Guest Editorial Cyber, Physical, and System Security for Smart Grid

The vision of a 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.

In the past few years, smart grid security has attracted tremendous attention from industry, government, and academia, and significant research efforts have been pushed forward. This special issue brings together the most recent advances in this field, aiming at providing a reliable and robust security environment for the operation of smart grid to realize its envisioned economic, environmental, and social benefits. Twenty-one papers have been accepted from open call, and their brief summaries are listed below.

1. "Malicious Data Attacks on the Smart Grid," by Oliver Kosut, Liyan Jia, Robert Thomas, and Lang Tong, studies malicious attacks against power systems by controlling meters and develops both adversarial and countermeasures for the control center.

2. "Integrity Data Attacks in Power Market Operations," by Le Xie, Yilin Mo, and Bruno Sinopoli, studies the economic impact of false data injection attack on electrical power market operations and shows their impact.

3. "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," by Amir-Hamed Mohsenian-Rad, and Alberto Leon-Garcia, investigates the impact of Internet-based load altering attacks and overviews different defense mechanisms.

4. "A Lightweight Message Authentication Scheme for Smart Grid Communications," by Mostafa Fouda, Zubair Fadlullah, Nei Kato, Rongxing Lu, and Xuemin Shen, proposes a secure and reliable framework for smart grid with the focus on developing a light-weight authentication scheme tailored for advanced metering infrastructure (AMI).

5. "Multicast Authentication in the Smart Grid With One-Time Signature," by Qinghua Li and Guohong Cao, identifies the requirements of multicast communication and multicast authentication in smart grid and develops a tailored multicast authentication scheme based on the security technique of one-time signature.

6. "P^2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid," by Zhenyu Yang, Shucheng Yu, Wenjing Lou, and Cong Liu, identifies the privacy preserving issues in Vehicle-to-Grid (V2G) networks and proposes a precise reward scheme for it.

7. "UBAPV2G: A Unique Batch Authentication Protocol for Vehicle-to-Grid Communications," by Huaqun Guo, Yongdong Wu, Feng Bao, Hongmei Chen, and Maode Ma, provides an efficient batch authentication protocol for security of vehicle-to-grid (V2G) power system that satisfies stringent real time requirement.

8. "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System," by Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu, and Lei Zhang, studies through experiments the energy consumption issues of different security algorithms on the platform of wireless sensor nodes.

9. "Cognitive Radio Network for the Smart Grid: Experimental System Architecture, Control Algorithms, Security, and Microgrid Testbed," by Robert C. Qiu, Zhen Hu, Zhe Chen, Nan Guo, Raghuram Ranganathan, Shujie Hou, and Gang Zheng, investigates the new idea of using cognitive radio network for smart grid with a microgrid testbed proposed.

10. "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," by Thomas Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford, investigates the use of Petri nets for modeling coordinated cyber-physical attacks on the smart grid, and the modeling approach is demonstrated for an example attack on smart meters.

11. "ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms," by Georgios Kalogridis, Rafael Cepeda, Stojan Denic, Tim Lewis, and Costas Efthymiou, studies how home energy management algorithms can help reduce the exposure of sensitive energy usage information and proposes privacy metrics.

12. "A Secure Framework for Protecting Customer Collaboration in Intelligent Power Grids," by Hyejin Son, Tae Yoon Kang, Hwangnam Kim, and Jae Hyung Roh, studies how customers can securely and trustfully collaborate with each other to enable power sharing and smart power planning.

13. "A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid," by Hairong Qi, Xiaorui Wang, Leon Tolbert, Fangxing Li, Fang Zheng Peng, Peng Ning, and Massoud Amin, presents a location-centric hybrid system architecture, as opposed to the existing centralized architecture, to

Digital Object Identifier 10.1109/TSG.2011.2175834

facilitate fault prevention, detection, and mitigation at various levels of the power system.

14. "Protecting Smart Grid Automation Systems Against Cyberattacks," by Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, and Kenneth Rohde, proposes a conceptual layered framework for protecting power grid automation systems against cyber attacks.

15. "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids," by Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert Green II, and Mansoor Alam, proposes a distributed intrusion detection system for smart grids by developing and deploying an intelligent module at the multiple layers of smart grids.

16. "Security Framework for Wireless Communications in Smart Distribution Grid," by Xudong Wang and Ping Yi, proposes a wireless mesh network based communication architecture for smart grid and a security framework therein.

17. "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks," by Biplab Sikdar and Joe Chow, presents a set of strategies to protect the anonymity of synchrophasor data against a type of cyber attacks called passive traffic analysis attacks.

18. "An Early Warning System Based on Reputation for Energy Control Systems," by Cristina Alcaraz, Carmen Fernandez-Gago, and Javier Lopez, proposes an early warning system for energy control systems based on reputation and on wireless sensor networks using the ISA 100.11a standard for alarm management.

19. "Cyber Attack Exposure Evaluation Framework for the Smart Grid," by Adam Hahn and Manimaran Govindarasu, studies a security model evaluating cyber attack exposure and derives quantitative security metrics for large-scale networked environments such as smart grid.

20. "Secure Lossless Aggregation Over Fading and Shadowing Channels For Smart Grid M2M Networks," by Andrea Bartoli, Juan Hernandez-Serrano, Miquel Soriano, Mischa Dohler, Apostolos Kountouris, and Dominique Barthel, presents a secure lossless aggregation protocol for achieving a viable security-communication trade-off tailored formachine-to-machine (M2M) communication in smart grid.

21. "Anomaly Detection for Cybersecurity of the Substations" by Chee-Wooi Ten, Junho Hong, and Chen-Ching Liu, investigates anomaly detection in the computer network environment of a substation and proposes an anomaly inference algorithm for early cyber intrusion detection at the substations.

KUI REN, *Guest Editor-in-Chief*
Electrical and Computer Engineering Department
Illinois Institute of Technology
Chicago, IL 60616 USA
kren@ece.iit.edu
ZUYI LI, *Guest Editor*
Electrical and Computer Engineering Department
Illinois Institute of Technology
Chicago, IL 60616 USA
lizu@iit.edu
ROBERT CAIMING QIU, *Guest Editor*
Department of Electrical and Computer Engineering
Tennessee Technological University
Cookeville, TN 38505 USA
RQiu@tntech.edu

Kui Ren (SM'11) received the B.S. and M.S. degrees from Zhejiang University, China, and the Ph.D. degree from Worcester Polytechnic Institute, Worcester, MA.

He is currently an Assistant Professor of Electrical and Computer Engineering Department at the Illinois Institute of Technology, Chicago. His research interests include smart grid security, security & privacy in cloud computing, lower-layer security mechanisms for wireless networks, and sensor & mesh network security. His research is supported by National Science Foundation, Department of Energy, and Amazon Web Services.

Dr. Ren is a recipient of NSF CAREER Award in 2011. He serves as an Associate Editor for IEEE WIRELESS COMMUNICATIONS and IEEE TRANSACTIONS ON SMART GRID. He is Guest Editor-in-Chief for the IEEE TRANSACTIONS ON SMART GRID Special Issue on Cyber, Physical, and System Security for Smart Grid.

Zuyi Li (SM'08) received the B.S. degree in electrical engineering from Shanghai Jiaotong University, Shanghai, China, in 1995, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 1998, and the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, in 2002.

Presently, he is an Associate Professor in the Electrical and Computer Engineering Department at the Illinois Institute of Technology. His research interests include electricity market design and operation, renewable energy integration, and microgrid design and operation.

Dr. Li is an Editor for IEEE TRANSACTIONS ON POWER DELIVERY and serves on the editorial board for *Electric Power Components and Systems*.

Robert Caiming Qiu (SM'01) received the Ph.D. degree in EE from the Polytechnic Institute of New York University.

He is a Professor in the Department of ECE, Tennessee Technological University, Cookeville. He was Founder-CEO of Wiscom Technologies, Inc., for WCDMA chipsets. Wiscom was sold to Intel. He worked for GTE Labs (now Verizon), Waltham, MA, and Bell Labs, Lucent, Whippany, NJ. He holds over five patents in WCDMA and authored over 50 journal papers/book chapters.

Dr. Qiu serves as Associate Editor, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is a Guest Book Editor on UWB from John Wiley and three special issues.