Vulnerability Analysis of Distribution Networks under Renewable Disruptions

Devendra Shelar and Saurabh Amin

shelard@mit.edu; amins@mit.edu

FORCES all hands meeting, Oakland, CA
June 16th, 2014

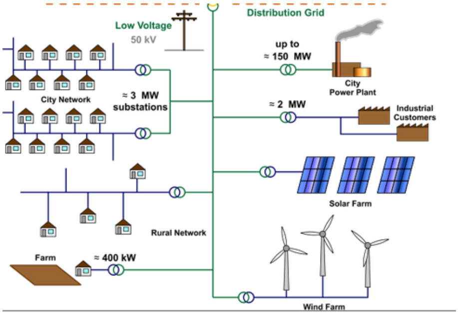
Massachusetts Institute of Technology

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Electricity distribution network vulnerabilities

Motivation

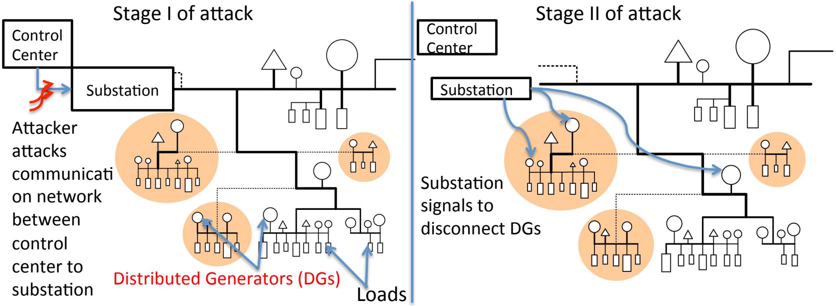
- IT systems manage distributed generators (DGs) & other operations
- Security risks introduce new vulnerabilities in distribution networks



Our focus

1. Worst case attacks: Denial-of-service (DoS) or manipulation of DGs
2. Secure network control: using reactive power control and load shaping

Attacker-defender interaction



Questions:

- Which DGs are most critical?
- How should defender respond?

Acknowledgement: Discussion with Bruno Prestat and Pascal Sitbon (EPRI) and Dr. Alexandra von Meier (UC Berkeley)

Network interdiction

Perfect information attacker (leader)-defender (follower) game:

- Attacker choices: compromise DGs
- Defender choices: control available DGs to provide reactive power (VAR) control and/or manipulate available loads

Problem 1

Find attacker's interdiction plan and defender control strategy when

- Attacker chooses DG interdiction plan to maximize sum of line loss and load shedding, and
- Defender responds by providing VAR control and manipulates loads, while maintaining ratings of protection equipment.

$$\max_{\delta} \quad \min_{u} \sum_{(i,j)\in\mathcal{E}} r_{ij}\ell_{ij} + \sum_{i\in\mathcal{N}_0} (1-\gamma_i)C_i$$

s.t. powerflow, DG, ratings, resource constraints

$$u := (P, Q, p^g, p^c, q^g, q^c, \nu, \ell, \gamma), \gamma \in [0,1]^n, \quad \delta \in \{0,1\}^n.$$

A related problem

Problem 2

Find attacker's interdiction plan and defender control strategy when

- Attacker chooses DG interdiction plan to cause loss of voltage regulation, and
- Defender responds by providing VAR control. (Load and ratings constraints may or may not be satisfied.)

$$
\begin{aligned}
\min_{\delta} \quad & \max_{u} \; \min_{i \in \mathcal{N}_0} \nu_i \\
\text{s.t.} \quad & \text{powerflow, DG, resource constraints} \\
& u := (P, Q, p^g, q^g, \nu) \\
& \delta \in \{0,1\}^n
\end{aligned}
$$

Case of fixed defender choices

Aforementioned bilevel-problems are hard!

- Outer problem: integer-valued attack variables
- Inner problem: nonlinear in control variables

For fixed defender choices:

Problem 1': $$\max_{\delta} \sum_{(i,j)\in\mathcal{E}} r_{ij}\ell_{ij} + \sum_{i\in\mathcal{N}_0} (1-\gamma_i) C_i$$

s.t. powerflow, dg, ratings, resource constraints

Problem 2': $$\min_{\delta} \min_{i\in\mathcal{N}_0} \nu_i$$

s.t. powerflow, dg, resource constraints

We use structural results for Problems 1' and 2' to compute interdiction plans for the case with defender response (Problems 1 and 2).

Main result: Optimal interdiction plan

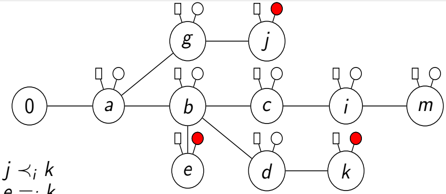
- Let ν_i^{old}/ν_i^{new} be $|V_i|^2$ before/after the attack
- $\Delta(\nu_i) = \nu_i^{old} - \nu_i^{new}$

Theorem

For a tree network, given nodes i (pivot), $j, k \in \mathcal{N}_0$:

- If DGs at j, k are homogenous and j is before k w.r.t. i, then DG disruption at k will have larger effect on ν_i at i;
- If DGs at j, k are homogenous and j is at the same level as k w.r.t. i, then DG disruptions at j and k will have the same effect on ν_i at i;

$$\Delta_j(\nu_i) < \Delta_k(\nu_i)$$
$$\Delta_e(\nu_i) \approx \Delta_k(\nu_i)$$



$j \prec_i k$
$e =_i k$
$b \prec k$

Current work

Algorithms

- Optimality properties of proposed algorithm;
- Re-formulation as Mixed-Integer Second-Order Cone Program;
- Evaluation on benchmark distribution feeder networks.

Validation

Mapping of the optimal attack plans to cyber-attacks and co-simulation.

Thank You