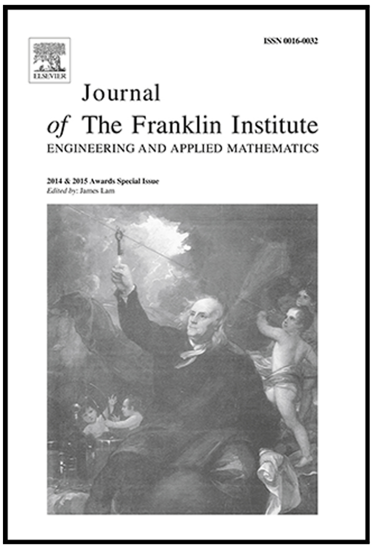

Periodic Event-Triggered Resilient Control for Cyber-Physical Systems Under Denial-of-Service Attacks

Yuan-Cheng Sun, Guang-Hong Yang

PII: S0016-0032(18)30412-5
DOI: 10.1016/j.jfranklin.2018.06.009
Reference: FI 3504

To appear in: *Journal of the Franklin Institute*

Received date: 20 January 2018
Revised date: 21 May 2018
Accepted date: 6 June 2018

Please cite this article as: Yuan-Cheng Sun, Guang-Hong Yang, Periodic Event-Triggered Resilient Control for Cyber-Physical Systems Under Denial-of-Service Attacks, *Journal of the Franklin Institute* (2018), doi: 10.1016/j.jfranklin.2018.06.009

Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 00 (2018) 1–17

Journal
of The
Franklin Institute

Periodic Event-Triggered Resilient Control for Cyber-Physical Systems Under Denial-of-Service Attacks

Yuan-Cheng Sun[a], Guang-Hong Yang[a,b,*]

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

Abstract

This paper studies the problem of designing a resilient control strategy for cyber-physical systems (CPSs) under denial-of-service (DoS) attacks. By constructing an H_∞ observer-based periodic event-triggered control (PETC) framework, the relationship between the event-triggering mechanism and the prediction error is obtained. Then, inspired by the maximum transmission interval, the input-to-state stability of the closed-loop system is proved. Compared with the existing methods, a Zeno-free periodic PETC scheme is designed for a continuous-time CPS with the external disturbance and measurement noise. In particular, the objective of maximizing the frequency and duration of the DoS attacks is achieved without losing robustness. Finally, two examples are given to verify the effectiveness of the proposed approach.

Keywords: Cyber-physical systems; periodic event-triggered control; denial-of-service attack; input-to-state stability

1. Introduction

In recent years, cyber-physical systems (CPSs) have been widely used in various engineering fields owing to advances in computing and communication technologies. However, the use of networks and heterogeneous digital elements has made these CPSs vulnerable to various cyber attacks, such as deception attacks, replay attacks, bias injection attacks, zero-dynamics attacks, denial-of-service (DoS) attacks and so on. Unlike traditional systems where attacks limit their impact to the cyber level, malicious attacks to CPSs can impact the physical world [1].Thus these is a strong demand for analysis, synthesis and design methods to guarantee the security and reliability of CPSs despite the presence of malicious attacks[2, 3].

Among the various malicious attacks, DoS attacks make the actuator and sensor data to be blocked rather than reach their respective destinations and lead to the absence of data for the related components. Such kind of attack is very common in network communications, and a lot of works have been made for the CPSs under DoS attacks [4–8]. A basic research field on security problem of CPSs is the stability analysis under DoS attacks. In [9], the authors characterize frequency and duration of the DoS attacks under which input-to-state stability of the closed-loop system can be presented, and the transmission times is scheduled. A resilient control method is presented in [10] to maximize frequency and duration of the DoS attacks under which closed-loop stability is not destroyed. In [11], based on the studies on [10], a control architecture that approximate co-location while enable remote implementation is designed.

[*] Corresponding author.
Email addresses: dksyc294@126.com (Yuan-Cheng Sun), yangguanghong@ise.neu.edu.cn (Guang-Hong Yang)