Mitigating Load-Altering Attacks Against Power Grids Using Cyber-Resilient Economic Dispatch

Zhongda Chu, Member, IEEE, Subhash Lakshminarayana, Senior Member, IEEE
Balarko Chaudhuri, Senior Member, IEEE and Fei Teng, Senior Member, IEEE

Abstract—Large-scale Load-Altering Attacks (LAAs) against Internet-of-Things (IoT) enabled high-wattage electrical appliances pose a serious threat to power system security and stability. This paper investigates, for the first time, the optimal mitigation strategy from a system perspective against such attacks. In particular, a Cyber-Resilient Economic Dispatch (CRED) concept is proposed and seamlessly integrated with attack detection and identification to form a cyber resiliency enhancement framework. Instead of only relying on local resources, CRED coordinates the frequency droop control gains of Inverter-Based Resources (IBRs) in the system to mitigate the destabilizing effect of LAAs while minimizing the overall operational cost. To achieve this, the LAA-inclusive system frequency dynamics is formulated and the corresponding system stability constraints are explicitly derived based on parametric sensitivities, which are further incorporated into the system scheduling model with minimum error through a novel recursive linearization method. In addition, a distributionally robust approach is proposed to account for the uncertainty associated with system dynamics driven by the LAA detection/parameter estimation errors. The overall performance of the proposed CRED model is demonstrated through extensive simulations in a modified IEEE reliability test system.

Index Terms—Economic dispatch, cyber-resilience, load altering attacks, system stability, sensitivity analysis