Robust chaotic communication via high gain observer

Wen Yu*
Departamento de Control Automatico,
CINVESTAV-IPN, A.P. 14-740,
Av.IPN 2508, México D.F., 07360, México
E-mail: yuw@ctrl.cinvestav.mx
*Corresponding author

América Morales
Programa de Matemática Aplicadas y Computación,
Instituto Mexicano del Petróleo,
Eje Central Lazano Cardenas 152,
Mexico D.F., 07730, Mexico

Guillermo Fernández
Departamento de Física y Matemáticas,
Universidad Iberoamericana,
Av. Prolingación Paseo de la Reforma #880,
México D.F., 01210, México

Abstract: In order to synchronise transmitter and receiver in chaotic communication, an identical chaotic receiver of transmitter should be applied. It is impossible to construct a replica of the transmitter when there exist uncertainties in transmitter end and transmission line. In this paper a new kind of receiver, called robust receiver, is proposed for robust chaotic communication. The receiver design is based on proportional-plus-Integral (PI) and Proportional (P) forms high gain observers, the chaotic receiver can be different from the transmitter. We prove that the communication single error can be arbitrary small if we select a proper observer gain in the receiver. A chaotic systems is used to illustrate the robust chaotic communication.

Keywords: synchronisation; data communication; nonlinear filters; robustness.


Biographical notes: Wen Yu received the BS Degree from Tsinghua University, Beijing, China in 1990 and the MS and PhD Degrees, both in Electrical Engineering, from Northeastern University, Shenyang, China, in 1992 and 1995, respectively. From 1995 to 1996, he served as a Lecturer in the Department of Automatic Control at Northeastern
1 Introduction

Since Pecora and Carroll’s observation on the possibility of synchronising two chaotic systems in so-called drive-response configuration (Pecora and Carroll, 1990), several synchronisation schemes have been developed. Synchronisation can be classified into two types: mutual synchronisation (bidirectional coupling) (Ushio, 1999) and master-slave synchronisation (unidirectional coupling) (Pecora and Carroll, 1990). The general idea for transmitting information via chaotic systems is that, an information signal influences in some way in the transmitter system which produces a chaotic output, so the information in this signal is invisible to the observer who has no knowledge about the transmitter system. The chaos-based secure communications have updated their fourth generation (Tao, 1999). Continuous synchronisation is adopted in the first three generations while the impulsive synchronisation is used in the fourth generation. Less than 94Hz of bandwidth is needed to transmit the synchronisation signal for a third-order chaotic transmitter in the fourth generation while 30-kHz bandwidth needed for transmitting the synchronisation signals in the other three generations (Yang and Chua, 1997).

The techniques for chaos communication can be divided into three categories:

- chaos masking (Kocarev et al., 1992), an information signal is added directly to the output of the chaotic system in the transmitter
- chaos modulation (Boutayeb et al., 2002; Hasler, 2002; Liao and Huang, 1999; Wu and Chua, 1994), it is based on the synchronisation of inverse systems, where the information signal is injected into a chaotic transmitter as a nonlinear filter
- chaos shift keying (Parlitz et al., 1992), the information signal is supposed to be binary, it is mapped into two chaotic systems coupled in master-slave configuration.
In all cases, the information signal is recovered if the transmitter and receiver chaotic systems are synchronised. Many examples of information transmission using synchronising systems can be found (Hasler, 2002; Liao and Huang, 1999; Boutayeb et al., 2002). In order to synchronise both sides, the transmitter and receiver sides should be identical (Hasler, 2002).

Observer schemes are widely used for chaotic communication. Among the most successful schemes is the Luenberger observer (Luenberger, 1964), which comprises a copy of the system plus a correction that is proportional to the observation error. Several extensions of the Luenberger observer have been proposed to cope with uncertainties in the system model. Linear state observer (Liao and Huang, 1999) and nonlinear observer (Boutayeb et al., 2002) in the control theory literature can be applied to design chaotic receivers, the main part of the observer (receiver) is a duplicate of the transmitter. But in some cases, such as there exists transmission noise, the transmitter parameters are not known exactly, the chaos system cannot reach synchronisation. Parameter identification methods can overcome this problem when the uncertain in the transmitter is regarded as some unknown parameters (Huijberts et al., 2000). Another interesting method to deal with uncertainties in chaotic communication is fuzzy model-based design (Lian et al., 2001), where transmitter and receiver are assumed to be modelled by the same fuzzy models. The effects of noise in transmission line are discussed in Alvarez et al. (2002) and Hasler (2002), where the receivers require structural information of the transmitters. How to design a robust receiver with respect to nonparametric uncertainties in the transmitter or even the transmitter is unknown, to the best of our knowledge, it has not yet been established in the literature.

In this paper, a novel design approach for chaotic communication is proposed. The main difference with the above methods is that the uncertainty in the transmitter can be structural, we only assumed it is bounded. We use high-gain observer, which have Proportional-plus-Integral (PI) form or Proportional (P) form. The natural application of PI and P observers have been proved for linear system with constant disturbances (Anderson and Moore, 1991). This paper will deal with non-constant model uncertainties in the transmitter side. Sufficient conditions for robust stability of the transmission signal are provided.

2 High gain observer for chaotic communication

In normal chaotic communication, the transmitter and the receiver are chaotic systems. They can be described in the form of the following nonlinear system

\[ \dot{\xi} = f(\xi) + g(\xi)u, \quad y = h(\xi) \]  

(1)

where \( \xi \in \mathbb{R}^n \) is the state of chaotic system, \( u \in \mathbb{R} \) is control input, \( y \in \mathbb{R} \) is measurable output. For many chaotic system, such as Chua’s circuit, there exists a mapping \( x = T(\xi) \) such that system (1) can be transformed into the following normal form (the conditions for this transform can be found in Isidori (1995))

\[ \dot{x}_i = x_{i+1}, \quad \dot{x}_n = F(x) + G(x)u, \quad y = x_1 \]  

(2)

where \( i = 1 \ldots n - 1 \). In the case of \( n = 2 \)

\[ \dot{x}_1 = x_2, \quad \dot{x}_2 = H(x_1, x_2, u), \quad y = x_1 \]  

(3)
where \( H(x_1, x_2, u) = F(x_1, x_2) + G(x_1, x_2)u \). Some chaotic systems can be described by equation (3) directly, for example Duffing equation (Chen and Dong, 1993),

\[
\dot{x}_1 = x_2, \quad \dot{x}_2 = p_1 x_1 - p_2 x_2^3 - px_2 + q \cos(\omega t) + u_t \tag{4}
\]

where \( p, p_1, p_2, q \) and \( \omega \) are constants. \( u_t \) is control input. It is known that the solution of equation (4) exhibits almost periodic and chaotic behaviour, if we select \( p_1 = 1.1, p_2 = 1, p = 0.4, q = 2.1, \omega = 1.8, u_t = 0 \). Van der Pol Oscillator Venkatasubramanian (1994) has also the form of equation (3),

\[
\dot{x}_1 = x_2, \quad \dot{x}_2 = a_1 [(1 - a_2 x_1^2) x_2 - a_3 x_1] + u_t. \tag{5}
\]

In uncontrolled case, if we select \( a_1 = 1.5, a_2 = 1, a_3 = 1 \), the Van der Pol oscillator equation (5) has a chaotic response.

In this paper, we use 'chaos modulation' to realise chaotic communication, where the information signal \( s \) is injected into the transmitter. A slight modification of normal chaotic system (3) is the transmitter

\[
\dot{x}_1 = x_2 + l_1 s, \quad \dot{x}_2 = H(x) + l_2 s, \quad y = x_1 + s \tag{6}
\]

where \( x = (x_1, x_2)^T \in \mathbb{R}^n \) is the transmitter state, \( s \) is the information signal \( H(x) \) is a real nonlinear function, \( (x_1 + s) \) is chaotic masking, \( l_1 s \) and \( l_2 s \) are chaotic modulation, \( l_1 \) and \( l_2 \) are constants, \( y \) is the signal in transmission line. A normal observer-based receiver has the following form

\[
\dot{\hat{x}_1} = \dot{\hat{x}_2} + l_1 (y - \hat{y}), \quad \dot{\hat{x}_2} = H(\hat{y}, \hat{x}_2) + l_2(y - \hat{y}), \quad \hat{y} = \hat{x}_1 \tag{7}
\]

where \( \hat{x}_1, \hat{x}_2 \) and \( \hat{y} \) are the states and the output in the receiver side. The information signal is recovered as \( \hat{s} = y - \hat{y} \). It can be seen that the receiver (7) is a replica of the transmitter (6). The drawbacks of such scheme are that \( H \) in the transmitter should be known, and it is difficult to choose \( l_1 \) and \( l_2 \) such that \( \hat{s} \to s \). Riccati inequality (LMI tools) (Boutayeb et al., 2002; Liao and Huang, 1999) and observability matrix (Alvarez et al., 2002) can be used to obtain them. In this paper we assume the nonlinear function \( H(x) \) is poorly known because of uncertainties in the transmitter. An estimation of \( H(x) \) is available, we define it as \( \hat{H}(x) \). The modelling error is

\[
\eta(x) = H(x) - \hat{H}(x). \tag{8}
\]

Because the modelling error \( \eta \) is not available in the receiver side, we will estimate it in an observer in order to improve signal recovery accuracy. The receiver is a high gain observer in PI form,

\[
\begin{align*}
\dot{\hat{x}_1} &= \hat{x}_2 + \tau^{-1} (y - \hat{y}) \\
\dot{\hat{x}_2} &= \hat{H}(\hat{x}) + \hat{\eta} + 2\tau^{-2} (y - \hat{x}_2) \\
\dot{\hat{\eta}} &= \tau^{-2} (y - \hat{x}_2), \quad \hat{y} = \hat{x}_1
\end{align*} \tag{9}
\]

where \( \hat{x} = (\hat{x}_1, \hat{x}_2)^T \), \( \hat{\eta} \) is the estimation of \( \eta \), \( \tau > 0 \) is the observer gain. One can see that the dynamic of \( \hat{x}_2 \) comprises known part of the transmitter plus a correction term that is proportional to the velocity observation error \( (\hat{y} - \hat{x}_2) \). Also it can be seen that the
time derivative \( \dot{y} \) appears in the right-hand side of the system (9). In principle one could use numerical differentiation to obtain approximation of \( \dot{y} \), however, this procedure can yield excessive amplification of measurement noise. A more systematic approach to implement equation (9) is to introduce the new coordinates to avoid noise-enlarge problem,

\[
\omega_1 = \dot{x}_2 - 2\tau^{-1}y, \quad \omega_2 = \dot{\eta} - \tau^{-2}y.
\]

Now the dynamic of the receiver is equivalent to

\[
\dot{\omega}_1 = \dot{H}(\dot{x}) - 2\tau^{-1}\dot{x}_2 + \ddot{\eta}, \quad \dot{\omega}_2 = -\tau^{-2}\dot{x}_2.
\] (10)

It is interesting to note that the system (9) has the structure of PI form for \( \dot{x}_2 \). In fact, since

\[
\ddot{\eta}(t) = \dot{\eta}(0) + \tau^{-2}\int_0^t [\dot{y}(\tau) - \dot{x}_2(\tau)]d\tau
\]

we have

\[
\dot{x}_2 = \dot{H}(\dot{x}) + \{\ddot{\eta}(0) + 2\tau^{-1}(\dot{y} - \dot{x}_2) + \tau^{-2}\int_0^t [\dot{y}(\tau) - \dot{x}_2(\tau)]d\tau\}.
\]

The term in the brackets is actually a PI correction term acting on the estimation error \( \dot{y} - \dot{x}_2 \). The aim of the integral correction term is to compensate for uncertainties in the nonlinear function \( \dot{H}(\dot{x}) \). To avoid the use of derivative in the measurement signal, the PI observer uses an implicit integral action. The schematic diagram of the chaotic communication based on high gain observer is shown in Figure 1.

Although we have restricted ourselves to the case of second-order chaotic system, the observer construction and stability analysis which will be discussed in the next section can be extended to the \( n \)-dimensional case. The transmitter is a set of \( n \) first-order differential equations,

\[
\dot{x}_i = x_{i+1}, \quad \dot{x}_{n-1} = x_{n-2} + l_1s, \quad \dot{x}_n = \dot{H}(x) + l_2s
\]

where \( i = 1, \ldots, n-2 \). Similarly to the second-order system, the receiver is

\[
\dot{x}_i = \dot{x}_{i+1} + \tau^{-1}x_i(\dot{y} - \dot{x}_2) \\
\dot{x}_n = \dot{H}(\dot{x}) + \dot{\eta} + \tau^{-n}\beta_{n-1}(\dot{y} - \dot{x}_2) \\
\dot{\eta} = \tau^{-n}\beta_n(\dot{y} - \dot{x}_2)
\] (11)

where the constants \( \beta_j \)’s are chosen such that the polynomial \( s^n + \beta_n s^{n-1} + \ldots + \beta_1 = 0 \) has all its roots in the open left-hand side of the complex plane. By defining the new variables \( \omega_j = \dot{x}_{j+1} - \tau^{-j}\beta_j y, \ j = 1, \ldots, n-1, \) and \( \omega_n = \ddot{\eta} - \tau^{-n}\beta_ny \), the observer can be rewritten as

\[
\dot{\omega}_j = \dot{x}_{j+2} - \tau^{-j}\beta_{j-1}\dot{x}_n \\
\dot{\omega}_{n-1} = \dot{H}(\dot{x}) - \tau^{-(n-1)}\beta_{n-1}\dot{x}_n, \quad \ddot{\omega}_n = -\tau^{-n}\beta_n\dot{x}_n
\] (12)

where, the estimated states and modelling error are given by \( \dot{x}_i = \omega_{i-1} + \tau^{-(i-1)}\beta_{i-1}y, \ i = 2, \ldots, n, \) and \( \ddot{\eta} = \omega_n + \tau^{-n}\beta_ny. \)
If the transmitter is unknown completely, i.e., $\hat{H}(x) = 0$, integral correction is longer needed to estimate modeling error $\eta$. We use the following P form high gain observer,

$$
\dot{x}_1 = \dot{x}_2 + k_1 \tau^{-1}(y - \hat{y}), \quad \dot{x}_2 = k_2 \tau^{-2}(y - \hat{y}), \quad \hat{y} = \dot{x}_1
$$

(13)

where $k_1$ and $k_2$ are positive constants, they are chosen such that the roots of $s^2 + k_1 s + k_2 = 0$ have negative real parts. In $n$-dimensional case, the P form high gain observer-based receiver is

$$
\dot{x}_j = \dot{x}_{j+1} + \frac{k_j}{\tau^j}(y - \hat{y})
$$

$$
\dot{\hat{x}}_{n-1} = \dot{x}_{n-2} + \frac{k_{n-1}}{\tau^{n-1}}(y - \hat{y}), \quad \dot{\hat{x}}_n = \frac{k_n}{\tau^n}(y - \hat{y})
$$

(14)

where the constants $k_j$ are chosen such that the polynomial $\mu^n + k_{n-1} \mu^{n-1} + \ldots + k_1 = 0$ has all its roots in the open left-hand side of the complex plane. In order to recovery the encrypted signal, it is required that the signal estimation error $s - \hat{s}$ between transmitter (6) and receiver (9) tends to zero. Next section will give this answer.
3 Stability analysis of the chaotic communication

To establish the stability properties of the proposed chaotic communication, we define the following errors for PI form high gain observer $e_1 = \tau^{-1}(x_1 - \hat{x}_1)$, $e_2 = \tau^{-1}(x_2 - \hat{x}_2)$, $e_3 = \eta - \hat{\eta}$. By $\hat{y} - \hat{x}_2 = x_2 + \hat{s} - \hat{x}_2 + l_1 s$, the error dynamics is given by

$$\dot{e} = \tau^{-1}Ae + \tau^{-1}C(s, \hat{s}) + B_1 e + B_2 \hat{H} + B_3 \hat{\eta}$$

where $e = [e_1, e_2, e_3]^T$, $\hat{H} = H(x) - \hat{H}(\hat{x})$, $\hat{\eta} = (\frac{\partial \eta}{\partial x_1})(x_2 + l_1 s) + (\frac{\partial \eta}{\partial x_2})[H(x) + l_2 s] + (\frac{\partial \eta}{\partial s})\hat{s}$.\n
$A = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & -1 & 0 \end{bmatrix}$, $C(s, \hat{s}) = \begin{bmatrix} l_2 s_1 \\ l_3 s_1 - 2s_1 \end{bmatrix}$, $B_1 = [0, 0, 0]^T$, $B_2 = (0, 1, 0)^T$, $B_3 = (0, 0, 1)^T$, $s_1 = l_1 s + \hat{s}$. For the chaotic communication, the following properties are right

- $H(x)$ at transmitter end (6) is Lipschitz with respect to $x$, i.e.,

$$|\hat{H}| \leq \beta_1 \|x - \hat{x}\| = \beta_1 \|B_2\|\|e\|$$

where $\beta_1$ is a positive real scalar.

- The state of chaotic system evolves in a compact $\Omega$, $(\frac{\partial \eta}{\partial x_1})$, $(\frac{\partial \eta}{\partial x_2})$ and $(\frac{\partial \eta}{\partial s})$ are bounded by Lipschitz condition, also the signal $\hat{s}$ is assumed to be bounded, so

$$\left| \begin{bmatrix} \frac{\partial \eta}{\partial x_1} \\ \frac{\partial \eta}{\partial x_2} \end{bmatrix} \begin{bmatrix} x_2 + l_1 s \\ H(x) + l_2 s \end{bmatrix} + \begin{bmatrix} \frac{\partial \eta}{\partial s} \end{bmatrix} s \right|$$

is bounded, we have

$$\|B_3 \hat{\eta}\|_{\Lambda_\eta} = (B_3 \hat{\eta})^T \Lambda_\eta (B_3 \hat{\eta}) \leq \beta_2$$

where $\beta_2$ is a positive real constant and $\Lambda_\eta$ is a positive definite matrix.

- The elements of $C(s, \hat{s})$ are periodical and bounded functions

$$\|C(s, \hat{s})\|_{\Lambda_c} = C^T \Lambda_c C \leq \beta_3$$

where $\Lambda_c$ is a positive definite matrix. Next theorem gives the upper bound of the encrypted signal $s$.

Notice that the matrix $A$ in equation (15) is stable, so exists a positive-definite matrix $P$ such that

$$PA + A^T P = -I.$$

**Theorem 1:** If we use PI form high gain receiver (9) and (10) to recover the information signal in the transmitter end (6), and the observer gain satisfies

$$\tau \leq \min \left(1, \frac{1}{\gamma} \right)$$

where $\gamma = \lambda(PA^{-1}P) + \lambda(P\Lambda^{-1}_\eta P) + 2\beta_1 \lambda(||P||) + 2\lambda(||P||)$, then the encrypted signal error ($\hat{s} = s - \hat{s}$) in the chaotic communication is globally bounded.
186 W. Yu et al.

and converges to a neighbourhood of the origin

\[
\limsup_{T \to \infty} \frac{1}{T} \int_0^T s^2 dt \leq \frac{\tau}{\beta_3}
\]

(20)

where \( \beta_3 \) are defined in equation (18).

Proof: Consider the Lyapunov function

\[ V = e^T Pe. \]

Its time derivative along equation (15) is

\[ \dot{V} = -\tau^{-1}||e||^2 + 2e^T P[\tau^{-1} C + \tau B_1 e + B_2 \tilde{H} + B_3 \dot{\eta}]. \]

(21)

Because the facts pointed in equations (16), (17) and (18), equation (21) becomes

\[ \dot{V} \leq -\tau^{-1}||e||^2 + 2\tau^{-1}e^T PC + 2\tau\lambda_{\max}(||P||)||e||^2 \\
+ 2\beta_1 \lambda_{\max}(||P||)||e||^2 + 2e^T PB_3 \dot{\eta}. \]

(22)

Using matrix inequality

\[ X^T Y + (X^T Y)^T \leq X^T A^{-1} X + Y^T A Y \]

where \( X, Y \in \mathbb{R}^{n \times k} \) are any matrices, \( A \) is any positive definite matrix, we can estimate

\[ 2\tau^{-1}e^T PC \leq e^T P A_{\eta}^{-1} P e + \tau^{-2} C^T A C \leq \lambda(P A_{\eta}^{-1} P)||e||^2 + \tau^{-2} \beta_3 \]

\[ 2e^T PB_3 \dot{\eta} \leq \lambda(P A_{\eta}^{-1} P)||e||^2 + \beta_2. \]

(23)

So

\[ \dot{V} \leq -\alpha ||e||^2 + \beta \]

(24)

where

\[ \beta = \tau^{-1} - a - \tau b \]
\[ \alpha = \tau^{-2} \beta_3 + \beta_2 \]

a, b, \( \beta_2 \) and \( \beta_3 \) are positive constants, \( a = \lambda(P A_{\eta}^{-1} P) + \lambda(P A_{\eta}^{-1} P) + 2\lambda(||P||) \beta_1 \), \( b = 4\lambda(||P||) \), \( \lambda(A) \) is the maximum eigenvalue of \( A \). From equation (19) we know

\[ \tau^{-1} \geq \lambda(P A_{\eta}^{-1} P) + \lambda(P A_{\eta}^{-1} P) + 2\beta_1 \lambda(||P||) + 2\lambda(||P||). \]

Since \( \frac{V}{\lambda_{\max}(P)} \leq ||e||^2, \dot{V} \leq -\alpha ||e||^2 + \beta \leq -\frac{\alpha}{\lambda_{\max}(P)} V + \beta. \) If we start from \( V(0) \geq \frac{\beta}{\alpha} \lambda_{\max}(P), V < 0. \) This means that \( V \) is globally bounded. Integrating equation (21) from 0 up to \( T \) yields

\[ V_T - V_0 \leq -\alpha \int_0^T ||e||^2 dt + \beta T. \]
We have
\[
\frac{1}{T} \int_0^T \|e\|^2 dt \leq \frac{1}{\alpha T} (V_0 - V_T + \beta T) \leq \frac{V_0}{\alpha T} + \frac{\beta}{\alpha}.
\]
So
\[
\limsup_{T \to \infty} \frac{1}{T} \int_0^T \|e\|^2 dt \leq \frac{\beta}{\alpha}.
\]
Because \(e_1 = \tau^{-1}(y - \hat{y})\) and \(\hat{s} = y - \hat{y} = \tilde{x}_1 + s, \tau < 1\)
\[
\|e\|^2 = \tau^{-2}[x_1 - \hat{x}_1]^2 + [x_2 - \hat{x}_2]^2 + [\eta - \hat{\eta}]^2 > e_1^2 > \tilde{s}^2,
\]
so
\[
\limsup_{T \to \infty} \frac{1}{T} \int_0^T \tilde{s}^2 dt < \limsup_{T \to \infty} \frac{1}{T} \int_0^T \|e\|^2 dt \leq \frac{\beta}{\alpha}.
\]
Because
\[
\frac{\beta}{\alpha} = \tau^{-1} - a - \tau b = \frac{1 - a \tau - \tau^2 b}{\beta_3 + \tau^2 \beta_2} \leq \frac{\tau}{\beta_3},
\]
equation (20) is established.

**Remark 1:** In order to ensure the stability, it is clear that the parameters \(\alpha\) and \(\beta\) must be strictly positive, or \(\tau\) should be small enough. The convergence radius in a neighbourhood of the origin is \(\frac{\tau}{\beta_3}\), if we choose \(\tau\) small enough, the encrypted signal error \((s - \hat{s})\) can be arbitrarily small. The encrypted signal error \(s - \hat{s}\) is globally bounded and converges to a neighbourhood of the origin, this result is actually practical stability for signal recovery.

For P form high gain observer as in equation (13). The stability analysis is based on the following transformation. We define a new pair of variables \(\tilde{z}_1 = x_1 - \hat{x}_1, \tilde{z}_2 = \tau(x_2 - \hat{x}_2)\), the error dynamic is
\[
\tau \dot{\tilde{z}} = A_p \tilde{z} + \tau^2 B_p H(\tilde{z}_1, \tilde{z}_2, s)
\]
where \(\tilde{z} = [\tilde{z}_1^T, \tilde{z}_2^T]^T, A_p = \begin{bmatrix} -k_1 & 1 \\ -k_2 & 0 \end{bmatrix}, B_p = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\). We select \(k_1\) and \(k_2\) such that \(A_p\) is stable, i.e., \(\det(\mu I - A_p) = \mu^2 + k_1 \mu + k_2\) has all its roots in the open left-hand side of the complex plane.

**Theorem 2:** If the synchronisation parameters are selected \(l_1 = \frac{k_1}{\tau}, l_2 = \frac{k_2}{\tau}\), the signal recovery error between the high gain observer-based receiver (13) and the chaotic transmitter (6) converges to the following residual set
\[
D = \{\tilde{s} \mid \|\tilde{s}\| \leq 2\tau^2 C_T\}, \quad \tilde{s} = s - \hat{s}
\]
where $C_T = \sup_{t \in [0, T]} \|B_p H\|P\|$. $P$ is a solution of the following Lyapunov equation $A_p^T P + P A_p = -I$.

**Proof:** Due to the fact that $A_p$ is stable, there exists a positive definite matrix $P$ such that the Lyapunov equation $A_p^T P + P A_p = -I$ is established. Consider following Lyapunov function $V(\tilde{z}) = \tau \tilde{z}^T P \tilde{z}$. The derivation along the solutions of equation (25) is

$$
\dot{V} = \tau \tilde{z}^T P \tilde{z} + \tau \tilde{z}^T P \dot{\tilde{z}} = [A_p \tilde{x} + \tau^2 B_p H(\tilde{z}_1, \tilde{z}_2, s)]^T P \tilde{z} + \tilde{z}^T P [A_p \tilde{x} + \tau^2 B_p H(\tilde{z}_1, \tilde{z}_2, s)]^T P \tilde{z} \leq \tau \tilde{z}^T (A_p^T P + P A_p) \tilde{z} + 2\tau^2 \|B_p H(\tilde{z}_1, \tilde{z}_2, s)\|P\|P\|\|\tilde{z}\|.
$$

By equation (17), the state of chaotic system evolves in a compact $\Omega$, so $\|B_p H(\tilde{z}_1, \tilde{z}_2, s)\|$ is bounded for any finite time $T$. We conclude that $\|B_p H(\tilde{z}_1, \tilde{z}_2, s)\|P\|$ is bounded. If we define $\overline{K}(\tau) = 2\tau^2 C_T, C_T = \sup_{t \in [0, T]} \|B_p H(\tilde{z}_1, \tilde{z}_2, s)\|P\|,$

$$
\dot{V} \leq -\|\tilde{z}\|^2 + \overline{K}(\tau)\|\tilde{z}\|.
$$

It is noted that if $\|\tilde{z}(t)\| > \overline{K}(\tau)$, then $\dot{V} < 0, \forall t \in [0, T]$. So the total time during which $\|\tilde{z}(t)\| > \overline{K}(\tau)$ is finite. Let $T_k$ denotes the time interval during $\|\tilde{z}(t)\| > \overline{K}(\tau)$. If only finite times that $\tilde{z}(t)$ stay outside the ball of radius $\overline{K}(\tau)$ and then reenter, $\tilde{z}(t)$ will eventually stay inside of this ball. If $\tilde{z}(t)$ leave the ball infinite times, since the total time $\tilde{z}(t)$ leave the ball is finite, $\sum_{k=1}^{\infty} T_k < \infty$, so $\lim_{k \to \infty} T_k = 0$. Now $\tilde{z}(t)$ is bounded via an invariant set argument. From equation (25) $\tilde{z}(t)$ is also bounded. Let $\|\tilde{z}_k(t)\|$ denote the largest tracking error during the $T_k$ interval. Then equation (20) and bounded $\tilde{z}(t)$ imply that

$$
\lim_{k \to \infty} \|\tilde{z}_k(t)\| - \overline{K}(\tau) = 0.
$$

So $\|\tilde{z}_k(t)\|$ will convergence to $\overline{K}(\tau)$. Because $\tilde{s} = \tilde{y} - \tilde{y} = \tilde{x}, \tilde{s} = [1, 0] \tilde{x} = [1, 0] \left[ \begin{array}{c} 0 \\ 0 \end{array} \right] \tilde{z}$, and $\tau < 1$. So $\|\tilde{s}\|$ converges to the ball of radius $\overline{K}(\tau)$. Since $C_T$ is bounded, we can select $\tau$ arbitrarily small (the gain of the receiver (13) becomes bigger) in order to make the observer error small enough. So $\|\tilde{s} - \tilde{s}\|$ can be arbitrarily small when $\tau \to 0$.

**Remark 2:** As the second-order case, the signal recovery error in $n-$dimensional case converges to any accuracy $(2\tau^2 C_T)$ by selecting sufficiently small values of observer gain $\tau$. The synchronisation parameter is chosen as the observer gain is $[\xi_1 \cdots \xi_n]^T$.

The PI and P form observer-based receivers proposed in this papers require the chaotic transmitter has the normal form as in equation (2), such as Duffing equation and Van der Pol oscillator. It cannot be applied directly to other types of chaotic systems, for example Chua’s circuit,

\[
\begin{align*}
C_1 \dot{\xi}_1 &= G(\xi_2 - \xi_1) - g(\xi_1) + u \\
C_2 \dot{\xi}_2 &= G(\xi_1 - \xi_2) + \xi_3, \quad L \dot{\xi}_3 = -\xi_2, \quad y = \xi_3
\end{align*}
\]
where \( g(\xi_1) = m_0 x_1 + \frac{1}{2} (m_1 - m_0) \cdot |\xi_1 + B_p| + |\xi_1 - B_p| \). \( \xi_1, \xi_2, \xi_3 \) denote, respectively, the voltages across \( C_1 \) and \( C_2 \) and the current through \( L \). If we make transformation as \( x_1 = \xi_3, x_2 = -\frac{1}{L} \xi_2, x_3 = \frac{L}{C_1} (\xi_2 - \xi_1) - \frac{1}{C_2} \xi_3, \) then Chua's circuit becomes normal form as
\[
\dot{x}_1 = x_2, \quad \dot{x}_2 = x_3, \quad \dot{x}_3 = f + gu, \quad y = x_1
\]
where \( g = \frac{G}{c_1 c_2}, f = \frac{G}{c_2} \{ -x_3 + \frac{G}{c_1} [2x_2 + \frac{1}{c_2} x_1 + \frac{G}{c_4} x_3 - \frac{1}{c_3} g(x_1 + \frac{1}{c_2} x_1 + \frac{G}{c_4} x_3)] \} - \frac{1}{c_2 L} x_1 \). High gain observer-based receivers can also be applied for Chua's circuit.

### 4 Numerical simulation

In this section, the information signal \( s \) is first chosen as one-dimensional sinusoidal signal with frequency of 30 Hz as in Boutayeb et al. (2002) and Liao and Huang (1999), i.e., \( s = 0.1 \sin(60\tau t) \). First we use Duffing equation to transmit the signal, the transmitter is (6) with \( H(x) = -1.1 y - y^3 - 0.4 x_2 + 2.1 \cos(1.8 t) \), the initial condition for the transmitter is \( x(0) = [0, 0]^T \). Three types of receivers are applied to compare the theory results proposed in this paper, the initial conditions for the receivers are \( \hat{x}(0) = [1, 1]^T \).

- **High-gain observer in PI form** is as in equation (9) and (10). We assume \( H(x) \) is partly known, \( H(\hat{x}) = -\dot{\hat{y}} - 0.5 \dot{\hat{x}}_2 \). The parameters for the transmitter are \( l_1 = 20, l_2 = 35 \). To illustrate performance of PI receiver, we use two different observer gains \( \tau_1 = 0.1, \tau_2 = 0.05 \) to show how to recover the encrypted signal, see Figure 2. From Theorem 1 we know the signal error is less than \( \frac{2}{\tau} \), a small \( \tau \) can lead a better accuracy, but transient response is worse. The transmitter parameters \( l_1 \) and \( l_2 \) do effect the receiver. Although the transmitter is known partly, the encrypted signal can be recovered successfully if \( \tau \) is small enough.

- **High-gain observer in P form** is as in equation (13). We choose \( k_1 = k_2 = 1 \), so \( A \) is stable and \( P = \begin{bmatrix} 1 & -\frac{3}{2} \\ -\frac{3}{2} & \frac{3}{2} \end{bmatrix} > 0 \). We let \( \sup(C_T) = 100 \), and select \( \tau = 0.01 \). According to Theorem 2, the synchronisation parameters should be \( l_1 = 10^2, l_2 = 10^4 \). Figure 2 gives signal recovery errors of two types of receivers. We can see that P form high-gain observer does not use any information of the transmitter, but it requires the transmitter satisfies the condition \( l_1 = \frac{2}{\tau}, l_2 = \frac{2.2}{\tau} \).

- **Model-base observer** requires complete information of the transmitter. We use linear observer (Liao and Huang, 1999) to compare with our results, see Figure 3. We find that model-based observer gives the best performance, but if the transmitter is unknown or partly known, this kind of receiver does not work. Another advantage of model-based receiver is that it can be applied to any chaotic transmitter as in equation (1), but high-gain observer is only suitable for the chaotic system which has the normal form as in equation (2).

We define the maximum relative error is defined as \( e_{\text{max}} = \max(|x - \hat{x}|) \). After transient process \( t > 1.5 s \), for model-base observer \( e_{\text{max}} \approx 0.2 \%. \) For P form high-gain
observers with $l_1 = 10^2$, $l_2 = 10^4$, $e_{\text{max}} \cong 0.5\%$; with $l_1 = 0.9 \times 10^2$, $l_2 = 0.9 \times 10^4$, $e_{\text{max}} \cong 2\%$. For PI form high-gain observers ($\tau = 0.05$), $e_{\text{max}} \cong 1.5\%$

Because the use of the sinusoidal signal is not enough to show the effectiveness of the proposed approach, now we use chirp signal (see Figure 4) to approximate voice data to show how the transmission of digital data in the communications is carried out. We use the same P and PI high-gain observers to construct the receivers, the signal errors are shown in Figure 4. After transient process ($t > 1.5\,\text{s}$), for P form high-gain observers with $l_1 = 0.9 \times 10^2$, $l_2 = 0.9 \times 10^4$, $e_{\text{max}} \cong 3.6\%$. For PI form high-gain observers ($\tau = 0.05$), $e_{\text{max}} \cong 2.1\%$.

**Figure 2** The encrypted signal is recovered by PI form high gain observer (see online version for colours)

![Figure 2](image)

**Figure 3** Signal errors for different types of receivers (see online version for colours)

![Figure 3](image)
5 Conclusion

In this paper, we propose two types of high-gain observer for chaotic communication. Uncertainties at transmitter end and transmission line are considered. We prove that the communication single error can be arbitrarily small by selecting a proper observer gain in the receiver end.

References


