Guest Editorial: Special Section on Cyber Physical Power Systems (CPPS)

Ming NI[1], Dong LIU[2], Chanan SINGH[3]

With the deep and pervasive application of information and communication technologies, power grid has become one of the vital cyber physical systems (CPS). However, the traditional analysis or control methods for power grid mainly focus on the physical power system, and treat the cyber and physical systems separately. To fully understand the interdependence and interplay of the cyber and physical systems, CPS should be studied as an integrated system. By studying the CPS, the mutual dependence of cyber and physical parts can be revealed, the risk due to the cyber-physical interaction can be reduced, and the methods for promoting the overall system efficiency can be derived. The special section is dedicated to reflect the latest progress and key technologies in cyber physical power systems (CPPS).

This special section includes a total of eleven papers which focus on the false data injection attacks, the general cyber security issue, the cascading failure, the emerging new technologies in CPPS. We had the honor of serving as the Guest Editor-in-Chief for this special section and would like to take this opportunity to thank the following Guest Editors for the special section who contributed to the review and the selection of the final papers: Dr. Qinglai GUO, Tsinghua University, China; Dr. Joydeep MITRA, Michigan State University, USA; Dr. Anurag SRIVASTAVA, Washington State University, USA; Dr. Simon TINDEMANS, Technische Universiteit Delft, Netherlands; Dr. Junhua ZHAO, Chinese University of Hong Kong (Shenzhen), China; and Dr. Visvakumar ARAVINTHAN, Wichita State University, USA.

Among the eleven papers included in the special section, 3 of them discuss the methods for the detection and defense of false data injection attacks, 3 of them deal with the cyber security issue in CPPS, 2 of them present the approaches on modeling and analysis of cascading failures in CPPS, and other 3 papers introduce some new technologies used in CPPS.

1) False data injection attacks in CPPS

Paper “Detection of false data injection attacks using unscented Kalman filter” points out that state estimation (SE), which is the most important real-time function in modern energy management systems (EMSs), is vulnerable to false data injection attacks, due to the undetectability of those attacks using standard bad data detection techniques. Therefore, paper proposes using the unscented Kalman filter (UKF) in conjunction with a weighted least square (WLS) based SE algorithm in real-time, to detect discrepancies between state variable estimates and, as a consequence, to identify false data attacks.

Paper “Graph theoretical defense mechanisms against false data injection attacks in smart grids” uses a graph-theoretical formulation based defense mechanism for mitigating false data injection attacks in smart grids. It discusses the characteristics of typical smart grid graph such as planarity. Then it proposes three different approaches for finding optimal protected meters set: a fast and efficient heuristic algorithm that works well in practice, an approximation algorithm that provide guarantee for the quality of the protected set, and an exact algorithm that find the optimal solution.

Paper “Set-theoretic detection of data corruption attacks on cyber physical power systems” addresses a set-theoretic method for the detection of data corruption cyberattacks on the load frequency control loop of a networked power system. Based on the

Received: 13 September 2018
✉ Ming NI
ni-ming@sgepri.sgcc.com.cn
Dong LIU
dongliu@sjtu.edu.cn
Chanan SINGH
singh@ece.tamu.edu
1. NARI Group Corporation, Nanjing 211106, China
2. Shanghai Jiao Tong University, Shanghai 200240, China
3. Texas A&M University, TX 77843, USA

overall discrete-time network dynamics a convex and compact polyhedral robust invariant set is extracted and is used as a set-induced anomaly detector.

2) Cyber security issus in CPPS

The significance of modern power grids is acknowledged every time there is a major threat. Paper "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information" points out that a key focus recently has been in assessing the risk of a coordinated cyber-physical attack and minimizing the impact of a successful attack. Most of the cyber-attackers will have limited system information and conventional power grid 'N-1' security analysis cannot be extended to assess the risk. This paper presents a graph theory based centrality indices for vulnerability assessment of the power system due to various bus and branch contingencies using limited system information and provides preliminary defense mechanism to prevent such an attack.

Paper "Cyber-secure decentralized energy management for IoT-enabled active distribution networks" provides a strategic solution for enhancing the cybersecurity of power distribution system operations when information and operation technologies converge in active distribution network (ADN). The paper first investigates the significance of Internet of Things (IoT) in enabling fine-grained observability and controllability, and then proposes a cyber-secure decentralized energy management framework that takes advantage of software-defined networking technologies that can secure communications among IoT devices in individual microgrids, and exploits potentials for introducing blockchain technologies that can preserve the integrity of communications among networked microgrids in ADN.

Paper "A tri-level programming model for attack-resilient control of power grids" proposes the novel approaches to aid power system planner to improve power grid resilience by making appropriate hardening strategies against man-made attack or natural hazards. The vulnerability indices are introduced, which return the most vulnerable component in the system based on a tri-level defender-attacker-operator (DAO) interdiction problem which solves iteratively. The output of DAO is the set of hardening strategies that optimally allocated along the network to mitigate the impact of the worst-case damages.

3) Cascading failures in CPPS

The utilization levels of the transmission network can be enhanced by the use of automated protection schemes that rapidly respond to disturbances. However, such corrective systems may suffer from malfunctions that have the potential to exacerbate the impact of the disturbance. Paper "Risk-based method to secure power systems against cyber-physical faults with cascading impacts: a system protection scheme application" addresses a holistic assessment of the cyber (protection logic) and physical (network) systems, considering the failures in each part and their interplay. An iterative optimization method is proposed that relies on power system response simulations in order to perform detailed impact assessments and compare candidate solutions.

Paper "Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems" presents a model of cascading failures in CPPS based on an improved percolation theory, and then proposes failure mitigation strategies. In this model, the power flow in the power grid, along with the data transmission and delay in the cyber layer, is considered in the improved percolation theory.

4) New technologies used in CPPS

The increasingly complex interaction among different energy entities calls for a secure, efficient, and robust cyber infrastructure. As an emerging distributed computing technology, Blockchain provides a secure environment to support such interactions. Paper "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems" gives a prospective on using Blockchain as a secure, distributed cyber infrastructure for the future grid. A Blockchain based smart grid cyber-physical infrastructure model is proposed. Some promising application domains of Blockchain in future grids and potential challenges are also presented in this paper.

Paper "Demand dispatch in cyber-physical load aggregation system with multilevel incentives" presents a demand dispatch strategy for aggregated electric water heaters (EWHs) in a load aggregation system at demand side, based on the theory of cyber-physical system. The objective is to solve the problem of water heater load control when the cyber-physical load aggregation system participates in demand dispatch of the power grid. A multilevel incentive model, an EWH appliance model and a thermostat setpoint control rule are introduced. Based on the models and the rules, an implementation framework of the demand dispatch strategy is designed between the cyber space and the physical space, including state awareness, real-time analysis, scientific decision-making and precise execution.

While local control for photovoltaic (PV) plants improves the network security, it lacks the optimization benefits from centralized control strategies. Paper "Effects of centralized and local PV plant control for voltage regulation in LV feeder based on cyber-physical simulations" considers the coordination of the two control strategies. Through modeling and simulation in an established real-time cyber-physical simulation platform, the LV network is evaluated with both local and centralized control. A set of boundaries for coordinating between the two strategies are identified, which can help network operators in deciding suitable control in different operating situations.