Dynamics of Continuous, Discrete and Impulsive Systems
Series **B:** *Applications & Algorithms* **10 (2003)** 403-416

ROBUST IMPULSIVE SYNCHRONIZATION AND APPLICATION TO COMMUNICATION SECURITY

Anmar Khadra[1], Xinzhi Liu[1] and Xuemin Shen[2]

[1]Department of Applied Mathematics
University of Waterloo, Waterloo, Ontario N2L 3G1
[2]Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario N2L 3G1

Abstract. Criteria on uniform equi-boundedness and uniform equi-Lagrange stability of a certain type of impulsive systems have been investigated. These criteria are applied to impulsively synchronize two Lorenz chaotic systems and show how parameter mismatch between them play a fundamental role in influencing system performance. A robust secure communication scheme based on masking and modulating message signals with impulsive synchronization is then proposed. Simulation results are presented to demonstrate the secure scheme.

Keywords. Impulsive systems, equi-boundedness, equi-Lagrange stability, impulsive synchronization, robustness.

1 Introduction

Impulsive systems provide a natural framework for mathematical modeling of many physical phenomena. Examples of such models include some population growth models [9] and maneuvers of spacecraft [12]. In this paper, we are interested in impulsive synchronization of two chaotic systems [10, 14, 19]. This feature was simultaneously investigated for both autonomous and non-autonomous error dynamics between the chaotic systems involved [18]. In addition, a more general format of it was also introduced in [17] using the notion of practical stability. Applications of the feature to communication security was found to be very promising [15, 16]. Since then, many theoretical and experimental studies have been conducted in this field, especially in solving problems arising from the transmission processes of the encrypted signals [4, 5, 6, 7, 13]. However, the problem of robustness has not been addressed in a comprehensible way.

Inaccuracy in designing identical chaotic systems is unavoidable and the robustness of cryptosystems in building a secure communication scheme is considered fundamentally important. Therefore we study impulsive synchronization and its insensitivity to relatively large parameter mismatch between two chaotic systems. In addition, we characterize robustness in terms of equi-Lagrange stability [8] and apply it to design a new secure communication scheme

The rest of this paper is organized as follows. In Section 2, we state and prove several results concerning equi-boundedness and equi-Lagrange stability. These results are required to obtain sufficient conditions for impulsive synchronization of two chaotic systems. In Section 3, an example consisting of two non-identical Lorenz systems is considered in order to show the robustness of impulsive synchronization of these two systems. A new secure scheme based on chaotic masking [2] and chaotic modulation [3] in proposed in Section 4, followed by concluding remarks in Section 5.

2 Basic Theory

Consider the following impulsive 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 $\Delta\mathbf{x}(t_k) = \mathbf{x}(t_k^+) - \mathbf{x}(t_k^-)$, $\mathbf{x}(t_k^+) = \lim_{t \to t_k^+} \mathbf{x}(t)$, and the moments of impulse satisfy $0 = t_1 < t_2 < \ldots < t_k < \ldots$ and $\lim_{k\to\infty} t_k = \infty$. Furthermore, we introduce the following classes of functions for later use.
$\mathcal{K}_0 := \{g \in C[\mathbb{R}_+, \mathbb{R}_+] : g(s) > 0 \text{ if } s > 0 \text{ and } g(0) = 0\}$, $\mathcal{K} := \{g \in \mathcal{K}_0 : g(s) \text{ is strictly increasing in } s\}$, $\mathcal{KR} := \{g \in \mathcal{K} : \lim_{s\to\infty} g(s) = \infty\}$,
$\mathcal{PC} := \{p : \mathbb{R}_+ \to \mathbb{R}_+ : p(t) \in C((t_k, t_{k+1}]) \text{ and } p(t_k^+) \text{ exists},\ k = 1, 2, \ldots\}$,
$S^c(M) := \{\mathbf{x} \in \mathbb{R}^n : ||\mathbf{x}|| \geq M\}$, $S^c(M)^0 := \{\mathbf{x} \in \mathbb{R}^n : ||\mathbf{x}|| > M\}$,
$\nu_0(M) := \{V : \mathbb{R}_+ \times S^c(M) \to \mathbb{R}_+ : V(t,\mathbf{x}) \in C((t_k, t_{k+1}] \times S^c(M))$, locally Lipschitz in $\mathbf{x}$ and $V(t_k^+, \mathbf{x})$ exists for $k = 1, 2, \ldots\}$,
where $M \geq 0$. We also introduce 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*

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

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) uniformly equi-Lagrange stable *if (S2) and (B2) hold together.*

We shall need the following Theorem [1, 11].

Theorem 1 *The solutions of system (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*

$$D^+V(t, \mathbf{x}) \leq p(t)c_k(V(t, \mathbf{x})),\ (t, \mathbf{x}) \in (t_k, t_{k+1}) \times S^c(M)^0, \qquad (2)$$

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*

$$V(t_k^+, \mathbf{x} + \mathbf{I}(t_k, \mathbf{x})) \leq \Psi_k(V(t_k, \mathbf{x})), \qquad (3)$$

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*

$$\int_{t_k}^{t_{k+1}} p(s)ds + \int_{y}^{\Psi_k(y)} \frac{ds}{c_k(s)} \leq -\gamma_k, \qquad (4)$$

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

The next result is on equi-Lagrange stability.

Theorem 2 *The solutions of system (1) are equi-Lagrange stable if*

(T2.1) system (1) is equi-bounded;

(T2.2) condition (T1.2) holds for $V \in \nu_0(0)$ *with inequality (2) 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 (3) holds, for all* $(t_k, \mathbf{x}) \in \mathbb{R}_+ \times \mathbb{R}^n$ *and for all* $k = 1, 2, \ldots$;

(T2.4) there exist a constant $\rho > 0$ *and functions* $C_k \in \mathcal{K}$ *such that* $C_k(s) \leq c_k(s)$ *and* $C_k(s) > \rho > 0$, *for all* $s \in \mathbb{R}_+$ *and for all* $k = 1, 2, \ldots$;

(T2.5) inequality (4) holds, for all $y > 0$, *and* $\sum_{k=1}^{\infty} \gamma_k = \infty$.

Proof: To prove equi-Lagrange stability, we need to show that system (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 $\mathbf{x}(t_0) = \mathbf{x}_0$. Since 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 (2) and (3), we have

$$\left\{ \begin{array}{rcl} D^+ m(t) & \leq & p(t) c_k(m(t)), \ t \neq t_k \\ m(t_k^+) & \leq & \Psi_k(m(t_k)), \ k = 1, 2, \dots. \end{array} \right. \tag{5}$$

Using (5), we obtain

$$\int\limits_{m(t_k^+)}^{m(t)} \frac{ds}{c_k(s)} \leq \int\limits_{t_k}^{t} p(s) ds \leq \int\limits_{t_k}^{t_{k+1}} p(s) ds, \ t \in (t_k, t_{k+1}], \tag{6}$$

and

$$\int\limits_{m(t_k)}^{m(t_k^+)} \frac{ds}{c_k(s)} \leq \int\limits_{m(t_k)}^{\Psi_k(m(t_k))} \frac{ds}{c_k(s)}. \tag{7}$$

Adding (6) and (7), we get, in view of (4),

$$\int\limits_{m(t_k)}^{m(t)} \frac{ds}{c_k(s)} \leq \int\limits_{t_k}^{t_{k+1}} p(s) ds + \int\limits_{m(t_k)}^{\Psi_k(m(t_k))} \frac{ds}{c_k(s)} \leq -\gamma_k. \tag{8}$$

With inequality (8), we conclude that $m(t) \leq m(t_k)$, for all $t \in (t_k, t_{k+1}]$, i.e., $m(t_{k+1}) \leq m(t_k)$. This means that the sequence $\{m(t_k)\}_{k=1}^{\infty}$ is non-increasing. 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 $k = 1, 2, \dots$, we obtain

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

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

$$\begin{array}{rcl} m(t_{n+1}) - m(t_1) & = & m(t_{n+1}) - m(t_n) + m(t_n) - \dots + m(t_2) - m(t_1) \\ & \leq & \int\limits_{m(t_n)}^{m(t_{n+1})} \frac{C_n(\mathcal{L})}{c_n(s)} ds + \dots + \int\limits_{m(t_1)}^{m(t_2)} \frac{C_1(\mathcal{L})}{c_1(s)} ds \\ & \leq & -\gamma_n C_n(\mathcal{L}) - \gamma_{n-1} C_{n-1}(\mathcal{L}) - \dots - \gamma_1 C_1(\mathcal{L}) \\ & = & -\sum\limits_{k=1}^{n} \gamma_k C_k(\mathcal{L}). \end{array}$$

This implies, by conditions (T2.4) and (T2.5), that

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

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

Now in order to apply the above theorems, we shall consider the following system.

$$\left\{ \begin{array}{rcl} \dot{\mathbf{x}} &=& A(t)\mathbf{x} + \mathbf{g}(\mathbf{x}) + \mathbf{\Phi}(\mathbf{u}(t)), \ t \neq t_k \\ \Delta\mathbf{x} &=& B_k\mathbf{x}, \ t = t_k, \ k = 1, 2, \ldots, \end{array} \right. \tag{9}$$

where $A(t) = (a_{ij}(t))$ is an $n \times n$ continuous functional matrix, $\mathbf{g}$ and $\mathbf{\Phi}$ are continuous non-linear maps satisfying $||\mathbf{g}(\mathbf{x})|| \leq L_1||\mathbf{x}||$ and $||\mathbf{\Phi}(\mathbf{u}(t))|| \leq L_2||\mathbf{u}(t)||$, for some constants $L_1, L_2 > 0$, $\mathbf{u}(t)$ is an arbitrary bounded control function and B_k are $n \times n$ constant matrices for all $k = 1, 2, \ldots$.

Theorem 3 *Solutions to system (9) are uniformly equi-bounded if the largest eigenvalue of $(I + B_k^T)(I + B_k)$, denoted by λ_k, satisfies*

$$\lambda_k \leq \exp(-2\alpha_k), \tag{10}$$

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

$$\ell_k = \sup_{t \in (t_k, t_{k+1}]} p(t),$$

$$p(t) = \max_{t \in \mathbb{R}_+} \{f(t) + 2L_1, 2L_2||\mathbf{u}(t)||\}$$

and

$$f(t) = \max_{1 \leq i \leq n} \left\{ |q_{ii}(t)| + \frac{1}{2}\sum_{\substack{l=1 \\ l \neq i}}^{n} |q_{il}(t)| + \frac{1}{2}\sum_{\substack{j=1 \\ j \neq i}}^{n} |q_{ji}(t)| \right\},$$

where $q_{ij} := a_{ij} + a_{ji}$. Moreover, if $\gamma_k = 1/k$, for all $k = 1, 2, \ldots$ and $\mathbf{\Phi}(\mathbf{u}(t)) = \mathbf{0}$, then system (9) is uniformly equi-Lagrange stable.

Proof: We shall first prove that system (9) is uniformly equi-bounded by achieving the conditions of Theorem 1. 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

$$D^+V(\mathbf{x}) = \mathbf{x}^TQ(t)\mathbf{x} + [\mathbf{x}^T\mathbf{g}(\mathbf{x}) + \mathbf{g}(\mathbf{x})^T\mathbf{x}] + [\mathbf{x}^T\mathbf{\Phi}(\mathbf{u}(t)) + \mathbf{\Phi}(\mathbf{u}(t))^T\mathbf{x}],$$

where $Q(t) = (q_{ij}(t)) := A(t)^T + A(t)$ is a symmetric matrix. Notice that

$$\begin{aligned}
\mathbf{x}^TQ(t)\mathbf{x} &= \sum_{i,j=1}^{n} q_{ij}(t)x_ix_j = \sum_{i=1}^{n} q_{ii}(t)x_i^2 + \sum_{i=1}^{n}\sum_{\substack{j=1\\ i\neq j}}^{n} q_{ij}(t)x_ix_j \\
&\leq \sum_{i=1}^{n} |q_{ii}(t)|x_i^2 + \sum_{i=1}^{n}\sum_{\substack{j=1\\ i\neq j}}^{n} |q_{ij}(t)||x_ix_j| \\
&\leq \sum_{i=1}^{n} |q_{ii}(t)|x_i^2 + \sum_{\substack{i,j=1\\ i\neq j}}^{n} \frac{|q_{ij}(t)|}{2}\left[x_i^2 + x_j^2\right] \\
&= \sum_{i=1}^{n}\left[|q_{ii}|(t) + \frac{1}{2}\sum_{\substack{j=1\\ j\neq i}}^{n}|q_{ij}(t)|\right]x_i^2 + \frac{1}{2}\sum_{j=1}^{n}\left[\sum_{\substack{i=1\\ i\neq j}}^{n}|q_{ij}(t)|\right]x_j^2 \\
&= \sum_{i=1}^{n}\left\{|q_{ii}(t)| + \frac{1}{2}\sum_{\substack{l=1\\ l\neq i}}^{n}|q_{il}(t)| + \frac{1}{2}\sum_{\substack{j=1\\ j\neq i}}^{n}|q_{ji}(t)|\right\}x_i^2 \\
&\leq \max_{1\leq i\leq n}\left\{|q_{ii}(t)| + \frac{1}{2}\sum_{\substack{l=1\\ l\neq i}}^{n}|q_{il}(t)| + \frac{1}{2}\sum_{\substack{j=1\\ j\neq i}}^{n}|q_{ji}(t)|\right\}\sum_{i=1}^{n}x_i^2 \\
&= f(t)\ \mathbf{x}^T\mathbf{x},
\end{aligned}$$

for all $t \geq 0$. Moreover, $\mathbf{x}^T\mathbf{g}(\mathbf{x}) + \mathbf{g}(\mathbf{x})^T\mathbf{x} \leq 2L_1\mathbf{x}^T\mathbf{x}$ and $\mathbf{\Phi}(\mathbf{u}(t))^T\mathbf{x} + \mathbf{x}^T\mathbf{\Phi}(\mathbf{u}(t)) \leq 2L_2||\mathbf{u}(t)||(\mathbf{x}^T\mathbf{x})^{1/2}$. This implies that

$$\begin{aligned}
D^+V(\mathbf{x}) &\leq f(t)\mathbf{x}^T\mathbf{x} + 2L_1\mathbf{x}^T\mathbf{x} + 2L_2||\mathbf{u}(t)||(\mathbf{x}^T\mathbf{x})^{1/2} \\
&= [f(t) + 2L_1]\,V(\mathbf{x}) + 2L_2||\mathbf{u}(t)||(V(\mathbf{x}))^{1/2} \\
&\leq \max_{t\in\mathbb{R}_+}\{f(t) + 2L_1, 2L_2||\mathbf{u}(t)||\}\left\{V(\mathbf{x}) + V(\mathbf{x})^{1/2}\right\} \\
&= p(t)c(V(\mathbf{x})),
\end{aligned}$$

where $c(s) := s + s^{1/2}$. Clearly $p \in \mathcal{PC}$ and $c \in \mathcal{K}$. Thus conditions (T1.1) and (T1.2) are satisfied over $\mathbb{R}_+ \times \mathbb{R}^n$. Now if $||\mathbf{x}(t_k)|| \leq M$, then, by inequality (10), we have

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

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

$$\Psi_k(s) := \exp(-2\alpha_k)s, \text{ for all } s \geq 0. \tag{11}$$

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., $\Psi(s) \leq \Psi_k(s) \leq s$. Furthermore, by inequality (10), for $||\mathbf{x}(t_k) + B_k\mathbf{x}(t_k)|| > M$, we have, for $k = 1, 2, \ldots$,

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

This implies that condition (T1.4) is satisfied. In addition,

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

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

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

Notice that $\exp(\alpha_k) \leq \exp(\mathcal{B})$ 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 $y > \lambda := M^2$, that

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

for every $y \geq \lambda := M^2$. Thus condition (T1.5) is satisfied. We therefore conclude that system (9) is uniformly equi-bounded as desired. It remains to show, with the choices of $\gamma_k = 1/k$, for all $k = 1, 2 \ldots$, and $\mathbf{\Phi}(\mathbf{u}(t)) = \mathbf{0}$, that system (9) is uniformly equi-Lagrange stable. This is done by applying Theorem 2 as follows. The upper right derivative of $V(\mathbf{x})$, in this case, satisfies

$$\begin{aligned} D^+V(\mathbf{x}) &\leq [f(t) + 2L_1]||\mathbf{x}||^2 \\ &= \widetilde{p}(t)\widetilde{c}(V(\mathbf{x})), \end{aligned}$$

where $\widetilde{p}(t) := f(t) + 2L_1$ and $\widetilde{c}(s) := s$. Thus, by employing the mapping $\Psi_k(s)$, defined by (11), for all $k = 1, 2, \ldots$, we conclude that conditions (T2.1), (T2.2), (T2.3) and (T2.4) are all satisfied. Moreover, for $k = 1, 2, \ldots$,

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

for all $y > 0$. Therefore condition (T2.5) is also satisfied. This implies, by Theorem 2, that system (9) is equi-Lagrange stable. □

It should be mentioned that, in the proof of Theorem 3, we may conclude that the smaller the $||\mathbf{\Phi}(\mathbf{u}(t))||$, the smaller the upper bound on $||\mathbf{x}(t)||$, for all $t \geq t_0 + T$, for some $T > 0$. This is due to the fact that when $||\mathbf{\Phi}(\mathbf{u}(t))|| = \mathcal{O}(\epsilon)$, for some $\epsilon > 0$, then $c(s) = s + \epsilon s^{1/2}$, i.e., $s^{1/2}$ becomes significantly smaller than s. This implies that inequality (4) will enforce a very small upper bound on the solutions of (9) starting from time $t_0 + T$.

3 Lorenz Chaotic System

This section demonstrates how equi-Lagrange stability is an integral factor in illustrating the robustness of impulsive synchronization between two non-identical chaotic systems by formulating the following example.

Consider the driving system given by this Lorenz chaotic system

$$\dot{\mathbf{x}} = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \mathbf{x} + \begin{pmatrix} 0 \\ -xz \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ xy \end{pmatrix}, \tag{12}$$

where σ, r and b are suitable positive constants. Whereas the driven system is a non-identical Lorenz chaotic system which is driven by the signal $-xz$ and is given by

$$\begin{cases} \dot{\mathbf{u}} = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \mathbf{u} + \begin{pmatrix} 0 \\ -xz \\ 0 \end{pmatrix} + \begin{pmatrix} -\mu u \\ -\nu v \\ uv \end{pmatrix}, & t \neq t_k \\ \Delta \mathbf{u} = -B_k \mathbf{e}, \quad t = t_k, \ \forall\ k = 1, 2, \ldots, \end{cases} \tag{13}$$

where $\mu, \nu \geq 0$ are constants and $\mathbf{e} = \mathbf{x} - \mathbf{u}$. It follows that the error dynamics is give by

$$\begin{cases} \dot{\mathbf{e}} = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \mathbf{e} + \begin{pmatrix} 0 \\ 0 \\ xy - uv \end{pmatrix} + \begin{pmatrix} \mu u \\ \nu v \\ 0 \end{pmatrix}, & t \neq t_k \\ \Delta \mathbf{e} = B_k \mathbf{e}, \quad t = t_k, \ \forall\ k = 1, 2, \ldots, \end{cases} \tag{14}$$

Let

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

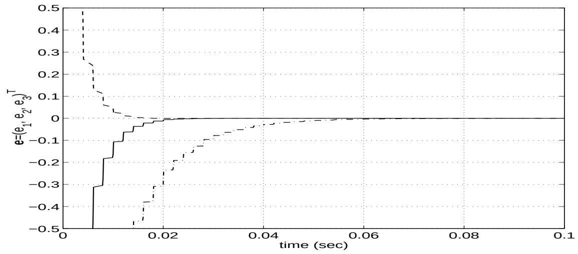

Figure 1: Error dynamics $\mathbf{e}$ with $\mu = \nu = 0$ and $B_k = -\text{diag}(0.02, 0.06, 0.01)$.

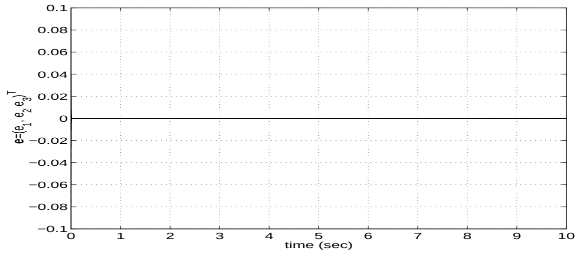

Figure 2: Error dynamics $\mathbf{e}$ with $\mu = \nu = 0.01$ and $B_k = -\text{diag}(0.5, 0.33, 0.2)$.

and take $V(\mathbf{e}) := \mathbf{e}^T\mathbf{e}$, we obtain

$$D^+V(\mathbf{e}) \quad = \quad \mathbf{e}^TQ\mathbf{e} + 2(xy - uv)e_3 + [(\mu u, \nu v, 0)\mathbf{e} + \mathbf{e}^T(\mu u, \nu v, 0)^T],$$

where $Q := A^T + A$. Let d be the largest eigenvalue of Q and $L = \max(\mu, \nu)$. Notice that

$$\begin{aligned} 2(xy - uv)e_3 &\leq 2|xy - uv||e_3| \\ &\leq 2[|x||y - v| + |v||x - u|]|e_3| \\ &\leq 2|x||e_2e_3| + 2|v||e_1e_3| + e_3^2 \\ &\leq |x|(e_2^2 + e_3^2) + |v|(e_1^2 + e_3^2) + e_3^2 \\ &\leq (|x| + |v| + 1)||\mathbf{e}||^2. \end{aligned}$$

Thus

$$\begin{aligned} D^+V(\mathbf{e}) &\leq (d + |x| + |v| + 1)\mathbf{e}^T\mathbf{e} + 2L\sqrt{u^2 + v^2}\,(\mathbf{e}^T\mathbf{e})^{1/2} \\ &\leq \max_{t\in\mathbb{R}_+}\left\{(d + |x| + |v| + 1), 2L\sqrt{u(t)^2 + v(t)^2}\right\}[\mathbf{e}^T\mathbf{e} + (\mathbf{e}^T\mathbf{e})^{1/2}] \end{aligned}$$

Let $p(t) = \max_{t\in\mathbb{R}_+}\left\{(d + |x| + |v| + 1), 2\sqrt{u(t)^2 + v(t)^2}\right\}$ and $c(s) = s + s^{1/2}$. We may conclude, by imposing the conditions of Theorem 3 on the matrices B_k, for all $k = 1, 2, \ldots$, that the error dynamics, described in system (14), is uniformly equi-bounded. Furthermore, choosing $\gamma_k = 1/k$, for all $k = 1, 2, \ldots$, and letting $\mu = \nu = 0$, we can also conclude that system (14) is uniformly equi-Lagrange stable. Note that if μ and ν are chosen such

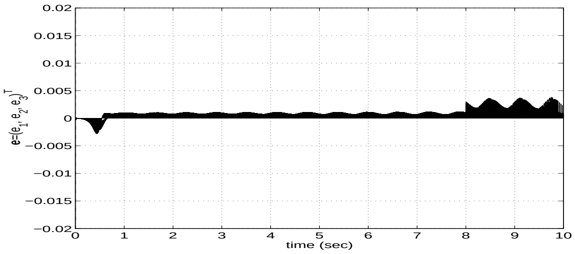

Figure 3: Error dynamics $\mathbf{e}$ with $\mu = \nu = 1$ and $B_k = -\text{diag}(0.5, 0.6, 0.2)$.

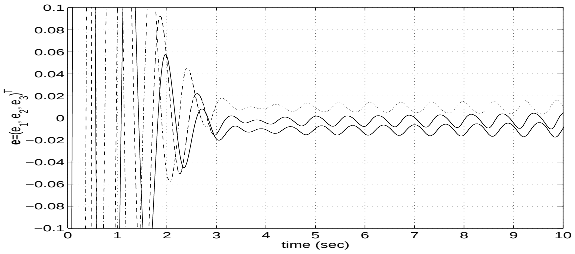

Figure 4: Error dynamics $\mathbf{e}$ with $\mu = \nu = 0.01$ by implementing the masking method proposed in [2].

that $0 \leq \mu, \nu << 1$, then impulsive synchronization shows very robust results as illustrated in the following examples. In these numerical examples, a forth order Runge-Kutta method with step size 10^{-5} is used. Moreover, we choose the values of the parameters and the initial conditions 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 $(u_0, v_0, w_0) = (2.7, -2.1, 2.502)$. Thus starting with the first and simplest case when $\mu = \nu = 0$ and $B_k = B = -\text{diag}(0.02, 0.06, 0.01)$, we obtain Figure 1 which shows how the error dynamics components reach zero in a small finite time given by 0.1. In the second example, we take $\mu = \nu = 0.01$ and $B_k = B = -\text{diag}(0.5, 0.33, 0.2)$. The impulsive synchronization, in this case, is achieved as shown in Figure 2. We can see from the above examples, impulsive synchronization exhibits a very robust behaviour towards parameter mismatch. In fact, with relatively large differences in parameters, the performance of this model is still acceptable. For example, in the case when $\mu = \nu = 1$, the simulation of this model is shown in Figure 3, where the error is of the order of 0.003 starting from time $t = 8$ seconds (it is even smaller for time $t < 8$ seconds). This promising behaviour indicates that in practice, the condition $\mu, \nu << 1$ can be relaxed and still reach desirable results. In comparison with the method of chaotic masking proposed by Cuomo and Oppenheim in [2], this robust behaviour fails completely as shown clearly in Figure 4, where the error is of the order of 0.02 for $\mu = \nu = 0.01$.

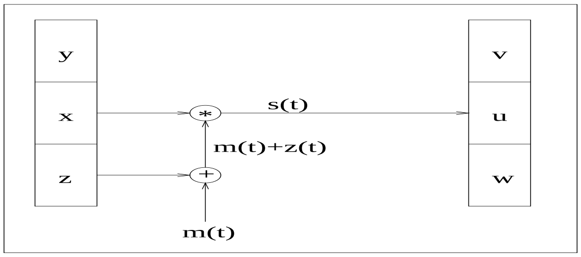

Figure 5: Chaotic masking-modulation of $m(t)$.

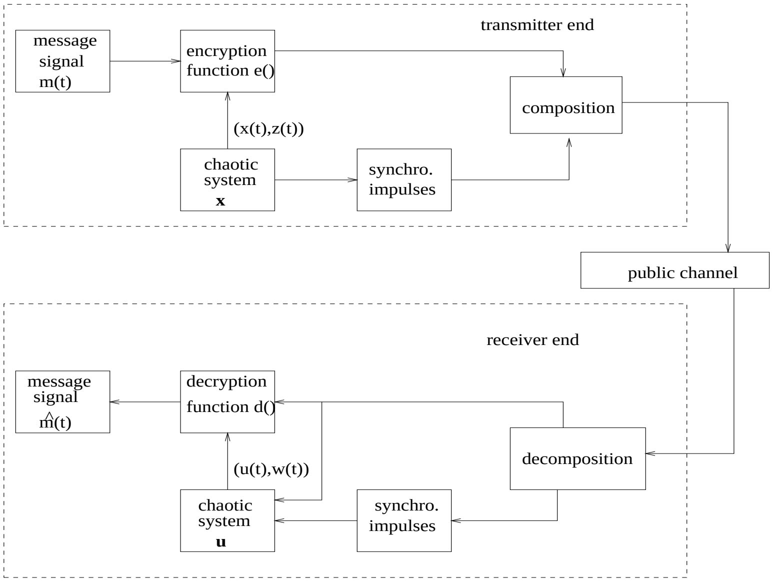

Figure 6: Proposed cryptosystem.

4 Applications to Secure Communication

We are interested in applying the results from Section 3 to design a robust cryptosystem that combines masking and modulating methods with impulsive synchronization. The proposed cryptosystem contains two chaotic systems $\mathbf{x}$ and $\mathbf{u}$, not necessarily identical, which are used to mask-modulate and unmask the message signal $m(t)$, respectively. As shown in Figure 5, one chaotic system $\mathbf{x} = (x, y, z)^T$ is at the transmitter end and the other $\mathbf{u} = (u, v, w)^T$ is at the receiver end. The masking-modulating process of $m(t)$ is done through two operations: addition and multiplication, viz. $f(t) := e(m(t)) = x(t)(m(t) + z(t))$, where $f(t)$ is the encrypted signal that will be used to drive the chaotic system $\mathbf{u}$ at the receiver end.

Figure 6 shows the cryptosystem structure which is similar to the one in [15]. The message signal is encrypted using the above scheme to generate $f(t)$.

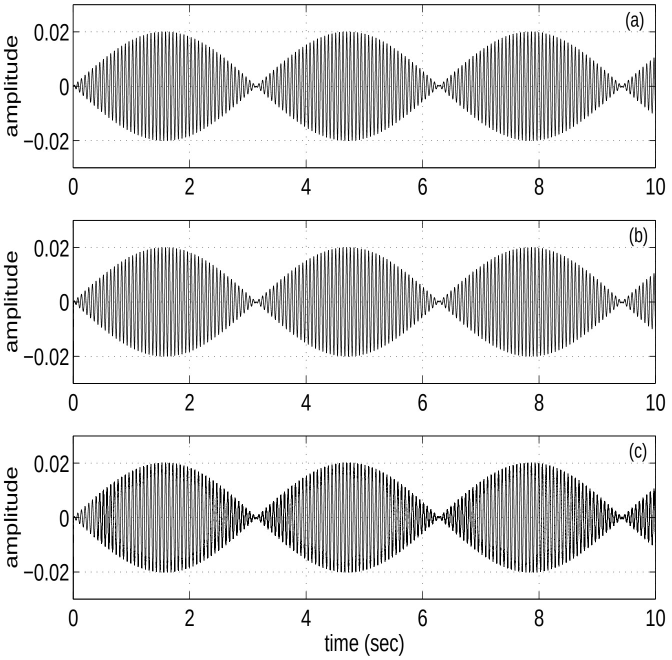

Figure 7: Accuracy of the decryption process. (a) Original message $m_1(t)$. (b) Decrypted message $m_1(t)$ for $\mu = \nu = 0$. (c) Decrypted message $m_1(t)$ for $\mu = \nu = 0.01$.

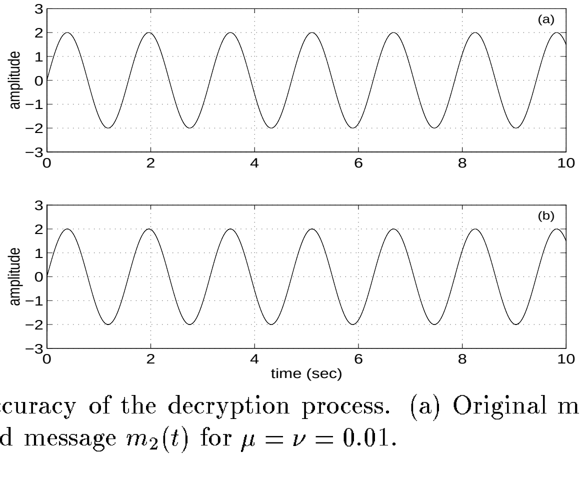

Figure 8: Accuracy of the decryption process. (a) Original message $m_2(t)$. (b) Decrypted message $m_2(t)$ for $\mu = \nu = 0.01$.

$s(t)$ is the transmitted signal; it consists of a sequence of time frames of length T. Each time frame is divided into two regions: Synchronizing-impulses region of length Q, where the impulses are loaded, and the encryption region of length $T-Q$, where $f(t)$ is loaded. The two regions are combined at the transmitter and then sent across a public channel to the receiver. At the receiver, each time frame of $s(t)$ is decomposed into the encrypted message $f(t)$ and the synchronizing impulses. At this point, $f(t)$ is used to drive the system $\mathbf{u}$, whereas the impulses are used to impulsively synchronize $\mathbf{u}$ with $\mathbf{x}$. When synchronization is achieved, we have $v(t) \approx y(t)$ and $w(t) \approx z(t)$. Thus, the decryption process becomes feasible and these two signals, $v(t)$ and $w(t)$ may be used to recover the original message in the following way

$$m(t) \approx \widehat{m}(t) = d(f(t)) = \frac{f(t)}{u(t)} - w(t).$$

As an example of the above scheme, we shall try to encrypt the message signals given by $m_1(t) = 0.02\sin(t)\sin(100t)$ which possesses high frequency and then we shall do the same for the message signal $m_2(t) = 2sin(4t)$ which possesses small frequency. This will be done using the two chaotic systems $\mathbf{x}$ and $\mathbf{u}$ given by (12) and (13), respectively. We shall start first with $m_1(t)$ and with the case when $\mu = \nu = 0$ and $B_k = B = -\mathrm{diag}(0.1, 0.06, 0.02)$, for all $k = 1, 2, \ldots$. The simulations of the original message $m_1(t)$ and the decrypted message $m_1(t)$ are shown in Figures 7(a) and 7(b), respectively. Moreover, and most importantly, in the case when $\mu, \nu = 0.01$, the encryption and the decryption of $m_1(t)$ show excellent and very accurate results in comparison with masking method proposed in [2], as shown in Figure 7(c). Accurate results are also obtained for the low frequency-large amplitude signal $m_2(t)$, as shown in Figure 8. i.e., this scheme is more robust and performs equally well with low-frequency and high-power-level type of messages.

5 Conclusion

We have demonstrated that impulsive synchronization of two chaotic systems is very robust towards parameter mismatch between them. The robustness is useful in desgning chaos based cryptosystems.

References

[1] G. Ballinger and X. Z. Liu, “On Boundedness of Solutions of Impulsive Systems”, Non-linear Studies, **4**(1), 121-131, 1997.

[2] K. M. Cuomo and A. Oppenheim, “Chaotic Signals and Systems for Communications”, IEEE ICASSP, **3**, 137-140, 1993.

[3] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua, “ Spread Spectrum Communication Through Modulation of Chaos”, Int. J. Bifur. Chaos, **3**(2), 469-477, 1993.

[4] M. Itoh, “Experimental Study of Impulsive Synchronization”, Proc. of the 1999 IEEE Int. Symposium on Circuits and Sys., Orlando, 410-413, 1999.

[5] M. Itoh, T. Yang and L. O. Chua, "Experimental Study of Impulsive Synchronization of Chaotic and Hyperchaotic Circuits", Int. J. Bifur. Chaos, **9**(7), 1393-1424, 1999.

[6] M. Itoh, T. Yang and L. O. Chua, "Conditions for Impulsive Synchronization of Chaotic and Hyperchaotic Systems", Int. J. Bifur. Chaos, **11**(2), 551-560, 2001.

[7] M. Itoh, N. Yamamoto, T. Yang and L. O. Chua, "Performance Analysis of Impulsive Synchronization", Proc. of the 1999 European Conf. on Circuit Theory and Design, Stresa, 353-356, 1999.

[8] V. Lakshmikantham and X. Z. Liu, "Stability Analysis in Terms of Two Measures", World Scientific Publishing Co. Pte. Ltd., 1993.

[9] X. Z. Liu, "Stability Results for Impulsive Differential Systems with Applications to Population Growth Models", Dynamics and Stability of Systems, **9**(2), 163-174, 1994.

[10] X. Z. Liu, "Impulsive Stabilization and Control of Chaotic Systems", Non-linear Analysis, **47**, 1081-1092, 2001.

[11] X. Z. Liu and G. Ballinger, "On Boundedness of Solutions of Impulsive Systems in Terms of Two Measures", Non-linear World, **4**, 417-434, 1997.

[12] X. Z. Liu and A. R. Willms, "Impulsive Controllability of Linear Dynamical Systems with Applications to Maneuvers of Spacecraft", MPE, **2**, 277-299, 1996.

[13] A. I. Panas, T. Yang and L. O. Chua, "Experimental Results of Impulsive Synchronization Between Two Chua's Circuits", Int. J. Bifur. Chaos, **8**(3), 639-644, 1998.

[14] J. A. Suykens, T. Yang and L. O. Chua, "Impulsive Synchronization of Chaotic Lur'e Systems by Measurement Feedback", Int. J. Bifur. Chaos, **8**(6), 1371-1381, 1998.

[15] T. Yang and L. O. Chua, "Impulsive Stabilization for Control and Synchronization of Chaotic Systems: Theory and Application to Secure Communication", IEEE Trans. Circuits and Sys.-I, **44**(10), 976-988, 1997.

[16] T. Yang and L. O. Chua, "Impulsive Control and Synchronization of Non-linear Dynamical Systems and Application to Secure Communication", Int. J. Bifur. Chaos, **7**(3), 645-664, 1997.

[17] T. Yang and L. O. Chua, "Generalized Synchronization of Chaos Via Linear Transformations", Int. J. Bifur. Chaos, **9**(1), 215-219, 1999.

[18] T. Yang, J. A. Suykens and L. O. Chua, "Impulsive Control of Non-autonomous Chaotic Systems Using Practical Stabilization", Int. J. Bifur. Chaos, **8**(7), 1557-1564, 1998.

[19] T. Yang, L. B. Yang and C. M. Yang, "Impulsive Control of Lorenz System", Physica D, **110**, 18-24, 1997.

Received August 2001; revised September 2002.