An adaptive chaotic secure communication scheme with channel noise and time delay

Jinde Cao and Yonghui Sun

Department of Mathematics, Southeast University, Nanjing 210096, China

Email: jdcao@seu.edu.cn, jdcaoseu@gmail.com

Abstract

In this paper, by using synchronization scheme of chaotic neural networks with delay, an adaptive secure communication scheme with channel noise and time delay is proposed. Based on the idea of chaotic masking-modulation, the transmitted message is encrypted by the chaotic signal, and via the adaptive feedback control techniques, the transmitter and the receiver are synchronized with channel noise, so the masked signal can be perfectly recovered by the receiver in the presence of channel noise. In light of the Lyapunov stability theory for stochastic differential equations, several theoretical results are rigorously established. Finally, a numerical example is provided to verify the effectiveness of the proposed scheme, and the time required for recovering the information signal and the performance of the recovered signal very sensitively depending on the time delay and the frequency of the information signal will also be found from the simulation results.

Key Words - Adaptive feedback control, synchronization, chaotic neural networks, delay, channel noise, chaotic masking-modulation.

I. INTRODUCTION

During the past decade, for its successful application to secure communication [2]-[18] and other fields, chaos synchronization has attracted a lot of interests since the works by Pecora and Carroll in 1990 [1]. Different synchronization strategies have been developed to synchronize chaotic systems, such as feedback control [20], adaptive control [19]-[20], impulsive control [21], etc. Recently, it has been revealed that if the network's parameters and time delays are appropriately chosen, delayed neural networks (DNNs) can exhibit some complicated dynamics and even chaotic behaviors [29], hence, there

This work was supported by the National Natural Science Foundation of China under Grant 60574043, International Joint Project funded by NSFC and the Royal Society of the United Kingdom, and the Natural Science Foundation of Jiangsu Province of China under Grant BK2006093.

has been a great deal of activity studying the synchronization of chaotic DNNs [20], [32].

In the fields of secure communication, so far, many ideas and methods have been proposed to tackle the problem of chaotic secure communication including chaotic masking [8]-[9], chaotic shift keying [10] and chaos modulation [11]-[12]. In [8], Mensour and Longtin studied the unidirectional synchronization of high-dimensional chaos with application to private communication. In [12], Bowong, Kakmeni and Fotsin considered the secure communication via parameter modulation by designing a robust adaptive observer. In [31], Wu proposed a new chaotic communication scheme using adaptive synchronization of two unified chaotic systems, and other results [30]. Though many methods for chaos synchronization have been proposed [3]-[7], scarce papers consider the adaptive feedback control for the private communication based on the idea of *chaotic masking-modulation*. Therefore, in this context, it is fair to say that there is a need for settling this problem.

And what is more, a realistic communication system design should take the communication delays into account, since the delays are inevitably to degrade the performance of secure system. Therefore, in the past decade, the chaotic secure communication with time delay based on synchronization has received increasing attention, see [17], [18] and the references therein.

It should be noted that the works mentioned ignored the channel noise, which is ubiquitous in the transmission of the masked signal, and the noise's effect should be taken into account when to evaluate the performance of a chaos communication scheme. As a consequence, secure communication in the presence of channel noise is becoming an important issue. Some experimental results have already been obtained. In [13], Minai and Pandian proposed a method for the secure transmission of encrypted message using chaos and noises. In [14], Wang and Wang considered the robust demodulation problem when there exist disturbances and noises in the channel. In [15], Murali numerically investigated the secure communication based on the heterogenous chaotic systems with channel noise and nonidentity of parameters. Other related results, see [7] and [16].

On the other hand, more and more experimental and numerical results show that noise plays an important role in chaos synchronization in different ways, see [24]-[26]. Hence, developing the corresponding theoretical results on chaos synchronization with noise perturbation is becoming a hot topic. Some theoretical results have been reported, see [28] and other results.

Actually, in most cases, the existence of noise in the public channel always tampers the recovery of the transmitted signal, or the encrypted signal unfortunately can not be recovered by the receiver. Though the theoretical results of secure communication based on chaos synchronization in different senses *without channel noise* have been fruitfully established, the corresponding theoretical results of secure communication with channel noise and time delay are limited.

Motivated by the above discussions, the main purpose is to investigate the problem of adaptive secure communication with channel noise and time delay. Based on the LaSalle invariance principle of stochastic differential equations, inspired by the ideas of adaptive feedback control in [20], several theoretical results are derived to guarantee the synchronization of the transmitter and the receiver with channel noise, so the masked signal can be recovered by the receiver in the presence of noise and time delay. The simulations provided later can be found a fairly good agreement with the theoretical results.

The remaining of this paper is organized as follows. In Section 2, the problem of secure communication with channel noise and time delay based on the adaptive synchronization of chaotic delayed neural networks is presented. In Section 3, the suitable parameters update laws ensuring synchronization of the transmitter and the receiver are presented, several theoretical results are developed. In Section 4, a numerical example is taken to demonstrate the effectiveness of the derived results. Finally, in Section 5, the paper is completed with a conclusion.

II. NOTATIONS AND PRELIMINARIES

Notations: For any symmetric matrix A, $A > 0$ means A is a positive definite matrix; $E\{\cdot\}$ stands for the mathematical expectation operator; $\|x\|^2$ is used to denote a vector norm defined by $\|x\|^2 = \sum_{i=1}^{n} x_i^2$; 'T' represents the transpose of the matrix; I is an identical matrix; $\omega(t)$ is an m-dimensional Brownian motion.

In this paper, we consider the following chaotic DNNs:

$$dx(t) = [-Cx(t) + Af(x(t)) + Bf(x(t-\tau)) + U]dt, \tag{1}$$

where $x(t) = (x_1(t), x_2(t), \cdots, x_n(t))^{\mathrm{T}} \in \mathbb{R}^n$ is the state vector associated with the neurons; $C = \mathrm{diag}(c_1, c_2, \cdots, c_n) > 0$; $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times n}$ represent the connection weight matrix and the delayed connection weight matrix, respectively; f is the activation function, $f(x(t)) = (f_1(x_1(t)), f_2(x_2(t)), \cdots, f_n(x_n(t)))^{\mathrm{T}} \in \mathbb{R}^n$, $f(x_\tau(t)) = (f_1(x_1(t-\tau_1)), f_2(x_2(t-\tau_2)), \cdots, f_n(x_n(t-\tau_n)))^{\mathrm{T}} \in \mathbb{R}^n$, where $\tau > 0$ is the transmission delay and U is the constant external input.

The secure communication scheme is based on the chaotic masking-modulation techniques, which means that the message is inserted into a chaotic signal, the carrier signal containing the information remain undetectable by chaotic masking-modulation techniques, meanwhile, after being transmitted through the hostile environment, the masked message can be detected and recovered from the chaotic signal by the receiver with channel noise and time delay.

By using the adaptive feedback control techniques, the transmitter and the receiver with channel noise and time delay are designed as follows:

Transmitter:

$$dx(t) = [-Cx(t) + Af(x(t)) + Bf(x(t-\tau)) + K\epsilon x(t) \odot m(t)]dt, \tag{2}$$

where $m(t)$ is a k-dimensional message signal transmitted, $k \leq n$, $x(t) \odot m(t) = [x_1 m_1, x_2 m_2, \cdots, x_k m_k, 0, \cdots, 0]^{\mathrm{T}}$, ϵ is a *masking weight* and diagonal matrix K is the time-varying feedback gains.

Receiver with channel noise:

$$\begin{aligned} dy(t) &= [(-C+K)y(t) + Af(y(t)) + Bf(x(t-\tau)) + Ks(t)]dt \\ &\quad + H(t, y(t)-x(t), y(t-\tau)-x(t-\tau))d\omega(t), \end{aligned} \tag{3}$$

where $s(t) = x(t) \odot [\epsilon m(t) \ominus \mathbf{1}]$ is a transmitted signal, $\mathbf{1} = [1, 1, \cdots, 1]^{\mathrm{T}}_{n\times 1}$, $\epsilon m(t) \ominus \mathbf{1} = [\epsilon m_1 - 1, \epsilon m_2 - 1, \cdots, \epsilon m_k - 1, -1, \cdots, -1]^{\mathrm{T}}$, and $H(t, y(t)-x(t), y(t-\tau)-x(t-\tau))d\omega(t)$ can be seen as

the channel noise when the signal $s(t)$ is transmitted through the public channel.

Problem description: If the transmitter (2) and the receiver (3) can be synchronized with channel noise, the masked message $m(t)$ can be recovered exactly as $r(t) = \frac{1}{\epsilon}[s(t) \oslash y(t) + \mathbf{1}]_{k\times 1}$ by the receiver (3) in the presence of channel noise, where $s(t) \oslash y(t) = [s_1/y_1, s_2/y_2, \cdots, s_n/y_n]^{\mathrm{T}}$, so our task is turning to the synchronization of the transmitter (2) and the receiver (3) with noise perturbation via a suitable controller.

Throughout this paper, the following assumptions are needed:

(A_1) $f_i(x)$ satisfies the Lipschitz condition. That is, for each $i = 1, 2, \cdots, n$, there exists a constant $\beta_i > 0$ such that

$$|f_i(x) - f_i(y)| \leq \beta_i |x - y|, \quad \forall\ x, y \in \mathbb{R}.$$

(A_2) There exist constant matrices G_1 and G_2 of appropriate dimensions such that

$$\text{trace}[H^{\mathrm{T}}(t, x, y)H(t, x, y)] \leq \|G_1 x\|^2 + \|G_2 y\|^2, \quad \forall\ (t, x, y) \in \mathbb{R}^+ \times \mathbb{R}^n \times \mathbb{R}^n.$$

(A_3) $f(0) \equiv 0$, $H(t, 0, 0) \equiv 0$.

Let $e(t) = y(t) - x(t)$ be the synchronization error, from systems (2) and (3), it yields the error system

$$de(t) = [-Ce(t) + Ag(e(t)) + Bg(e(t-\tau)) + Ke(t)]dt + H(t, e(t), e(t-\tau))d\omega(t), \tag{4}$$

where

$$g(e(t)) = f(x(t) + e(t)) - f(x(t)), \quad g(e_\tau(t)) = f(x_\tau(t) + e_\tau(t)) - f(x_\tau(t)).$$

Under assumptions (A_1) and (A_3), it is easy to get

$$|g_i(e_i(t))| = |f_i(x_i(t) + e_i(t)) - f_i(x_i(t))| \leq \beta_i |e_i(t)|, \tag{5}$$

and $g(0) = 0$. Hence, together with (A_2), it follows from [22] that the error system (4) admits a trivial solution $e(0) \equiv 0$.

Definition 1: The receiver (3) can synchronize the transmitter (2) with channel noise and time delay, if the trivial solution of the error system (4) is asymptotically stable in mean square with the initial conditions x_0 and y_0, i.e.,

$$\lim_{t\to\infty} E\|e(t)\|^2 = \lim_{t\to\infty} E\|y(t, x_0 + e_0) - x(t, x_0)\|^2 = 0. \tag{6}$$

3. MAIN RESULTS

In this section, with the suitable parameter update laws, several theoretical results are derived to guarantee the synchronization of systems (2) and (3) with channel noise and time delay.

Theorem 1: Under assumptions $(A_1) - (A_3)$, the receiver (3) can be synchronized with the transmitter (2) with channel noise and time delay, if the time-varying feedback gains $K = \text{diag}(k_1, k_2, \cdots, k_n)$ with the update law are chosen as:

$$\dot{k_i} \ = \ -\alpha_i e_i^2(t), \tag{7}$$

in which $\alpha_i > 0$ are arbitrary constants, respectively.

Proof. Construct the following non-negative function as

$$V = \frac{1}{2}e^{\mathrm{T}}(t)e(t) + \frac{1}{2}\sum_{i=1}^{n}\frac{1}{\alpha_i}(k_i + l_i)^2 + \int_{t-\tau}^{t} e^{\mathrm{T}}(s)Qe(s)ds, \tag{8}$$

where l is a constant and matrix $Q > 0$ to be determined.

By Itô-differential rule, we can obtain that

$$dV = \mathcal{L}V(t, e(t))dt + V_e(t, e(t))H(t, e(t), e(t-\tau))d\omega(t), \tag{9}$$

where the weak infinitesimal operator $\mathcal{L}$ [23] is given as follows

$$\begin{aligned}
\mathcal{L}V(t, e(t)) &= e^{\mathrm{T}}(t)\big[-Ce(t) + Ag(e(t)) + Bg(e(t-\tau)) + Ke(t)\big] - \sum_{i=1}^{n}(k_i + l_i)e_i^2(t) \\
&\quad + e^{\mathrm{T}}(t)Qe(t) - e^{\mathrm{T}}(t-\tau)Qe(t-\tau) + \frac{1}{2}\text{trace}[H^{\mathrm{T}}(t, e(t), e(t-\tau))H(t, e(t), e(t-\tau))] \\
&= e^{\mathrm{T}}(t)\big[-Ce(t) + Ag(e(t)) + Bg(e(t-\tau))\big] + e^{\mathrm{T}}(t)Qe(t) - e^{\mathrm{T}}(t-\tau)Qe(t-\tau) \\
&\quad - \sum_{i=1}^{n} l_i e_i^2(t) + \frac{1}{2}\text{trace}[H^{\mathrm{T}}(t, e(t), e(t-\tau))H(t, e(t), e(t-\tau))].
\end{aligned} \tag{10}$$

By condition (5) and the elementary inequality

$$\begin{aligned}
e^{\mathrm{T}}(t)Ag(e(t)) &\le \frac{1}{2}e^{\mathrm{T}}(t)A^{\mathrm{T}}Ae(t) + \frac{1}{2}g^{\mathrm{T}}(e(t))g(e(t)) \\
&\le \frac{1}{2}e^{\mathrm{T}}(t)A^{\mathrm{T}}Ae(t) + \frac{1}{2}e^{\mathrm{T}}(t)\Sigma^{\mathrm{T}}\Sigma e(t),
\end{aligned} \tag{11}$$

$$\begin{aligned}
e^{\mathrm{T}}(t)Bg(e(t-\tau)) &\le \frac{1}{2}e^{\mathrm{T}}(t)B^{\mathrm{T}}Be(t) + \frac{1}{2}g^{\mathrm{T}}(e(t-\tau))g(e(t-\tau)) \\
&\le \frac{1}{2}e^{\mathrm{T}}(t)B^{\mathrm{T}}Be(t) + \frac{1}{2}e^{\mathrm{T}}(t-\tau)\Sigma^{\mathrm{T}}\Sigma e(t-\tau),
\end{aligned} \tag{12}$$

where $\Sigma = \text{diag}(\beta_1, \beta_2, \cdots, \beta_n)$, and from assumption (A_2), it holds

$$\text{trace}[H^{\mathrm{T}}(t, e(t), e(t-\tau))H(t, e(t), e(t-\tau))] \le e^{\mathrm{T}}(t)G_1^{\mathrm{T}}G_1e(t) + e^{\mathrm{T}}(t-\tau)G_2^{\mathrm{T}}G_2e(t-\tau). \tag{13}$$

Substituting (11)-(13) into (10), it is derived that

$$\begin{aligned}
\mathcal{L}V(t, e(t)) &\le -e^{\mathrm{T}}(t)[L + C - \frac{1}{2}A^{\mathrm{T}}A - \frac{1}{2}B^{\mathrm{T}}B - \frac{1}{2}\Sigma^{\mathrm{T}}\Sigma - \frac{1}{2}G_1^{\mathrm{T}}G_1 - Q]e(t) \\
&\quad + e^{\mathrm{T}}(t-\tau)[\frac{1}{2}\Sigma^{\mathrm{T}}\Sigma + \frac{1}{2}G_2^{\mathrm{T}}G_2 - Q]e(t-\tau),
\end{aligned} \tag{14}$$

where $L = \text{diag}(l_1, l_2, \cdots, l_n)$, it can be chosen as $L = -C + \Sigma^{\mathrm{T}}\Sigma + I + \frac{1}{2}\big\{\lambda_{\max}(A^{\mathrm{T}}A) + \lambda_{\max}(B^{\mathrm{T}}B) + \lambda_{\max}(G_1^{\mathrm{T}}G_1) + \lambda_{\max}(G_2^{\mathrm{T}}G_2)\big\}I$, and the matrix Q satisfies that $Q = \frac{1}{2}\Sigma^{\mathrm{T}}\Sigma + \frac{1}{2}G_2^{\mathrm{T}}G_2$, then yields

$$\mathcal{L}V(t, e(t)) \le -e^{\mathrm{T}}(t)e(t). \tag{15}$$

Based on LaSalle invariance principle of stochastic differential equations, which was proposed in [23], it yields $e(t) \to 0$, then we derive $E\|e(t;\xi)\|^2 \to 0$. This completes the proof.

Remark 1: The main contribution here is to deal with the problem of the adaptive secure communication with channel noise and time delay. Several theoretical results are rigorously developed to synchronize the transmitter and the receiver, so the encrypted message can be exactly recovered by the receiver in the presence of channel noise. Some simulations results provided later can be found a perfect agreement with the derived theoretical results.

Remark 2: In [8]-[9], the authors studied the secure communication based on chaotic masking via different synchronization strategies. However, the channel noise, which is ubiquitous in the public channel during the course of the signal transmitted were ignored, so our results are more reliable and general than those in [8]-[9].

Remark 3: In [8], the authors investigated the secure communication based on synchronization of coupled systems via a feedback control. Firstly, the chaotic masking-modulation techniques used in this paper is more general and securer than the chaotic masking techniques they used. Secondly, the feedback gains in earlier papers were fixed in prior and must be the maximal, which means a waste in real application, ours concurs this drawback and varies with the synchronization error to a constant.

If we break the idea of chaotic masking-modulation, and consider the secure communication scheme based on chaotic masking, the transmitter and the receiver are designed as:

Transmitter:

$$dx(t) = [-Cx(t) + Af(x(t)) + Bf(x(t-\tau)) + K\epsilon \odot m(t)]dt, \tag{16}$$

where $m(t)$ is a k-dimensional message signal transmitted, $k \leq n$, $K\epsilon \odot m(t) = [k_1\epsilon m_1, k_2\epsilon m_2, \cdots, k_k\epsilon m_k, 0, \cdots, 0]^{\mathrm{T}}$, ϵ is the *masking weight* and K is the time-varying gains.

Receiver:

$$\begin{aligned} dy(t) &= [(-C+K)y(t) + Af(y(t)) + Bf(y(t-\tau)) + Ks(t)]dt \\ &\quad + H(t, y(t)-x(t), y(t-\tau)-x(t-\tau))d\omega(t), \end{aligned} \tag{17}$$

where $s(t) = x(t) \oplus \epsilon m(t)$ is the transmitted signal, $x(t) \oplus \epsilon m(t) = [x_1 + \epsilon m_1, x_2 + \epsilon m_2, \cdots, x_k + \epsilon m_k, x_{k+1}, \cdots, x_n]^{\mathrm{T}}$, the following results are true.

Theorem 2: Under assumptions $(A_1)-(A_3)$, the receiver (16) can be synchronized with the transmitter (15) with channel noise and time delay, if the time-varying feedback gains $K = \mathrm{diag}(k_1, k_2, \cdots, k_n)$ with the update law are chosen as:

$$\dot{k_i} = -\alpha_i e_i^2(t), \tag{18}$$

in which $\alpha_i > 0$ are arbitrary constants, respectively.

If the channel noise is ignored when the signal is transmitted through the public channel, we can derive the following results:

Corollary 1: Under assumptions $(A_1)-(A_3)$, the receiver (3) can be synchronized with the transmitter (2) without channel noise, if the time-varying feedback gains $K = \mathrm{diag}(k_1, k_2, \cdots, k_n)$ with the update

law are chosen as:

$$\dot{k_i} \;=\; -\alpha_i e_i^2(t), \tag{19}$$

in which $\alpha_i > 0$ are arbitrary constants, respectively.

4. ILLUSTRATIVE EXAMPLE

In this section, a numerical example is employed to illustrate the effectiveness of the obtained results.

Example. Consider the following chaotic DNNs [29]:

$$dx(t) = [-Cx(t) + Af(x(t)) + Bf(x(t-\tau)) + U]dt, \tag{20}$$

where $f(x) = \tanh(x)$,

$$C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 2.0 & -0.1 \\ -5.0 & 4.5 \end{bmatrix}, \quad B = \begin{bmatrix} -1.5 & -0.1 \\ -0.2 & -4 \end{bmatrix}.$$

Here time delay $\tau = 1$, and the external input $U = 0$. If the initial value is $x_0 = [0.4, 0.6]^{\mathrm{T}}$ for $-1 \le t \le 0$ and time step size is $\delta t = 0.02$, the chaotic attractors can be seen in Fig. 1.

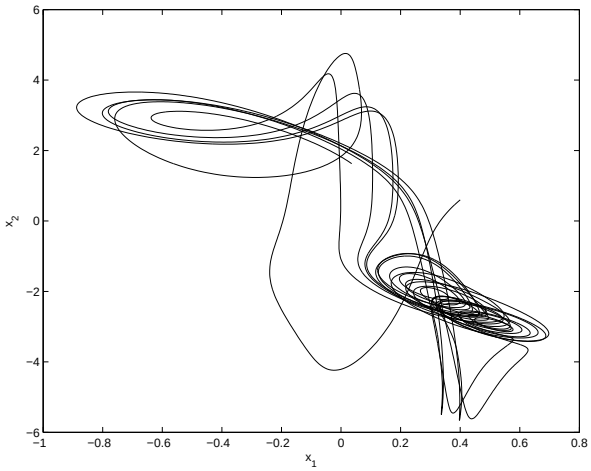

Fig. 1. Chaotic attractors of system .

Based on the main results of this paper, the transmitter and the receiver are designed as follows:

Transmitter:

$$dx(t) = [-Cx(t) + Af(x(t)) + Bf(x(t-\tau)) + M(t)]dt, \tag{21}$$

where $M(t) = [k_1 \epsilon x_1(t) m(t), 0]^{\mathrm{T}}$, $m(t)$ is a message signal, and in this example it is chosen as the $\sin$ signal $m(t) = \sin(\theta t)$, it can be hidden by the chaotic carrier signal $x_1(t)$, θ is the frequency of the signal. Here the masking weight $\epsilon = 0.1$, the message signal can not be detected in the course of transmitting, and does not affect the chaotic behaviors.

Receiver:

$$dy(t) = [(-C + K)y(t) + Af(y(t)) + Bf(y(t-\tau)) + KS(t)]dt + H(t, e(t), e(t-\tau))d\omega(t), \tag{22}$$

where $S(t) = [s(t), -x_2(t)]^{\mathrm{T}}$, $s(t) = x_1(t)[\epsilon m(t) - 1]$ is the transmitted signal, $\omega(t) = [\omega_1, \omega_2]^{\mathrm{T}}$ is a 2-dimensional Brownian motion, and the channel noise intensity matrix is

$$H(t, e(t), e(t-\tau)) = \begin{bmatrix} a_1 e_1(t) + b_1 e_{\tau 1}(t) & 0 \\ 0 & a_2 e_2(t) + b_2 e_{\tau 2}(t) \end{bmatrix},$$

where $a_1 = -0.2, a_2 = 0.1, b_1 = 0.1, b_2 = 0.2$. From our main results, if the suitable parameter update laws are designed in the form of (7), the transmitter (21) and the receiver (22) can be synchronized with channel noise, so the message signal $m(t)$ can be recovered as $r(t) = [s(t)/y_1(t) + 1]/\epsilon$.

In the simulations, the Euler-Maruyama numerical scheme is adopted. The initial conditions of the transmitter (21) and the receiver (22) are taken as $x_0 = [0.4, 0.6]^{\mathrm{T}}$ and $y_0 = [0.2, 0.3]^{\mathrm{T}}$, respectively. Some initial parameters are given as follows: $T = 200$ and time step size is $\delta t = 0.02$. Take the initial conditions of the feedback strength and the parameters as follows $[k_1(0), k_2(0)]^{\mathrm{T}} = [1, 1]^{\mathrm{T}}$, $[\alpha_1, \alpha_2]^{\mathrm{T}} = [0.5, 0.5]^{\mathrm{T}}$.

A. $m(t) = \sin(0.2t), \tau = 1$

We choose the information signal as $m(t) = \sin(0.2t)$ in Fig. A2 and time-delay $\tau = 1$. Fig. A1 displays the dynamics of the receiver with channel noise. Then with the suitable parameters update laws, the transmitter and the receiver can be synchronized with channel noise. Fig. A3 shows that the trajectories of synchronization errors $e_1(t)$ and $e_2(t)$ tend to zero after $t > 30$, and Fig. A4 unfolds the time response of the feedback gains. Fig. A5 is the chaotic transmitted signal including the encrypted message. Fig. A6 depicts the recovered signal. Fig. A7 illustrates the error between signal $m(t)$ and the recovered signal. It is easy to find from Fig. A8 that the information signal $m(t)$ is recovered accurately after $t > 30$, and what is more, it is clearly shown that the information signal is recovered with very small fluctuation for small mismatch $|m(t) - r(t)| \geq e^{-35}$ after $t \approx 125$.

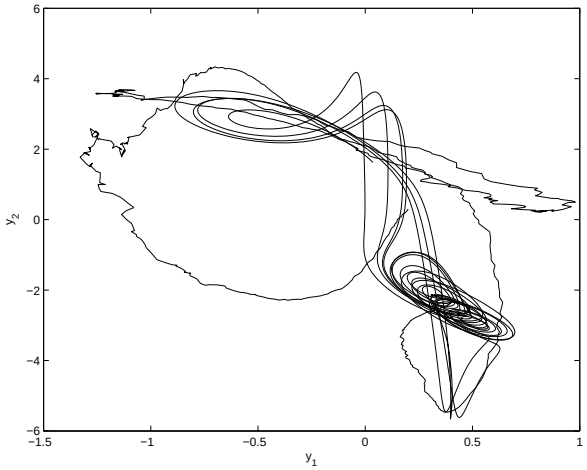

Fig. A1. Chaotic behavior of the receiver with channel noise.

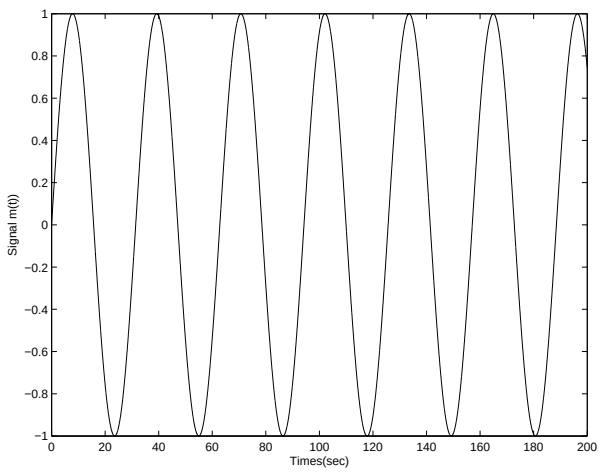

Fig. A2. The sin signal $m(t)$.

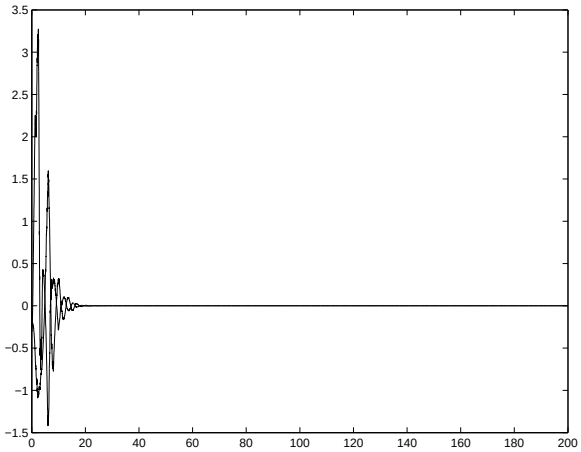

Fig. A3. Synchronization errors $e_i, i = 1, 2$.

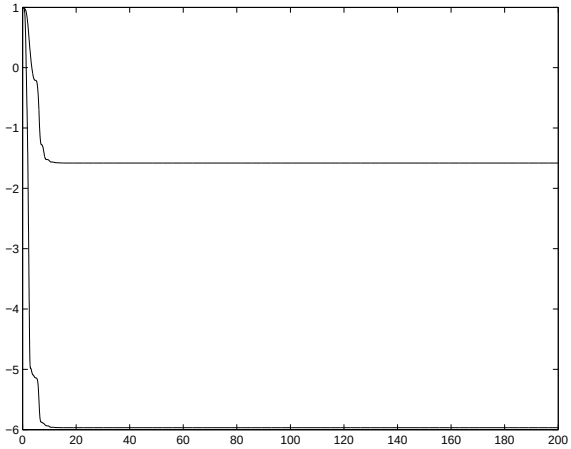

Fig. A4. Feedback gains $k_i, i = 1, 2$.

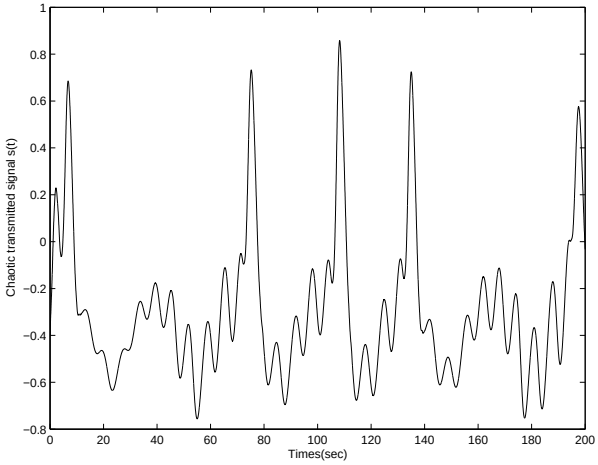

Fig. A5. Chaotic transmitted signal $s(t)$.

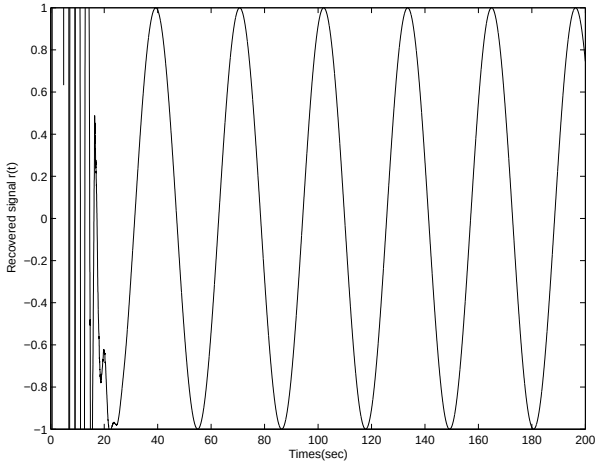

Fig. A6. The recovered message $r(t)$.

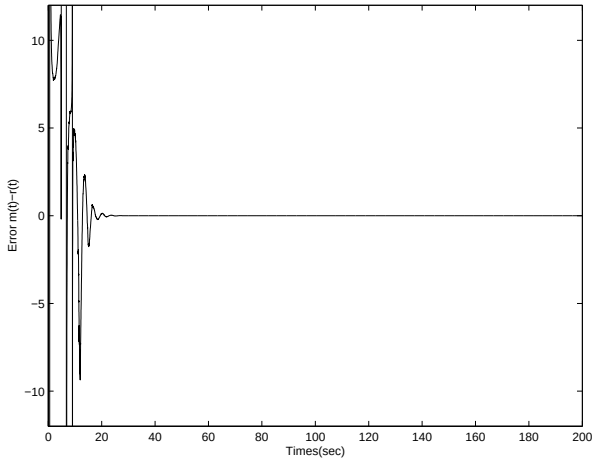

Fig. A7. Error between $m(t)$ and $r(t)$.

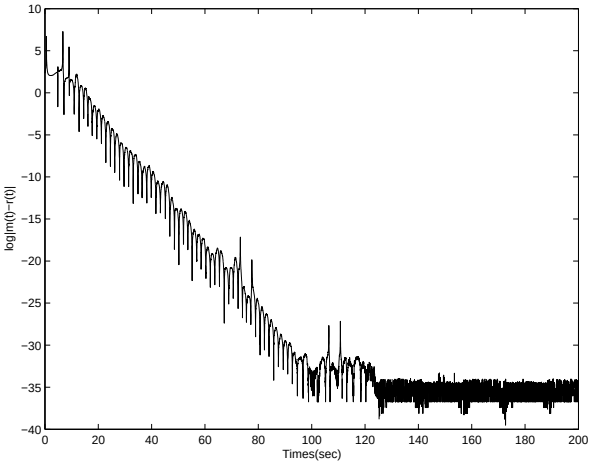

Fig. A8. Communication with channel noise.

B. $m(t) = \sin(0.2t), \tau = 1.1$

Here, we choose the information signal as $m(t) = \sin(0.2t), \tau = 1.1$, which can be seen from Fig. B2. Fig. B1 is the dynamics of the transmitter with channel noise. Fig. B3 shows that the trajectories of synchronization errors $e_1(t)$ and $e_2(t)$ tend to zero after $t > 30$, and Fig. B4 depicts the time response

of the feedback gains. Fig. B5 is the chaotic transmitted signal including the encrypted message. Fig. B6 depicts the recovered signal. Fig. B7 illustrates the error between signal $m(t)$ and the recovered signal. It is easy to find from Fig. B8 that the information signal $m(t)$ is recovered accurately after $t > 50$. It is clearly shown that the information signal is recovered with very small fluctuation for small mismatch $|m(t) - r(t)| \geq e^{-35}$ after $t \approx 150$, which is longer than that of **A** with the same frequency.

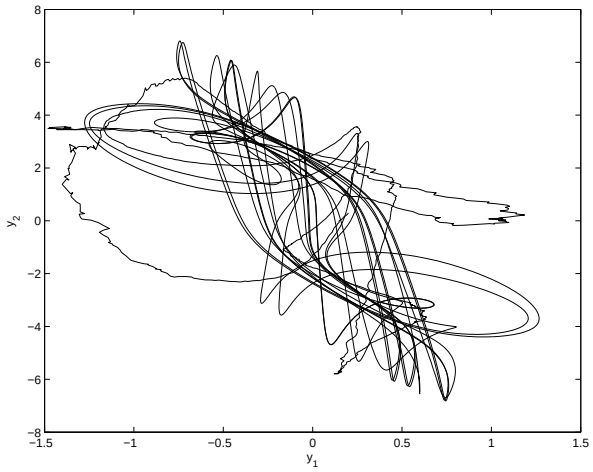

Fig. B1. Chaotic behavior of the receiver with channel noise.

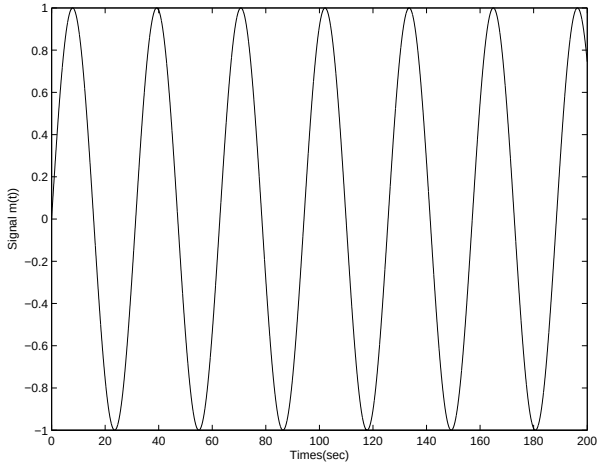

Fig. B2. The sin signal $m(t)$.

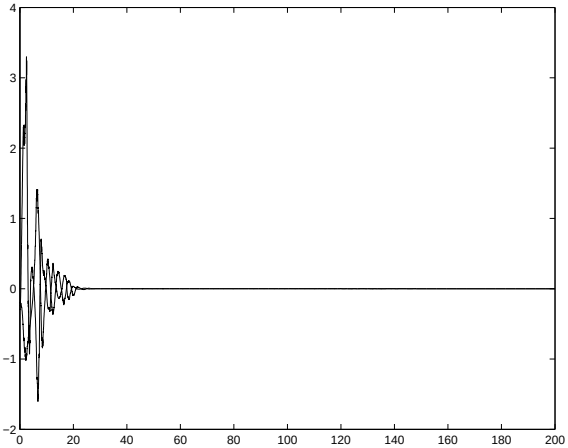

Fig. B3. Synchronization errors $e_i, i = 1, 2$.

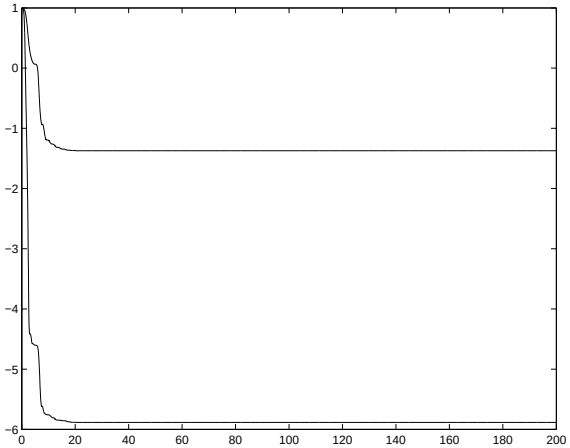

Fig. B4. Feedback gains $k_i, i = 1, 2$.

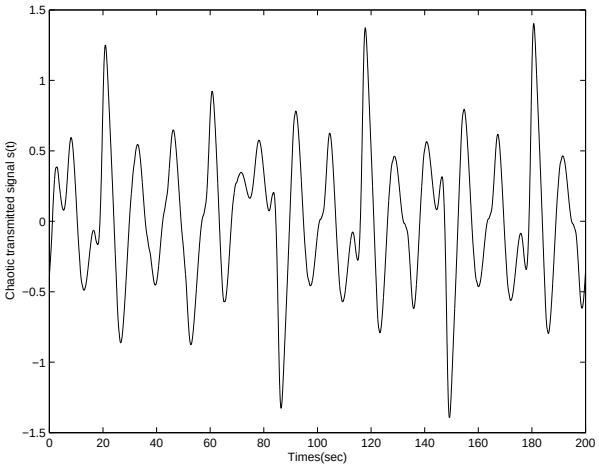

Fig. B5. Chaotic transmitted signal $s(t)$.

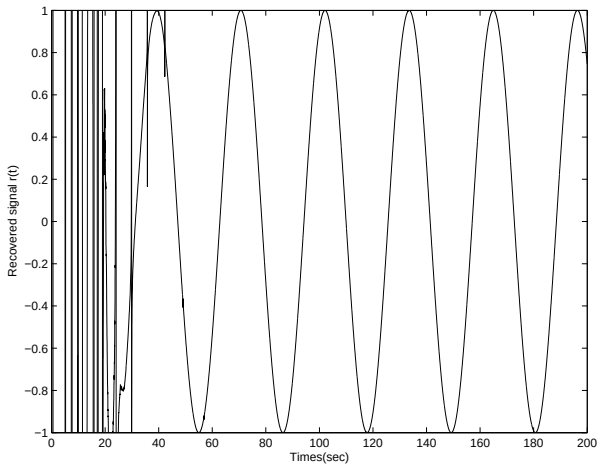

Fig. B6. The recovered message $r(t)$.

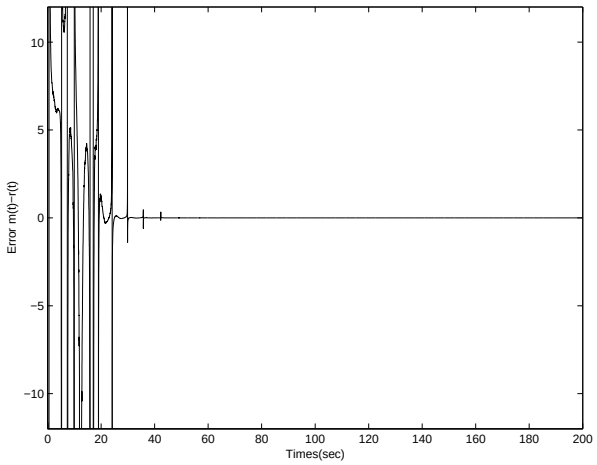

Fig. B7. Error between $m(t)$ and $r(t)$.

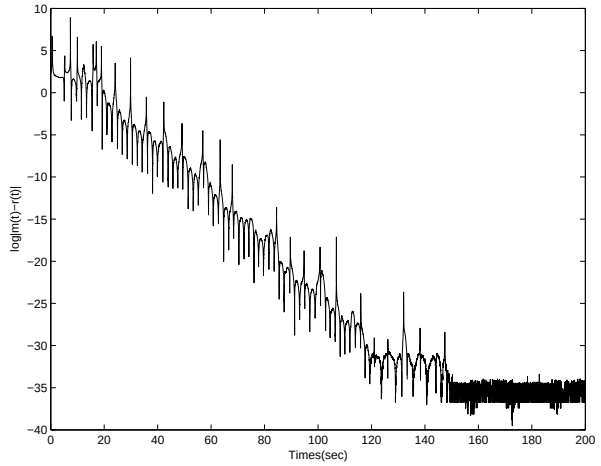

Fig. B8. Communication with channel noise.

C. $m(t) = \sin(0.1t), \tau = 1$

The information signal is taken as $m(t) = \sin(0.1t)$, the frequency of which is less than that of **A**, which can be seen from Fig. C2 and time delay is $\tau = 1$. Fig. C1 displays the dynamics of the transmitter with channel noise. With the suitable parameters update laws, the transmitter and the receiver can be synchronized with channel noise, Fig. C3 shows that the trajectories of synchronization errors $e_1(t)$ and $e_2(t)$ tend to zero after $t > 30$, and Fig. C4 unfolds the the time response of the feedback gains. Fig. C5 is the chaotic transmitted signal including the encrypted message. Fig. C6 depicts the recovered signal. Fig. C7 illustrates the error between signal $m(t)$ and the recovered signal $r(t)$. Fig. C8 easy to find that the information signal $m(t)$ is recovered accurately after $t > 50$. Apparently, the information signal is recovered with very small fluctuation for small mismatch $|m(t) - r(t)| \geq e^{-35}$ after $t \approx 120$, which is shorter than that of **A** with a less frequency.

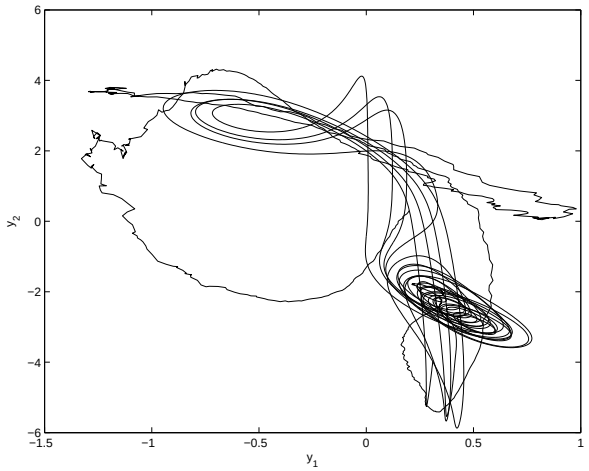

Fig. C1. Chaotic behavior of the receiver with channel noise.

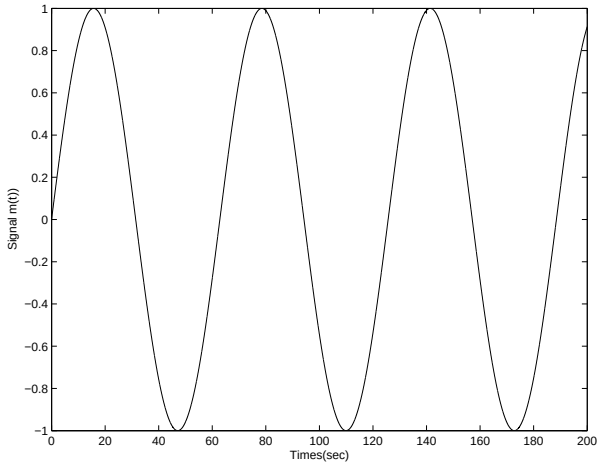

Fig. C2. The sin signal $m(t)$.

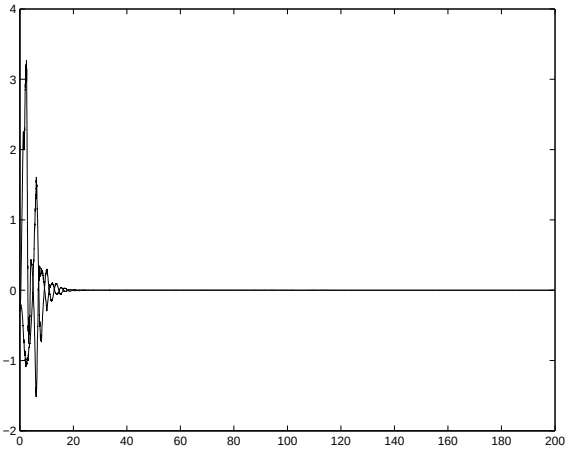

Fig. C3. Synchronization errors $e_i, i = 1, 2$.

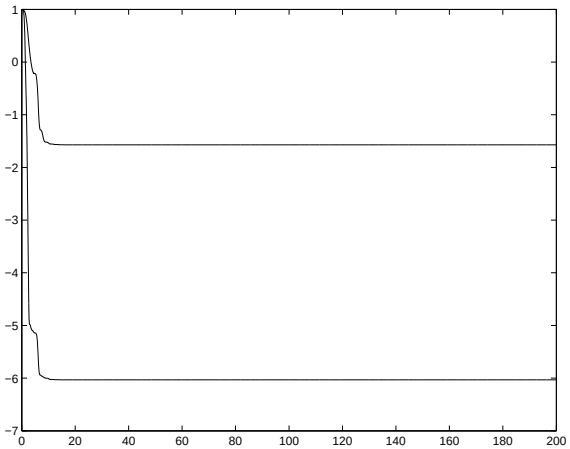

Fig. C4. Feedback gains $k_i, i = 1, 2$.

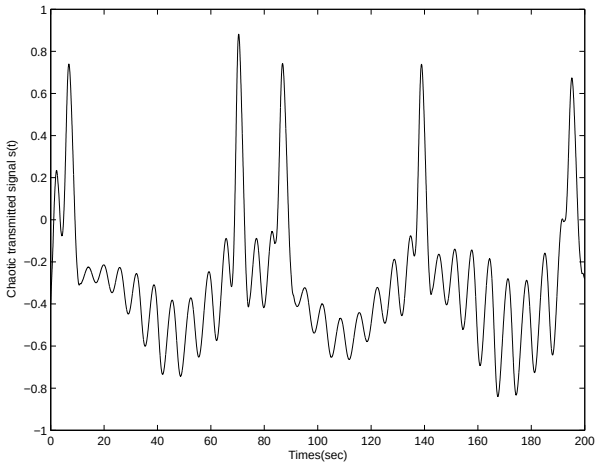

Fig. C5. Chaotic transmitted signal $s(t)$.

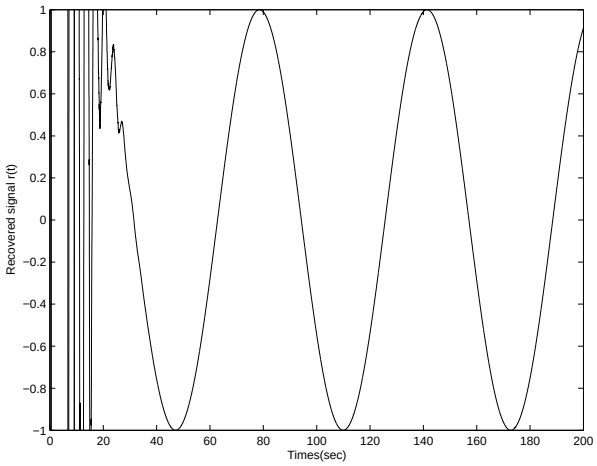

Fig. C6. The recovered message $r(t)$.

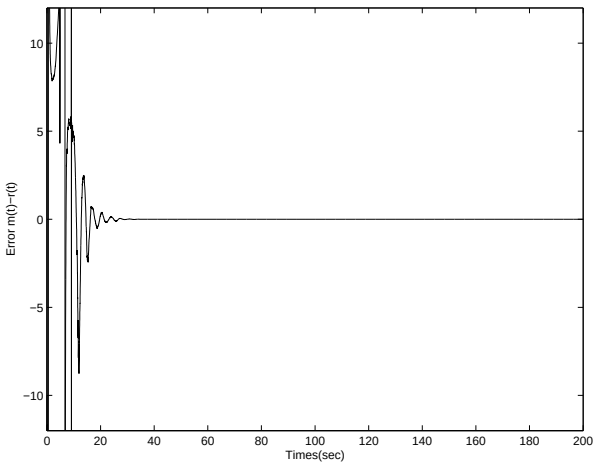

Fig. C7. Error between $m(t)$ and $r(t)$.

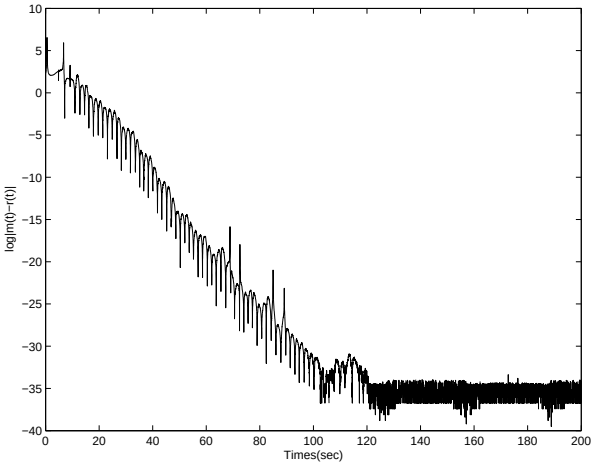

Fig. C8. Communication with channel noise.

5. CONCLUSIONS

In this paper, we have investigated the problem of adaptive secure communication with channel noise and time delay. By using the adaptive feedback control techniques, and employing the chaotic masking-modulation approach, several theoretical results have been derived to synchronize the transmitter and the receiver, the encrypted message can be exactly recovered by the receiver in the presence of channel noise. Moreover, we broke the chaotic masking-modulation scheme and derived some other useful results based on chaotic masking. At last, an example is provided to illustrate the derived results.

REFERENCES

[1] L. Pecora, T. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett., 64 (1990) 821-824.

[2] Y. Zhang, Z. He, A secure communication scheme based on cellular neural networks, Proc. IEEE Int. Conf. Intelligent Processing Systems, 1 (1997) 521-524.

[3] M. Boutayeb, M. Darouach, H. Rafaralahy, Generalized state-space observers for chaotic synchronization and secure communication, IEEE Trans. Circuits Syst. I, 49 (2002) 345-349.

[4] V. I. Ponomarenko, M. D. Prokhorov, Extracting information masked by the chaotic signal of a time-delay system, Phys. Rev. E, 66 (2002) 026215.

[5] J. Y. Chen, K. W. Wong, L. M. Cheng, J. W. Shuai, A secure communication scheme based on the phase synchronization of chaotic systems, Chaos, 13 (2003) 508-514.

[6] S. Bowong, F. M. M. Kakmeni, R.Koina, A new sycnhronization principle for a class of Lur's systems with application in secure communication, Int. J. Bifur. Chaos, 14 (2004) 2477-2491.

[7] M. Chen, D. Zhou, Y. Shang, A new private communication scheme based on the idea of fault detection and identification, Phys. Lett. A, 351 (2006) 177-183.

[8] B. Mensour, A. Longtin, Synchronization of delay-differential equations with application to private communication, Phys. Lett. A, 244 (1998) 59-70.

[9] C. Li, X. Liao, K. Wong, Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication, Physica D, 194 (2004) 187-202.

[10] H. Lu, W. K. S. Tang, Chaotic phase shift keying in delayed chaotic anticontrol systems, Int. J. Bifur. Chaos, 12 (2002) 1017-1028.

[11] C. Hua, B. Yang, G. Ouyang, X. Guan, A new chaotic secure communication scheme, Phys. Lett. A, 342 (2005) 305-308.

[12] S. Bowong, F. M. M. Kakmeni, H. Fotsin, A new adaptive observer-based synchronization scheme for private communication, Phys. Lett. A, 355 (2006) 193-201.

[13] A. A. Minai, T. D. Pandian, Communicating with noise: How chaos and noise combine to generate secure encryption keys, Chaos, 8 (1998) 621-627.

[14] X. Wang, Z. Wang, A robust demodulation application communication using chaotic signals, Int. J. Bifur. Chaos, 13 (2003) 227-231.

[15] K. Murali, Heterogeneous chaotic systems based cryptography, Phys. Lett. A, 272 (2000) 184-192.

[16] S. Li, G. Álvarez, G. Chen, X. Mou, Breaking a chaos-noise-based secure communication scheme, Chaos, 15 (2005) 013703.

[17] A. Khadra, X.Z. Liu, X. Shen, Impulsively synchronizingchaotic systems with delay and applications to secure communication, Automatica, 41 (2005) 1491-1502.

[18] Y. Liu, G. Ge, H. Zhao, Y. Wang, L. Gao, Synchronization of hyperchaotic harmonics in time-delay systems and its application to secure communication, Phys. Rev. E, 62 (2000) 7898-7904.

[19] J. Lu, J. Cao, Adaptive complete synchronization of two identical or different chaotic (hyperchaotic) systems with fully unknown parameters, Chaos, 15 (2005) 043901.

[20] J. Cao, J. Lu, Adaptive synchronization of neural networks with or without time-varying delay, Chaos, 16 (2006) 013133.

[21] B. Liu, X. Liu, G. Chen, H. Wang, Robust impulsive synchronization of uncertain dynamical networks, IEEE Trans. Circuits Syst. I, 52 (2005) 1431-1441.

[22] A. Friedman, Stochastic Differential Equations and Applications, Academic Press, New York, 1976.

[23] X. Mao, A note on the LaSalle-type theorems for stochastic differential delay equations, J. Math. Anal. Appl., 268 (2002) 125-142.

[24] G. Hu, L. Pivka, A. Zheleznyak, Synchronization of a one-dimensional array of Chua's circuits by feedback control and noise, IEEE Trans. Circuits Syst. I, 42 (1995) 736-740.

[25] E. Sáchez, M. Matías, V. Muñuzuri, Analysis of synchronization of chaotic systems by noise: An experimental study, Phys. Rev. E, 56 (1997) 4068-4071.

[26] R. Torala, C. R. Mirasso, E. Hernadez-Garcia, O. Piro, Analytical and numerical studies of noise-induced synchronization of chaotic systems, Chaos, 11 (2001) 665-673.

[27] W. Lin, Y. He, Complete synchronization of the noise-perturbed Chua's circuits, Chaos, 15 (2005) 023705.

[28] W. Lin, G. Chen, Using white noise to enhance synchronization of coupled chaotic systems, Chaos, 16 (2006) 013134.

[29] H. Lu, Chaotic attractors in delayed neural networks, Phys. Lett. A, 298 (2002) 109-116.

[30] M. Feki, An adaptive chaos synchronization scheme applied to secure communication, Chaos, Solitons & Fractals, 18 (2003) 141-148.

[31] X. Wu, A new chaotic communication scheme based on adaptive synchronization, Chaos, 16 (2006) 043118.

[32] X. Huang, J. Cao, Generalized synchronization for delayed chaotic neural networks: a novel coupling scheme, Nonlinearity, 19 (2006) 2797-2811.