Evaluating power system vulnerability to false data injection attacks via scalable optimization

Submitted by grigby1 on Mon, 11/27/2017 - 12:24pm

Title	Evaluating power system vulnerability to false data injection attacks via scalable optimization
Publication Type	Conference Paper
Year of Publication	2016
Authors	Chu, Z., Zhang, J., Kosut, O., Sankar, L.
Conference Name	2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)
Date Published	nov
Keywords	Algorithm design and analysis, bi-level optimization problem, composability, false data injection cyber-attacks, Generators, IEEE 118-bus system, integer programming, Linear programming, Load flow, lower bounds, Metrics, mixed-integer linear program, Optimization, physical power flow maximization, Polish system, power grid vulnerability analysis, power system security, power system vulnerability evaluation, pubcrawl, Resiliency, scalable optimization, security of data, Smart grids, state estimation, Upper bound, upper bounds, vulnerability assessments, worst-case attack consequences

Abstract

Physical consequences to power systems of false data injection cyber-attacks are considered. Prior work has shown that the worst-case consequences of such an attack can be determined using a bi-level optimization problem, wherein an attack is chosen to maximize the physical power flow on a target line subsequent to re-dispatch. This problem can be solved as a mixed-integer linear program, but it is difficult to scale to large systems due to numerical challenges. Three new computationally efficient algorithms to solve this problem are presented. These algorithms provide lower and upper bounds on the system vulnerability measured as the maximum power flow subsequent to an attack. Using these techniques, vulnerability assessments are conducted for IEEE 118-bus system and Polish system with 2383 buses.

URL	https://ieeexplore.ieee.org/document/7778771/
DOI	10.1109/SmartGridComm.2016.7778771

Citation Key chu_evaluating_2016

Algorithm design and analysis bi-level optimization problem composability false data injection cyber-attacks Generators IEEE 118-bus system integer programming Linear programming Load flow lower bounds Metrics mixed-integer linear program optimization physical power flow maximization Polish system power grid vulnerability analysis power system security power system vulnerability evaluation pubcrawl Resiliency scalable optimization security of data Smart Grids state estimation Upper bound upper bounds vulnerability assessments worst-case attack consequences