Call For Papers

Special Session: Security control and state estimation for cyber-physical systems
Conference: The 2022 International Conference on Cyber-physical Social Intelligence (ICCSI)

Date: October 21-24, 2022
Location: Nanjing, China
Meeting mode: Hybrid
Web site: https://iccsi2022.agist.org

Along with the pervasive utilization of open yet unprotected communication networks, the Cyber-Physical Systems (CPSs) are vulnerable to cyber threats. As a result, the security of communication network, which is of utmost importance in the networked-related systems, has provoked an increasing research interest and a multitude of results have been reported in the literature. This special issue provides an introduction to a variety of cyber threats/attacks and summarizes recent progress in applying fundamentals of systems theory and decision sciences to this new and increasingly promising area with focus on the modeling, control and state estimation. So far, there are mainly two types of cyber attacks which can affect the systems behavior directly or through feedback, namely, the denial-of-Service (DoS) attacks and the deception attacks . The DoS attack deteriorates the system performance by preventing the information from reaching the destination, while the deception attack aims at manipulating the system toward the adversaries' desired behaviors by tampering with the control actions or system measurements. However, with the purpose of degrading system performance as severely as possible, the adversaries usually prefer to performing the so-called mixed attacks that are integrating different sorts of attacks forms. Such mixed attacks impose extreme difficulties on the analysis, control and state estimation of the targeted systems, which remains open and challenging. We encourage prospective authors to submit related distinguished research papers on the subject of both: theoretical approaches and practical case reviews.

Interested topics include (but not limited to):

- Modeling of cyber-attacks
- Security control of CPS subject to cyber-attacks
- Security state estimation of CPS subject to cyber-attacks
- Detection of cyber-attacks against CPS
- Distributed control/filtering over sensor networks with malicious attacks
- Networked control systems subject to cyber-attacks

Important Dates:

May 15, 2022,	Full paper submission
July 1, 2022,	Acceptance/Rejection notification
August 31, 2022,	Final camera-ready papers due

Special Session Co-chairs:

Professor. Lifeng Ma (Nanjing University of Science and Technology, China), email malifeng@njust.edu.cn
Associate Professor. Lidong He (Nanjing University of Science and Technology, China), email lidonghe@njust.edu.cn

All inquiries about the session, including the letter of intent, should be sent to any of the co-chairs above