Towards Improving the Resilience of Power Systems

Devendra Shelar | shelard@mit.edu
August 30, 2018

Collaborators: Saurabh Amin, Ian Hiskens
Research Focus

- Smart grid resilience
- Algorithms for bilevel optimization problems
- Modeling of cyberphysical failures
Outline

• Motivation: Resilience-Aware operations

• Attack models and Problem formulation

• Main results
Cyber-Physical disruptions

Hurricane Maria (September 2017)
• Customers facing blackouts for months

Metcalf Substation (April 2013)
• Sniper attack on 17 transformers
• Telecommunication cables cut
• 15 million $ worth of damage
• 100 mn $ for security upgrades

Ukraine attack (Dec ‘15, ‘16)
• First ever blackouts caused by hackers
• Controllers damaged for months
Research challenge

Existing literature considers:
  • Physical security of transmission networks
  • DC powerflow models

Limited focus on:
  • Smart Distribution networks (DNs)
  • Optimal attacker/defender strategies based on:
    • Network topology
    • Tradeoffs in resource allocation

My approach combines:
  • Physics-based optimal attack
  • Semantics-aware software memory attack
Distribution network attack scenarios

- **Agent**
  - Disgruntled employee
  - External hacker
  - Buggy SCADA implementation

- **NESCO Vulnerabilities (EPRI)**
  - Mass remote disconnect of smart meters
  - Simultaneous disconnect of DERs
  - Rapid overcharging of electric vehicles

- **Impact:** *supply-demand disturbances* (sudden or prolonged)
Background: Security-constrained OPF

- **Economic Dispatch** problem to ensure an operational power system despite contingencies
- Accounts for **appropriate corrective actions** for the said contingency

Main issues
- Only captures N-k contingencies for small k. Typically k = 1 or 2
- Assumes a priori fixed set of contingencies
- Does not model strategic attacker-induced failures

J. A. Momoh, et al. - "A review of selected optimal power flow literature to 1993. II. Newton, linear programming and interior point methods"
Our formulation: Resilience-Aware OPF

Stage I
Minimize $C_{\text{allocation}}$
Over all allocations

Stage II
Maximize
Over all disruptions

Stage III
Minimize $C_{\text{post-contingency}}$
Over all responses

Subject to
• Network constraints
• Component constraints
• Voltage constraints
Resilience-Aware OPF (3-Stages)

Pre-contingency state

\[
\min_{a \in \mathcal{A}} C_{alloc}(a) + \max_{d \in \mathcal{D}, u \in \mathcal{U}} \min L(a, d, u)
\]

Worst-case post-contingency state

Subject to

• Network constraints
• Component constraints
• Voltage constraints

RAOPF (Stages II and III)
A specific attack scenario

**Adversary:**
- Hack DER SCADA and disrupt DERs
- Create supply-demand disturbance
- Cause frequency and voltage violations
- Induce network failures (cascades)

![Diagram of a specific attack scenario involving Distributed Energy Resources (DERs) with incorrect commands.]
A 3-regime picture

Grid-connected regime
• Can absorb the impact of disturbances

Islanding mode regime
• Larger disturbances may force microgrid islanding

Cascade regime
• High severity voltage excursions, then more DER disconnects (cascades), more load shedding

When TN and DN level disturbances clear, the system can return to its nominal regime
Our approach

Most attacker-defender interactions can be modeled as
- Supply-demand imbalance induced by attacker
  - Control (reactive and proactive) by the system operator

- Abstraction: Bilevel (or multilevel) optimization problems

- Supplements simulation based approaches
  - For example, co-simulation of cyber and power simulators
Resilience-aware OPF (Stages II and III)

Stage II - Adversarial node disruptions
a. Which nodes to compromise ($\delta$)?

... can include other attack models

Stage III - Optimal dispatch / response ($x^c$)
a. Exercise load control or not
b. Disconnects loads/DGs?
c. Maintain voltage regulation

... possible to consider frequency regulation

Goals:
1. Identify critical nodes
2. Determine optimal response
Modeling of Grid-connected/Cascade regimes

\[ \max_{d \in \mathcal{D}} \min_{u \in \mathcal{U}} L(d, u) \]

Subject to

- Network constraints
- Component constraints
- Voltage constraints
\[ G = (\mathcal{N}, \mathcal{E}) \]

Network model

\[ P_{ij} + jQ_{ij} \]

**Power flow**

\[ r_{ij} + jx_{ij} \]

**Impedance**

\[ P_{jk} + jQ_{jk} \]

\[ p_{c_k} + jq_{c_k} \]

**Nominal load**

\[ p_{g_l} + jq_{g_l} \]

**Actual generation**

\[ v_0 \]

\[ v_i \]

\[ v_j \]

\[ v_k \]

\[ v_l \]
Defender model in Grid-connected regime

• Defender response: only load control
• $u = \beta$

• $\beta_i \in [\beta_i, 1]$: load control parameter at node $i$

$$pc_i = \beta_i \bar{pc}_i, \quad qc_i = \beta_i \bar{qc}_i$$

Defender response:
How much load control should be exercised?
Losses in Grid-connected regime

\[ L_{\text{GC regime}} = W_{\text{AC}}P_0 + W_{\text{VR}}t + \sum_{i \in \mathcal{N}} W_{\text{LC}_i}(1 - \beta_i) \]

Where

\[ t \geq \max_{i \in \mathcal{N}} |v_0^{\text{nom}} - v_i| \]
Defender model in Cascade regime

Defender response: load control, connectivity control

\[ u = (\beta, kg, kc) \]

\[ kg_i = \begin{cases} 
1, & \text{if DG } i \text{ is disconnected} \\
0, & \text{otherwise.}
\end{cases} \]

\[ kc_i = \begin{cases} 
1, & \text{if load } i \text{ is disconnected} \\
0, & \text{otherwise.}
\end{cases} \]

Connectivity constraints are mixed-integer linear:

- Connected implies no violations
- Violation implies not connected

\[ kg_i = 0 \implies v_i \in [v_{gi}, \overline{v}_{gi}] \]

\[ v_i \notin [v_{gi}, \overline{v}_{gi}] \implies kg_i = 1 \]

Similarly for loads!

Defender response:
Which loads and DGs to disconnect?
Losses in Cascade regime

\[ L_{\text{CS regime}} \equiv L_{\text{GC regime}} \quad + \quad \text{Cost of load disconnection} \]

\[ \sum_{i \in N} W_{SD,i} kC_i \]
Attacker model

Attacker strategy: $d = (\delta, \Delta v_0)$

$$\delta_i = \begin{cases} 1, & \text{if node } i \text{ is attacked} \\ 0, & \text{otherwise} \end{cases}$$

Attacker’s resource budget

$$\sum_i \delta_i \leq k$$

- $\Delta v_0$: amount by which substation voltage drops
  - Due to physical disturbance or temporary fault in the TN

Attacker strategy:

- Which nodes to compromise?
Effect of attacker actions

• DER disruption makes its output zero.

\[ k g_i \geq \delta_i \]
\[ p g_i = (1 - k g_i) \bar{p} g_i \]
\[ q g_i = (1 - k g_i) \bar{q} g_i \]

• TN-side disturbance impacts substation voltage

\[ v_0 = v_0^{\text{nom}} - \Delta v_0 \]
Linear power flows

Power conservation

\[ P_{ij} = \sum_{k:j \rightarrow k} P_{jk} + pc_j - pg_j \]

\[ Q_{ij} = \sum_{k:j \rightarrow k} Q_{jk} + qc_j - qg_j \]

Voltage drop

\[ v_j = v_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij}) \]

\[ v_0 = v_0^{\text{nom}} - \Delta v \]

System state

\[ x = (pc, qc, pg, qg, v) \]
Cascade regime

\[ L := \max_{d \in D} \min_{u \in U} L^{\text{CS regime}}(d, u) \]

Subject to

- Network constraints
- Component constraints
- Voltage constraints

This is a mixed-integer bilevel linear program: NP-hard!
Islanding regime

\[
\max \min_{d \in \mathcal{D}, u \in \mathcal{U}} L_{\text{MI regime}}^{\text{MI regime}} (d, u)
\]

Subject to
- Network constraints
- Component constraints
- Voltage constraints

\[L_{\text{MI regime}} \equiv L_{\text{CS regime}} + \text{Cost of islanding}\]

\[
\sum_{(i,j) \in \chi} W_{\text{MG,ij}} km_{ij}
\]
System resilience

• $\mathcal{L}_{max} = \sum_{i \in N} W_{SD,i}$: maximum loss
  • Cost of disconnection of all loads

• System resilience
  • Percentage decrease in system performance relative to maximum loss
  • $= 100 \left( 1 - \frac{\mathcal{L}}{\mathcal{L}_{max}} \right)$
Benders Decomposition vs. Optimal

Grid-connected and Cascade regime

Grid-connected, cascade, and Islanding regime
Uncontrolled (multi-round) cascade

In reality, defender may not be able to instantaneously detect and identify attack, and optimally respond to it

No response cascade algorithm
• Initial contingency
• For $r = 1,2,...$
  • Compute power flows
  • Determine the nodes that violate the voltage bounds
  • Disconnect the loads or non-controllable DGs accordingly
Uncontrolled vs Cascade regime

N = 36
### Performance of Benders Decomposition

Res\textsubscript{Worst-case} = \left(1 - \frac{L}{L_{max}}\right) \times 100 \%

Entries are resilience metric of DN (in percentage), number of iterations (written in brackets), time (in seconds), attack cardinality.

<table>
<thead>
<tr>
<th>(R_{target})</th>
<th>N = 24</th>
<th>N = 36</th>
<th>N = 118</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>98.75, (3), 0.04, 1</td>
<td>98.96, (11), 0.22, 5</td>
<td>98.52, (27), 1.86, 14</td>
</tr>
<tr>
<td>95</td>
<td>91.15, (6), 0.08, 2</td>
<td>93.82, (13), 0.27, 6</td>
<td>94.66, (39), 3.34, 17</td>
</tr>
<tr>
<td>90</td>
<td>89.75, (10), 0.16, 3</td>
<td>88.08, (15), 0.34, 8</td>
<td>89.94, (50), 5.44, 26</td>
</tr>
<tr>
<td>85</td>
<td>82.41, (11), 0.18, 4</td>
<td>82.93, (17), 0.4, 10</td>
<td>84.96, (69), 9.23, 44</td>
</tr>
<tr>
<td>80</td>
<td>74.38, (14), 0.26, 5</td>
<td>76.99, (21), 0.52, 14</td>
<td>79.71, (86), 613.42, 52</td>
</tr>
<tr>
<td>75</td>
<td>74.38, (14), 0.26, 5</td>
<td>71.1, (23), 0.59, 16</td>
<td>Failure</td>
</tr>
<tr>
<td>65</td>
<td>58.01, (20), 0.41, 9</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>49.65, (23), 0.47, 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Failure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary (so far)

• Resource allocation and dispatch in electricity DNs
  • under strategic cyber-physical failures
  • Multi-regime defender response

• Benders decomposition approach for solving bilevel MILPs

• Structural results on worst-case attacks and defender response
Learning of Power Transmission Dynamics from partial PMU observations

Devendra Shelar | shelard@mit.edu
August 30, 2018

Collaborators: Andrey Lokhov, Nathan Lemons, Sidhant Misra, Marc Vuffray
Motivation

• State estimation
  • Optimal resource allocation for improved resiliency
  • Secure and efficient operations

• Dynamic model estimation
  • Detection of faults/attacks
  • Prompt and accurate response

• Data-driven approach
Preliminaries

• Dynamical equation: $x_{t+1} = Ax_t + Fv_t$
• $A \in \mathbb{R}^{N \times N}$ : dynamic matrix,
• $x_t \in \mathbb{R}^N$ : state vector
• $v_t \in \mathbb{R}^N$ : Noise vector
• $F$ : Noise-scaling matrix
Assumptions

• Temporal independence of noise vectors
  • $v_i$ and $v_j$ are independent for all $i \neq j$

• Spatial independence of noise vectors
  • $F$ is a diagonal matrix (there is no spatial mixing of noise)
Learning under full observability

Given: observations $x_t$ for $t = 1, 2, \cdots, n + 1$

Result:

• Maximum likelihood estimator of $A$ [1]
  \[ \hat{A} = \Sigma_1^{-1} \Sigma_0 \]

Where

\[ \Sigma_0 = \frac{1}{n} \sum_{t=1}^{n} x_t x'_t \quad \text{and} \quad \Sigma_1 = \frac{1}{n} \sum_{t=1}^{n} x_{t+1} x'_t \]

• Also the solution of least squares regression

Linear Swing Dynamics model

• Network \((\mathcal{V}, \mathcal{E})\)
• \(\mathcal{V}\) set of nodes, \(N = |\mathcal{V}|\) number of nodes
• \(\mathcal{E}\) set of edges

Swing equation

\[
M_i \ddot{\theta}_i + D_i \left( \dot{\theta}_i - \omega^0 \right) = P_i^{(m)} - P_i^{(e)}
\]

• \(P_i^{(m)}\) : mechanical power input
• \(-P_i^{(e)}\) : electrical power output
Power system model

Using change of variables

- $\delta_i$: phase deviations from steady state values
- $\omega_i$: relative generator rotor speed relative nominal frequency

\[
M_i \dot{\omega}_i + D_i \omega_i = -\sum_{(i,j) \in \mathcal{E}} \beta_{ij} (\delta_i - \delta_j) + \delta P_i
\]

\[
\begin{bmatrix}
\dot{\delta}
\dot{\omega}
\end{bmatrix} = 
\begin{bmatrix}
0_{N \times N} & I_{N \times N}
-M^{-1}L & -M^{-1}D
\end{bmatrix}
\begin{bmatrix}
\delta
\omega
\end{bmatrix} + 
\begin{bmatrix}
0 & 0
0 & M^{-1}
\end{bmatrix}
\begin{bmatrix}
\delta P
\end{bmatrix}
\]
Discrete dynamical model

- Using discretization with timestep $T$
  - $A = (I + A_d T)$

\[
\begin{bmatrix}
\delta_{t+1} \\
\omega_{t+1} \\
x_{t+1}
\end{bmatrix} =
\begin{bmatrix}
I_{N \times N} & TI_{N \times N} & \delta \\
-TM^{-1}L & I_{N \times N} - TM^{-1}D & \omega \\
A & T & I
\end{bmatrix}
\begin{bmatrix}
\delta \\
\omega \\
x_t
\end{bmatrix} +
\begin{bmatrix}
0 & 0 & 0 \\
0 & TM^{-1} & 0 \\
F & 0 & 0
\end{bmatrix}
\begin{bmatrix}
\delta P \\
v_t
\end{bmatrix}
\]

\[x_{t+1} = Ax_t + Fv_t\]
Learning under partial observability

• $\mathcal{H} \subseteq \mathcal{V}$ set of hidden nodes (without PMUs)
• $\mathcal{O} = \mathcal{V} \setminus \mathcal{H}$ set of observable nodes (with PMUs)
Rearrangement of dynamic matrix

\[
\begin{bmatrix}
\delta_{t+1}^O \\
\omega_{t+1}^O \\
\delta_{t+1}^H \\
\omega_{t+1}^H \\
\end{bmatrix} =
\begin{bmatrix}
A_{\delta^O} & A_{\delta^H} \\
A_{\omega^O} & A_{\omega^H} \\
\end{bmatrix}
\begin{bmatrix}
\delta_t^O \\
\omega_t^O \\
\delta_t^H \\
\omega_t^H \\
\end{bmatrix}
+ 
\begin{bmatrix}
G & 0 \\
0 & H \\
\end{bmatrix}
\begin{bmatrix}
0 \\
v_t^O \\
0 \\
v_t^H \\
\end{bmatrix}
\]

By change of notation,

\[
\begin{bmatrix}
y_{t+1} \\
z_{t+1} \\
\end{bmatrix} =
\begin{bmatrix}
B & C \\
D & E \\
\end{bmatrix}
\begin{bmatrix}
y_t \\
z_t \\
\end{bmatrix}
+ 
\begin{bmatrix}
G & 0 \\
0 & H \\
\end{bmatrix}
\begin{bmatrix}
u_t \\
w_t \\
\end{bmatrix}
\]

Problem statement

• Given measurements from observable nodes $y_t$ for $t = 1, 2, \cdots, n$
• Goal: To recover dynamic matrix $A$
  • Or equivalently, recover sub-matrices $B$, $C$, $D$, $E$
Some simple observations

• Stable system implies
  \[ |\lambda_{max}(E)| \leq |\lambda_{max}(A)| < 1 \]

• Thus, \( E^k \approx 0 \) for sufficiently large \( k \)

• Large susceptance values imply more unstable system
Eliminating hidden node measurements

\[
\therefore y'_{t+k+1} = [y'_{t+k} \; y'_{t+k-1} \cdots y'_t] \begin{bmatrix}
B' \\
(CD)' \\
\vdots \\
(CE^{k-1}D)'
\end{bmatrix} + \left( [G \; CH \cdots CE^{k-1}H] \begin{bmatrix}
u_{t+k} \\
w_{t+k-1} \\
\vdots \\
w_t
\end{bmatrix} \right)'
\]

\[y'_{t+k} = Y'_t X + \eta_t\]
Connectivity restrictions

• Each observable node is connected to at most one hidden node
  • $|\{(o, h) \in \mathcal{E} : h \in \mathcal{H}\}| \leq 1 \ \forall \ o \in \mathcal{O}$

• Each hidden node is connected to exactly one observable node
  • $|\{(o, h) \in \mathcal{E} : o \in \mathcal{O}\}| \leq 1 \ \forall \ h \in \mathcal{H}$
Some simple properties

\[
y'_{t+k+1} = [y'_{t+k} y'_{t+k-1} \cdots y'_t] \begin{bmatrix} B' \\ (CD)' \\ \vdots \\ (CE^{k-1}D)' \end{bmatrix} + \left( \begin{bmatrix} G & CH & \cdots & CE^{k-1}H \\ \vdots \\ w_{t+k-1} \end{bmatrix} \right)' \
\]

\[
y'_{t+k} = Y'_t X + \eta_t
\]

Properties

- \(G\) is diagonal by assumption
- Under connectivity restriction, for all \(m = 0,1, \cdots, k - 1\), \(CE^m H\) is of the form \([0 \ 0 \ x \ 0]\), where
  - \(x \in R^{Q \times H}\) with
    - exactly 1 non-zero entry per column, and
    - at most 1 non-zero entry per row.
Implications

For timesteps $t = i, i + k, i + 2k, \ldots$

- The noise vectors $\eta_t$ satisfy both temporal and spatial independence
- Thus, we can use least squares estimator

$$
\begin{bmatrix}
y_{t+k+1}' \\
y_{t+2k+1}' \\
\vdots \\
y_{t+ck+1}'
\end{bmatrix} =
\begin{bmatrix}
Y_t' \\
Y_{t+k}' \\
\vdots \\
Y_{t+ck}'
\end{bmatrix} X + \eta_t
$$

$r \approx SX$
Least squares estimator

• \( \hat{X} = (S'S)^{-1}(S'r) \), or equivalently,

\[
\begin{bmatrix}
B' \\
(CD)' \\
\vdots \\
(CE^{k-1}D)'
\end{bmatrix}
= \left(\begin{bmatrix}
\Sigma_0 & \Sigma_1 & \cdots & \Sigma_k \\
\Sigma_{-1} & \Sigma_0 & \cdots & \Sigma_{k-1} \\
\Sigma_{-k} & \Sigma_{-k+1} & \cdots & \Sigma_0
\end{bmatrix}\right)^{-1} \left(\begin{bmatrix}
\Sigma_k \\
\Sigma_{k-1} \\
\vdots \\
\Sigma_0
\end{bmatrix}\right)
\]

Where

\[
\Sigma_i = \frac{1}{l - j + 1} \sum_{j=1}^{l} y_{jk+i} y'_{jk}
\]

• Allows, recovery of B matrix in a straightforward manner.
Recovering submatrices $C$, $E$, and $D$

• Under the connectivity restrictions, $C$ and $D$ are sparse matrices such that $C = \begin{bmatrix} 0 & 0 \\ x & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & 0 \\ z & 0 \end{bmatrix}$ and $E^i = \begin{bmatrix} R_{1i} & R_{2i} \\ R_{3i} & R_{4i} \end{bmatrix}$
  
  • $x \in \mathbb{R}^{\mathcal{O} \times \mathcal{H}}$ with exactly 1 non-zero entry per column and at most 1 non-zero entry per row.
  
  • $z \in \mathbb{R}^{\mathcal{H} \times \mathcal{O}}$ with exactly 1 non-zero entry per row and at most 1 non-zero entry per column.
  
  • $R_{ji} \in \mathbb{R}^{\mathcal{H} \times \mathcal{H}}$ is a diagonal matrix for $j = 1,2,3,4$ and $i = 1,2,\ldots$

• Hence, given values of $CE^1D$, $CE^2D$ and $CE^3D$, are relatively simpler non-linear expressions of entries in $C$, $E$ and $D$. 

Concluding remarks

Summary
• Connectivity restriction can be leveraged to learn the dynamical model with partial observability.
• These properties may be applicable to other domains
• Identifying properties of non-linear optimization model

Future work
• Relaxing assumptions such as connectivity restriction and using smaller values of $k$. 
Questions?

Thank you
Benders Decomposition approach

- Reformulate budget-k-max-loss problem as target-loss-min-cardinality problem. Let $L_{target}$ be minimum target loss.

Attacker Master problem
- Initialize with no cuts

\[
\min \sum_i \delta_i \\
\text{s.t. Bender cuts} \\
\delta_i \in \{0,1\}
\]

Defender problem (Same as Stage III)

\[
\min_{u \in U} \min_{\delta} L(\delta, u) \\
\text{s.t.} \\
\quad \text{Network constraints} \\
\quad \text{Component constraints} \\
\quad \text{Voltage bounds}
\]
Benders Decomposition approach

Attacker MIP

\[
\min \sum_i \delta_i \\
\text{s.t. } \text{Benders cuts} \\
\delta_i \in \{0,1\}
\]

Defender MIP

\[
\min_{u \in U} L(\delta^*, u)
\]

\[\delta^* \]

\[L(\delta^*, u^*) \geq L_{target}\]

\[u^* = (u^*_I, u^*_C)\]

Benders cut

\[L_P(\delta^*, u^*_I)\]

Exit
Benders Decomposition approach

$$\text{LP}\left(\delta^{\text{iter}}, u_I\right) \equiv \min c^Ty$$

s.t. $Ay \geq b + Q\delta^{\text{iter}}$

Fixed attacker strategy for current iteration

Response with fixed integer values

Benders cut

Optimal dual vector solution to LP

Small number $\approx 10^{-6}$

Right hand side of LP
Technical Detail

• Bad Benders cuts may arise
  • If no Stage III constraints have non-zero coefficients for both attack variables and continuous inner variables
  • Which indeed is the case in our problem!
  • May perform as badly as brute force!

• Suggestion! Approximate reformulation?
  • Ensure positive coefficients of attack variables in constraints having continuous inner variables
  • Significant computational speed-up
    • Solutions for 118 node network obtained in less than 2 minutes
  • Approximation error produces sub-optimal min-cardinality attacks
Resilience-Aware OPF - Trilevel formulation

\[
\min_{a \in \mathcal{A}} C_{alloc}(a) + \max_{d \in \mathcal{D}} \min_{u \in \mathcal{U}} L(a, d, u)
\]

Subject to
- Network constraints
- Component constraints
- Voltage constraints
Resiliency-aware Resource Allocation (Stage I)

Stage I - Allocation of DERs over radial networks
a. Size and location
b. Active and reactive power setpoints ($x^n$)?

Suppose, some controllable DERs are not vulnerable to attack.
Resiliency-Aware OPF - Trilevel formulation

Frequency deviation model
\[ f^{\text{nom}} - f^c = -f^{\text{reg}}(P_0^o - P_0^c) \]

Voltage deviation model
\[ v^{\text{nom}} - v_0^c = -v^{\text{reg}}(Q_0^o - Q_0^c) \]

Pre-contingency resource allocation
\[ a = (p g^o, q g^o) \]
Defender Response and Allocation: Diversification

- Some DERs contribute to $L_{VR}$ more than $L_{AC}$, and vice versa.
- Diversification holds for “heterogeneous allocation” with downstream DERs with more reactive power.
- Post-contingency losses are the same for uniform vs. heterogeneous resource allocations.
- Pre-contingency voltage profile is better for heterogeneous resource allocation.
Going from LPF to NPF

Lower and upper bound the optimal loss for non-linear power flows with optimal losses computed using linear power flows.

**Theorem:** Let \( \mathcal{L}, \hat{\mathcal{L}}, \) and \( \check{\mathcal{L}} \) denote the optimal losses using NPF, LPF, and \( \epsilon \)-LPF respectively. Then,

\[
\hat{\mathcal{L}} \leq \mathcal{L} \leq \check{\mathcal{L}} + \frac{\mu N}{2\mu + 4}.
\]

**Remarks**
- For \( \mu = 0.5, N = 37, \frac{\mu N}{2\mu + 4} = 3.7. \) With typical \( \epsilon \) (max. ratio of line loss to power flows), the gap between the bounds is small (3-5%).
Our contributions

Regulation objectives

Attacker model → Bilevel problem → Defender model

Regime?

Grid-Connected regime
- DER disruptions
  - Greedy Approach
  - IEEE TCNS 2016 [1]
- DN vulnerability to simultaneous EV overcharging [2]
- Security of Economic Dispatch
  - KKT based reformulation
  - DSN 2017 [3]

Cascade / Islanding regimes
- Multiple regimes
  - Inner problem: mixed-integer vars
  - Benders decomposition

Uncontrolled vs Cascade vs Islanding

Value of timely disconnections

N = 24
Strategic deployment of portable DERs for post-hurricane power restoration efforts

• A simpler problem
  • Given
    • set of subnetworks
    • repair times of lines
    • inventory of portable DERs with varying capabilities

• Question
  • What is optimal deployment of portable DERs such that lost demand is minimized?
Portable DERs for power restoration

• More challenging problem
  • What is the optimal deployment of portable DERs before the hurricane to minimize expected lost demand?
Technical detail

Original constraints

\[

g_i \geq \delta_i \\
p_i = (1 - g_i) \overline{p_i} \\
q_i = (1 - g_i) \overline{q_i}
\]

LP constraints

\[
0 \geq 0 \\
1 \geq 0 \\
1 \geq 1
\]

Reformulated constraints: Choose \( \eta = 10\varepsilon \)

\[

g_i \geq \delta_i \\
p_i = (1 - (1 - \eta)g_i - \eta \delta_i) \overline{p_i} \\
q_i = (1 - (1 - \eta)g_i - \eta \delta_i) \overline{q_i}
\]

Cases

\( \delta_i = 1, g_i = 1 \checkmark \)
\( g_i = 0, \delta_i = 0 \checkmark \)
\( g_i = 1, \delta_i = 0 \, ? \)
Going from LPF to NPF

**Theorem:** Let $\mathcal{L}$, $\hat{\mathcal{L}}$, and $\check{\mathcal{L}}$ be optimal solutions to attacker-defender game under NPF, LPF, and $\epsilon$-LPF respectively; and denote the optimal losses by, respectively. Then,

$$\hat{\mathcal{L}} \leq \mathcal{L} \leq \check{\mathcal{L}} + \frac{\mu N}{2\mu + 4}.$$

**Remarks**

- Voltages for $\hat{\mathcal{L}}$ (resp. $\check{\mathcal{L}}$) upper (resp. lower) bound voltages for $\mathcal{L}$
- Power flows for $\hat{\mathcal{L}}$ (resp. $\check{\mathcal{L}}$) lower (resp. upper) bound power flows for $\mathcal{L}$
- For $\mu = 0.5, N = 37, \frac{\mu N}{2\mu + 4} = 3.7$. With typical $\epsilon$ (max. ratio of line loss to power flows), the gap between the bounds is small (3-5%).
- Better bounds can be derived
Two simpler problems

\[ \hat{L} (\text{LPF model}) \equiv \left\{ \begin{array}{l} \max_{\delta} \min_{\phi} L(x(\delta, \phi)) \\ \text{s.t. constraints,} \\ \text{linear power flow (LPF) or (\epsilon - LPF)} \end{array} \right. \]

LPF state: \( \hat{x} = [\hat{v}, \hat{\ell}, sc, sg, \hat{S}] \in \hat{X} \)

\[ \hat{S}_{ij} = \sum_k \hat{S}_{jk} + s_j + z_{ij} \ell_{ij} \]

\[ \hat{v}_j = \hat{v}_i - 2\text{Re}(\bar{z}_{ij}\hat{S}_{ij}) + |z_{ij}|^2 \ell_{ij} \]

\( \epsilon \)-LPF state: \( \bar{x} = [\bar{v}, \bar{\ell}, sc, sg, \bar{S}] \in \bar{X} \)

\[ \bar{S}_{ij} = \sum_k \bar{S}_{jk} + (1 + \epsilon)s_j \]

\[ \bar{v}_j = \bar{v}_i - 2\text{Re}(\bar{z}_{ij}\bar{S}_{ij}) \]

\( \epsilon \) chosen based on the size of the tree network and the max ratio of line losses to power flows
• Downstream nodes are more critical for voltage regulation
• Greedy approach computes “near-optimal” solutions
• Load control is not effective for higher intensity attacks
• Load control reaches higher saturation levels for higher weightage for $L_{VR}$
Defender model (Cascade regime)

Defender response: \( u = (\beta, k_g, k_c) \)

\[
\begin{align*}
    k_g_i &= \begin{cases} 
        1, & \text{if DG } i \text{ is disconnected} \\
        0, & \text{otherwise.}
    \end{cases} \\
    k_c_i &= \begin{cases} 
        1, & \text{if load } i \text{ is disconnected} \\
        0, & \text{otherwise.}
    \end{cases}
\end{align*}
\]

Connectivity condition:

\[
\begin{align*}
    k_g_i &= 0 \quad \Rightarrow \quad v_i \in [v_{g_i}, \overline{v_{g_i}}] \\
    v_i &\notin [v_{g_i}, \overline{v_{g_i}}] \quad \Rightarrow \quad k_g_i = 1
\end{align*}
\]

Voltage bounds for DG
Similarly for loads!

Defender response:
Which loads and DGs to disconnect?
Strategic deployment of portable DERs for post-hurricane power restoration efforts

• Damage to lines result in subnetworks (SNs)

• Usual restoration steps are:
  • Repair the damaged lines
  • Connect to main grid
  • Restore the power supply

• How can portable DERs help?
Literature survey

(T1) Interdiction and cascading failure analysis of power grids
• R. Baldick, K. Wood, D. Bienstock: Network Interdiction, Cascades
• A. Verma, D. Bienstock: N-k vulnerability problem
• X. Wu, A. Conejo: Grid Defense Planning

(T2) Data-integrity attacks
• E. Bitar, K. Poolla, A Giani: Data integrity, Observability
• H. Sandberg, K. Johansson: Secure control, networked control
• B. Sinopoli, J. Hespanha: Secure estimation and diagnosis
Defender Response and Allocation: Diversification

- Some DERs contribute to $L_{VR}$ more than $L_{AC}$, and vice versa.
Defender Response and Allocation: Diversification

- Diversification holds for “heterogeneous allocation” with downstream DERs with more reactive power.
Defender Response and Allocation: Diversification

- Post-contingency losses are the same for uniform vs. heterogeneous resource allocations
- Pre-contingency voltage profile is better for heterogeneous resource allocation

Heterogeneous resource allocation can support more loads than uniform one.
Effect of power factor on losses

N = 12

N = 36
Optimal attacker set-points

Typically,

• **Small line losses**: in comparison to power flows
• **Small impedances**: sufficiently small line resistances

Assume for simplicity:

• **No reverse power flows**: power flows from substation to downstream

What are optimal attacker set-points?

**Proposition**: For a defender action $\phi$, and given attacker choice of $\delta$, the optimal attacker set-point is given by:

$$pd^a = 0, \quad qd^a = -j\overline{sg}_i$$
Greedy Approach

For fixed defender action:

- For a fixed attacker action, the ordering of nodes with respect to their voltages remain the same between $\hat{L}$ and $\tilde{L}$.
- For any fixed node, the ordering of optimal attacker actions with respect to their impact on this node remains the same between $\hat{L}$ and $\tilde{L}$. 

For fixed defender action:

- For a fixed attacker action, the ordering of nodes with respect to their voltages remain the same between $\hat{L}$ and $\tilde{L}$.
- For any fixed node, the ordering of optimal attacker actions with respect to their impact on this node remains the same between $\hat{L}$ and $\tilde{L}$.
Defender model

• Defender response: $u = (pr, qr, \beta)$

  $pr_i, qr_i$: active and reactive power output of reserves (controllable DGs) at node $i$
  
  • $0 \leq pr_i \leq \overline{pr}_i, pr_i^2 + qr_i^2 \leq \overline{s}_i^2$

  $\beta_i \in [\underline{\beta}_i, 1]$: load control parameter at node $i$
  
  • $pc_i = \beta_i \overline{pc}_i, \quad qc_i = \beta_i \overline{qc}_i$

Defender response:

How to optimally dispatch reserves?
How much load control should be exercised?
Optimal interdiction plan: fixed defender choices

Proposition

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

• If DGs at $j, k$ are homogeneous and $j$ is before $k$ w.r.t. $i$, then DG disruption at $k$ will have smaller effect on $\nu_i$ (relative to disruption at $j$)

• If DGs at $j, k$ are homogeneous 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 $\nu_i$

\[
\Delta_j(\nu_i) < \Delta_k(\nu_i) \\
\Delta_e(\nu_i) \approx \Delta_k(\nu_i)
\]
Resiliency-aware Resource Allocation (Stage II)

Stage II - Adversarial node disruptions
a. Which nodes to compromise ($\delta$)?
b. Set-point manipulation ($sp^a$)?

... can include other attack models
Resiliency-aware Resource Allocation

Stage I - Allocation of DERs over radial networks
   a. Size and location
   b. Active and reactive power setpoints ($x^n$)?

Stage II - Adversarial node disruptions
   a. Which nodes to compromise ($\delta$)?
   b. Set-point manipulation ($sp^a$)?

Stage III - Optimal dispatch / response ($x^c$)
   a. Maintain voltage
   b. Exercise load control or not

Goals:
1. Determine the best resource allocation
2. Identify vulnerable / critical nodes
3. Determine optimal dispatch post-contingency
Resiliency-aware Resource Allocation

Stage II - Adversarial node disruptions
   a. Which nodes to compromise ($\delta$)?
   b. Set-point manipulation ($sp^a$)?

Stage III - Optimal dispatch / response ($x^c$)
   a. Maintain voltage
   b. Exercise load control or not

Goals:
1. Identify vulnerable / critical nodes
2. Determine optimal dispatch post-contingency