Proceedings of the Canadian Society for Mechanical Engineering International Congress
32nd Annual Conference of the Computational Fluid Dynamics Society of Canada
Canadian Society of Rheology Symposium
CSME-CFDSC-CSR 2025
May 25–28, 2025, Montréal, Québec, Canada

Security and Resilience in Cyber-Physical Systems for Smart Grids

Jin Li[1], Youmin Zhang[1]
[1] Department of Mechanical, Industrial and Aerospace Engineering, Concordia University, Montreal, Quebec, Canada
charlesliqd@gmail.com, ymzhang@encs.concordia.ca

ABSTRACT

This research delves into the vital integration of Cyber-Physical Systems (CPS) within smart grids, aiming to confront the pressing challenges posed by cyberattacks and physical faults. The intricate nature of CPS, characterized by the close interdependence of physical and cyber components, reveals vulnerabilities that can jeopardize the reliability and security of critical infrastructures, particularly energy systems. By focusing on the development of robust methodologies for detection, diagnosis, and resilience within smart grids, this study positions itself as a crucial response to these threats.

Among its key contributions, the research emphasizes the effective application of innovative observer-based techniques, adaptive Unscented Kalman Filters, and second-order sliding mode algorithms for the timely detection and mitigation of faults and cyberattacks. A groundbreaking distributed state estimation framework is proposed, which empowers scalable and accurate monitoring of interconnected CPS components. This framework leverages local estimators and weighted fusion techniques to deliver comprehensive global state estimates while ensuring computational efficiency.

Furthermore, attack-resilient control strategies are meticulously crafted to withstand threats, including Denial-of-Service (DoS) and False Data Injection (FDI) attacks, thereby safeguarding stable and secure system operations. The inclusion of a model-based diagnosis mechanism significantly enhances the system's responsiveness to concurrent faults and cyberattacks.

Validation of these methodologies is achieved through extensive simulations conducted on a MATLAB/Simulink-based smart grid benchmark. These simulations encompass various scenarios, including normal operations, fault injections, and cyberattacks, effectively showcasing the proposed system's capability to maintain stability, reliability, and efficiency even under adverse conditions. By merging theoretical advancements with practical implementations, this study effectively bridges the divide between academic research and industrial application, offering scalable solutions to resolve real-world smart grid challenges.

The anticipated outcomes promise enhanced security and reliability within smart grids, scalable detection frameworks, and practical fault-tolerant mechanisms. These advancements are not just enhancements; they represent a transformative leap in the operational resilience of smart grids and lay the groundwork for future research in CPS security. This pioneering work establishes a foundation for incorporating emerging technologies, such as artificial intelligence, blockchain, and digital twins, further bolstering the security and efficiency of CPS. By addressing critical gaps in CPS monitoring and control, this research contributes significantly to the emergence of robust, efficient, and secure smart grid systems, with profound implications for both academia and industry.

Keywords: Cyber-Physical Systems (CPS), Smart Grids, Fault Detection and Diagnosis (FDD), Cyberattack Resilience, Observer-Based Techniques, Sliding Mode Control, Distributed State Estimation, Adaptive Kalman Filters.