Available online at www.sciencedirect.com
SCIENCE DIRECT®
Chaos, Solitons and Fractals 25 (2005) 573–578
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

A sliding mode observer based secure communication scheme

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

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

Accepted 23 November 2004

Abstract

In the drive-response framework, this paper proposes a new secure communication scheme using the concept of equivalent control. For a given chaotic drive system, a sliding mode observer based response system can be constructed to synchronize the drive system. If they satisfy certain conditions, the hidden message can be recovered directly by the concept of equivalent control. Theoretical analysis and numerical simulation verify the effectiveness of the proposed scheme.

1. Introduction

In the past decades the synchronization of chaotic systems and its application to secure communication have been an interesting topics in the field of chaos [1–11]. In their seminal paper, Pecora and Carroll (1990) addressed the synchronization of chaotic systems in the drive-response framework. System decomposition method [1], iteration method [2] and observer based method [4–11] had been proposed to realize different synchronization phenomena. One important reason for chaos synchronization is the successful application of chaos to secure communication. So far, many ideas and methods have been proposed to realize the problem of chaotic secure communication including the inverse system method [3], the observer method [4,6,10,11] and the system theory method [9].

In this paper, we also consider the secure communication problem in the drive-response framework. Differing from many secure communication methods, this paper can recover the hidden message directly using the concept of equivalent control, which is utilized widely in the field of fault diagnosis [12,13]. For a given chaotic drive system with the hidden message, a sliding mode observer based response system is constructed to synchronize the drive system. With the help of a discontinuous action, an ideal sliding motion takes place on a certain hyperplane, which results in the recovery of the hidden message via the concept of equivalent control. Theoretical analysis and numerical simulation verify the effectiveness of the proposed scheme.

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

0960-0779/$ - see front matter
doi:10.1016/j.chaos.2004.11.075

2. Problem statement

We consider the following chaotic systems:

$$\begin{aligned} \dot{x} &= Ax + f(x,y) + Bm \\ y &= Cx \end{aligned} \tag{1}$$

where $x \in R^n$ is the state vector, $y \in R^p$ is the output vector, $m \in R^p$ is the message vector, and f:$R^n \times R^p \to R^n$ is a nonlinear vector-valued function. Here the matrices B and C are full column rank and full row rank respectively.

Generally speaking, only partial states of system (1) can be measured. Therefore, without loss of generality, the matrix C can be denoted by $C = [I_p\ 0]$. Further, in the secure communication scheme, the gain B of message $m(t)$ could be arbitrarily. In the paper, the gain B is chosen as $B = [I_p\ 0]^T \in R^{n \times p}$, which implies that matrices B and C have the same rank.

In order to recover the message m, we must make the following assumptions:

Assumption A1. The function $f(x, y)$ is Lipschitz with respect to the state x, where γ is a Lispchitz constant.

Assumption A2. The message m is norm bounded by a known positive constant δ, namely $\|m\| \leqslant \delta$.

3. Chaotic secure communication

Recently, the concept of equivalent control has been utilized in the field of fault diagnosis, whose aim is to analyze possible faults in the actuators and sensors. From the works [12,13], we know that the concept of equivalent control can recover the actuator and sensor faults directly without using the residual signal, the basis for evaluating the faults. Here in the chaotic secure communication scheme, if we regard the message hidden in chaotic systems as the faults, the hidden message can be possibly recovered by the concept of equivalent control.

In this paper we try to apply this idea to the secure communication problem. In the drive-response framework, a sliding mode observer based response system for system (1) is constructed as follows:

$$\dot{\hat{x}} = A\hat{x} + f(\hat{x}, y) + Bv(t) + K(y - C\hat{x}) \tag{2}$$

where K is a feedback gain matrix, and v is a discontinuous control law to be determined.

The following theorem shows that the response system (2) can synchronize the drive system (1).

Theorem 1. *For the drive system* (1), *Assumptions* A1 *and* A2 *hold. The response system* (2) *can globally synchronize the drive system* (1) *if the following conditions are satisfied*:

(i) *there exist a symmetric positive definite matrix* P, *a gain matrix* K *and a positive constant* β *such that*

$$(A - KC)^{\mathrm{T}}P + P(A - KC) + \gamma^2 PP + (\beta + 1)I_n < 0 \tag{3}$$

$$B^{\mathrm{T}}P = TC \tag{4}$$

where T *is a constant matrix.*

(ii) *The discontinuous control law* $v(t)$ *is chosen as*

$$v(t) = \begin{cases} (\rho + \delta)\frac{T(y - C\hat{x})}{\|T(y - C\hat{x})\|}, & if\ \|T(y - C\hat{x})\| \neq 0 \\ 0, & if\ \|T(y - C\hat{x})\| = 0 \end{cases} \tag{5}$$

where ρ *is a positive constant.*

Proof. Let the error signal be $e = x - \hat{x}$. So the error dynamics between system (1) and system (2) is given by

$$\dot{e} = (A - KC)e + f(x,y) - f(\hat{x}, y) + Bm - Bv \tag{6}$$

From condition (i), we choose a Lyapunov function as $V(t) = e^{\mathrm{T}}\ Pe$. Therefore, the derivative of $V(t)$ along the solution of error dynamics (6) is