



Defense Measures and Support Technologies for Network Attacks in Power Cyber-physical Systems

Introduction and topics

Under the vision of carbon peak and carbon neutrality, constructing the next generation of power systems with renewable energy as the main body will cause profound changes in the power system structure, system characteristics, operation modes, and significant risks. It will also bring new challenges to the security and stability of the operation of the power system. In particular, the large-scale penetration of digitization and information technology in the perception and control of power systems, such as data acquisition and monitoring and control systems (SCADA), wide area measurement systems (WAMS), et al., as well as increased demand for the integration of generation, power grid, load, and storage, will make the control system of the power system more susceptible to manufactured external damage.

Integrating digital and information technologies brings about cyber security issues that cannot be ignored and are more likely to cause large-scale power outages. The openness and standardization of communication protocols will significantly reduce the difficulty of attackers attacking information systems. Intelligent sensing, measurement, and control devices generally lack security protection and even have serious security vulnerabilities, posing more potential attack points for PGCPs, thereby increasing the risk of network attacks. Frequent cyberattacks targeting the information and physical systems of the power grid have resulted in very negative consequences. In 2017, the WannaCry ransomware virus broke out, affecting over 100,000 terminals in more than 100 countries and regions worldwide and affecting various industries such as education, finance, energy, and healthcare to varying degrees. In September 2019, the Nuclear Power Corporation of India Ltd (NPCIL) confirmed that the internal network of the Kudankulam nuclear power plant in Tamil Nadu, India, was infected with malicious software.

This panel session mainly focuses on the risks and countermeasures brought by cyberattacks on the operation of the power system. The speakers will respectively introduce their latest research results on identifying abnormal states of power systems, the cyberattacks and defense measures in power systems, the intelligent information technology of power systems, and the cyber-physical-social systems supporting intelligent and low-carbon power systems.

Panel Session Chairs



Yingjun Wu

Hohai University

Yingjun Wu received a doctoral degree from Politecnico di TORINO (PoliTO) in Italy in 2013. He is an Associate Professor at the School of Energy and Electrical Engineering at Hohai University. He has hosted over 30 research projects and published over 70 papers, issued 8 patents, developed 1 intelligent power distribution simulation system, and won the first prize for management innovation achievements in Jiangsu Province. He serves as the Secretary General of the IEEE PES Nanjing Branch, a member of the IEEE PES Youth Technology Committee (YP TAC SC), an Executive Director of the IEEE PES (China) onshore wind power grid connection and consumption technology branch, and members of several IEEE PES (China) Satellite Technology Committees. He also serves as the visiting deputy editor-in-chief and editorial board member of academic journals such as FRONT ENERGY RES, ELECTRONICS-SWITZ, and Power Demand Side Management. He has also served as the chairman of the IEEE APPEEC-2020 Invited Report Subcommittee and the chairman of multiple international conference venues.



Qiang Yang

Zhejiang University

Qiang Yang (M'03-SM'18) received Ph.D. degree in Electronic Engineering and Computer Science from Queen Mary, University of London, London, U.K., in 2007 and worked in the Department of Electrical and Electronic Engineering at Imperial College London, U.K., from 2007 to 2010. He visited the University of British Columbia and the University of Victoria Canada as a visiting scholar in 2015 and 2016. He is currently a full Professor at the College of Electrical Engineering, Zhejiang University, China, and has published more than 240 technical papers, filed 50 national patents, co-authored 2 books, and edited 2 books and several book chapters. His research interests over the years include smart energy systems, large-scale complex network modeling, control and optimization, learning based optimization and control. He is a Fellow of the British Computer Society (BCS), a Senior Member of IEEE, and the Senior Member of China Computer Federation (CCF).

SPONSORS



ORGANIZERS



CO-ORGANIZERS

