Securing FACTS-Based Wide Area Damping Controllers Using Modified Conditional Generative Adversarial Networks

Masoud Babaei Vavdareh[1], Mohsen Ghafouri[1], Amir Ameli[2]

[1]Concordia University, [2]Lakehead University

The performance of wide-area damping controllers (WADCs) heavily depends on the accuracy and authenticity of the measurements received from phasor measurement units (PMUs). These controllers receive PMU data and send the control commands back to grid actuators, e.g., flexible AC transmission systems (FACTS) devices. The use of cyber systems required for transferring PMU measurements, however, makes the controller and entire power system prone to a variety of cyber attacks, e.g., false data injection attacks (FDIAs). On this basis, this paper (i) proposes an FDIA model against FACTS-based WADCs and (ii) develops detection and mitigation methods for the proposed attacks. First, FDIAs are designed to destabilize the system, considering realistic limitations on the power grids. Then, a modified conditional generative adversarial network (MCGAN) is utilized for the detection and mitigation of these FDIAs. To detect this attack, a detector is developed from the discriminator of MCGAN, using the fine-tuning technique. The use of this proposed method enhances detection performance in imbalanced datasets and effectively identifies unseen high-risk attacks. Following the detection, a mitigation method is implemented based on the coordination of a graph-based interpolation and the tuned generator of the developed MCGAN. This method effectively mitigates the impact of the FDIAs on the FACTS-based WADCs. The effectiveness of the attack model, as well as the detection and mitigation methods, is assessed using the two-area Kundur and New England 39-Bus test systems.

979-8-3315-8138-1