Interactions of AGC Cyber-Attacks and Remedial Action Schemes in a Two-Area System

Abdulmannan Ajabnoor[1], Zhi Jin Zhang[2], Maryam Saeedifard[1], Dominic Groß[3]

[1]Georgia Institute of Technology, [2]University of British Columbia, [3]University of Wisconsin-Madison

Automatic generation control (AGC) adjusts generator set-points through communication to maintain frequency stability and scheduled power transfer between neighboring areas of power systems. Due to cyber-vulnerabilities in communication networks, the AGC signal is susceptible to attacks, potentially leading to abnormal frequency deviations. This paper analyzes an attack strategy targeting AGC and the factors influencing its success. First, the paper outlines the attacker model and briefly reviews the feedback attack policy. Then, it examines the impact of power system parameters on the likelihood of a successful attack, using a decision tree algorithm, establishing guidelines to identify worst-case scenarios from a system operator's perspective. Adhering to these guidelines can increase the probability of a successful attack, which is verified using phasor simulation with detailed turbine/governor and protection models. Additionally, the paper examines the attacker threat model, which identifies the attack surface required to steer the system frequency to an unsafe state while avoiding the activation of the remedial action scheme (RAS). If an attacker gains access, they could prevent the tripping of generator circuit breakers, thereby increasing the risk of a system-wide collapse and/or blackout.

979-8-3315-8138-1