Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Physics Letters A 351 (2006) 177–183
PHYSICS LETTERS A
www.elsevier.com/locate/pla

# A new private communication scheme based on the idea of fault detection and identification

Maoyin Chen [a,*], Donghua Zhou [a], Yun Shang [b]

[a] Department of Automation, Tsinghua University, Beijing 100084, PR China
[b] College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, PR China

Received 1 December 2003; accepted 26 October 2005

Available online 2 November 2005

Communicated by A.R. Bishop

**Abstract**

By use of the idea of fault detection and identification, this Letter proposes a new scheme to resolve the problem of chaotic private communication. From the point of view of fault detection and identification the scalar message signal hidden in the chaotic systems can be regarded as the component fault signal, thereby it can be detected and recovered using the model-based methods of fault detection and identification. The famous Duffing oscillator is used to illustrate and verify the effectiveness of this scheme.


*Keywords:* Private communication; Fault detection and identification; Equivalent control

## 1. Introduction

In the past decades the synchronization of chaotic systems has been a topic in the field of chaos control [1–5]. One important reason is the successful application of chaos to private communication [6–14]. In fact, chaotic private communication can be considered as the problem of designing generalized state-space observers [11] or the problem of system identification [24]. Furthermore, many ideas and methods in control theories can be applied to chaotic private communication, including the observer method [11,14], the inverse system method [13] and the system method [12]. This means that it is necessary to study possible applications of control theories to the problem of chaotic private communication.

In the nonlinear control theory the problem of fault detection and identification attracts lots of interest to study [16–22]. This is because there is an increasing demand for high reliability in many industrial processes. Various methods have been proposed, among which the model-based fault-detection techniques have yielded the best result [16–22]. The model-based fault-detection techniques always utilized the concept of equivalent control to generate the residuals which act as indicators of faults in real application process [18,21]. Though many methods for fault detection and identification have been proposed in the past decades, scarce papers consider their applications to private communication.

This Letter tries to apply the idea of fault detection and identification to chaotic private communication. From the point of view of fault detection and identification the message signal hidden in the emitter can be regarded as the component fault, then it can be detected and identified at the receiving end by use of the model-based methods of fault detection and identification. In this Letter the famous Duffing oscillator is chosen to be the benchmark to explain this application. For Duffing oscillator (the emitter) we can choose two driving signals and construct a receiver with discontinuous control laws. Under the help of the driving signals and some discontinuous laws, the hidden message signal can be detected and identified by use of the concept of equivalent control, one of the model-based methods of fault detection and identification. Simulation results show that the hidden message signal can be recovered approximately even if driving signals are contaminated by channel noises.

* Corresponding author.
*E-mail address:* maoyinchen@163.com (M. Chen).

0375-9601/$ – see front matter 
doi:10.1016/j.physleta.2005.10.089

## 2. Problem statement

The dynamics of Duffing oscillator is described by

$$\dot{x} = y,$$
$$\dot{y} = x - ay - x^3 + b\cos(wt), \tag{1}$$

where $a$, $b$ and $w$ are parameters. Though Duffing oscillator is a simple deterministic non-autonomous system, it can exhibit complex behaviors such as bifurcation and chaos when parameters $a$, $b$ and $w$ are chosen suitably. Typically, if $a = 0.15$, $b = 0.3$ and $w = 1.0$, the Duffing oscillator is chaotic.

In this Letter Duffing oscillator is used to illustrate a new private communication scheme. Suppose that the scalar message signal $m(t)$ is applied to the first and second equations of Eq. (1), i.e.,

$$\dot{x} = y + d_1 m(t),$$
$$\dot{y} = x - ay - x^3 + b\cos(wt) + d_2 m(t), \tag{2}$$

where $d_i$ $(i = 1, 2)$ are two modulated constants of message $m(t)$. Notice that these two constants shouldn't be zero.

In the framework of private communication Eq. (2) is regarded as an emitter. Therefore, our problem in this Letter is to choose one or more suitable driving signals and to design a receiver such that at the receiving end the hidden message signal $m(t)$ can be recovered. Here suppose that this signal is bounded by a positive constant $\delta$.

## 3. The new scheme of private communication

In the past decades the problem of fault detection and identification has been a topic in the nonlinear control field [16–22]. Though many control ideas and methods can be applied to chaotic private communication, scarce papers consider the application of the idea of fault detection and identification to chaotic private communication. Here this Letter first applies this idea to private communication. From the point of view of fault detection and identification the parts $d_1 m(t)$ and $d_2 m(t)$ in the first and second equations of Eq. (2) can be considered as component faults of Eq. (2).

In this Letter two driving signals are defined by

$$s(t) = k_1 x + k_2 y, \tag{3}$$
$$z(t) = x - ay - x^3 + b\cos(wt), \tag{4}$$

where $k_i$ $(i = 1, 2)$ are two nonzero constants to be determined. Eq. (4) means that the right-hand side of the second equation in Eq. (2), except for the hidden message, can be regarded as a scalar signal, which is seen in Ref. [15]. In addition to the signal $z(t)$, this Letter also utilizes the signal $s(t)$ to recover the message signal $m(t)$. Therefore, the private communication scheme in this Letter needs two channels to send necessary driving signals.

At the receiving end the receiver is constructed as follows:

$$\dot{\bar{x}} = \bar{y} + v_1,$$
$$\dot{\bar{y}} = z + s - k_1\bar{x} - k_2\bar{y} + v_2,$$
$$\dot{\bar{z}} = z + s - k_1\bar{x} - k_2\bar{y} - \bar{z} + v_z, \tag{5}$$

where $v_i$ $(i = 1, 2)$ and $v_z$ are discontinuous control laws, which make the states $\bar{x}$, $\bar{y}$ and $\bar{z}$ of Eq. (5) approach $x$, $y$ and $z$, respectively. It is these discontinuous control laws that make the hidden message be recovered using the idea of fault detection and identification.

### 3.1. Analysis of error dynamics

Define the estimation error as follows:

$$e = \begin{pmatrix} e_1 \\ e_2 \\ e_z \end{pmatrix} = \begin{pmatrix} x - \bar{x} \\ y - \bar{y} \\ z - \bar{z} \end{pmatrix}. \tag{6}$$

From Eqs. (2)–(6), the dynamics of the error is given by

$$\dot{e}_1 = e_2 - v_1 + d_1 m,$$
$$\dot{e}_2 = -k_1 e_1 - k_2 e_2 - v_2 + d_2 m,$$
$$\dot{e}_z = -k_1 e_1 - k_2 e_2 - e_z - v_z + \dot{z}. \tag{7}$$

In compact notation one can write Eq. (7) as follows:

$$\dot{\bar{e}} = A\bar{e} - \bar{v} + \bar{d}m,$$
$$\dot{e}_z = -K^{\mathrm{T}}\bar{e} - e_z - v_z + \dot{z}, \tag{8}$$

where

$$A = \begin{pmatrix} 0 & 1 \\ -k_1 & -k_2 \end{pmatrix}, \qquad \bar{e} = \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}, \qquad \bar{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix},$$
$$\bar{d} = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}, \qquad K = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}. \tag{9}$$

Here it is worth noting that nonzero constants $k_i$ $(i = 1, 2)$ should be chosen such that the matrix $A$ is stable.

Suppose that the emitter (2) is chaotic, which means there exists a positive constant $\delta_z$ such that $|\dot{z}| < \delta_z$. In the sequel we will prove that Eq. (8) can be exponentially stable at origin provided that some discontinuous control laws are constructed. Let

$$V(e) = \bar{e}^{\mathrm{T}} P \bar{e} + e_z^2 \tag{10}$$

be a Lyapunov function of Eq. (8), where matrix $P$ is positive-definite. Along the solution of Eq. (8), the derivative of $V(t)$ with respect to time is described by

$$\dot{V} = 2\bar{e}^{\mathrm{T}}\left[A^{\mathrm{T}}P + PA\right]\bar{e} + 2\bar{e}^{\mathrm{T}}P(-\bar{v} + \bar{d}m)$$
$$- 2e_z^2 - 2e_z K^{\mathrm{T}}\bar{e} - 2e_z v_z + 2e_z\dot{\bar{z}}.$$

Applying the following inequality

$$-2\xi^{\mathrm{T}}\eta \leqslant \gamma\xi^{\mathrm{T}}\xi + \frac{1}{\gamma}\eta^{\mathrm{T}}\eta,$$

in which $\xi$, $\eta$ are vectors with same dimensions and $\gamma$ is an arbitrary positive constant, we have

$$-2e_z^{\mathrm{T}} K^{\mathrm{T}}\bar{e} \leqslant \mu e_z^2 + \frac{1}{\mu}\bar{e}^{\mathrm{T}} K K^{\mathrm{T}}\bar{e} \tag{11}$$