Guest Editorial
Smart Grid Cyber-Physical Security

THIS special section is devoted to the latest research advances in cyber-physical security and privacy of smart grids. A smart grid integrates advanced communication technologies and efficient bi-directional energy dispatch into the physical grid with the goal of achieving effective and efficient power management. However, the integration would make the mission-critical energy infrastructure more vulnerable to a wide variety of malicious cyber-attacks. Therefore, it is imperative to investigate the critical threats to the smart grid cyber-physical security and privacy, as well as to propose effective countermeasures to improve security and resilience of the smart grid.

In this special section, we took a two-phase approach in the paper selection process. In the first phase, we received 52 four-page short paper submissions, and accepted 21 of them. In the second phase, we invited those authors to submit full papers, and accepted 10 papers in total for this special section. The selected papers cover the following important topics in the field of smart grid security from both theoretical and practical standpoints, including privacy protection, intrusion detection, fault tolerance, anti-interference communication, and robust cyber architectures. An overview of the selected works is summarized as follows.

The first paper, "Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid against Internal Adversaries," studies the privacy-preserving data aggregation, an important problem of consumer privacy protection in the smart grid environment. This work proposes a new scheme against internal attackers using Paillier public key cryptography. The scheme does not use bilinear pairing or hash-to-point operations so that it is computationally more efficient than the existing solutions.

The second paper, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," focuses on an emerging category of threats to smart grids, i.e., coordinated cyber-physical attacks. Through analyzing the prerequisites of the implementation of the attacks, the corresponding countermeasures to detect those threats in both cyber and physical space are proposed. Both the implementation of coordinated cyber-physical attacks and the effectiveness of countermeasures are verified in IEEE test power systems.

The third paper, "Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks," introduces a new attack mechanism that uses both jamming and spoofing to intervene in normal wireless communications of the smart grid adopting cognitive radio networking approaches. To increase the adversarial implication to the grid, both the attack return values and the success probabilities under the constraint of the available power are considered. The main algorithm supporting the proposed attack mechanism is derived by a dynamic programming approach. This work is helpful to prevent the wireless communication of smart grids from malicious attacks.

The fourth paper, "Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids," aims to address the existing gap between the security as well as the resilience requirements and the provisioning of cost-effective smart grid communications. The work explores two intrusion detection system network design problems for smart grids, which optimally places detection devices on a communication path while providing resilient communications infrastructures. Moreover, a column-generation model-based approach is developed to address the problems with short computational time. The extensive numerical results demonstrate the applicability and efficiency of the proposed methodology.

The fifth paper, "OCPP Protocol: Security Threats and Challenges," investigates key security properties of the transmission protocols in smart grids, which specify communication between charging points and energy management systems. The authors focus on the scenario, where the attacks interfering with the grid power reservation are initiated by electric vehicles and a man-in-the-middle energy theft or fraud. A set of threats for the protocol are identified while a practical analysis is carried out in this work.

The sixth paper, "Achieving Privacy Protection Using Distributed Load Scheduling: A Randomized Approach," presents a general framework to protect residential users' privacy in smart grids. Unlike most existing protection works with high costs, the proposed schemes minimize the weighted sum of the privacy leakage by exploring the capacity of all energy-shiftable end-devices of residential users. The authors formulate the load scheduling of these devices as a mixed integer programming problem and deal with it using a randomized approach in various scenarios. It is concluded from extensive simulations that the proposed schemes outperform the existing privacy protection works in terms of lower power consumption and less mutual information.

The seventh paper, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," addresses DDoS attacks in the Advanced Metering Infrastructure (AMI) system in smart grids. In particular, the work introduces honeypots into the AMI network as a decoy system to detect and gather attack information. The interactions between the attackers and the defenders are modeled as a strategic honeypot game, and the optimal strategies for both

Digital Object Identifier 10.1109/TSG.2017.2735244

sides are derived. Simulation results prove that the proposed honeypot schemes greatly improve the defense efficiency and further enhance the security of AMI networks.

The eighth paper, “Differentially Private Smart Metering with Fault Tolerance and Range-Based Filtering,” notices that an operation center and gateways may be semi-honest while the users may launch electricity theft and false data injection (FDI) attacks. To address the challenging threat, this study presents a new privacy-preserving smart metering scheme, which leverages data aggregation, privacy differentiation, fault tolerance, and range-based filtering in the security design. Through the performance comparison between the proposed schemes and the existing approaches, they demonstrate enhanced security and efficiency.

The ninth paper, “Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking,” studies the problem of how to make microgrids achieve resilient and secure operations in the face of various cyber threats. The authors first incorporate SDN technologies into microgrids, which facilitates the deployment of novel and cost-effective security solutions. The work also proposes a new cyber-physical testing platform, which consists of a power distribution system simulator together with an SDN emulator working in a distributed control environment. The results indicate that the proposed SDN-based communication architecture significantly enhances the resilience and security of microgrids.

The tenth paper, “Real-time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism,” investigates FDI attacks in smart grids, which is considered as a severe threat to the grid control and data acquisition system. By exploiting deep learning techniques to recognize the characteristics of FDI attacks, a highly accurate detection mechanism with relaxed assumptions is proposed. The work is illustrated in four cases using IEEE test systems. The results demonstrate the improved resilience and accuracy in FDI attack detection.

In conclusion, this special section of IEEE TRANSACTIONS ON SMART GRID offers considerable and timely contributions to advance the cyber-physical security in smart grids. This section will be valuable for the readers who are interested in the cutting-edge cyber-physical security technology in the smart grid.

Finally, we sincerely express our gratitude to the Editor-in-Chief of IEEE TRANSACTIONS ON SMART GRID, Dr. Jianhui Wang for all the valuable advice and constructive comments. We would also like to thank all the anonymous reviewers for their hard work on reviewing the papers. Last but not least, we appreciate all the authors who spent time and effort to respond to this call-for-papers. We truly hope that the readers will enjoy and benefit from this special section.

YAN ZHANG, *Guest Editor*
University of Oslo
Oslo, Norway

DAVID YAU, *Guest Editor*
Singapore University of Technology and Design
Singapore

SAMAN ZONOUZ, *Guest Editor*
Rutgers University
New Brunswick, NJ, USA

DONG JIN, *Guest Editor*
Illinois Institute of Technology
Chicago, IL, USA

MEIKANG QIU, *Guest Editor*
Pace University
New York, NY, USA

MELIKE EROL-KANTARCI, *Guest Editor*
University of Ottawa
Ottawa, ON, Canada