Abstract

Adversarial conditions impacting modern power systems present emerging challenges in the energy industry, a challenge that is further accentuated by the evolution of power systems into cyber-physical smart grids (CPSG). The intricate nature of the components within the CPSG, along with their interactions, contributes to the complex ways in which adversarial conditions may affect a power grid. The growing prevalence of components such as information and communication technologies (ICTs), distributed energy resources (DERs), and fluctuating supplies and demands due to the infusion of renewable sources and electric vehicles (EVs), is making the challenge of ensuring the secure and cost-effective operation of a CPSG increasingly complicated.

Cyber attacks stand out as a significant adversarial condition in CPSGs, driven by the attacker's malicious intent to undermine the secure and economic operations of CPSGs for potential monetary gains, strategic advantages, or geopolitical influence. In recent times, load redistribution (LR) attacks have emerged as one of the most practical and realistic forms of cyber attacks involving the injection of false data in load and line power flow measurements by exploiting vulnerabilities in ICTs.

Adversarial conditions in CPSGs may not always stem from malicious intent but can result from uncertainties in various factors affecting grid operations. Some of the most common forms of such adversarial conditions are those that arise from intermittency associated with the DERs and uncoordinated EV charging. DER-related uncertainties often lead to challenges in mitigating congestion in the transmission lines of the CPSG, a problem expected to become more prevalent with the increasing adoption of DERs like solar and wind energy. Additionally, uncoordinated EV charging in future CPSGs can trigger various grid issues, such as high voltage and high-frequency deviations, elevated power losses, and reduced energy efficiency.

This work aims to develop and study AI-driven methods to effectively address some types of adversarial conditions that have emerged in recent years due to the ongoing evolution of the CPSG. In particular, the contributions of this thesis are as follows:

1. *Defense Against LR Attacks:* This thesis centers on the multifaceted aspects of LR attacks within the Smart Grid. The key contributions in this domain encompass:

    - Examining an attacker's potential to influence grid operations is a crucial area of research, as it enables grid operators or defenders to construct robust defense mechanisms against potential attacks. In pursuit of this goal, we have introduced a deep learning (DL) approach for analyzing the LR attack on the Smart Grid. This research provides valuable insights into the attacker's capacity to launch a real-time and localized LR attack, eliminating the need for sensitive, confidential, and intricate grid information.
    - We have devised a protection-centric defensive strategy to thwart the more novel, stealthy and *state-of-the-art* variant of LR attacks, known as dummy LR attacks.
    - We have proposed a methodology to pinpoint critical loads susceptible to LR attacks in the grid. This addresses the challenge of data deluge on ML detectors designed explicitly for LR attacks, a problem exacerbated by the grid's expanding nature. Our findings illustrate that detecting an LR attack can be accomplished by monitoring only the critical loads within the grid, streamlining the detection process instead of monitoring all loads across the entire grid.

2. *Congestion Mitigation Under Supply Side Uncertainties:* In this work, we tackle the adversarial condition of congestion in the transmission lines of the grid stemming from uncertainty in the grid caused by the intermittent nature of solar power. Initially, we introduced an ML formulation designed to estimate grid congestion directly from generation data. Subsequently, we presented an ML-based real-time optimal power flow approach for effective congestion management.

3. *Hybrid Centralised Decentralised EV Coordination for Grid Management:* In this research, we have focused on addressing the inadvertent adversarial

condition stemming from the uncoordinated charging of a large-scale EV penetration within the Smart Grid.

Keywords: Smart Grid, Cyber Security of Grid, Load Redistribution Attack, Dummy Load Redistribution Attack, Critical Loads, Machine Learning, Deep Learning, Renewable Energy, Solar Power, Congestion Management, Real-Time Optimal Power Flow, Robust Electric Vehicle Coordination.