Applied Mathematical Modelling 38 (2014) 4717–4732

Contents lists available at ScienceDirect

Applied Mathematical Modelling

journal homepage: www.elsevier.com/locate/apm

Universal prediction-based adaptive fault estimator applied to secure communication

Jason Sheng-Hong Tsai [a,*], Wen-Teng Hsu [a], Chao-Lung Wei [a], Shu-Mei Guo [b,*], Leang-San Shieh [c]

[a] Control System Laboratory, Department of Electrical Engineering, National Cheng Kung University, Tainan 701, Taiwan, ROC
[b] Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan, ROC
[c] Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204-4005, USA

ARTICLE INFO

Article history:
Received 17 April 2012
Received in revised form 3 March 2014
Accepted 20 March 2014
Available online 31 March 2014

Keywords:
Secure communication
Nonlinear system
Prediction-based adaptive observer
Fault detection and diagnosis
Performance recovery
Digital redesign

ABSTRACT

In this paper, a communication scheme that could use a nonlinear dynamical system to create encrypted keys with an additional dimension is proposed, and the scheme could keep encrypted keys not to diverge. Since the divergence of encrypted keys (nonlinear signals) easily happens in non-linear systems coupled with other systems, the adaptive control approach, proposed in this paper, uses the universal state-space adaptive observer-based fault diagnosis/estimator and the high-performance tracker to eliminate the divergence of encrypted keys. At the same time, the receiver of communication retrieves informal messages by the universal state-space adaptive observer-based fault diagnosis/estimator and the high-performance tracker. Thus, this paper takes advantage of the merit of digital redesign methodology for a practical implementation of secure-communication, and the estimator solves the problem of secure communication. Thus developed a new approach could add more dimensions into nonlinear secure-communication systems without having the problem of divergence of encrypted keys.

1. Introduction

Chaotic-secure-communication system is to use the feature of chaos which produces irregular and unpredictable signals by different parameters. The parameters of chaotic system are the encryption key in the transmitter and the receiver. Two chaotic systems with the same parameters can synchronize to produce identical signals in the transmitter and the receiver [1]. Thus, the signals of encryption have the features of chaotic systems, irregular and unpredictable, and, at the same time, the signals could be good encryption-keys because of identical trajectories. So, a secret message is encoded in chaotic signals, produced from state of chaotic systems such as Lerenz, Chau etc. However, it should be noticed that encrypted messages, which are created by chaotic systems with high dimensions, are easily diverged, so traditional chaotic systems do not have many dimensions. In this paper, we redesign a communication scheme that could create secure signals with additional dimensions, and the scheme could keep encrypted keys not to diverge. Since the divergence of encrypted keys (or nonlinear signals) easily happens in non-linear systems coupled with other systems, the adaptive control approach, proposed in this paper, is using the universal state-space adaptive observer-based fault diagnosis/estimator and the high-performance

* Corresponding authors.
E-mail addresses: shtsai@mail.ncku.edu.tw (J. Sheng-Hong Tsai), guosm@mail.ncku.edu.tw (S.-M. Guo).

http://dx.doi.org/10.1016/j.apm.2014.03.028
0307-904X/

tracker to eliminate the divergence of encrypted messages. And, the same method using in the receiver could retrieve informal messages. So, the communication scheme provides a higher security-degree.

Firstly, the additional dimension of encryption in this paper is using the linear time-varying uncertain system in communication systems. The study of robust stability of linear time-varying uncertain system has gained increasing attention in recent years. The Lyapunov function can be homogeneous of arbitrary degree in the state. It is worthwhile to mention that the class of methods are based on piecewise quadratic Lyapunov function [2]. The demand on reliability for safety–critical systems grows. For example, spacecraft and probes require robust control and fault tolerant capabilities, because these systems are potentially subjected to unexpected anomalies and faults in actuators, sensors, components, or subsystems. The problem of fault detection, isolation, and recovery (FDIR) for the satellite's orbital and attitude models through construction of residual generators based on least-squares parameter estimation techniques has been proposed [3].

Since we couple an additional nonlinear system to create signals, the encrypted keys induced by created signals are easy to diverge. We use the fault detection and diagnosis (FDD) for actuator and state faults to eliminate the divergence of encrypted keys, and, on the other hand, the receiver of secure communication could use the same method to retrieve what is eliminated, the informal signal. FDD areas have been thriving enormously over the past 30 years, particularly in applications such as aerospace, electric power, robotics, automobiles, etc. The practical FDD problem along with prognostics from control engineering perspective and the potential software agent solutions are proposed in [4].

Many passive [5] and/or active [6,7] actuator fault tolerant controls (FTC) have been developed, such as a sufficient condition for the solvability of the stabilizing output feedback control problem [8], sliding mode designs [9], adaptive technique designs [10–13], fault detection and diagnosis designs [14,15], multiple-model designs [16], neural network designs [17–19] and so on.

A parameter adaptation algorithm for observer has been offered through the overall estimation of error equations [20]. Some results in the design of adaptive observers with an arbitrary exponential convergence rate are also presented. Joint state and bias estimation has been studied [21]. Besides, the adaptive observer of the continuous-time system has been proposed to estimate unanticipated decay factors for a linear time-varying MIMO system [22]. Fault detection and identification is an active research field in several application areas. When the typical actual faults occur, it is possible to create suitable fault detection and isolation approaches [23] to detect them. Also, a Kalman filter-based adaptive observer has been proposed in [24] for actuator fault detection/estimation and performance recovery, but the state fault has not been considered.

Theoretically, an analog controller with the high-gain property for a continuous-time system can be well-designed for the high-performance tracking purpose. However, the excessive amplitude of the analog control input often exceeds the so-called limit of control input saturation in actual systems, so it may not be implemented in practice. Nevertheless, based on the digital redesign method [25], in theory, we can determine a realizable low-gain sampled-data controller and make high design performance as efficient as the original analog controller.

This paper is to propose the prediction-based adaptive observer and tracker, an application of FDD, for the sampled-data linear time-varying system, with an additional dimension of secure communications, so that it (i) improves the traditional adaptive observer methodology in literature [23,24] to yield a high-performance adaptive observer; (ii) presents an universal mechanism for both the fault detection/estimation and fault-tolerant tracker for the occurrence of unanticipated fault either in state, induced by system component fault in integrator, or input of a given sampled-data linear time-varying system; (iii) applies to eliminate the divergence of nonlinear signals and retrieve messages in secure communications.

This paper takes advantage of the merit of digital redesign methodology to convert a theoretically well-designed analog controller/observer for linear systems into its corresponding digital controller/observer for a practical implementation, and the estimator solves the problem of secure communication. The effectiveness and efficiency of proposed design methodology are illustrated through tracking control simulation examples. In the conclusion, we try to develop a new approach to add more dimensions into the nonlinear secure-communication system induced by the added nonlinear signals to be synchronized at both the transmitter and receiver without having the problem of divergence of encrypted keys.

2. An improved prediction-based adaptive observer

Firstly, the analog/digital adaptive observer and its robustness analysis in literature [22,23,25] is summarized. Secondly, based on the digital redesign approach, the prediction-based adaptive observer for state estimation and actuator fault detection and diagnosis for a sampled-data linear time-varying system and its robustness analysis will be proposed, where the estimated state and FDD at time index $t = kT$ depends on measurement up to the same time index $t = kT$. Finally, the prediction-based adaptive observer is proposed to enhance the estimation efficiency and speed up the compensation for slowly-changing time-varying actuator fault.

2.1. Adaptive observer

Literature [22] considers the linear time-varying (LTV) multiple-input-multiple-output (MIMO) system in the state-space form

$$\dot{x}(t) = A(t)x(t) + B(t)u(t) + \Lambda(t)\theta(t), \quad (1a)$$

$$y(t) = C(t)x(t), \quad (1b)$$