Resilient Observer-based Security Control for Cyber-Physical Systems against Actuator Fault and Denial of Service Attack

Ximing Yang
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
yxm961115123@163.com

Tieshan Li
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
tieshanli@126.com

Yue Long
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
longyue@uestc.edu.cn

Hanqing Yang
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
hqyang5517@uestc.edu.cn

***Abstract*—Cyber-physical systems (CPSs), widely regarded as the core of modern industrial technological advancements due to their tightly integrated architecture that blends communication, computation, and physical components, have garnered significant attention over the past decade. Due to their structural uniqueness, CPSs exhibit unparalleled flexibility and efficiency and have been deeply researched and applied in various advanced fields such as intelligent transportation and smart manufacturing with the continuous advancement of communication and control technologies. Nevertheless, we cannot overlook the accompanying issues, particularly the security challenges posed by open communication networks and the inherent limitations of physical components. Therefore, ensuring the security and reliability of CPSs is of paramount importance. In this work, considering the physical limitations and information security challenges that CPSs may encounter, such as actuator faults and denial-of-service (DoS) attacks, we first address the issue of actuator faults present in the system without considering DoS attacks. Based on a state observer, we reconstruct the partially unmeasurable states. Then, utilizing the error between the measurable system output and the reconstructed system output, we design a mechanism for fault detection and reconstruction. This approach ensures that the observer is pre-designed to obtain real-time fault information. Subsequently, to guarantee the performance of state and fault estimation under the influence of DoS attacks, we designed a resilient mechanism based on sampling strategies. Through this mechanism, the pre-designed observer is transformed into a novel resilient observer that can determine whether sampled information is trustworthy by detecting deviations between the sampling time and the current time. In this way, the impact of attacked information on estimation effectiveness is reduced. Subsequently, utilizing the state and fault information obtained from the resilient observer, and combined with a compensation mechanism, we construct a fault-tolerant controller to mitigate actuator faults, thereby minimizing their influence. By analyzing the stability of the error system and the closed-loop system, we ensure that all signals within both systems are bounded. Finally, an experiment based on an unmanned ground vehicle system is conducted to verify the effectiveness of the proposed method. In our future work, we will continue our research on reducing the consumption of network transmission resources and addressing control problems in complex nonlinear CPSs.**

***Index Terms*—Cyber-physical systems, security, actuator fault, denial-of-service attack.**

This work was supported in part by the National Natural Science Foundation of China under Grant 51939001, Grant 62273072, and Grant 62203088, in part by the Natural Science Foundation of Sichuan Province under Grant 2022NSFSC0903. (Corresponding author: Tieshan Li.)