

Special Issue on "Cyber, Physical and System Security for Smart Grid"

Smart Grid technology aims at facilitating the reliable and efficient delivery of electricity to consumers using two-way digital technology, which allows utility providers and consumers to constantly monitor and adjust electricity use for the purpose of energy saving, cost reduction, and reliability enhancement. The development and deployment of Smart Grid technology has become an urgent global priority as its envisioned economic, environmental, and social benefits will be enjoyed not only now but also by generations to come. Numerous worldwide science foundations and governments are currently supporting the development and deployment of Smart Grid technology.

The vision of Smart Grid relies heavily on the information and communications technologies as they will empower today's power grid with the unprecedented capability of supporting two-way energy and information flow, isolating and restoring power outages more quickly, facilitating the integration of renewable energy sources into the grid, and empowering the consumer with tools for optimized energy consumption. One critical aspect of the Smart Grid related information and communications technologies is the cyber, physical and system security. Cyber, physical and system security includes the protection of networks and servers from unauthorized accesses and malicious attacks. Cyber, physical and system security also covers the protection of compromised control and measurement units from doing harm to the system, physical security, secure state estimation, intrusion detection, etc. Although critical, cyber and system security of Smart Grid are still largely remaining unaddressed, and many important questions need to be answered and critical problems need to be solved.

This special issue is intended to bring together the most recent advances in the field of cyber, physical and system security of Smart Grid from industry, government, and academia. This special issue covers all aspects of cyber, physical and system security of Smart Grid that are involved in providing a reliable and robust security environment for the operation of Smart Grid to realize its envisioned economic, environmental, and social benefits.

Topics of Interest include but not limited to:

- Communication security in Smart Grid
- Attacks and defenses mechanisms in Smart Grid
- Intrusion detection in Smart Grid
- Physical and Infrastructure Security in Smart Grid
- Secure key management and access control in Smart Grid
- Consumer privacy protection in Smart Grid
- System security architecture for Smart Grid
- Wireless security in Smart Grid
- Software security relevant to Smart Grid
- Security standard for Smart Grid
- Authentication and authorization in Smart Grid
- Vulnerability analysis in Smart Grid
- Security of Supervisory Control and Data Acquisition (SCADA) system
- Security of electric grid state estimation

SUBMISSION GUIDELINES

This special issue solicits original work that must not be under consideration for publication in other venues. Two-page extended abstracts are solicited for the first round of review. Authors of selected abstracts will be invited to submit the full papers in the second round. Authors should refer to the IEEE Transactions on Smart Grid author guidelines at <http://www.ieee-pes.org/publications/information-for-authors> for information about content and formatting of submissions.

Please submit a PDF version of the abstracts including a cover letter with author contact information via e-mail to kuiren@gmail.com before the deadlines.

IMPORTANT DATES

Jun 15th, 2010: Deadline for extended abstract submission
Jul 15th, 2010: Completion for first-round of reviews
Oct 1st, 2010: Deadline for full paper submission

Jan 1st, 2011: Final decision notification
Mar 15th, 2011: Publication materials due

GUEST EDITORS

Kui Ren, Department of ECE, Illinois Institute of Technology
Email: kui.ren@iit.edu

Zuyi Li, Department of ECE, Illinois Institute of Technology
Email: zuyi.li@iit.edu