A control perspective on communication using chaotic systems

A control perspective on communication using chaotic systems [1]

H.J.C. Huijberts* H. Nijmeijer** R.M.A. Willems*

* Faculty of Mathematics and Comp. Sci., Eindhoven Univ. of Techn., P.O. Box 513, 5600 MB Eindhoven, The Netherlands. Email: {hjch,willems}@win.tue.nl

** Faculty of Mathematical Sciences, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands. Email: H.Nijmeijer@math.utwente.nl

and

Faculty of Mech. Eng., Eindhoven Univ. of Techn., P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Abstract

Secure communication using chaotic systems is considered from a control point of view. It is shown that a synchronization-based scheme for secure communication described in the literature may in fact be interpreted as an adaptive identification scheme. Two examples where the existing scheme fails to achieve the reconstruction of an encoded message are treated using adaptive identification techniques.

1 Introduction

In recent years there has been a tremendous interest in studying the behavior of complex systems. Two particularly interesting ideas which have emerged during this time are (chaos) synchronization and chaos control. Recent reviews on these subjects can be found in, for instance, two special issues devoted to the subject, see [4],[14] (where in fact [4] is a follow up of an earlier special issue on the same subject of the same journal ([3])).

Synchronization and controlled synchronization of complex/chaotic systems is a topic that has become popular because of its possible use in secure communication, see [12],[11]. Recently, in [9] a control perspective on synchronization was given, which enables to resolve various synchronization problems as an observer problem. Thus, [9] illustrates, amongst others, the benefits of incorporating control theoretic ideas in the study of communication using chaotic systems.

It is the purpose of the present paper to further illustrate these benefits. More specifically, we will look at some problems in communication using chaotic systems for which (standard) synchronization-based schemes may not yield the reconstruction of encoded messages, but that can be resolved using control theoretic ideas.

In communication using chaotic systems, one considers a transmitter system Σ_T depending on a parameter λ of the form

$$\Sigma_T \quad \begin{cases} \dot{x} &= f(x,\lambda), & x \in I\!R^n \\ y &= h(x), & y \in I\!R \end{cases} \tag{1}$$

where λ is a slowly time-varying message satisfying $\lambda_{\min} \leq \lambda(t) \leq \lambda_{\max}$ $(\forall t)$ and $y \in I\!R$ is the transmitted signal (i.e., the coded message). It is assumed that the system Σ_T is chaotic (or at least sufficiently complex) for all constant λ satisfying $\lambda_{\min} \leq \lambda \leq \lambda_{\max}$. The task is now to build a receiver system Σ_R that reconstructs the message $\lambda(t)$ from the coded message $y(t)$.

If one considers the problem of reconstruction of λ as described above from a control theoretic point of view, two possible ways to approach the problem come to mind. The first approach is that of system inversion. Interpreting λ in (1) as an input and y as a measurement, one sees that (1) gives a mapping from λ to y. In the problem of system inversion, the task is to find an (asymptotic) inverse of this mapping. This approach will be pursued in future research (note, however, that this idea has also been pursued in [7]). The second approach, that will be pursued in this paper, is that of system identification. In system identification, the task is to estimate unknown (possibly slowly time-varying) parameters of a system, based on measurements taken from the system. For linear systems, system identification is well-established (for an overview, see e.g. [13]). In this paper, it will be shown on two examples that this identification may be helpful in communication us-

[1] This paper is to appear in the Proceedings of the 1998 Conference on Decision and Control, Tampa, USA.

ing chaotic systems. Although both examples concern chaotic, and thus nonlinear, systems, it is possible to use the standard "linear" identification algorithms once the systems are decomposed properly.

The organization of this paper is as follows. In the following section, we discuss a synchronization-based scheme for secure communication using chaotic systems that was proposed in [5]. It will be shown that the reconstruction scheme proposed in [5] may be interpreted as a scheme based on (linear) system identification methods. Further, it will be argued that the scheme proposed in [5] breaks down if one wishes to enhance the security of the scheme. In Sections 3 and 4, it will then be illustrated that, using control theoretic ideas, one can still build a reconstruction scheme when the scheme from [5] breaks down. In Section 5, some conclusions will be drawn.

2 A synchronization-based scheme for secure communication

We consider the following set up for secure communication that was proposed in [5]. The transmitter is a system Σ_T of the form

$$\Sigma_T \quad \left\{ \begin{array}{rcl} \dot{x}_1 &=& f_1(x) + g(x)\lambda \\ \dot{x}_2 &=& f_2(x) \\ \dot{x}_3 &=& f_3(x) \\ y &=& x_1 \end{array} \right. \tag{2}$$

where λ is a slowly time-varying message satisfying $\lambda_{\min} \leq \lambda(t) \leq \lambda_{\max}$ $(\forall t)$ and $y \in \mathbb{R}$ is the transmitted signal (i.e., the coded message). Further, a second system is considered, that has the form

$$\left\{ \begin{array}{rcl} \dot{\hat{x}}_2 &=& f_2(x_1, \hat{x}_2, \hat{x}_3) \\ \dot{\hat{x}}_3 &=& f_3(x_1, \hat{x}_2, \hat{x}_3) \end{array} \right. \tag{3}$$

It is assumed that the (x_2, x_3)-subsystem in (2) synchronizes, with (3), in the sense that for Σ_T, together with the system (3), we have for all initial conditions that $\lim_{t\to+\infty}(\hat{x}_2(t), \hat{x}_3(t)) = (x_2(t), x_3(t))$.

We next briefly indicate how one would go about to obtain a reconstruction scheme for the system (2) by employing methods from identification theory as described in e.g. [13]. If one assumes that the systems (2) and (3) have synchronized, the dynamics of y in (2) are given by

$$\dot{y} = u_1(t) + \lambda u_2(t)$$

where

$$\begin{array}{rcl} u_1(t) &:=& f_1(x_1(t), \hat{x}_2(t), \hat{x}_3(t)) \\ u_2(t) &:=& g(x_1(t), \hat{x}_2(t), \hat{x}_3(t)) \end{array} \tag{4}$$

If we let $Y(s), U_1(s), U_2(s)$ denote the Laplace-transforms of $y(t), u_1(t), u_2(t)$ respectively, this gives

$$Y(s) = \frac{1}{s}U_1(s) + \frac{\lambda}{s}U_2(s)$$

Choosing $k > 0$, and defining $\kappa(s) := s + k$, this may be rewritten as

$$Y(s) = \frac{k}{\kappa(s)}Y(s) + \frac{1}{\kappa(s)}U_1(s) + \frac{\lambda}{\kappa(s)}U_2(s)$$

We now consider a linear time-invariant system with output $\tilde{y}$ and inputs y, u_1, u_2 that in the frequency domain satisfies

$$\tilde{Y}(s) = \frac{k}{\kappa(s)}Y(s) + \frac{1}{\kappa(s)}U_1(s) + \frac{\lambda}{\kappa(s)}U_2(s)$$

where $\tilde{Y}(s)$ denotes the Laplace-transform of $\tilde{y}$. A realization of this system is given by (assuming that u_1, u_2 are give by (4))

$$\left\{ \begin{array}{rcl} \dot{\tilde{w}}_0 &=& -k\tilde{w}_0 + ky + u_1 = \\ && \quad -k\tilde{w}_0 + ky + f_1(x_1, \hat{x}_2, \hat{x}_3) \\ \dot{\tilde{w}}_1 &=& -k\tilde{w}_1 + u_2 = \\ && \quad -k\tilde{w}_1 + g(x_1, \hat{x}_2, \hat{x}_3) \\ \tilde{y} &=& \tilde{w}_0 + \lambda\tilde{w}_1 \end{array} \right. \tag{5}$$

Now note that we have that $\tilde{Y}(s) = Y(s)$. Together with the fact that the internal dynamics of (5) (i.e., the dynamics (5) for $u_1 \equiv 0$, $u_2 \equiv 0$, $y \equiv 0$) are exponentially stable, this implies that $\tilde{y}(t) \to y(t)$ $(t \to +\infty)$, where the convergence is exponential. Besides (5), we consider the following linear system, of which the output $\hat{y}$ depends on an estimation $\hat{\lambda}$ of λ:

$$\left\{ \begin{array}{rcl} \dot{w}_0 &=& -kw_0 + ky + u_1 = \\ && \quad -kw_0 + ky + f_1(x_1, \hat{x}_2, \hat{x}_3) \\ \dot{w}_1 &=& -kw_1 + u_2 = \\ && \quad -kw_1 + g(x_1, \hat{x}_2, \hat{x}_3) \\ \hat{y} &=& w_0 + \hat{\lambda}w_1 \end{array} \right. \tag{6}$$

Note that the internal dynamics of (5) and (6) are identical. It then follows again from the exponential stability of these dynamics that $w_i(t) \to \tilde{w}_i(t)$ $(t \to +\infty)$ exponentially $(i = 0, 1)$. We then obtain:

$$\begin{array}{l} \hat{y} - y = \hat{y} - \tilde{y} + (\tilde{y} - y) = \cdots = \\ \quad (w_0 - \tilde{w}_0) + \lambda(w_1 - \tilde{w}_1) + \\ \qquad (\tilde{y} - y) + (\hat{\lambda} - \lambda)w_1 = \epsilon(t) + (\hat{\lambda} - \lambda)w_1 \end{array}$$

where $\epsilon(t) = \tilde{y}(t) - y(t)$. It may then be shown (see [13] for details) that with an update law for λ of the form

$$\dot{\hat{\lambda}} = -g\psi(t, w)(\hat{y} - y), \quad g > 0 \tag{7}$$

we will have that $\hat{\lambda}(t) \to \lambda$ $(t \to \infty)$ *provided* $\psi(t, w(t))$ is bounded, $\psi(t, w(t))w_1(t) \geq 0$ $(\forall t)$, and the signal $\psi(t, w(t))w_1(t)$ is *persistingly exciting*, which means that there should exist $\alpha_1, \alpha_2, \delta > 0$ such that for all $t \geq 0$ we have

$$\alpha_1 \leq \int_t^{t+\delta} \psi(\tau, w(\tau))^2 w_1(\tau)^2 d\tau \leq \alpha_2$$

From the above analysis, the estimator obtained in [5] may also be derived (although the derivation in [5] is somewhat different). Observe that we have that $\tilde{y}(t) = \tilde{w}_0(t) + \lambda\tilde{w}_1(t) \rightarrow y(t)$ $(t \rightarrow +\infty)$. Solving for λ, this gives the following estimator $\tilde{\lambda}$ for λ:

$$\tilde{\lambda} = \frac{y - \tilde{w}_0}{\tilde{w}_1}$$

which is exactly the estimator obtained in [5]. It seems that in [5] the authors do not need $\tilde{w}_1$ to be persistingly exciting. However, it is easily seen that $\tilde{\lambda}$ above satisfies $\tilde{\lambda}(t) \rightarrow \lambda$ $(t \rightarrow +\infty)$ if and only if $\tilde{w}_1$ is bounded away from zero for $t \rightarrow +\infty$ and does not escape to infinity in finite time. These conditions are fulfilled if $\tilde{w}_1$ is persistingly exciting. A disadvantage of the estimator $\tilde{\lambda}$ when compared to $\hat{\lambda}$ is that $\tilde{\lambda}$ will behave badly at zero-crossings of $\tilde{w}_1(t)$. In [5], the authors cope with this problem by adding an extra filter, which finally results in a *dynamic* update law for $\tilde{\lambda}$ of the form

$$\begin{aligned}\dot{\tilde{\lambda}} = \quad & -g\tfrac{\mathrm{sign}(\tilde{w}_1)}{1+|\tilde{w}_1|}(\tilde{w}_0 + \tilde{w}_1\tilde{\lambda} - y) = \\ & -g\tfrac{\mathrm{sign}(\tilde{w}_1)}{1+|\tilde{w}_1|}(\tilde{y} - y)\end{aligned}$$

Note that this update law has the form (7), with $\psi(t, \tilde{w}) = \mathrm{sign}(\tilde{w}_1)/(1 + |\tilde{w}_1|)$. This leads to the conclusion that the scheme proposed in [5] may be interpreted as a scheme based on (linear) system identification methods.

Also concerning the security of the scheme proposed in [5] some comments are in order. Note that the "distance" between the message and the transmitted signal is quite small, in the sense that already the first time-derivative of the transmitted signal along solutions of (2) explicitly depends on λ (in control theoretic terms, this expressed by saying that the *relative degree* (cf. [8]) of x_1 with respect to λ equals one). However, intuitively, one would say that in order to have *secure* communication, a high relative degree is required, since a high "distance" between the message and the transmitted signal should give a better masking of the message. However, in cases of higher relative degree the above scheme fails, since then in general the important assumption of the existence of a synchronizing subsystem that is independent of the unknown parameter λ does not hold any more. In the next two sections this is illustrated by means of two examples. Further, in these examples it is shown that, in spite of the fact that a synchronizing subsystem does not exist any more, one can still build a reconstruction mechanism by employing the methods from (linear) identification theory outlined above.

3 Chua's circuit with partial synchronization

In dimensionless form, Chua's circuit is described by the equations

$$\left\{\begin{array}{lcl} \dot{x}_1 &=& \alpha(-x_1 + x_2 - \phi(x_1)) \\ \dot{x}_2 &=& x_1 - x_2 + x_3 \\ \dot{x}_3 &=& -\lambda x_2 \end{array}\right. \tag{8}$$

where

$$\phi(x_1) = m_1 x_1 + \frac{m_0 - m_1}{2}(|\,x_1 + 1\,| - |\,x_1 - 1\,|)$$

This system is known to have a so called double scroll chaotic attractor for $\alpha = 15.6$, $m_0 = -\frac{8}{7}$, $m_1 = -\frac{5}{7}$, and $23 < \lambda < 31$ (see e.g. [1]). We assume that $y = x_2$ is the transmitted signal. Note that with this choice of y we have that the relative degree of y with respect to λ equals 2. Note further that, although it has been shown experimentally that the (x_1, x_3)-subsystem synchronizes with the system

$$\left\{\begin{array}{lcl} \dot{\hat{x}}_1 &=& \alpha(-\hat{x}_1 + x_2 - \phi(\hat{x}_1)) \\ \dot{\hat{x}}_3 &=& -\lambda x_2 \end{array}\right.$$

(see e.g. [6]), the Corron-Hahs scheme cannot be applied directly, since the synchronizing system depends explicitly on the unknown parameter λ. In order to come up with a a reconstruction scheme for λ, we employ the following strategy. We first assume that, besides x_2, we can also measure x_1. The equations for x_2 and x_3 in (8) then have the following form:

$$\left\{\begin{array}{lcl} \dot{x}_2 &=& -x_2 + x_3 + u \\ \dot{x}_3 &=& -\lambda x_2 \\ y &=& x_2 \end{array}\right. \tag{9}$$

where we interpret $u := x_1$ as an input. Thus, (9) has the form of a linear control system depending on an unknown parameter λ. In the same vein as in the previous section, one may then derive the following reconstruction scheme for λ:

$$\left\{\begin{array}{lcll} \dot{w}_{01} &=& w_{02} & \\ \dot{w}_{02} &=& -k_0 w_{01} - k_1 w_{02} + y = & \\ & & \quad -k_0 w_{01} - k_1 w_{02} + x_2 & \\ \dot{w}_{11} &=& w_{12} & \\ \dot{w}_{12} &=& -k_0 w_{11} - k_1 w_{12} + u = & \\ & & \quad -k_0 w_{11} - k_1 w_{12} + x_1 & \\ \hat{y} &=& (k_0 - \hat{\lambda})w_{01} + (k_1 - 1)w_{02} + w_{12} & \\ \dot{\hat{\lambda}} &=& g w_{01} p(\hat{y} - y), & (g > 0) \\ \dot{p} &=& -g(w_{01}^2 p^2 - \gamma p), & (\gamma > 0) \end{array}\right. \tag{10}$$

where $k_0, k_1 \in \mathbb{R}$ are such that the polynomial $\kappa(s) := s^2 + k_1 s + k_2$ is Hurwitz. Note that, when we compare the last two equations in (10) with (7), we see that we have $\psi(t, w) = -w_{01}p(t)$. This estimation scheme is called the *least squares estimator with exponential forgetting factor* (cf. [13]). Thus, if x_1 could be measured,

the reconstruction of λ could be achieved by employing the scheme (10). To achieve reconstruction when x_1 cannot be measured, we add the following estimator of x_1 to our reconstruction scheme:

$$\dot{\hat{x}}_1 = \alpha(-\hat{x}_1 + x_2 - \phi(\hat{x}_1)) \qquad (11)$$

and let the reconstruction scheme (10) depend on $\hat{x}_1$ instead of x_1. It may then be shown that still λ can be reconstructed, provided $\hat{x}_1(t)$ approaches $x_1(t)$ sufficiently fast. In [6], it was shown experimentally that this will indeed be the case for constant λ. However, one needs to be somewhat careful here for the following reasons. Define the error signal $e(t) := \hat{x}_1(t) - x_1(t)$. Then, for the parameter values given above, e satisfies the following differential equation:

$$\dot{e} = 15.6(-\frac{2}{7}e + \frac{3}{7}(\mathrm{sat}(e + x_1) - \mathrm{sat}(x_1))) \qquad (12)$$

where $\mathrm{sat}(\cdot)$ is the saturation function given by $\mathrm{sat}(x) = \frac{1}{2}(\mid x + 1 \mid - \mid x - 1 \mid)$. A first observation is that the equilibrium $e = 0$ of (12) is unstable when $x_1(t) \equiv 0$. This implies in particular that when (8) is initialized in the origin, we will not have that e tends to zero. It may be argued that from a practical point of view this is not a serious objection, since in practice one will have (8) "running" when communicating. However, as was shown in e.g. [3], the system (8) for the given parameter values is chaotic in the sense of Shil'nikov. This implies in particular that the origin is a homiclinic point for (8), which gives by the above that e will also not tend to zero when (8) is initialized on the homoclinic orbit. Also, the fact that (8) is chaotic in the sense of Shil'nikov implies the existence of a Poincaré map in the neighborhood of the origin that is in fact a horseshoe map. Together with what has already been discussed above, this leads to the conclusion that the best one could hope is that the equilibrium $e = 0$ of (12) is asymptotically stable for a *generic* choice of x_1.

Further evidence for the asymptotic stability of $e = 0$ for (12) with a generic choice of x_1 is obtained in the following way. Consider in the (x_1, e)-plane the compact set S enclosed by the straight lines $e = -\frac{3}{2}(x_1 \pm 1)$, $e = -3(x_1 \pm 1)$, $e = \pm 3$. Further, consider the function $V(e) := \frac{1}{2}e^2$. It may then be shown that $\dot{V} = e\dot{e} \geq 0$ on $S \cup \{x_1 - \mathrm{axis}\}$, and $\dot{V} = 0$ on $\partial S \cup \{x_1 - \mathrm{axis}\}$. A first conclusion that may be drawn from this, is that $\{e \in I\!R \mid \ |e| \leq 3\}$ is a globally attracting invariant set of (12) for *all* x_1. Also, the position of S in the (x_1, e)-plane suggests that we will have asymptotic stability of $e = 0$ for (12) if the residence time of $x_1(t)$ in the region $|x_1| > 1$ is large in comparison with the residence time in the region $|x_1| \leq 1$. Simulations for constant values of λ between 23 and 31 indicate that (asymptotically) we will have that $|x_1(t)| \leq 1$ for about 20% of the time, while $x_1(t) < -1$ respectively $x_1(t) > 1$ for about 40% of the time.

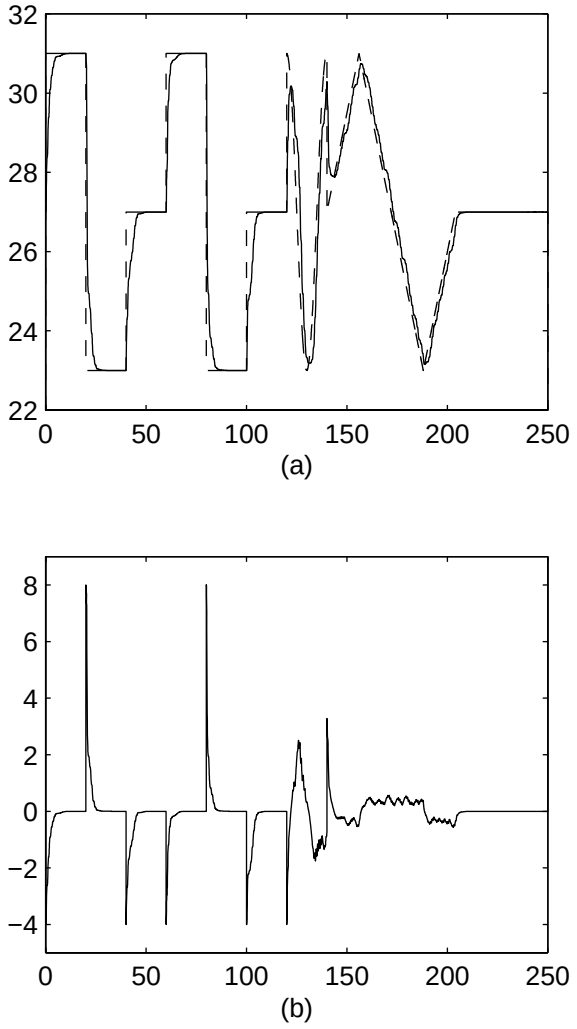

Figure 1: Simulation results for the Chua system: (a) λ (dashed) and $\hat{\lambda}$ (solid) (b) estimation error

In Figure 1 the proposed reconstruction scheme is illustrated by means of a simulation. Here, the parameters were chosen as $k_0 = 256$, $k_1 = 32$, $g = 800$, $\gamma = 0.001$.

In this section, we started with a partially synchronizing subsystem (11) rather than a completely synchronizing subsystem as in [5]. However, there is also another (generalized) synchronization aspect present in the scheme. Namely, it follows that once we have that $\hat{\lambda} = \lambda$, we will have that $\hat{y} \rightarrow y$, or, in other words, we will have that $(k_0 - \lambda)w_{01} + (k_1 - 1)w_{02} + w_{12}$ and x_2 will synchronize. Taking time-derivatives, this gives on its turn that also $(k_0 - k_1\lambda)w_{01} + (k_0 - \lambda)w_{02} - k_0 w_{11}$ and x_3 will synchronize. Thus we see that, although our scheme is only based on partial synchronization beforehand, it will also exhibit generalized synchronization once λ has been estimated correctly.

4 Rössler system without synchronization

We consider the following Rössler system:

$$\left\{\begin{array}{rcl} \dot{x}_1 &=& -x_2 - x_3 \\ \dot{x}_2 &=& x_1 + \lambda x_2 \\ \dot{x}_3 &=& 2 + (x_1 - 4)x_3 \\ y &=& x_3 \end{array}\right. \tag{13}$$

where we assume that λ is a slowly time-varying message satisfying $0.3 < \lambda(t) < 0.5$ $(\forall t)$ and $x_3(0) > 0$. Note that for this system we have that the relative degree of y with respect to λ equals 3. Further, it is known (see e.g. [12]) that for (13) the (x_1, x_2)-subsystem does not synchronize with the system

$$\left\{\begin{array}{rcl} \dot{\hat{x}}_1 &=& -\hat{x}_2 - x_3 \\ \dot{\hat{x}}_2 &=& \hat{x}_1 + \lambda \hat{x}_2 \end{array}\right.$$

Thus, in this case the Corron-Hahs approach breaks down completely. However, using control theoretic ideas, it is possible to reconstruct λ based on the measurement y. A first step in this reconstruction is the observation that (13) may be transformed into a system with so called linearizable error dynamics (see e.g. [10]). More specifically, note that, since $x_3(0) > 0$, we have that $x_3(t) > 0$ $(\forall t \geq 0)$. Thus, for (13) the coordinate change $\xi_1 = x_1$, $\xi_2 = x_2$, $\tilde{y} = \xi_3 = \log x_3$ is well-defined. In these new coordinates, (13) takes the form

$$\begin{pmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 1 & \lambda & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{A(\lambda)} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} + \underbrace{\begin{pmatrix} -e^{\tilde{y}} \\ 0 \\ 2e^{\tilde{y}} - 4 \end{pmatrix}}_{\Phi(\tilde{y})}$$
$$\tilde{y} = \xi_3 \tag{14}$$

Thus, (14) consists of a linear system $\dot{\xi} = A(\lambda)\xi + u$, where $A(\lambda)$ depends linearly on λ, interconnected with a static nonlinearity $u = \Phi(\tilde{y})$ that only depends on (a function of) the transmitted signal x_3. Using linear identification techniques, λ may now be reconstructed, based on the known signals $\tilde{y}$ and u, by using the following adaptive identification scheme:

$$\left\{\begin{array}{rcll} \dot{w}_i &=& Kw_i + Lu_i & (i = 0, 1, 2) \\ \hat{y} &=& \phi_0(w) + \hat{\lambda}\phi_1(w) & \\ \dot{\hat{\lambda}} &=& -g\,\mathrm{sign}(\phi_1(w))(\hat{y} - y) & g > 0 \end{array}\right. \tag{15}$$

where $u_0 := \log(x_3)$, $u_1 := -x_3$, $u_2 := \frac{2}{x_3} - 4$,

$$K = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -k_0 & -k_1 & -k_2 \end{pmatrix}, \quad L = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$k_0, k_1, k_2 \in \mathbb{R}$ are such that the polynomial $\kappa(s) := s^3 + k_2 s^2 + k_1 s + k_0$ is Hurwitz, and $\phi_0(w) := k_0 w_{01} + (k_1 - 1)w_{02} + k_2 w_{03} + w_{12} + w_{21}$, $\phi_1(w) := w_{03} - w_{11} - w_{22}$.

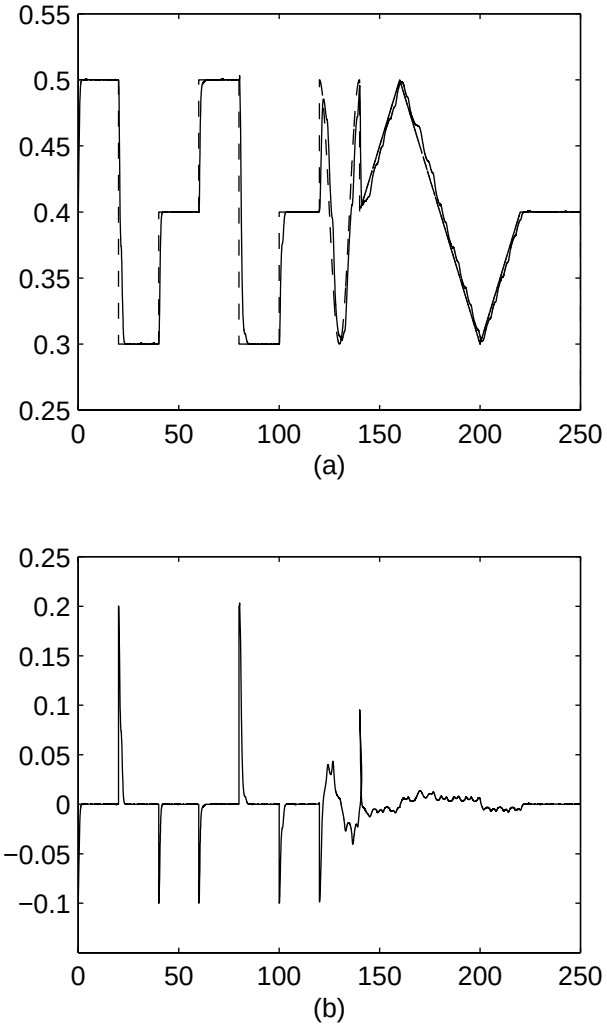

Figure 2: Simulation results for the Rössler system: (a) λ (dashed) and $\hat{\lambda}$ (solid) (b) estimation error

In Figure 2 the proposed reconstruction scheme is illustrated by means of a simulation. Here, the parameters were chosen as $k_0 = 512$, $k_1 = 192$, $k_2 = 24$, $g = 500$.

It may further be shown that, like in Section 3, the scheme (15) will exhibit generalized synchronization once λ has been estimated correctly.

5 Conclusions

We have studied secure communication via chaotic systems using ideas from systems and control. Since in general the unknown message -which is to be reconstructed- is not available beforehand, direct standard synchronization schemes may not be effective. We therefore propose an adaptive identification scheme that would enable the message reconstruction without explicitly assuming (partial) synchronization. This

method forms a generalization of a method developed in [5] and is applicable in a far more general setting than [5]. It should be noted that the message to be reconstructed has to be slowly time-varying, so that the identification is fast enough for the reconstruction. Typically in communication this will be the case, in particular when dealing with piecewise constant (0-1) messages. Two illustrative simulations on the proposed identification schemes are included, together with a discussion of the validity of the imposed conditions.

References

[1] Alligood, K.T., T.D. Sauer and J.A. Yorke, **Chaos - An introduction to dynamical systems**, Springer, New York, 1997.

[2] Boyd, S., and S.S. Sastry, *Necessary and sufficient conditions for parameter convergence in adaptive control*, Automatica, **22** (1986), pp. 629-639.

[3] Special Issue, *Chaos synchronization and control: theory and applications*, IEEE Trans. Circ. Syst. I, **40** (1993).

[4] Special Issue, *Chaos synchronization and control: theory and applications*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 853-1039.

[5] Corron, N.J. and D.W. Hahs, *A new approach to communications using chaotic signals*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 373-382.

[6] Chua, L.O., L. Kocarev, K. Eckert and M. Itoh, *Experimental chaos synchronization in Chua's circuit*, Int. J. Bif. Chaos, **2** (1992), pp. 705-708.

[7] Feldmann, U., M. Hasler and W. Schwarz, *Communication by chaotic signals: the inverse system approach*, Int. J. Circ. Theory Appl., **24** (1996), pp. 551-579.

[8] Isidori, A., **Nonlinear control systems** (2nd Edition), Springer, Berlin, 1989.

[9] Nijmeijer, H., and I.M.Y. Mareels, *An observer looks at synchronization*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 882-890.

[10] Nijmeijer, H., and A.J. van der Schaft, **Nonlinear dynamical control systems**, Springer-Verlag, New York, 1990.

[11] Ott, E., T. Sauer and J.A. Yorke (Eds.), **Coping with chaos: analysis of chaotic data and the exploitation of chaotic systems**, Wiley Interscience, New York, 1994.

[12] Pecora, L.M., and T.L. Carroll, *Synchronization in chaotic systems*, Phys. Review Lett., **64** (1990), pp. 821-824.

[13] Sastry, S., and M. Bodson, **Adaptive control - Stability, convergence, and robustness**, Prentice Hall, Englewood Cliffs, 1989.

[14] Special Issue, *Control of chaos and synchronization*, Syst. Control Lett., **31** (1997), pp. 259-322.