FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Distributed Control of Electricity Distribution Networks in the face of DER disruptions

Devendra Shelar and Saurabh Amin
Departments of Civil and Environmental Engineering
MIT

FORCES Research Exchange & Advisory Board Meeting, May 2015

Berkeley University of California
Massachusetts Institute of Technology
NSF
Michigan
Vanderbilt University

Outline

1. Motivation and Focus
2. Vulnerability analysis & centralized control under DER disruptions
3. A distributed control strategy

Vulnerability analysis & control of distribution networks

Questions

- How to assess vulnerability of electricity networks to disruptions of Distributed Energy Resources (DERs)?
- How to design decentralized defender (network operator) strategies?

Approach

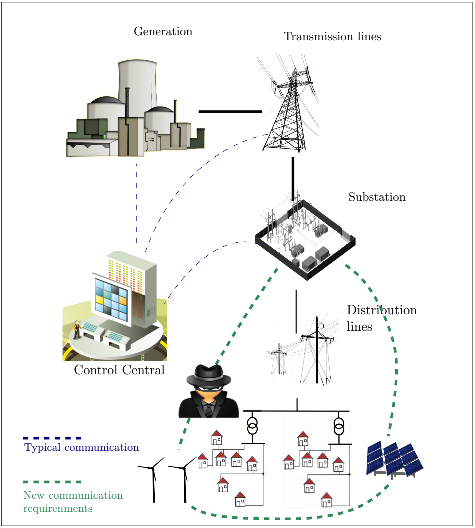
Attacker-defender model; Network interdiction formulation;
Characterization of worst-case attacks; Defender strategies

Results (*ACC'15, CDC'15 (under review), IEEE TNCS (TBS)*)

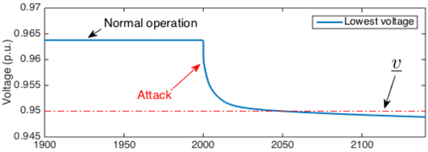
- Interdiction model captures threats to DERs / smart inverters;
- Structural results on worst case attacks that maximize voltage deviations and / or frequency deviation from nominal operation;
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints;
- <u>Ongoing:</u> Distributed defender control strategy (uses measurements and knowledge of worst affected node).

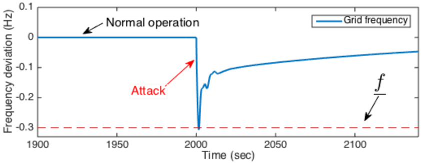
Main idea: Model of DER disruptions

Vulnerability: Control Center and Substation communications

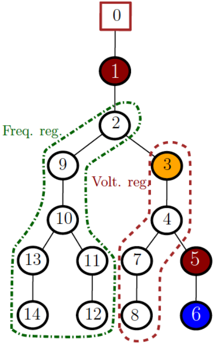


- Hack substation communications
- Introduce incorrect set-points and disrupt DERs
- Create supply-demand mismatch
- Cause voltage & freq. violations
- Induce cascading failures





Main idea: Decentralized defender response

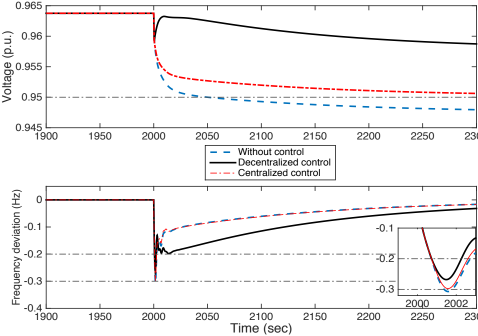


Attacker-Defender interaction

- Attacker: disrupt DERs at 1, 5, 6
- Critical node 3 partitions network:
  - Subnet 1: control frequency
  - Subnet 2: regulate voltage.
- Defender: New set-points

Approach

- Resource-constrained attacker: loss of voltage & freq. regulation
- Worst-case attacks (maximin)
- Compute defender response (Distributed control)



Outline

1. Motivation and Focus
2. Vulnerability analysis & centralized control under DER disruptions
3. A distributed control strategy

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), loss of frequency regulation (LOFR), 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 and LOFR 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
- Alejandro D. Dominguez-Garcia: Distributed control, reliability

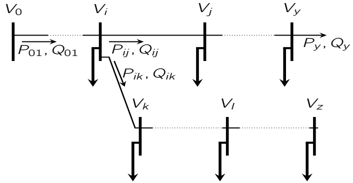
Resilience and security of networked systems

- Ross Baldick, Kevin Wood: Interdiction for transmission networks
- Daniel Bienstock, *et al.*: Cascading failures with linear power flow
- Tamer Başar, Cedric Langbort: Network security games:
- Henrik Sandberg, Kalle Johansson: Metrics, false-data injection
- 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

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

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

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

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

- Voltage & frequency limits

$$\underline{\nu}_i \le \nu_i \le \bar{\nu}_i \quad \text{and} \quad \underline{f} \le f \le \bar{f}$$

- Maximum injected power

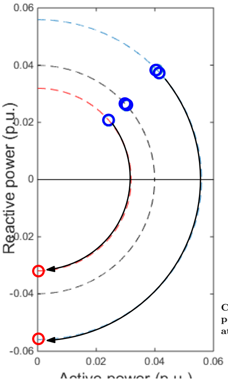
$$-\sqrt{\overline{sg}_i^2 - (pg_i)^2} \le qg_i \le \sqrt{\overline{sg}_i^2 - (pg_i)^2}$$

Attacker model

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

- 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.



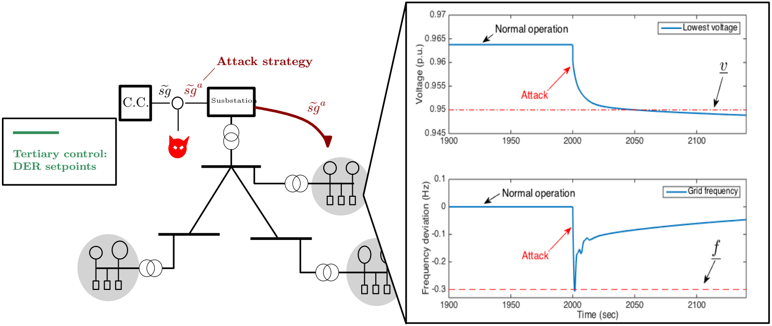
Change on set-points due to the attack

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 $\tilde{sg}^a$ that lead voltage and frequency below (or above) the permitted thresholds.

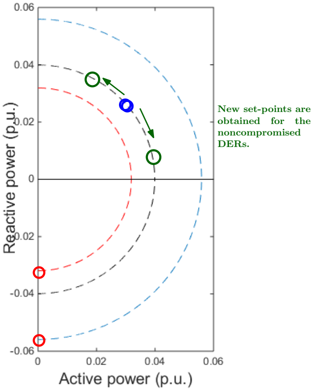


This could cause disconnection of DERs or load-shedding which, if uncontrolled, may result in failures in other DNs.

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.



Power injected by each DER constrained by:

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

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

Losses

- Loss of voltage regulation

$$L_{\mathrm{LOVR}} \equiv \max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+$$

- Loss of frequency regulation

$$L_{LOFR} \equiv \tilde{w}(\underline{f}_{dev} - f_{dev})_+$$

- Cost incurred due to load control

$$L_{\mathrm{LL}} \equiv \sum_{i \in \mathcal{N}_0} C_i (1 - \gamma_i)$$

Composite loss function

$$L(\psi, \phi) = L_{\mathrm{LOVR}} + L_{LOFR} + L_{\mathrm{LL}}$$

Problem statement

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

$$\max_{\psi} \quad \min_{\phi} \quad \left(\max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+ + \sum_{i \in \mathcal{N}_0} C_i (1 - \gamma_i) + \tilde{w} (\underline{f}_{dev} - f_{dev})_+ \right)$$
$$\text{s.t. Power flow, DER constraints, and resource contraints}$$

This bilevel-problem is hard!

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

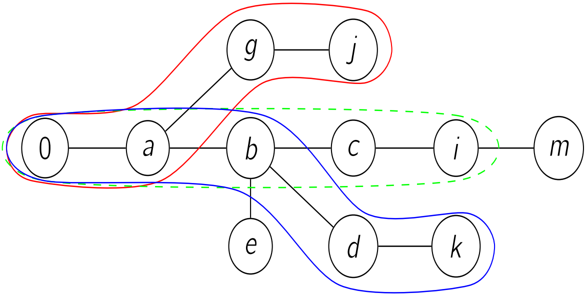
Simple case

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

$$\max_{\delta} \quad \left(\max_{i \in \mathcal{N}_0} w_i(\underline{\nu}_i - \nu_i)_+ \right)$$
$$\text{s.t. Power flow, DER constraints, and resource contraints}$$

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

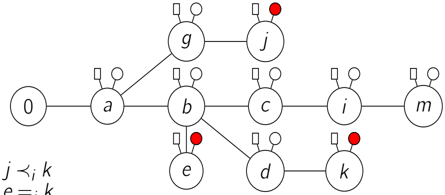
For a tree network, given nodes i (pivot), $j, k \in \mathcal{N}_0$:

- 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

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

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



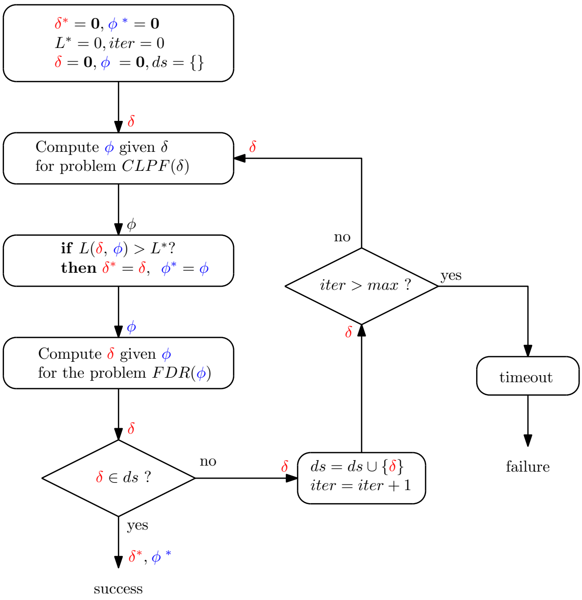
$j \prec_i k$
$e =_i k$
$b \prec k$

Computing optimal attack: fixed defender choices

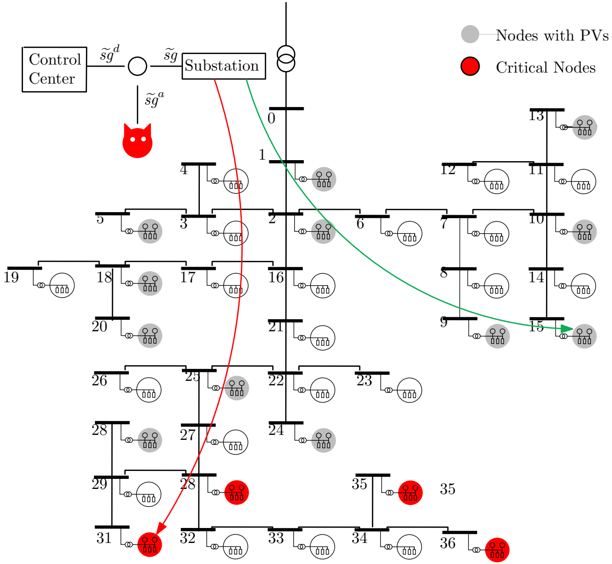
procedure Optimal Attack Plan
  for $i \in \mathcal{N}_0$ **do**
    for $j \in \mathcal{N}_0$ **do**
      Compute $\Delta_j(\nu_i)$
    end for
    Sort js in decreasing order of $\Delta_j(\nu_i)$ values
    Compute J_i^* by picking js corresponding to top M $\Delta_j(\nu_i)$ values.
  end for
  $k := w_i \arg\min_{i \in \mathcal{N}_0} \nu_i - \Delta_{J_i^*}(\nu_i)$
  return $J^* := J_k^*$ (Pick J_i^* which violates voltage constraint the most)
end procedure

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

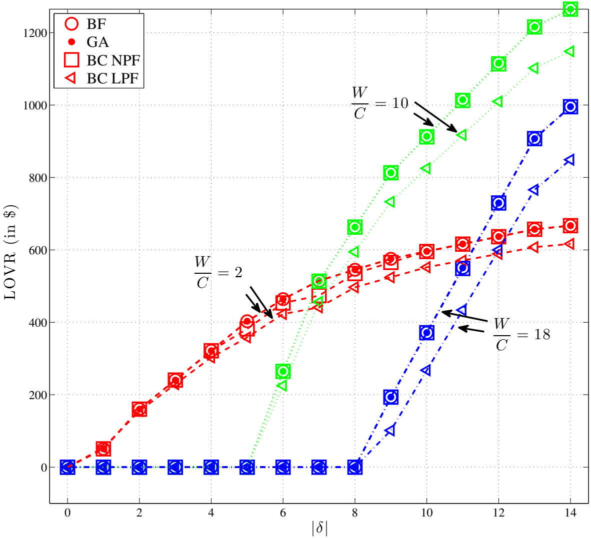
Greedy algorithm for optimal attack: defender response



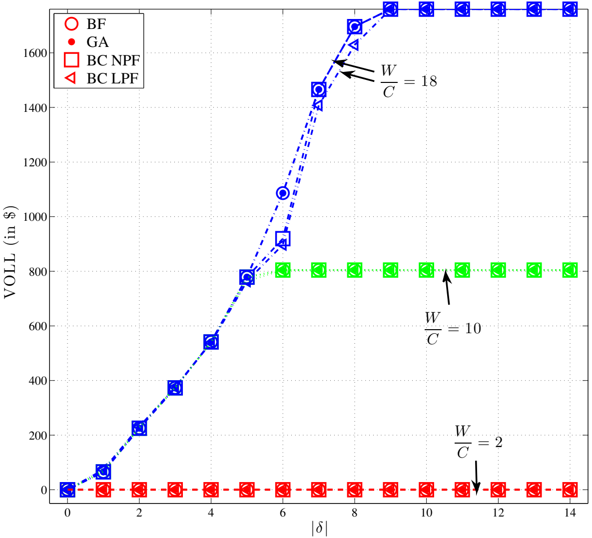
IEEE 37-node network



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

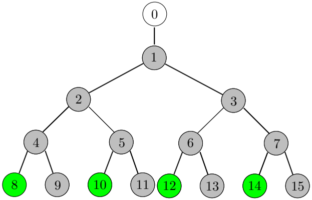


Results: VOLL vs δ, $\quad \underline{\gamma} = 0.5$

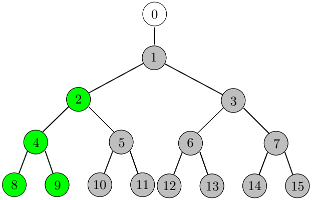


Main insights

- 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).



Design 1



Design 2

Theorem

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

1. Motivation and Focus
2. Vulnerability analysis & centralized control under DER disruptions
3. A distributed control strategy

Why decentralized control?

Desirable properties of defender response:

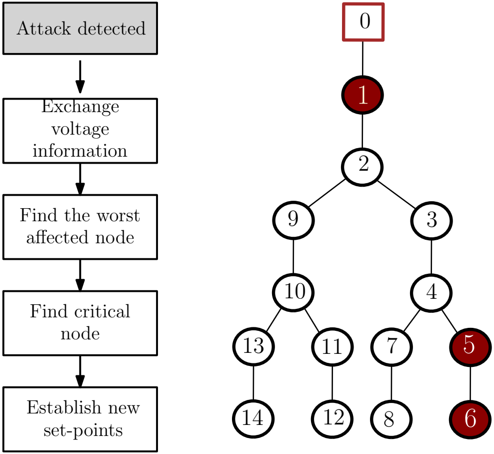
1. **Security**: Centralized control strategy undesirable since CC-SS communications are compromised in our attack model;
2. **Compensation to owners**: Upstream DERs likely to be owned by distribution utilities $\Rightarrow \uparrow$ costs when set-points change for larger DERs (esp. $\downarrow$ real power production)
3. **Flexibility**: Topology of DNs might be variable across time: configuration of worst affected nodes may also change.

We design a decentralized control strategy and find new set-points for non-compromised nodes using

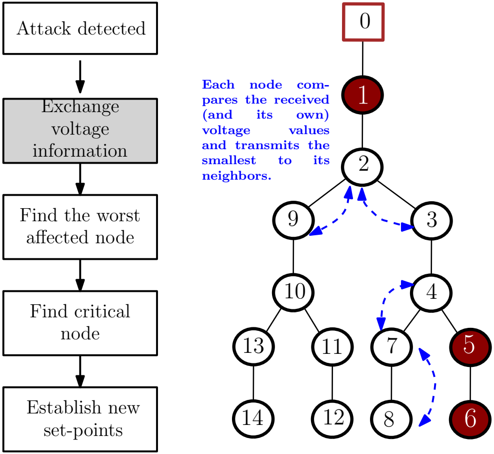
- Information: local measurements (voltage & freq.) and location of the node with lowest voltage;
- Diversification: each node contributes either to voltage or to frequency regulation.

Joint work with D. Shelar and J. Giraldo.

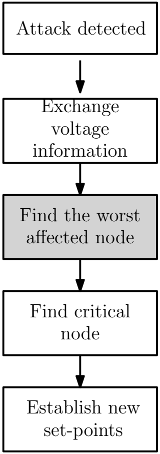
Distributed control strategy



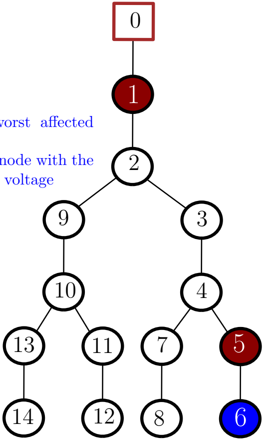
Distributed Control Strategy



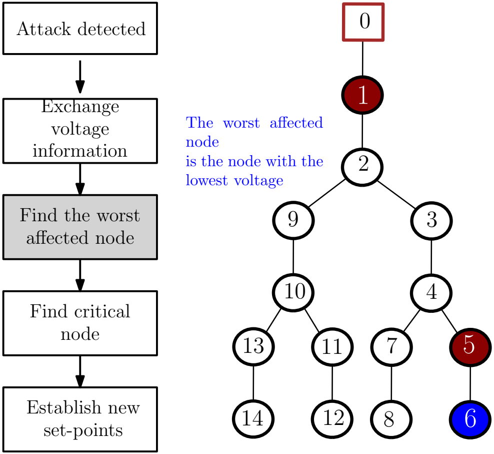
Distributed control strategy



The worst affected node
is the node with the
lowest voltage

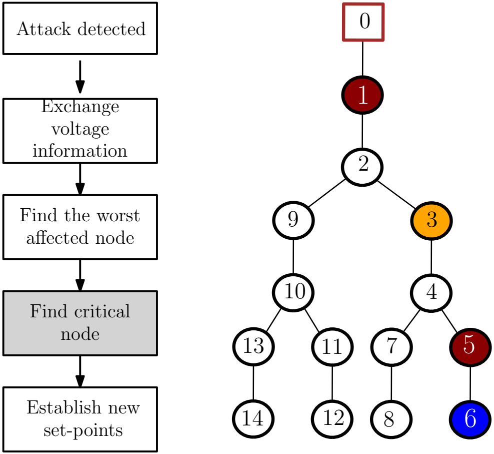


Distributed control strategy



Key assumption: The location of the worst-node t does not change before and after the defender response.

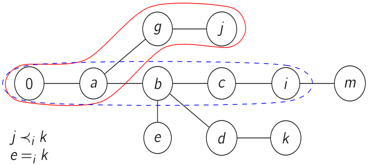
Decentralized Control Strategy



It is the node that partitions the graph into two disjoints subsets $\mathcal{N}_f, \mathcal{N}_v$ of $\mathcal{N}_0$. $j \in \mathcal{N}_f$ contribute to frequency regulation and $j \in \mathcal{N}_v$ to voltage regulation.

Distributed control strategy

Finding the critical node



$j \prec_i k$
$e =_i k$
$b \prec k$
$\mathcal{P}_j = \{(0,a),(a,g),(g,j)\}$
$\mathcal{P}_i \cap \mathcal{P}_j = \{(0,a)\}$

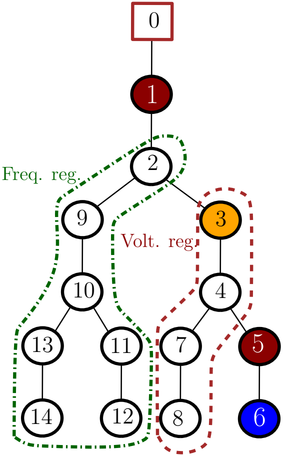
Theorem

Let t be a worst affected node and let $n_{jt} = |\mathcal{P}_j \cap \mathcal{P}_t|$ denote the number of edges on the intersection of the paths $\mathcal{P}_j, \mathcal{P}_t$.

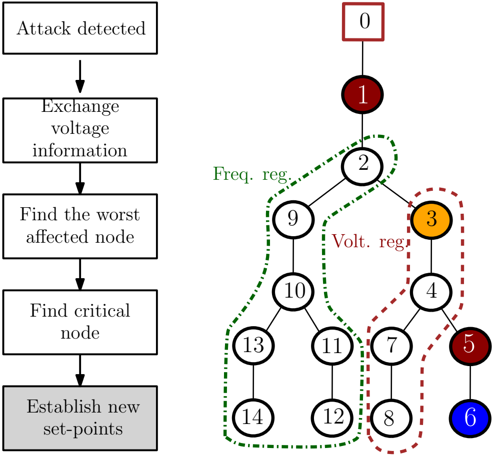
- There exists a level n^*, s.t. the critical node $\tau = \arg \min_{n_{jt} \geq n^*} |\mathcal{P}_j|$ partitions the graph into two disjoints subsets $\mathcal{N}_f, \mathcal{N}_v$ of $\mathcal{N}_0$.
- All nodes $j \in \mathcal{N}_f$ contribute to frequency regulation and all nodes $k \in \mathcal{N}_v$ to voltage regulation.

Distributed control strategy

1. Attack detected
2. Exchange voltage information
3. Find the worst affected node
4. Find critical node
5. Establish new set-points



Distributed control strategy



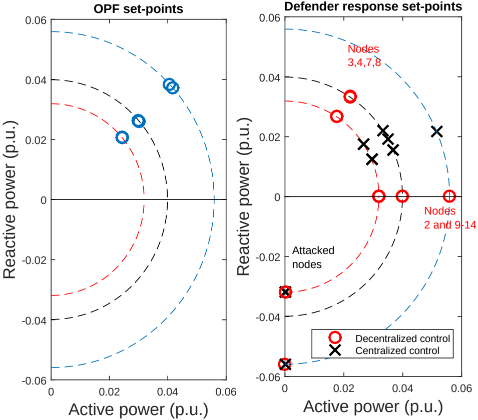
Frequency regulation

$$\widetilde{pg}_i^d = \overline{sg}_i, \widetilde{qg}_i^d = 0.$$

Voltage regulation

$$\widetilde{pg}_i^d = \frac{r\overline{sg}_i}{\sqrt{r^2+x^2}},$$
$$\widetilde{qg}_i^d = \frac{x\overline{sg}_i}{\sqrt{r^2+x^2}}.$$

Using the proposed decentralized strategy for the aforementioned example, we find the set of nodes that contribute to frequency and voltage regulation. The critical node is 3 and worst affected node is 6.



Vulnerability analysis & control of distribution networks

Questions

- How to assess vulnerability of electricity networks to disruptions of Distributed Energy Resources (DERs)?
- How to design decentralized defender (network operator) strategies?

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 voltage deviations and / or frequency deviation from nominal operation;
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints;
- Ongoing: Distributed defender control strategy (uses measurements and knowledge of worst affected node).