Information Sciences 423 (2018) 145–156

Contents lists available at ScienceDirect

Information Sciences

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

Improved adaptive resilient control against sensor and actuator attacks

Liwei An[a], Guang-Hong Yang[b,a,*]

[a] College of Information Science and Engineering, Northeastern University, Shenyang, 110819, China
[b] State Key Laboratory of Synthetical Automation of Process Industries, Northeastern University, Liaoning, Shenyang, 110819, China

ARTICLE INFO

Article history:
Received 13 July 2017
Revised 11 September 2017
Accepted 15 September 2017
Available online 19 September 2017

Keywords:
Sensor attacks
Actuator attacks
Adaptive control
Resilient control
Asymptotic stability
State constraints

ABSTRACT

In this paper, an improved adaptive resilient control scheme is proposed for mitigating adversarial attacks in cyber-physical systems (CPSs). By introducing a two-step backstepping approach, an adaptive bound estimation mechanism and a Nussbam function with faster growth rate, the effects of unknown sensor and actuator attacks are successfully mitigated. An exponentially-decaying barrier Lypunov function is used to constrain state variables. Compared with the existing results where only uniform ultimate boundedness is achieved, the developed controller guarantees that the closed-loop system is asymptotically stable and simultaneously the state constraints are not violated even in the presence of the time-varying sensor and actuator attacks. Simulation results are presented to verify the efficacy of the proposed scheme.

1. Introduction

Recently the security of cyber-physical systems (CPSs) has become a topic of scientific inquiry and received wide attention from many researchers.Since computational processes/softwares are integrated into networks with data processing/accessing facilities over the Internet [6], CPSs become vulnerable to adversarial attacks and threats. Despite advances in IT security encryption techniques in information systems, these methods alone are not sufficient for guaranteeing the security of CPSs against the attacks from physical devices or interactions between physical and cyber layers [8]. To complement the existing computer security architecture, it is necessary to study the CPS security from the system's perspective.

Cyber attacks have become one of the major threats to CPSs. Attack-resilient control guarantees the controlled system to restore the nominal operation in the shortest time after it suffers cyber attacks, and simultaneously relieves the performance degradation as much as possibly [25,33]. Recently, some resilient control strategies have been proposed for various types of attacks, for example, denial-of-service (DoS) attacks [1,3,4], false data injection attacks [8,26,28] and replay attacks [19,32]. In particular, attackers can often gain access to a set of sensing and actuation computing platforms and modify their software or environment to launch a coordinated attack against the system architecture [20]. Hence, developing new control algorithms against sensor and actuator coordinated attacks is of significant importance in both theory and practice.

On the other hand, adaptive control relies on the potential of the parameter adjustments to assure security and reliability of closed-loop systems in the presence of various unknown faults and attacks. Hence, the resultant solvable conditions can be more relaxed and the better control performance can also be achieved. The problem of resilient control against

[*] Corresponding author.
E-mail addresses: 1610312@stu.neu.edu.cn (L. An), yangguanghong@ise.neu.edu.cn, yangguanghong@mail.neu.edu.cn (G.-H. Yang).

https://doi.org/10.1016/j.ins.2017.09.042
0020-0255/© 2017 Elsevier Inc. All rights reserved.

adversarial attacks is closely related to fault-tolerant control. Recently, the problem of adaptive fault-tolerant control has been extensively studied [13,14,22,23,29]. From a system theoretical point of view, faults and attacks are fundamentally same. However, the attacks may be undetectable because they are strategically optimized in a coordinated way by malicious adversaries while the faults cannot collude with each other. Therefore, the attacks are usually with some system information such that the traditional adaptive fault-tolerant control schemes cannot be directly applied. At the performance level, the attack-resilient control expects the controlled system to restore the nominal operation with simultaneously minimizing the performance loss. Recently, some results on adaptive control with guaranteed performance have been developed [17,18]. Unfortunately, these methods are mostly implemented for SISO strict-feedback systems, whereas CPSs are typically MIMO systems with general structure. In [30], a class of systematic adaptive control architectures are proposed for linear dynamical systems subject to sensor uncertainties and attacks. In [7], an adaptive control strategy against sensor and actuator attacks is presented, which guarantees ultimate boundedness of the dynamical systems in the face of time-varying state-dependent sensor and actuator attacks.

In this paper, the problem of adaptive control architecture will be further investigated for addressing the security of CPSs. To mitigate the effects due to time-varying, state-dependent sensor and actuator attacks, a new adaptive backstepping control scheme is proposed for continuous-time linear systems. Technically, we summarize the contributions of this paper on the basis of the reference [7] as following.

(1) More drastic sensor attacks which make the sign of state feedback gain become unknown can be tolerated by introducing a Nussbam function.
(2) By directly estimating the bounds of unknown attack uncertainties instead of themselves, the proposed scheme can ensure the asymptotic stability of the closed-loop system even in the presence of time-varying sensor and actuator attacks.
(3) An exponentially-decaying barrier Lyaounov function related to multiple variables is proposed to constrain system states. By varying certain design parameters, the transient performance in terms of convergence rate and maximum overshoot can also be improved especially when the attacks occur.

The paper is organized as follows. In Section 2 we describe the system and attack models. The backstepping-based adaptive stabilizing controller is constructed in Section 3. In Section 4, the simulation example on an aircraft system is provided, and finally we conclude the work of this paper in Section 5.

2. Preliminaries and problem formulation

2.1. System descriptions and assumptions

Consider a class of linear CPSs under attacks in the same form as [7], described by

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B[u(t) + \delta_a(t, x(t))] \\ \tilde{x}(t) &= x(t) + \delta_s(t, x(t)) \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the system state, $u(t) \in \mathbb{R}^m$ is the control input and $\tilde{x}(t)$ is the compromised system state which is available for feedback. $\delta_a(t, x(t)) \in \mathbb{R}^m$ and $\delta_s(t, x(t)) \in \mathbb{R}^n$ capture actuator and sensor attacks, respectively. Similar to [7], the actuator and sensor attacks are considered to be state dependent, and $\delta_a(t, x(t))$ can be parameterized as $\delta_a(t, x(t)) = W^T(t)\varphi(x(t))$, and $\delta_s(t, x(t))$ can also be parameterized as $\delta_s(t, x(t)) = w(t)x(t)$.

Assumption 1. The weighting parameter $w(t)$ satisfies $1 + w(t) \neq 0$ and the sign of $(1 + w(t))$ is unknown, and there exist two unknown positive constants $\bar{w}$ and $\bar{\dot{w}}$ such that $\|w(t)\| \leq \bar{w}$ and $\|\dot{w}(t)\| \leq \bar{\dot{w}}$.

Assumption 2. There exists an unknown positive constant $\bar{W}$ such that $\|W(t)\| \leq \bar{W}$.

Remark 1. The considered attack model in system (1) has been investigated in [7], where the adaptive control architecture has been established. The stability analysis and controller design are considered for the CPSs with single-packet transmissions, which means that data is lumped together into one network packet and transmitted at the same time [27]. Thus, all state variables share the same time-varying weight $\omega(t)$. Such a sensor attack model can represent some attack types such as linear deception attacks [5,15]. In this paper, we will further develop an improved adaptive resilient control for achieving better control performance.

Remark 2. As Ao et al. [2] reported, a cyber attacker may corrupt the sensor's output or the designed input to cheat existing monitoring systems. It means when an attacker generates the attack signals, the system information may be involved. Hence, we assume the adversary has all measurement outputs (i.e., full state information in system (1)) available. Further, in the case where the parametrization does not hold for the attacks, one can consider a neural network universal function approximator to parameterize $\delta_a(t, x(t))$ on a compact subset of $\mathbb{R}^p$ [30].

Remark 3. In [12], a robust adaptive fault-tolerant control scheme is proposed for addressing actuator failures. However, the proposed scheme is on longer effective for system (1) since the perfect measurement become unavailable due to the effect of the sensor attack. It is highly desirable to develop a new adaptive resilent control to mitigate the attack's impact.