Asian Journal of Control, Vol. 15, No. 6, pp. 1686–1699, November 2013
Published online 22 May 2013 in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/asjc.728

INTERMITTENT IMPULSIVE SYNCHRONIZATION OF HYPERCHAOS WITH APPLICATION TO SECURE COMMUNICATION

Hongtao Zhang, Xinzhi Liu, Xuemin (Sherman) Shen, and Jun Liu

ABSTRACT

In this paper, a hyperchaotic system is presented as the chaotic carrier to encrypt information in secure communication. The sensitivity to the system parameters and delay of the hyperchaotic system, *i.e.*, its chaotic degree indicated by the number of positive Lyapunov exponents, increases with its system parameter and delay, guaranteeing a large enough key space when one selects its system parameter and delay as the secret key. Furthermore, we develop an intermittent impulsive synchronization scheme (IISS) to achieve chaos synchronization, a crucial process in chaos-based secure communication. In our scheme, impulsive control is only activated in the control windows, not during the whole time, which breaks through the limitation on the upper bound of the impulsive intervals in the general impulsive synchronization scheme (GISS). Specifically, IISS improves the security of the chaos-based secure communication scheme since the encrypted signal (cipher) is transmitted in the free windows, different from the synchronization signal in the control windows. Finally, a secure communication scheme employing our hyperchaotic system and IISS technique is proposed and numerical results are given to demonstrate the performance of this scheme.

Key Words: chaos synchronization, intermittent impulsive control, secure communication, Hopf bifurcation, cryptography.

I. INTRODUCTION

Hyperchaos has attracted a great deal of attention from scholars over the past two decades due to its potential application to secure communication [1,4,5,8,9,11,13,19,25,35] and references therein. Hyperchaotic signal with extreme sensitivity to initial conditions and noise-like dynamics is a natural carrier utilized to mask information in cryptography. Accordingly, how to generate hyperchaotic systems becomes an active issue. Recently, some new multi-scroll attractors and hyperchaotic systems have been presented in [7,17,20–22,28–31,33,34]. Specifically, the delay differential equation (DDE) has been used to generate chaos since the discovery of the Mackey-Glass system, a physiological model that possesses chaotic behaviors. A few modified versions have been reported [29,31], in which a piecewise nonlinearity is utilized to substitute the original nonlinearity of the Mackey-Glass system. Most recently, Yalçin and Özoguz [34] presented a new DDE model to generate chaos and, employing a hard limiter series, generalized it to three- , four-, and five-scroll chaotic attractors. This system only possesses one positive Lyapunov exponent, and is not hyperchaotic. Sprott [28] found the simplest DDE for generating chaos, which is hyperchaotic, but unbounded. Because of its simple mathematical structure and abundant dynamical behaviors, DDE is a potential candidate as the chaos generator in chaos-based secure communication. Motivated by this, we construct a family of novel chaotic/hyperchaotic systems from DDE. Different from the above systems, our systems are bounded and very sensitive to their parameter and delay, *i.e.*, their chaotic degree, indicated by the number of their positive Lyapunov exponents, is directly controlled by their parameter and delay. On keeping the system structure fixed, via parameter and delay control, one can obtain various hyperchaotic attractors with a desired number of positive Lyapunov exponents. This property makes them a natural choice for secure communication. According to Kerckhoffs's principle, a cryptosystem should be secure even if everything about this system, except the secrete key, is public knowledge. In the scheme based on our attractors, one can keep the parameter and delay secret as the key. Even though the system structure of our attractors is known to the eavesdropper, he still can not discover the chaos generator employed because of the sensitivity.

Chaos synchronization plays a critical role in chaos-based secure communication, where the plain-text is encrypted by the chaotic signal at the transmitter, and then the cipher-text is transmitted to the receiver across a public channel (unsafe channel). At the receiver, chaos synchronization is usually expected to recover the plain-text, *i.e.*, the decryption of the cipher-text requires the receiver's own copy

Manuscript received January 15, 2012; revised January 28, 2013; accepted March 17, 2013.

H. Zhang and X. Shen are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.

X. Liu (corresponding author, e-mail: xzliu@math.uwaterloo.ca) is with Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.

J. Liu is with Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield S1 3JD, United Kingdom.

of the chaotic signal which is synchronized with that of the transmitter. Since the introduction of synchronizing two identical chaotic systems with different initial conditions by Pecora and Carroll in 1990 [25], a variety of synchronization techniques have been rapidly developed, including active control between two Lorenz systems [2], a backstepping approach between two Genesio systems [24], adaptive control [26], delay feedback synchronization [3,16], a variable structure method [12], a sliding model control [36], nonlinear feedback control [23], and intermittent feedback control [32]. Different from continuous feedback control, impulsive synchronization only requires small synchronizing impulses. These impulses are sampled from the state variables of the master system (the drive system) at discrete moments and then drive the slave system (the response system) at the same time. When the attractivity of the error system between the master and the slave systems is achieved, impulsive synchronization is said to have been realized. A generalization of impulsive synchronization with time-varying impulse intervals is investigated in [18]. Impulsive synchronization subject to delay and uncertain systems has been studied in [15]. The robustness of impulsive synchronization coupled by linear delayed impulses has been discussed in [14].

Impulsive synchronization technology has a good perspective in practice because of redundancy reduction of the synchronization signal, compared to continuous feedback control. However, there exists a restriction to limit its wide application, which is the upper bound on impulsive intervals (the time intervals between the impulses) during the synchronization process [35]. Usually, the impulsive intervals are small, *i.e.*, the impulsive controller at the receiver needs to be activated frequently. In some scenarios such as the orbital transfer of a satellite, control of money supply in a financial market, *etc.*, the control windows (the time periods the controller can work) are strictly restricted. Once the free windows (the time periods the controller can not activate) are larger than the upper bound of the impulsive intervals, GISS will not function normally any more. To adress this problem, we propose IISS to replace GISS and establish corresponding synchronization criteria to achieve chaos synchronization, based on the method of linear matrix inequalities (LMI) and the Lyapunov-Razumikhin theory. In our synchronization scheme, the impulsive controller is only activated in the control windows, not during the entire time. This property also provides a way to improve the security of chaos-based secure communication schemes since one can separately transmit the encrypted signal in free windows and the synchronization signal in control windows, to avoid that the eavesdropper derives the chaotic signal used to encrypt the plain-text from the synchronization signal. To the best of our knowledge, there is no existing work studying this challenging problem. Our analytic results may be used as a guideline for some engineering applications.

The remainder of this paper is organized as follows. In Section II, some basic definitions, assumptions, and lemmas are introduced. In Section III, a family of novel hyperchaotic attractors are constructed, which are sensitive to their parameter and delay. In Section IV, synchronization criteria are established, based on Lyapunov-Razumikhin theory and LMI. In Section V, a numerical example is given to demonstrate the effectiveness of our synchronization results. In section VI, a secure communication system, employing our hyperchaotic systems and IISS technique, is proposed and a numerical simulation exhibits its good security performance. Finally, conclusions are given in Section VII.

II. PRELIMINARIES

In this section, we introduce some definitions, assumptions and preliminary lemmas, which will be used in the proofs of later synchronization theorems. Let R denote the set of real numbers, R_+ the set of nonnegative real numbers and R^n the n-dimensional Euclidean linear space equipped with the Euclidean norm $\|\cdot\|$. Throughout this paper, $P > 0$ (<0, ≤ 0, ≥ 0) denotes a symmetrical positive (negative, semi-negative, semi-positive) definite matrix P, P^T the transpose of P and $\lambda_{M(m)}(P)$ the maximum (minimum) eigenvalue of P. Let $\varphi(t^+) = \lim_{s \overrightarrow{>} t^+} \varphi(s)$, $\varphi(t^-) = \lim_{s \overrightarrow{<} t^-} \varphi(s)$ and $\varphi(t) = \varphi(t^+)$.

Let $a, b \in R$ with $a < b$ and $S \subset R^n$. Define $PC([a, b], R^n) = \{\varphi : [a, b] \to S | \varphi(t^+) = \varphi(t),\ \forall t \in [a, b);\ \varphi(t^-)$ exists in $S,\ \forall t \in (a, b]$ and $\varphi(t^-) = \varphi(t)$ for all but at most a finite number of points $t \in (a, b]\}$.

For $\tau > 0$, we equip the linear space $PC([-\tau, 0], R^n)$ with the norm $\|\cdot\|_\tau$ defined by $\|\varphi\|_\tau = \sup_{-\tau \leq S \leq 0} \|\varphi(s)\|$. Throughout this paper, we assume that $f(t)$, $(i = 1, 2, \ldots, n)$ satisfies the Lipschitz condition, *i.e.*,

H1. There exists a positive constant L such that

$$\|f(x) - f(y)\| \leq L\|x - y\|, \text{ for all } x, y \in R^n.$$

Chaos Synchronization. Let $x(t)$ and $y(t)$ be the solutions of the master system and the corresponding slave system, respectively. If $\lim_{t \to \infty} \|x(t) - y(t)\| = 0$, then it is said that the slave system is synchronized with the master system. Obviously, from the definition of synchronization, if the solution of the error system $e(t) = x(t) - y(t)$ satisfies $\lim_{t \to +\infty} \|e(t)\| = 0$, then chaos synchronization is achieved.

Lemma 1 [27]**.** For any vectors $x,\ y \in R^n$ and positive constant ξ, the following matrix inequality holds: $2x^T y \leq \xi x^T x + \frac{1}{\xi} y^T y$.

Lemma 2 [10]**.** Suppose that function $y(t)$ is nonnegative when $t \in (-\tau, \infty)$ and satisfies

$$\frac{dy(t)}{dt} \le k_1 y(t) + k_2 y(t-\tau), \quad t \ge 0,$$

where k_1 and k_2 are non-negative constants. Then, we have

$$y(t) \le \|y(0)\|_\tau e^{(k_1+k_2)t}, \quad t \ge 0.$$

Lemma 3. Let $\tau > 0$ and $V(t) \in C^1[J, R_+]$, where $J = [a - \tau, b)$, $0 < b - a \le \Delta$. Suppose that there exist constants $l > 0$ and $\beta \in (0, 1)$ such that

$$V'(t) \le lV(t), \text{ whenever } V(t) \ge \beta V(t+s), s \in [-\tau, 0]; \quad (1)$$

and there exists constant $\eta > 0$ such that $V(s) \le \eta$, $s \in [a - \tau, a)$, $V(a) \le \beta\eta$, and

$$l\Delta + \ln\beta < 0. \quad (2)$$

Then there exists d, $(\exp\{l\Delta + ln\beta\} < d < 1)$, such that $V(t) < d\eta$ for $t \in [a, b)$.

Proof. Suppose that, for the sake of contradiction, there exists a $t^* > a$ such that $V(t^*) = d\eta$ and $V(t) < d\eta$, $t \in [a, t^*)$. Let $t_0 = \sup\{t \in [a, t^*], V(t) \le \beta\eta\}$. Then $V(t_0) = \beta\eta$ and $\beta\eta \le V(t) \le d\eta$, $t \in [t_0, t^*]$. Thus for $t \in [t_0, t^*]$, we have

$$\beta V(t+s) \le \beta\eta \le V(t), s \in [-\tau, 0],$$

which implies, by (1), $V'(t) \le lV(t)$, $t \in [t_0, t^*]$. Integrating from t_0 to t^* gives

$$\ln(V(t^*)) - \ln(V(t_0)) \le l(t^* - t_0) \le l\Delta.$$

Let $d = \exp\{\frac{1}{2}(l\Delta + \ln\beta)\}$. On the other hand, in terms of (2), we have

$$\ln(V(t^*)) - \ln(V(t_0)) = \ln(d\eta) - \ln(\beta\eta) = \ln d - \ln\beta$$
$$= \frac{1}{2}(l\Delta + \ln\beta) - \ln\beta > (l\Delta + \ln\beta) - \ln\beta = l\Delta,$$

which is a contradiction. Thus the lemma is proved.

Remark 1. The condition (1) of Lemma 3 is used in the contradiction argument in the proof, *i.e.*, if the conclusion of Lemma 3 was not true, then we would have this condition $V(t) \ge \beta V(t+s)$, $s \in [-\tau, 0]$ satisfied for $t \in [t_0, t^*]$, and consequently we arrive at a contradiction. In other words, $V'(t) \le lV(t)$ is necessary only when $V(t) \ge \beta V(t+s)$, for all $s \in [-\tau, 0]$. If there exists some $s^* \in [-\tau, 0]$ such that $V(t) < \beta V(t+s^*)$ at time t, then $V'(t) \le lV(t)$ is not required in Lemma 3.

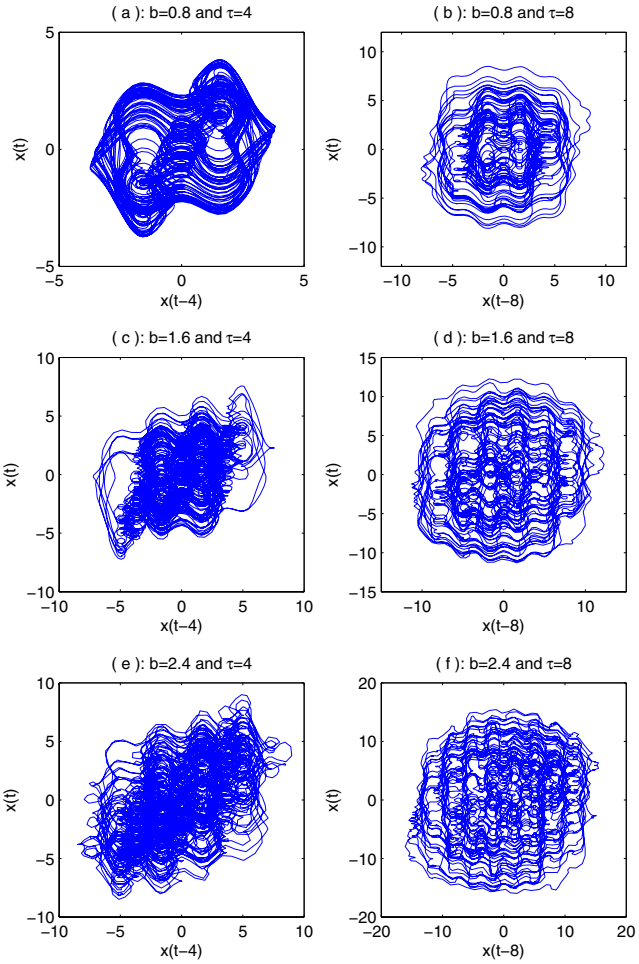


Fig. 1. The phase portraits of $x(t-\tau) - x(t)$ when (a) $b = 0.8$ and $\tau = 4$, (b) $b = 0.8$ and $\tau = 8$, (c) $b = 1.6$ and $\tau = 4$, (d) $b = 1.6$ and $\tau = 8$, (e) $b = 2.4$ and $\tau = 4$, and (f) $b = 2.4$ and $\tau = 8$.

III. HYPERCHAOTIC ATTRACTORS

DDE is a potential candidate as chaos generator in engineering applications because of its simple structure with abundant dynamical behaviors. We consider the following equation [37]:

$$\dot{x}(t) = -ax(t-\tau) + b\sin(cx(t-\tau)), \quad (3)$$

where a, b and c are constants, and $\tau > 0$ is delay. Fix $a = 0.16$ and $c = 1.8$, and let b and τ be variable. Fig. 1 shows the phase portraits of (3). b and τ increase their chaotic degree, indicated by the number of positive Lyapunov exponents.

Since more than one positive Lyapunov exponent usually taken as an indication of hyperchaos (provided the system is bounded), we calculate the positive Lyapunov exponents and Lyapunov dimensions using the method in [6] and the MATLAB LET toolbox.

For $b = 0.8$, (3) has seven equilibrium points (0, ± 1.5681, ± 4.0071, ± 4.5899). Hopf bifurcation occurs at four points (± 1.5681, ± 4.5899). The system has one positive Lyapunov exponent $\lambda = 0.0493$ and Lyapunov dimension $d = 3.1035$ when $\tau = 4.0$; and two positive Lyapunov exponents $\lambda_1 = 0.0718$, $\lambda_2 = 0.0189$ and Lyapunov dimension $d = 5.0807$ when $\tau = 8.0$. For $b = 1.6$, (3) has eleven equilibrium points (0, ± 1.6531, ± 3.7013, ± 4.9484, ± 7.4481, ± 8.1932). Hopf bifurcation occurs at six points (± 1.6531, ± 4.9484, ± 8.1932). The system has two positive Lyapunov exponents $\lambda_1 = 0.0795$, $\lambda_2 = 0.0319$ and Lyapunov dimension $d = 5.4147$ when $\tau = 4.0$; and four positive Lyapunov exponents $\lambda_1 = 0.1061$, $\lambda_2 = 0.0705$, $\lambda_3 = 0.0339$, $\lambda_4 = 0.0078$ and Lyapunov dimension $d = 10.0316$ when $\tau = 8.0$. For $b = 2.4$, (3) has fourteen equilibrium points (0, ± 1.6786, ± 3.6366, ± 5.0317, ± 7.2854, ± 8.3706, ± 10.9723, ± 11.6698). Hopf bifurcation occurs at eight points (± 1.6786, ± 5.0317, ± 8.3706, ± 11.6698). The system has three positive Lyapunov exponents $\lambda_1 = 0.0925$, $\lambda_2 = 0.0593$, $\lambda_3 = 0.0259$ and Lyapunov dimension $d = 7.8487$ when $\tau = 4.0$; and six positive Lyapunov exponents $\lambda_1 = 0.1210$, $\lambda_2 = 0.0927$, $\lambda_3 = 0.0634$, $\lambda_4 = 0.0410$, $\lambda_5 = 0.0191$, $\lambda_6 = 0.0067$ and Lyapunov dimension $d = 14.8941$ when $\tau = 8.0$.

Remark 2. The dynamics of (3) are sensitive to parameter b and delay τ. The chaotic degree of the hyperchaotic attractors increases with b and τ increasing. It can also be observed that the number of Hopf bifurcation points has a close relationship with the chaotic degree. By increasing b, we can increase the number of Hopf bifurcation points of (3). Therefore, we can achieve hyperchaos with more positive Lyapunov exponents and higher Lyapunov dimension.

IV. SYNCHRONIZATION CRITERIA

In this section, based on the Lyapunov-Razumikhin theorem and LMI approach, we derive synchronization criteria via general impulsive control and intermittent impulsive control, respectively.

4.1 Problem formulation

First, we present impulsive synchronization schemes including GISS and IISS. Consider a class of general DDEs as the master system (drive system), described by

$$\begin{cases} \dfrac{dx(t)}{dt} = Ax(t) + Bx(t-\tau) + Cf(x(t-\tau)), & t > 0, \\ x(t) = \phi, & -\tau \le t \le 0, \end{cases} \tag{4}$$

where $x(t) \in R^n$ is the state variable, A, B and C are $n \times n$ constant matrices, $f: R^n \to R^n$ is continuous nonlinear function satisfying $f(0) = 0$, τ is the delay, and $\phi \in PC([-\tau, 0], R^n)$ are the initial conditions.

4.1.1 General Impulsive Synchronization Scheme (GISS)

In GISS, the corresponding slave system (response system) is designed by

$$\begin{cases} \dfrac{dy(t)}{dt} = Ay(t) + By(t-\tau) + Cf(y(t-\tau)), & t \ne T_k, \\ \Delta y(t) = U_k(x(t), y(t)), & t = T_k, \end{cases} \tag{5}$$

where T_k ($k = 1, 2, \ldots$) is the kth impulsive instant satisfying $0 = T_1 < T_2 < \ldots < T_i < \ldots$ with $\lim_{k\to\infty} T_k = \infty$ and $U_k(x(t)) = B_k(x(t) - y(t))$ is the impulsive control at the k-th impulsive instant. $\{T_k, U_k\}$ is called the impulsive control law and define the impulsive interval $\Delta_k = T_{k+1} - T_k$. The initial conditions of (5) are given by

$$y(t) = \psi(t), \quad -\tau \le t \le 0,$$

where $\psi \in PC([-\tau, 0], R^n)$.

Let $e(t) = x(t) - y(t)$. The error system is given by

$$\begin{cases} \dfrac{de(t)}{dt} = Ae(t) + Be(t-\tau) + C\tilde{f}(t-\tau), & t \ne T_k, \\ \Delta e(t) = -B_k e(t), & t = T_k, \end{cases} \tag{6}$$

where $\tilde{f}(t) = f(x(t)) - f(y(t))$.

4.1.2 Intermittent Impulsive Synchronization Scheme (IISS)

In our intermittent impulsive synchronization scheme, impulsive control is only activated in control windows, not during the whole time. Define free windows $[m\omega, m\omega + \delta]$ and control windows $[m\omega + \delta, (m+1)\omega]$ where $m = 0, 1, \ldots$ and $0 < \delta < \omega < \infty$. The corresponding slave system (response system) is designed as follows:

$$\begin{cases} \dfrac{dy(t)}{dt} = Ay(t) + By(t-\tau) + Cf(y(t-\tau)), \\ \quad t \in [m\omega, m\omega + \delta), \\ \begin{cases} \dfrac{dy(t)}{dt} = Ay(t) + By(t-\tau) + Cf(y(t-\tau)), & t \ne T_{m,l}, \\ \Delta y(t) = U_{m,l}(x(t), y(t)), & t = T_{m,l}, \end{cases} \\ \quad t \in [m\omega + \delta, (m+1)\omega), \end{cases} \tag{7}$$

where $m = 0, 1, \ldots$, $l = 1, 2, \ldots, M_m$, M_m is a positive integer related to m, $T_{m,l}$ denotes the lth impulsive instant in the $m+1$-th control window, $m\omega + \delta = T_{m,1} < T_{m,2} < \ldots < T_{m,M_m} \le (k+1)\omega$, and $U_{m,l}(x(t), y(t)) = B_{m,l}(x(t) - y(t))$ is the impulsive control. $\{T_{m,l}, U_{m,l}\}$ is

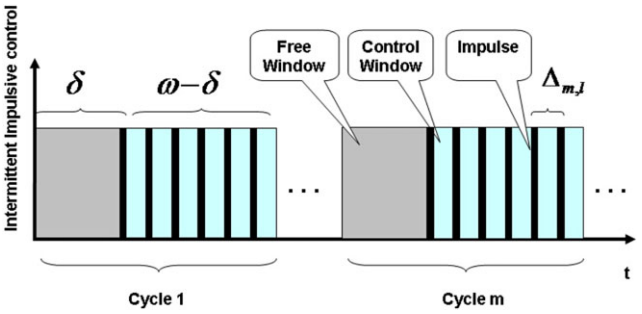


Fig. 2. The principle diagram of IISS.

called the intermittent impulsive control law. Let $T_{m,M_m+1} = (m+1)\omega$ and define the impulsive interval $\Delta_{m,l} = T_{m,l+1} - T_{m,l}$. The principle diagram of IISS is shown in Fig. 2.

Let $e(t) = x(t) - y(t)$. Also, we obtain the following error system:

$$\begin{cases} \dfrac{de(t)}{dt} = Ae(t) + Be(t-\tau) + C\tilde{f}(t-\tau), t \in [m\omega, m\omega+\delta), \\ \begin{cases} \dfrac{de(t)}{dt} = Ae(t) + Be(t-\tau) + C\tilde{f}(t-\tau), t \neq T_{m,l}, \\ \Delta e(t) = -B_{m,l}e(t), t = T_{m,l}, t \in [m\omega+\delta, (m+1)\omega), \end{cases} \end{cases} \tag{8}$$

where $\tilde{f}(t) = f(x(t)) - f(y(t))$.

4.2 General impulsive synchronization criterion

Theorem 1. In GISS, suppose that for an impulsive control law $\{T_k, U_k\}$:

(i) there exist a positive definite matrix P and constants $\alpha_1 > 0$, $\alpha_2 > 0$ and $\xi > 0$ such that

$$\begin{bmatrix} A^TP + PA + \xi PCC^TP - \alpha_1 P & PB \\ B^TP & \dfrac{L^2}{\xi} I - \alpha_2 P \end{bmatrix} \leq 0; \tag{9}$$

(ii) there exists a real number $\beta \in (0, 1)$ such that

$$(I - B_k^T)P(I - B_k) - \beta P \leq 0; \tag{10}$$

(iii) there exists a positive number Δ ($\Delta \geq \Delta_k$) such that

$$\frac{\Delta}{\beta}(\beta\alpha_1 + \alpha_2) + \ln\beta < 0, \tag{11}$$

where $\Delta_k = T_{k+1} - T_k$.

Then the slave system (5) can be synchronized with the master system (4) by the impulsive control law $\{T_k, U_k\}$.

Proof. Define $V(t) = e(t)^T Pe(t)$. For $t \in (T_k, T_{k+1})$, we have

$$\begin{aligned} V'(t) &= \dot{e}(t)^T Pe(t) + e(t)^T P\dot{e}(t) \\ &= 2e(t)^T PAe(t) + 2e(t)^T PBe(t-\tau) \\ &\quad + 2e(t)^T PC\tilde{f}(t-\tau) \end{aligned} \tag{12}$$

In terms of Lemma 1 and H1, we obtain

$$\begin{aligned} V'(t) &\leq e(t)^T(PA + A^TP)e(t) + 2e(t)^T PBe(t-\tau) \\ &\quad + \xi e(t)^T PCC^TPe(t) + \frac{1}{\xi}\tilde{f}(t-\tau)^T\tilde{f}(t-\tau) \\ &\leq e(t)^T(PA + A^TP + \xi PCC^TP)e(t) \\ &\quad + 2e(t)^T PBe(t-\tau) + \frac{L^2}{\xi}e(t-\tau)^Te(t-\tau) \\ &= \zeta^T \begin{bmatrix} A^TP + PA + \xi PCC^TP - \alpha_1 P & PB \\ B^TP & \dfrac{L^2}{\xi} I - \alpha_2 P \end{bmatrix} \zeta \\ &\quad + \alpha_1 V(t) + \alpha_2 V(t-\tau), \end{aligned} \tag{13}$$

where $\xi = [e(t)\ e(t-\tau)]^T$.

By condition (i), we have

$$V'(t) \leq \alpha_1 V(t) + \alpha_2 V(t-\tau), \tag{14}$$

which implies, if $V(t) \geq \beta V(t+s)$, $s \in [-\tau, 0]$, then

$$V'(t) \leq \frac{1}{\beta}(\beta\alpha_1 + \alpha_2)V(t). \tag{15}$$

When $t = T_k$, we get, by condition (ii)

$$\begin{aligned} V(T_k) &= e^T(T_k^-)(I - B_k)^T P(I - B_k)e(T_k^-) \\ &\leq \beta e^T(T_k^-)Pe(T_k^-) = \beta V(T_k^-) \leq \beta\|V(T_k)\|_\tau, \end{aligned} \tag{16}$$

where $\|V(T_k)\|_\tau = \sup_{-\tau \leq s \leq 0} \|V(T_k + s)\|$. Last in-equality follows since $V(T_k^-) \leq \sup_{-\tau \leq s \leq 0} \|V(T_k + s)\|$.

By (15), (16), condition (iii), and Lemma 3, we have

$$V(t) < \rho\|V(T_k)\|_\tau, \quad t \in (T_k, T_{k+1}), \tag{17}$$

where $\exp\left\{\dfrac{\Delta}{\beta}(\beta\alpha_1 + \alpha_2) + \ln\beta\right\} < \rho < 1$. Define

$$\begin{aligned} &DT_1 = T_1; \\ &DT_2 = \inf_j\{T_j : DT_1 + \tau \leq T_j \leq DT_1 + \tau + \Delta\}; \\ &\quad\vdots \\ &DT_i = \inf_j\{T_j : DT_{i-1} + \tau \leq T_j \leq DT_{i-1} + \tau + \Delta\}; \\ &\quad\vdots \end{aligned}$$

Obviously, by (16) and (17), when $t = DT_i$ we have

$$V(DT_i) \le \beta \|V(DT_i)\|_\tau, \tag{18}$$

and when $t \in (TD_i, TD_{i+1})$ we have

$$V(t) < \rho \|V(DT_i)\|_\tau. \tag{19}$$

From the definition of DT_i, we see $DT_{i+1} - DT_i \ge \tau$, which implies

$$\|V(DT_{i+1})\|_\tau < \rho \|V(DT_i)\|_\tau. \tag{20}$$

Thus, by (18), (19), and (20), we obtain

$$V(t) \le \rho^i \|V(0)\|_\tau, \quad t \in [DT_i, DT_{i+1}]. \tag{21}$$

On the other hand, since $DT_i \le DT_{i-1} + (\tau + \Delta) \le \ldots \le DT_1 + (i-1)(\tau + \Delta)$, then $t \to \infty$ implies $i \to \infty$. We have

$$\lim_{t\to\infty} \|e(t)\| \le \lim_{t\to\infty} \sqrt{\frac{V(t)}{\lambda_m(P)}} \le \lim_{i\to\infty} \sqrt{\frac{\rho^i \|V(0)\|_\tau}{\lambda_m(P)}} = 0. \tag{22}$$

Therefore, from the definition of synchronization, the slave system (5) is synchronized with the master system (4) by impulsive control law $\{T_k, U_k\}$.

Remark 3. Conditions (i)–(ii) of Theorem 1 are related to the impulsive controllers U_k and condition (iii) is the restriction for the impulsive intervals Δ_k. If the controllers are strong enough (*i.e.*, $B_k \approx I$) and the impulsive intervals are small enough (*i.e.*, $\Delta_k \approx 0$), then all conditions are always satisfied. This implies that, in theory, one can always achieve chaos synchronization by GISS. In reality, sometimes impulsive control can be only applied in some specific windows (controllable windows), not during the whole time, due to some practical constraints. Therefore, we present intermittent impulsive synchronization criteria to extend our results as follows.

4.3 Intermittent impulsive synchronization criterion

Theorem 2. Suppose that for an intermittent impulsive control law $\{T_{m,l}, U_{m,l}\}$:

(i) there exist a positive definite matrix P and constants $\alpha_1 > 0$, $\alpha_2 > 0$ and $\xi > 0$ such that

$$\begin{bmatrix} A^T P + PA + \xi PCC^T P - \alpha_1 P & PB \\ B^T P & \frac{L^2}{\xi} I - \alpha_2 P \end{bmatrix} \le 0; \tag{23}$$

(ii) there exist real numbers $\beta_{m,l} \in (0, 1)$ such that

$$(I - B_{m,l}^T) P (I - B_{m,l}) - \beta_{m,l} P \le 0; \tag{24}$$

(iii) there exists a real number d ($\beta_{m,l} < d < 1$) such that for each m, l,

$$\frac{\Delta_{m,l}}{\beta_{m,l}} (\beta_{m,l}\alpha_1 + \alpha_2) + \ln \beta_{m,l} \le \ln d, \tag{25}$$

where $\Delta_{m,l} = T_{m,l+1} - T_{m,l}$ and $T_{m,M_m+1} = (m+1)\omega$;

(iv) the time delay satisfies $\tau \le \omega - \delta - \Delta$ and

$$d^{\left\lfloor \frac{\omega-\delta}{\tau+\Delta} \right\rfloor} e^{(\alpha_1+\alpha_2)\delta} < 1, \tag{26}$$

where $\Delta = \max_{m,l}\{\Delta_{m,l}\}$ and $\lfloor a \rfloor$ denotes the nearest integer less than or equal to a.

Then the slave system (7) is synchronized with the master system (4) by the intermittent impulsive control $\{T_{m,l}, U_{m,l}\}$.

Proof. Define $V(t) = e(t)^T P e(t)$. When $t \in [m\omega, m\omega + \delta]$, the impulsive controller is not activated. Similar with (14), we have

$$V'(t) \le \alpha_1 V(t) + \alpha_2 V(t - \tau). \tag{27}$$

In terms of Lemma 2, we have

$$V(t) \le \|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)(t-m\omega)}, \quad t \in [m\omega, m\omega + \delta). \tag{28}$$

When $t \in [m\omega + \delta, (m+1)\omega]$, the system runs in controllable periods. Thus, the impulsive controller works. First, considering $t = T_{m,1}$, we get by condition (ii)

$$\begin{aligned} V(T_{m,1}) &= e(T_{m,1}^-)^T (I - B_{m,1})^T P (I - B_{m,1}) e(T_{m,1}^-) \\ &\le \beta_{m,1} e(T_{m,1}^-)^T P e(T_{m,1}^-) = \beta_{m,1} V(T_{m,1}^-) \\ &\le \beta_{m,1} \|V(T_{m,1})\|_\tau. \end{aligned} \tag{29}$$

When $t \in (T_{m,1}, T_{m,2})$, we have $V'(t) \le \alpha_1 V(t) + \alpha_2 V(t - \tau)$, which implies, if $V(t) \ge \beta_{m,1} V(t + s)$, $s \in [-\tau, 0]$,

$$V'(t) \le \frac{1}{\beta_{m,1}} (\beta_{m,1}\alpha_1 + \alpha_2) V(t). \tag{30}$$

By (29), (30), condition (iii), and Lemma 3, we have

$$V(t) < d \|V(T_{m,1})\|_\tau, \quad t \in [T_{m,1}, T_{m,2}). \tag{31}$$

Similarly, we have

$$\begin{cases} V(t) \le \beta_{m,l} \|V(T_{m,l})\|_\tau \ t = T_{m,l}, \\ V(t) < d \|V(T_{m,l})\|_\tau, t \in [T_{m,l}, T_{m,l+1}), \end{cases} \tag{32}$$

where $l = 1, 2, \ldots, M_m$, and $T_{m,M_m+1} = (m+1)\omega$. Define

$$\begin{aligned} &DT_{m,1} = T_{m,1};\\ &DT_{m,2} = \inf_j\{T_{m,j} : DT_{m,1} + \tau \le T_{m,j} \le DT_{m,1} + \tau + \Delta\};\\ &\quad\vdots\\ &DT_{m,i} = \inf_j\{T_{m,j} : DT_{m,i-1} + \tau \le T_{m,j} \le DT_{m,i-1} + \tau + \Delta\};\\ &\quad\vdots \end{aligned}$$

Let $i_M = \max\{i : T_{m,1} \le DT_{m,i} \le T_{m,M_m}\}$ and define $DT_{m,i_M+1} = T_{m,M_m+1}$. Obviously, in terms of (32), when $t = DT_{m,i}$ we have

$$\begin{cases} V(t) \le d\,\|V(DT_{m,l})\|_\tau\ t = DT_{m,l},\\ V(t) < d\,\|V(DT_{m,l})\|_\tau, t \in [DT_{m,l}, DT_{m,l+1}). \end{cases} \tag{33}$$

From the definition of $DT_{m,i}$, we see $DT_{m,i+1} - DT_{m,i} \ge \tau$ for i ($1 \le i \le i_M - 1$), which implies

$$\|V(DT_{i+1})\|_\tau < d\,\|V(DT_i)\|_\tau, \quad 1 \le i \le i_M - 1. \tag{34}$$

Thus, by (33) and (34), we obtain

$$\begin{cases} V(t) \le \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, \quad t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \|V(m\omega+\delta)\|_\tau, \quad t \in [DT_{m,i}, DT_{m,i+1}). \end{cases}$$

By (28) and (29), we have

$$\|V(m\omega+\delta)\|_\tau \le \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}. \tag{35}$$

Furthermore,

$$\begin{cases} V(t) \le \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}). \end{cases} \tag{36}$$

From the definition of $DT_{m,i}$, since

$$DT_{m,i} \le DT_{m,i-1} + (\tau+\Delta) \le \cdots \le DT_{m,1} + (i-1)(\tau+\Delta),$$

we have $i \ge \dfrac{DT_{m,i} - DT_{m,1}}{\tau+\Delta} + 1$. On the other hand, we have

$$DT_{m,i_M} > T_{m,M_m} - \tau > (m+1)\omega - \Delta - \tau.$$

Then, $i_M \ge \dfrac{DT_{m,i_M} - DT_{m,1}}{\tau+\Delta} + 1 > \dfrac{\omega-\delta}{\tau+\Delta}$, which implies $i_M \ge \left\lfloor \dfrac{\omega-\delta}{\tau+\Delta} \right\rfloor + 1$.

By (36), we have

$$\begin{aligned} \|V((m+1)\omega)\|_\tau &\le \|V((m+1)\omega)\|_{DT_{m,i_M+1} - DT_{m,i_M-1}}\\ &\le d^{i_M-1}\|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}\\ &\le d^{\left\lfloor \frac{\omega-\delta}{\tau+\Delta} \right\rfloor} \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}. \end{aligned} \tag{37}$$

Let $\theta = d^{\left\lfloor \frac{\omega-\delta}{\tau+\Delta} \right\rfloor} e^{(\alpha_1+\alpha_2)\delta}$. We have

$$\|V(m\omega)\|_\tau \le \theta^m \|V(0)\|_\tau.$$

Furthermore,

$$\begin{cases} V(t) \le \theta^m \|V(0)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i\theta^m \|V(0)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}). \end{cases} \tag{38}$$

By condition (iv), we have $\lim_{t\to\infty} V(t) = 0$. Therefore,

$$\lim_{t\to\infty}\|e(t)\| \le \lim_{t\to\infty}\sqrt{\frac{V(t)}{\lambda_m(P)}} \le \lim_{i\to\infty}\sqrt{\frac{\rho^i\|V(0)\|_\tau}{\lambda_m(P)}} = 0. \tag{39}$$

The proof is complete.

Remark 4. In the proof of Theorem 2, $V(t)$ converges exponentially to zero along the trajectory of the error system (8). Also, the synchronization error $e(t)$ converges exponentially to zero. This implies that chaos synchronization is achieved very fast.

Corollary 1. Suppose that for an intermittent impulsive control law $\{T_{m,l}, U_{m,l}\}$:

(i) there exist a positive definite matrix P and constants $\alpha_1 > 0$, $\alpha_2 > 0$ and $\xi > 0$ such that

$$\begin{bmatrix} A^TP + PA + \xi PCC^TP - \alpha_1 P & PB\\ B^TP & \dfrac{L^2}{\xi} I - \alpha_2 P \end{bmatrix} \le 0;$$

(ii) there exist real numbers $\beta_{m,l} \in (0, 1)$ such that

$$(I - B_{m,l}^T)P(I - B_{m,l}) - \beta_{m,l}P \le 0;$$

(iii) there exists a real number d $\beta_{m,l} < d < 1$ such that for each m, l,

$$\frac{\Delta_{m,l}}{\beta_{m,l}}(\beta_{m,l}\alpha_1 + \alpha_2) + \ln\beta_{m,l} \le \ln d,$$

where $\Delta_{m,l} = T_{m,l+1} - T_{m,l}$ and $T_{m,M_m+1} = (m+1)\omega$;

(iv) the time delay satisfies $\omega - \delta - \Delta \le \tau \le \omega - \delta$ and $de^{(\alpha_1+\alpha_2)\delta} < 1$, where $\Delta = \max_{m,l}\{\Delta_{m,l}\}$.

Then the slave system (7) is synchronized with the master system (4) by the intermittent impulsive control $\{T_{m,l}, U_{m,l}\}$.

Proof. Since conditions (i)–(iii) are same as those of Theorem 2, we also have

$$\begin{cases} V(t) \le \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \|V(m\omega)\|_\tau\, e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}). \end{cases}$$

By condition (iv), we have

$$\begin{aligned}\|V((m+1)\omega)\|_\tau &\le \|V((m+1)\omega)\|_{\omega-\delta}\\ &\le d\|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)\delta}.\end{aligned}$$

Then, $\|V(m\omega)\|_\tau \le \mu^m \|V(0)\|_\tau$, $\mu = de^{(\alpha_1+\alpha_2)\delta}$. Furthermore,

$$\begin{cases} V(t) \le \mu^m \|V(0)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \mu^m \|V(0)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}).\end{cases}$$

By condition (iv), we have $\lim_{t\to\infty} V(t) = 0$, which implies $\lim_{t\to\infty} \|e(t)\| = 0$. The proof is complete.

Corollary 2. Suppose that for an intermittent impulsive control law $\{T_{m,l}, U_{m,l}\}$:

(i) there exist a positive definite matrix P and constants $\alpha_1 > 0$, $\alpha_2 > 0$ and $\xi > 0$ such that

$$\begin{bmatrix} A^TP + PA + \xi PCC^TP - \alpha_1 P & PB \\ B^TP & \dfrac{L^2}{\xi} I - \alpha_2 P \end{bmatrix} \le 0;$$

(ii) there exist real numbers $\beta_{m,l} \in (0, 1)$ such that

$$(I - B_{m,l}^T) P (I - B_{m,l}) - \beta_{m,l} P \le 0;$$

(iii) there exists a real number d $\beta_{m,l} < d < 1$ such that for each m, l,

$$\frac{\Delta_{m,l}}{\beta_{m,l}}(\beta_{m,l}\alpha_1 + \alpha_2) + \ln \beta_{m,l} \le \ln d,$$

where $\Delta_{m,l} = T_{m,l+1} - T_{m,l}$ and $T_{m,M_m+1} = (m+1)\omega$;

(iv) the time delay satisfies $\tau \le \Delta_0$ and

$$d^{\bar{M}-1} e^{(\alpha_1+\alpha_2)\delta} < 1,$$

where $\Delta_0 = \min_{m,l}\{\Delta_{m,l}\}$ and $\bar{M} = \min_m \{M_m\}$.

Then the slave system (7) is synchronized with the master system (4) by the intermittent impulsive control $\{T_{m,l}, U_{m,l}\}$.

Proof. Similarly, we also have

$$\begin{cases} V(t) \le \|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}).\end{cases}$$

Since $\tau \le \Delta_0$, then

$$DT_{m,i} = T_{m,i}, \quad i = 1, 2, \ldots, M_m + 1.$$

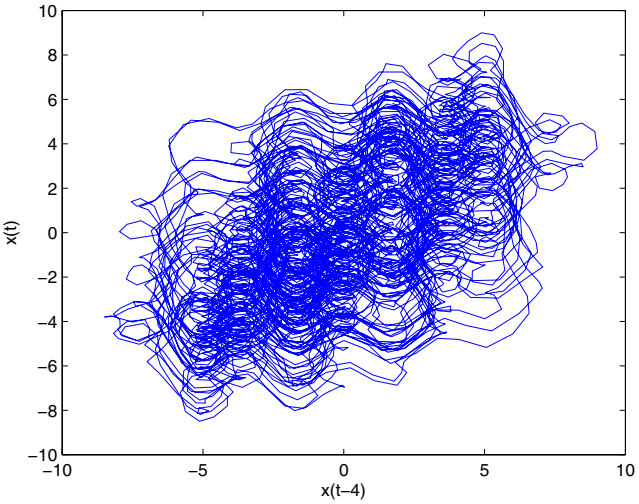


Fig. 3. Phase portrait $x(t-4) - x(t)$ of the hyperchaotic system with $a = 0.16$, $b = 2.4$, $c = 1.8$ and $\tau = 4$.

By condition (iv), we have

$$\begin{aligned}\|V((m+1)\omega)\|_\tau &\le \|V((m+1)\omega)\|_{T_{m,M_m+1}-T_{m,M_m-1}}\\ &\le d^{M_m-1}\|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)\delta}\\ &\le d^{\bar{M}-1}\|V(m\omega)\|_\tau e^{(\alpha_1+\alpha_2)\delta}.\end{aligned}$$

Then, we obtain $\|V(m\omega)\|_\tau \le \nu^m \|V(0)\|_\tau$, where $\nu = d^{\bar{M}-1} e^{(\alpha_1+\alpha_2)\delta}$.

Furthermore,

$$\begin{cases} V(t) \le \nu^m \|V(0)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [m\omega, m\omega+\delta),\\ V(t) \le d^i \nu^m \|V(0)\|_\tau e^{(\alpha_1+\alpha_2)\delta}, t \in [DT_{m,i}, DT_{m,i+1}).\end{cases}$$

By condition (iv), we have $\lim_{t\to\infty} V(t) = 0$, *i.e.*, $\lim_{t\to\infty} \|e(t)\| = 0$. The proof is complete.

V. NUMERICAL EXAMPLE

In this section, a numerical example is given to demonstrate the effectiveness of our synchronization criteria. We employ a fourth order Runge-Kutta method with step size 10^{-5} and consider a hyperchaotic system as the master system, described by

$$\frac{dx(t)}{dt} = -ax(t-\tau) + b\sin(cx(t-\tau)), \tag{40}$$

where $a = 0.16$, $b = 2.4$, $c = 1.8$ and $\tau = 4$. The initial condition is $\phi(s) = 2\sin(6\pi(s+\tau)/\tau)$, $s \in [-\tau, 0]$. The corresponding slave system is in the same form of the master system with the initial condition $\psi(s) = 3\cos(10\pi(s+\tau)/\tau)$, $s \in [-\tau, 0]$. This hyperchaotic system has three positive Lyapunov exponents: $\lambda_1 = 0.0925$, $\lambda_2 = 0.0593$ and $\lambda_3 = 0.0259$, as shown in Fig. 3.

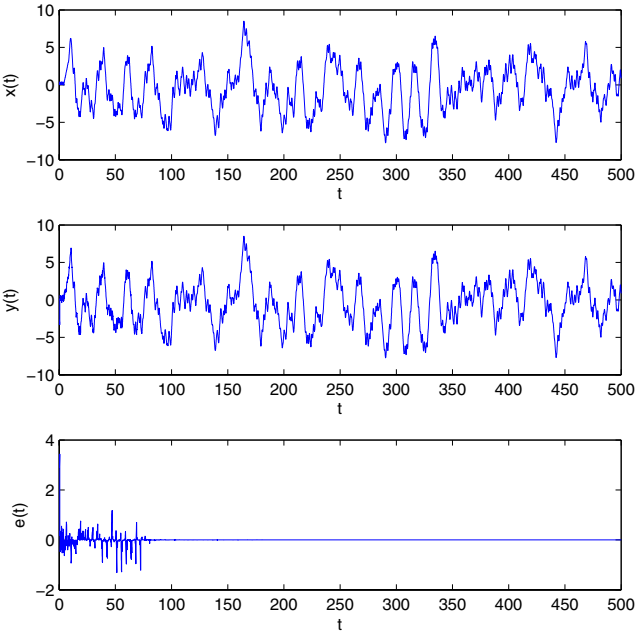


Fig. 4. The state trajectories and synchronization error of GISS with $\Delta_k = 0.50$ and $B_k = 0.95I$.

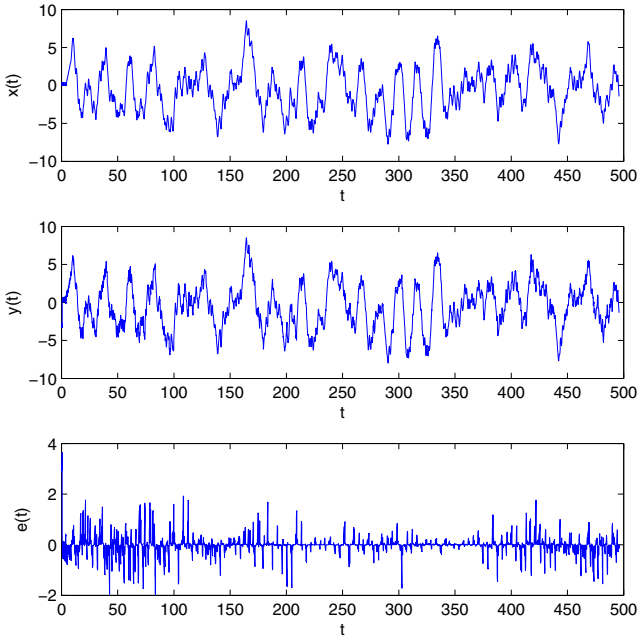


Fig. 5. The state trajectories and synchronization error of GISS with $\Delta_k = 0.72$ and $B_k = 0.95I$.

Comparing to (4) gives

$$A = 0, B = -0.16, C = 2.4, f(x) = \sin(1.8x), \text{and } L = 1.8.$$

First, considering GISS, we choose impulsive control parameters: $\Delta_k = 0.60$ and $B_k = 0.95I$. Let $P = I$. Thus, conditions (9)-(11) are satisfied. By Theorem 1, we know that the corresponding slave system is synchronized with the master system (4) by GISS. The state trajectories and the synchronization error are shown in Fig. 4. Our simulation results show that when the impulsive intervals satisfy $\Delta_k \leq 0.70$ the synchronization can always be achieved. However, if Δ_k further increases, GISS could not guarantee synchronization any more. It can be clearly observed from Fig. 5 that GISS fails when $\Delta_k = 0.72$.

Assume that $\omega = 20$ and $\delta = 10$. Thus, the free windows are $[20m, 20m + 10]$ and the control windows are $[20m + 10, 20m + 20]$. Since the free window width is far larger than the upper bound of impulsive intervals (0.70), GISS fails in this scenario. Now, we consider IISS. Choose control parameters $\Delta_{m,l} = 0.10$ and $B_{m,l} = 0.95I$ and let $P = I$. By Theorem 2, we know that the corresponding slave system is synchronized with the master system (40). The state trajectories and the synchronization error are shown in Fig. 6. Simulation results indicate that when impulsive intervals satisfy $\Delta_k \leq 0.21$, the synchronization can always be achieved.

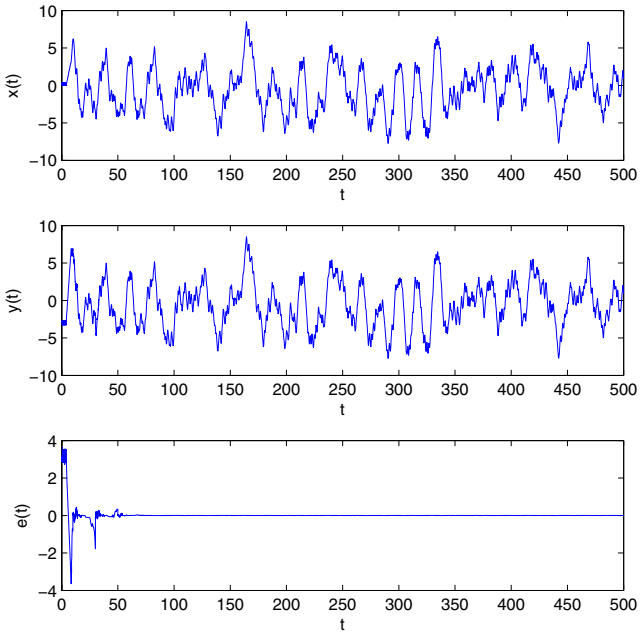


Fig. 6. The state trajectories and synchronization error of IISS with $\Delta_{m,l} = 0.10$ and $B_{m,l} = 0.95I$ when $\delta = 10$.

Remark 5. In the above example, the control window width $\omega - \delta$ is a half of the whole period width ω. The general impulsive synchronization approach is not applicable any more because the free window width δ is larger than the impulsive intervals.

Fixing the control parameter $B_{m,l} = 0.95I$, next we try to find the relationship between impulsive intervals and the free

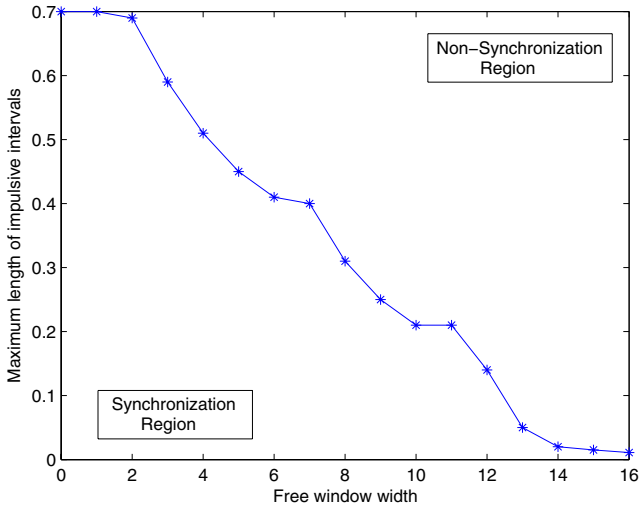


Fig. 7. The relationship between the maximum length of impulsive intervals and the free window width to guarantee synchronization.

window to guarantee synchronization. Simulation results are shown in Fig. 7.

Remark 6. Fig. 7 shows that the upper bound of the free window width decreases as the length of impulsive interval increases. In other words, to guarantee synchronization, if one wants to reduce the control window width, more frequent impulsive controls are needed. Further simulation shows that when $\tau > \omega - \delta$, the error system rapidly turns unstable, as shown in Fig. 8.

VI. APPLICATIONS TO SECURE COMMUNICATION

In this section, we shall establish a cryptosystem based on our hyperchaotic systems and IISS technique. The framework diagram is shown in Fig. 9, which consists of three parts: the transmitter, the receiver and the public channel (unsafe channel). The transmitter contains a hyperchaotic system X. (a, c) of X is public. (b, τ) of X is kept secret as the secret key and sent to the receiver across the private channel (safe channel) or across a public channel by public key cryptography. At the receiver, an identical hyperchaotic system Y is constructed by the public knowledge (a, c) and the secret key (b, τ). X and Y are the same hyperchaotic systems with different initial conditions. Suppose that the eavesdropper could never get the secret key. After the above configuration, our cryptosystem works as follows. Firstly, at the transmitter, one samples the synchronization signal $x(T_{m,l})$ from the hyperchaotic signal $x(t)$ $(t \in [m\omega + \delta, (m+1)\omega])$ of X and sends it to the receiver in the control windows. The information signal $m(t)$ is encrypted by encryption function $E(m(t),$

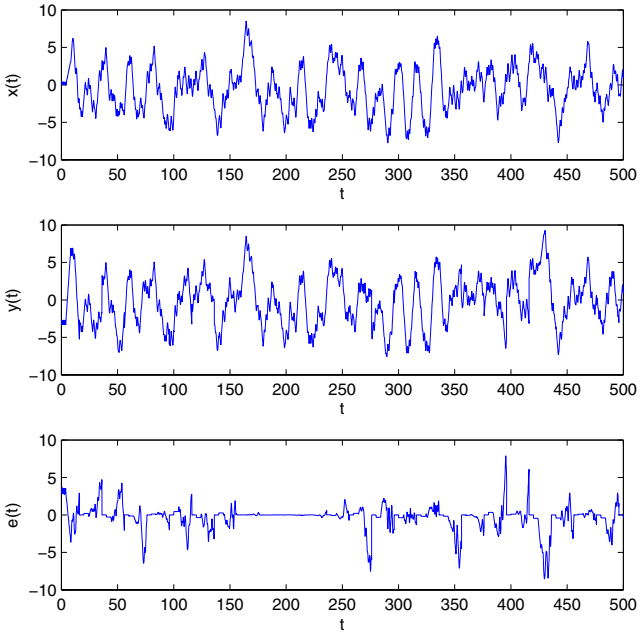


Fig. 8. The state trajectories and synchronization error of IISS with $\Delta_{m,l} = 0.0001$ and $B_{m,l} = 0.95I$ when $\delta = 16.1$.

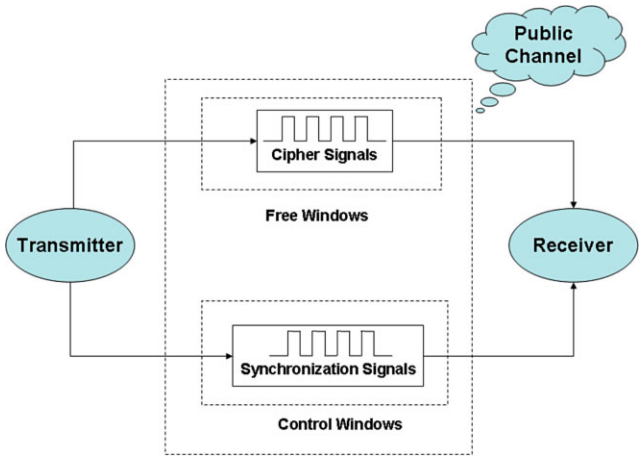


Fig. 9. The chaos-based secure communication.

$x(t))$ $(t \in [m\omega, m\omega + \delta])$ and the cipher signal $c(t)$ is sent to the receiver in the free windows after the transient synchronization region. At the receiver, one uses the synchronization signal $x(T_{m,l})$ to synchronize Y to X, employing the IISS technique. Then he can decrypt $c(t)$ by decryption function $D(c(t),$ $y(t))$ in the free windows, where $y(t)$ is the state variable of Y and obtain the decrypted signal $\tilde{m}(t)$. The principle diagram is shown in Fig. 10.

For instance, Alice wants to safely transmit the plain text "chaos cryptography" to Bob by our cryptosystem. The following encryption and decryption algorithms are required.

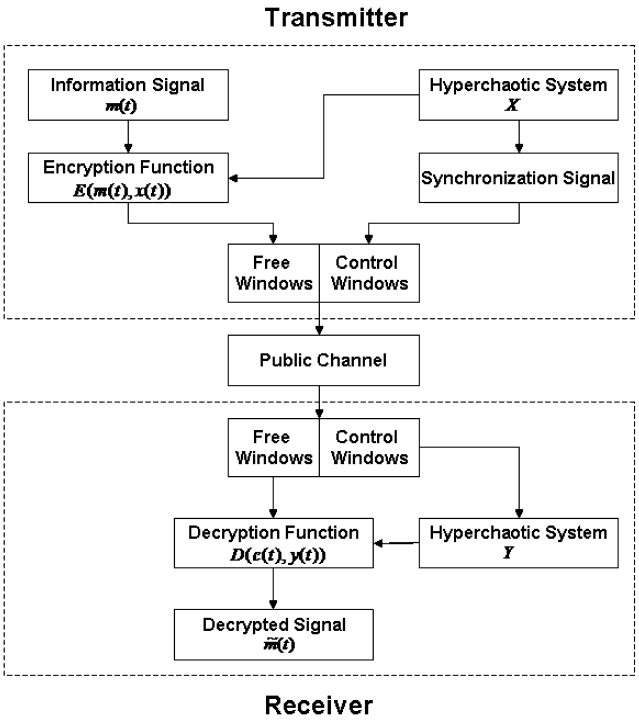


Fig. 10. The principle diagram of encryption and decryption.

Encryption algorithm.

1. Alice selects suitable constants a, b, c and τ. Keeps (b, τ) secret as the secret key and safely transmits it to Bob. Then publishes (a, c);
2. Constructs a hyperchaotic system X with (a, b, c, τ) and samples the synchronization signal $\{x(T_{m,l})\}$ from the state variable of the hyperchaotic system X;
3. Transfers the plain text PT to its corresponding binary representation by ASCII conversion,

$$\begin{aligned} B(PT) = [&0110001101101000011000010110\\ &1111011100110010000001100011 0\\ &1110010011110010111000001 1101\\ &0001101111011001110111 0010011\\ &0000101110000011010000111 1001]. \end{aligned}$$

For each letter, an 8-bit binary code is assigned. Each bit $B(PT)(i)$ ($i = 1, 2, \ldots, 144$) is denoted by $B(i)$. There are totally 144 bits for the plain text "chaos cryptography". And then generates the information signal by

$$m(i) = \begin{cases} 0.01, & B(i) = 1; \\ -0.01, & B(i) = 0. \end{cases}$$

4. Let $ST = \inf\{t : e(s) < 0.01, \quad s \geq t\}$ and define synchronization region: $\Omega_1 = [ST, \infty)$ and encryption region: $\Omega_2 = \Omega_1 \cap [m\omega, \ m\omega + \delta]$. Alice selects a starting point $T_e = m_0\omega \in \Omega_2$ and encrypts $B(i)$ by

$$c(i) = x(T_e + 0.05i) + m(i),$$

where $T_e + 0.05i \in [m_0\omega, m_0\omega + \delta]$.
5. Sends $\{T_{m,l}, x(T_{m,l}), Te, c(i)\}$ to Bob across public channel.

Decryption algorithm.

1. Bob firstly uses the secret key (b, τ) and the public knowledge (a, c) to set up the hyperchaotic system Y.
2. When $\{T_{m,l}, x(T_{m,l}), Te, c(i)\}$ is received, he synchronizes Y to X by the synchronization signal $\{T_{m,l}, x(T_{m,l})\}$ and derives $y(T_e + 0.05i)$ ($i = 1, 2, \ldots, 144$) from the state variable of Y.
3. Decrypts $c(i)$ to $m1(i)$ by

$$m1(i) = c(i) - y(T_e + 0.05i), i = 1, 2, \ldots, 144,$$

and transfers $m1(i)$ to binary representation by

$$B1(i) = \begin{cases} 1, & m1(i) > 0; \\ 0, & m1(i) < 0. \end{cases}$$

4. Recovers the plain text from $B1(i)$ by inverse ASCII conversion.

Assume that the hyperchaotic systems, X and Y, are with parameters $a = 0.16$ and $c = 1.8$, the secret key is $\{b = 2.4, \ \tau = 4.0\}$, the intermittent impulsive controller is with $\omega = 20$, $\delta = 10$, $\Delta_{m,l} = 0.10$ and $B_{m,l} = 0.95I$, and the starting point is $T_e = 80s$. Fig. 11 shows the hyperchaotic signals and the error signal, where the dashed rectangle is the encryption area. The information signal $m(i)$, the encrypted signal $c(i)$ and the decrypted signal $m1(i)$ are shown in Fig. 12. When the secret key is mismatched with 1% error (*i.e.*, $b = 2.376$ and $\tau = 3.96$ at the receiver) and other conditions are the same, the eavesdropper obtains the decrypted signal $m2(i)$ as shown in Fig. 12.

Remark 7. Fig. 12 shows that $m1(i)$ is almost the same as $m(i)$. Specifically,

$$|m1(i) - m(i)| = |x(T_e + 0.05i) - y(T_e + 0.05i)| < 0.01.$$

In terms of the filter in step (3) of decryption algorithm, $B1(i) = B(i)$ ($i = 1, 2, \ldots, 144$) can be always achieved. However, even though the eavesdropper guesses a key very close to the secret key (with 1% error), the decrypted signal $m2(i)$ is totally different from the information signal $m(i)$. It verifies that our hyperchaotic system is very sensitive to the secret key (b and τ). This property guarantees that the key

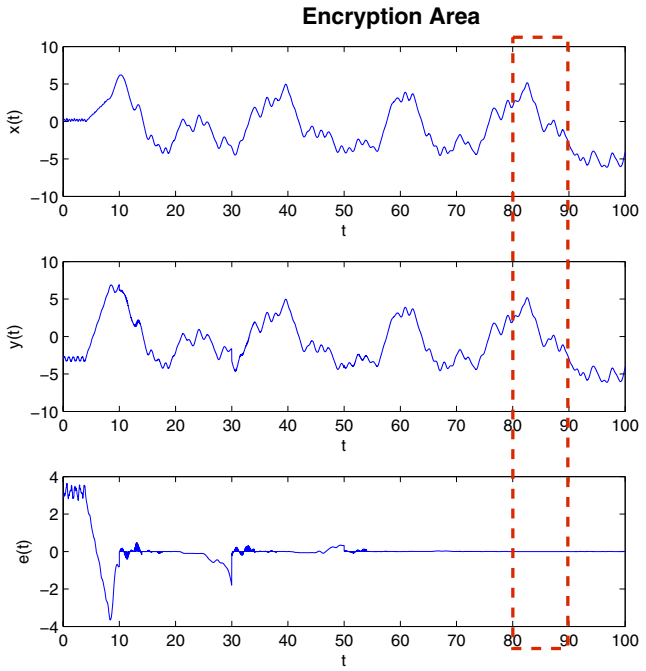


Fig. 11. The hyperchaotic signals and the error signal.

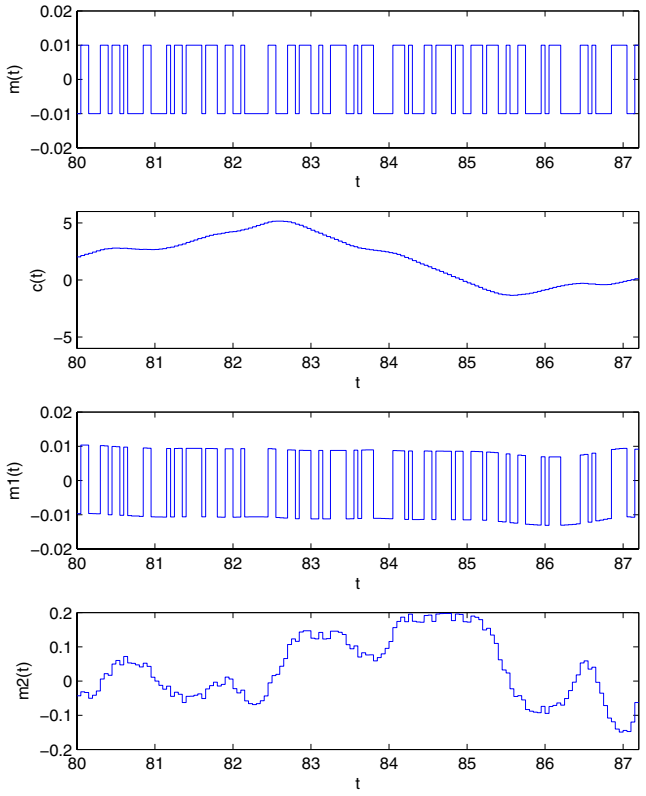


Fig. 12. The trajectories of $m(i)$, $c(i)$, $m1(i)$ and $m2(i)$.

space of our scheme is large enough. In other words, our hyperchaotic systems are natural for secure communication.

VII. CONCLUSIONS

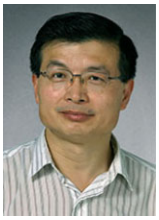
A hyperchaotic system from DDE has been introduced, which is natural for secure communication because of its sensitivity to parameter and delay. Furthermore, we have proposed a new synchronization scheme, IISS, to achieve chaos synchronization, which breaks through the limit of the upper bound of impulsive intervals in GISS. A secure communication scheme, based on our hyperchaotic system and IISS technique, has also been proposed. Simulation results have demonstrated that our cryptosystem is more secure. To further improve its performance, there are two outstanding issues needing to be solved. One is concerned with the robustness to channel noise and delay impulses, while the other is concerned with synchronization rate and synchronization error. In future work, we will furthermore explore how various factors, such as delay, disturbance, impulsive intervals, synchronization signals, parameter mismatch, *etc.*, impact the synchronization rate.

REFERENCES

1. Ayati, M., H. Khaloozadeh, and X. Liu, "Synchronizing chaotic systems with parametric uncertainty via a novel adaptive impulsive observer," *Asian J. Control*, Vol. 13, No. 6, pp. 807–817 (2011).
2. Bai, E. W. and K. E. Lonngren, "Sequential synchronization of two Lorenz systems using active control," *Chaos Solitons Fractals*, Vol. 11, No. 7, pp. 1041–1044 (2000).
3. Chen, C., G. Feng, and X. Guan, "Robust synchronization of chaotic Lur'e systems via delayed feedback control," *Phys. Lett. A*, Vol. 321, No. 5, pp. 344–354 (2004).
4. Cuomo, K. M. and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, Vol. 71, No. 1, pp. 65–68 (1993).
5. Dimassi, H. and A. Lora, "Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication," *IEEE Trans. Circuits Syst. I- Regul. Pap.*, Vol. 58, No. 4, pp. 800–812 (2011).
6. Doyne Farmer, J. "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, Vol. 4, No. 3, pp. 366–393 (1982).
7. Elwakil, A. S. and S. Ozoguz, "Multiscroll chaotic oscillators: the nonautonomous approach," *IEEE Trans. Circuits Syst. II- Express Briefs*, Vol. 53, No. 9, pp. 862–866 (2006).
8. Goedgebuer, J. P., L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos

generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.*, Vol. 80, No. 10, pp. 2249–2252 (1998).
9. Grassi, G. and S. Mascolo, "A system theory approach for designing cryptosystems based on hyperchaos," *IEEE Trans. Circuits Syst. I- Regul. Pap.*, Vol. 46, No. 9, pp. 1135–1138 (1999).
10. Halanay, A. *Differential Equations: Stability, Oscillations, Time Lags*, volume 23. Academic Press, New York (1966).
11. Halle, K. S., C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation Chaos*, Vol. 3, pp. 469–469 (1993).
12. Huang, N. S. *et al*. "Control and synchronization of discrete-time chaotic systems via variable structure control technique," *Phys. Lett. A*, Vol. 234, No. 4, pp. 262–268 (1997).
13. Karimi, H. R., M. Zapateiro, and N. Luo, "Adaptive synchronization of master–slave systems with mixed neutral and discrete time-delays and nonlinear perturbations," *Asian J. Control*, Vol. 14, No. 1, pp. 251–257 (2012).
14. Khadra, A., X. Z. Liu, and X. Shen, "Analyzing the robustness of impulsive synchronization coupled by linear delayed impulses," *IEEE Trans. Autom. Control*, Vol. 54, No. 4, pp. 923–928 (2009).
15. Li, P., J. Cao, and Z. Wang, "Robust impulsive synchronization of coupled delayed neural networks with uncertainties," *Physica A*, Vol. 373, pp. 261–272 (2007).
16. Li, P. and J. Lam, "Synchronization in networks of genetic oscillators with delayed coupling," *Asian J. Control*, Vol. 13, No. 5, pp. 713–725 (2011).
17. Li, Y., X. Liu, and H. Zhang, "Dynamical analysis and impulsive control of a new hyperchaotic system," *Math. Comput. Model.*, Vol. 42, No. 11-12, pp. 1359–1374 (2005).
18. Li, Z. G., C. Y. Wen, and Y. C. Soh, "Analysis and design of impulsive control systems," *IEEE Trans. Autom. Control*, Vol. 46, No. 6, pp. 894–897 (2001).
19. Liu, X., X. Shen, and H. Zhang, "Intermittent impulsive synchronization of chaotic delayed neural networks," *Int. J. Dyn. Syst. Differ. Equ.*, Vol. 19, No. 1–2, pp. 149–169 (2011).
20. Liu, X., X. Shen, and H. Zhang, "Multi-scroll chaotic and hyperchaotic attractors generated from chen system," *Int. J. Bifurcation Chaos*, Vol. 22, No. 2, p. 1250033, (2012). DOI: 10.1142/s0218127412500332.
21. Liu, X., K. L. Teo, H. Zhang, and G. Chen, "Switching control of linear systems for generating chaos," *Chaos Solitons Fractals*, Vol. 30, No. 3, pp. 725–733 (2006).
22. Lü, J., F. Han, X. Yu, and G. Chen, "Generating 3-D multi-scroll chaotic attractors: A hysteresis series switching method," *Automatica*, Vol. 40, No. 10, pp. 1677–1687 (2004).
23. Park, J. H., "Chaos synchronization between two different chaotic dynamical systems," *Chaos Solitons Fractals*, Vol. 27, No. 2, pp. 549–554 (2006).
24. Park, J. H. "Synchronization of Genesio chaotic system via backstepping approach," *Chaos Solitons Fractals*, Vol. 27, No. 5, pp. 1369–1375 (2006).
25. Pecora, L. M. and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, Vol. 64, No. 8, pp. 821–824 (1990).
26. Salarieh, H. and M. Shahrokhi, "Adaptive synchronization of two different chaotic systems with time varying unknown parameters," *Chaos Solitons Fractals*, Vol. 37, No. 1, pp. 125–136 (2008).
27. Sanchez, E. N. and J. P. Perez, "Input-to-state stability (ISS) analysis for dynamic neural networks," *IEEE Trans. Circuits Syst. I- Regul. Pap.*, Vol. 46, No. 11, pp. 1395–1398 (1999).
28. Sprott, J. C. "A simple chaotic delay differential equation," *Phys. Lett. A*, Vol. 366, No. 4-5, pp. 397–402 (2007).
29. Tamasevicius, A., G. Mykolaitis, and S. Bumeliene, "Delayed feedback chaotic oscillator with improved spectral characteristics," *Electron. Lett*, Vol. 42, No. 13, pp. 736–737 (2006).
30. Wang, H., X. J. Zhu, Z. Z. Han, and S. W. Gao, "A new stepping design method and its application in chaotic systems," *Asian J. Control*, Vol. 14, No. 1, pp. 230–238 (2012).
31. Wang, L. and X. Yang, "Generation of multi-scroll delayed chaotic oscillator," *Electron. Lett*, Vol. 42, No. 25, pp. 1439–1441 (2006).
32. Xia, W. and J. Cao, "Pinning synchronization of delayed dynamical networks via periodically intermittent control," *Chaos*, Vol. 19, No. 1, pp. 013120 (2009).
33. Yalçin, M. E. "Multi-scroll and hypercube attractors from a general jerk circuit using Josephson junctions," *Chaos Solitons Fractals*, Vol. 34, No. 5, pp. 1659–1666 (2007).
34. Yalçin, M. E. and S. Özoguz, "n-scroll chaotic attractors from a first-order time-delay differential equation," *Chaos*, Vol. 17, No. 3, pp. 033112 (2007).
35. Yang, T. and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication," *IEEE Trans. Circuits Syst. I- Regul. Pap.*, Vol. 44, No. 10, pp. 976–988 (1997).
36. Yau, H. T., "Design of adaptive sliding mode controller for chaos synchronization with uncertainties," *Chaos Solitons Fractals*, Vol. 22, No. 2, pp. 341–347 (2004).
37. Zhang, H., X. Liu, X. Shen, and J. Liu, "A family of novel chaotic and hyperchaotic attractors from delay differential equation," *Dynam. Cont. Dis. Ser. B*, Vol. 19, No. 3, pp. 411–430 (2012).

Hongtao Zhang received B.Sc. degree in power and mechanical engineering from Wuhan University, Wuhan, China, in 2001, M.Sc. degree in control theory and control engineering from Huazhong University of Science and Technology, Wuhan, China, in 2004, and Ph.D. degree in electrical and computer engineering from University of Waterloo, Waterloo, Ontario, Canada, in 2010. He is currently Post-Doctoral Fellow in applied mathematics joint with mechanical and mechatronics engineering at University of Waterloo. His research interests include hybrid dynamics, chaos control, network synchronization and their potential applications to secure communication, biological systems, hybrid electric vehicles, etc.



Xinzhi Liu received B.Sc. degree in mathematics from Shandong Normal University, Jinan, China, in 1982, and M.Sc. and Ph.D. degrees, all in applied mathematics, from University of Texas, Arlington, in 1987 and 1988, respectively. He was Post-Doctoral Fellow at University of Alberta, Edmonton, AB, Canada, from 1988 to 1990. He joined Department of Applied Mathematics, University of Waterloo, Waterloo, ON, Canada, in 1990, where he became Associate Professor in 1994 and a Professor in 1997. His research areas include systems analysis, stability theory, hybrid dynamical systems, impulsive control, chaos synchronization, nonlinear oscillations, artificial neural networks, and communication security. He is the author or coauthor of over 150 research articles and two research monographs and five other books. He is Chief Editor of the journal, DCDIS Series A: Mathematical Analysis, and Chief Editor of Journal, DCDIS Series B: Applications and Algorithms, and Associate Editor of four other journals. He served as General Chair for several international scientific conferences.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received B.Sc.(1982) degree from Dalian Maritime University (China) and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as Technical Program Committee Chair for IEEE VTC'10 Fall, Symposia Chair for IEEE ICC'10, Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, Technical Program Committee Chair for IEEE Globecom'07, General Co-Chair for Chinacom'07 and QShine'06, Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; Founding Area Editor for IEEE Transactions on Wireless Communications; Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc.; and Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007 and 2010 from University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.

Jun Liu received B.Sc. degree in applied mathematics from Shanghai Jiao-Tong University, Shanghai, China, in 2002, the M.Sc. degree in mathematics from Peking University, Beijing, China, in 2005, and Ph.D. degree in applied mathematics from University of Waterloo, Waterloo, Canada, in 2010. He is currently Lecturer in Department of Automatic Control and Systems Engineering at University of Sheffield, Sheffield, UK. Between 2011 and 2012, he was Postdoctoral Scholar in Control and Dynamical Systems at California Institute of Technology. His research interests are in the theory and applications of nonlinear, hybrid and networked control systems. Dr. Liu is a recipient of Zhang Si-Ying Outstanding Youth Paper Award of 2010 Chinese Control and Decision Conference (CCDC).