Vulnerability Analysis Of Optimal Power Flow Problem Under Cyber-Physical Security Attacks

Devendra Shelar and Saurabh Amin

Massachusetts Institute of Technology

INFORMS
November 15th, 2016

Vulnerable Electricity Networks: Key issues

- In addition to reliability failures, power grids are increasingly vulnerable to cyber-physical security (CPS) attacks
- Such CPS attacks can be modeled as bilevel optimization problems
- We present two CPS attack scenarios
  - Dynamic Line Rating (DLR) Manipulation
  - Distributed Energy Resource (DER) disruption
- Structural insights allow for greedy and efficient (approximate) algorithms

Two motivating attack models

California Sniper Attack

Ukraine Cyber Attack

Related work

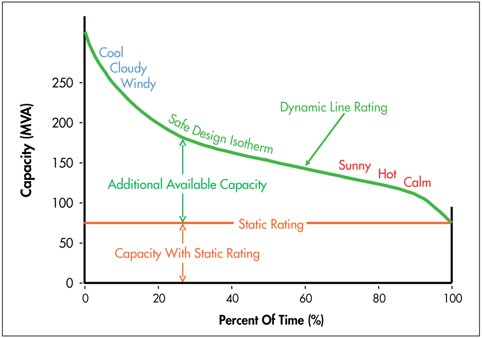
- A. Verma, D. Bienstock: N-k vulnerability problem
  - Attacker disrupts generators or manipulates line impedances to maximinimize load shedding
  - DC Power Flow approximation
- S.Wright et al.: Vulnerability Analysis of Power Systems
  - Attacker increases the line impedances to maximinimize
    - Loss of voltage regulation, OR Load shedding
  - Use both active and reactive power
- R. Baldick, K. Wood, D. Bienstock: Network Interdiction, Cascades

Use bilevel optimization models with outer problem as attack model, and the inner problem being optimal power flow **(OPF) problem**

- Ensure demand is fully met while minimizing costs subject to generator, capacity, supply-demand balance, power flow constraints

DLR Manipulations in Transmission Networks

Figure 1: Tapping into existing capacity above the static rating



Source: Valley Group

Line capacity violations have cause cascading failures in the past, e.g., July 2012 blackout in India

Bilevel problem (Stackelberg game)

- Leader: Attacker compromises the DLRs using false data injection attack;
- Follower: Defender's economic dispatch solution is optimal for new *manipulated* system, but possibly infeasible for the old *actual* system.

Problem statement:

- Determine an optimal attack plan to maximinimize line rating violations

Solution Approaches

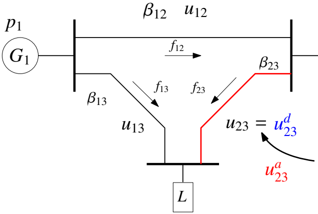
Benders Decomposition (Kevin Wood et al.)

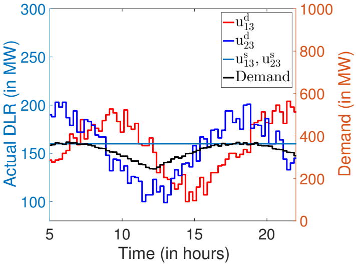
- Alternately consider follower problem, with fixed attacker actions, and master problem with fixed defender actions
- Sequentially generate Benders cut for the Master Problem until zero optimality gap
- Results in systematic vertex enumeration of the inner problem

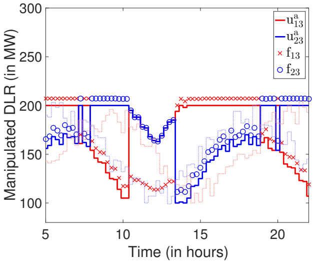
Kuhn-Tucker Single-level reformulation (Bard et al.)

- Apply KKT optimality conditions for the inner problem, and reformulate complementarity constraints
- Use Branch-n-Bound techniques to solve the resulting Mixed-Integer Linear Program (MILP)

Insights

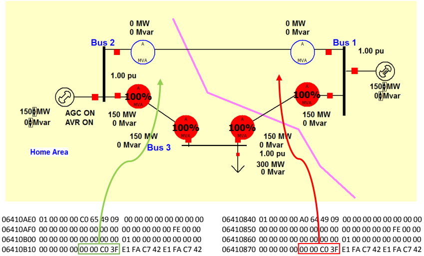




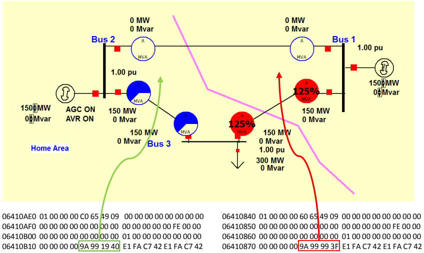


- Attacker strategy, by and large, exhibits a bang-bang policy
  - Some DLRs are set to maximum
  - Other DLRs are set to minimum (as long as feasible operating point exists)
- Similar results hold for larger (118 node) testcase

Implementation of attack in Powerworld simulator



(c) Pre-attack system state (safe).



(d) Post-attack system state (unsafe).