dot{z} = xy - 8/3z\,. \tag{55}$$

It is well-known that this system exhibits chaotic behavior when $m(t) = 0$, see e.g. [Thompson, 1986]. With $u = (xyz)^T$, this system is of the form given by (36) with $b = (1 \;\; 0 \;\; 0)^T$. It can be shown easily that this system cannot be transformed into the form given by (30). By using $o = x$ as the signal transmitted to the receiver, we have $o = Cu$ with $C = (1 \;\; 0 \;\; 0)$. For the receiver, we use the observer given by (4) as follows:

$$\dot{\hat{x}} = -10\hat{x} + 10\hat{y} + k_1(x - \hat{x})\,, \tag{56}$$



(a) (b) (c) (d)

Fig. 2. Simulation result for Duffing system, case *ii* (a) Transmitted signal x, (b) $x_1 = x$ versus $x_2 = \dot{x}$, (c) message, (d) recovered message m_r (solid), error (dotted).

$$\dot{\hat{y}} = 28\hat{x} - \hat{y} - \hat{x}\hat{z} + k_2(x - \hat{x})\,, \tag{57}$$

$$\dot{\hat{z}} = \hat{x}\hat{y} - 8/3\hat{z} + k_3(x - \hat{x})\,. \tag{58}$$

For this system, we choose $k_2 = 28$, and $k_3 = 0$ as the observer gains, the gain k_1 is yet to be determined. It can easily be shown that in this case we have $C(A - KC)^{-1} = 1/(k_1 + 10)(-1 \quad -10 \quad 0)$, hence by choosing k_1 sufficiently large, the effect of the nonlinear terms may become negligible on the measured error $e_m = Ce$, see (38). In the simulations, we choose the message m as a square wave whose magnitude is alternating between $\pm\overline{m} = 10$ and the period T is given as $T = 10$ sec. Note that in this case $G(s)$ in (29) becomes $G(s) = 1/(s + k_1 + 10)$, hence the recovered message may be given as $\hat{m} = (k_1 + 10)e_m$, see (32). The results of the simulation are shown in Fig. 3. Here, Fig. 3(a) shows the transmitted message x, and Fig. 3(b) shows x versus y. As can be seen, the solutions are chaotic. In the receiver part, we considered two cases. We first choose $k_1 = 190$, and the recovered message $m_r = (k_1 + 10)e_m$ is shown in Fig. 3(c) (dotted line) together with the message (solid line). To show the effect of increased gain, we also choose $k_1 = 1990$, the recovered message m_r is passed through a low-pass filter. Figure 3(d) shows this filtered m_r (solid line) and the message (dotted line). As can be seen, by increasing the gain, we may reduce the error in the message recovery. Note that since the message is discrete, in both

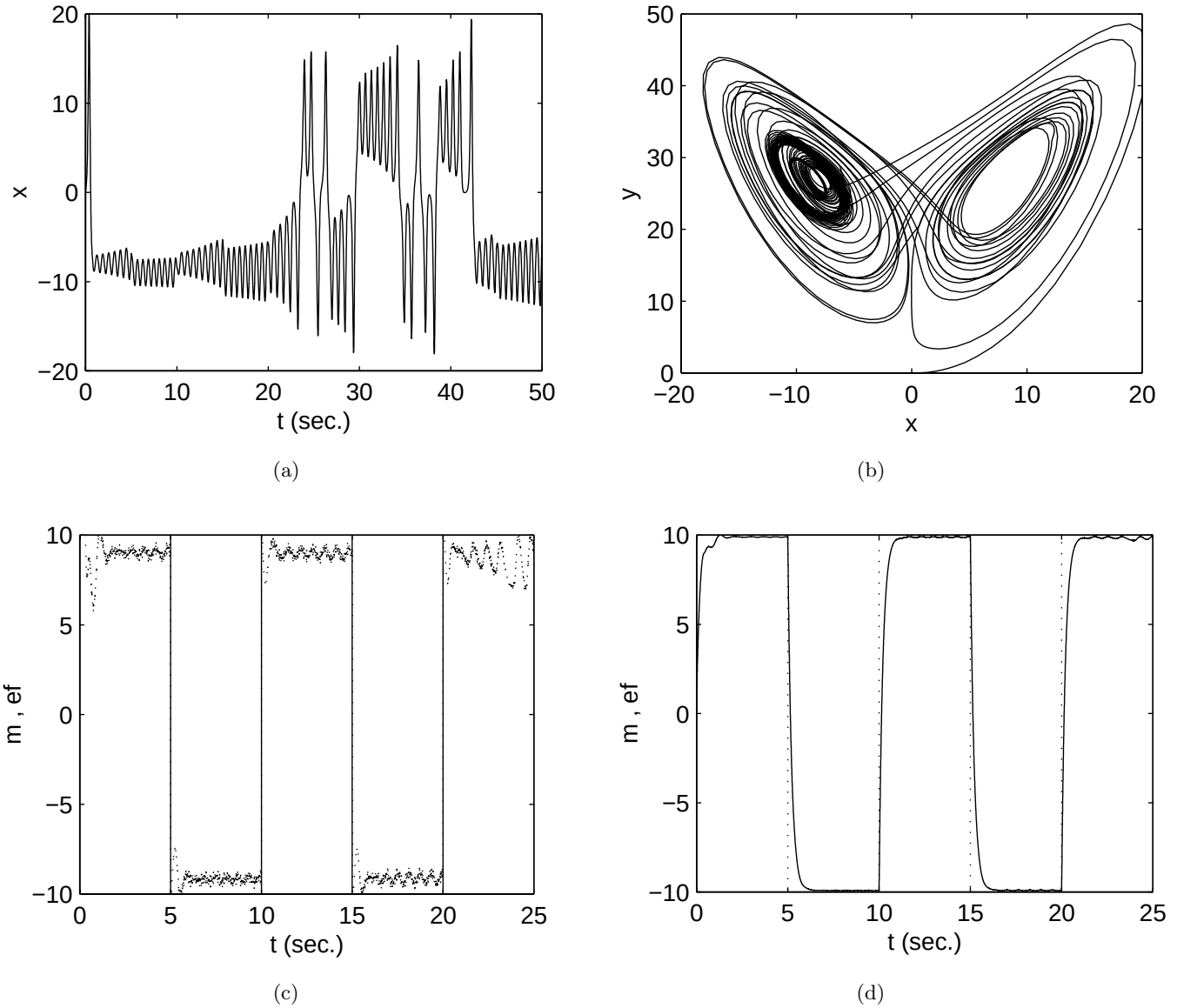


Fig. 3. Simulation result for Lorenz system, (a) Transmitted signal x, (b) x versus y, (c) Message (solid), recovered message (dotted) for $k_1 = 190$, (d) message (dotted), recovered message (solid) for $k_1 = 1990$.

cases we may reconstruct the signal at the receiver by simply comparing m_r with a threshold value, see (33). Also note that the message magnitude is comparable with the transmitted signal.

Case iv. To demonstrate the robustness of the proposed scheme with respect to noise and parameter mismatch, we use the following model of the well-known Chua's circuit:

$$\dot{x} = \alpha(y - h(x)) + m\,, \tag{59}$$

$$\dot{y} = x - y + z\,, \tag{60}$$

$$\dot{z} = -\beta y\,, \tag{61}$$

where $h(x)$ is a piecewise linear function given as:

$$h(x) = \frac{2}{7}x - \frac{3}{14}(|x+1| - |x-1|)\,, \tag{62}$$

and m is the message to be transmitted. This system is known to exhibit double scroll characteristics for $\alpha = 9$, $\beta = 14.286$; see e.g. [Yalçın *et al.*, 2000] for more references as well as an electronic circuit implementation of this system. For the output of this system, we choose $o = x$, i.e. $C = (1 \;\; 0 \;\; 0)$, see (27), (39). This system is in the form given by (27)

with

$$A = \begin{pmatrix} 0 & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & 0 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, g = \begin{pmatrix} -\alpha h(x) \\ 0 \\ 0 \end{pmatrix}. \tag{63}$$

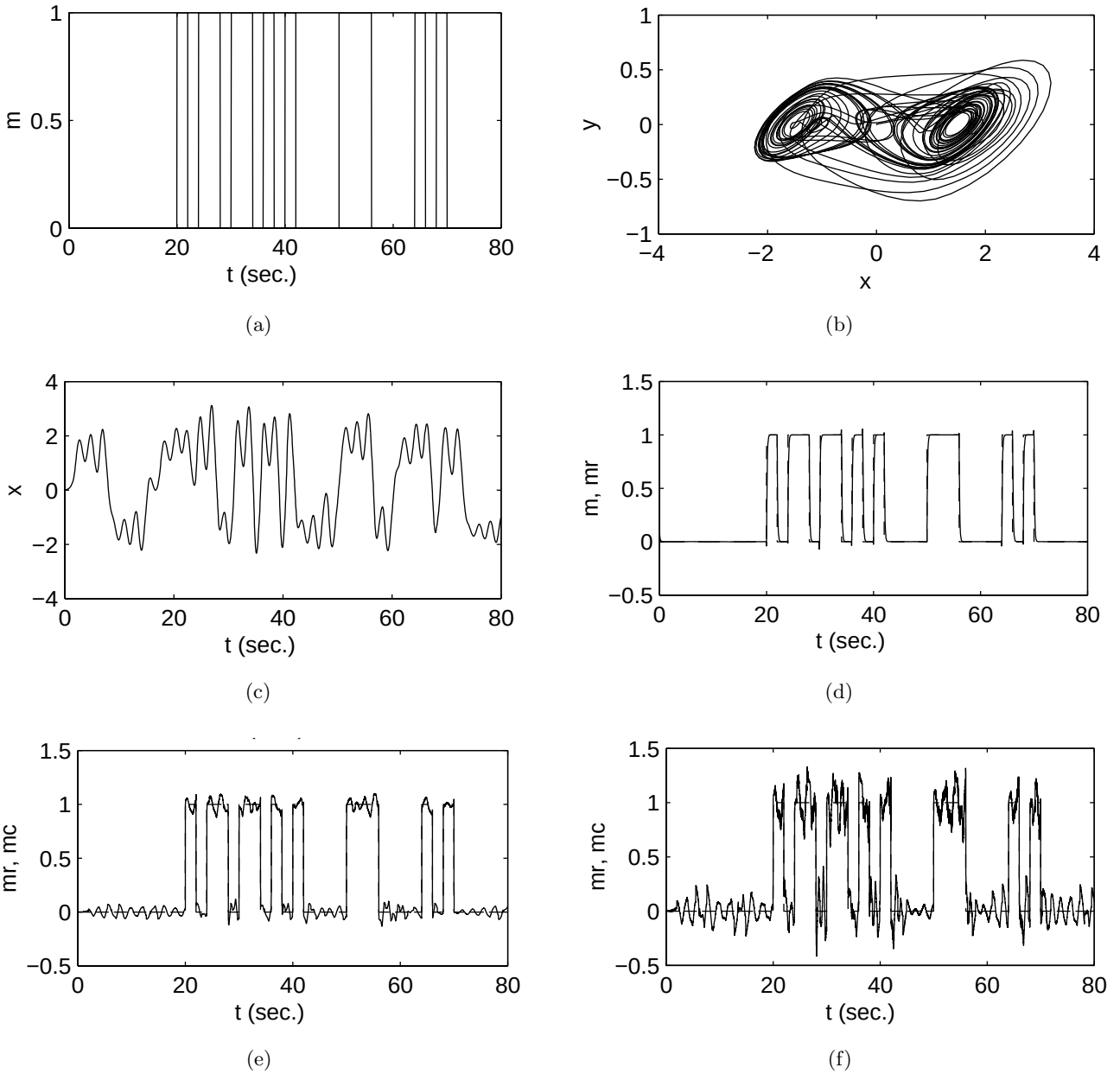
We note that the signal received by the response system will be $o + n = x + n$, where n is the noise. For the response system, we use the following

$$\dot{\hat{x}} = \hat{\alpha}(\hat{y} - h(x+n)) + k_1(x + n - \hat{x}), \tag{64}$$

$$\dot{\hat{y}} = \hat{x} - \hat{y} + \hat{z} + k_2(x + n - \hat{x}), \tag{65}$$

$$\dot{\hat{z}} = -\hat{\beta}\hat{y} + k_3(x + n - \hat{x}). \tag{66}$$

In the simulations, for the message we used the coded version of the word "chaos". For coding, we used the standard international alphabet code



(a) (b) (c) (d) (e) (f)

Fig. 4. Simulation result for Chua's circuit, (a) message m (b) x versus y, (c) transmitted message x with noise (d) message m (solid), recovered message m_r (dashed) in ideal case (e) recovered message m_r (solid), reconstructed message m_c (dashed) for $n_m = 0.01$, $\Delta\mu = 0.168$, (f) recovered message m_r (solid), reconstructed message m_c (dashed) for $n_m = 0.05$, $\Delta\mu = 0.337$.

no. 2, see e.g. [Gegg, 1997]. This message is shown in Fig. 4(a). We simulated (59)–(61) with this message and with the parameters indicated above. The resulting x versus y graph is shown in Fig. 4(b), which clearly indicates the chaotic behavior. Note that we have $\overline{m} = 1$ (maximum message magnitude), hence the message magnitude is comparable with the chaotic signal used in message transmission. The signal transmitted to the response system with the added noise is shown in Fig. 4(c). Here, as noise we used a random signal whose maximum magnitude is limited by $n_m = 0.01$.

For the response system given by (64)–(66), we chose the gains as $k_1 = 100$, $k_2 = 1$, $k_3 = 0$, (i.e. $K = (100 \;\; 1 \;\; 0)^T$). It can easily be shown that with this choice, $A - KC$ is a stable matrix. Note that in this case, $G(s)$ in (29) becomes $G(s) = 1/(s + k_1)$, hence the recovered message may be given as $m_r = k_1 e_m = k_1(x + n - \hat{x})$.

For the simulations, we considered the following cases:

Case 1. We simulated (64)–(66) with $\hat{\alpha} = \alpha = 9$, $\hat{\beta} = \beta = 14.286$, and with $n = 0$. The message is as given in Fig. 4(a). The recovered message m_r and the corrected message m_c (as given by (33)) are shown in Fig. 4(d). As can be seen, the message error is quite small, and that the message is reconstructed without any error.

Case 2. We simulated (64)–(66) with $\hat{\alpha} = 8.91$, $\hat{\beta} = 14.143$. The message is as given in Fig. 4(a) and as for the noise we used a random signal whose magnitude is limited to $n_m = 0.01$. Note that in this case, $\Delta\alpha = |\alpha - \hat{\alpha}| = 0.09$, $\Delta\beta = |\beta - \hat{\beta}| = 0.143$ and $\Delta\mu = \sqrt{(\Delta\alpha)^2 + (\Delta\beta)^2} = 0.168$. The recovered message m_r and the corrected message m_c are shown in Fig. 4(e). As can be seen, the message error is small, and that the message is reconstructed without any error.

Case 3. We simulated (64)–(66) with $\hat{\alpha} = 8.82$, $\hat{\beta} = 14$. The message is as given in Fig. 4(a) and as for the noise we used a random signal whose magnitude is limited to $n_m = 0.05$. Note that in this case, $\Delta\alpha = |\alpha - \hat{\alpha}| = 0.18$, $\Delta\beta = |\beta - \hat{\beta}| = 0.286$ and $\Delta\mu = \sqrt{(\Delta\alpha)^2 + (\Delta\beta)^2} = 0.337$. The recovered message m_r and the corrected message m_c are shown in Fig. 4(f). Although the message error is higher as compared to Case 2 (due to increased parameter mismatch and noise), the message is reconstructed without any error.

Remark 4. We did not consider the security of our scheme. In [Short, 1994], the security of communication schemes based on chaotic carriers when the hidden information signal is buried in the order of -30 dB with respect to the chaotic carrier were analyzed and it was concluded that such schemes may be useful to increase the privacy in communication, but may not provide a high level of security. It was also concluded in [Short, 1994] that the hidden signal added to the chaotic carrier at low power makes it even easier to recover the hidden signal. We do not claim any level of security for the schemes proposed in this paper, and probably the conclusions of Short [1994] apply to our schemes as well when the message levels are low. But note that, as is evident in the simulations, message levels in the proposed modulation scheme are not necessarily low, whereas in most of the chaotic masking schemes, the message level is required to be sufficiently lower than that of the chaotic carrier. Considering the results of Short [1994], the flexibility in adjusting the message level might improve the security of our scheme. Also note that the scheme given in Sec. 5 is based on modulation only, hence the message is not added to the signal transmitted to the receiver, see (27). This property may improve the security of our scheme. However, a detailed security analysis is quite tedious and such an analysis is beyond the scope of this paper. Such an analysis requires and deserves further research.

Also note that, as explained in [Kolumbán *et al.*, 1997], most of the conventional communication schemes are susceptible to multipath propagation effects. These effects arise from the interactions between the signals at the receiver which travel along different propagation paths. In conventional (especially digital) communication schemes, the transmitted symbols are usually chosen from periodic waveform segments, whereas in chaotic modulation case, the relevant waveforms are nonperiodic. Since the cross-correlations between segments of a chaotic waveform are usually lower than that of a periodic signal, the chaotic modulation should yield a better performance under multipath propagation conditions, see [Kolumbán *et al.*, 1997]. Thus, in addition to increased privacy in communications, chaotic modulation may also offer simple yet robust wideband communication schemes.

7. Conclusion

In this paper we proposed two message transmission schemes by using chaotic systems. In these schemes we use observer based synchronization technique, see e.g. [Morgül & Solak, 1996, 1997; Morgül, 1999; Nijmeijer & Mareels, 1997]. The first proposed message transmission scheme is a slight modification of the scheme proposed in [Liao & Huang, 1999]. This scheme is based on chaotic masking, i.e. the signal transmitted to the receiver is the sum of a chaotic signal and the message to be transmitted, and may have some disadvantages. To eliminate these disadvantages, we proposed another scheme. This scheme is based on chaotic modulation as opposed to chaotic masking. More precisely, the message to be transmitted is injected into the chaotic drive system as an input, and a signal generated by the drive system is sent to the response system. We show that in some cases it is possible to recover the message under certain conditions. The method is first applied to a special class of chaotic systems, see (27). For such systems, we investigated three cases. These cases are (i) when the message is a band-limited signal, (ii) when the message is discrete, and (iii) when the message is differentiable. We show that in the first and second cases it is possible to recover the message with small error, and in the third case we may asymptotically recover the message, i.e. the error asymptotically decays to zero. Moreover, the decay rate may be adjusted by using appropriate gains in the observer. Also, in case the message is discrete, we may even reconstruct the message by comparing the recovered message with a threshold. We then show that this technique may be used in a broader class of systems. We also showed that the proposed schemes are robust with respect to noise and parameter mismatch. Finally we present some simulation results. These results indicate that while it is also possible to transmit band-limited signal for the systems of the form (27), the proposed scheme is particularly suited in sending discrete signals. We also presented a simulation result indicating the robustness of the proposed scheme. Also note that, the allowable message magnitude in the proposed schemes is in general comparable with the transmitted signal. This may be useful when the transmitted signal is subjected to noise.

We do not investigate the security of our scheme, and do not claim any level of security. But note that in the proposed modulation scheme, the message level is not necessarily required to be small, whereas in most of the schemes the message magnitude is required to be sufficiently lower than that of the chaotic carrier. This point may be considered as an advantage of our scheme. Also the second proposed scheme is not based on chaotic masking. The effect of the proposed chaotic modulation scheme on the security requires and deserves further investigation. We also note that the chaotic modulation may increase the privacy in communications, see [Short, 1994], and may also offer simple and robust wideband communication schemes under multipath propagation conditions [Kolumbán *et al.*, 1997].

References

Boccaletti, S., Grebogi, C., Lai, Y. C., Mancini, H. & Maza, D. [2000] "The control of chaos: Theory and applications," *Phys. Rep.* **329**, 103–197.

Chen, G. [1997] "Control and synchronization of chaotic systems (a bibliography)," ftp.egr.uh.edu/pub/TeX/chaos.tex loginname: anonymous, password: your e-mail address.

Cuomo, K. M. & Oppenheim, A. V. [1993] "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* **71**, 65–68.

Gegg, W. D. [1977] *Analog and Digital Communication*, (John Wiley, NY).

Grassi, G. & Mascolo, S. [1997] "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal," *IEEE Trans. Circuits Syst.-I* **44**, 1011–1014.

Hasler, M. [1995] "Engineering chaos for secure communication systems," *Phil. Trans. Roy. Soc. Lond.* **A353**(1701), 115–126.

Khalil, H. K. [2002] *Nonlinear Systems*, 3rd edition (Prentice Hall, Upper Saddle River).

Kocarev, L., Halle, K. S., Eckert, K. & Chua, L. O. [1992] "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**(3), 709–713.

Kocarev, L. & Parlitz, U. [1995] "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.* **75**, 5028–5031.

Kolumbán, G., Kennedy, M. P. & Chua, L. O. [1997] "The role of synchronization in digital communications using chaos. Part 1: Fundamentals of digital communications," *IEEE Trans. Circuits Syst.-I* **44**, 927–936.

Kolumbán, G., Kennedy, M. P. & Chua, L. O. [1998] "The role of synchronization in digital communications using chaos. Part 2: Chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst.-I* **45**, 1129–1140.

Liao, T. L. & Huang, N. S. [1999] "An observer-based approach to chaotic synchronization with applications

to secure communications," *IEEE Trans. Circuits Syst.-I* **46**(9), 1144–1150.

Morgül, Ö. & Solak, E. [1996] "On the observer based synchronization of chaotic systems," *Phys. Rev.* **E54**(5), 4803–4811.

Morgül, Ö. & Solak, E. [1997] "On the synchronization of chaotic systems by using state observers," *Int. J. Bifurcation and Chaos* **7**(6), 1307–1322.

Morgül, Ö. [1999] "Necessary condition for observer-based chaos synchronization," *Phys. Rev. Lett.* **82**(1), 169–176.

Nijmeijer, H. & Mareels, I. M. Y. [1997] "An observer looks at synchronization," *IEEE Trans. Circuits Syst.-I* **44**(10), 882–890.

Okşaşoğlu, A. & Akgül, T. [1995] "Chaotic masking scheme with a linear inverse system," *Phys. Rev. Lett.* **75**(25), 4595–4597.

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.

Pecora, L. M. & Carroll, T. L. [1991] "Driving systems with chaotic signals," *Phys. Rev.* **A44**, 2374–2383.

Short, K. [1994] "Steps towards unmasking secure communications," *Int. J. Bifurcation and Chaos* **4**(4), 959–977.

Solak, E. [1996] *Nonlinear Observer Design with Application to the Synchronization of Chaotic Systems*, M. Sc. thesis, Bilkent University.

Thompson, J. M. [1986] *Nonlinear Dynamics and Chaos* (Wiley).

Yalçın, M. E., Suykens, J. A. K. & Vandewalle, J. [2000] "Experimental confirmation of 3 and 5 scroll attractors from generalized Chua's circuit," *IEEE Trans. Circuits Syst.-I* **47**(3), 425–429.