Physics Letters A 372 (2008) 6627–6632

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Chaotic secure communication based on strong tracking filtering

Li Xiongjie [a,b,*], Xu Zhengguo [b], Zhou Donghua [b]

[a] Zhejiang Business Technology Institute, Ningbo 315012, PR China
[b] Department of Automation, Tsinghua University, Beijing 100084, PR China

ARTICLE INFO

Article history:
Received 21 June 2008
Accepted 18 September 2008
Available online 24 September 2008
Communicated by A.R. Bishop

PACS:
05.45.Vx
05.45.Gg

Keywords:
Secure communication
Strong tracking filtering
Chaos
Message estimation

ABSTRACT

A scheme for implementing secure communication based on chaotic maps and strong tracking filter (STF) is presented, and a modified STF algorithm with message estimation is developed for the special requirement of chaotic secure communication. At the emitter, the message symbol is modulated by chaotic mapping and is output through a nonlinear function. At the receiver, the driving signal is received and the message symbol is recovered dynamically by the STF with estimation of message symbol. Simulation results of Holmes map demonstrate that when message symbols are binary codes, STF can effectively recover the codes of the message from the noisy chaotic signals. Compared with the extended Kalman filter (EKF), STF has a lower bit error rate.

1. Introduction

In the past decades chaos has been an interesting topic in the field of nonlinear science. It is well known that chaotic systems are highly sensitive to initial conditions, and they can be regarded as the carrier of messages in the application to secure communication. So far, many ideas and methods have been proposed to resolve the problem of chaotic secure communication, such as the inverse system method [1], the observer method [2] and [3], the system theory method [4], the extended Kalman filtering method [5] and [6], the particle filtering method [7] and [8]. In Refs. [9,10] and [11], we also utilized the concept of equivalent control to directly recover the messages hidden in chaotic systems, which is a useful supplement for chaotic secure communication.

Another progress in signal processing is the strong tracking filter (STF) that Zhou and Frank (1996) proposed [12] for the state estimation of nonlinear processes, with its name coming from the fact that (i) it has strong tracking ability to the states no matter whether the states change abruptly or slowly, and whether the process has reached steady state or not, and (ii) it has definite robustness against model uncertainties. STF is in fact the extension of the Extended Kalman Filter with introducing sub-optimal fading factors. STF is especially applicable for estimating the states and parameters of nonlinear time-varying random systems.

In this Letter, we apply STF to the problem of chaotic secure communication. To begin with, a scheme for implementing secure communication based on chaotic maps and STF is proposed. Then, a modified STF algorithm, namely a STF with message estimation, is developed to meet the special requirements of chaotic secure communication. At last, the modified STF algorithm is used to dynamically estimate the messages hidden in chaotic Holmes map, when message symbols are binary codes, the modified STF can effectively recover the codes of the message from the noisy chaotic signals, simulation results demonstrate the effectiveness of the proposed approach.

The rest of this Letter is organized as follows: Section 2 provides a scheme for implementing secure communication based on chaotic maps and strong tracking filter. Section 3 presents message estimation with a Bayesian classifier and a modified strong tracking algorithm which estimation message on line. Section 4 gives some numerical simulations. In the end, Section 5 concludes the Letter.

2. A scheme for implementing secure communication

Consider the following chaotic maps in the form of

$$\begin{aligned} \boldsymbol{x}(k+1) &= \boldsymbol{f}\big(\boldsymbol{x}(k)\big) + \boldsymbol{s}(k) + \boldsymbol{w}(k), \\ \boldsymbol{y}(k) &= \boldsymbol{h}\big(\boldsymbol{x}(k)\big) + \boldsymbol{v}(k) \end{aligned} \tag{1}$$

* Corresponding author at: Department of Mechanical & Electrical Engineering, Zhejiang Business Technology Institute, Nantu Lianfeng overpass, Ningbo 315012, Zhejing, PR China. Tel.: +86 0574 87422117; fax: +86 0574 87422061.
E-mail address: lixiongjie@tsinghua.org.cn (X. Li).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2008.09.028

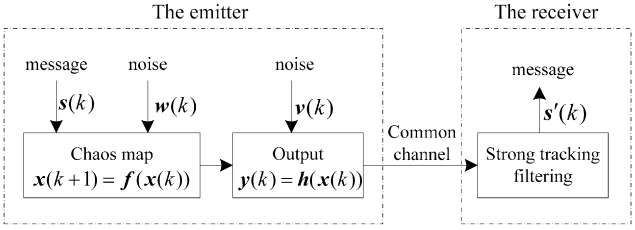

Fig. 1. The STF-based secure communication scheme.

where integer $k \geqslant 0$ is the disperse time index variable, $\boldsymbol{x} \in \boldsymbol{R}^n$ is the state vector, $\boldsymbol{y} \in \boldsymbol{R}^m$ is the output vector, $\boldsymbol{f}(\cdot): \boldsymbol{R}^n \to \boldsymbol{R}^n$ is the nonlinear function, and $h(\cdot)$: $\boldsymbol{h}(\cdot): \boldsymbol{R}^n \to \boldsymbol{R}^m$ stands for the nonlinear output function. Further, the system noise $\boldsymbol{w} \in \boldsymbol{R}^n$ is zero-mean Gaussian white noise with variance $\boldsymbol{Q}$, the measurement noise $\boldsymbol{v} \in \boldsymbol{R}^m$ is also zero-mean Gaussian white noise with variance $\boldsymbol{R}$.

In the above system, the vector $\boldsymbol{s} \in \boldsymbol{R}^n$ stands for the message vector. At the kth step each element of the message vector s_k belongs to the set $\boldsymbol{S} = \{\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \ldots, \boldsymbol{\theta}_M\}$ where $\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \ldots, \boldsymbol{\theta}_M$ are different constant vectors. Here, we assume that the vectors $\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \ldots, \boldsymbol{\theta}_M$ do not change the chaos nature of map (1).

In the field of chaotic secure communication, the chaotic map (1) can be regarded as the emitter, and the output signal $\boldsymbol{y}(k)$ is the driving signal, which is sent to the receiver through public channels. Therefore, our problem in this Letter is to dynamically estimate the modulated message $\boldsymbol{s}(k)$ using the driving signal $\boldsymbol{y}(k)$, even if the driving signal is arbitrarily nonlinear and there exist noises in the emitter (1).

In order to realize the above task, we first illustrate our scheme for implementing secure communication based on chaotic maps and STF. And then, a modified STF algorithm which estimates message on line is developed to meet the special requirements of chaotic secure communication in the subsequent section. The communication scheme is shown in Fig. 1. At the emitter, the message $\boldsymbol{s}(k)$ is modulated by the chaotic map $\boldsymbol{x}(k+1) = \boldsymbol{f}(\boldsymbol{x}(k))$ with the nonlinear output $\boldsymbol{y}(k) = \boldsymbol{h}(\boldsymbol{x}(k))$, which are disturbed by noises $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$. At the receiver, if the driving signal $\boldsymbol{y}_k$ is received, the particle filters will dynamically estimate the messages.

3. Strong tracking filters with message estimation

In this section, we first introduce the message estimation with an approximate Bayesian classifier, and then we propose a modified STF algorithm with message estimation using the above-mentioned Bayesian classifier.

3.1. Message estimation with a Bayesian classifier

The probability of each element of the set $\boldsymbol{S}$, which is denoted as $\Pr(\boldsymbol{s}(k) = \theta_l)$ for $l = 1, 2, \ldots, M$, is assumed to be known as prior knowledge. In order to maximize the channel efficiency in our communication scheme, the encoding is designed to achieve the maximum entropy of the messages to be transferred, which is used in many other communication systems. Therefore, the prior probability of each element is $1/M$, when the maximum entropy is attained. On receiving the driving signal $\boldsymbol{y}(k+1)$, according to Bayesian formula [13], we have

$$\Pr\big(\boldsymbol{s}(k) = \theta_l | \boldsymbol{y}(k+1)\big) = \frac{p(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_l)\Pr(\boldsymbol{s}(k) = \theta_l)}{\sum_{j=1}^{M} p(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_j)\Pr(\boldsymbol{s}(k) = \theta_j)} \tag{2}$$

for $l = 1, 2, \ldots, M$. Then we approximate the prior probability density $p(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_l)$

$$p\big(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_l\big) \approx p_v\big(\boldsymbol{y}(k+1) - h\big(\boldsymbol{x}_{\theta_l}(k+1|k)\big)\big) \tag{3}$$

for $l = 1, 2, \ldots, M$, $\boldsymbol{x}_{\theta_l}(k+1|k) = \boldsymbol{f}(\boldsymbol{x}(k|k)) + \theta_l$ where $p_v(\cdot)$ is the probability density function of the measurement noise. Hence, the posterior probability can be approximated by

$$\begin{aligned}
&\Pr\big(\boldsymbol{s}(k) = \theta_l | \boldsymbol{y}(k+1)\big) \\
&= \frac{p(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_l)\Pr(\boldsymbol{s}(k) = \theta_l)}{\sum_{j=1}^{M} p(\boldsymbol{y}(k+1)|\boldsymbol{s}(k) = \theta_j)\Pr(\boldsymbol{s}(k) = \theta_j)} \\
&\approx \frac{p_v(\boldsymbol{y}(k+1) - h(\boldsymbol{x}_{\theta_l}(k+1|k)))\Pr(\boldsymbol{s}(k) = \theta_l)}{\sum_{j=1}^{M} p_v(\boldsymbol{y}(k+1) - h(\boldsymbol{x}_{\theta_j}(k+1|k)))\Pr(\boldsymbol{s}(k) = \theta_j)} \\
&\propto p_v\big(\boldsymbol{y}(k+1) - h\big(\boldsymbol{x}_{\theta_l}(k+1|k)\big)\big)\Pr\big(\boldsymbol{s}(k) = \theta_l\big)
\end{aligned} \tag{4}$$

for $l = 1, 2, \ldots, M$. An approximate Bayesian classifier is formed to estimate the message $\boldsymbol{s}'(k)$ by

$$\boldsymbol{s}'(k) = \arg \max_{\theta_l,\, l=1,2,\ldots,M} p_v\big(\boldsymbol{y}(k+1) - h\big(\boldsymbol{x}_{\theta_l}(k+1|k)\big)\big)\Pr\big(\boldsymbol{s}(k) = \theta_l\big). \tag{5}$$

3.2. The modified strong tracking filter algorithm

The core of the STF is to introduce a time-varying sub-optimal fading factor [12] into the Extended Kalman Filter, to adjust the covariance matrix and the corresponding gain matrix with the state prediction error in real time. The goal is to make the least number for the error variance of the state estimation, together with estimation of the chaos.

To apply STF to chaotic secure communication, we introduce a few necessary improvements on the original STF algorithm proposed in Ref. [12]. We summarize the modified STF algorithm as the following Algorithm 1. In the subsequent section, this algorithm will be used to estimate the modulated message $\boldsymbol{s}(k)$.

Algorithm 1.

Step 1: Initialization. Choose the initial state $\hat{\boldsymbol{x}}(0|0)$ and $\boldsymbol{P}(0|0)$.

Step 2: Message estimation and state prediction. On receiving the driving signal $\boldsymbol{y}(k+1)$, the approximate Bayesian classifier is formed to estimate the message $\boldsymbol{s}'(k)$ by

$$\boldsymbol{s}'(k) = \arg \max_{\theta_l,\, l=1,2,\ldots,M} p_v\big(\boldsymbol{y}(k+1) - h\big(\boldsymbol{x}_{\theta_l}(k+1|k)\big)\big)\Pr\big(\boldsymbol{s}(k) = \theta_l\big) \tag{6}$$

state step prediction:

$$\hat{\boldsymbol{x}}(k+1|k) = \boldsymbol{f}\big(\hat{\boldsymbol{x}}(k|k)\big) + \boldsymbol{s}'(k). \tag{7}$$

Step 3: Part linearization:

$$\boldsymbol{F}\big(\hat{\boldsymbol{x}}(k|k)\big) = \left.\frac{\partial \boldsymbol{f}(\boldsymbol{x}(k))}{\partial \boldsymbol{x}}\right|_{\boldsymbol{x}(k)=\hat{\boldsymbol{x}}(k|k)}, \tag{8}$$

$$\boldsymbol{H}\big(\hat{\boldsymbol{x}}(k+1|k)\big) = \left.\frac{\partial \boldsymbol{h}(\boldsymbol{x}(k+1))}{\partial \boldsymbol{x}}\right|_{\boldsymbol{x}(k+1)=\hat{\boldsymbol{x}}(k+1|k)}. \tag{9}$$

Step 4: The error vectors sequence:

$$\boldsymbol{y}(k+1) = \boldsymbol{y}(k+1) - \boldsymbol{h}\big(\hat{\boldsymbol{x}}(k+1|k)\big). \tag{10}$$

Step 5: The sub-optimal fading factor matrix $\boldsymbol{\lambda}(k+1) = \operatorname{diag}\{\lambda_1(k+1), \lambda_2(k+2), \ldots, \lambda_n(k+1)\}$, where $\lambda_i(k+1)$ by:

$$\lambda_i(k+1) = \begin{cases} \lambda_0, & \lambda_0 > 1, \\ 1, & \lambda_0 \leqslant 1, \end{cases} \tag{11}$$

for $i = 1, 2, \ldots, n$, where λ_0 by:

$$\lambda_0 = \frac{\operatorname{tr}[\boldsymbol{N}(k+1)]}{\operatorname{tr}[\boldsymbol{M}(k+1)]}, \tag{12}$$