Moving-Target Defense for Detecting Coordinated Cyber-Physical Attacks in Power Grids

Title	Moving-Target Defense for Detecting Coordinated Cyber-Physical Attacks in Power Grids
Publication Type	Conference Paper
Year of Publication	2019
Authors	Lakshminarayana, Subhash, Belmega, E. Veronica, Poor, H. Vincent
Conference Name	2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)
Date Published	oct
Keywords	CCPA detection, compositionality, Coordinate measuring machines, coordinated cyber-physical attacks detection, cost reduction, Cyber-physical systems, cyberattack, D-FACTS device deployment, distributed flexible AC transmission system devices, False Data Injection, flexible AC transmission systems, game theory, game-theoretic approach, grids transmission line reactances, human factors, IEEE bus systems, links subset, MATPOWER simulator, Moving Target Defense strategy, MTD design criteria, operators defense cost reduction, power engineering computing, power grids, power system security, power transmission economics, power transmission lines, power transmission reliability, pubcrawl, Resiliency, security of data, sensor measurements, set theory, Smart Grid Sensors, state estimation, systems operational time, telecommunication security, Transmission line matrix methods, Transmission line measurements, undetectable line outages

Abstract This work proposes a moving target defense (MTD) strategy to detect coordinated cyber-physical attacks (CCPAs) against power grids. A CCPA consists of a physical attack, such as disconnecting a transmission line, followed by a coordinated cyber attack that injects false data into the sensor measurements to mask the effects of the physical attack. Such attacks can lead to undetectable line outages and cause significant damage to the grid. The main idea of the proposed approach is to invalidate the knowledge that the attackers use to mask the effects of the physical attack by actively perturbing the grid's transmission line reactances using distributed flexible AC transmission system (D-FACTS) devices. We identify the MTD design criteria in this context to thwart CCPAs. The proposed MTD design consists of two parts. First, we identify the subset of links for D-FACTS device deployment that enables the defender to detect CCPAs against any link in the system. Then, in order to minimize the defense cost during the system's operational time, we use a game-theoretic approach to identify the best subset of links (within the D-FACTS deployment set) to perturb which will provide adequate protection. Extensive simulations performed using the MATPOWER simulator on IEEE bus systems verify the effectiveness of our approach in detecting CCPAs and reducing the operator's defense cost.

DOI 10.1109/SmartGridComm.2019.8909767

Citation Key lakshminarayana_moving-target_2019

cyberattack security of data telecommunication security game theory cyber-physical systems Resiliency pubcrawl cost reduction power grids False Data Injection power engineering computing power system security Human Factors state estimation Compositionality set theory CCPA detection Coordinate measuring machines coordinated cyber-physical attacks detection D-FACTS device deployment distributed flexible AC transmission system devices flexible AC transmission systems game-theoretic approach grids transmission line reactances IEEE bus systems links subset MATPOWER simulator Moving Target Defense strategy MTD design criteria operators defense cost reduction power transmission economics power transmission lines power transmission reliability sensor measurements systems operational time Transmission line matrix methods Transmission line measurements undetectable line outages Smart Grid Sensors