Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 9518403, 10 pages
https://doi.org/10.1155/2019/9518403

Research Article

State Estimation and Event-Triggered Control for Cyber-Physical Systems under Malicious Attack

Yongzhen Guo[1,2], **Baijing Han**[3,4], **Weiping Wang**[3,4] and **Manman Yuan**[3,4]

[1]*School of Automation, Beijing Institute of Technology, Beijing 100081, China*
[2]*China Software Testing Center, Beijing 100048, China*
[3]*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China*
[4]*China Beijing Key Laboratory of Knowledge Engineering for Materials Science, Beijing 100083, China*

Correspondence should be addressed to Yongzhen Guo; yzguo@cstc.org.cn and Weiping Wang; shiya666888@126.com

Received 5 July 2019; Revised 27 September 2019; Accepted 15 October 2019; Published 14 November 2019

Academic Editor: Xiao-Qiao He

Copyright © 2019 Yongzhen Guo et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper is concerned with the security state estimation and event-triggered control of cyber-physical systems (CPSs) under malicious attack. Aiming at this problem, a finite-time observer is designed to estimate the state of the system successfully. Then, according to the state information, the event-triggered controller is designed through the event-triggered communication. It is proved that the system is uniformly and finally bounded. Finally, the effectiveness of the proposed method is verified by a simulation example.

1. Introduction

Nowadays, in modern control systems, network systems, information systems, and control systems show the characteristics of in-depth integration. In order to study this kind of system, the concept of cyber-physical system (CPS) has been put forward in [1]. CPS is a highly integrated and interactive intelligent system between computing units and physical objects in the network environment. However, it is precisely because of the close relationship between information processing and dynamic processes that it is particularly vulnerable to errors or attacks in data transmission. And this can result in much losses or major damage, such as the Brazilian power grid blackouts and the shock waves against Iran virus attack. The security of CPSs has attracted wide attention of the scientific community.

Due to the vulnerability of CPSs, various types of attacks are injected into those systems in a covert and unpredictable way. At present, there are some articles related to the security of information physical systems, which generally contain two categories. The first category focuses on attack detection, such as [2–6]. The second category focuses on safety state estimation and safety controller design. But most of the current research focuses on the former, and the secure state estimation and the control for CPSs have not been fully investigated. So how to ensure state estimation and control safely in the presence of attacks are still an urgent problem to be solved.

State estimation plays an important role in control theory. It can explain the dynamic characteristics of the system more clearly than the traditional method, and it also can achieve special control tasks. Especially when the state of system cannot be measured directly, state estimation is particularly important. Moreover, designing an appropriate observer is an effective way to solve the problem of state estimation in [7, 8]. Observer is a type of dynamic system that is derived from the actual values of the system's external variables (input variables and output variables), and it is also called a state reconstructor. They are similar to the reference generator, but their scope of application is different. The reference generator is mainly used for the circuit generation.

When an unknown subset of sensors was arbitrarily destroyed by an opponent, Mishra et al. studied the security estimation of the linear dynamic system in [9]. Mitra and

Sundaram studied the problem of collaboratively estimating the state of an LTI system monitored by a network of sensors (nodes) in [10]. When some sensors or actuators were destroyed, Mishra et al. [9] studied the estimation and control of linear systems. A safety state estimation algorithm is proposed. Liao and Chakrabortty [11] also developed a set of algorithms that can detect the identities of malicious data manipulators in large-power system models. However, the above algorithmic method has the disadvantage of losing the correctness guarantee, while the observer-based method has a fast response and saves the computing resources. A novel state observer was proposed in [12, 13]. Lu and Yang studied the problem of security state estimation of network physical systems and proposed a new security Luenberger observer in reference [14]. It should be noted that in [9,13–15], the results allow only exponential convergence of the estimation error, or a limited but sufficiently large step to obtain the safety state estimation, which means that it may take quite a long time. This requires a specified finite-time estimate. Although Ao et al. [16] introduced two concepts of elastic observability index and sparse index of the system and designed a finite-time state observer with state correction, the actuator attack is not taken into account. Thus, studying the finite-time state estimate under actuator attack is meaningful.

However, in addition to security state estimation for CPSs, different security control strategies need to be considered to reduce the performance degradation caused by attacks. Recently, a lot of research about the control of CPSs has been lunched, such as [14,17–20]. Many effective and novel design methods have been proposed, including linear feedback, sliding mode control, elastic control, and T-S fuzzy control.

For stochastic network attacks in the system, Liu et al. [21] proposed a distributed controller mechanism for stochastic network attacks and verified the stability of the system with Lyapunov function. In [22], a continuous-time controller based on the observer was presented to solve the problem of system reliability control. An improved adaptive resilient control scheme to mitigate the system's antagonistic attacks was provided in [23]. In addition, Pang et al. and Ding et al. [24, 25] solved the problem of elastic nonlinear control according to the application of industrial 4.0. And Dolk et al. [26] proposed a systematic design framework for output-based dynamic event-triggered control (ETC) systems under denial-of-service (DoS) attacks. In reference [8], an adaptive event trigger scheme based on random sensor fault was proposed. However, most of the above studies are aimed at observer continuous control, and few of them are designed to event-triggered control because of the network resources of CPSs are limited in the integration of computing, network, and physical processes. It is of great significance to study event-triggered control of CPSs under malicious attacks. Although Dolk et al. and Nowzari et al. [26, 27] discussed the event-triggered control for CPSs, they did not consider the malicious attacks.

Motivated by the above reasons, this paper studies the problem of the secure state estimation and event-triggered control for CPSs. The main contributions of this paper are summarized as follows:

(1) Inspired by Ao et al. in [16], we have proposed a finite-time observer to estimate the state of the system with actuator attacks. Ao et al. [16] studied the state estimation of systems against sensor attacks, while this article focuses on actuator attacks.

(2) Inspired by the study of Zhang and Feng in reference [28], considering the resource constraints of the system, event-triggered control is introduced into the attacked cyber-physical system. Finally, it is proved that the system is uniformly ultimately bounded.

(3) Finally, based on the Lyapunov stability analysis method, it is proved that the time interval is not equal to 0, which effectively avoids the Zeno behavior.

2. System Model

The system model is

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + D\eta(t), \\ y(t) = Cx(t), \end{cases} \tag{1}$$

where $x \in R^n$ represents the system state vector; $u \in R^m$ and $\eta \in R^m$ denote the control input vector and the actuator attack; $y \in R^q$ is the output vector; and A, B, D, and C are the system matrices with appropriate dimensions with $m \geq q$, where $m = \text{rank}C$ and $q = \text{rank}D$.

Assumption 1. The pairs (A, B) and (C, A) are controllable and observable, respectively.

Assumption 2. The system is feedback.

3. Design of the Finite-Time Observer

3.1. Transform of the System. In this part, a finite-time observer for system (1) can be designed. We define $x = T\overline{x}$ with $T = [\, N \;\; D \,]$, $N \in R^{n\times(n-q)}$. Then, the system can be transformed into

$$\begin{cases} \overline{x}(t+1) = \overline{A}\overline{x}(t) + \overline{B}u(t) + \overline{D}\eta(t), \\ y(t) = \overline{C}\overline{x}(t), \end{cases} \tag{2}$$

where $\overline{x} = [\, \overline{x}_1 \;\; \overline{x}_2 \,]$, in which $\overline{x}_1 \in R^{n-q}$ and $\overline{x}_2 \in R^q$. The transformed system (2) under the transformation $x = T\overline{x}$ is given by

$$\begin{aligned} \overline{A} &= T^{-1}AT = \begin{bmatrix} \overline{A}_{11} & \overline{A}_{12} \\ \overline{A}_{21} & \overline{A}_{22} \end{bmatrix}, \\ \overline{B} &= T^{-1}B = \begin{bmatrix} \overline{B}_1 \\ \overline{B}_2 \end{bmatrix}, \\ \overline{D} &= T^{-1}D = \begin{bmatrix} 0 \\ I_q \end{bmatrix}, \\ \bar{C} &= CD = [\, CNCD \,]. \end{aligned} \tag{3}$$

Due to the transformation, only the system state $\overline{x}_2$ of system (2) depends on the attack signal η. Using the transformation $\overline{y} = [\,\overline{y}_1 \;\; \overline{y}_2\,]^T = U^{-1}y$, with

$$U = [\,CD \;\; Q\,],$$
$$U^{-1} = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}, \tag{4}$$

where $Q \in R^{m\times(m-q)}$, $U_1 \in R^{q\times m}$, and $U_2 \in R^{(m-q)\times m}$, we have

$$\overline{y}_1 = U_1 y = U_1 CN\overline{x}_1 + \overline{x}_2, \tag{5}$$

$$\overline{y}_2 = U_2 y = U_2 CN\overline{x}_1. \tag{6}$$

Substituting $\overline{x}_2 = U_1 y - U_1 CN\overline{x}_1$ obtained from (5) in (2). The transformed system (2) under the transformation (4) is

$$\begin{aligned} \overline{x}_1(t+1) &= \widetilde{A}_1\overline{x}_1(t) + \overline{B}_1 u(t) + E_1 y(t), \\ y_2(t) &= \widetilde{C}_1\overline{x}_1(t), \end{aligned} \tag{7}$$

with the matrix

$$\begin{aligned} \widetilde{A}_1 &= \overline{A}_{11} - \overline{A}_{12}U_1 CN, \\ E_1 &= \overline{A}_{12}U_1, \\ \widetilde{C}_1 &= U_2 CN. \end{aligned} \tag{8}$$

3.2. Main Result. In this part, the finite-time observer for system (1) is designed. The finite-time observer consists of two observers for the transformed (7) as follows:

$$\begin{aligned} \dot{z}_1(t) &= \left(\widetilde{A}_1 - L_1\widetilde{C}_1\right)z_1(t) + \overline{B}_1 u(t) + L_1^* y(t), \\ \dot{z}_2(t) &= \left(\widetilde{A}_1 - L_1\widetilde{C}_1\right)z_2(t) + \overline{B}_1 u(t) + L_2^* y(t), \end{aligned} \tag{9}$$

with $L^* = LU_2 + E_1$,

$$q(t) = M\left[z(t) - e^{F\tau}z(t-\tau)\right], \tag{10}$$

with $z = [\,z_1 \;\; z_2\,]^T$. In equation (10), q is the estimate of the transformed system (7). The state estimate of system (1) is obtained by using the transformation

$$\widehat{x}(t) = T\begin{bmatrix} q(t) \\ U_1 y(t) - U_1 CNq(t) \end{bmatrix}. \tag{11}$$

Hence, the finite-time observer for system (1) is

$$\begin{aligned} \dot{z}(t) &= Fz(t) + Hy(t) + Gu(t), \\ q(t) &= M\left[z(t) - e^{F\tau}z(k-\tau)\right], \\ \widehat{x}(t) &= T\begin{bmatrix} q(t) \\ U_1 y(t) - U_1 CNq(t) \end{bmatrix}, \end{aligned} \tag{12}$$

where

$$\begin{aligned} H &= \begin{bmatrix} L_1^* \\ L_2^* \end{bmatrix}, \\ F &= \begin{bmatrix} F_1 & 0_{n-q,n-q} \\ 0_{n-q,n-q} & F_2 \end{bmatrix}, \\ G &= \begin{bmatrix} \overline{B}_1 \\ \overline{B}_1 \end{bmatrix}, \\ S &= \begin{bmatrix} I_{n-q} \\ I_{n-q} \end{bmatrix}, \\ M &= \left[\, I_{n-q} \;\; 0_{n-q,n-q} \,\right]\left[\, S \;\; e^{F\tau} \;\; S \,\right]^{-1}. \end{aligned} \tag{13}$$

In (12), define the matrices F_i, $i = 1, 2$, as $F_i = \widetilde{A}_1 - L_i\widetilde{C}_1$. It is assumed that $z(t) = S\left[\, I_{n-q} \;\; 0_{n-q,q} \,\right]T^{-1}\,\widehat{x}(t_0)$, $\forall t \in [t_0 - \tau, 0]$ with arbitrary but bounded $\widehat{x}(t_0)$.

Theorem 1. *Suppose that the inverse of the matrix* $\left[\, S \;\; e^{F\tau} \;\; S \,\right]$ *exists. Then, (12) defines a finite-time observer for the system (1) and the observer estimates the exact state of system (1) in finite time* τ*, i.e.,* $\widehat{x}(t) = x(t)$, $\forall t \geq t_0 + \tau$.

Proof. The finite-time observer (12) estimates the states of system (1) in finite time τ. One obtains from (12) and (9)

$$\begin{aligned} &\frac{d}{dt}\left(z(t) - S\overline{x}_1(t)\right) \\ &\quad = Fz(t) + Hy(t) + Gu(t) \\ &\qquad - S\left[\widetilde{A}_1\overline{x}_1(t) + \overline{B}_1 u(t) + E_1 y(t)\right] \\ &\quad = Fz(t) - S\widetilde{A}_1\overline{x}_1(t) + \left(G - S\overline{B}_1\right)u(t) + \left(H - SE_1\right)y(t) \\ &\quad = Fz(t) - \begin{bmatrix} L_1U_2 \\ L_2U_2 \end{bmatrix}y(t) - S\widetilde{A}_1\overline{x}_1(t) \\ &\quad = Fz(t) - \begin{bmatrix} F_1 & 0_{n-q,n-q} \\ 0_{n-q,n-q} & F_2 \end{bmatrix}S\overline{x}_1(t) \\ &\quad = F\left(z(t) - S\overline{x}_1(t)\right). \end{aligned} \tag{14}$$

□

Hence, $z(t)$ is in the time interval $[t_0, t_0 + \tau]$ with $z(t_0) = S\widehat{\overline{x}}_1(t_0)$, where $\widehat{\overline{x}}_1(t_0) = \left[\, I_{n-q} \;\; 0_{n-q,q} \,\right]T^{-1}\widehat{x}(t_0)$,

$$\begin{aligned} z(t) &= S\overline{x}_1(t) + e^{F\left(t-t_0\right)}\left[z\left(t_0\right) - S\overline{x}_1\left(t_0\right)\right] \\ &= S\overline{x}_1(t) + e^{F\left(t-t_0\right)}S\left[\widehat{\overline{x}}_1\left(t_0\right) - \overline{x}_1\left(t_0\right)\right]. \end{aligned} \tag{15}$$

From equation (15), one can obtain for $t \geq t_0 + \tau$

$$z(t-\tau) = S\overline{x}_1(t-\tau) + e^{F\left(t-t_0-\tau\right)}\left[\widehat{\overline{x}}_1\left(t_0\right) - \overline{x}_1\left(t_0\right)\right], \tag{16}$$

and then, for $t \geq t_0 + \tau$,

$$\begin{aligned} q(t) &= M\left[z(t) - e^{F\tau} z(k-\tau)\right] \\ &= \underbrace{MS}_{I_{n-q}} \overline{x}_1(t) + Me^{F(t-t_0)} S\left[\widehat{\overline{x}}_1(t_0) - \overline{x}_1(t_0)\right] \\ &\quad - \underbrace{Me^{F\tau}}_{0_{n-q,n-q}} S\overline{x}_1(t-\tau) - \underbrace{Me^{F\tau} e^{F(t-t_0-\tau)}}_{e^{F(t-t_0)}} S\left[\widehat{\overline{x}}_1(t_0) - \overline{x}_1(t_0)\right] \\ &= \overline{x}_1(t). \end{aligned} \tag{17}$$

Then, for $t \geq t_0 + \tau$, the estimate $\widehat{x}(t)$ of system (1) is

$$\widehat{x}(t) = T\begin{bmatrix} \widehat{x}_1(t) \\ U_1 y(t) - U_1 CN\widehat{x}_1(t) \end{bmatrix}. \tag{18}$$

We define the observation error $e(t) = \widehat{x}(t) - x(t)$. From (18), it is followed that $\widehat{x}_1(t) = x(t)$ for all $t \geq t_0 + \tau$. Therefore, also $e(t) = 0$ for all $t \geq t_0 + \tau$.

Remark 1. The method assumes that the attacker knows the entire physical model. If only partial knowledge of the system is available, the finite-time observer designed in this paper is not available because the observer is designed according to the system parameters, but we can implement the complete model of the system according to the parameter estimation method and then design the observer accordingly. We will carry out related research in the future work.

Remark 2. If the actual physical system is nonlinear, while the attacker only has access to one linear model of it (some operating point) and designs the attack based on that model only, in this case, we should design multiple observer according to the state information of each node as the Ref. [10] says. The attacker can attack one node and affect the closed-loop stability. In the multiple observer setup, the state observer is distributed among multiple computing nodes. So we can design the corresponding observer for the node attacked, according to the nonlinear or linear model of the system. Then by analyzing the stability of each node, we can achieve the closed-loop stability. This is also our future research. In this manuscript, we assume the system is linear, and this is just a special case.

As a summary, a finite-time observer is presented in this section. The observer estimates the exact state of the CPS in a predefined finite time despite the actuator attacks. In the next section, we will discuss the control of the system.

4. Design of the Event-Triggered Controller

In order to better design the controller, in this section, we rewrite the model of system (1) as follows. The symbol means the same implications as before:

$$\begin{cases} \dot{x}(t) = Ax(t) + B(u(t) + E\eta(t)), \\ y(t) = Cx(t). \end{cases} \tag{19}$$

4.1. Definition of Event Detectors. In this paper, we consider continuous-time event detectors. In order to reduce the energy consumption caused by sensor data acquisition and frequent communication and to reduce the dependence on global state information in event-triggered control, we design a distributed event-triggered controller in this section. The new state and attack signal will be sampled for control input calculation when the following judgement algorithm is satisfied:

$$t_{k+1} = \inf\left\{t > t_k \mid e(t) \geq \gamma(t)\right\}, \quad \forall k \in N, \tag{20}$$

where $e(t) = \|x(t) - x(t_k)\|^2 + \|\eta(t) - \eta(t_k)\|^2$, $\gamma(t) = \varepsilon^{-\alpha t} + \varepsilon_0$, and $\varepsilon > 1$, $0 \leq \alpha < 1$ and $\varepsilon_0 \geq 0$.

4.2. Main Result. We have already assumed that system (1) is feedback. So under the event-triggered mechanism, the controller can be designed as

$$\mu(t) = Kx(t_k) - E\eta(t_k), \tag{21}$$

where K is the controller parameter with the appropriate dimension. We use the following theorem to ensure that the system is ultimately bounded. Throughout the discussion, we take the norm $\|\cdot\|$ of a specific vector as the Euclidean norm.

Theorem 2. *Consider the line system (19) under the attack from actuator with sampling instants determined by using (20). For given gain matrices K, if there is a symmetric positive definite matrix $P^T = P > 0$ satisfying the following matrix inequality,*

$$Q \triangleq (A + BK)^T P + P(A + BK) < 0, \tag{22}$$

then the system is finally stable and converges to a certain area:

$$\vartheta(\varepsilon_0) = \left\{x(t) \mid \|x(t)\| \leq \sqrt{\frac{\varepsilon_0}{\delta\lambda_{\min}(p)}}\right\}, \tag{23}$$

where $\delta = \lambda_{\min}(-Q)/\lambda_{\max}(p)$.

Proof. We define $\alpha(t) = x(t) - x(t_k)$ and $\beta(t) = \eta(t) - \eta(t_k)$. Based on system (19), we can obtain

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B\left(Kx(t_k) - E\eta(t_k) + E\eta(t)\right) \\ &= Ax(t) + BKx(t) - BK\alpha(t) - BE\eta(t) + BE\beta(t) \\ &= (A + BK)x(t) - BK\alpha(t) + BE\beta(t). \end{aligned} \tag{24}$$

□

Considering the Lyapunov function $v(t) = x(t)^T Px(t)$, the time derivative of $v(t)$ for $t \in [t_k, t_{k+1}]$ is

$$\begin{aligned}\dot{v}(t) &= \dot{x}^T(t)Px(t) + x^T(t)P\dot{x}(t)\\ &= ((A+BK)x(t) - BK\alpha(t) + BE\beta(t))^T Px(t)\\ &\quad + x^T(t)P((A+BK)x(t) - BK\alpha(t) + BE\beta(t))\\ &= x^T(t)\Big((A+BK)^T P + P(A+BK)\Big)x(t)\\ &\quad - \alpha^T(t)K^T B^T P - X^T(t)PBK\alpha(t)\\ &\quad + \beta^T(t)K^T B^T P + X^T(t)PBK\beta(t)\\ &= x^T(t)\Big((A+BK)^T P + P(A+BK) + PBKK^T B^T P\\ &\qquad - PBKK^T B^T P\Big)x(t)\\ &\quad - \left\|\beta(t) - K^T B^T Px(t)\right\|^2 + \|\beta(t)\|^2\\ &\quad - \left\|\alpha(t) - K^T B^T Px(t)\right\|^2 + \|\alpha(t)\|^2\\ &\le -\lambda_{\min}(-Q)\|x(t)\|^2 + \|\alpha(t)\|^2 + \|\beta(t)\|^2.\end{aligned} \tag{25}$$

Notice the sampling instants defined in (20). We can know that as long as $t \in [t_k, t_{k+1}]$, $e(t) \le \gamma(t)$ holds. Hence, for $\forall t \in [t_k, t_{k+1}]$, we have

$$\begin{aligned}\dot{v}(t) &\le -\lambda_{\min}(-Q)x(t)^2 + \gamma(t)\\ &\le -\frac{\lambda_{\min}(-Q)}{\lambda_{\max}(P)}x^T(t)Px(t)\\ &= -\delta v(t) + \gamma(t).\end{aligned} \tag{26}$$

Notice that $\gamma(t) = \varepsilon^{-\alpha t} + \varepsilon_0 = e^{-(\alpha \ln \varepsilon)t} + \varepsilon_0$ and both $v(t)$ and $\gamma(t)$ are continuous for all $t > 0$. Then, $v(t) \le e^{-\delta t}v(0) + \int_0^t e^{-\delta(t-s)}\gamma(s)ds$ always holds for all $t > 0$.

From the above discussion, we can obtain

$$\begin{aligned}v(t) &\le e^{-\delta t}v(0) + e^{-\delta t}\int_0^t e^{(-\delta - \alpha \ln \varepsilon)s}ds\\ &\quad + \int_0^t e^{-\delta(t-s)}\varepsilon_0 ds\\ &= e^{-\delta t}\left(v(0) - \frac{\varepsilon_0}{\delta}\right) + \frac{\varepsilon_0}{\delta} + e^{-\delta t}\int_0^t e^{(\delta - \alpha \ln \varepsilon)s}ds.\end{aligned} \tag{27}$$

There are three situations to discuss below. If $\delta - \alpha \ln \varepsilon = 0$, we obtain

$$v(t) \le e^{-\delta t}\left(v(0) - \frac{\varepsilon_0}{\delta} + t\right) + \frac{\varepsilon_0}{\delta}. \tag{28}$$

If $\delta - \alpha \ln \varepsilon > 0$, we obtain

$$\begin{aligned}v(t) &\le e^{-\delta t}\left(v(0) - \frac{\varepsilon_0}{\delta}\right) + \frac{\varepsilon_0}{\delta} + \frac{e^{-\delta t}}{\delta - \alpha \ln \varepsilon}\left(e^{(\delta - \alpha \ln \varepsilon)t} - 1\right)\\ &= e^{-\delta t}\left(v(0) - \frac{\varepsilon_0}{\delta} - \frac{1}{\delta - \alpha \ln \varepsilon}\right) + \frac{\varepsilon_0}{\delta} + \frac{e^{-\delta t}}{\delta - \alpha \ln \varepsilon}.\end{aligned} \tag{29}$$

If $\delta - \alpha \ln \varepsilon < 0$, we have

$$v(t) \le e^{-\delta t}\left(v(0) - \frac{\varepsilon_0}{\delta} - \frac{1}{\delta - \alpha \ln \varepsilon}\right) + \frac{\varepsilon_0}{\delta} + \frac{\varepsilon^{-\delta t}}{\delta - \alpha \ln \varepsilon}. \tag{30}$$

Similar to the discussion of Theorem 2 in [28], we can conclude that, no matter what the value of $\delta - \alpha \ln \varepsilon$ is, the global uniform limit of system (19) can be guaranteed. The proof is completed.

Remark 3. In Theorem 2, under the event-driven condition (20), the exponentially decreasing event-driven condition is used to ensure the global uniform limit boundedness of the event-driven observer control system (19). Obviously, if we choose $\alpha = 0$, the event-driven condition (20) will be reduced to the constant event-driven condition considered in [28]. In addition, if we choose $\varepsilon_0 = 0$, we can also get global asymptotic stability.

Remark 4. The malicious attack in this paper is not a specific type of attack. Any type of attack that satisfies the system can be used. Dolk et al. [26] proposed a systematic design framework for output-based dynamic event-triggered control (ETC) systems under denial-of-service (DoS) attacks. Compared with the methods in [11, 26], the method in this paper is more conservative and general.

4.3. Minimum Interevent Interval. We now prove that there is a minimum time interval to exclude the Zeno behavior of the sampling.

Theorem 3. *With the sampling instants determined by using (20), the Zero behavior of the sampling does not exist.*

Proof. Let t_k be a sampling instant, and then in the time interval $[t_k, t_{k+1})$, $\dot{x}(t_k)$ is constant. For $t \in [t_k, t_{k+1})$, according to the definition of $e(t)$ in (20), we can obtain

$$\begin{aligned}\|\dot{\alpha}(t)\| &= \left\|(A+BK)x(t_k) + A\alpha(t) - BE\beta(t)\right\|,\\ \|\dot{\beta}(t)\| &= \|\dot{\eta}(t)\| = \left\|\beta(t) + \eta(t_k)\right\|,\end{aligned} \tag{31}$$

where

$$\begin{aligned}
\|\alpha(t)\| &= \left\|e^{A(t-t_k)}\alpha(t)\right\| \\
&\quad + \left\|\int_{t_k}^{t}\left[e^{A(t-s)}(A+BK)x(t_k) - BE\beta(t)\right]\mathrm{d}s\right\| \\
&= \left\|\int_{t_k}^{t}\left[e^{A(t-s)}(A+BK)x(t_k) - BE\beta(t)\right]\mathrm{d}s\right\| \\
&\le \left\|\int_{t_k}^{t} e^{\|A\|(t-s)}\left\|(A+BK)x(t_k) - BE\beta(t)\right\|\mathrm{d}s\right\| \\
&\le \left\|\int_{t_k}^{t} e^{\|A\|(t-s)}\left(\|(A+BK)\|\left\|x(t_k)\right\| - \|BE\|\|\beta(t)\|\right)\mathrm{d}s\right\| \\
&\le \left\|\int_{t_k}^{t} e^{\|A\|(t-s)}\|(A+BK)\|\left\|x(t_k)\right\|\mathrm{d}s\right\|, \\
\|\beta(t)\| &= \left\|e^{A(t-t_k)}\beta(t_k) + \int_{t_k}^{t} e^{(t-s)}\eta(t_k)\mathrm{d}s\right\| \\
&= \left\|\int_{t_k}^{t} e^{(t-s)}\eta(t_k)ds\right\| \le \left\|\int_{t_k}^{t} e^{(t-s)}\left\|\eta(t_k)\right\|\mathrm{d}s\right\|, \\
e(t) &\le \left\|\int_{t_k}^{t} e^{\|A\|(t-s)}\|(A+BK)\|\left\|x(t_k)\right\|\mathrm{d}s\right\|^2 \\
&\quad + \left\|\int_{t_k}^{t} e^{(t-s)}\left\|\eta(t_k)\right\|\right\|^2 \\
&\le \left(\phi(t_k)\int_{t_k}^{t} e^{\|A\|(t-s)}\mathrm{d}s\right)^2 + \left(\left\|\eta(t_k)\right\|\int_{t_k}^{t} e^{(t-s)}\mathrm{d}s\right)^2,
\end{aligned} \tag{32}$$

where

$$\phi(t_k) = \|A+BK\|\left\|x(t_k)\right\|. \tag{33}$$

If $\|A\| \neq 0$, we have

$$e(t) \le \left(\frac{\phi(t_k)}{\|A\|}\left(e^{\|A\|(t-t_k)} - 1\right)\right)^2 + \left(\left\|\eta(t_k)\right\|\left(e^{(t-t_k)} - 1\right)\right)^2. \tag{34}$$

Let $\overline{T} = t - t_k$, according to the definition of sampling instants (20), and the next event will not be generated before $e(t) = \gamma(t)$; then, we have

$$e(t) \le \left(\frac{\phi(t_k)}{\|A\|}\left(e^{\|A\|(t-t_k)} - 1\right)\right)^2 + \left(\left\|\eta(t_k)\right\|\left(e^{(t-t_k)} - 1\right)\right)^2. \tag{35}$$

This shows that $\overline{T}$ cannot be zero, thus $\overline{T} > 0$.

Similarly, if $\|A\| = 0$, we have

$$e(t) \le (\phi(t_k)(t-t_k))^2 + \left(\left\|\eta(t_k)\right\|\left(e^{(t-t_k)} - 1\right)\right)^2, \tag{36}$$

and the lower bound $\overline{T}$ can be computed by

$$(\overline{T}\phi(t_k))^2 + \left(\left\|\eta(t_k)\right\|\left(e^{\overline{T}} - 1\right)\right)^2 = \varepsilon^{-\alpha(\overline{T}+t_k)} + \varepsilon_0, \tag{37}$$

which also guarantees that $\overline{T} > 0$.

With the above discussion, we can conclude that there exists a minimum interevent interval. This completes the proof.

As a summary, this section designs an event-triggered observer to solve the control of the CPS despite the actuator attacks. It proves that the system is ultimately bounded by the controller. And the Zeno behavior is effectively avoided. In the next section, the simulation will be presented. □

5. Simulation

Without loss of generality, first, we present the simulation of safety state estimate. In this part, the finite-time observer is applied to a DC motor with actuator attack. The linear model of the DC motor is

$$\begin{aligned}
\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix} &= \begin{bmatrix} -41 & 0 & 0 & 0\\ -2.7667 & -16.6667 & 2.7667 & 0\\ 5.5333 & 5.5333 & -0.0667 & 0\\ 0 & 0 & 1 & 0\end{bmatrix} \\
&\quad \times \begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix} + \begin{bmatrix}2 & 0\\ 0 & 333.3333\\ 0 & 0\\ 0 & 0\end{bmatrix} \times u(t) + \begin{bmatrix}2\\ 0\\ 0\\ 0\end{bmatrix}\eta(t), \\
y &= \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix} \times \begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix},
\end{aligned} \tag{38}$$

where x_1 represents the stator current, x_2 is the rotor current, x_3 is the angular velocity, and x_4 is the angular acceleration. We choose the convergent time τ, for example, as $\tau = 0.5$ s, and the parameter L is chosen such that the assumptions of Theorem 1 are fulfilled. The actuator attack $\eta(t)$ is chosen $\eta(t) = 50\sin(20\pi t)$. Figures 1 and 2 show the simulation results with an initial condition $x(0) = [\,20\ \ 5\ \ -10\ \ -5\,]^T$, and the finite-time observer (12) has a zero initial condition. Figure 1 shows the states of x_1 and x_4 and their estimates. Due to the limited space, only the states of x_1 and x_4 and their estimates are listed to verify the validity. Figure 2 shows the estimation errors. It can be seen that the finite-time observer converges in the predefined finite time $\tau = 0.5$, i.e., the estimation errors $e_i(t) = \hat{x}_i(t) - x_i(t)$; e_1, e_2, e_3, and e_4 are exactly equal to zero after the convergent time τ.

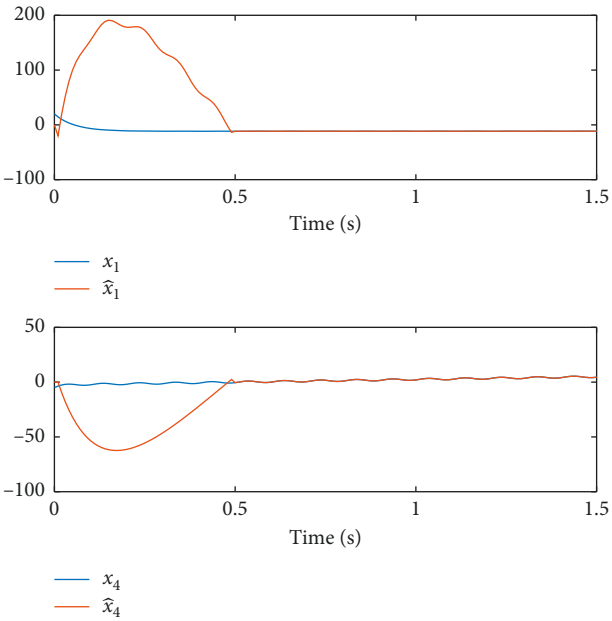


FIGURE 1: The states of x_1 and x_4 of the system under the actuator attack and their estimation $\hat{x}_1$ and $\hat{x}_4$.

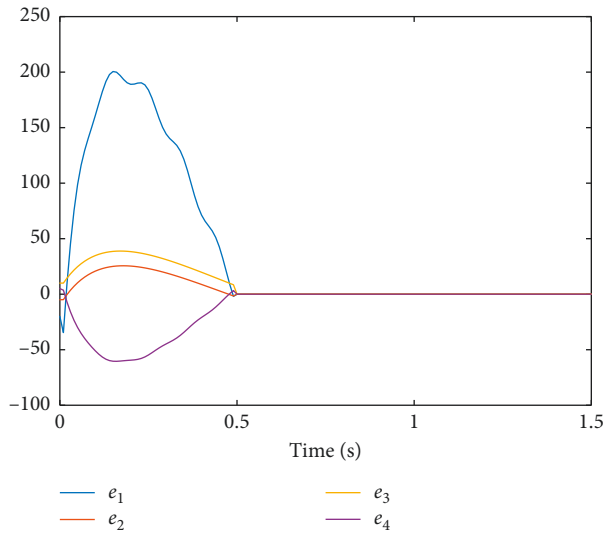


FIGURE 2: The estimation errors e_1, e_2, e_3, and e_4 for the finite-time observer (12).

Remark 5. Similar to reference [16], the states of x_1 and x_4 and their estimates are related to the initial state of the system and the initial state of the observer. Because the designed observer in this paper is finite time, the estimates are irregular before 0.5 s. In addition, the initial state of the system and the initial state of the observer have no effect on the final results, and we can change the initial state to adjust the estimates.

An example of the an inverted pendulum system with a car [28] to simulate the event-triggered control is presented. The linearized system model with actuator attack is given by

$$\begin{bmatrix} \dot{x} \\ \ddot{x} \\ \dot{\theta} \\ \ddot{\theta} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & \dfrac{-(I+ml^2)b}{I(M+m)+Mml^2} & \dfrac{m^2gl^2}{I(M+m)+Mml^2} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \dfrac{-mlb}{I(M+m)+Mml^2} & \dfrac{mgl(M+m)}{I(M+m)+Mml^2} & 0 \end{bmatrix} \times \begin{bmatrix} x \\ \dot{x} \\ \theta \\ \dot{\theta} \end{bmatrix} + \begin{bmatrix} 0 \\ \dfrac{I+ml^2}{I(M+m)+Mml^2} \\ 0 \\ \dfrac{ml}{I(M+m)+Mml^2} \end{bmatrix} \times (u+\eta),$$

$$y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} x \\ \dot{x} \\ \theta \\ \dot{\theta} \end{bmatrix}. \tag{39}$$

For this example, assuming that $M = 0.5$ kg, $m = 0.5$ kg, $b = 0.1$ N/m/s, $l = 0.3$ m, and $M = 0.006$ kg·m^2. We assume the system's initial condition is $[0.98 \;\; 0 \;\; 0.2 \;\; 0]^T$. By using pole assignment technique, one has the control gains as $K = [17.0368 \;\; 13.0877 \;\; -50.0520 \;\; -9.8150]$. It can be confirmed that the matrix inequality (22) is feasible for the positive definite matrix P.

Taking $\varepsilon = e, \alpha = 0.5, \varepsilon_0 = 0.2$, and the actuator attack $\eta(t)$ is chosen $\eta(t) = 0.2t$. Under the event-driven condition (20), the simulation results are shown in Figures 3–7. Figure 3 presents the state of the system with the actuator attack under the event-triggered controller (21) and the state of the system without the actuator attack under the event-triggered controller in [28], respectively. Figure 4 presents the state of the system with the actuator attack under the event-triggered controller (21) and continuous controller $u(t) = Kx(t)$, respectively. It can be seen that the state of the CPS system is globally uniformly ultimately bounded whether or not attacks exist, and the performance of CPS system with the event-triggered controller is almost the same as the continuous controller. The interevent intervals are given in Figures 5 and 6. Figure 7 shows the signal $e(t)$. Moreover, we also chose $\eta(t) = 3$ and $\eta(t) = \sin(t)$ to show different ways the system can be attacked. The results are shown in Figures 8 and 9. It can be seen that the system is ultimately bounded in these different cases.

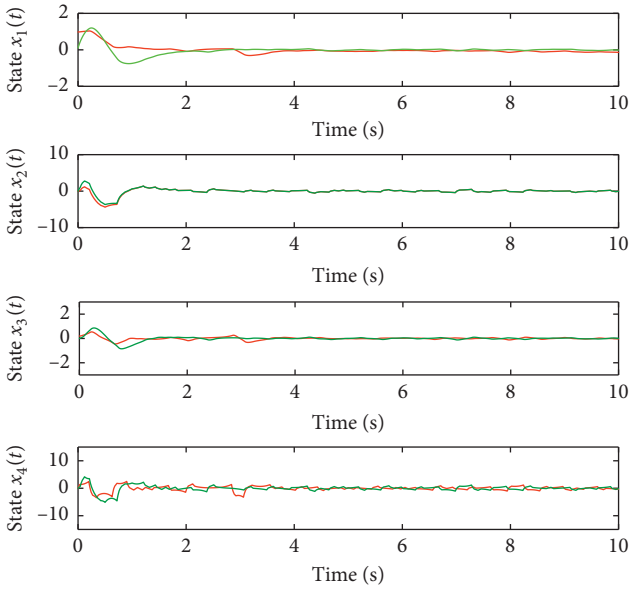


FIGURE 3: State responses with actuator attack (green line) and state responses without actuator attack (red line).

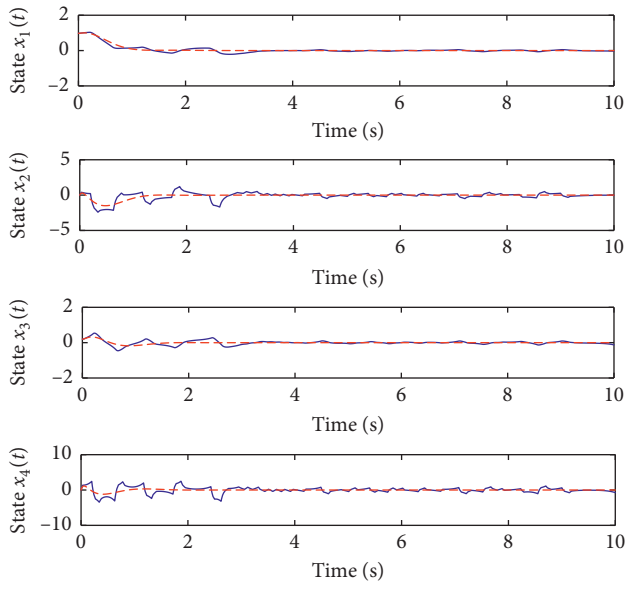


FIGURE 4: State responses with actuator attack: event-triggered controller (blue line) and continuous controller (red line).

Remark 6. The system model parameters A, B, and C are related to the state and control inputs of the system. Therefore, the specific computational complexity is also related to the system. However, based on this, the attack $\eta(t)$ added to the model in this manuscript and the complexity is not increased. So the system is more conservative than the system in references [16] and [28].

6. Conclusion

This paper is concerned with the secure state and event-triggered control problem for continuous-time cyber-

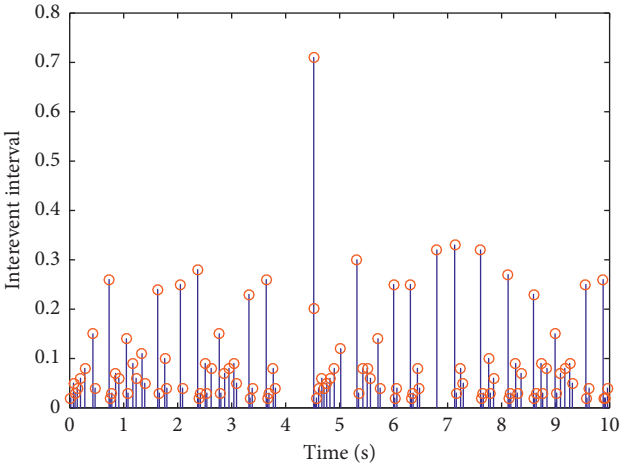


FIGURE 5: The release interval of control signal with actuator attack.

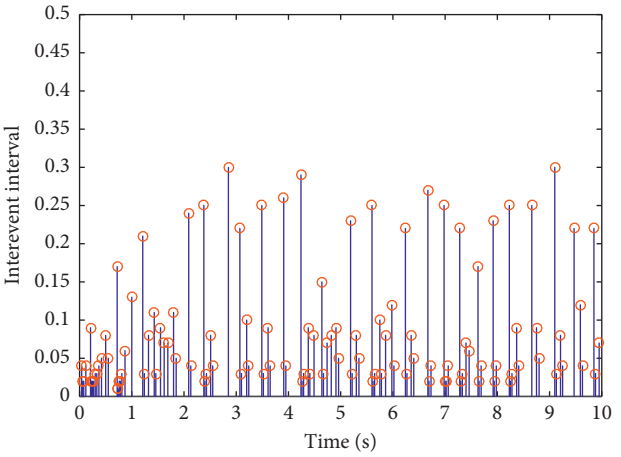


FIGURE 6: The release interval of control signal without actuator attack.

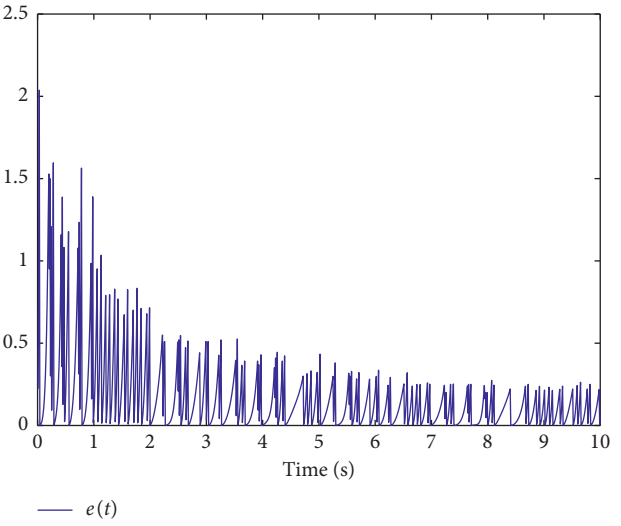


FIGURE 7: The measuring error signal $\|e(t)\|$.

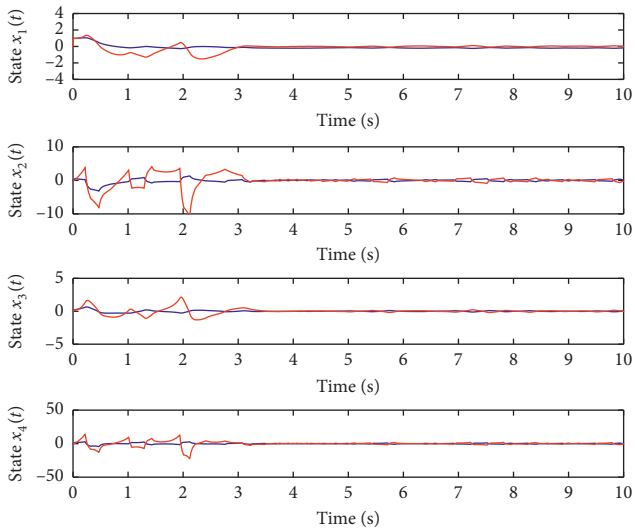


FIGURE 8: State responses with actuator attack $\eta(t) = 3$ (blue line) and state responses without actuator attack (red line).

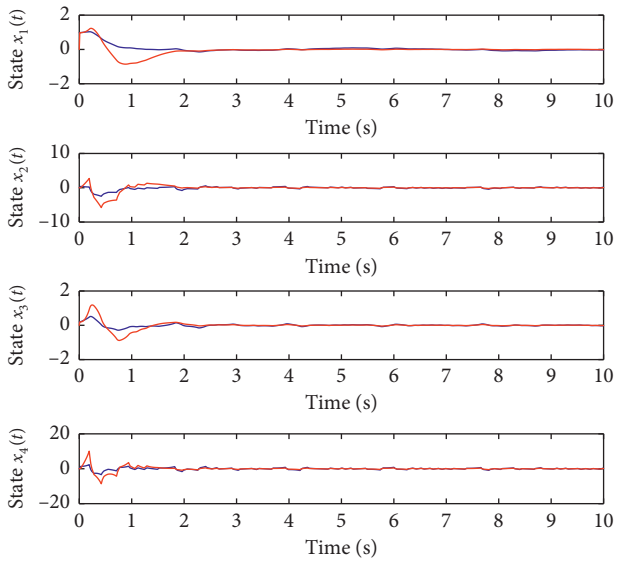


FIGURE 9: State responses with actuator attack $\eta(t) = \sin(t)$ (blue line) and state responses without actuator attack (red line).

physical systems under actuator attacks. First, a finite-time observer is constructed to estimate the state of the system. Then, a controller is designed based on the event-triggered communication. Unlike a sampled data control system, the controller is updated only when certain error signals exceed a given threshold. So it can reduce the loss of communication resources. In addition, the results show that the global uniform limit boundedness of CPS can be established. Simulation examples verify the effectiveness of the proposed method.

It should be pointed that, for simplicity, the disturbance and measurement noise are not considered in system (1). If those issues are considered, the event-triggered control problem becomes much more complicated. This is also the subject for our future research.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Plan under Grant no. 2016YFB0800902, the National Key Research and Development Program of China under Grant no. 2018YFB0803505, the University of Science and Technology Beijing under Grant no. FRF-BD-19-012A, the National Natural Science Foundation of China under Grant no. U1836106, and the Natural Science Foundation of Anhui Province under Grant no. 1708085QA16.

References

[1] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the HotSec*, San Jose, CA, USA, July 2008.

[2] J. Giraldo, D. Urbina, A. Cardenas et al., "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, p. 76, 2018.

[3] M. Lv, W. Yu, Y. Lv, J. Cao, and W. Huang, "An integral sliding mode observer for cps cyber security attack detection," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 4, Article ID 043120, 2019.

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[5] A. Chattopadhyay and U. Mitra, "Attack detection and secure estimation under false data injection attack in cyber-physical systems," in *Proceedings of the 2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, IEEE, Princeton, NJ, USA, March 2018.

[6] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2018.

[7] S. Mishra, N. Karamchandani, P. Tabuada, and S. Diggavi, "Secure state estimation and control using multiple (insecure) observers," in *Proceedings of the 53rd IEEE Conference on Decision and Control*, pp. 1620–1625, IEEE, Los Angeles, CA, USA, December 2014.

[8] J. Qiu, K. Sun, T. Wang, and H. Gao, "Observer-based fuzzy adaptive event-triggered control for pure-feedback nonlinear systems with prescribed performance," *IEEE Transactions on Fuzzy Systems*, vol. 27, 2019.

[9] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2016.

[10] A. Mitra and S. Sundaram, "Secure distributed state estimation of an LTI system over time-varying networks and analog erasure channels," in *Proceedings of the 2018 Annual American Control Conference (ACC)*, pp. 6578–6583, IEEE, Milwaukee, WI, USA, June 2018.

[11] M. Liao and A. Chakrabortty, "Optimization algorithms for catching data manipulators in power system estimation

loops," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 3, pp. 1203–1218, 2018.

[12] C.-H. Xie and G.-H. Yang, "Secure estimation for cyber-physical systems with adversarial attacks and unknown inputs: AnL2-gain method," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 6, pp. 2131–2143, 2018.

[13] Y. Li, L. Shi, and T. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 846–856, 2018.

[14] A.-Y. Lu and G.-H. Yang, "Secure Luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks," *Automatica*, vol. 98, pp. 124–129, 2018.

[15] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2017.

[16] W. Ao, Y. Song, C. Wen, and J. Lai, "Finite time attack detection and supervised secure state estimation for cpss with malicious adversaries," *Information Sciences*, vol. 451-452, pp. 67–82, 2018.

[17] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Information Sciences*, vol. 459, pp. 354–368, 2018.

[18] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 8, pp. 1049–1053, 2017.

[19] J. Liu, E. Tian, X. Xie, and H. Lin, "Distributed event-triggered control for networked control systems with stochastic cyber-attacks," *Journal of the Franklin Institute*, 2018.

[20] P. Frasca, S. Tarbouriech, and L. Zaccarian, "Hybrid models of opinion dynamics with opinion-dependent connectivity," *Automatica*, vol. 100, pp. 153–161, 2019.

[21] J. Liu, Y. Gu, X. Xie, Y. Dong, and J. H. Park, "Hybrid-driven-based H∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018.

[22] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3432–3439, 2018.

[23] G. Wang, G. B. Giannakis, and J. Chen, "Robust and scalable power system state estimation via composite optimization," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6137–6147, 2019.

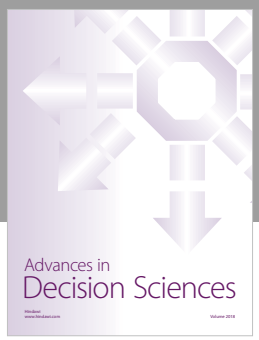
[24] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–10, 2018.

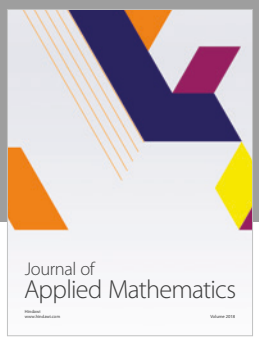
[25] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2018.

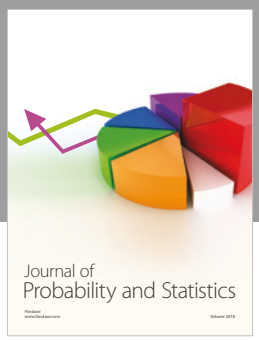
[26] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2016.

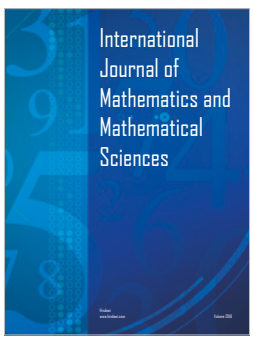
[27] C. Nowzari, E. Garcia, and J. Cortés, "Event-triggered communication and control of networked systems for multi-agent consensus," *Automatica*, vol. 105, pp. 1–27, 2019.

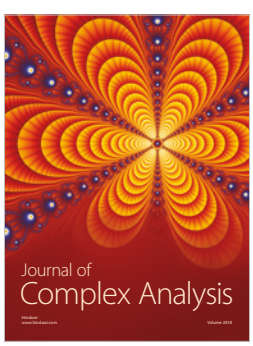
[28] J. Zhang and G. Feng, "Event-driven observer-based output feedback control for linear systems," *Automatica*, vol. 50, no. 7, pp. 1852–1859, 2014.

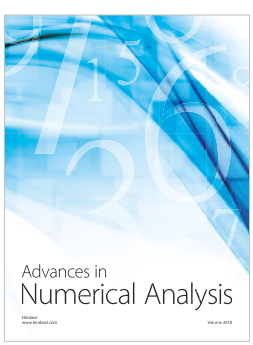


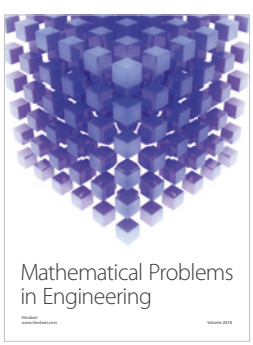


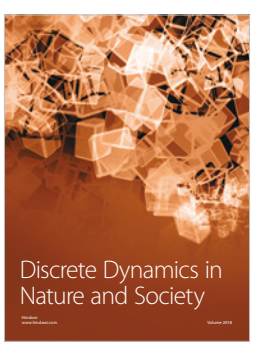


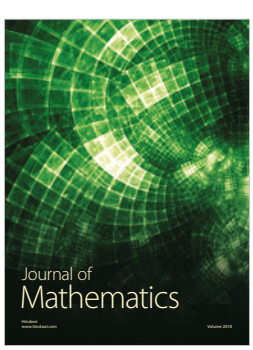


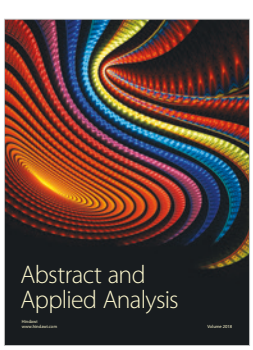


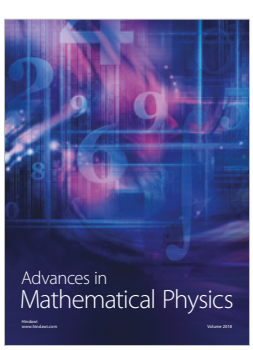












Hindawi

Submit your manuscripts at
www.hindawi.com