UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Electric Grid Power Flow Model Camouflage
Against Topology Leaking Attacks
by
Ian Markwood

For the Ph.D. degree in Computer Science & Engineering

The power flow model for DC power grids has been used theoretically to launch false data injection attacks (FDIAs) against state estimation. We recognize FDIAs are just one possible attack using the power flow model and that the grid topology information within the model implies its discovery may also facilitate topology-based attacks. We show attackers can derive the power flow model, and thus the topology also. Indeed, with incomplete data, attackers can accurately reconstruct regions of the model, or topology, all that is necessary to launch an attack. We also illustrate how to cause such attackers to derive instead a convincing fake model by camouflaging the real model. Consequently, no sensitive information will leak, so attacks based on this fake model will be ineffective, alerting grid administrators to the attacker's efforts.

November 17, 2017
3:00pm
ENB 337

THE PUBLIC IS INVITED

Examining Committee
Yao Liu, Ph.D., Major Professor
Jay Ligatti, Ph.D.
Simon Ou, Ph.D.
Richard Gitlin, Ph.D.
Dan Shen, Ph.D.

Miguel Labrador, Ph.D.
Graduate Program Director
Computer Science and Engineering
College of Engineering

Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering

Disability Accommodations:

If you require a reasonable accommodation to participate, please contact the
Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.