Analyzing Vulnerability of Electricity Distribution Networks to DER disruptions

Devendra Shelar
Saurabh Amin

Massachusetts Institute of Technology

ACC 2015

Outline

Vulnerability analysis & control of distribution networks

Questions

- How to assess vulnerability of electricity networks to disruptions of Distributed Energy Resources (DERs)?
- What is the optimal attacker interdiction plan?

Approach

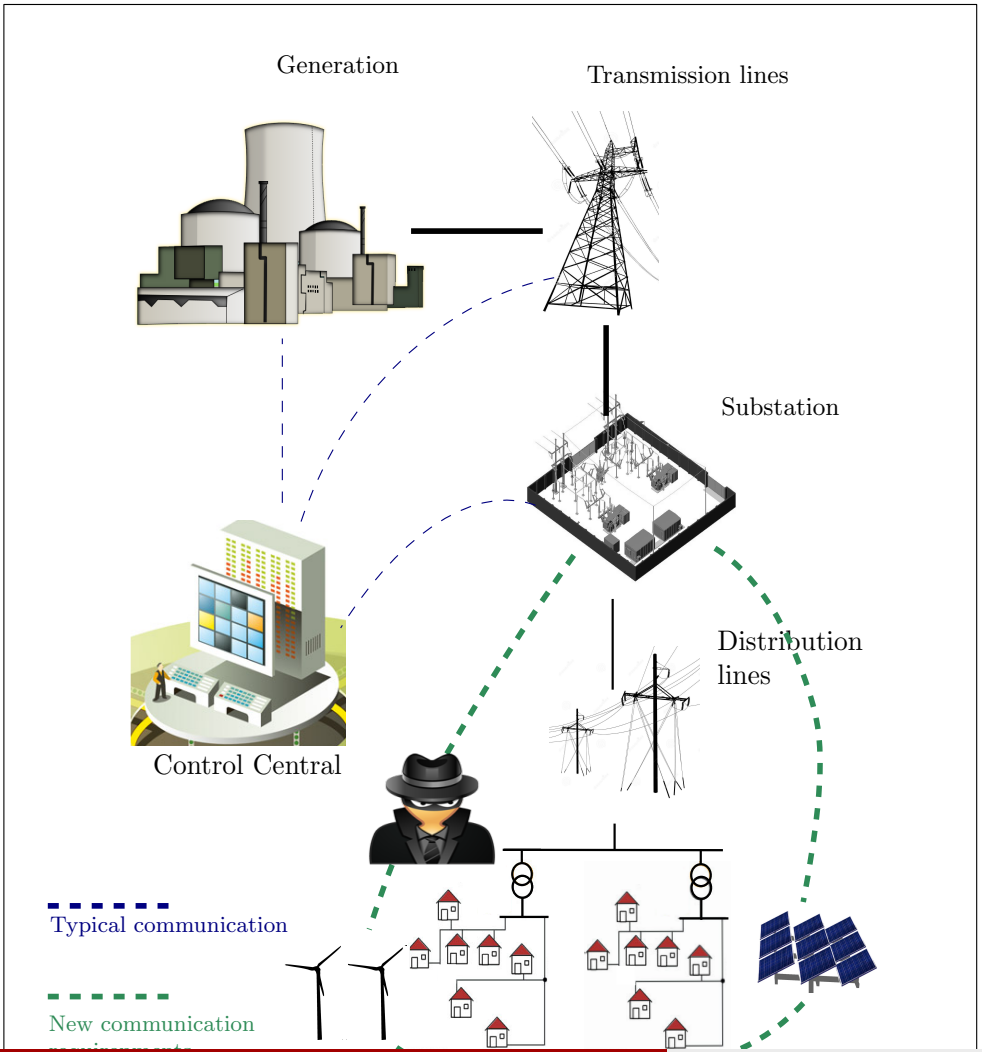
Attacker-defender model; Network interdiction formulation; Characterization of worst-case attacks; Defender strategies

Results

- Interdiction model captures threats to DERs / smart inverters;
- Structural results on worst case attacks that maximize weighted sum of cost due to loss of voltage regulation and cost of load control;
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints;

Main idea: Model of DER disruptions

Vulnerability: Control Center and Substation communications



- Hack control center-substation communications
- Introduce incorrect set-points and disrupt DERs
- Create supply-demand mismatch
- Cause voltage bounds violations
- Induce cascading failures

Outline

Network interdiction

Network interdiction problem

- Perfect information leader-follower game;
- Attacker moves first and defender moves next.

Problem statement:

- Determine attacker's interdiction plan (compromise DERs) to maximize the sum of loss of voltage regulation (LOVR), and load shedding (LL),
- Under defender choices:
  - Non-compromised DERs provide active and reactive power (VAR);
  - Demand at consumption nodes may be partly satisfied;
  - Small LOVR acceptable.

Related work

Control of distribution systems

- Steven Low, Javad Lavaei, *et al.*: Convex optimal power flow (on tree networks)
- Konstantin Turitsyn *e. al.*, Ian A. Hiskens. *et. al.*: Distributed optimal VAR control balancing voltage regulation and line losses

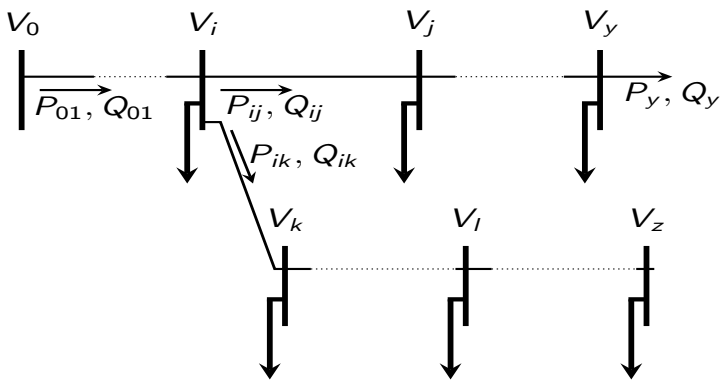
Resilience and security of networked systems

- Ross Baldick, Kevin Wood: Interdiction for transmission networks
- Daniel Bienstock, *et al.*: Cascading failures with linear power flow
- Rakesh Bobba, Robin Berthier: AMI security, false-data injection

Network model

Tree networks

- $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ - tree network of nodes and edges
- $\nu_i = |V_i|^2$ - square of voltage magnitude at node i
- $\ell_{ij} = |I_{ij}|^2$ - square of current magnitude from node i to j
- $z_{ij} = r_{ij} + \mathbf{j}x_{ij}$ - impedance on line (i, j)
- P_{ij}, Q_{ij} - real and reactive power from node i to node j
- $S_{ij} = P_{ij} + \mathbf{j}Q_{ij}$ - complex power flowing on line $(i, j) \in \mathcal{E}$



Power flow and operational constraints

- Generated power: $sg_i = pg_i + jqg_i$
- Consumed power: $sc_i = pc_i + jqc_i$
- Power flow

$$P_{ij} = \sum_{k:j\to k} P_{jk} + pc_j - pg_j + r_{ij}\ell_{ij}$$

$$Q_{ij} = \sum_{k:j\to k} Q_{jk} + qc_j - qg_j + x_{ij}\ell_{ij}$$

$$\nu_j = \nu_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij}) + (r_{ij}^2 + x_{ij}^2)\ell_{ij}$$

$$\ell_{ij} = \frac{P_{ij}^2 + Q_{ij}^2}{\nu_i}$$

- Voltage limits

$$\underline{\nu}_i \leq \nu_i \leq \overline{\nu}_i$$

- Maximum injected power

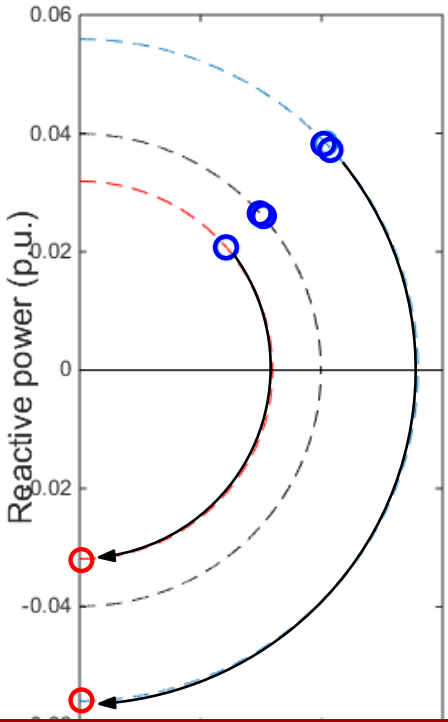
$$-\sqrt{\overline{sg}_i^2 - (pg_i)^2} \leq qg_i \leq \sqrt{\overline{sg}_i^2 - (pg_i)^2}$$

Attacker model

Attacker strategy: $\psi = (\delta, \widetilde{pg}^a, \widetilde{qg}^a)$

- δ is a vector, with elements $\delta_i = 1$ if DER i is compromised and zero otherwise;
- $\widetilde{pg}^a$: Active power set-points induced by the attacker;
- $\widetilde{qg}^a$: Reactive power set-points induced by the attacker.
- Satisfy resource constraint $\sum_{i=1}^{n} \delta_i \leq M$

  M: attacker's budget.



Change on set-points due to the attack

Power injected by each DER constrained by:

$$-\sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^a)^2} \leq \widetilde{qg}_i^a \leq \sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^a)^2}$$

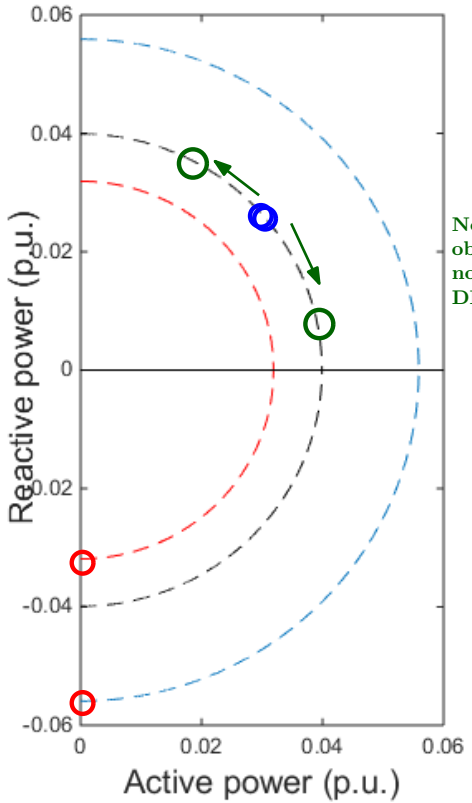
Attacker's impact with no defender response

- Scenario: Attacker introduces incorrect set-points $\widetilde{sg}^a$ that lead voltage below (or above) the permitted thresholds.
- DER Interconnection guidelines would mandate disconnections of other non-compromised DERs.
- This could cause disconnection of DERs or load-shedding which, if uncontrolled, may result in failures in other DNs.

Defender model

Defender response: $\phi = (\gamma, \widetilde{pg}^d, \widetilde{qg}^d)$

- $\gamma \in [0, 1]$ the portion of controlled loads;
- $\widetilde{pg}^d$: New active power set-points set by defender;
- $\widetilde{qg}^d$: New reactive power set-points set by the defender.



New set-points are obtained for the noncompromised DERs.

$$pc_i = \gamma_i pc_i^{\mathrm{d}}, \quad qc_i = \gamma_i qc_i^{\mathrm{d}}$$

Power injected by each DER constrained by:

$$-\sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^d)^2} \leq \widetilde{qg}_i^d \leq \sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^d)^2}$$

Final PV output

$pg_i = \delta_i \widetilde{pg}_i^a + (1 - \delta_i)\widetilde{pg}_i^d$

$qg_i = \delta_i \widetilde{qg}_i^a + (1 - \delta_i)\widetilde{qg}_i^d$

How to choose the defender response (set-points)?

Losses

- Loss of voltage regulation

$$\mathcal{L}_{\text{LOVR}} \equiv \max_{i \in \mathcal{N}_0} W_i(\underline{\nu}_i - \nu_i)_+$$

- Cost incurred due to load control

$$\mathcal{L}_{\text{VOLL}} \equiv \sum_{i \in \mathcal{N}_0} C_i(1 - \gamma_i)$$

Composite loss function

$$\mathcal{L}(\psi, \phi) = \mathcal{L}_{\text{LOVR}} + \mathcal{L}_{\text{VOLL}}$$

Problem statement

Find attacker's interdiction plan to maximize composite loss $L(\psi, \phi)$, given that defender optimally responds

$$\max_{\psi} \quad \min_{\phi} \quad \left(\max_{i \in \mathcal{N}_0} W_i(\underline{\nu}_i - \nu_i)_+ + \sum_{i \in \mathcal{N}_0} C_i(1 - \gamma_i) \right)$$

s.t. Power flow, DER constraints and resource contraints

$$\phi = (\gamma, \widetilde{pg}^d, \widetilde{qg}^d)$$

$$\psi = (\delta, \widetilde{pg}^a, \widetilde{qg}^a)$$

$$\delta \in \{0,1\}^N, \gamma \in \prod_{i \in \mathcal{N}_0} [\underline{\gamma}_i, 1]$$

This bilevel-problem is hard!

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

Outline

Bilevel Network Interdiction Problem

$$
\begin{aligned}
\text{[ADLP1]} \quad z_1^* &= \min_{\mathbf{x}\in X} z_1(\mathbf{x}), \text{where} \\
z_1(\mathbf{x}) &\equiv \max_{\mathbf{y}} \ \mathbf{c}^T\mathbf{y} \\
&\text{s.t.} \ \ A\mathbf{y} \le b \\
&\qquad 0 \le \mathbf{y} \le U(\mathbf{1}-\mathbf{x}). \\
\text{[ADLP2]} \quad z_2^* &= \min_{\mathbf{x}\in X} z_2(\mathbf{x}), \text{where} \\
z_2(\mathbf{x}) &\equiv \max_{\mathbf{y}} \ (\mathbf{c}^T - \mathbf{x}^T\overline{R})\mathbf{y} \\
&\text{s.t.} \ \ A\mathbf{y} \le b \\
&\qquad 0 \le \mathbf{y} \le U(\mathbf{1}-\mathbf{x})
\end{aligned}
$$

where $\overline{R} = \text{diag}(\bar{\mathbf{r}})$, $\bar{\mathbf{r}} = (\bar{\mathbf{r}}_1 \ldots \bar{\mathbf{r}}_n)^T$ and $\bar{\mathbf{r}}_k$ is an upper bound to the optimal dual variable for the constraint $y_k \le u_k(1 - x_k)$.

- Can be solved using Bender's decomposition

Simple case

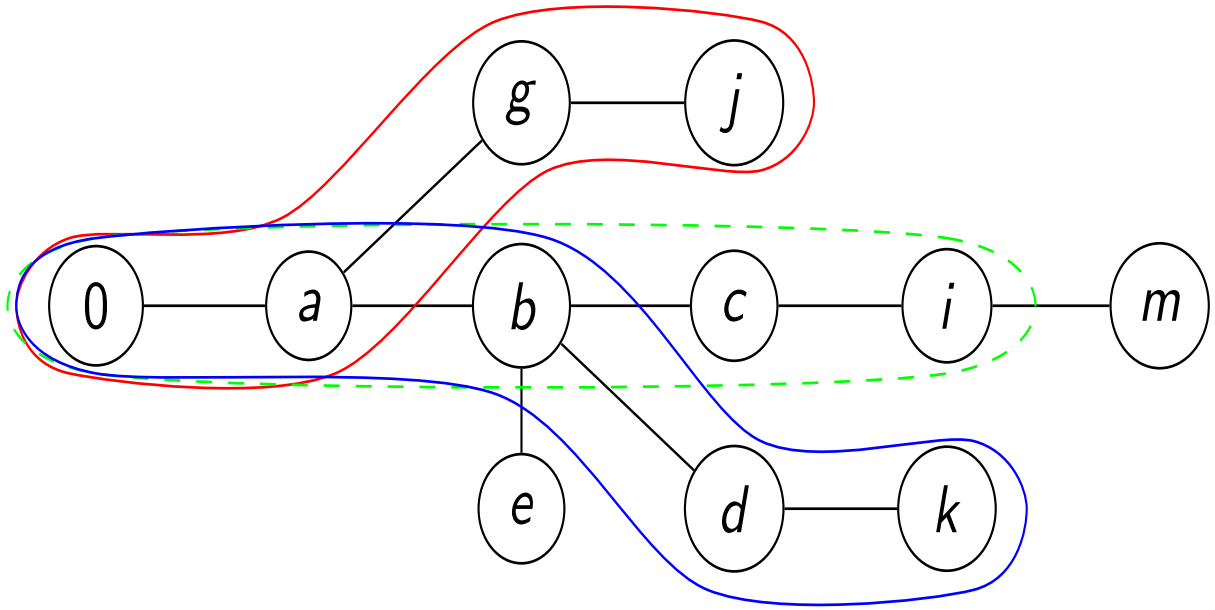
For a fixed defender choice and ignoring loss of freq. regulation:

$$\max_{\delta} \quad \left(\max_{i \in \mathcal{N}_0} W_i (\underline{\nu}_i - \nu_i)_+ \right)$$

s.t. Power flow, DER constraints, and resource contraints

Results for this simple case also extend to the case when R/X ratio is homogeneous and defender responds with only DER control.

Precedence description



In the above figure

- $j \prec_i k$: Node j is before node k with respect to node i
- $e =_i k$: Node e is at the same level as node k with respect to node i
- $b \prec k$: Node b is before node k because of b is ancestor of k

Optimal interdiction plan

Theorem

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

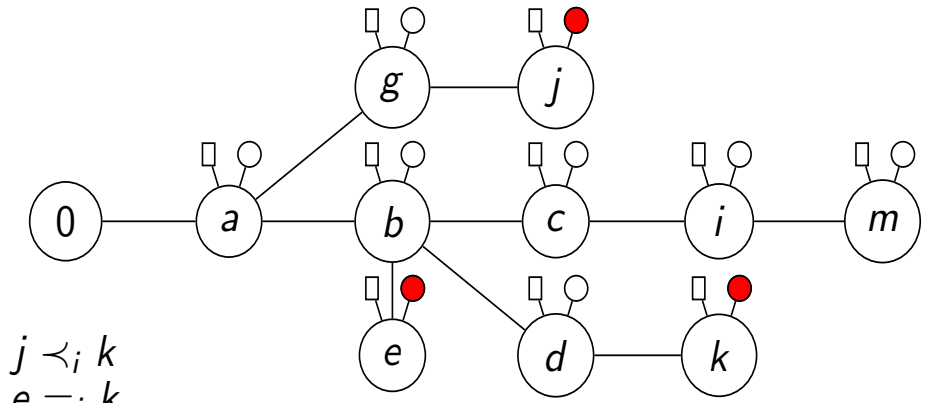
- If DGs at j, k are homogenous and j is before k w.r.t. i, then DG disruption at k will have larger effect on ν_i at i (relative to disruption at node j);
- If DGs at j, k are homogenous and j is at the same level as k w.r.t. i, then DG disruptions at j and k will have the same effect on ν_i at i;

Let ν_i^{old}/ν_i^{new} be $|V_i|^2$ before/after the attack

$\Delta(\nu_i) = \nu_i^{old} - \nu_i^{new}$

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

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



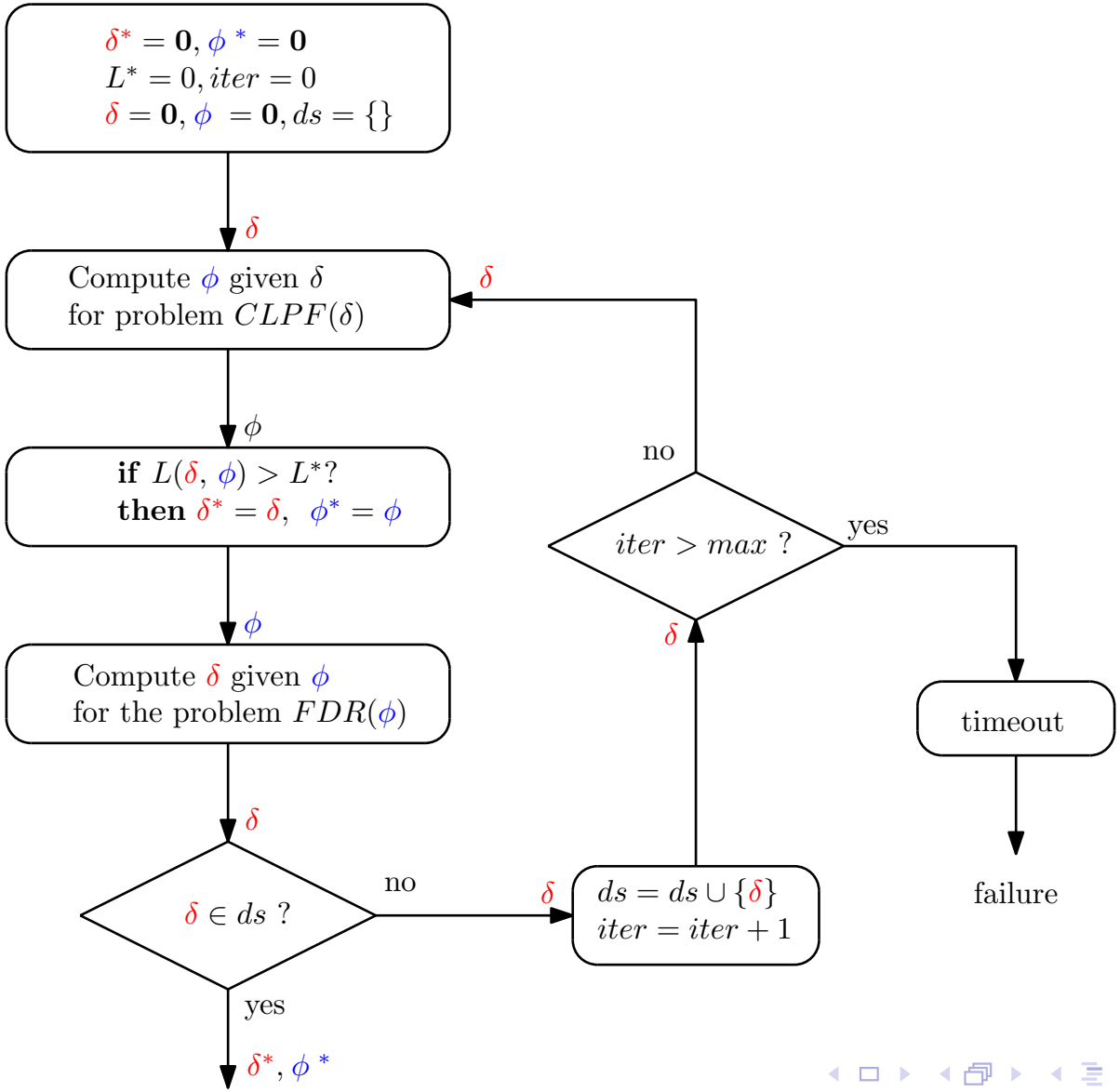
$j \prec_i k$
$e =_i k$
$b \prec k$

Computing optimal attack: fixed defender choices

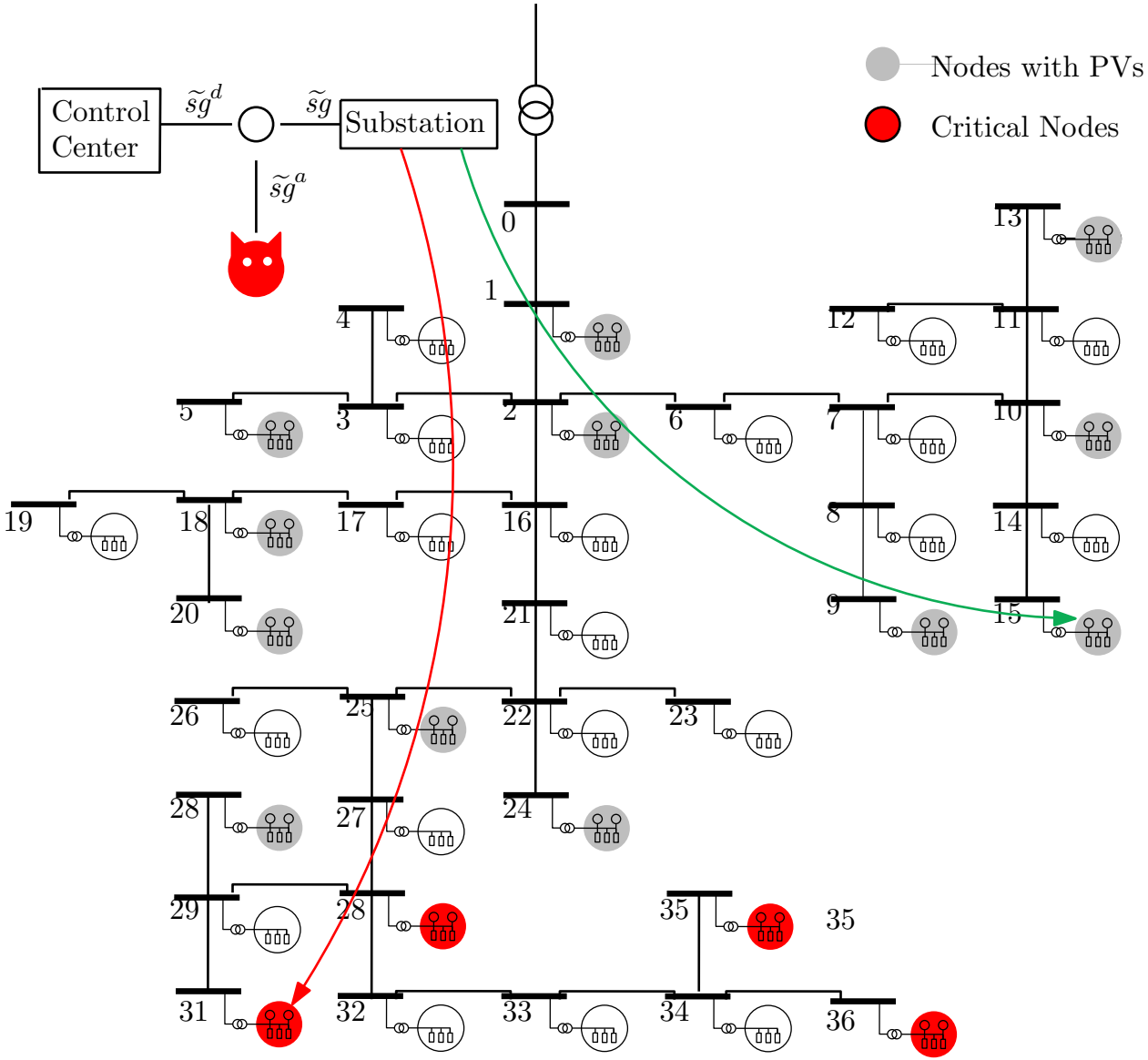
1: **procedure** OPTIMALATTACKFORFIXEDRESPONSE
2: **for** $i \in \mathcal{N}_0$ **do**
3: **for** $j \in \mathcal{N}_0$ **do**
4: Compute $\Delta_j(\nu_i)$
5: **end for**
6: Sort js in decreasing order of $\Delta_j(\nu_i)$ values
7: Compute J_i^* by picking js corresponding to top M $\Delta_j(\nu_i)$ values.
8: **end for**
9: $k := W_i \arg\min_{i \in \mathcal{N}_0} \quad \nu_i - \Delta_{J_i^*}(\nu_i)$
10: **return** $J^* := J_k^*$ (Pick J_i^* which violates voltage constraint the most)
11: **end procedure**

- $\mathcal{O}(n^2 log\ n)$

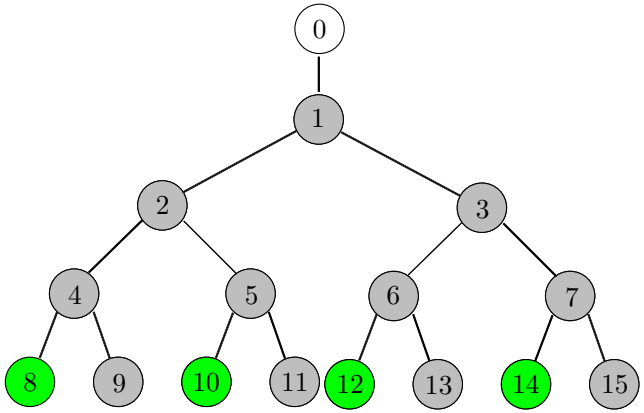
Greedy algorithm for optimal attack: defender response



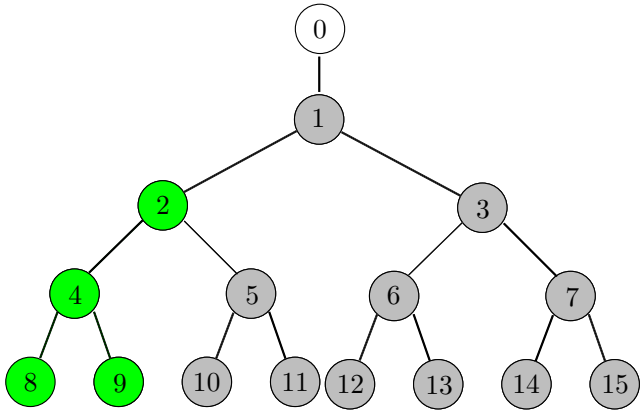
IEEE 37-node network



Secure network designs: which DERs to secure?



Design 1



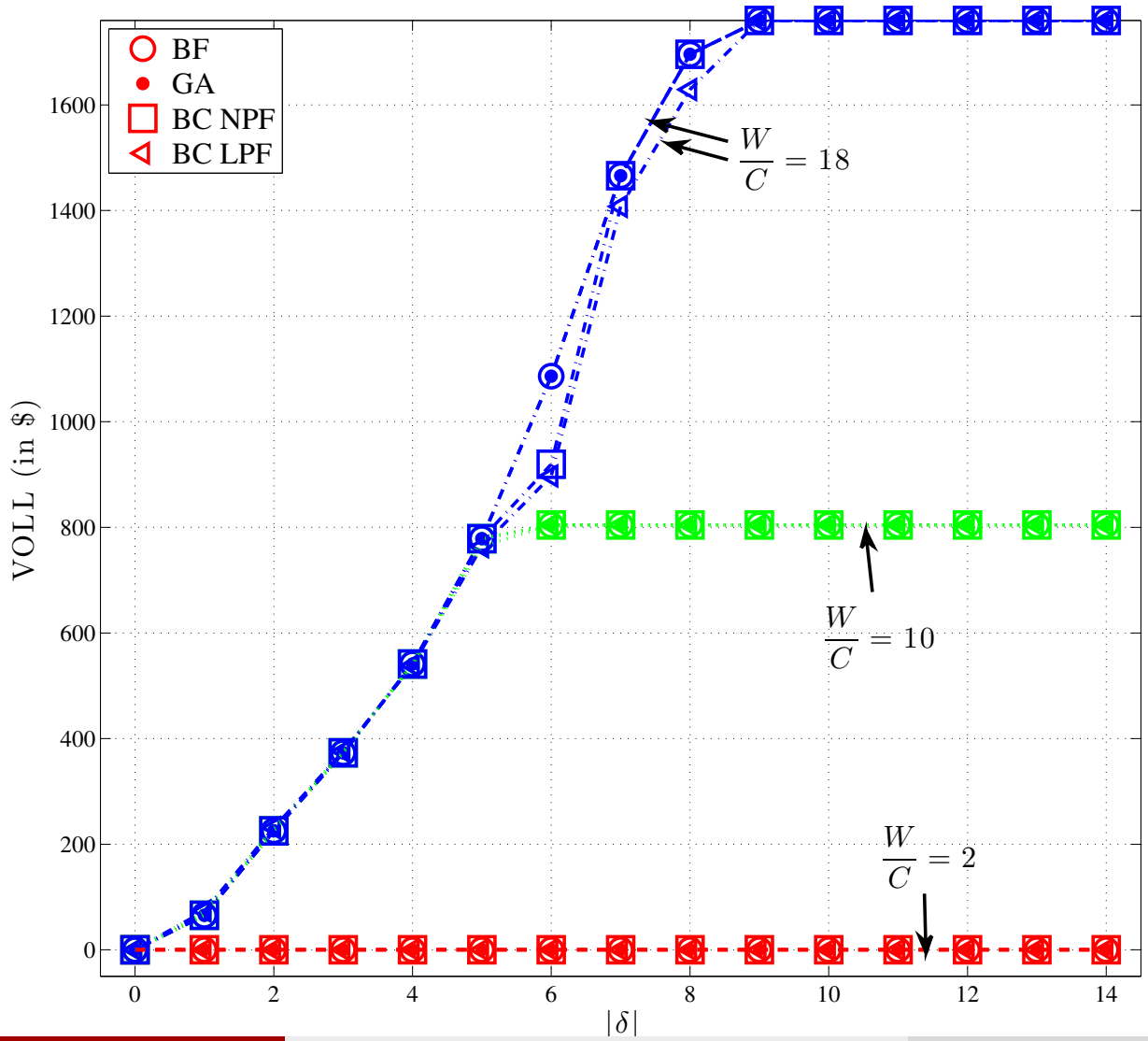
Design 2

Consider a DN with balanced tree topology, homogeneous R/X ratio, and homogenous nodes. In an optimally secure design:

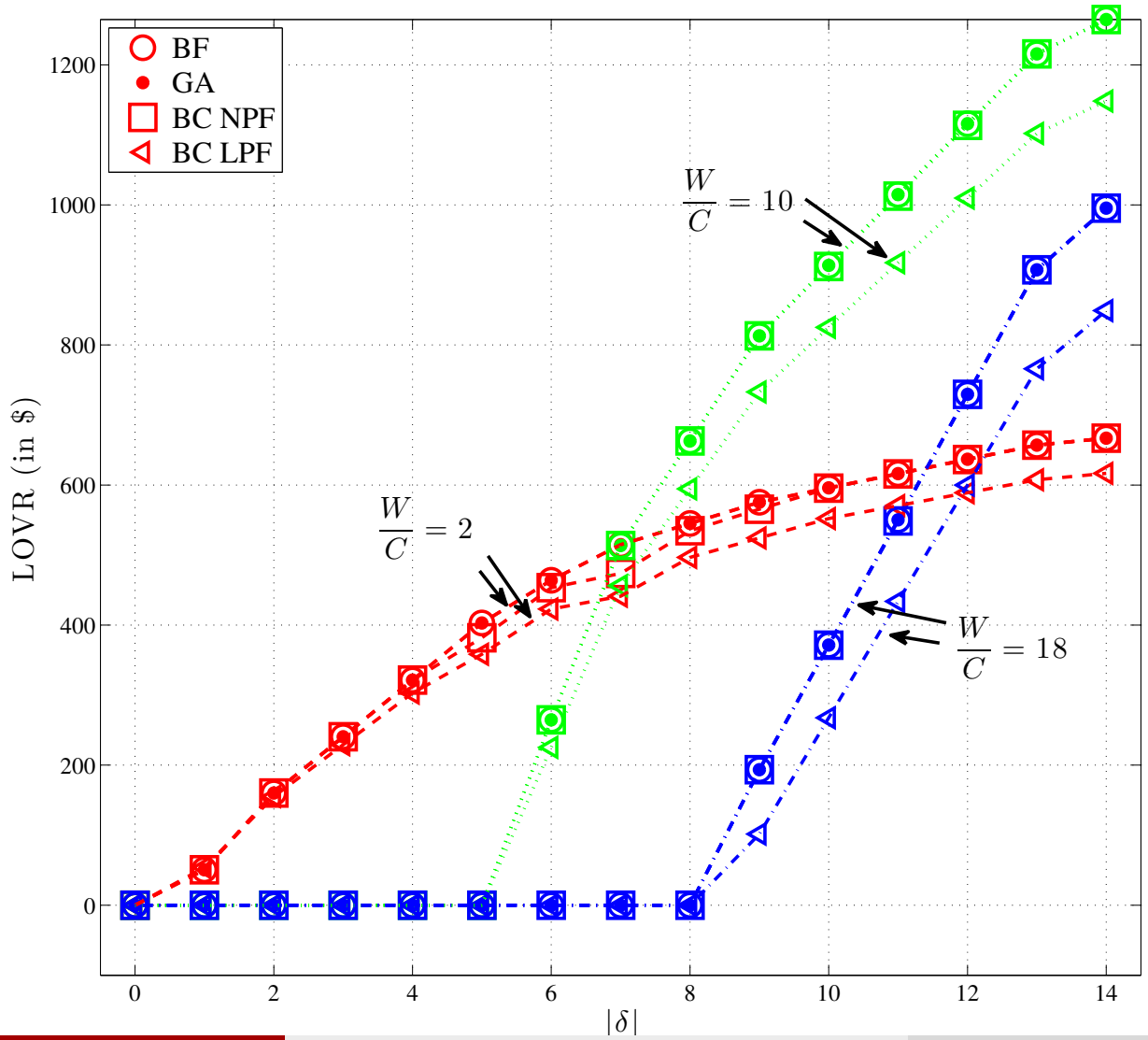
- If any node is secure, all its child nodes must also be secure;
- There exists at most one intermediate level (depth) that contains both vulnerable and secure nodes;
- In this intermediate level, the secure nodes are "uniformly distributed".

Outline

Results: VOLL vs $|\delta|$, $\underline{\gamma} = 0.5$



Results: LOVR vs $|\delta|$, $\underline{\gamma} = 0.5$



Results: Homogeneous Network

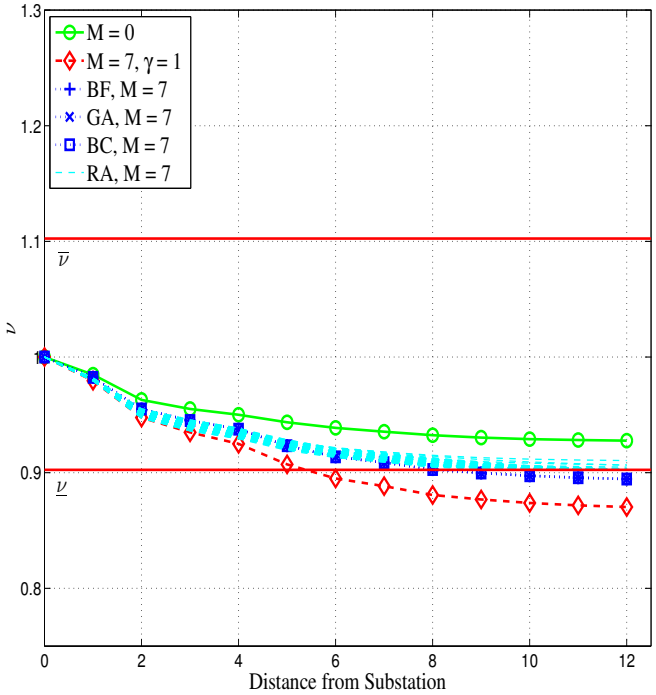


Figure : ν vs Distance from Substation

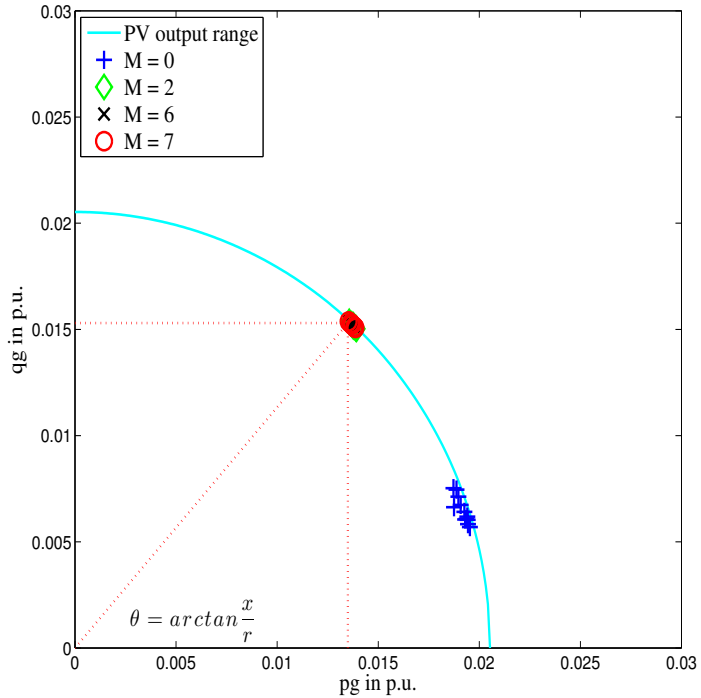


Figure : Reactive Power vs Real Power Output of PVs

Results: Homogeneous vs Heterogeneous Network

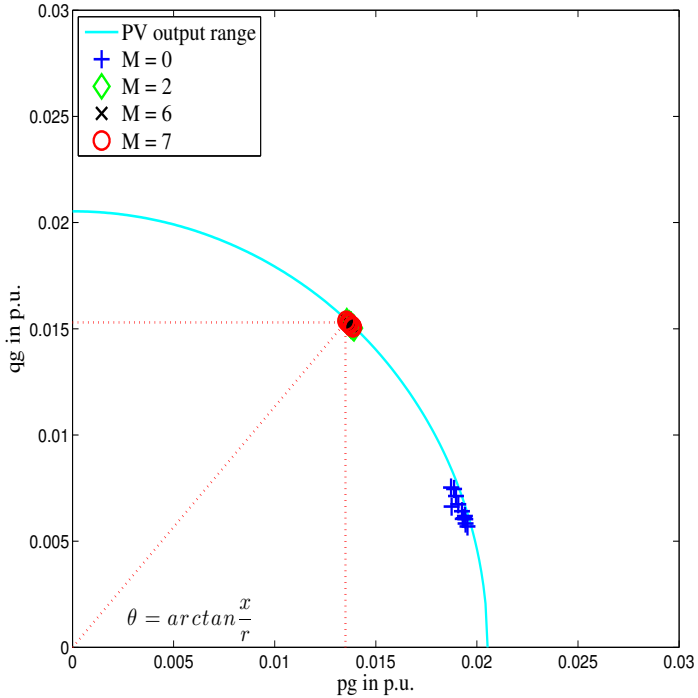


Figure : ν vs Distance from Substation

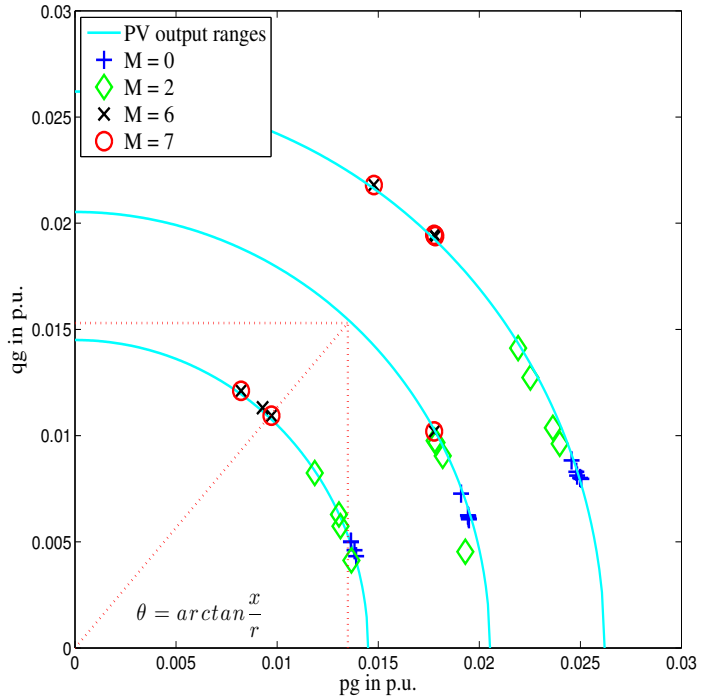


Figure : Reactive Power vs Real Power Output of PVs

Main insights

- Results using greedy algorithm compare very well with results from (more computationally intensive) brute force and Bender's cut;
- Optimal attack plans with defender response (using both DER control and load control) show downstream preference;
- When cost of load control is high (resp. low), defender permits (resp. does not permit) increase in cost due to LOVR;
- For small # of compromised DERs, load control is preferred over LOVR;
- Beyond a certain attack intensity, load control is not effective and attacker starts targeting upstream nodes (and their voltage bounds).

Vulnerability analysis & control of distribution networks

Questions

- How to assess vulnerability of electricity networks to disruptions of Distributed Energy Resources (DERs)?
- What is the optimal attacker interdiction plan?

Approach

Attacker-defender model; Network interdiction formulation; Characterization of worst-case attacks; Defender strategies

Results

- Interdiction model captures threats to DERs / smart inverters;
- Structural results on worst case attacks that maximize weighted sum of cost due to loss of voltage regulation and cost of load control;
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints;