Security and Communication Networks

Special Issue on

Cyber-Physical Security for Critical Infrastructures: Smart Grids and Transportation Networks

CALL FOR PAPERS

Critical infrastructures, such as the smart grids, transportation networks, food chain, and healthcare delivery systems, are crucially supporting the nation's security, public health and safety, and economic vitality. The "next-generation" critical infrastructures are envisioned to be cyber-physical systems that integrate the advanced communications, networking, sensing, and computing technologies with the traditional physical systems to provide more efficient and reliable operation and facilitate new consumer-centric applications through greater situational awareness. Such integration no doubt provides unprecedented opportunities for enabling more efficient, consumer-centric, and resilient modern critical infrastructures, but it also creates a host of unfamiliar vulnerabilities stemming from cyber intrusion and corruption potentially leading to devastating physical effects. The security of a system is as strong as its weakest link. Thus, the scale and complexity of the "next-generation" critical infrastructures along with its increased connectivity and cyber-physical coupling make the task of the protection particularly challenging.

The goal of this special issue is to foster transformative and multidisciplinary solutions that effectively address the challenges in securing the next-generation critical infrastructures. We invite the submissions from academia, government, and industry presenting novel research results in both practical and theoretical aspects of cyber-physical security for the smart grids and transportation networks.

Potential topics include but are not limited to the following:

- Cyber-physical vulnerability assessment for the smart grids and transportation networks
- Emerging and future threats, identification, and management for the smart grids and transportation networks
- Industrial control systems/SCADA security for the smart grids and transportation networks
- Edge and cloud computing for the smart grids and transportation networks
- Communications and networking technologies for securing the smart grids and transportation networks
- Data-driven cyber-physical detection and defense strategy for protecting the smart grids and transportation networks
- Disaster-resilient controls and operations management for the smart grids and transportation networks
- Situational awareness and visualization for the smart grids and transportation networks
- Game-theoretic technologies for securing for the smart grids and transportation networks
- Physical-layer and cross-layer security technologies for the smart grids and transportation networks

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/secrin/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Jin Wei, The University of Akron, Akron, USA
jwei1@uakron.edu

Guest Editors
Deepa Kundur, University of Toronto, Toronto, Canada
dkundur@ece.utoronto.ca

Bri-Mathias Hodge, National Renewable Energy Laboratory, Golden, USA
bri-mathias.hodge@nrel.gov

Submission Deadline
Friday, 5 October 2018

Publication Date
February 2019