

Synchronization for Uncertain Chaotic Systems with Channel Noise and Chaos-based Secure Communications

Junqi Yang and Fanglai Zhu

1 Introduction

Chaos synchronization and chaos-based secure communication have been a hot topic in the literatures [1–8]. Some recent work in chaos-based secure communication can be found in [5–8]. For example, an adaptive observer-based synchronization scheme for private communication is proposed in [5]. Based on the singular system observer, an approach for chaotic synchronization and private communication is developed in [6]. Within the drive-response configuration, the synchronization of chaotic systems and chaos-based secure communication are discussed in [7]. The problems of the synchronization and secure communication are explored using techniques based on knowledge of statistics in [8].

This chapter discusses the topics of synchronization and secure communication, but the chaotic system with channel noise is used as the transmitter, which is a distinction from the above-mentioned papers. The receiver is the combination of robust sliding mode observer and a first robust differentiator, which can not only synchronize the transmitter but also recover the information signal.

J. Yang

College of Electronics and Information Engineering, Tongji University,
Shanghai 201804, China

College of Electrical Engineering and Automation, Henan Polytechnic University,
Jiaozuo, Henan 454000, China

e-mail: yjq@hpu.edu.cn; 2010_yjq@tongji.edu.cn

F. Zhu (✉)

College of Electronics and Information Engineering, Tongji University,
Shanghai 201804, China

e-mail: zhufanglai@tongji.edu.cn

2 General Model and Problem Statement

Consider a class of uncertain chaotic system with channel noise which is used as the transmitter in chaos-based secure communication:

$$\begin{cases} \dot{x} = Ax + Bf(x) + Bs + D\eta \\ y = Cx + Ed \end{cases} \tag{1}$$

where $x \in \mathbb{R}^n$ is the state vector, $y \in \mathbb{R}^p$ is the drive or transmitted signal, $s \in \mathbb{R}^m$ is the information signal vector which should be recovered in the receiver end, $f(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R}^m$ stands for the nonlinear term, $\eta \in \mathbb{R}^q$ is the disturbance vector, and $d \in \mathbb{R}^l$ is the channel noise vector which is assumed to be a piecewise continuous vector function. We assume that $\text{rank } B = m$, $\text{rank } C = p$, $\text{rank } D = q$, $\text{rank } E = l$, $\text{rank } H = m + q$, and $n \geq p \geq w$, where $H = [B \ D]$ and $w = m + q + l$.

Assumption 1 For System (1), the following condition

$$\text{rank} \left(\begin{bmatrix} s_*I - A & 0 & H \\ C & E & 0 \end{bmatrix} \right) = n + w \tag{2}$$

holds for all complex number s_* with $\text{Re}(s_*) \geq 0$.

Assumption 2 $\text{rank}[CH \ E] = w$.

Assumption 3 The state $x(t)$, nonlinear function $f(x)$, information signal $s(t)$, disturbance vector $\eta(t)$ and their derivatives, are all bounded in norm.

Assumption 4 The nonlinear function $f(x)$ satisfy Lipschitz conditions

$$\|f(x) - f(\hat{x})\| \leq L_f \|x - \hat{x}\|, \quad \forall x, \hat{x} \in \mathbb{R}^n \tag{3}$$

where the Lipschitz constant L_f are unknown.

Lemma 1 [9] For any piecewise continuous vector function $f(t) \in \mathbb{R}^l$, and a stable $l \times l$ matrix A_f , there will always exist an input vector $\zeta \in \mathbb{R}^l$ such that differential equation $\dot{f} = A_f f + \zeta$ holds.

Based on Lemma 1, the measurement noise d can be regarded as the output of the following dynamical system

$$\dot{d} = A_d d + v \tag{4}$$

where $v \in \mathbb{R}^l$ is an additive unknown bounded noise and $A_d \in \mathbb{R}^{l \times l}$ is Hurwitz.

If we set $\bar{x} = [x^T \ d^T]^T$ as an augmented state vector, we obtain

$$\begin{cases} \dot{\bar{x}} = \bar{A}\bar{x} + \bar{B}f(K\bar{x}) + \bar{B}s + \bar{D}\phi \\ y = C\bar{x} \end{cases} \tag{5}$$

where

$$\bar{A} = \begin{bmatrix} A & 0 \\ 0 & A_d \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{D} = \begin{bmatrix} D & 0 \\ 0 & I_l \end{bmatrix}, \bar{C} = \begin{bmatrix} C^T \\ E^T \end{bmatrix}^T, K = [I_n \quad 0], \phi = \begin{bmatrix} \eta \\ \nu \end{bmatrix}$$

Lemma 2 *The System (4) is minimum phase, i.e., the invariant zeros of the triple $\{\bar{A}, \bar{C}, \bar{H}\}$ are all in the open left-hand complex plane, or*

$$\text{Rank} \begin{bmatrix} s_* I - \bar{A} & \bar{H} \\ \bar{C} & 0 \end{bmatrix} = n + w + l \tag{6}$$

holds for all complex number s_* with $\text{Re}(s_*) \geq 0$ if and only if (2) holds for all complex number s_* with $\text{Re}(s) \geq 0$, where $\bar{H} = [\bar{B} \quad \bar{D}]$.

Based on (2), it is easy to prove Lemma 2.

Lemma 3 [10] *Lemma 2 together with the observer matching condition*

$$\text{rank} \bar{H} = \text{rank}(\bar{C}\bar{H}) = w \tag{7}$$

holds if and only if for symmetric positive definite matrix $\bar{Q} \in \mathbb{R}^{(n+l) \times (n+l)}$, there exist matrices $\bar{L} \in \mathbb{R}^{(n+l) \times p}$, $\bar{F} = [\bar{F}_1 \quad \bar{F}_2] \in \mathbb{R}^{(m+q+l) \times p}$ and a symmetric positive definite matrix $\bar{P} \in \mathbb{R}^{(n+l) \times (n+l)}$ such that

$$\begin{cases} (\bar{A} - \bar{L}\bar{C})^T \bar{P} + \bar{P}(\bar{A} - \bar{L}\bar{C}) = -\bar{Q} \\ \bar{H}^T \bar{P} = \bar{F} \bar{C} \end{cases} \tag{8}$$

holds where $\bar{F}_1 \in \mathbb{R}^{m \times p}$ and $\bar{F}_2 \in \mathbb{R}^{(q+l) \times p}$.

Because of Assumption 2, we have $\text{rank}(\bar{C}\bar{H}) = \text{rank}[CH \quad E] = w$ and $\text{rank} \bar{H} = \text{rank} H + l = w$. So, the observer matching condition (5) is satisfied.

3 Synchronization and Channel Noise Estimation Based on Robust Sliding Mode Observers

Consider the following system with the same state and output equations as (4)

$$\begin{cases} \dot{\bar{x}} = \bar{A}\bar{x} + \bar{B}f(K\bar{x}) + \bar{H}\varphi \\ y = \bar{C}\bar{x} \end{cases} \tag{9}$$

where $\varphi = [s^T \quad \phi^T]^T$. There exists a positive constant ρ_φ such that $\|\varphi\| \leq \rho_\varphi$.

Theorem 1 Under Assumptions 1–4, an adaptive robust full-order observer (10) with (11) and (12) is designed as

$$\dot{\hat{x}} = \bar{A}\hat{x} + \bar{B}f(K\hat{x}) + \frac{1}{2}\hat{k}\bar{B}\bar{F}_1(y - \bar{C}\hat{x}) + \bar{L}(y - \bar{C}\hat{x}) + \alpha(y, \hat{x}, t) \quad (10)$$

$$\dot{\hat{k}} = l_k \|\bar{F}_1(y - \bar{C}\hat{x})\|^2 \quad (11)$$

$$\alpha(y, \hat{x}, t) = \rho_\varphi \frac{\bar{H}\bar{F}(y - \bar{C}\hat{x})}{\|\bar{F}(y - \bar{C}\hat{x})\|} \quad (12)$$

and the state estimation \hat{x} converges to the actual state \bar{x} asymptotically.

Proof The error dynamic system between (10) and the first equation of (9) is

$$\dot{\tilde{x}} = (\bar{A} - \bar{L}\bar{C})\tilde{x} + \bar{B}\tilde{f} + \bar{H}\varphi - \frac{1}{2}\hat{k}\bar{B}\bar{F}_1(y - \bar{C}\hat{x}) - \alpha(y, \hat{x}, t) \quad (13)$$

where $\tilde{x} = \bar{x} - \hat{x}$, $\tilde{f} = f(K\bar{x}) - f(K\hat{x})$. Consider the Lyapunov function $V = \tilde{x}^T \bar{P}\tilde{x} + \frac{1}{2}l_k^{-1}\tilde{k}^2$, where $\tilde{k} = k - \hat{k}$ and k is a constant which will be determined later. The derivative of V along the error dynamic System (13) is

$$\dot{V} = \tilde{x}^T \bar{Q}\tilde{x} + 2\tilde{x}^T \bar{P}\bar{B}\tilde{f} + 2\tilde{x}^T \bar{P}\bar{H}\varphi - \tilde{x}^T \bar{P}\bar{B}\bar{F}_1\hat{k}(y - \bar{C}\hat{x}) - 2\tilde{x}^T \bar{P}\alpha + l_k^{-1}\tilde{k}\dot{\tilde{k}}$$

The second equation of (8) means that $\bar{B}^T \bar{P} = \bar{F}_1 \bar{C}$, we can obtain

$$2\tilde{x}^T \bar{P}\bar{H}\varphi \leq 2\|\varphi\| \|\bar{H}^T \bar{P}\tilde{x}\| \leq 2\rho_\varphi \|\bar{F}\bar{C}\tilde{x}\| \quad (14)$$

$$\tilde{x}^T \bar{P}\bar{B}\bar{F}_1\hat{k}(y - \bar{C}\hat{x}) = \hat{k}\tilde{x}^T \bar{P}\bar{B}\bar{F}_1\bar{C}\tilde{x} = \hat{k}\|\bar{F}_1\bar{C}\tilde{x}\|^2 \quad (15)$$

$$2\tilde{x}^T \bar{P}\alpha = 2\rho_\varphi \|\bar{F}\bar{C}\tilde{x}\| \quad (16)$$

We can obtain $\|\tilde{f}\| = \|f(K\bar{x}) - f(K\hat{x})\| \leq L_f \|K\| \|\tilde{x}\| = L_f \|\tilde{x}\|$, so

$$2\tilde{x}^T \bar{P}\bar{B}\tilde{f} \leq 2L_f \|\bar{F}_1\bar{C}\tilde{x}\| \|\tilde{x}\| \leq \frac{L_f^2}{\varepsilon} \|\bar{F}_1\bar{C}\tilde{x}\|^2 + \varepsilon \|\tilde{x}\|^2 \quad (17)$$

where $\varepsilon > 0$. Here k is selected as $k = L_f^2/\varepsilon$. Based on (14)–(17), we have

$$\dot{V} \leq -\tilde{x}^T (\bar{Q} - \varepsilon I)\tilde{x} + ((L_f^2/\varepsilon) - \hat{k}) \|\bar{F}_1\bar{C}\tilde{x}\|^2 - l_k^{-1}\tilde{k}\dot{\tilde{k}} = -\tilde{x}^T (\bar{Q} - \varepsilon I)\tilde{x} = -\omega(t) \quad (18)$$

From the above inequality, free parameters ε can be chosen to be small enough such that $(\bar{Q} - \varepsilon I)$ is a positive definite matrix, i.e., $\dot{V} < 0$. So based on Lyapunov

stability theory, we know that the equilibrium $\tilde{x} = 0$ is stable. Now integrating (18) from zero to t yields $V(t) + \int_0^t \omega(\tau) d\tau \leq V(0)$ and the above inequality means that $\int_0^t \omega(\tau) d\tau \leq V(0)$, since $V \geq 0$. As t approach to infinity, the above integral is less than or equal to $V(0)$, so $\lim_{t \rightarrow \infty} \int_0^t \omega(\tau) d\tau$ exists and is finite. By Barbalat's Lemma, we have $\lim_{t \rightarrow \infty} \omega(t) = 0$ which implies that $\lim_{t \rightarrow \infty} \tilde{x}(t) = 0$.

After we obtain the state estimation \hat{x} from adaptive robust sliding mode observer (10)–(12), according to $\bar{x} = [x^T \ d^T]^T$ we can get the state and channel noise estimations as $\hat{x} = [I_n \ 0_{n \times l}] \hat{\bar{x}}$, $\hat{d} = [0_{l \times n} \ I_l] \hat{\bar{x}}$.

4 Chaos-Based Secure Communication

4.1 The Derivative Estimation of Drive Signal

In this section, a first-order robust exact differentiator is considered to exactly estimate the derivative of drive signal. Then, a method which can recover the information signal is developed.

Denote $y = \bar{C}\bar{x} = [y_1^T \ y_2^T \ \dots \ y_p^T]^T$, $y_i = \bar{C}_i\bar{x}$, where \bar{C}_i is the i th row of matrix \bar{C} . Differentiating y_i ($i = 1, 2, \dots, p$) with respect to time t , we have

$$\dot{y}_i = \bar{C}_i\dot{\bar{x}} = \bar{C}_iA\bar{x} + \bar{C}_iBf(K\bar{x}) + \bar{C}_i\bar{H}\varphi \tag{19}$$

If we introduce a new variable $y_{is} = \psi_i(\bar{x}, t) = \bar{C}_iA\bar{x} + \bar{C}_iBf(K\bar{x}) + \bar{C}_i\bar{H}\varphi$, and regard $y_{io} = y_i$ as the output equation, the system (19) can be expanded into

$$\dot{y}_i = y_{is}, \dot{y}_{is} = \psi_i, y_{io} = y_i \tag{20}$$

where ψ_i is unknown but bounded in norm by some known constant or known function of time because of Assumption 3.

In order to exactly estimate \dot{y}_i in a finite time, the following first-order robust exact differentiator is proposed based on the work in [11].

$$\begin{cases} \dot{\xi}_i = \alpha_{i1}, \alpha_{i1} = -\lambda_{i,1}|\xi_i - y_i|^{1/2}\text{sign}(\xi_i - y_i) + \xi_{is} \\ \dot{\xi}_{is} = -\lambda_{i,2}\text{sign}(\xi_{is} - \alpha_{i1}) \end{cases} \tag{21}$$

where $\lambda_{i,j} > 0$ ($j = 1, 2$) are the observer gains. If we denote $z_{i,0} = \xi_i - y_i$ and $z_{i,j} = \lambda_{i,j}|z_{i,j-1}|^{(2-j)/(3-j)}\text{sign}(z_{i,j-1})$, then (21) is equivalent to

$$\dot{\xi}_i = \xi_{is} - z_{i,1}, \dot{\xi}_{is} = -z_{i,2} \tag{22}$$

The error dynamic system between (20) and (22) is $\dot{e}_i = e_{is} - z_{i,1}$, $\dot{e}_{is} = -z_{i,2} - \dot{\psi}_i$, where $e_i = \xi_i - y_i$, $e_{is} = \xi_{is} - y_{is}$. Now by a similar way to [11], we can show that the sliding mode moving appears on the manifold $e_i = e_{is} = 0$ in a finite time by choosing $\lambda_{i,j}$ properly. So, the exact estimate of \dot{y}_i can be obtained as ξ_{is} . So, $\xi_s = [\xi_{1s} \ \cdots \ \xi_{ps}]^T$ is the estimate of $\dot{y} = [\dot{y}_1 \ \cdots \ \dot{y}_p]^T$ in a finite time.

4.2 The Chaos-Based Secure Communication Mechanism

The robust exact differentiator (21) together with the sliding mode observer (10) becomes the receiver. The recovery of S and η can be obtained in receiver end.

Theorem 2 *Under Assumption 1–4, we provide information signal recovery and disturbance estimation methods as follows*

$$\hat{\varphi} = (M^T M)^{-1} M^T [\xi_s - \bar{C} \bar{A} \hat{x} - \bar{C} \bar{B} f(K \hat{x})] \tag{23}$$

$$\hat{s} = [I_m \ 0_{m \times q} \ 0_{m \times l}] \hat{\varphi}, \quad \hat{\eta} = [0_{q \times m} \ I_q \ 0_{q \times l}] \hat{\varphi} \tag{24}$$

where $M = \bar{C} \bar{H}$. $\hat{\varphi}$ is the estimate of $\varphi = [s^T \ \eta^T \ v^T]^T$, so \hat{s} and $\hat{\eta}$ are the information signal recovery of S and disturbance vector η , respectively.

Proof According to (7), we have $M\varphi = \dot{y} - \bar{C} \bar{A} \bar{x} - \bar{C} \bar{B} f(K \bar{x})$. $M^T M$ is invertible because M is of full column rank. So

$$\varphi = (M^T M)^{-1} M^T [\dot{y} - \bar{C} \bar{A} \bar{x} - \bar{C} \bar{B} f(K \bar{x})] \tag{25}$$

The error equation between (23) and (25) is $\tilde{\varphi} = (M^T M)^{-1} M^T [\tilde{\xi}_s - \bar{C} \bar{A} \tilde{x} - \bar{C} \bar{B} \tilde{f}]$, where $\tilde{\varphi}(t) = \varphi(t) - \hat{\varphi}(t)$, $\tilde{\xi}_s(t) = \dot{y}(t) - \xi_s(t)$, $\tilde{x}(t) = \bar{x}(t) - \hat{x}(t)$, and $\tilde{f} = f(K \bar{x}) - f(K \hat{x})$. So we have $\lim_{t \rightarrow \infty} \tilde{\varphi}(t) = 0$ since $\lim_{t \rightarrow \infty} \tilde{\xi}_s = 0$, $\lim_{t \rightarrow \infty} \tilde{x} = 0$, and $\lim_{t \rightarrow \infty} \tilde{f}(t) = 0$.

5 Simulation

In order to demonstrate the effectiveness of the proposed scheme, a four-dimension hyperchaos system is given by [12]

$$\begin{cases} \dot{x}_1 = ax_1 - 1.2x_2 \\ \dot{x}_2 = 1.1x_1 - 0.1x_2x_3^2 \\ \dot{x}_3 = 0.65x_1 - 0.05x_2 - 1.2x_3 - 5x_4 \\ \dot{x}_4 = 0.1x_1 + 0.62x_3 + 0.8x_4 \end{cases} \tag{26}$$

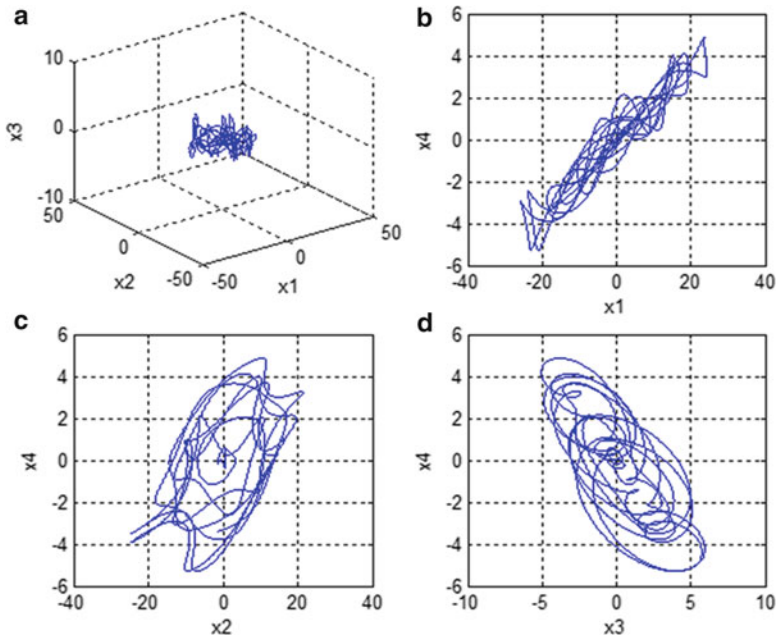


Fig. 1 The phase portraits of (26) with η and d

It is known that the system shows hyperchaos behavior if the parameter is chosen as $a = 0.58$. Suppose that the parameters a is affected by disturbance of $\eta = 0.02 \sin(t + 2.5)$, then the system with disturbance and injecting information signal can be written as in the form of (1) with

$$A = \begin{bmatrix} 0.58 & -1.2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0.65 & -0.05 & -1.2 & -5 \\ 0.1 & 0 & 1.62 & 0.8 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, D = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, C = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$E = [0 \ 0 \ 1]^T$ and the nonlinear term $f(x) = -0.1x_2x_3^2$, where $H = [B \ D]$. Let $A_d = -2$, according to (4) we can get $\bar{A}, \bar{B}, \bar{C}, \bar{D}, K$, and $\bar{H} = [\bar{B} \ \bar{D}]$. By Matlab's LMI toolbox, we can obtain $\bar{Q}, \bar{P}, \bar{L}$ and \bar{F} which can satisfy (6).

We set the information signal and additive noise as $s = 1.5 \cos(2t + 8.5)$ and $v = \cos(t + 4.5)$, respectively. Figure 1a is the project on the x_1, x_2 , and x_3 . Figure 1b, c are the projects on x_1-x_4 and x_2-x_4 , respectively, and Fig. 1d is the project on x_3-x_4 . We know that the chaotic properties are still kept even if the original chaotic system is suffering from some parameter deviation η and the unknown injecting information signal S .

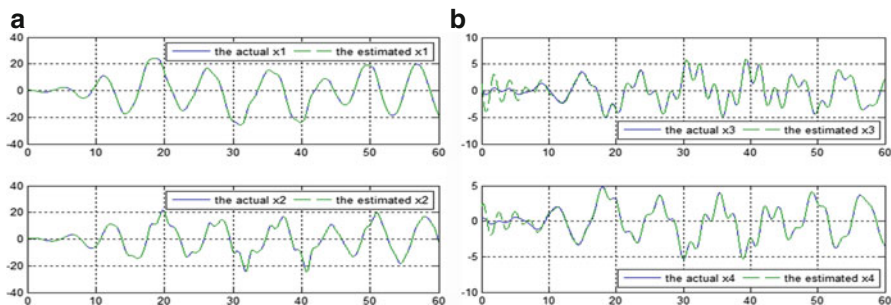


Fig. 2 The chaos synchronization for all states. (a) State estimation for x_1 and x_2 and (b) state estimation for x_3 and x_4

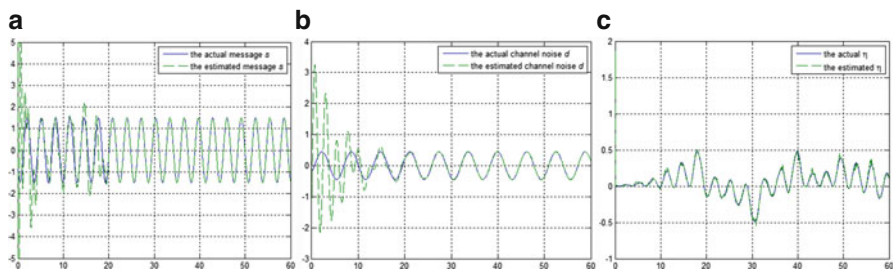


Fig. 3 Information recovery and estimates of channel noise and parameter disturbance. (a) Recovery of signal S , (b) the estimated d and (c) the estimated η

In the simulation, the initial values are set as $x(0) = [0.5 \ 0.3 \ 0.2 \ 0.4]^T$, $\hat{x}(0) = [0.2 \ 0.5 \ 1.2 \ 2.1]^T$, the state estimations can be obtained from Fig. 2, which shows that the performances of robust full-order observer are satisfactory.

The simulation for both information signal and the channel noise reconstruction performances are given in Fig. 3a, b, respectively. Figure 3c shows the estimation performances of disturbance. From Fig. 3, we know that the recovering and estimated effectiveness is good.

6 Conclusion

In this chapter, we discussed the problems of chaotic synchronization and chaos-based secure communication for a class of uncertain chaotic system with channel noise. An augmented system is formed based on an augmented vector. The combination of an adaptive robust sliding mode observer and a first-order robust exact

differentiator is regarded as the receiver. A novel information recovering method which can not only recover the information signal but also reconstruct the unknown parameter disturbance and channel noise is developed. The proposed method doesn't require constant information signal, so we just assume that the method and its derivative is bounded.

Acknowledgments This work was supported by the National Nature Science Foundation of China under Grant 61074009. This work is also supported by the Fundamental Research Funds for the Central Universities and supported by Shanghai Leading Academic Discipline Project under Grant B004.

References

1. Pecora LM, Carroll TL (1990) Synchronization in chaotic system. *Phys Rev Lett* 64:821–824
2. Huang T, Li C, Liao X (2007) Synchronization of a class of coupled chaotic delayed systems with parameter mismatch. *Chaos* 17:033121-5
3. Zhang W, Huang J, Wei P (2011) Weak synchronization of chaotic neural networks with parameter mismatch via periodically intermittent control. *Appl Math Model* 35:612–620
4. Zhu F (2008) Full-order and reduced-order observer-based synchronization for chaotic systems with unknown disturbances and parameters. *Phys Lett A* 372:223–232
5. Bowong S, Kakmeni FMM, Fotsin H (2006) A new adaptive observer-based synchronization scheme for private communication. *Phys Lett A* 355:193–201
6. Wang H, Zhu X, Gao S, Chen Z (2011) Singular observer approach for chaotic synchronization and private communication. *Commun Nonlinear Sci Numer Simulat* 16:1517–1523
7. Zhu F (2009) Observer-based synchronization of uncertain chaotic system and its application to secure communications. *Chaos Solitons Fractals* 40:2384–2391
8. Li K, Zhao M, Fu X (2009) Projective synchronization of driving-response systems and its application to secure communication. *IEEE Trans Circuits Syst* 56:2280–2291
9. Saif M, Guan Y (1993) A new approach to robust fault detection and identification. *IEEE Trans Aerosp Electron Syst* 29:685–695
10. Corless M, Tu J (1998) State and input estimation for a class of uncertain systems. *Automatica* 34:757–764
11. Levant A (2003) High-order sliding modes: differentiation and output-feedback control. *Int J Control* 76:924–941
12. Chen D, Chen H, Ma X, Long Y (2010) Hyperchaos system with only nonlinear term and comparative study of its chaotic control. *J Comput Appl* 30:2045–2048