Application of Impulsive Synchronization to Communication Security

Anmar Khadra, Xinzhi Liu, and Xuemin Shen, *Senior Member, IEEE*

***Abstract*—In this paper, criteria on uniform equi-boundedness and equi-Lagrange stability for impulsive systems are derived. These criteria are used to synchronize two nonidentical chaotic systems by impulsively controlling a nonautonomous second order system, which leads to the development of an induced-message scheme for communication system security. With the scheme, message signals are not transmitted across public channels, but induced at the receiver end. The scheme overcomes the transmission time-frame congestion in impulsive cryptosystems discussed in the literature and improves system security. Simulation results are given to demonstrate the performance of the proposed scheme.**

***Index Terms*—Equi-boundedness, equi-Lagrange stability, impulsive synchronization, impulsive systems, induced-message cryptosystem, robustness.**

I. Introduction

IMPULSIVE differential equations have gained considerable attention in science and engineering [14], [15], [17], [24], [31], [32] in recent years, since they provide a natural framework for mathematical modeling of many physical phenomena. Examples include population-growth models [14] and maneuvers of spacecraft [17]. Impulsive control, which is based on the theory of impulsive differential equations, has gained renewed interests recently for controlling chaotic systems. It allows the stabilization of a chaotic system using only small control impulses, even though the chaotic behavior may follow unpredictable patterns (in general, chaotic signals are broadband, noise like, and difficult to predict) [15], [24], [32]. The impulsive control of nonautonomous chaotic systems, such as the Duffing's oscillator, is investigated in [30]. Instead of controlling the nonautonomous chaotic system to an equilibrium position, the stabilization of the chaotic system is achieved in a small region of the phase space using the notion of practical stability.

The study of impulsive synchronization of two identical chaotic systems is one of the most important applications of impulsive control. In [21], [27], and [28], two autonomous chaotic systems, the drive system and the driven system, have been considered for impulsive synchronization. Samples of the state variables of the drive system at discrete instances are used to drive the driven system. These samples are called the synchronization impulses and are employed to impulsively control the error system between the drive and the driven systems. The asymptotic stability of the error dynamics is established, assuring the synchronization between the two systems and an upper bound on the time interval between the impulses is obtained. A generalization of this particular type of synchronization to time-varying impulse intervals has been further developed in [13], where less conservative conditions on the Lyaponov function are obtained in the sense that it is required to be nonincreasing along a subsequence of the switching. Further detailed analysis of impulsive control and impulsive synchronization of chaotic systems are presented in [11], [12], [25], [26].

A number of interesting chaotic spread spectrum communication security systems based on continuous and impulsive synchronization have been proposed [2], [3], [5], [10], [19], [27], [29]. In the systems, message signals are masked or modulated by chaotic spreading signals (encryption) and the resulting signals are transmitted to the receivers across public channels. An identical synchronization between the chaotic systems in the transmitter and that in the receiver [20] is required for recovering the encrypted signal at the receiver end. A number of robust communication systems employing the two types of synchronization have been developed [9], [22], [23]. It has been shown that impulsive synchronization systems may be combined with conventional cryptographic techniques [27], [28] to achieve the two desired properties of increasing the complexity and reducing the redundancy of the transmitted signals. It has been further established that impulsive synchronization achieves efficient bandwidth utilization [20]. However, the proposed impulsive synchronization systems suffer from the transmission time-frame congestion [4], [6], [8], [18]. The impulsive synchronization systems rely on combining the encrypted signal with the synchronization impulses in the form of time frames each of length T s and transmitting them across a unidirectional public channel. The impulses occupy Q s of the total length of the time frame T, where $Q < T$ and the encrypted signal is carried on the remaining $T - Q$ s. The accuracy of synchronization depends on both the period T and the width of the impulse samples Q, where the minimum impulse width for synchronization increases as the impulse period increases [7]. This indicates that if the transmitted encrypted signal in each time frame becomes larger than a certain limit, the impulse width Q will occupy the whole time frame T, and becomes absolutely not negligible, causing the time-frame-congestion problem.

Manuscript received May 7, 2002; revised September 25, 2002. This work was supported in part by the Natural Sciences and Engineering Research Council, Canada. This paper was recommended by Associate Editor O. Feely.

A. Khadra and X. Liu are with the Department of Applied Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

X. Shen is with the Department of Electrical and Computer Engineering, Faculty of Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: xshen@bbcr.uwaterloo.ca).

Digital Object Identifier 10.1109/TCSI.2003.808839

In this paper, a new cryptosystem is proposed to resolve the time-frame-congestion problem and to enhance the security of the transmission. First, impulsive synchronization of second-order chaotic systems is studied. Conditions for uniform equi-boundedness and equi-Lagrange stability are derived for a particular type of impulsive system. Second, an induced-message scheme based on these conditions is developed for communications system security. It is shown that the induced-message scheme can improve the secure transmission by reducing time-frame congestion described in [4], [6]–[8], [18] and by preventing the transmission of the key and encrypted signals across the public channels. The remainder of the paper is organized as follows. In Section II, several conditions concerning uniform equi-boundedness and equi-Lagrange stability are stated and proved. In Section III, these conditions are applied to obtain sufficient conditions for impulsively controlling a second order nonautonomous impulsive system. In Section IV, the induced-message cryptosystem is presented. Simulation results are shown in Section V, followed by the conclusions in Section VI.

II. Preliminaries

To facilitate the discussion, it is convenient to introduce the notations as shown at the bottom of the page where $M \geq 0$.

Impulsive differential equations are usually defined as an ordinary differential equation coupled with a difference equation, as expressed in the following system:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{f}(t, \mathbf{x}), & t \neq t_k \\ \Delta \mathbf{x} = \mathbf{I}(t, \mathbf{x}), & t = t_k \end{cases} \tag{1}$$

where $\Delta \mathbf{x}(t_k) = \mathbf{x}(t_k^+) - \mathbf{x}(t_k^-)$, $\mathbf{x}(t_k^+) = \lim_{t \to t_k^+} \mathbf{x}(t)$, $\mathbf{x}(t_k^-) = \lim_{t \to t_k^-} \mathbf{x}(t)$, and the moments of impulse satisfy $0 = t_1 < t_2 < \cdots < t_k < \cdots$ and $\lim_{k \to \infty} t_k = \infty$. Let $\mathbf{f}, \mathbf{I} : \mathbb{R}_+ \times \mathbb{R}^n \to \mathbb{R}^n$ be continuous on $(t_k, t_{k+1}] \times \mathbb{R}^n$ and $\mathbf{f}(t_k^+, \mathbf{x})$, $\mathbf{I}(t_k^+, \mathbf{x})$ exist for each $k = 1, 2, \ldots$. This guarantees that, for each $(t_0, \mathbf{x}_0) \in \mathbb{R}_+ \times \mathbb{R}^n$, there exists a local solution of (1) satisfying the initial condition $\mathbf{x}(t_0^+) = \mathbf{x}_0$ [11]. Let $\mathbf{x}(t) := \mathbf{x}(t, t_0, \mathbf{x}_0)$ be any solution of (1) satisfying $\mathbf{x}(t_0^+) = \mathbf{x}_0$ and $\mathbf{x}(t)$ be left continuous at each $t_k > t_0$ in its interval of existence, i.e., $\mathbf{x}(t_k^-) = \mathbf{x}(t_k)$. We have the following definitions.

Definition 1: Let $M \geq 0$ and $V \in \nu_0(M)$. Define the upper right derivative of $V(t, \mathbf{x})$ with respect to the continuous portion of system (1), for $(t, \mathbf{x}) \in \mathbb{R}_+ \times S^c(M)^0$ and $t \neq t_k$, by

$$D^+V(t, \mathbf{x}) := \lim_{\delta \to 0^+} \sup \frac{1}{\delta} [V(t + \delta, \mathbf{x} + \delta \mathbf{f}(t, \mathbf{x})) - V(t, \mathbf{x})]. \tag{2}$$

From Definition 1, if $V(t, \mathbf{x})$ has continuous partial derivatives with respect to t and $\mathbf{x}$, then, by (2), we have

$$D^+V(t, \mathbf{x}) = \dot{V}(t, \mathbf{x}) = \frac{\partial V(t, \mathbf{x})}{\partial t} + \frac{\partial V(t, \mathbf{x})}{\partial \mathbf{x}} \cdot \mathbf{f}(t, \mathbf{x}).$$

Furthermore, if $\mathbf{x}(t)$ is a solution of (1) on some open interval $J \subset \mathbb{R}_+$, for $(t, \mathbf{x}(t)) \in J \times S^c(M)^0$ and $t \neq t_k$, we have

$$D^+V(t, \mathbf{x}(t)) = \lim_{\delta \to 0^+} \sup \frac{1}{\delta} [V(t + \delta, \mathbf{x}(t + \delta)) - V(t, \mathbf{x}(t))].$$

Definition 2: Solutions of the impulsive system (1) are said to be

(S1) equi-attractive in the large if for each $\epsilon > 0$, $\alpha > 0$ and $t_0 \in \mathbb{R}_+$, there exists a number $T := T(t_0, \epsilon, \alpha) > 0$ such that $\|\mathbf{x}_0\| < \alpha$ implies $\|\mathbf{x}(t)\| < \epsilon$, for $t \geq t_0 + T$;

(S2) uniformly equi-attractive in the large if T in (S1) is independent of t_0.

Definition 3: Solutions of the impulsive system (1) are said to be

(B1) equi-bounded if for each $\alpha > 0$, $t_0 \in \mathbb{R}_+$, there exists a constant $\beta := \beta(t_0, \alpha) > 0$ such that $\|\mathbf{x}_0\| \leq \alpha$ implies that $\|\mathbf{x}(t)\| < \beta$, for $t > t_0$;

(B2) uniformly equi-bounded if β in (B1) is independent of t_0;

(B3) equi-Lagrange stable if (S1) and (B1) hold together;

(B4) unformly equi-Lagrange stable if (S2) and (B2) hold together.

We shall need the following result [1], [16].

Theorem 1: The solutions of (1) are uniformly equi-bounded if

(T1.1) $V \in \nu_0(M)$, for some $M \geq 0$ and there exist functions $a, b \in \mathcal{KR}$ such that $b(\|\mathbf{x}\|) \leq V(t, \mathbf{x}) \leq a(\|\mathbf{x}\|)$, $(t, \mathbf{x}) \in \mathbb{R}_+ \times S^c(M)$;

(T1.2) there exist functions $p \in \mathcal{PC}$ and $c_k \in \mathcal{K}_0$ such that

$$D^+V(t, \mathbf{x}) \leq p(t) c_k(V(t, \mathbf{x})),\ (t, \mathbf{x}) \in (t_k, t_{k+1}) \times S^c(M)^0 \tag{3}$$

$$\begin{aligned}
\mathcal{K}_0 &:= \{g \in C[\mathbb{R}_+, \mathbb{R}_+] : g(s) > 0 \text{ if } s > 0 \text{ and } g(0) = 0\} \\
\mathcal{K} &:= \{g \in \mathcal{K}_0 : g(s) \text{ is strictly increasing in } s\} \\
\mathcal{KR} &:= \left\{g \in \mathcal{K} : \lim_{s \to \infty} g(s) = \infty\right\} \\
\mathcal{PC} &:= \left\{p : \mathbb{R}_+ \to \mathbb{R}_+ : p(t) \in C((t_k, t_{k+1}]) \text{ and } p\left(t_k^+\right) \text{ exists}, k = 1, 2, \ldots\right\} \\
S^c(M) &:= \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \geq M\} \\
S^c(M)^0 &:= \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| > M\} \\
\nu_0(M) &:= \Big\{V : \mathbb{R}_+ \times S^c(M) \to \mathbb{R}_+ : V(t, \mathbf{x}) \in C((t_k, t_{k+1}] \times S^c(M)) \\
&\qquad \text{locally Lipschitz in } \mathbf{x} \text{ and } V\left(t_k^+, \mathbf{x}\right) \text{ exists for } k = 1, 2, \ldots\Big\}
\end{aligned}$$

for $k = 1, 2, \ldots$;
(T1.3) there exists a constant $N \geq 0$ such that if $\|\mathbf{x}(t_k)\| \leq M$, then $\|\mathbf{x} + \mathbf{I}(t_k, \mathbf{x})\| \leq N$, for $k = 1, 2, \ldots$;
(T1.4) there exist functions $\Psi \in \mathcal{KR}$ and $\Psi_k \in \mathcal{K}_0$ such that $\Psi(s) \leq \Psi_k(s) \leq s,\ s \in \mathbb{R}_+$ and

$$V\left(t_k^+, \mathbf{x} + \mathbf{I}\left(t_k, \mathbf{x}\right)\right) \leq \Psi_k\left(V\left(t_k, \mathbf{x}\right)\right) \tag{4}$$

whenever $(t_k, \mathbf{x}), (t_k, \mathbf{x} + \mathbf{I}(t_k, \mathbf{x})) \in \mathbb{R}_+ \times S^c(M)^0$, for $k = 1, 2, \ldots$;
(T1.5) there exist constants $\lambda > 0$ and $\gamma_k \geq 0$ such that

$$\int_{t_k}^{t_{k+1}} p(s)ds + \int_{y}^{\Psi_k(y)} \frac{ds}{c_k(s)} \leq -\gamma_k \tag{5}$$

where $y \geq \lambda,\ k = 1, 2, \ldots$.

By strengthening the conditions of Theorem 1, we shall establish a criterion for equi-Lagrange stability.

Theorem 2: The solutions of (1) are equi-Lagrange stable if
(T2.1) (1) is equi-bounded;
(T2.2) condition (T1.2) holds for $V \in \nu_0(0)$ with inequality (3) being true for all $(t, \mathbf{x}) \in \mathbb{R}_+ \times \mathbb{R}^n$;
(T2.3) there exist functions $\Psi_k \in \mathcal{K}_0$ such that inequality (4) holds, for all $(t_k, \mathbf{x}) \in \mathbb{R}_+ \times \mathbb{R}^n$ and for all $k = 1, 2, \ldots$;
(T2.4) there exists a constant $\rho > 0$ and functions $C_k \in \mathcal{K}$ such that $C_k(s) \leq c_k(s)$, for all $s \in \mathbb{R}_+$ and for all $k = 1, 2, \ldots$;
(T2.5) (5) holds, for all $y > 0$ and

$$\sum_{k=1}^{\infty} \gamma_k = \infty.$$

Proof: To prove equi-Lagrange stability, we only need to show that (1) is equi-attractive in the large in view of assumption (T2.1). For simplicity, we set $m(t) := V(t, \mathbf{x}(t))$, where $\mathbf{x}(t) = \mathbf{x}(t, t_0, \mathbf{x}_0)$ is any solution of (1) such that $\mathbf{x}(t_0) = \mathbf{x}_0$. Due to the fact that system (1) is equi-bounded, the solution $\mathbf{x}(t) = \mathbf{x}(t, t_0, \mathbf{x}_0)$ of (1) exists on $[t_0, \infty)$, for all $\mathbf{x}_0 \in \mathbb{R}^n$. Since $V \in \nu_0(0)$, we have $D^+m(t) = D^+V(t, \mathbf{x}(t))$. By inequalities (3) and (4), we have

$$\begin{cases} D^+m(t) \leq p(t)c_k(m(t)), & t \neq t_k \\ m\left(t_k^+\right) \leq \Psi_k\left(m\left(t_k\right)\right), & k = 1, 2, \ldots. \end{cases} \tag{6}$$

Using (6), we obtain, for every $k = 1, 2, \ldots$

$$\begin{aligned} \int_{m(t_k^+)}^{m(t)} \frac{ds}{c_k(s)} &\leq \int_{t_k}^{t} p(s)ds \\ &\leq \int_{t_k}^{t_{k+1}} p(s)ds,\ t \in (t_k, t_{k+1}] \end{aligned} \tag{7}$$

$$\int_{m(t_k)}^{m(t_k^+)} \frac{ds}{c_k(s)} \leq \int_{m(t_k)}^{\Psi_k(m(t_k))} \frac{ds}{c_k(s)}. \tag{8}$$

Adding (7) and (8), we get, for $k = 1, 2, \ldots$, in view of condition (T2.5) and inequality (5)

$$\int_{m(t_k)}^{m(t)} \frac{ds}{c_k(s)} \leq \int_{t_k}^{t_{k+1}} p(s)ds + \int_{m(t_k)}^{\Psi_k(m(t_k))} \frac{ds}{c_k(s)} \leq -\gamma_k. \tag{9}$$

With (9), we conclude that $m(t) \leq m(t_k)$, for all $t \in (t_k, t_{k+1}]$, $k = 1, 2, \ldots$, i.e., $m(t_{k+1}) \leq m(t_k)$. This means that the sequence $\{m(t_k)\}_{k=1}^{\infty}$ is nonincreasing. Furthermore, since the sequence is bounded from below, it follows that the sequence possesses a limit, say $\mathcal{L} \geq 0$, as k approaches infinity. We shall prove $\mathcal{L} = 0$. Let us assume $\mathcal{L} > 0$ and try to reach a contradiction. Using the fact that $c_k \in \mathcal{K}_0$, $C_k \in \mathcal{K}$, $C_k(s) \leq c_k(s)$, for all $s \in \mathbb{R}_+$ and $m(t_k) \geq m(t_{k+1})$, for all $k = 1, 2, \ldots$, we obtain

$$\int_{m(t_k)}^{m(t_{k+1})} \frac{C_k(\mathcal{L})}{c_k(s)} ds \geq m(t_{k+1}) - m(t_k)$$

for all $k = 1, 2, \ldots$. Thus, for $n > 1$, we obtain

$$\begin{aligned} & m\left(t_{n+1}\right) - m\left(t_1\right) \\ =& m\left(t_{n+1}\right) - m\left(t_n\right) + m\left(t_n\right) - \cdots + m\left(t_2\right) - m\left(t_1\right) \\ \leq& \int_{m(t_n)}^{m(t_{n+1})} \frac{C_n(\mathcal{L})}{c_n(s)} ds + \cdots + \int_{m(t_1)}^{m(t_2)} \frac{C_1(\mathcal{L})}{c_1(s)} ds \\ \leq& -\gamma_n C_n(\mathcal{L}) - \gamma_{n-1} C_{n-1}(\mathcal{L}) - \cdots - \gamma_1 C_1(\mathcal{L}) \\ =& -\sum_{k=1}^{n} \gamma_k C_k(\mathcal{L}). \end{aligned}$$

Let $\rho = min_k C_k(\mathcal{L})$. This implies, by conditions (T2.4) and (T2.5), that

$$m\left(t_{n+1}\right) \leq m\left(t_1\right) - \rho \sum_{k=1}^{n} \gamma_k \longrightarrow -\infty$$

as $n \to \infty$, which is a contradiction. Therefore, we must have $\mathcal{L} = 0$, as we claimed. On the other hand, $m(t) \leq m(t_k)$, for all $t \in (t_k, t_{k+1}]$ and for all $k = 1, 2, \ldots$. Thus

$$\lim_{t \to \infty} m(t) = 0.$$

It follows that

$$\lim_{t \to \infty} \|\mathbf{x}(t)\| = \lim_{t \to \infty} b(\|\mathbf{x}(t)\|) = \lim_{t \to \infty} m(t) = 0.$$

i.e., (1) is equi-attractive in the large and, hence, it is equi-Lagrange stable, as required. □

In the following sections, theorems on equi-boundedness and equi-Lagrange stability are applied to a particular nonautonomous second order impulsive system. The system will be employed in designing a secure communication system.

III. Nonautonomous Second-Order Impulsive System

Consider the following second-order impulsive system which depends on $\widetilde{\mathbf{x}}$ and $\dot{\widetilde{\mathbf{x}}}$, simultaneously

$$\begin{cases} \ddot{\widetilde{\mathbf{x}}} = \widetilde{A}\dot{\widetilde{\mathbf{x}}} + \widetilde{\mathbf{g}}(\widetilde{\mathbf{x}}, \dot{\widetilde{\mathbf{x}}}) + \widetilde{\mathbf{\Phi}}\left(\dot{\widetilde{\mathbf{x}}}, \mathbf{u}(t)\right), & t \neq t_k \\ \Delta\widetilde{\mathbf{x}} = D_k\widetilde{\mathbf{x}},\ t = t_k, & k = 1, 2, \ldots \\ \Delta\dot{\widetilde{\mathbf{x}}} = \widetilde{D}_k\dot{\widetilde{\mathbf{x}}},\ t = t_k, & k = 1, 2, \ldots \end{cases} \tag{10}$$

where $\widetilde{A}$ is an $n \times n$ constant matrix, $\widetilde{\mathbf{g}}$ and $\widetilde{\mathbf{\Phi}}$ are continuous nonlinear maps satisfying

$$\dot{\widetilde{\mathbf{x}}}^T \widetilde{\mathbf{g}}\left(\widetilde{\mathbf{x}}, \dot{\widetilde{\mathbf{x}}}\right) \leq L_1\left[\|\widetilde{\mathbf{x}}\|^2 + \|\dot{\widetilde{\mathbf{x}}}\|^2\right]$$

and $\|\widetilde{\mathbf{\Phi}}(\dot{\widetilde{\mathbf{x}}}, \mathbf{u}(t))\| \leq L_2\|\dot{\widetilde{\mathbf{x}}}\| + L_3$, for some constant $L_2 > 0$ and $L_3 \geq 0$, $\mathbf{u}(t)$ is an arbitrary control function satisfying $\|\mathbf{u}(t)\| \leq K$, for some $K \geq 0$ and D_k and $\widetilde{D}_k$ are $n \times n$

constant matrices, for all $k = 1, 2, \ldots$. Set $\mathbf{x}_1 = \widetilde{\mathbf{x}}$, $\mathbf{x}_2 = \dot{\widetilde{\mathbf{x}}}$ and let $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2)^T$

$$A := \begin{pmatrix} 0 & I \\ 0 & \widetilde{A} \end{pmatrix} \quad B_k := \begin{pmatrix} D_k & 0 \\ 0 & \widetilde{D}_k \end{pmatrix}$$

be block matrices, where I is the identity matrix

$$\mathbf{g}(\mathbf{x}) := \begin{pmatrix} 0 \\ \widetilde{\mathbf{g}}(\mathbf{x}) \end{pmatrix} \text{ and } \mathbf{\Phi}(\mathbf{x}, \mathbf{u}(t)) := \begin{pmatrix} 0 \\ \widetilde{\mathbf{\Phi}}(\mathbf{x}_2, \mathbf{u}(t)) \end{pmatrix}.$$

Then, (10) becomes

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + \mathbf{g}(\mathbf{x}) + \mathbf{\Phi}(\mathbf{x}, \mathbf{u}(t)), & t \neq t_k \\ \Delta\mathbf{x} = B_k\mathbf{x}, \ t = t_k, & k = 1, 2, \ldots. \end{cases} \tag{11}$$

We shall investigate the equi-boundedness and equi-Lagrange stability of solutions of (10) using (11).

Theorem 3: System (11) is uniformly equi-bounded if the largest eigenvalue of $(I + B_k^T)(I + B_k)$, denoted by λ_k, satisfies

$$\lambda_k \leq \exp(-2\alpha_k) \tag{12}$$

for all $k = 1, 2, \ldots$ and for $\|\mathbf{x}(t_k)\|, \|\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)\| > M$ for some $M \geq 0$, where $\alpha_k := (1/2)[\gamma_k + \ell\Delta_{k+1}] + \delta$, $\gamma_k \geq 0$ are constants and $\{\gamma_k\}_{k=1}^{\infty}$ has an upper bound, $0 < \delta \ll \inf_k(\gamma_k + \ell\Delta_{k+1})$, $\Delta_k := t_k - t_{k-1} > r > 0$, for all $k = 2, 3, \ldots$ and

$$\ell := |d| + 2L_1 + 2L_2 + 2L_3$$

where d is the largest eigenvalue of $Q := A + A^T$. Moreover, if $\gamma_k = 1/k$, for all $k = 1, 2, \ldots$ and for all $\|\mathbf{x}(t_k)\| > 0$ and if $L_3 = 0$ then, (11) is uniformly equi-Lagrange stable.

Proof: Let $\mathcal{B} := \sup_k(\alpha_k)$, $M := (\exp(\mathcal{B}) - \exp(\delta))/(\exp(\delta) - 1) > 0$ and $V(t, \mathbf{x}) := V(\mathbf{x}) = \mathbf{x}^T\mathbf{x} = \|\mathbf{x}\|^2$. Choose $b(\|\mathbf{x}\|) = a(\|\mathbf{x}\|) = \|\mathbf{x}\|^2$. The upper-right derivative of V is given by

$$\begin{aligned} D^+V(\mathbf{x}) =& \dot{\mathbf{x}}^T\mathbf{x} + \mathbf{x}^T\dot{\mathbf{x}} \\ =& \mathbf{x}^TQ\mathbf{x} + 2\mathbf{g}(\mathbf{x})^T\mathbf{x} + 2\mathbf{\Phi}(\mathbf{x}, \mathbf{u}(t))^T\mathbf{x} \\ \leq& d\|\mathbf{x}\|^2 + 2L_1\|\mathbf{x}\|^2 + 2L_2\|\mathbf{x}\|^2 + 2L_3\|\mathbf{x}\| \\ =& (d + 2L_1 + 2L_2)\|\mathbf{x}\|^2 + 2L_3\|\mathbf{x}\| \\ \leq& (|d| + 2L_1 + 2L_2 + 2L_3)\left(V(\mathbf{x}) + V(\mathbf{x})^{1/2}\right) \\ =& p(t)c(V(\mathbf{x})) \end{aligned} \tag{13}$$

where $p(t) := |d| + 2L_1 + 2L_2 + 2L_3$ and $c(s) := s + s^{1/2}$. Clearly, $p \in \mathcal{PC}$ and $c \in \mathcal{K}$. Thus, conditions (T1.1) and (T1.2) are satisfied over $\mathbb{R}_+ \times \mathbb{R}^n$. If $\|\mathbf{x}(t_k)\| \leq M$, $k = 1, 2, \ldots$, then, by inequality (12), we have

$$\begin{aligned} \|\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)\| \leq& \|I + B_k\| \ \|\mathbf{x}(t_k)\| \\ \leq& \exp(-\alpha_k)\, M < \exp(-\delta)M := N \end{aligned}$$

for $k = 1, 2, \ldots$, and thus, condition (T1.3) is also satisfied. Define the mapping $\Psi_k(s)$, for all $k = 1, 2, \ldots$ as follows:

$$\Psi_k(s) := \exp(-2\alpha_k)\, s \qquad \text{for all } s \geq 0. \tag{14}$$

Clearly, $\Psi_k(s) \leq s$, for all $s \geq 0$, and $\Psi_k(s) \geq (1/2)\exp(-2\mathcal{B})s =: \Psi(s)$, for all $s \geq 0$. i.e., $\Psi(s) \leq \Psi_k(s) \leq s$. Fig. 1 shows a typical sketch of the mapping $\Psi_k(s)$ lying between the two lines $y = s$ and $\Psi(s)$. Furthermore, by

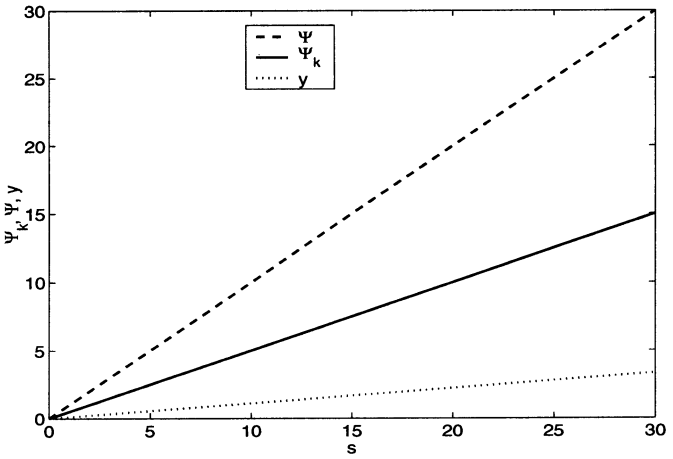


Fig. 1. Typical sketch of the mapping $\Psi_k(s)$.

inequality (12), for $\|\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)\| > M$, for $k = 1, 2, \ldots$, we have

$$\begin{aligned} V(\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)) =& (\mathbf{x}(t_k) + B_k\mathbf{x}(t_k))^T \\ & \cdot (\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)) \\ =& \mathbf{x}(t_k)^T\left(I + B_k^T\right)(I + B_k)\mathbf{x}(t_k) \\ \leq& \lambda_k\mathbf{x}(t_k)^T\mathbf{x}(t_k) \\ \leq& \exp(-2\alpha_k)\|\mathbf{x}(t_k)\|^2 \\ =& \Psi_k(V(\mathbf{x}(t_k))). \end{aligned}$$

This implies that condition (T1.4) is satisfied. In addition, it is easy to check that

$$\int \frac{ds}{s + s^{1/2}} = 2\ln\left(1 + s^{1/2}\right).$$

It follows that, for $k = 1, 2, \ldots$

$$\begin{aligned} \int_{t_k}^{t_{k+1}} p(s)ds + \int_y^{\Psi_k(y)} \frac{ds}{s + s^{1/2}} & \\ =& \ell\Delta_{k+1} + 2\ln\left[\frac{1 + \Psi_k^{1/2}(y)}{1 + y^{1/2}}\right] \\ =& \ell\Delta_{k+1} + 2\ln\left[\frac{1 + \exp(-\alpha_k)\, y^{1/2}}{1 + y^{1/2}}\right] \\ =& -\gamma_k - 2\delta + 2\ln\left[\frac{\exp(\alpha_k) + y^{1/2}}{1 + y^{1/2}}\right]. \end{aligned}$$

Notice that $\exp(\alpha_k) \leq \exp(\mathcal{B})$, for all $k = 1, 2, \ldots$ and the function

$$h(y) := \ln\left[\frac{\exp(\mathcal{B}) + y^{1/2}}{1 + y^{1/2}}\right]$$

is a decreasing function of y, for all $y \geq 0$. This implies, for $y \geq \lambda := M^2$ and $k = 1, 2, \ldots$, that

$$\begin{aligned} \int_{t_k}^{t_{k+1}} p(s)ds + \int_y^{\Psi_k(y)} \frac{ds}{s + s^{1/2}} & \\ \leq& -\gamma_k - 2\delta + 2h\left(M^2\right) \\ =& -\gamma_k - 2\delta + 2\ln\left[\frac{\exp(\delta)(\exp(\mathcal{B}) - 1)}{\exp(\mathcal{B}) - 1}\right] \\ =& -\gamma_k - 2\delta + 2\delta = -\gamma_k. \end{aligned}$$

Thus, condition (T1.5) is satisfied. We therefore conclude that (11) is uniformly equi-bounded as desired. It remains to show, with the choice of $\gamma_k = 1/k$, for all $k = 1, 2, \ldots$ and $L_3 = 0$, that (11) is uniformly equi-Lagrange stable. This is done by applying Theorem 2 as follows. We first consider the upper right derivative of $V(\mathbf{x})$

$$D^+V(\mathbf{x}) \leq (|d| + 2L_1 + 2L_2)\,\|\mathbf{x}\|^2 = \widetilde{p}(t)\widetilde{c}(V(\mathbf{x}))$$

where $\widetilde{p}(t) := |d| + 2L_1 + 2L_2$ and $\widetilde{c}(s) := s$. Thus, by employing the mapping Ψ_k, defined by (14), for all $k = 1, 2, \ldots$, we conclude that conditions (T2.1), (T2.2), (T2.3), and (T2.4) are all satisfied. Moreover, for $k = 1, 2, \ldots$

$$\int_{t_k}^{t_{k+1}} \widetilde{p}(s)ds + \int_{y}^{\Psi_k(y)} \frac{ds}{\widetilde{c}(s)} \leq \ell\Delta_{k+1} + \ln\left[\frac{\Psi_k(y)}{y}\right] < -\gamma_k$$

for all $y > 0$. Therefore, condition (T2.5) is also satisfied, since $\sum_{k=1}^{\infty}(1/k) = \infty$. This means that, by Theorem 2, solutions to (11) are uniformly equi-Lagrange stable, as required. □

If we return now to (10), Theorem 3 implies that $\lim_{t\to\infty} \widetilde{\mathbf{x}}(t) = \lim_{t\to\infty} \dot{\widetilde{\mathbf{x}}}(t) = \mathbf{0}$. In other words, if the conditions of Theorem 3 are satisfied, then, the solutions to (10) are uniformly equi-Lagrange stable. This important result will be applied considerably in the discussion of the next two sections. For now, we shall illustrate the above corollary by considering an example consisting of one pair of Lorenz chaotic systems and one pair of their derivatives. The uniform equi-Lagrange stability of the two error dynamics associated with those two pairs will be discussed and established by employing Theorem 3.

Let the first driving Lorenz chaotic system $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, m(t), a)$ be

$$\dot{\mathbf{x}} = A\mathbf{x} + \begin{pmatrix} 0 \\ -(x + am(t))z \\ xy \end{pmatrix} \tag{15}$$

where

$$A := \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix}, \qquad \sigma, r, b > 0$$

where $m(t) \in C^1([0, \infty))$ satisfies $|m(t)| \leq K_1$ and $|\dot{m}(t)| \leq K_2$, for some $K_1, K_2 > 0$ and $a = 0$ or 1. We shall see, in the next section, that $m(t)$ will represent the information signal in the induced-message model. The second driving system is the derivative of the Lorenz chaotic system given by (15), for $a = 1$ and is expressed by

$$\ddot{\mathbf{x}} = A\dot{\mathbf{x}} + \begin{pmatrix} 0 \\ -\dot{x}z - x\dot{z} \\ \dot{x}y + x\dot{y} \end{pmatrix} + \begin{pmatrix} 0 \\ -\dot{x}m(t) - x\dot{m}(t) \\ 0 \end{pmatrix}. \tag{16}$$

Let the first driven Lorenz chaotic system be

$$\begin{cases} \dot{\mathbf{u}} = A\mathbf{u} + \begin{pmatrix} 0 \\ -uw \\ uv \end{pmatrix}, & t \neq t_k \\ \Delta\mathbf{u} = -B_k\mathbf{e}, & t = t_k, \quad k = 1, 2, \ldots \end{cases} \tag{17}$$

where B_k are $n \times n$ constant matrices, for all $k = 1, 2, \ldots$, and $\mathbf{e} = \mathbf{x} - \mathbf{u}$ with $a = 0$. The second driven system is the derivative of the first driven system and is given by (18) shown at the bottom of the page, where $q = 0$ or 1, $\dot{\tilde{\mathbf{e}}} = \dot{\mathbf{x}} - \dot{\tilde{\mathbf{u}}}$, x, y, z, u, v and w are the chaotic signals. The above set up shown in Fig. 2 can be described as follows. x, y, and z, produced by the Lorenz chaotic system (15), with $a = 1$, are used to completely generate the derivative system (16). System (17), however, is driven impulsively by (15), with $a = 0$, while (18) is driven impulsively by (16) and continuously by the chaotic signals u, v and w from (17).

With (15)–(18), the error dynamics $\mathbf{e}$ for $a = 0$ and $\dot{\mathbf{e}}$ can be expressed as

$$\begin{cases} \dot{\mathbf{e}} = A\mathbf{e} + \begin{pmatrix} 0 \\ -xz + uw \\ xy - uv \end{pmatrix}, & t \neq t_k \\ \Delta\mathbf{e} = B_k\mathbf{e}, \; t = t_k, & k = 1, 2, \ldots \end{cases} \tag{19}$$

and in (20), shown at the bottom of the next page. Notice that the error dynamics $\mathbf{e}$ is uniformly equi-Lagrange stable provided that the matrices B_k, for all $k = 1, 2, \ldots$, are chosen to satisfy the conditions of Theorem 3, where $\mathbf{\Phi}(\mathbf{x}, \mathbf{u}(t)) = \mathbf{0}$, i.e., $\lim_{t\to\infty} \mathbf{e}(t) = \mathbf{0}$. By using a fourth-order Runge–Kutta method with step size 10^{-5}, Fig. 3 shows the error dynamics $\mathbf{e}$ in terms of its three components e_1, e_2 and e_3 converging to zero (for the rest of the paper, the first component of the error dynamics is represented by a solid curve, the second component is represented by a dashed curve and the third component is represented by a dashed-dotted curve). The values of parameters and initial conditions are chosen to be $\sigma = 10$, $r = 28$, $b = 8/3$, $\Delta_k = \Delta = 0.002$, $(x_0, y_0, z_0) = (1.12, -1, 0.5)$ and $(u_0, v_0, w_0) = (2.7, -2.1, 2.502)$. In fact, it was established in [9] that impulsive synchronization of systems $\mathbf{x}$ and $\mathbf{u}$ is quite robust even in the presence of relatively large parameter mismatch. In other words, (15) and (17) do not have to be identical in order to obtain good results for the uniform equi-Lagrange stability of system $\mathbf{e}$, as illustrated in Fig. 4, where we have 1% parameter mismatch. This property is very important since inaccuracy in designing identical chaotic systems is extremely unavoidable.

$$\begin{cases} \ddot{\mathbf{u}} = A\dot{\mathbf{u}} + \begin{pmatrix} 0 \\ -\dot{\tilde{u}}w - u\dot{\tilde{w}} \\ \dot{\tilde{u}}v + u\dot{\tilde{v}} \end{pmatrix} + q\begin{pmatrix} 0 \\ -\dot{\tilde{u}}m(t) - u\dot{m}(t) \\ 0 \end{pmatrix}, & t \neq t_k \\ \Delta\dot{\tilde{\mathbf{u}}} = -B_k\dot{\tilde{\mathbf{e}}}, \; t = t_k, & k = 1, 2, \ldots \end{cases} \tag{18}$$

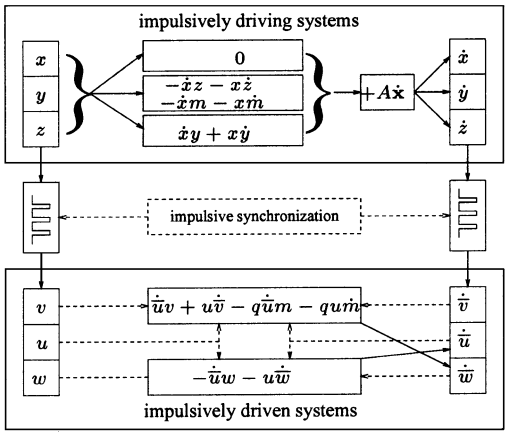


Fig. 2. Impulsive synchronization of two Lorenz chaotic systems.

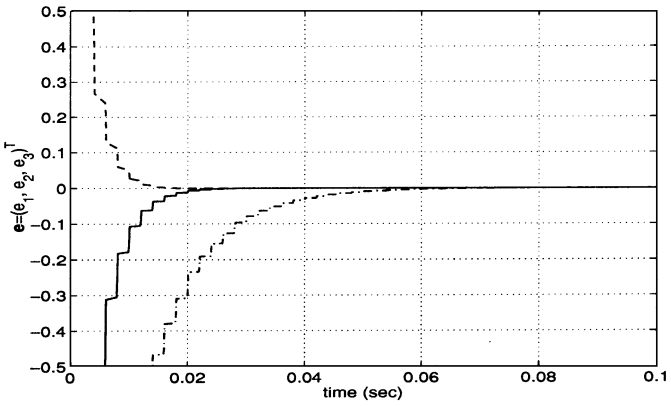


Fig. 3. Error dynamics $\mathbf{e}$ with 0% parameter mismatch and $B_k = -\text{diag}(0.02, 0.06, 0.01)$.

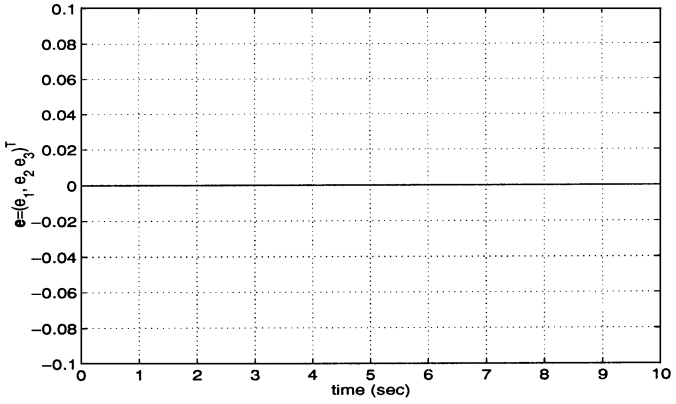


Fig. 4. Error dynamics $\mathbf{e}$ with 1% parameter mismatch and $B_k = -\text{diag}(0.5, 0.33, 0.2)$.

We shall now prove that system $\dot{\widetilde{\mathbf{e}}}$ is equi-Lagrange stable, which is to prove that (20) satisfies all the conditions described by Theorem 3. Let $\widetilde{\mathbf{e}} = (\mathbf{e}, \dot{\mathbf{e}})^T$ and choose $V(\widetilde{\mathbf{e}}) := \widetilde{\mathbf{e}}^T\widetilde{\mathbf{e}}$, then

$$\begin{aligned} D^+V(\widetilde{\mathbf{e}}) =& \dot{\widetilde{\mathbf{e}}}^T\widetilde{\mathbf{e}} + \widetilde{\mathbf{e}}^T\dot{\widetilde{\mathbf{e}}} \\ =& \left(\dot{\mathbf{e}}^T, \ddot{\mathbf{e}}^T\right)(\mathbf{e}, \dot{\mathbf{e}})^T + \left(\mathbf{e}^T, \dot{\mathbf{e}}^T\right)(\dot{\mathbf{e}}, \ddot{\mathbf{e}})^T \\ =& \dot{\mathbf{e}}^T\mathbf{e} + \ddot{\mathbf{e}}^T\dot{\mathbf{e}} + \mathbf{e}^T\dot{\mathbf{e}} + \dot{\mathbf{e}}^T\ddot{\mathbf{e}} \\ \le& 2L\|\mathbf{e}\|^2 + \dot{\mathbf{e}}^T\left(A^T + A\right)\dot{\mathbf{e}} \\ & - 2\left[(\dot{x}z - \dot{\bar{u}}w) + (x\dot{z} - u\dot{\bar{w}})\right]\dot{\bar{e}}_2 \\ & + 2\left[(\dot{x}y - \dot{\bar{u}}v) + (x\dot{y} - u\dot{\bar{v}})\right]\dot{\bar{e}}_3 \\ & - 2\left[(\dot{x} - q\dot{\bar{u}})m + (x - qu)\dot{m}\right]\dot{\bar{e}}_2 \end{aligned}$$

where $\dot{\mathbf{e}}^T\mathbf{e} \le L\|\mathbf{e}\|^2$, for some $L > 0$, which follows from (19). Note that $\dot{\widetilde{\mathbf{e}}}^T(A^T + A)\dot{\widetilde{\mathbf{e}}} \le d\,\dot{\widetilde{\mathbf{e}}}^T\dot{\widetilde{\mathbf{e}}}$, where d is the largest eigenvalue of $A^T + A$, as shown in the equations at the bottom of the next page. Thus, we may conclude that

$$\begin{aligned} D^+V(\widetilde{\mathbf{e}}) \le& [2L + d + 2|x| + 2|\dot{x}| + |v| \\ & + |w| + |\dot{\bar{v}}| + |\dot{\bar{w}}|]\|\widetilde{\mathbf{e}}\|^2 \\ & + \left[2K_1|\dot{x} - q\dot{\bar{u}}| + 2K_2|x - qu|\right]\|\widetilde{\mathbf{e}}\| \\ \le& \{2L + d + 2|x| + 2|\dot{x}| + |v| \\ & + |w| + |\dot{\bar{v}}| + |\dot{\bar{w}}| \\ & + 2K_1|\dot{x} - q\dot{\bar{u}}| + 2K_2|x - qu|\} \\ & \cdot \left[V(\widetilde{\mathbf{e}}) + V(\widetilde{\mathbf{e}})^{1/2}\right]. \end{aligned}$$

Thus, if the impulses of (20) are chosen to satisfy (12), then, for $q = 0$ and 1, it can be concluded that (20) is uniformly equi-bounded. Furthermore, if we let $q = 1$, then, the upper right derivative of $V(\widetilde{\mathbf{e}})$ will satisfy

$$\begin{aligned} D^+V(\widetilde{\mathbf{e}}) \le& [2L + d + 2|x| + 2|\dot{x}| + |v| + |w| \\ & + \left|\dot{\bar{v}}\right| + |\dot{\bar{w}}| + 2K_1 + 2K_2]\,V(\widetilde{\mathbf{e}}). \end{aligned}$$

This implies, by choosing $\gamma_k = 1/k$, for all $k = 1, 2, \ldots$, and applying Theorem 3, that solutions to system (20) are also equi-Lagrange stable, as desired. It should be further mentioned that if $m(t)$ exponentially decays in time, then, due to the properties of exponential functions, the convergence of $\dot{\widetilde{\mathbf{e}}}$ to zero becomes faster.

The following numerical examples are used to explain how uniform equi-Lagrange stability may be achieved by applying Theorem 3 and by employing the system described in Fig. 2. The parameters in the examples are $B_k = B = -\text{diag}(0.5, 0.6, 0.2)$, the period of the impulses $\Delta_k = \Delta = 0.002$, the initial conditions $(x_0, y_0, z_0) = (3.07, -2.37, 0.88)$, $(u_0, v_0, w_0) = (1.46, -1.87, 0.5)$ and

$$\begin{cases} \ddot{\widetilde{\mathbf{e}}} = A\dot{\widetilde{\mathbf{e}}} + \begin{pmatrix} 0 \\ -\dot{x}z + \dot{\bar{u}}w - x\dot{z} + u\dot{\bar{w}} \\ \dot{x}y - \dot{\bar{u}}v + x\dot{y} - u\dot{\bar{v}} \end{pmatrix} - \begin{pmatrix} 0 \\ (\dot{x} - q\dot{\bar{u}})m + (x - qu)\dot{m} \\ 0 \end{pmatrix}, & t \ne t_k \\ \Delta\dot{\widetilde{\mathbf{e}}} = B_k\dot{\widetilde{\mathbf{e}}},\ t = t_k, & k = 1, 2, \ldots \end{cases} \tag{20}$$

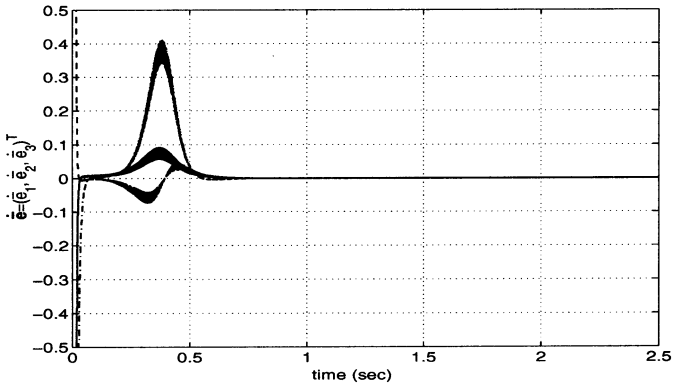


Fig. 5. Uniform equi-Lagrange stability of system (20), for $m(t) = 2\exp(-10t)\sin(4t)$.

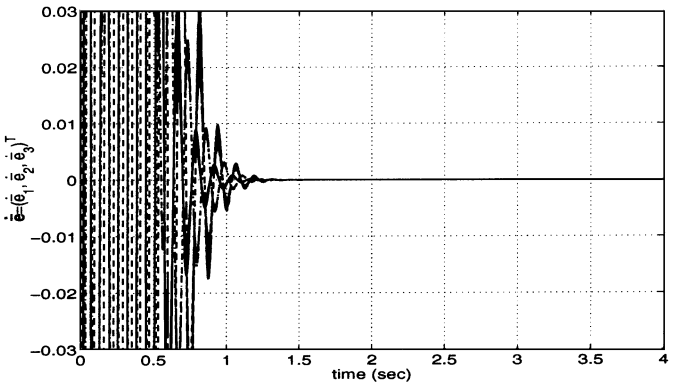


Fig. 6. Uniform equi-Lagrange stability of system (20), for $m(t) = 20\exp(-10t)\sin(50t)$.

$(\dot{\bar{u}}_0, \dot{\bar{v}}_0, \dot{\bar{w}}_0) = (3.9,\ 0.74, -1.62)$. In the following two examples a fourth-order Runge–Kutta method with step size 10^{-5} is used. In the first example, $m(t)$ has small upper bound and small frequency, whereas in the second example, $m(t)$ has large upper bound and large frequency. They are considered in order to show the performance of the system described in Fig. 2. For the first example, let $m(t) = 2\exp(-10t)\sin(4t)$. As shown in Fig. 5, the system converges to zero in 1.35 s. Note that the largest eigenvalue of B is 0.6 and it possesses all the required properties given in Theorem 3. For the second example, let $m(t) = 20\exp(-10t)\sin(50t)$, which possesses a relatively large amplitude and high frequency for short time t. Fig. 6 shows that the uniform equi-Lagrange stability is still achieved and the performance of the model is as desired. The conditions of Theorem 3 are satisfied by both the matrix B and system(20).

IV. Induced-Message Cryptosystem for Secure Communication

In the previous section, it has been demonstrated that the error dynamics $\mathbf{e}$ and $\dot{\bar{\mathbf{e}}}$, given by systems (19) and (20), are both uniformly equi-Lagrange stable, for $q = 1$ provided that the conditions of Theorem 3 are satisfied. In other words, $\lim_{t\to\infty}\mathbf{e}(t) = \lim_{t\to\infty}\dot{\bar{\mathbf{e}}}(t) = \mathbf{0}$, a property which is considered to be the cornerstone of several chaos-based secure communication schemes. We are interested in exploring the applications of this property in transmitting secret information between different parties. Fig. 7 shows a proposed cryptosystem consisting of a transmitter, a receiver and a public channel for communication. The transmitter and the receiver each contains a chaotic system, $\mathbf{x}$ and $\mathbf{u}$, respectively, to generate the encrypting key signals and to drive their derivative systems $\dot{\mathbf{x}}$ and $\dot{\bar{\mathbf{u}}}$, installed at the transmitter and the receiver ends, respectively. The system $\dot{\mathbf{x}}$ is used as the encryption block to

$$
\begin{aligned}
[(\dot{x}z - \dot{\bar{u}}w) + (x\dot{z} - u\dot{\bar{w}})]\dot{\bar{e}}_2 \le& |(\dot{x}z - \dot{\bar{u}}w) + (x\dot{z} - u\dot{\bar{w}})||\dot{\bar{e}}|_2 \\
=& |\dot{x}(z-w) + w(\dot{x} - \dot{\bar{u}}) + x(\dot{z} - \dot{\bar{w}}) + \dot{\bar{w}}(x-u)|\ |\dot{\bar{e}}_2| \\
=& |\dot{x}e_3 + w\dot{\bar{e}}_1 + x\dot{\bar{e}}_3 + \dot{\bar{w}}e_1|\ |\dot{\bar{e}}_2| \\
\le& |\dot{x}|\ |e_3\dot{\bar{e}}_2| + |w|\ |\dot{\bar{e}}_1\dot{\bar{e}}_2| + |x|\ |\dot{\bar{e}}_3\dot{\bar{e}}_2| + |\dot{\bar{w}}|\ |e_1\dot{\bar{e}}_2| \\
\le& |\dot{x}|\ ||\mathbf{e}||\ ||\dot{\bar{\mathbf{e}}}|| + \frac{1}{2}|w|\ ||\dot{\bar{\mathbf{e}}}||^2 + \frac{1}{2}|x|\ ||\dot{\bar{\mathbf{e}}}||^2 + |\dot{\bar{w}}|\ ||\mathbf{e}||\ ||\dot{\bar{\mathbf{e}}}|| \\
\le& \frac{1}{2}(|\dot{x}| + |w| + |x| + |\dot{\bar{w}}|)||\widetilde{\mathbf{e}}||^2 \\
[(\dot{x}y - \dot{\bar{u}}v) + (x\dot{y} - u\dot{\bar{v}})]\dot{\bar{e}}_3 \le& |(\dot{x}y - \dot{\bar{u}}v) + (x\dot{y} - u\dot{\bar{v}})|\ |\dot{\bar{e}}_3| \\
=& |\dot{x}(y-v) + v(\dot{x} - \dot{\bar{u}}) + x(\dot{y} - \dot{\bar{v}}) + \dot{\bar{v}}(x-u)|\ |\dot{\bar{e}}_3| \\
=& |\dot{x}e_2 + v\dot{\bar{e}}_1 + x\dot{\bar{e}}_2 + \dot{\bar{v}}e_1|\ |\dot{\bar{e}}_3| \\
\le& |\dot{x}|\ |e_2\dot{\bar{e}}_3| + |v|\ |\dot{\bar{e}}_1\dot{\bar{e}}_3| + |x|\ |\dot{\bar{e}}_2\dot{\bar{e}}_3| + |\dot{\bar{v}}|\ |e_1\dot{\bar{e}}_3| \\
\le& |\dot{x}|\ ||\mathbf{e}||\ ||\dot{\bar{\mathbf{e}}}|| + \frac{1}{2}|v|\ ||\dot{\bar{\mathbf{e}}}||^2 + \frac{1}{2}|x|\ ||\dot{\bar{\mathbf{e}}}||^2 + |\dot{\bar{v}}|\ ||\mathbf{e}||\ ||\dot{\bar{\mathbf{e}}}|| \\
\le& \frac{1}{2}(|\dot{x}| + |v| + |x| + |\dot{\bar{v}}|)||\widetilde{\mathbf{e}}||^2 \\
[(\dot{x} - q\dot{\bar{u}})m + (x - qu)\dot{m}]\dot{\bar{e}}_2 \le& |(\dot{x} - q\dot{\bar{u}})m + (x - qu)\dot{m}||\dot{\bar{\mathbf{e}}}|| \\
\le& \left[K_1|\dot{x} - q\dot{\bar{u}}| + K_2|x - qu|\right]||\widetilde{\mathbf{e}}||
\end{aligned}
$$

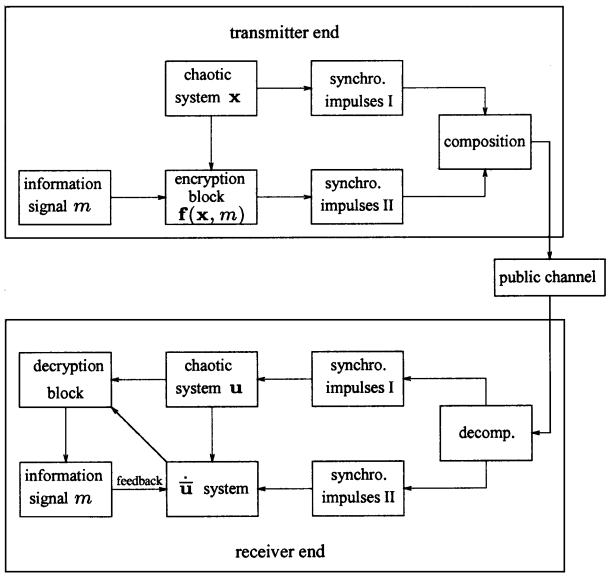


Fig. 7. Induced-message cryptosystem.

encrypt the information signal $f(t)$ at the transmitter end. In addition, the transmitter and the receiver each contains two synchronization impulses blocks. The first block is used to synchronize $\mathbf{u}$ with $\mathbf{x}$ and the other is used to synchronize $\dot{\overline{\mathbf{u}}}$ with $\dot{\mathbf{x}}$. The transmitter contains a composition block which combines the synchronization impulses from the two synchronization impulses blocks. This combining is done through time frames each of which has length $2Q$ s. The first Q s are loaded with the impulses to synchronize $\mathbf{x}$ and $\mathbf{u}$, whereas the second Q s are loaded with the impulses needed to synchronize $\dot{\mathbf{x}}$ and $\dot{\overline{\mathbf{u}}}$. These time frames are sent across the public channel and are decomposed at the decomposition block at the receiver end into two Q s. The first Q s are fed into the system $\mathbf{u}$, to recover the key signals and the second Q s are fed into the system $\dot{\overline{\mathbf{u}}}$, to induce the encrypted signal. At the decryption block, the recovered key signals are used to decrypt the induced encrypted information signal by applying the inverse of $\mathbf{f}$, $\mathbf{f}^{-1}$. Then, the decrypted signal $m(t)$ is fed back into the block $\dot{\overline{\mathbf{u}}}$ for better and faster recovery.

Impulsive synchronization can be achieved for the system in Fig. 7 even in the presence of parameter mismatch between chaotic systems involved, i.e., impulsive synchronization is very robust. Therefore, the two chaotic systems $\mathbf{x}$ and $\mathbf{u}$ can be taken to be nonidentical, and still obtain very good synchronization results. Furthermore, the encryption–decryption process of the above model may be described as follows. The encryption block at the transmitter end applies conventional cryptographic techniques to the information signal $f(t)$ to formulate the encrypted signal $\mathbf{f}(\mathbf{x}, m(t), 1)$, where $m(t) = f(t)\exp(-\theta t)$, for some chosen $\theta > 0$, as described in (16). Thus, the complexity of the encryption is increased. However, at the receiver end the chaotic system $\dot{\overline{\mathbf{u}}}$ is installed to synchronize with the system $\dot{\mathbf{x}}$ through applying impulses generated by the system $\dot{\mathbf{x}}$. Meanwhile, the system $\dot{\overline{\mathbf{u}}}$ is self-generated and driven by the components of $\mathbf{u}$ and the decrypted signal $m(t)$, by applying message feedback, so that it will have a formulation identical to the system $\dot{\mathbf{x}}$ in order for both to impulsively synchronize. By Theorem 3, the error dynamics $\dot{\overline{\mathbf{e}}}$, given by system (20), is uniformly equi-Lagrange stable. It should be noted that impulsive synchronization still works for an arbitrary mapping $\mathbf{h} \neq \mathbf{f}$ and, thus, the complexity of the encryption process of the information signal can be increased by increasing the complexity and the nonlinearity of $\mathbf{h}$. However, by choosing $\mathbf{h} \neq \mathbf{f}$, the transmission of the information signal to the receiver end requires two sequences of synchronizing impulses in addition to the sequence of impulses needed to recover the key signals (i.e., a total of three sequences for a complete recovery). This is unlike when $\mathbf{h} = \mathbf{f}$, which requires only one sequence to induce the encrypted signal. In addition, upon choosing $\mathbf{h} \neq \mathbf{f}$, we need to consider the total derivative of $\mathbf{h}$ with respect to t when formulating the system $\overline{\mathbf{x}}$. In other words, the encryption block at the transmitter end will involve the system

$$\dot{\overline{\mathbf{x}}} = \frac{\partial \mathbf{h}}{\partial t}(\mathbf{x}, m(t)).$$

It can be seen that the keys and the encrypted signal are not sent across the public channel. They are embedded inside the impulses and then induced at the receiver end using the impulses. The new system is also called the induced-message cryptosystem.

One advantage of the induced-message cryptosystem is that it may overcome the problem arising from the time-frame congestion in impulsive cryptosystems presented in [4], [6], [8], and [18]. In those impulsive cryptosystems, the transmitted signal consists of a sequence of time frames, each of which has a length of T s and is made up of two regions. The first region is the synchronization region of length Q s. It consists of the synchronization impulses needed to impulsively synchronize the two chaotic systems in both the transmitter and receiver. The second region contains the encrypted message signal and has a length of $T - Q$ s. Since Q is taken to be small compared to T, the loss of time in packing message signals is negligible [28]. The first experimental results on impulsive synchronization were presented in [18]. In the experiment, two Chua's oscillators were effectively synchronized by using narrow impulses ($Q/T = 0.16\%$, $1/T = 18$ kHz). It was found in [4], [6], and [8] that the minimum length of the interval Q increases in proportion to the frame length as it increases. In fact, it was experimentally established that for 5×10^{-5} s $\leq T \leq 5 \times 10^{-3}$ s, the ratio $Q/T \geq 50\%$ can achieve almost-identical synchronization and thus the lost time in packing the message signals is no more negligible. It was further realized that the situation becomes worse when implementing hyperchaotic systems where two impulsive synchronization regions (each of which is of length Q) are required for almost-identical synchronization (e.g., for 1.3×10^{-5} s $\leq T \leq 2 \times 10^{-5}$ s, $2Q/T = 100\%$). Therefore, it is more desirable to eliminate this problem by not transmitting the encrypted signal in the first place. We have shown that, in the induced-message cryptosystem proposed above, we are able to accomplish this property of not transmitting the encrypted signal. Instead, two sequences of synchronizing impulses are transmitted only. One sequence is needed to recover the key signals and the other sequence is required to induce the encrypted

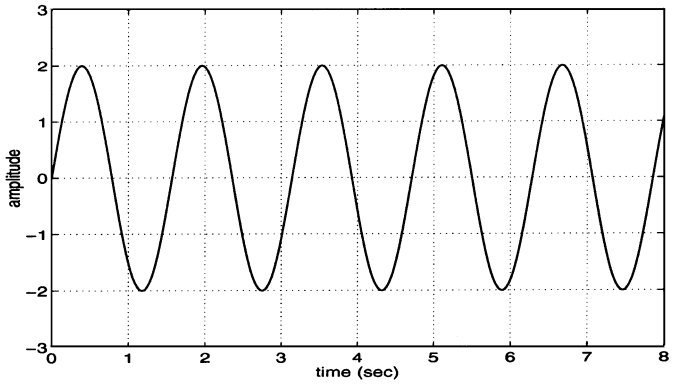


Fig. 8. Original message $f(t) = 2\sin(4t)$ before encryption.

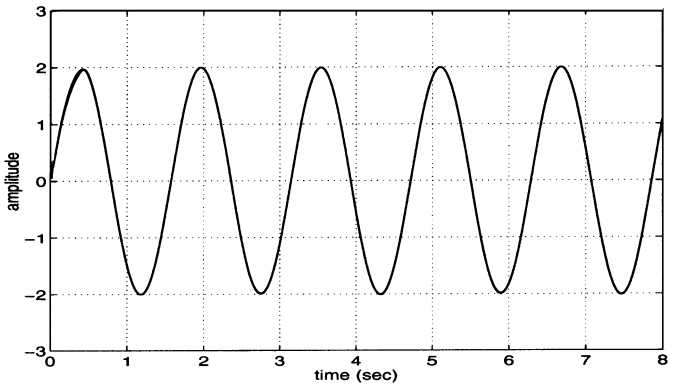


Fig. 9. Decrypted message $f(t) = 2\sin(4t)$.

signal. Thus, we reach the objective of increasing the security of the impulsive cryptosystem and prevent the frames from being congested by the synchronization region.

V. Simulation Results and Discussions

In the following simulations, a fourth-order Runge–Kutta method with step size 10^{-5} is used. The system parameters are $\sigma = 10,\ r = 28, b = 8/3, B_k = B = -\text{diag}(0.5, 0.6, 0.2)$, the period of the impulses is $\Delta_k = \Delta = 0.002$ and the initial conditions are $(x_0, y_0, z_0) = (3.07, -2.37, 0.88)$, $(u_0, v_0, w_0) = (1.46, -1.87, 0.5)$ and $(\dot{\overline{u}}_0, \dot{\overline{v}}_0, \dot{\overline{w}}_0) = (3.9,\ 0.74, -1.62)$. In the first example, the information signal $f(t) = 2\sin(4t)$, which has large amplitude and low frequency, as shown in Fig. 8, is considered. In this case $m(t) = 2\sin(4t)\exp(-\theta t)$, where θ is taken to be 1. The encryption process is identical to the one described in Fig. 2. i.e.,

$$\mathbf{h}(\mathbf{x}, m(t)) = \mathbf{f}(\mathbf{x}, m(t), 1)$$

given by (15). With the arguments in the previous section and in this section, we know that $\mathbf{u} \to \mathbf{x}$ and $\dot{\overline{\mathbf{u}}} \to \dot{\mathbf{x}}$. Therefore, the key signals x, y and z can be recovered by obtaining the signals u, v and w. Moreover, with the process of feeding back the decrypted message $m(t)$ into the system $\dot{\overline{\mathbf{u}}}$, the state variable $\dot{\overline{v}} \to \dot{y} = rx - y - (z + m(t))x$, which will allow $m(t)$ to be recovered by simply using the following operation:

$$m(t) \approx -\left[w + \frac{\dot{\overline{v}} - ru + v}{u}\right].$$

Then, $f(t)$ can be obtained by $f(t) = m(t)\exp(\theta t)$. Fig. 9 shows the result of the decryption process of the induced message $f(t) = 2\sin(4t)$ and Fig. 12 shows the error between the original message and the decrypted message decaying exponentially with time. Now, considering another type of information signal with low amplitude and very high frequency, such as $f(t) = 0.02\sin(t)\sin(100t)$, similar results are obtained as shown in Figs. 10 and 11.

It should be mentioned that the parameter θ has a very significant role in the dynamics of the induced-message cryptosystem. Increasing the value of this parameter will increase the accuracy of the decryption process and decrease the error between the real information signal and the induced one. In other words, the larger the values of θ, the faster the convergence and the

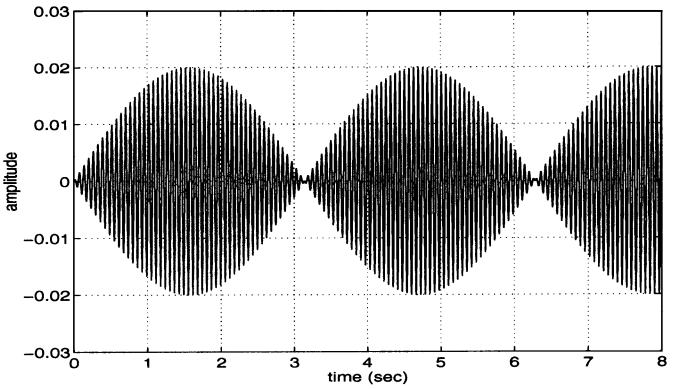


Fig. 10. Original message $f(t) = 0.02\sin(t)\sin(100t)$ before encryption.

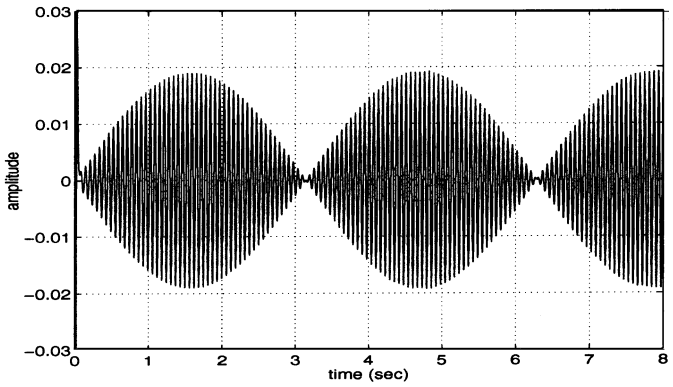


Fig. 11. Decrypted message $f(t) = 0.02\sin(t)\sin(100t)$.

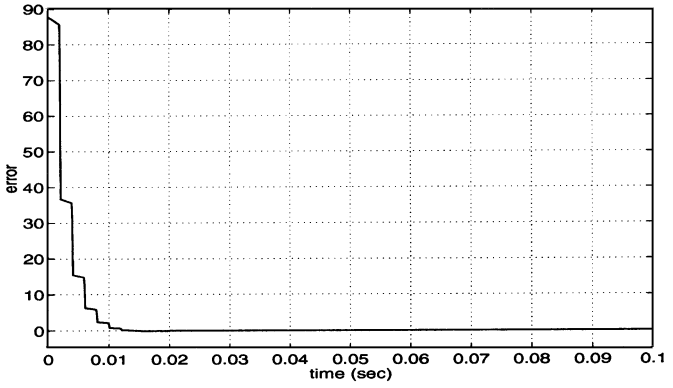


Fig. 12. Exponential decay of the error between original and decrypted messages.

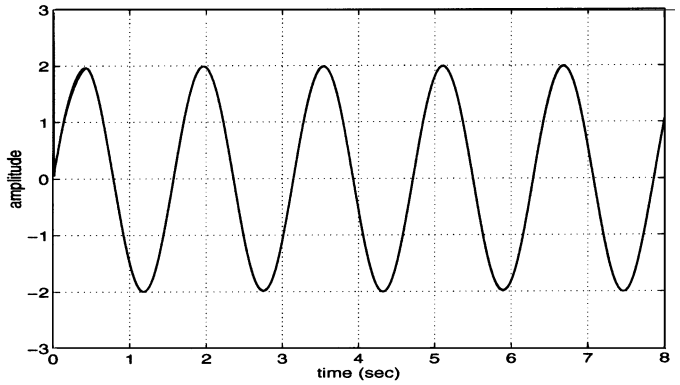


Fig. 13. Accurate decryption of the message $f(t) = 2\sin(4t)$ for $\theta = 0$.

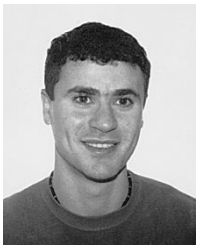
smaller the error. However, due to the software numerical integration errors, the decryption of the information signals may not be successful. This is due to that, for large θ, $\exp(-\theta t)$ is driven to zero very fast with time and the information signal may be lost. Therefore, the parameter θ has been chosen to be relatively small in the numerical integration process to recover the information signal. Fig. 13 shows that even with $\theta = 0$ and without message feedback, the message signal $f(t) = 2\sin(4t)$ can still be accurately recovered. This also indicates that the induced-message cryptosystem is very robust.

VI. Conclusion

We have developed an induced-message cryptosystem for secure communication. The cryptosystem induces the key signals and the encrypted information signal at the receiver end without transmitting them across public channels. Therefore, the system increases the security of information signals. In addition, the system also overcomes the time-frame-congestion problem described in several existing impulsive cryptosystems.

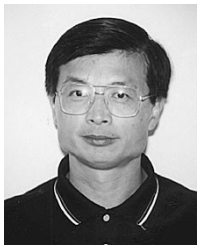
References

[1] G. Ballinger and X. Z. Liu, "On boundedness of solutions of impulsive systems," *Nonlin. Stud.*, vol. 4, no. 1, pp. 121–131, 1997.
[2] K. M. Cuomo and A. Oppenheim, "Chaotic signals and systems for communications," in *Proc. IEEE Int. Conf. Acoustics, and Speech, Signal Processing*, vol. 3, Apr. 1993, pp. 137–140.
[3] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation Chaos*, vol. 3, no. 2, pp. 469–477, 1993.
[4] M. Itoh, "Experimental study of impulsive synchronization," in *Proc. 1999 IEEE Int. Symp. Circuits Systems*, Orlando, FL, 1999, pp. 410–413.
[5] M. Itoh and H. Murakami, "New communication systems via chaotic synchronizations and modulations," *IEICE Trans. Fund.*, vol. E78-A, no. 3, pp. 285–290, 1995.
[6] M. Itoh, T. Yang, and L. O. Chua, "Experimental study of impulsive synchronization of chaotic and hyperchaotic circuits," *Int. J. Bifurcation Chaos*, vol. 9, no. 7, pp. 1393–1424, 1999.
[7] ——, "Conditions for impulsive synchronization of chaotic and hyperchaotic systems," *Int. J. Bifurcation Chaos*, vol. 11, no. 2, pp. 551–560, 2001.
[8] M. Itoh, N. Yamamoto, T. Yang, and L. O. Chua, "Performance analysis of impulsive synchronization," in *Proc. 1999 Eur. Conf. Circuit Theory and Design*, 1999, pp. 353–356.
[9] A. Khadra, X. Z. Liu, and X. Shen, "Robust impulsive synchronization and its application to communication security," *Int. J. Dyn. Continuous Discr. Impulsive Syst.*, vol. 10, pp. 403–416, 2003.
[10] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, no. 3, pp. 709–713, 1992.
[11] V. Lakshmikantham, D. D. Bainov, and P. S. Simeonov, *Theory of Impulsive Differential Equations*, Singapore: World Scientific, 1989.
[12] V. Lakshmikantham and X. Z. Liu, *Stability Analysis in Terms of Two Measures*, Singapore: World Scientific, 1993.
[13] Z. G. Li, C. Y. Wen, Y. C. Soh, and W. X. Xie, "The stabilization and synchronization of Chua's oscillators via impulsive control," *IEEE Trans. Circuits and Syst. I*, vol. 48, pp. 1351–1355, Nov. 2001.
[14] X. Z. Liu, "Stability results for impulsive differential systems with applications to population growth models," *Dyna. Stability Syst.*, vol. 9, no. 2, pp. 163–174, 1994.
[15] ——, "Impulsive stabilization and control of chaotic systems," *Non-Lin. Anal.*, vol. 47, pp. 1081–1092, 2001.
[16] X. Z. Liu and G. Ballinger, "On boundedness of solutions of impulsive systems in terms of two measures," *Non-Lin. World*, vol. 4, pp. 417–434, 1997.
[17] X. Z. Liu and A. R. Willms, "Impulsive controllability of linear dynamical systems with applications to maneuvers of spacecraft," *Math. Prob. Eng.*, vol. 2, pp. 277–299, 1996.
[18] A. I. Panas, T. Yang, and L. O. Chua, "Experimental results of impulsive synchronization between two Chua's circuits," *Int. J. Bifurcation Chaos*, vol. 8, no. 3, pp. 639–644, 1998.
[19] U. Parlitz and S. Ergezinger, "Robust communication based on chaotic spreading sequences," *Phys. Lett. A*, vol. 188, pp. 146–150, 1994.
[20] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.
[21] T. Stojanovski, L. Kocarev, and U. Parlitz, "Driving and synchronizing by chaotic impulses," *Phys. Rev. E*, vol. 43, no. 9, pp. 782–785, 1996.
[22] J. A. Suykens, P. F. Curran, and L. O. Chua, "Robust synthesis for master-slave synchronization of Lur'e systems," *IEEE Trans. Circuits Syst. I*, vol. 46, pp. 841–850, July 1999.
[23] J. A. Suykens, P. F. Curran, J. Vandewalle, and L. O. Chua, "Robust nonlinear H_∞ synchronization of chaotic Lur'e systems," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 891–904, Oct. 1997.
[24] J. A. Suykens, T. Yang, and L. O. Chua, "Impulsive synchronization of chaotic Lur'e systems by measurement feedback," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1371–1381, 1998.
[25] T. Yang, *Impulsive Control Theory*. Berlin, Germany: Spinger-Verlag, 2001, vol. 272.
[26] ——, *Impulsive Systems and Control: Theory and Applications*. Huntington, NY: Nova Science, 2001.
[27] T. Yang and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 976–988, Oct. 1997.
[28] ——, "Impulsive control and synchronization of nonlinear dynamical systems and application to secure communication," *Int. J. Bifurcation Chaos*, vol. 7, no. 3, pp. 645–664, 1997.
[29] ——, "Generalized synchronization of chaos via linear transformations," *Int. J. Bifurcation Chaos*, vol. 9, no. 1, pp. 215–219, 1999.
[30] T. Yang, J. A. Suykens, and L. O. Chua, "Impulsive control of nonautonomous chaotic systems using practical stabilization," *Int. J. Bifurcation Chaos*, vol. 8, no. 7, pp. 1557–1564, 1998.
[31] T. Yang, C. M. Yang, and L. B. Yang, "Control of Rössler system to periodic motions using impulsive control methods," *Phys. Lett. A*, vol. 232, pp. 356–361, 1997.
[32] T. Yang, L. B. Yang, and C. M. Yang, "Impulsive control of Lorenz system," *Phys. D*, vol. 110, pp. 18–24, 1997.



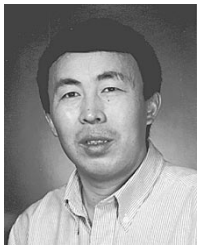
Anmar Khadra received the B.Sc. degree in pure mathematics (honors) with distinction from Concordia University, Montreal, QC, Canada, in 1997, and the M.Math degree in applied mathematics from the University of Waterloo, Waterloo, ON, Canada, in 1999, where he is currently working toward the Ph.D. degree in applied mathematics/electrical engineering.

His research interests are dynamical systems and communication security, in particular, stability theory, impulsive control, nonlinear systems, chaos theory, delayed impulsive systems, and cryptography.



Xinzhi Liu received the B.Sc. degree from Shandong Normal University, Jinan, China, in 1982, and the M.Sc. and Ph.D. degrees from University of Texas, Arlington, in 1987 and 1988, respectively, all in mathematics.

He was a Post-Doctoral Fellow at the University of Alberta, Edmonton, AB, Canada, from 1988 to 1990. He joined the Department of Applied Mathematics,University of Waterloo, Waterloo, ON, Canada, in 1990, where he became an 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 120 research articles and two research monographs and three other books. He is the Chief Editor of the journal, *Dynamics of Continuous, Discrete and Impulsive Systems* and Associate Editor of four other journals.



Xuemin (Sherman) Shen (M'97–SM'02) received the B.Sc. degree, from Dalian Marine University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees from Rutgers University, New Brunswick, NJ, in 1987 and 1990, respectively, all in electrical engineering.

From September 1990 to September 1993, he was first with Howard University, Washington, DC, and then University of Alberta, Edmonton, AB, Canada. Since October 1993, he has been with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, where he is an Associate Professor. His research focuses on mobility and resource management in interconnected wireless/wireline networks. Specifically, his interests are traffic-flow control, connection admission and access control, handoff, user location estimation, end-to-end performance modeling and evaluation, voice over mobile IP, stochastic process and H_∞ filtering. He is a coauthor of two books and has many publications in communications networks, control and filtering.

Dr. Shen is a Registered Professional Engineer, in the Province of Ontario, Canada.