Call For Paper

Special Session on LSMS2017&ICSEE2017

Secure Control for Networked Control Systems

Networked control systems are the industrial control systems combining modern communication and networking techniques, and now have a wide set of real-world applications such as Internet of powers, smart grids, Internet of medical devices, Internet of traffic managements and many other industrial Internet of things and cyber-physical systems etc. Such systems can benefit for the control performance and efficiency by the advantages of components inter-networking, but in turn expose the control kernel and components to cyber-attacks (e.g., DoS attacks, false data injection attacks and replay attacks etc.) as a challenging security issue. The state-of-the-art research lacks sufficient works that can tackle this challenge well. On the one hand, off-the-shelf network security solutions (e.g., network firewall, intrusion detection systems and anti-virus software) cannot address the control security issues due to the absence of knowledge on control internals, and also cannot adapt well to the control requirements.

On the other hand, existing safe control methods (e.g., fault diagnosis and fault tolerant control) can neither apply to solve the control security problems directly. These methods are usually designed to address the natural and inherent system faults, which are completely different from the security issues induced by cyber-attacks. In fact, the faults are usually follow some rules and statistical patterns, hence being able to avoid by some a priori knowledge and assumptions. While the attacks are more unpredictable, and even worse the attacking strategies may be purposely adjusted to hide known patterns.

This special session seeks new theoretical and practical research works beyond network security and safe control, and targeting secure control as a central topic.

Authors are invited to submit original papers that describe the latest results and advances in novel theories and their new application within the secure control contexts. Specifically, submitted articles MUST NOT substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conferences that have proceedings or journals.

The papers will be peer reviewed and selected on the basis of their quality and relevance to the topic of this special session.

TOPICS OF INTEREST

Topics include (but are not limited to):

- Secure control for networked control systems
- Secure control for industrial Internet-of-Things
- Secure control for smart grids
- Secure control for power systems
- Secure control for cyber-physical systems
- Secure control for complex networks
- Secure control for medical devices
- Secure control for micro/nano systems
- New network attacking and intrusion methods for control systems
- Threat modelling for networked control systems
- Intrusion detection for networked control systems
- Secure control against Denial-of-service (DoS) attacks
- Secure control against false data injection attacks
- Secure control against replay attacks

SUBMISSION GUIDELINES

Prospective authors are invited to submit full-length papers before the submission deadline through https://easychair.org/conferences/?conf=lsmsicsee2017, and should write [SC] at the end of the title in the submitted papers to indicate this submission is for the secure control special session in the conference.

Accepted papers will be published in the Springer Communications in Computer and Information Science (CCIS) proceedings (EI Compendex), which is under review. Some high-quality papers will be recommended for possible publication in SCI indexed international journals after expansion and further review, such as Neurocomputing, Transactions of the Institute of Measurement and Control, Cognitive Computation, etc.

SESSION CHAIR

Prof Fei, Minrui (Shanghai University, China)

IMPORTANT DATES

- Submission deadline: April 1, 2017
- Accept/reject notification: June 1, 2017
- Submission of camera-ready papers for final review: June 15, 2017

Email: mailto:secretary@lsms-icsee.org
Website: http://www.lsms-icsee.org
Submit your paper at: https://easychair.org/conferences/?conf=lsmsicsee2017