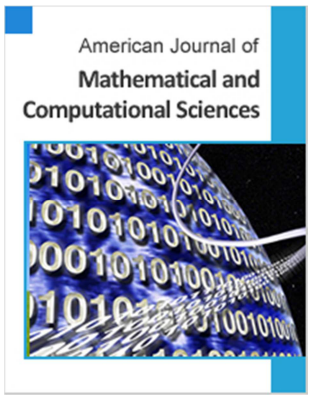
American Journal of Mathematical and Computational Sciences
2018; 3(1): 17-21
http://www.aascit.org/journal/ajmcs

American Association for Science and Technology



Keywords
Chaos Systems,
Secure Communication,
Adaptive Control

Received: July 27, 2017
Accepted: November 24, 2017
Published: January 16, 2018

Secure Communication Using Chaotic Synchronization

Yanjun Liang[1], Junqi Liang[2], Zhongsheng Wang[3]

[1]School of Computer and Information Engineering, Anyang Normal University, Anyang, China
[2]Shanghai Sunking Construction Management & Consulting Co, Ltd, Shanghai, China
[3]Department of Automation, Guangdong Polytechnic Normal University, Guangzhou, China

Email address
353572709@qq.com (Yanjun Liang)

Citation
Yanjun Liang, Junqi Liang, Zhongsheng Wang. Secure Communication Using Chaotic Synchronization. *American Journal of Mathematical and Computational Sciences*. Vol. 3, No. 1, 2018, pp. 17-21.

Abstract
Problem of chaotic synchronization for secure communication is studied. Partial state synchronization for a class of chaos systems with uncertain parameters is investigated. The different values of the uncertain parameters represent different chaos systems. Partial state variables synchronization control for the class of uncertain chaos systems is developed. In order to make certain state variables asymptotically stable and adaptive parameters identify the uncertain parameters, using partial state stability theory and adaptive control method, a Lyapunov function is constructed, partial state variables synchronization controller and adaptive regulator are designed for the class of uncertain chaos systems. Layapunov stability theory is employed in proving the theory correctness of the controller and regulators. Numerical simulation results illustrate the effectiveness of the proposed controller and adaptive regulators.

1. Introduction

Chaos is a unique form of nonlinear systems, and is an aperiodic motion form which exists widely in nonlinear systems. This motion form can find in almost every branch of natural science and social science.

In 1990, Pecora and Carroll realized synchronization of chaos [1], because chaotic synchronization has very broad application prospects in secure communications, signal processing and life sciences, and it has been one of the hottest research topics in nonlinear science over the past decade, and has aroused great attention and carried out extensive and in-depth research [2-3]. Because chaotic signal has characteristics such as aperiodicity, continuous broadband frequency spectrum, noise-like, very complex trajectory and unpredictability, the chaotic signal is very suitable as a carrier for secure communication. In recent years, chaos control theory has developed tremendously, and laid a theoretical foundation for chaotic secure communication, and lots of results have been achieved in the study of chaotic secure communication. A hybrid dislocated projective synchronization and secure communication scheme has been researched by Zhang and An in [4]. Mengue and Essimbi have studied the coupling of semiconductor laser chaotic secure communication scheme in [5]. Compound synchronization of four memristor chaotic oscillator systems and secure communication have been developed by Sun and Shen in [6]. Luo and Wang have studied finite-time stochastic combination synchronization of three different chaotic systems and its application in secure communication in [7]. Nguimdo and Colet have researched digital key for chaos communication performing time delay concealment in [8]. Role of chaos in quantum communication through a dynamical dephasing channel has been studied in [9] by Lemos and Benenti. Chaotic wireless

communication has been researched by Ren and Baptista in [10]. In addition, the chaotic secure communication of complex networks has also been greatly concerned in [11-12].

In this paper, partial state variables stabilization control for the class of uncertain chaos systems is developed for encryption communication. In order to make certain state variables asymptotically stable and adaptive parameters identify the uncertain parameters, using partial state stability theory and adaptive control method, a Lyapunov function is constructed, partial state variables stabilization controller and adaptive regulators are designed for a class of uncertain chaos systems. Our controller can guarantee the uniformly ultimate boundedness of the solution of the closed-loop system, and make the tracking error arbitrarily small for uncertain parameters. Numerical simulation results illustrate the effectiveness of the proposed controller and adaptive regulators.

2. System Structure

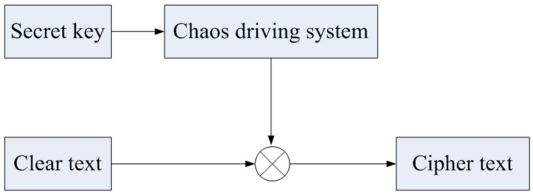


Figure 1. *Choas encryption system chart.*

The chart of chaos encryption communication system is shown in Figure 1, and it consists of secret key and clear text modules, chaos driving system and cipher text modules. The secret key is the input of chaos driving system, then do the operation of exclusive or with the clear text, and generate cipher text. The detail of chaos decode system is demonstrated by Figure 2, and it constitutes of the operation of exclusive or module, chaos response system module and uniformization module. This secure communication using chaotic synchronization is a security algorithm based on improved one-way sin ring iterative system. Using the improved lattice algorithm, it can generate the required pseudo-random sequence, the algorithm based on the initial function has good performance of anti-crack, and high security, high reliability, eliminates common drawbacks of bandwidth expansion, strong operability.

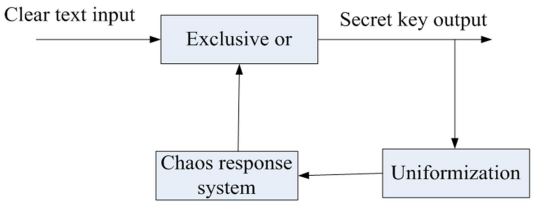


Figure 2. *Chaose decode system chart.*

3. Chaotic Encrypting and Synchronizing Module

Consider the following chaos systems

$$\dot{x}(t) = f(x) + F(x)\theta \tag{1}$$

where $x(t)$ is the state vector of the system, θ is the parameters vector of the system, and

$$\begin{aligned} &x \in R^n, \theta \in R^m, \\ &f = \mathrm{col}(f_1, f_2, \ldots f_m) \in C^1\left(R^n,\ R^n\right), \\ &F = (F_{ij})nm \in C^1\left(R^n,\ R^{nm}\right). \end{aligned} \tag{2}$$

Eq. (1) is the driving system which is used to drive the following response system:

$$\dot{z}(t) = f(z) + F(z)\alpha(t) \tag{3}$$

is synchronous with the drive system and the parameters $\alpha(t)$ can be regulated to parameters θ simultaneously, such that $\lim_{t\to+\infty} e(t) = 0$, $\lim_{t\to+\infty} \beta(t) = 0$, where $e(t) = z(t) - x(t)$ is defined as state error, and $\beta(t) = \alpha(t) - \theta$ is defined as parameter error.

Form (1) and (3), we have the error system

$$\dot{e}(t) = f(z) - f(x) + (F(z) - F(x))a(t) + F(x)\beta(t) + U(t) \tag{4}$$

Our control aim is to design appropriate controller to make partial state variables stable asymptotically, and regulator recognize the uncertain parameter θ.

4. Design of Controller and Adaptive Law

In order to design partial state variable controller for systems (4), we introduce two lemmas.

Consider differential equation

$$\dot{x} = f(t, x), \tag{5}$$

in which,

$$\begin{aligned} &f(t,x) \in C[I \times R^n, R^n], f(t,0) \equiv 0, \\ &x = col(y,z) = col(x_1, x_2, \ldots, x_m, x_{m+1}, x_{m+2}, \ldots, x_n) \in R^n, \\ &y = col(x_1, x_2, \ldots, x_m) \in R^m, \\ &z = col(x_{m+1}, x_{m+2}, \ldots, x_n) \in R^p, \\ &(m + p = n), \end{aligned}$$

$$\|x\| := (\sum_{i=1}^{n} x_i^2)^{1/2}, \|y\| := (\sum_{i=1}^{m} x_i^2)^{1/2},$$

$$\|z\| := (\sum_{i=m+1}^{n} x_i^2)^{1/2}.$$

Lemma 1 A necessary and sufficient condition of function $V(t, \boldsymbol{x}) \in C(I \times R^n, R)$, and $V(t,0) \equiv 0$ positive definite for

y is $\exists\phi(r)\in K$ in $\Omega=\{\|x\|\le H\}$ satisfying

$$V(t,\boldsymbol{x})\ge\varphi(\|y\|). \tag{6}$$

Proof The sufficiency is obvious, then we prove the necessity.

Let $\bar{\varphi}(r):=\inf\limits_{r\le\|x\|\le R}V(t,x)$, because $\varphi(r)$ is K function, we have $\bar{\varphi}(0)=0$, $\forall r>0$, $\bar{\varphi}(r)>0$, and it is monotone not decreasing function in $r\le R$.

Now, we prove $\bar{\varphi}(r)$ is continuous function. Because $V(t,x)$ is continuous function, $\forall\varepsilon>0$, $\exists\delta>0$, when $0\le r_2-r_1<\delta$, we have

$$\begin{aligned}\bar{\varphi}(r_2)-\bar{\varphi}(r_1)&=\inf_{r_2\le\|x\|\le R}V(t,x)-\inf_{r_1\le\|x\|\le R}V(t,x)\\&:=\inf_{r_2\le\|x\|\le R}V(t,x)-V(t,x_0)\\&\le V(t,x_1)-V(t,x_0)\\&<\varepsilon(\|x_1-x_0\|\le r_2-r_1<\delta),\end{aligned} \tag{7}$$

in which, when $x_0\in D_2=\{x\,|\,r_2\le\|x\|\le R\}$, we take $y=x_0$; when $x_0\in D_2=\{x\,|\,r_2\le\|x\|\le R\}$, take y as the point of intersection of half-lines Ox_0 and $\|x\|=r_2$, therefore $\bar{\varphi}(r)$ is continuous.

Let $\varphi(r):=\dfrac{r\bar{\varphi}(r)}{R}\le\bar{\varphi}(r)$, it is obvious that $\varphi(0)=0$, and when $0\le r_2<r_1\le R$, we have

$$\varphi(r_1)=\frac{r_1\bar{\varphi}(r_1)}{R}\le\frac{r_1\bar{\varphi}(r_2)}{R}<\frac{r_2\bar{\varphi}(r_2)}{R}=\varphi(r_2), \tag{8}$$

Therefore $\varphi(r)$ is strict monotone increasing function, and we have $\varphi\in K$, and

$$\varphi(\|y\|)\le\bar{\varphi}(\|x\|):=\inf_{\|x\|\le\xi\le R}V(t,\xi)\le V(t,x). \tag{9}$$

Lemma 2 If function $V(t,x)\in C(I\times R^n,R)$, and $V(t,\mathbf{0})\equiv 0$ satisfies (6), and its derivative makes $\dot{V}\big|_{(3)}\le-c(\|y\|)(c\in K)$, trivial solution of differential equations (5) is stable for y.

Proof It is easy to know that for each $t_0\ge 0$, there exists $\delta(t_0)>0$, and when $\|x_0\|<\delta(t_0)$, we have

$$\|y(t,t_0,x_0)\|<H(t\ge t_0). \tag{10}$$

Assume that $\lambda(t_0)<\sup\limits_{\|x_0\|<\delta}V(t_0,x)$, take

$$T(t_0,\varepsilon)=\lambda(t_0)/c(\varepsilon). \tag{11}$$

Now we prove that for $\forall\varepsilon\in(0,H),t_0\in I,\exists\delta(t_0)>0$ and $T(t_0,\varepsilon)>0$, and for $\forall x_0\in S_\delta=\{x\,|\,\|x\|<\delta\}$, there exists $t^*\in(t_0,t_0+T)$ making $\|y(t^*,t_0,x_0)\|<\varepsilon$. We use the proof by contradiction methord. If $\varepsilon\le\|y(t^*,t_0,x_0)\|<H$, when $t\in[t_0,t_0+T)$, from $\dot{V}\big|_{(3)}\le-c(\|y\|)(c\in K)$, we deduce that

$$\begin{aligned}0<\varphi(\varepsilon)&\le\varphi(\|y(t+T,t_0,x_0)\|\\&\le V(t+T,x(t+T,t_0,x_0))\\&\le V(t_0,x_0)-c(\varepsilon)T\\&=V(t_0,x_0)-\lambda(t_0)\le 0.\end{aligned} \tag{12}$$

It is not possible for (12), then we know that the conclusion is proved by the condition of the lemma and the dependency of solution to starting value. Therefore

$$\|y(t^*,t_0,x_0)\|<\varepsilon, \tag{13}$$

and it is proved for the lemma 2.

Next, we will design stabilization controller and adaptive regulator. We choose the controller in the following form

$$\begin{aligned}U(t)=&-\Gamma e(t)+f(x)-f(z)\\&+(F(x)-F(z))a(t)\end{aligned} \tag{14}$$

where Γ is any positive definite symmetric matrix. The regulating law of parameter error $\beta(t)$ takes the following form

$$\dot{\beta}(t)=-\lambda\beta(t)-F^{\mathrm{T}}(x)e(t) \tag{15}$$

Substituting (14) into the error system, we have the following error system and parameters identification system:

$$\begin{aligned}\dot{e}(t)&=-\Gamma e(t)+F(x)\beta(t),\\\dot{\beta}(t)&=F^{\mathrm{T}}x(t)e(t)-\lambda\beta(t)\end{aligned} \tag{16}$$

Then, we can get the following theorem.

Theorem 1 The closed-loop control systems (16) are stable asymptotically on effect of controller (14) and adaptive regulators (15).

Proof Take a Lyapunov function

$$V(t,x)=\frac{1}{2}(e^{\mathrm{T}}(t)e(t)+\beta^{\mathrm{T}}(t)\beta(t)), \tag{17}$$

we have

$$\begin{aligned}\left.\frac{dV}{dt}\right|_{(9)}&=e^{\mathrm{T}}(t)\dot{e}(t)+\beta^{\mathrm{T}}(t)\dot{\beta}(t)\\&=e^{\mathrm{T}}(t)[-\Gamma e(t)+F(x)\beta(t)]\\&+\beta^{\mathrm{T}}(t)[F^{\mathrm{T}}x(t)e(t)-\lambda(\alpha(t)-\theta)]\\&=-\Gamma e^{\mathrm{T}}(t)e(t)-\lambda\beta^{\mathrm{T}}(t)\beta(t)\end{aligned} \tag{18}$$

According lemma 2, the closed-loop control systems (16) are asymptotically stable for partial state variables and the adaptive regulator $\beta(t)$.

5. Numerical Simulations

In the study of chemical reaction with intermediate product, Rössler proposed the equations [15]

$$\begin{cases} \dot{x}_1 = -x_2 - x_3, \\ \dot{x}_2 = x_1 + ax_2, \\ \dot{x}_3 = b + x_3(x_1 - c), \end{cases} \tag{19}$$

in which x_1, x_2 and x_3 are state variables, $a, b, c \in R_+$ are uncertain parameters. When $a = b = 0.2$ and $c = 5.7$, it is a chaos system, and Figure 1 is its time response Figure.

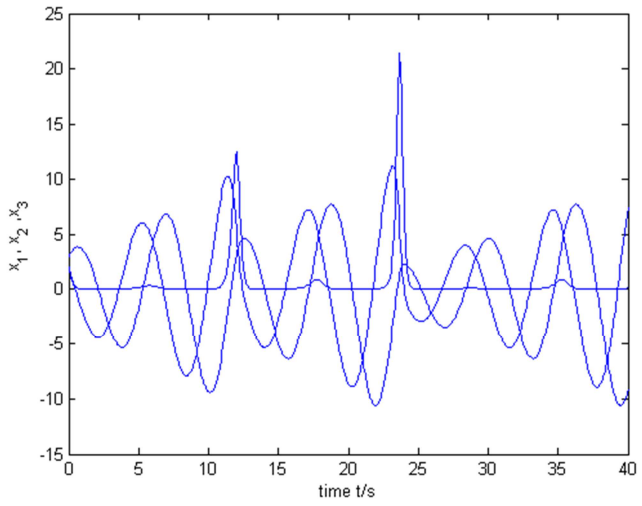


Figure 3. *Time response of Rössler systems*

In order to study the synchronization of the Rössler systems (1), the response systems are constructed as follows

$$\begin{cases} \dot{y}_1 = -y_2 - y_3 + u_1, \\ \dot{y}_2 = y_1 + a_1(t)y_2 + u_2, \\ \dot{y}_3 = b_1(t) + y_3(y_1 - c_1(t)). \end{cases} \tag{20}$$

Obviously, the response systems have the same structure as the drive systems (1), and the parameters $a_1(t), b_1(t), c_1(t) \in R_+$ are estimate for uncertain parameters a, b, c of the Rössler systems (1). In this paper, we study partial state variables stabilization control problem, and the parameter a is unknown, b, c known.

We can obtain the error systems from the drive systems (19) and the response systems (20), and they are as follows

$$\begin{cases} \dot{e}_1 = -e_2 - e_3 + u_1, \\ \dot{e}_2 = e_1 + a_1(t)y_2 - ax_2 + u_2, \\ \dot{e}_3 = b_1(t) - b + y_3y_1 - x_3x_1 - y_3c_1(t) + x_3c, \end{cases} \tag{21}$$

in which, $e_1 = y_1 - x_1$, $e_2 = y_2 - x_2$, $e_3 = y_3 - x_3$ are the errors of the state variables.

Our aim is to design appropriate controller to make partial state variables synchronization of the response systems (20) and the drive systems (19), namely, y_1 with x_1 and y_2 with x_2 synchronization, and recognized the uncertain parameter a, it is can also described as following

$$\begin{aligned} &\lim_{t\to\infty} e_1(t) = 0, \\ &\lim_{t\to\infty} e_2(t) = 0, \\ &\lim_{t\to\infty} \beta(t) = 0, \end{aligned} \tag{22}$$

in which, $\beta(t) = a(t) - a$ is parameter error.

In order to achieve the control aim (22), we design the controller and adaptive regulator as following

$$\begin{aligned} &u_1(t) = e_3(t) - e_1(t), \\ &u_2(t) = -(1 + a_1(t))e_2(t), \\ &\dot{\beta}(t) = -x_2(t)e_2(t), \end{aligned} \tag{23}$$

then, we have the theorem as follows

Theorem 2 The controllers and adaptive control laws described in (23) make the equations in (24) tenable.

$$\begin{aligned} &\lim_{t\to\infty} e_1(t) = 0, \\ &\lim_{t\to\infty} e_2(t) = 0, \\ &\lim_{t\to\infty} \beta(t) = 0, \end{aligned} \tag{24}$$

Proof Take a Lyapunov function

$$V(t,x) = \frac{1}{2}e_1^{\,2}(t) + \frac{1}{2}e_2^{\,2}(t) + \frac{1}{2}\beta^2(t) \tag{25}$$

for the error systems (3). According lemma 1, it is positive definite for $e_1(t)$ and $e_2(t)$, and its derivative along the error systems (3) is as follows

$$\begin{aligned} \frac{dV}{dt} &= e_1(t)\dot{e}_1(t) + e_2(t)\dot{e}_2(t) + \beta(t)\dot{\beta}(t) \\ &= e_1(t)(-e_2(t) - e_3(t) + u_1(t)) + (a_1(t) - a)\dot{a}_1(t) \\ &\quad + e_2(t)(e_1(t) + a_1(t)y_2(t) - ax_2(t) + u_2(t)) \\ &= -e_1(t)e_2(t) - e_1(t)e_3(t) + u_1(t)e_1(t) + \\ &\quad e_1(t)e_2(t) + a_1(t)y_2(t)e_2(t) - ax_2(t)e_2(t) + \\ &\quad u_2(t)e_2(t) + (a_1(t) + a)\dot{a}_1(t) \\ &= -e_1(t)e_3(t) + u_1(t)e_1(t) + a_1(t)y_2(t)e_2(t) - \\ &\quad ax_2(t)e_2(t) + u_2(t)e_2(t) + \\ &\quad (a_1(t) + a)(-x_2(t)e_2(t)) \\ &= -e_1(t)e_3(t) + (e_3(t) - e_1(t))e_1(t) + \\ &\quad a_1(t)y_2(t)e_2(t) - ax_2(t)e_2(t) + \\ &\quad (-(1 + a_1(t))e_2(t))e_2(t) + \\ &\quad (a_1(t) + a)(-x_2(t)e_2(t)) \\ &= -e_1^{\,2}(t) - e_2^{\,2}(t) \\ &\le 0 \end{aligned}$$

According lemma 2, the error systems (3) are asymptotically stable for errors $e_1(t)$, $e_2(t)$ and the adaptive regulator $\beta(t)$.

In order to further check the effectiveness of the controller and adaptive control laws described in (7), we use Matlab software to simulate the result of the control systems (3) with the effect of the controller and adaptive control laws. The results are shown in Figure 2, in which the parameters and the state variables are chosen as $a = 0.2$, $y(0) = (-5, -4, -4)$, $a_1(0) = 0.01$, $x(0) = (2, 3, 2)$.

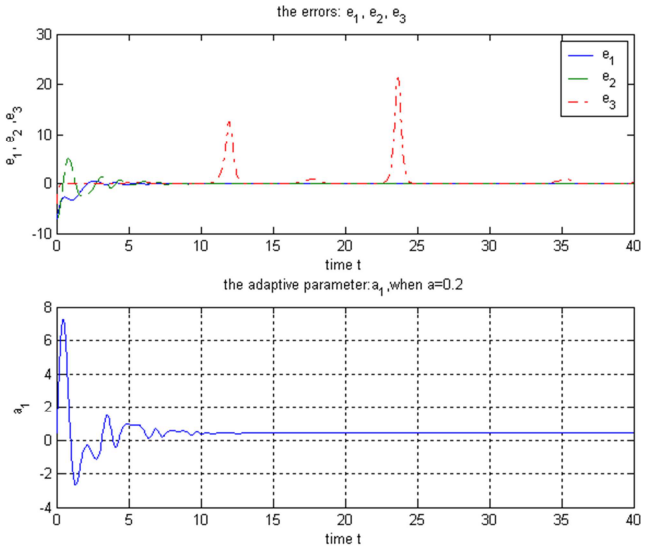


Figure 4. *The control curves.*

Figure 4 is the control curves of the state variable errors e_1, e_2 and e_3, from which we can see that the state variables e_1, e_2 have very good asymptotically stability with the effect of the controller and adaptive control laws, and $a_1(t)$ can respectively recognize the values of uncertain parameters a, and have very good real-time trait and strong robustness.

6. Conclusions

In this paper, partial state control theory is applied to secure communication. Because of inaccuracy generated by system modeling, parameter measurement and model linearization in practical application, it is inevitable that controlled system is affected by inaccuracy facts in engineering. One is interested in partial state variables of some practical problems in control engineering, and some state variables cannot be controlled or measured. On account of these conditions, the problem of partial state variables stabilization control for a class of uncertain chaos systems is studied. Using partial state stability theory and adaptive control method, partial state variables stabilization controller and adaptive regulators are designed, and numerical simulation results illustrate the effectiveness.

Acknowledgements

This work was supported in part by the Natural Science Foundations of China (61074092) and Henan Province Education Department Natural Science Foundations of China (12A120001 and 12A520003).

References

[1] L. M. Pecora, T. L. Carroll. Synchronization in chaotic system. Physical Review Letters, 1990, 64 (8): 821–824.

[2] G. Chen, X. Dong. From Chaos to Order. Singapore: WordScientific, 1998.

[3] E. Ott, C. Grebogi, JA Yorke. Controlling chaos. Physical Review Letters, 1990, 64 (11): 1196–1199.

[4] L. F. Zhang, X. L. An, J G Zhang. A new chaos synchronization scheme and its application to secure communications. Nonlinear Dynamics, 2013, 73 (1/2): 705-722.

[5] A. D. Mengue, B. Z. Essimbi. Secure communication using chaotic synchronization in mutually coupled semiconductor lasers. Nonlinear Dynamics, 2012, 70 (2): 1241-1253.

[6] J. W. Sun, Y. Shen, Q. Yin, et al. Compound synchronization of four memristor chaotic oscillator systems and secure communication. Chaos, 2013, 23 (1): 013140.

[7] R. Z. Luo, Y. L. Wang. Finite-time stochastic combination synchronization of three different chaotic systems and its application in secure communication. Chaos, 2012, 22 (2): 023109.

[8] R. M. Nguimdo, P. Colet, L. Larger, et al. Digital key for chaos communication performing time delay concealment. Physical Review Letters, 2011, 107 (3): 034103.

[9] G. B. Lemos, G. Benenti. Role of chaos in quantum communication through a dynamical dephasing channel. Physical Review A, 2010, 81 (6): 062331.

[10] H. P. Ren, S. P. Baptista, C. Grebogi. Wireless communication with chaos. Physical Review Letters, 2013, 110 (18): 184101.

[11] J. Zhou, L. Xiang, Z. R. Liu. Global synchronization in general complex delayed dynamical networks and its applications. Physica A: Statistical Mechanics and its Applications, 2007, 385 (2): 728-742.

[12] J. Zhou, T. Chen, L. Xiang. Chaotic lag synchronization of coupled delayed neural networks and its applications in secure communication. Circuits, Systems, and Signal Processing, 2005, 24 (5): 599-613.