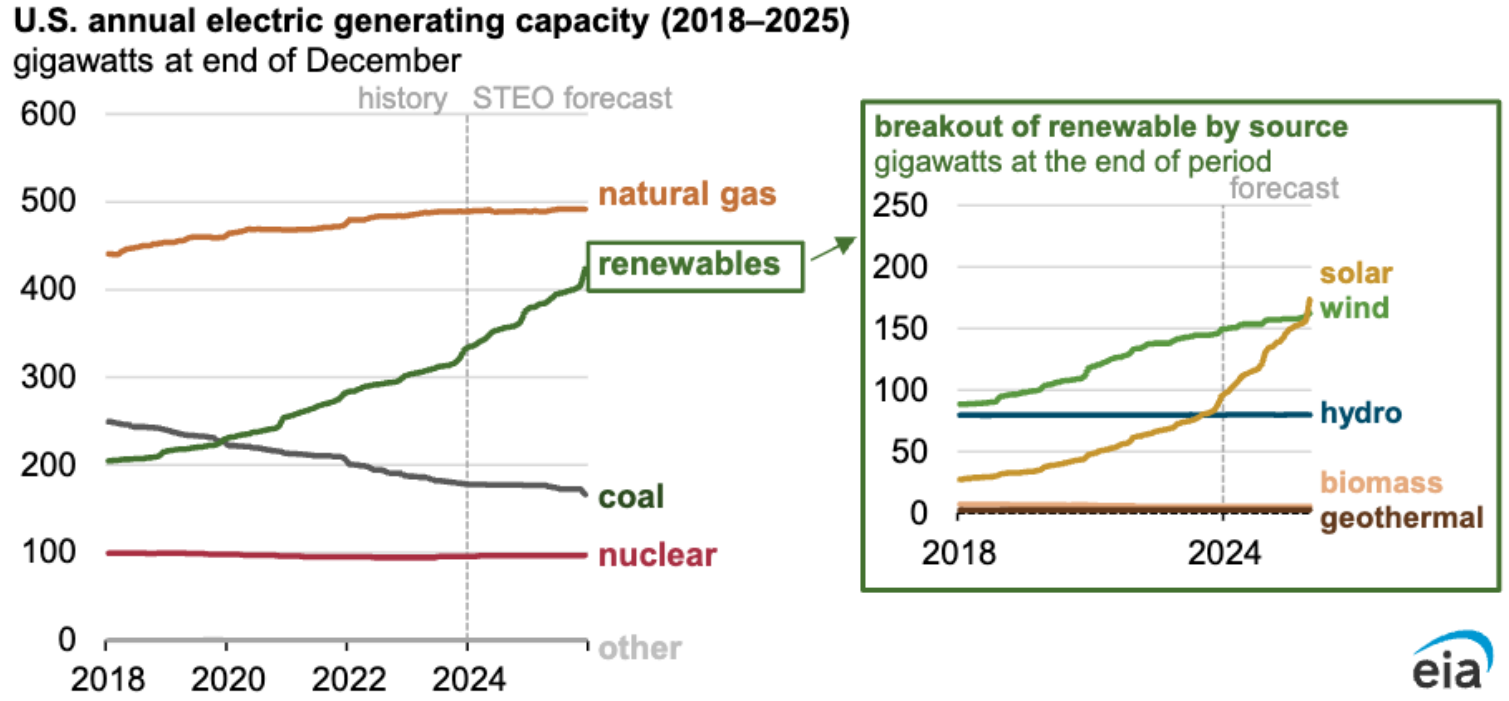
Enhancing power grid resilience to cyber-physical attacks using distributed retail electricity markets

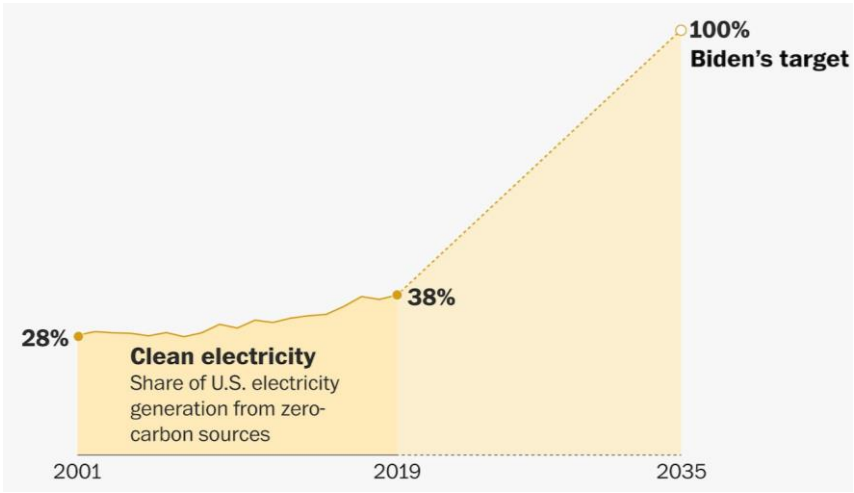
Vineet J Nair[1], Priyank Srivastava[2], Anuradha Annaswamy[1]

jvineet9@mit.edu

[1] Massachusetts Institute of Technology
[2] Indian Institute of Technology, Delhi

Rapid grid decarbonization to fight climate change





Data source: U.S. Energy Information Administration, *Short-Term Energy Outlook* (STEO), January 2024

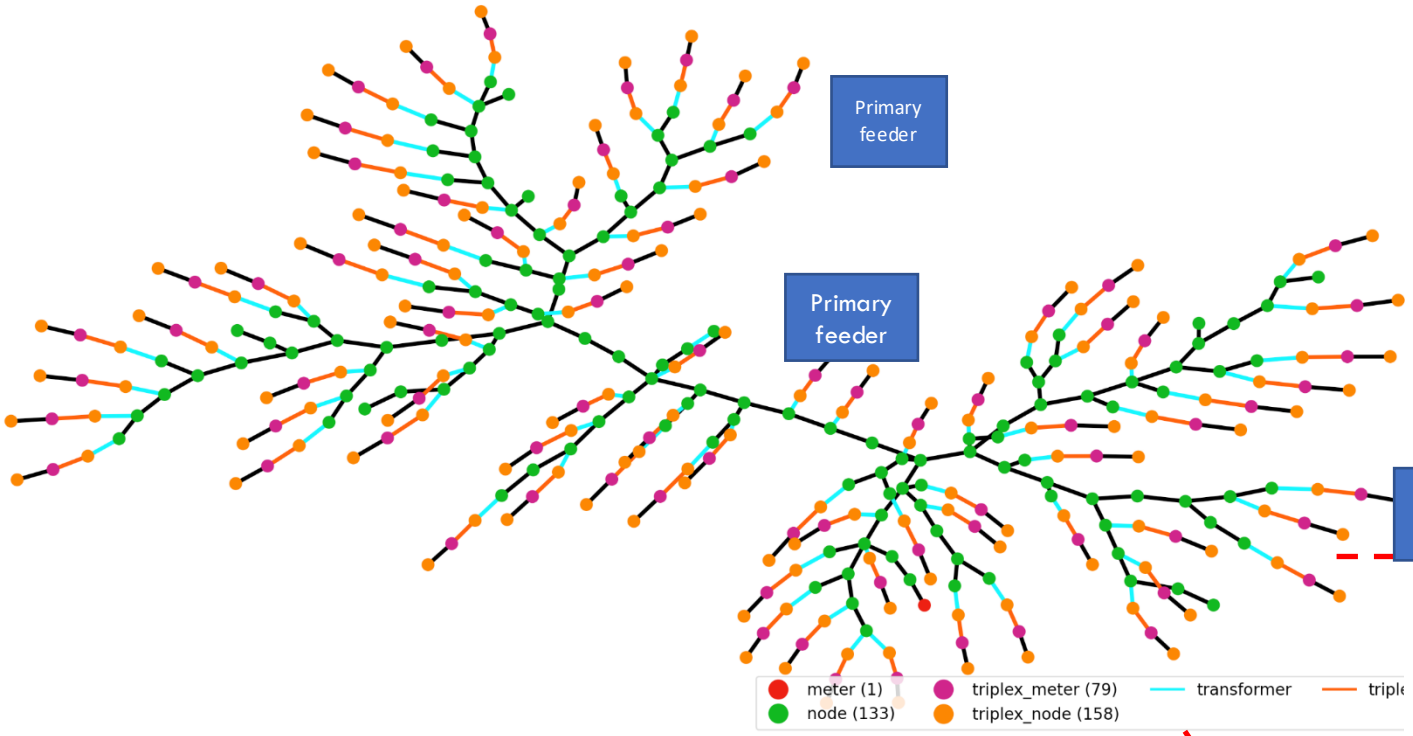
Distributed Energy Resources (DERs) & Internet-of-Things (IoT) devices

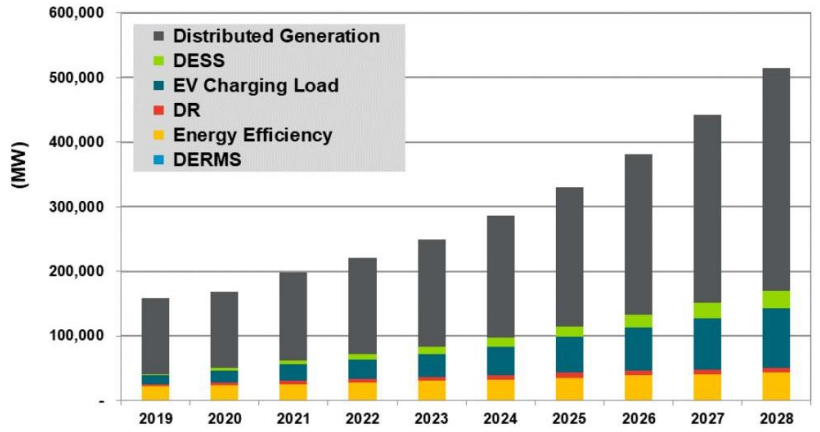
x 10,000 [1]

Grid-edge is becoming more complex, intelligent, capable

[1] GTM Research and Department of Energy
Image sourced: https://engineering.fb.com/connectivity/electrical-grid-mapping/, Google Images

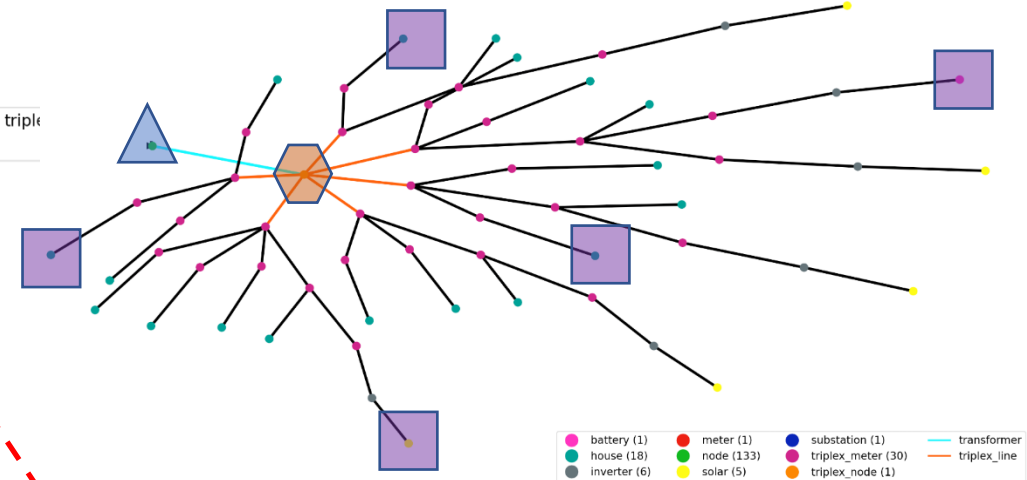
Distributed paradigm → Introduces more vulnerabilities





Increasing DER penetration

Secondary feeder



Consumer feeder

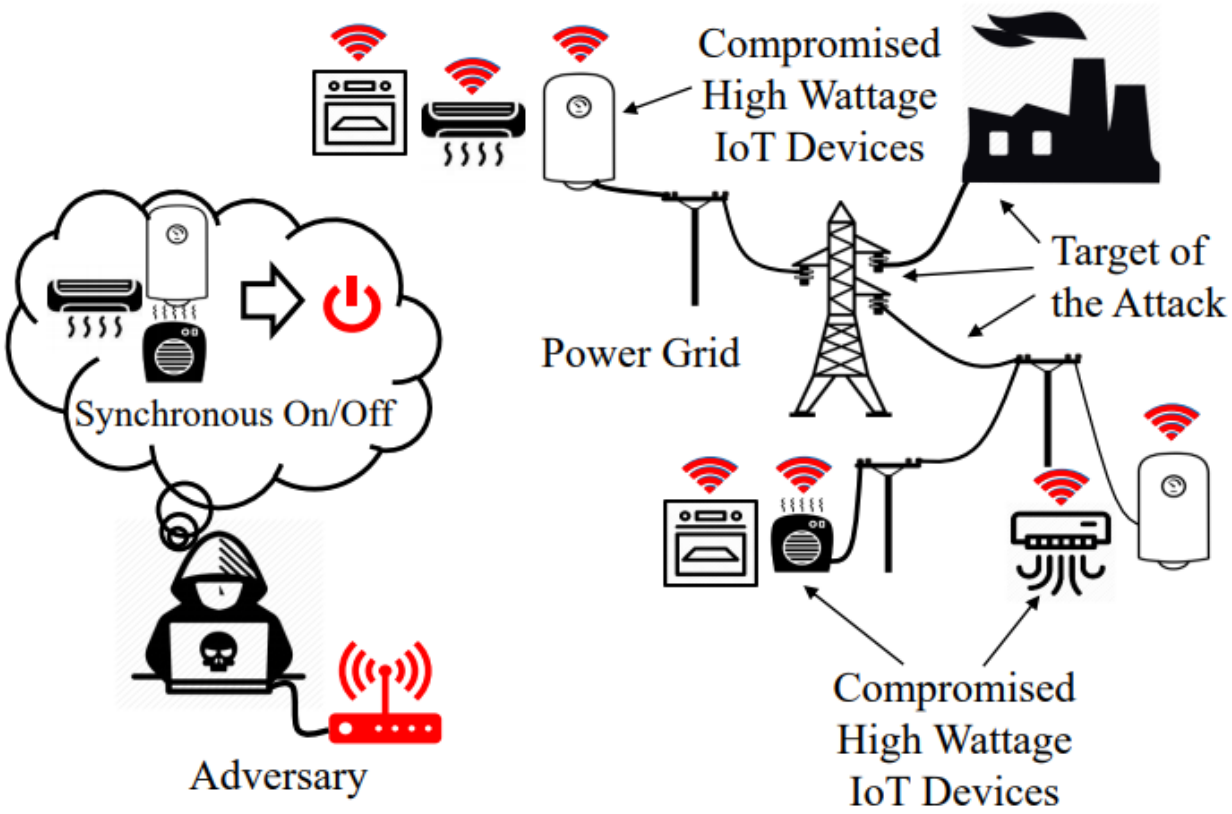
400 Secondary Feeders

1000 IoT devices
100 PVs (531.5 KW)
200 batteries

A typical distribution grid
(model for IEEE-123 node feeder)

Source: PNNL Gridlab-D Modeling Team

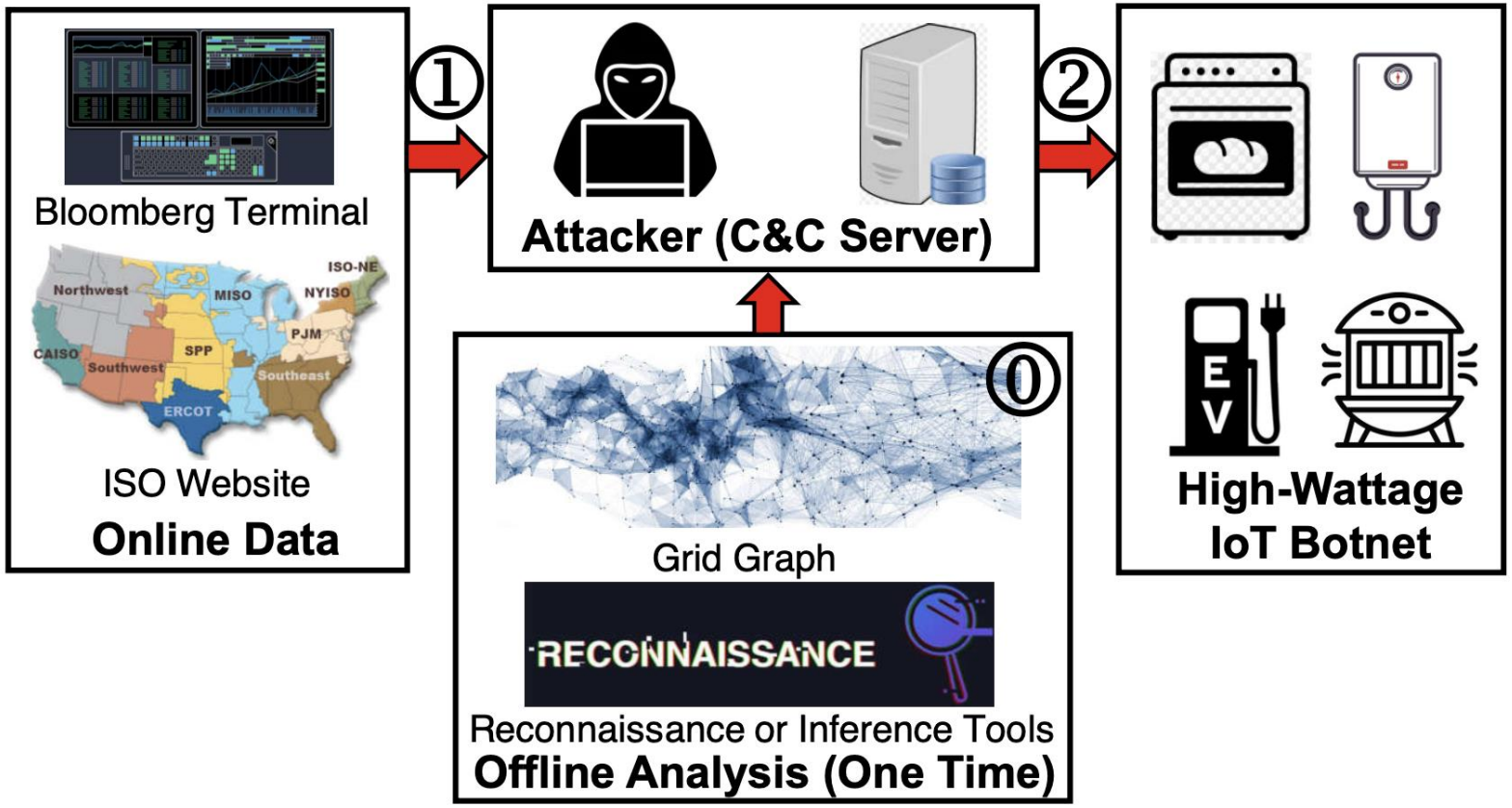
Example I: BlackIoT - Load alteration using IoT-networks



- Large scale manipulation of IoT devices – *botnets,* like Mirai botnets
- A 900MW step change in load with a tightly coordinated 600,000 IoT devices each controlling a 1500W HVAC unit

[1] Soltan et.al, "BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid" Usenix Security Symposium 2017
[2] Huang et.al, "Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks" Usenix Security Symposium 2018

Example II: MadIoT - Strategic Manipulation of Demand

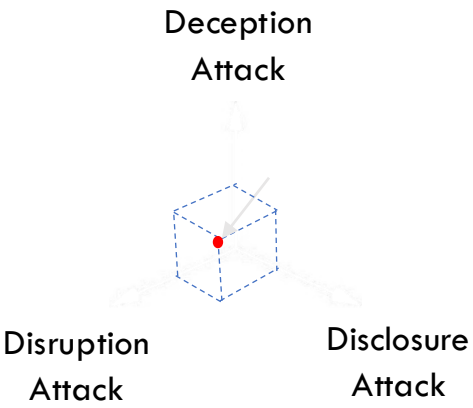


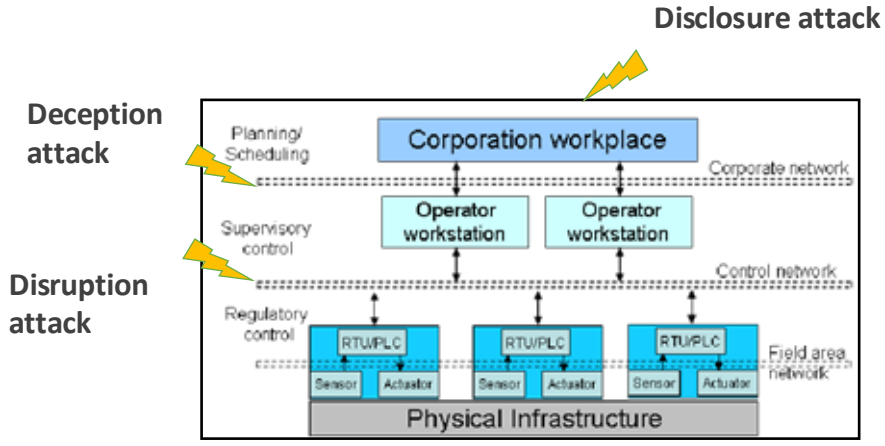
- Identify the most vulnerable nodes and time
- Only need to compromise 150,000 nodes now – much less than the previous attack

[1] Shekari et.al, "MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses" Usenix Security Symposium 2022

Example III: Ukraine Attack in 2015-16

- **Confidentiality Attack (Disclosure):**
  - Attack introduced via phishing emails containing malware
  - Enabled attacker communication with hacked systems
  - Enabled attacker to steal critical data and study system environment
- **Integrity Attack (Deception):**
  - Accessed control level over compromised VPN
  - Spoofed control commands
- **Availability Attack (Disruption):**
  - Overwrote substation firmware, permanently ensuring remote inoperability of breakers
- 30 substations switched off
- **230,000** customers left without power
- The 2016 attack also corrupted transmission control





Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

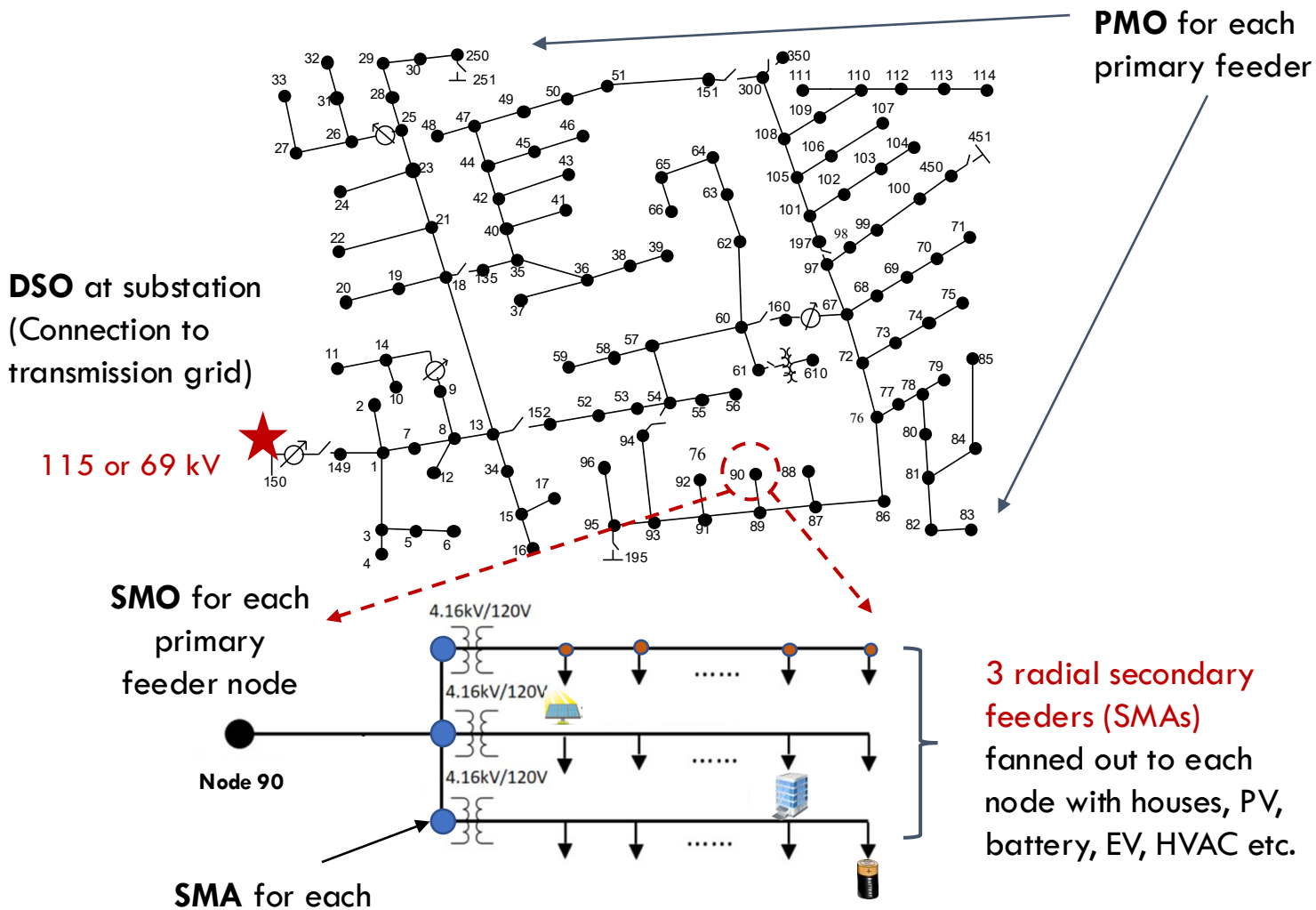
How can we strengthen cyber-physical grid resilience?

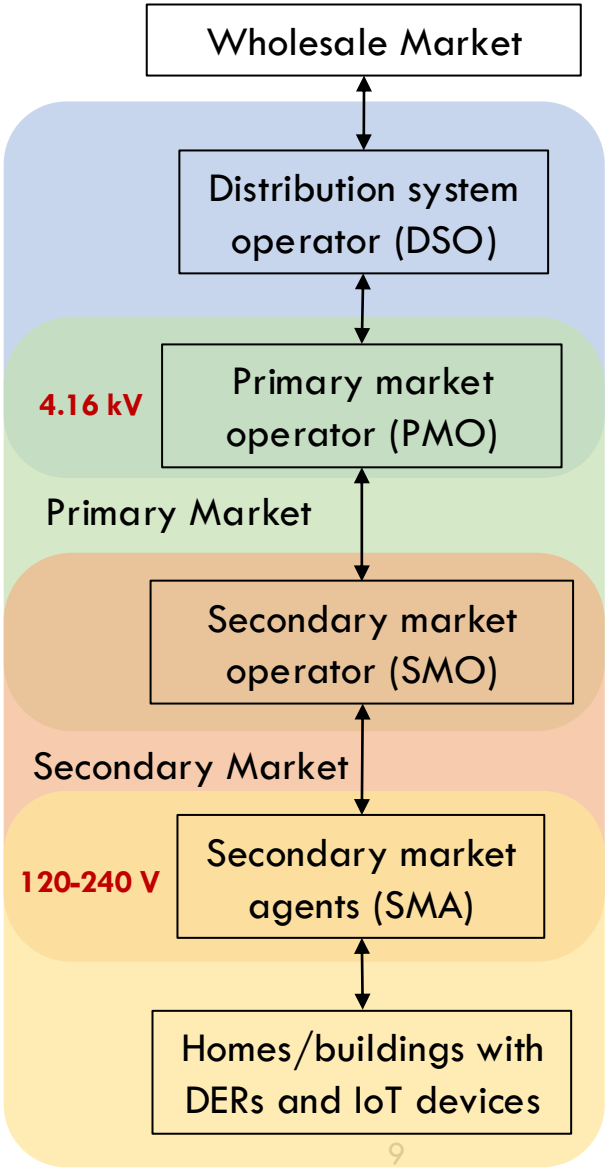
- Decarbonized power grid will necessarily include an increased cyber footprint, allowing a multitude of attack surfaces, cyber and physical
- Ukraine power grid attacks and other recent attacks on critical infrastructure (e.g. Colonial pipeline) underscore that such threats are real
- Combined presence of both cyber & physical attacks requires new tools for analysis of the emerging cyber-physical energy grid rich in DERs

Can we use **market-based coordination** of IoT devices & DERs (w/o direct control) to increase rather than decrease **resilience**?

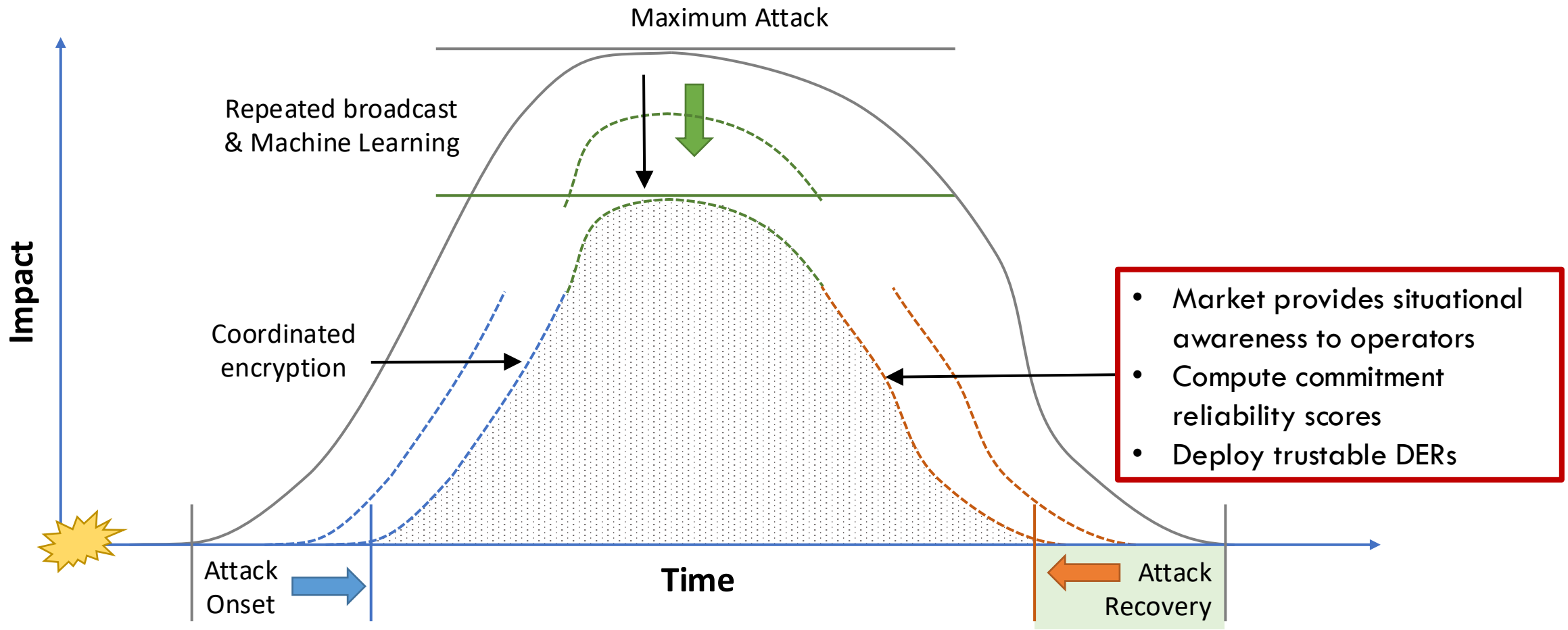
Shekari, Tohid, Alvaro A. Cardenas, and Raheem Beyah. "{MaDIoT} 2.0: Modern {High-Wattage}{IoT} Botnet Attacks and Defenses." 31st USENIX Security Symposium (USENIX Security 22). 2022.

Hierarchical local electricity market



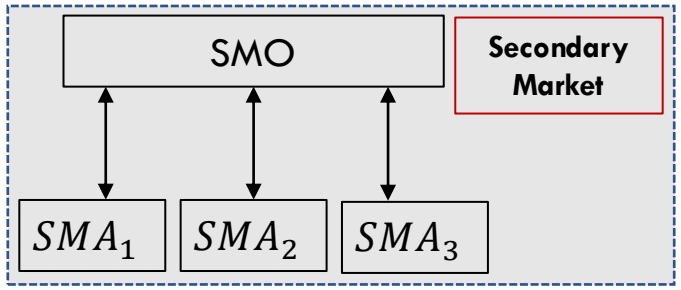


Using markets and IoT-enabled DERs for resilience



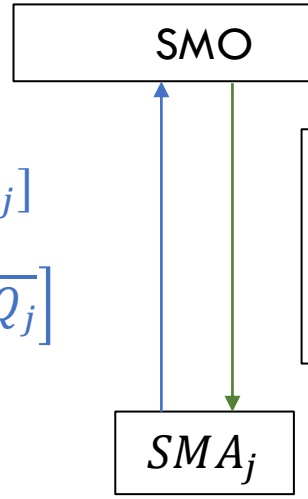
S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty , "A Systems and Control Perspective of CPS Security," Annual Reviews in Control, 2019.

Secondary market: Flexibility in bids



Bid $\overrightarrow{B_j} = [P_j^0, Q_j^0, \Delta P_j, \Delta Q_j]$

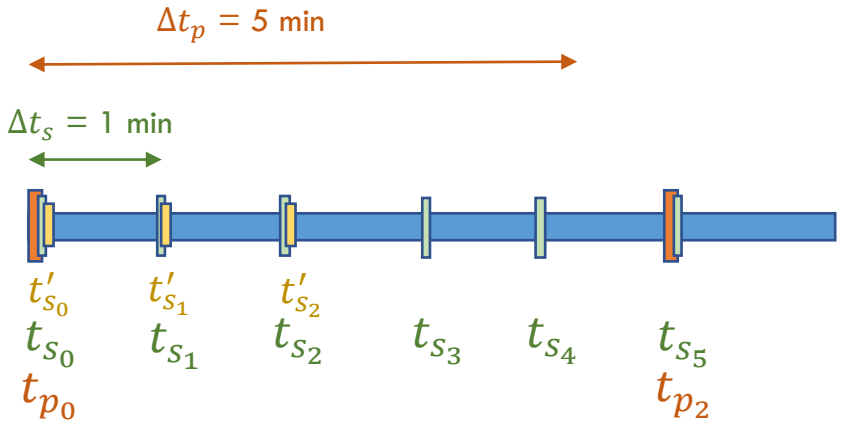
$\Delta P_j = \left[\underline{P_j}, \overline{P_j}\right], \Delta Q_j = \left[\underline{Q_j}, \overline{Q_j}\right]$

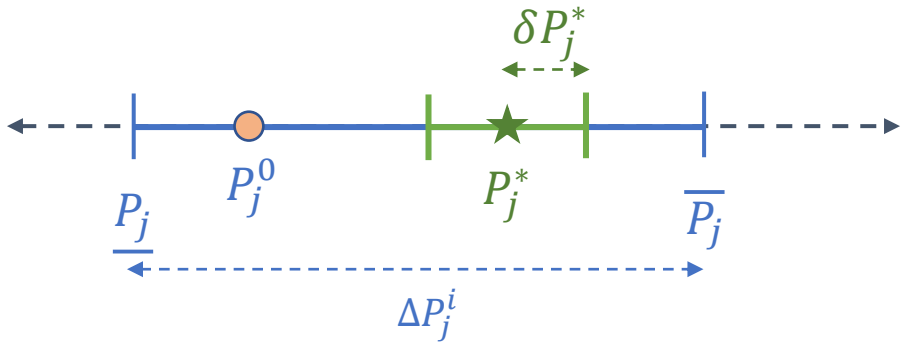


Cleared solution

$\overrightarrow{S_j^*} = \left[P_j^*, Q_j^*, \delta P_j^*, \delta Q_j^*, \mu_j^{P*}, \mu_j^{Q*}\right]$

$P_j = P_j^G - P_j^L, Q_j = Q_j^G - Q_j^L$





1. t_{s_0}: **Bidding** for $[t_{s_0}, t_{s_1}]$ period
2. t'_{s_0}: **Scheduling** (market clearing) for $[t_{s_0}, t_{s_1}]$
3. t'_{s_1} : **Settlements** (financial transactions) for $[t_{s_0}, t_{s_1}]$

All bids are for 1 period into the future & based on load or generation forecasts

SM constraints

- Operational active (and reactive) power limits: $\delta P_j, \delta Q_j \geq 0$

$$\underline{P_j} + \delta P_j \leq P_j \leq \overline{P_j} - \delta P_j, \underline{Q_j} + \delta Q_j \leq Q_j \leq \overline{Q_j} - \delta Q_j$$

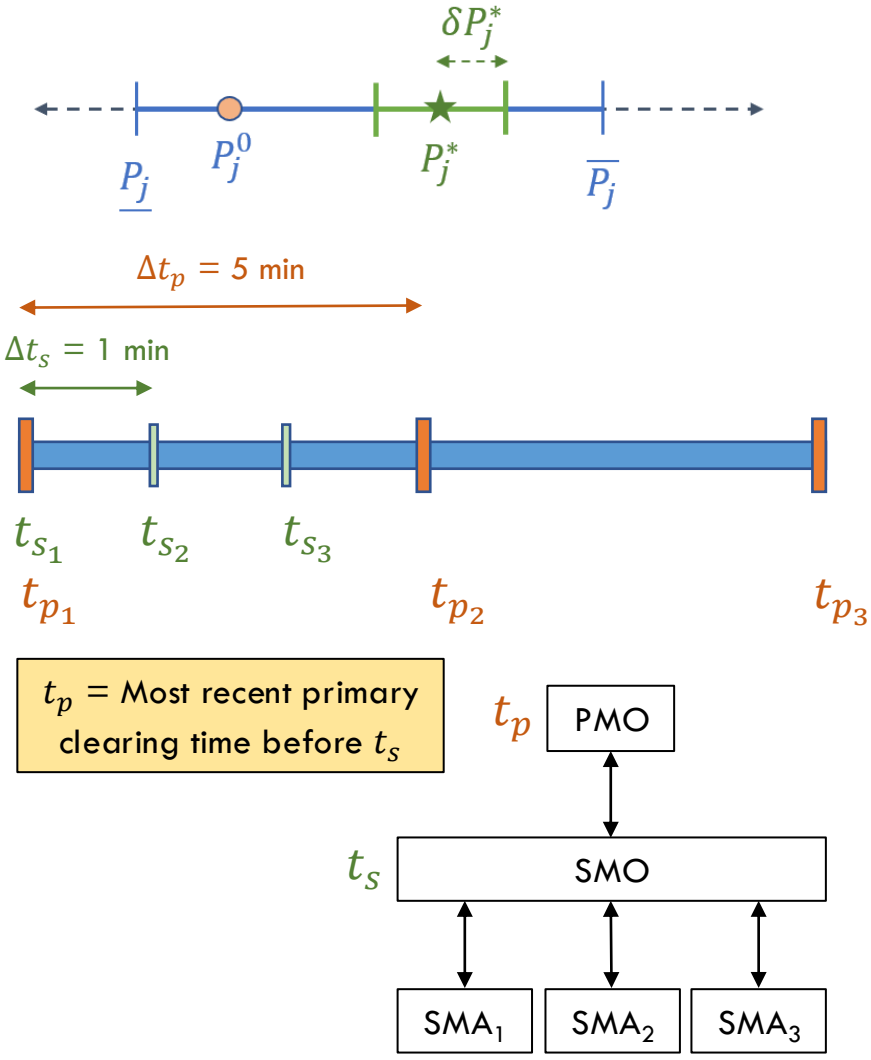
- Real-time tariff constraints: $0 \leq \mu_j^P, \mu_j^Q \leq \overline{\mu}$

- Power balance between lower (SMO) & upper (PMO) levels:

$$\sum_j P_j(t_s) = P^*(t_p),\ \sum_j Q^*(t_s) = Q^*(t_p)$$

- Budget constraint: SMO must break even over a set time horizon (e.g. 24h):

$$\sum_{t_p}\sum_{t_s}\sum_{j}\left(\mu_j^P P_j + \mu_j^Q Q_j\right)\Delta t_s \leq \sum_{t_p}\left(\mu^{P^*} P^* + \mu^{Q*} Q^*\right)\Delta t_p$$



Commitment scores for SMAs

- SMO rewards SMA for fulfilling bilateral contracts, penalizes violations
  → Measure of commitment reliability
- Higher scores (i.e. C closer to 1) → SMAs will more reliably follow the market
- Normalized deviations of actual P/Q injections of SMAs j from their cleared setpoints

$$e_j^{iP}(t_s) = \left[\!\left[\hat{P}_j^i > \overline{P}_j^{i^*} \right]\!\right] \left(\hat{P}_j^i - \overline{P}_j^{i^*} \right) + \left[\!\left[\hat{P}_j^i < \underline{P}_j^{i^*} \right]\!\right] \left(\underline{P}_j^{i*} - \hat{P}_j^i \right) + \left[\!\left[\underline{P}_j^{i^*} \leq \hat{P}_j^i \leq \overline{P}_j^{i^*} \right]\!\right] \max\left(\hat{P}_j^i - \overline{P}_j^{i^*}, \underline{P}_j^{i^*} - \hat{P}_j^i \right)$$

- Normalize by true solution & across all SMAs j under the SMO i:

$$\widetilde{e_j^{iP}}(t_s) = \frac{e_j^{iP}(t_s)}{|P_j^{i^*}(t_s)|} \Rightarrow \widetilde{e^{iP}}(t_s) = \frac{\mathbf{e^{iP}}(t_s)}{\|\mathbf{e^{iP}}(t_s)\|}$$

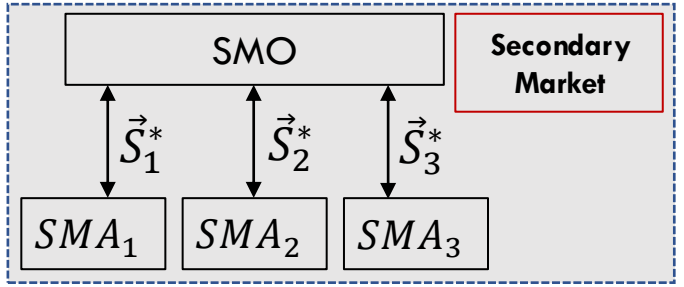
- Update score for each SMA at every timestep:

$$C_j^i(t_s) = \begin{cases} 1 & \text{if } t_s = 0 \\ C_j^i(t_s - 1) - \frac{\widetilde{e_j^{iP}}(t_s) + \widetilde{e_j^{iQ}}(t_s)}{2} & \text{if } t_s > 0 \end{cases} \Rightarrow$$

Min-max normalization
$\Rightarrow 0 \leq C_j^i(t_s) \leq 1 \; \forall \; t_s$

Secondary market: Optimization problem

- SMO i maximizes social welfare
- **Multi-objective, constrained optimization** at each time instant



$$\min_{\vec{S}_j^i} \sum_{j \in \mathcal{N}_{J,i}} \{f_{j,1}^i, f_{j,2}^i, f_{j,3}^i, f_{j,4}^i\}$$

$$f_{1,j}^i \succ f_{2,j}^i \succ f_{3,j}^i \succ f_{4,j}^i$$

Maximize aggregate reliability: $f_{j,1} = -C_j^i((P_j^i - P_j^{i0})^2 + (Q_j^i - Q_j^{i0})^2)$ ← Allocate larger share of flexibilities to more reliable assets

Minimize net cost to SMO: $f_{j,2}^i = \mu_j^{iP} P_j^i + \mu_j^{iQ} Q_j^i$

Maximize aggregate flexibility: $f_{j,3}^i = -(\delta P_j^i + \delta Q_j^i)$

Minimize disutility to SMA: $f_{j,4}^i = \beta_j^{iP}(P_j^i - P_j^{i0})^2 + \beta_j^{iQ}(Q_j^i - Q_j^{i0})^2$

- Use **hierarchical approach** to solve **multi-objective** problem
- Successively optimize each objective in descending order of importance
- Gets around issue of objective terms not being comparable in magnitude
- No longer need to normalize

$$\min_{\vec{S}_j^i} F_k = \sum_{j \in \mathcal{N}_{J,i}} f_{j,k}^i(\vec{S}_j^i) \;\forall\; k = 1,2,3,4$$

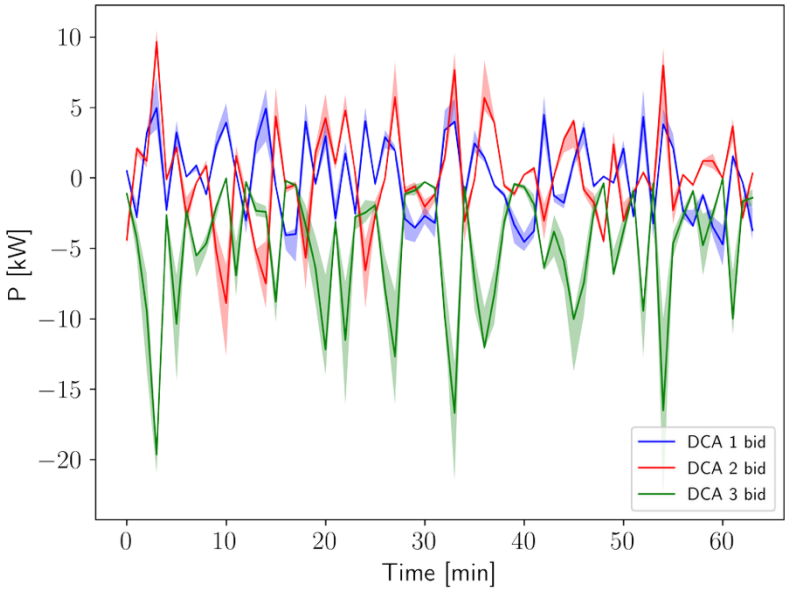
$$\text{s.t. } f_{j,\ell}^i(\vec{S}_j^i) \leq (1+\epsilon) \sum_{j \in \mathcal{N}_{J,i}} f_{j,\ell}^i(\vec{S}_j^{i^*}) = (1+\epsilon) F_\ell^*,$$

$$\forall\; \ell = 1,2,\ldots,k-1,\; k > 1$$

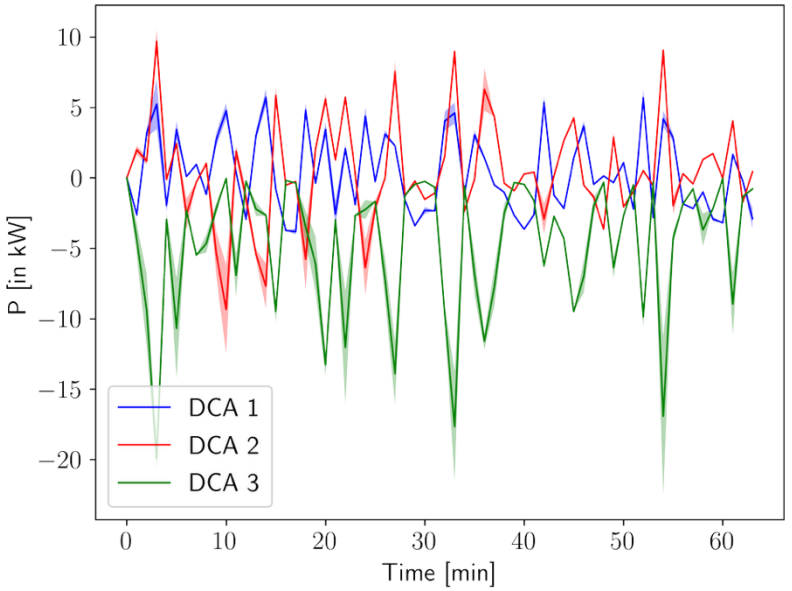
and all other constraints

Results: SM clearing & scheduling

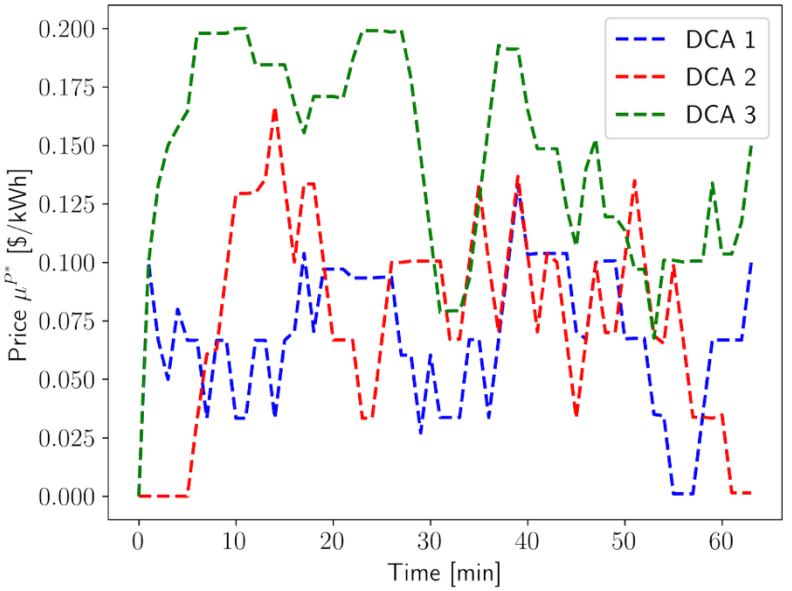
SMA bids into SM at node 7



SMA schedules from SMO 7

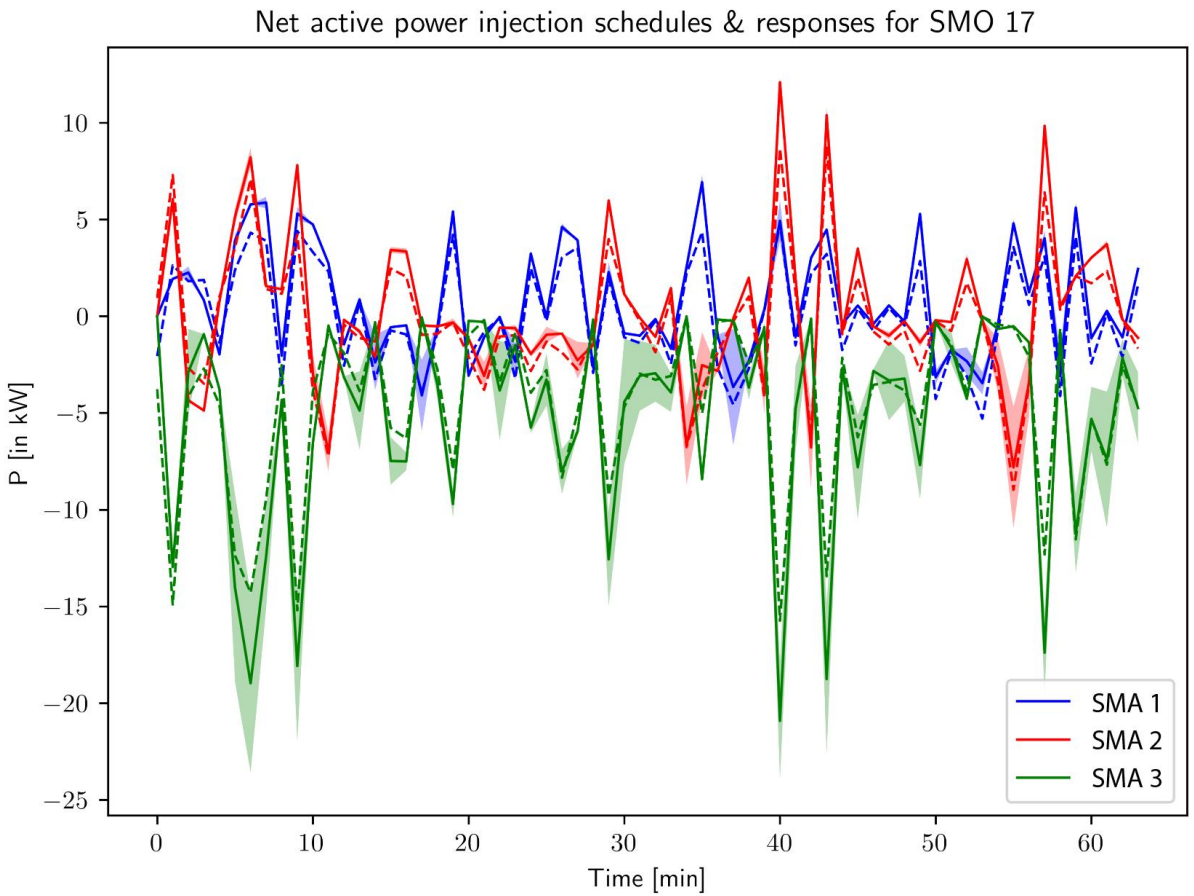


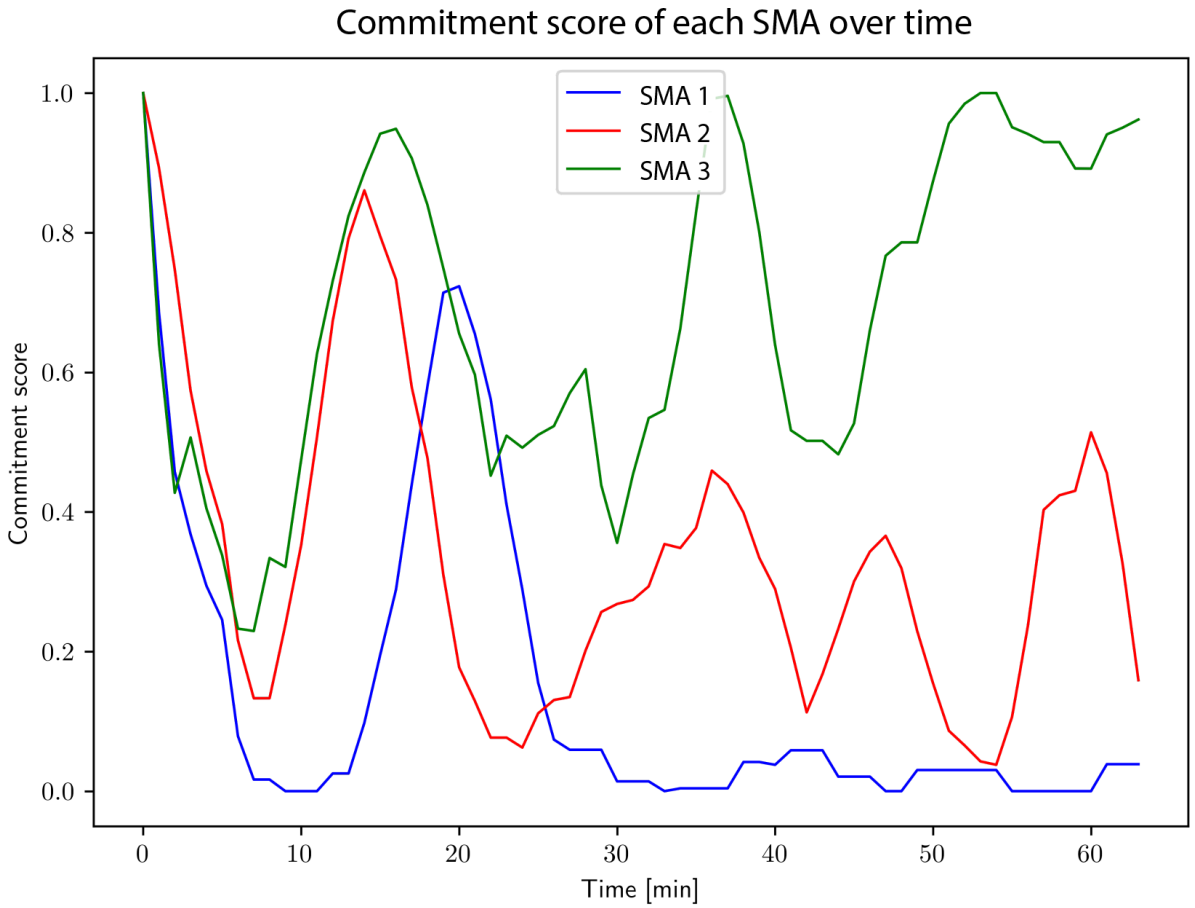
Local retail tariffs



Weighted rolling mean over 5-min primary clearing period to ensure budget balance: $\widetilde{\mu_j^P} = \frac{\sum_{t_s}^{t_s+\Delta t_p} \mu_j^P P_j}{\sum_{t_s}^{t_s+\Delta t_p} P_j} \quad \forall \; SMA\; j$

Actual responses of SMAs → Update commitment scores





Connecting secondary market to primary

- Before each primary clearing period, SMO i aggregates schedules across all of its SMA_j^i from latest secondary clearing
- SMO uses this combined solution to bid into primary market
- Use this to solve ACOPF at primary level to maximize social welfare of SMOs

$$P_i^0(t_p) = \sum_{j \in \mathcal{N}_{J,i}} P_j^{i^*}(t_p - \Delta t_s), Q_i^0(t_p) = \sum_{j \in \mathcal{N}_{J,i}} Q_j^{i^*}(t_p - \Delta t_s)$$

$$\Delta P_i = \left[\underline{P}_i = \sum_{j \in \mathcal{N}_{J,i}} P_j^{i^*} - \delta P_j^{i^*}, \overline{P}_i = \sum_{j \in \mathcal{N}_{J,i}} P_j^{i^*} + \delta P_j^{i^*} \right]$$

$$\Delta Q_i = \left[\underline{Q}_i = \sum_{j \in \mathcal{N}_{J,i}} Q_j^{i^*} - \delta Q_j^{i^*}, \overline{Q}_i = \sum_{j \in \mathcal{N}_{J,i}} Q_j^{i^*} + \delta Q_j^{i^*} \right]$$

$$f^{S-W}(y) = \sum_{i \in \mathcal{N}} \left[f_i^{\text{Load-Disutil}}(y) + f_i^{\text{Gen-Cost}}(y) \right] + \xi \left[\sum_{(ki) \in \mathcal{E}} f_{ki}^{\text{Loss}}(y) \right]$$

$$f_i^{\text{Load-Disutil}}(y) = \beta_i^P (P_i^L - P_i^{L0})^2 + \beta_i^Q (Q_i - Q_i^{L0})^2$$

$$f_i^{\text{Gen-Cost}}(y) = \begin{cases} \alpha_i^P (P_i^G)^2 + \alpha_i^Q (Q_i^G)^2, \\ \lambda_i^P P_i^G + \lambda_i^Q Q_i^G, \text{if } i \quad \text{is PCC} \end{cases}$$

$$f_{ki}^{\text{Loss}}(y) = R_{ki} |I_{ki}|^2$$

Nair, Venkataramanan, Haider, Annaswamy, IEEE Transactions on Smart Grid, 2022.

Primary retail market: Optimal power flow (OPF)

Nonlinear Convex Branch Flow Model (DistFlow)

$$min\ f(x)$$

Subject to:

$$v_j - v_i = \left(R_{ij}^2 + X_{ij}^2\right) l_{ij} - 2\left(R_{ij}P_{ij} + X_{ij}Q_{ij}\right)$$

$$P_{ij} = R_{ij} l_{ij} - P_j + \sum_{k \in \{k_j\}} P_{jk}$$

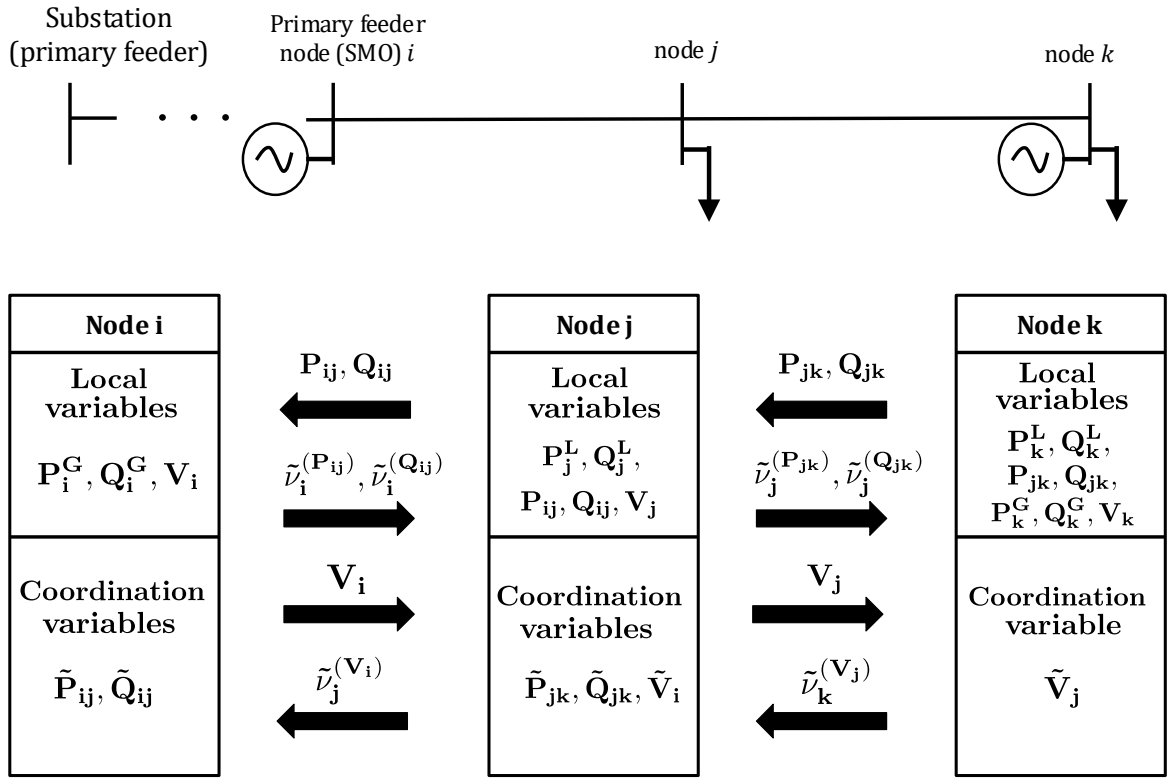
$$Q_{ij} = X_{ij} l_{ij} - Q_j + \sum_{k \in \{k_j\}} Q_{jk}$$

$$P_{ij}^2 + Q_{ij}^2 \leq v_i l_{ij}$$

$$P_j \in [\underline{P_j}, \overline{P_j}],\ Q_j \in \left[\underline{Q_j}, \overline{Q_j}\right],\ v_j \in [\underline{v_j}, \overline{v_j}]$$

where $l_{ij} = \left|I_{ij}\right|^2$ *and* $v_i = |V_i|^2$.

Valid for radial & balanced networks



- Decompose global optimization into smaller subproblems ('atoms') for each node in network
- Atoms only communicate with their immediate neighbors
- Fully distributed, more computationally tractable
- More resilient against communication failures/hacks (compared to centralized)

J. Romvary, G. Ferro, R. Haider, and A.M. Annaswamy. "A distributed proximal atomic coordination algorithm." IEEE Transactions on Automatic Control, 2021.

Distributed optimization approach

Global problem

$$\min_x \sum_{i=1}^{S} f_i(x) \text{ s.t. } Gx = b, \quad Hx \leq d$$

Atomized problem
(decomposed into atoms *j*)

$$\min_{a_j} \sum_{j \in K} f_j(a_j)$$

$$\text{s.t. } G_j a_j = b_j, \; H_j a_j \leq d_j, \; B_j a = 0 \; \forall j \in K$$

Coordination or consensus constraints

$$B_{im} \triangleq \begin{cases} -1, & \text{if } i \text{ is 'owned" and } m \text{ a related "copy"} \\ 1, & \text{if } m \text{ is "owned" and } i \text{ a related "copy"} \\ 0, & \text{otherwise} \end{cases}$$

Augmented Lagrangian

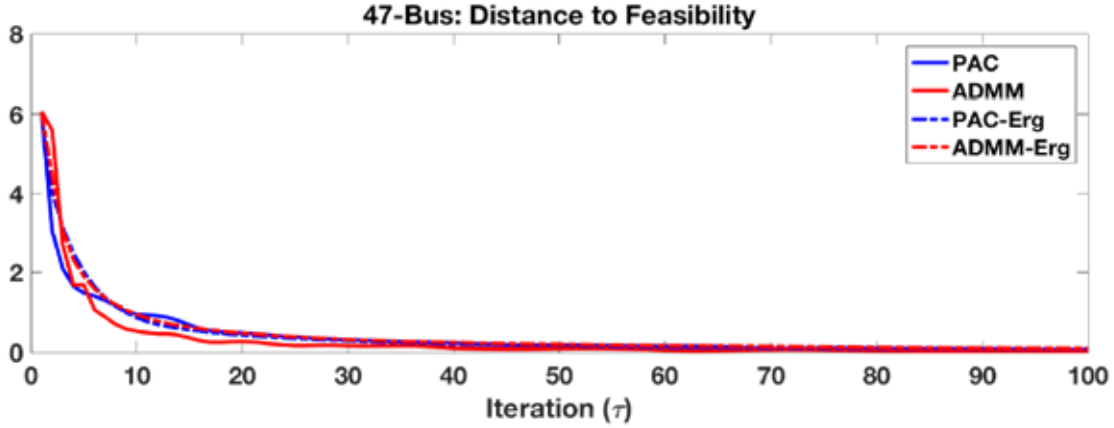
$$\begin{aligned} \mathcal{L}(a, \eta, \nu) &= \sum_{j \in K} \left[f_j(a_j) + \eta_j^T (G_j a_j - b_j) + \nu_j^T B_j a \right] \\ &= \sum_{j \in K} \left[f_j(a_j) + \eta_j^T (G_j a_j - b_j) + \nu^T B^j a_j \right] \\ &\triangleq \sum_{j \in K} \mathcal{L}_j(a_j, \eta_j, \nu) \end{aligned}$$

Distributed optimization: NST-PAC

- Primal-dual method based on Proximal Atomic Coordination (PAC)

$$
\begin{aligned}
a_j[\tau+1] &= \underset{a_j}{\operatorname{argmin}}\Big\{\mathcal{L}_j\left(a_j, \hat{\eta}_j[\tau], \hat{\nu}[\tau]\right) \\
&\quad + \frac{\rho_j\gamma_j}{2}\left\|G_j a_j - b_j\right\|_2^2 + \frac{\rho_j\gamma_j}{2}\left\|B_j a_j\right\|_2^2 \\
&\quad + \frac{1}{2\rho_j}\left\|a_j - a_j[\tau]\right\|_2^2\Big\} \qquad (5)\\
\hat{a}_j[\tau+1] &= a_j[\tau+1] + \alpha_j[\tau+1]\left(a_j[\tau+1] - a_j[\tau]\right)\\
\eta_j[\tau+1] &= \hat{\eta}_j[\tau] + \rho_j\gamma_j\left(G_j\hat{a}_j[\tau+1] - b_j\right)\\
\hat{\eta}_j[\tau+1] &= \eta_j[\tau+1] + \phi_j[\tau+1]\left(\eta_j[\tau+1] - \eta_j[\tau]\right)\\
&\text{Communicate } \hat{a}_j \text{ for all } j \in [K] \text{ with neighbors}\\
\nu_j[\tau+1] &= \hat{\nu}_j[\tau] + \rho_j\gamma_j B_j\hat{a}_j[\tau+1]\\
\hat{\nu}_j[\tau+1] &= \nu_j[\tau+1] + \theta_j[\tau+1]\left(\nu_j[\tau+1] - \nu_j[\tau]\right)\\
&\text{Communicate } \hat{\nu}_j \text{ for all } j \in [K] \text{ with neighbors}
\end{aligned}
$$

Convergence plot: Satisfying global constraints



- Convergence speed increased by using time-varying gains & Nesterov-accelerated gradient updates
- Further protects privacy by masking both primal and dual variables

Attack mitigation via distributed market-based coordination

- We focus on disruption (or denial-of-service) attacks that take one or more distributed generators offline
- PMO does not have direct control over any SMOs
- PMO doesn't have visibility over each SMO's injections

- PMO only monitors the feeder's net total power injection at substation (point of common coupling) = P_{PCC}
- Attack changes net injection → P'_{PCC}

- PMO artificially modifies coefficients in objective function from $\{\alpha_i, \beta_i, \xi\}$ to $\{\alpha'_i, \beta'_i, \xi'\}$
- PM redispatch with new, re-weighted objective → Optimally redispatches PM to mitigate attack

$$\sum_{i=1}^{n} \left(\frac{1}{2} \alpha_i P_i^{G^2} + \beta_i \left(P_i^L - P_i^{L0} \right)^2 \right) + \xi \cdot losses$$

$$\alpha'_i = \Delta_\alpha \alpha_i,\ \beta'_i = \Delta_\beta \beta_i,\ \xi' = \Delta_\xi \xi;\ \alpha, \beta, \xi, \Delta > 0$$

$$\Delta_\alpha = \Delta_\beta = \frac{|P_{PCC}|}{|P'_{PCC}|},\ \Delta_\xi = \frac{|P'_{PCC}|}{|P_{PCC}|}$$

Intuition behind coefficient updates

Suppose several local DGs are attacked → Increases net feeder load i.e. $|P'_{PCC}| > |P_{PCC}|$
This would result in the following coefficient updates:

1. $\Delta_\alpha < 1$: Lower cost coefficients to dispatch more local generation from remaining online SMOs instead of importing power from WEM

2. $\Delta_\beta < 1$: Reduce disutility coefficients to encourage demand response via load shifting/curtailment

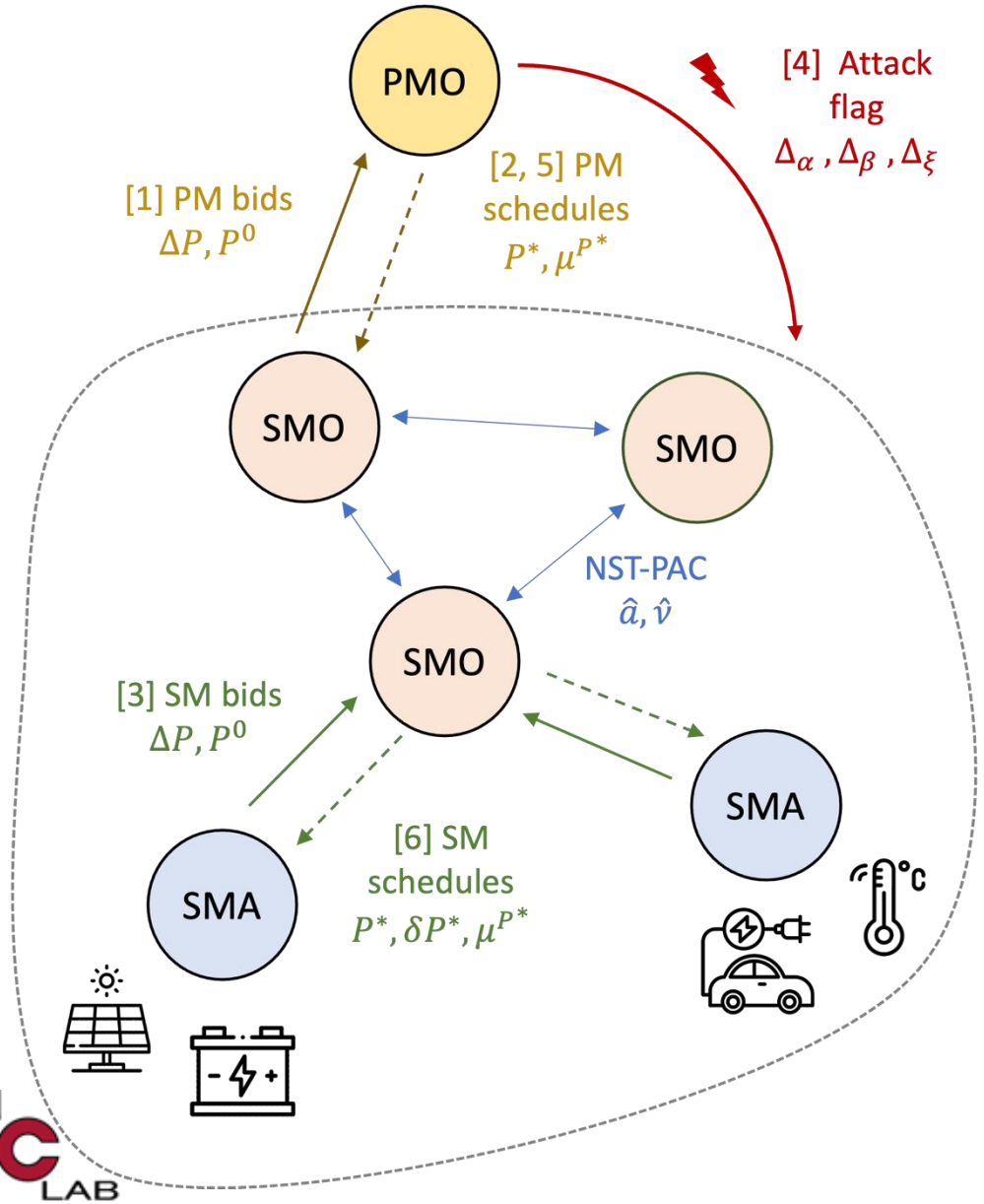
3. $\Delta_\xi > 1$: Penalize electrical line losses more heavily → Discourages imports from transmission grid in favor of dispatching more local DERs closer to the loads being served.

$$\sum_{i=1}^{n} \left(\frac{1}{2}\, \alpha_i P_i^{G^2} + \beta_i \left(P_i^L - P_i^{L0} \right)^2 \right) + \xi \cdot losses$$

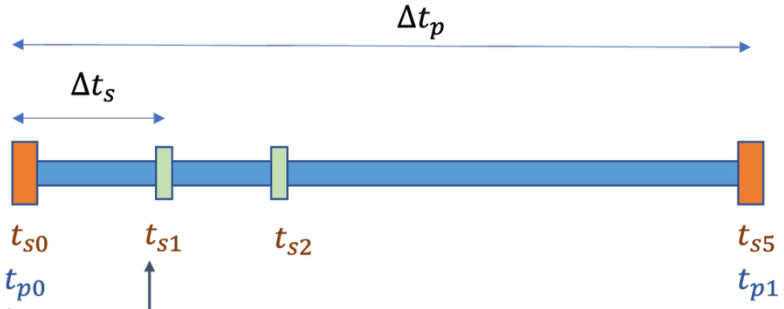
$$\alpha'_i = \Delta_\alpha \alpha_i,\ \beta'_i = \Delta_\beta \beta_i,\ \xi' = \Delta_\xi \xi;\ \alpha, \beta, \xi, \Delta > 0$$

$$\Delta_\alpha = \Delta_\beta = \frac{|P_{PCC}|}{|P'_{PCC}|},\ \Delta_\xi = \frac{|P'_{PCC}|}{|P_{PCC}|}$$

SM & PM response for all attacks



Mitigation involves both SM & PM redispatch

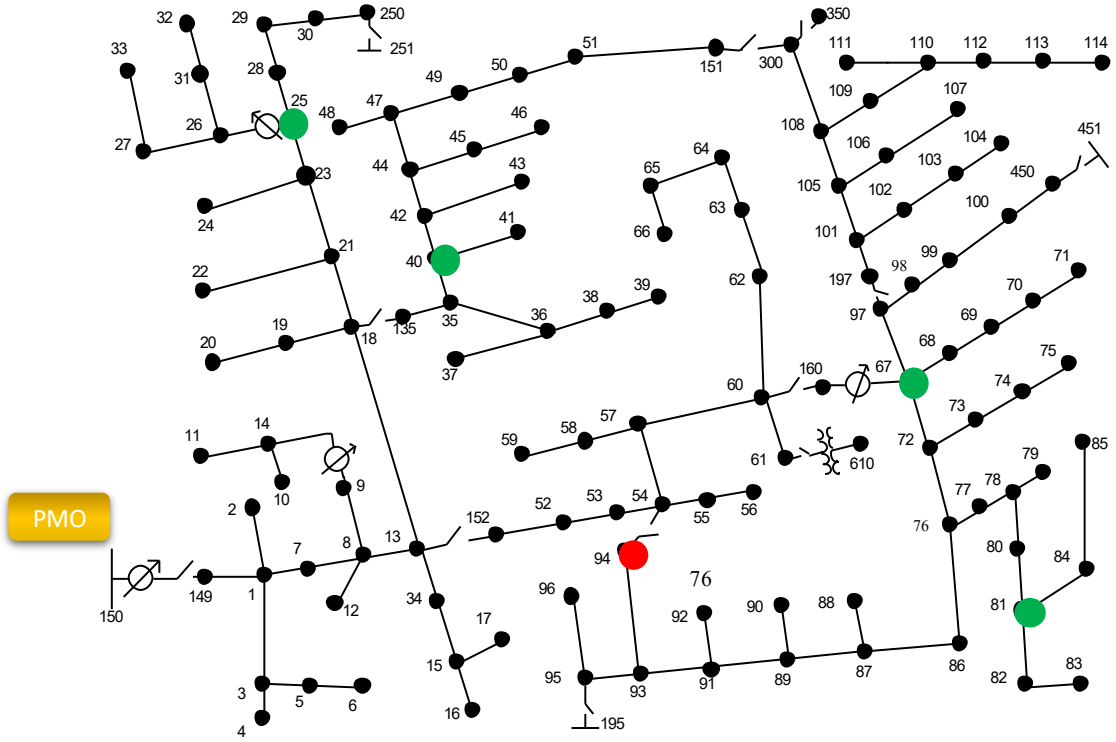


6. SM redispatch with new PM solution: SMOs disaggregate new setpoints amongst their SMAs within their flex bids for $[t_{s1}, t_{s2}]$

3. SMAs submit bids for $[t_{s1}, t_{s2}]$
4. SMO attacked
5. Mitigation:
   - PMO broadcasts cost coefficient updates to all SMOs
   - PM redispatches all SMOs for $[t_{s1}, t_{p1}]$ (within their flexibility limits)

1. SMOs submit flexibility bids for $[t_{p0}, t_{p1}]$
2. PMO clears all SMOs for $[t_{p0}, t_{p1}]$

Results: Medium-scale attack with mitigation



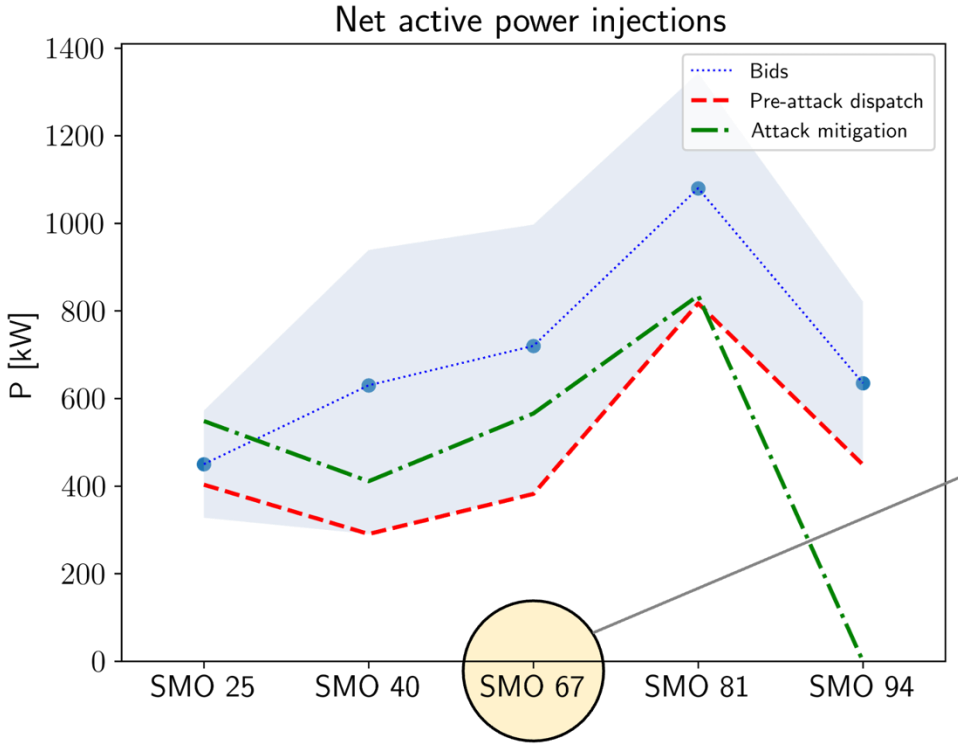
We simulate a single time step of the dispatch to focus on the instantaneous effects of the attack

1. Attack 1 large generator
   → Total of 261 kW generation loss
2. PMO alerts other trustable SMOs to redispatch their generation assets
3. SMOs redispatch SMAs who provide correct setpoints
4. Total import from the main grid stays at the same level

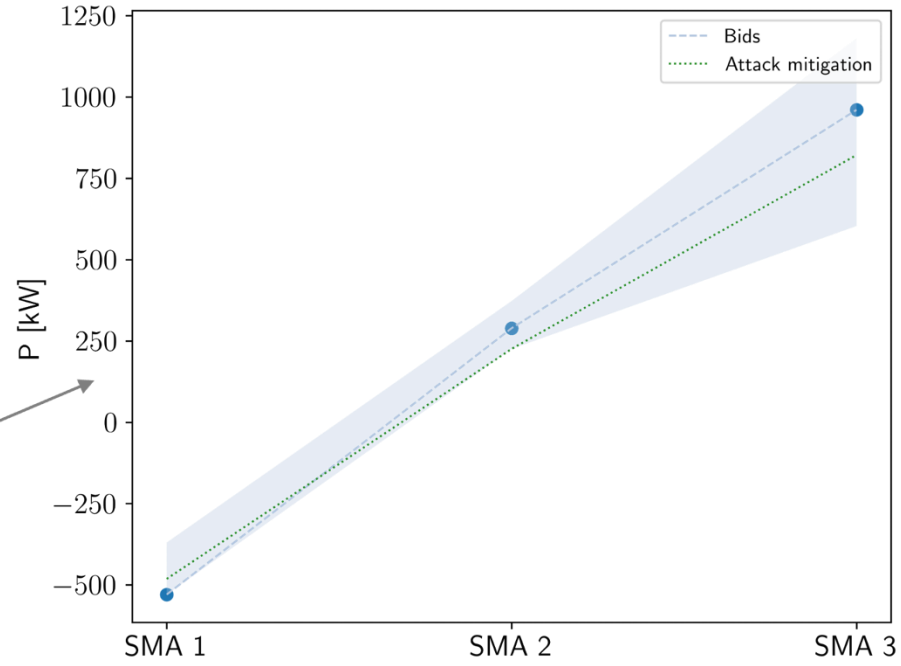
● : Attacked nodes

● : Trustable nodes with generators

Mitigation of medium-scale attack



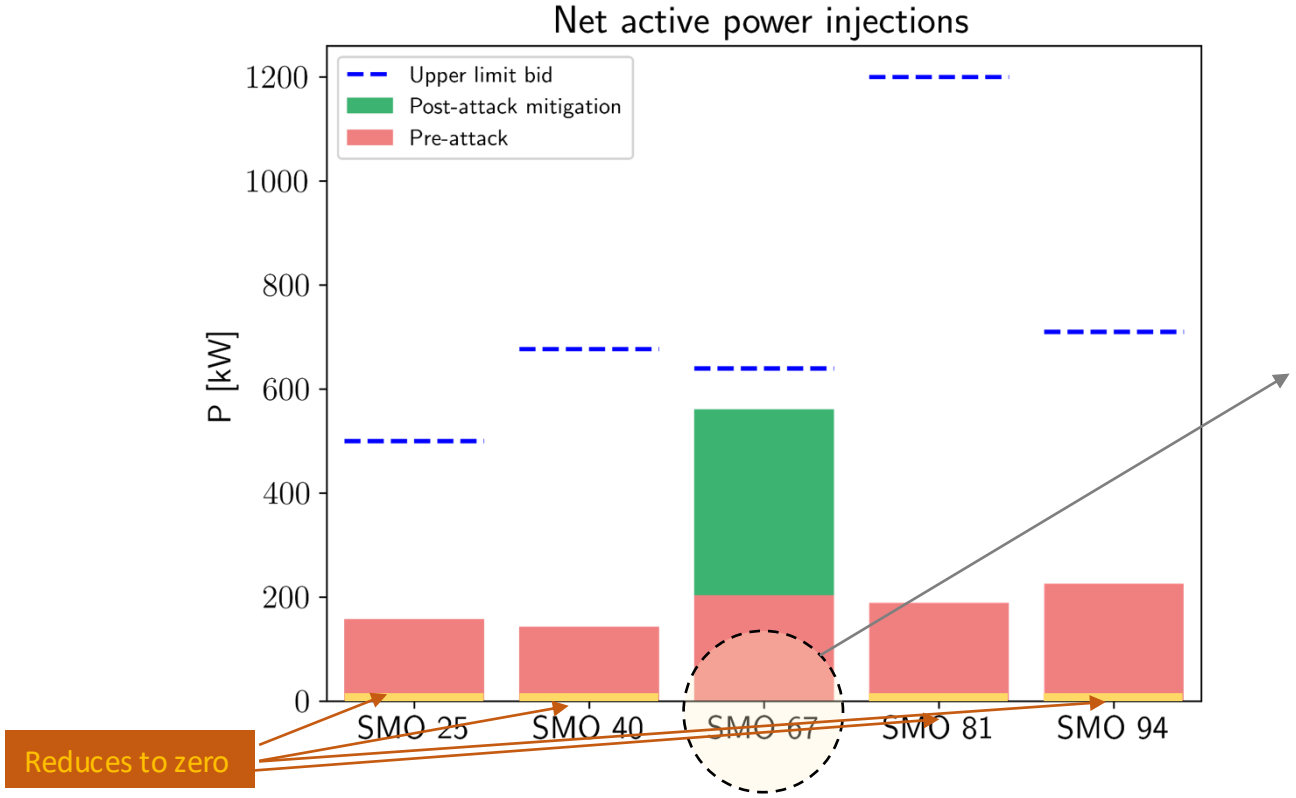
Changes in dispatch at key primary nodes



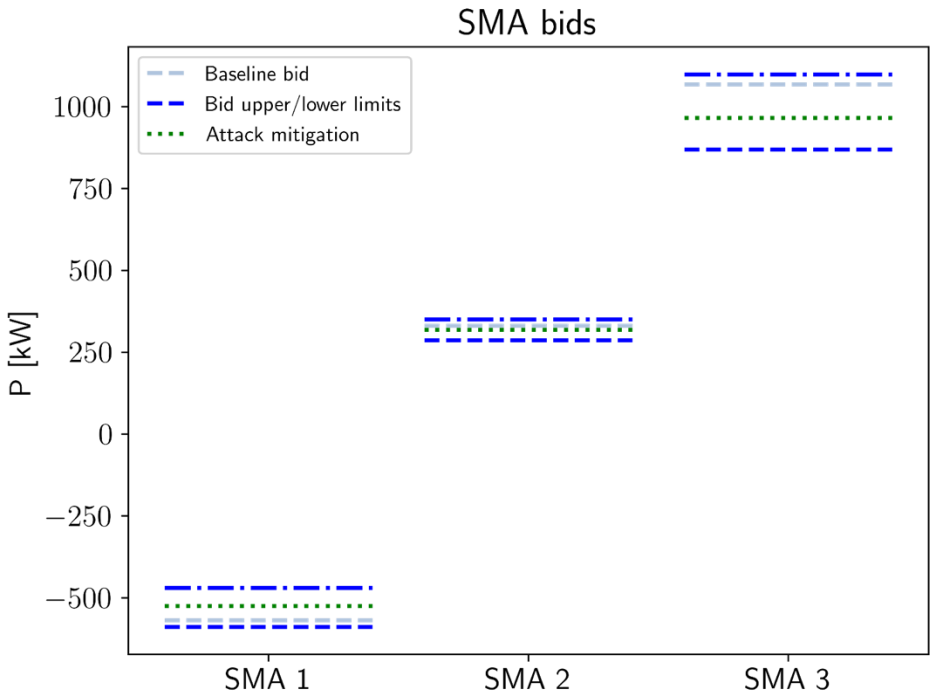
Disaggregation of new primary node setpoints across secondary feeders

- Attack @ node 94 increases power import from grid by **261 kW**
- Mitigation reduces total power imported back to pre-attack levels

Results: Large scale attack with mitigation



Changes in dispatch at key primary nodes

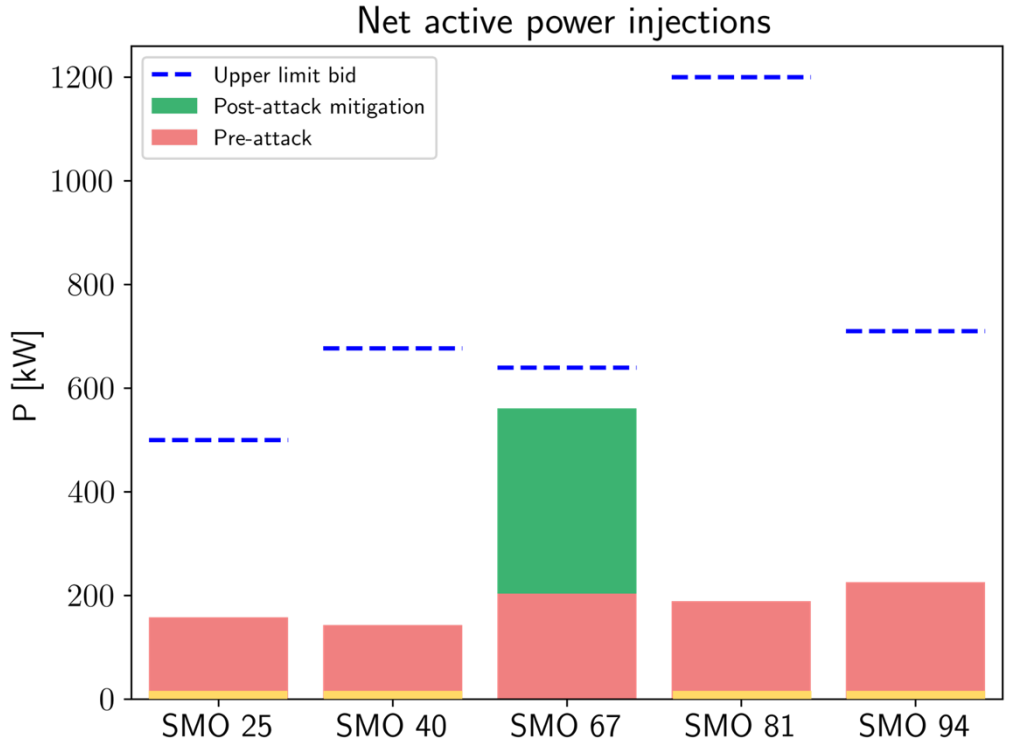


Disaggregation of new primary node setpoints across secondary feeders

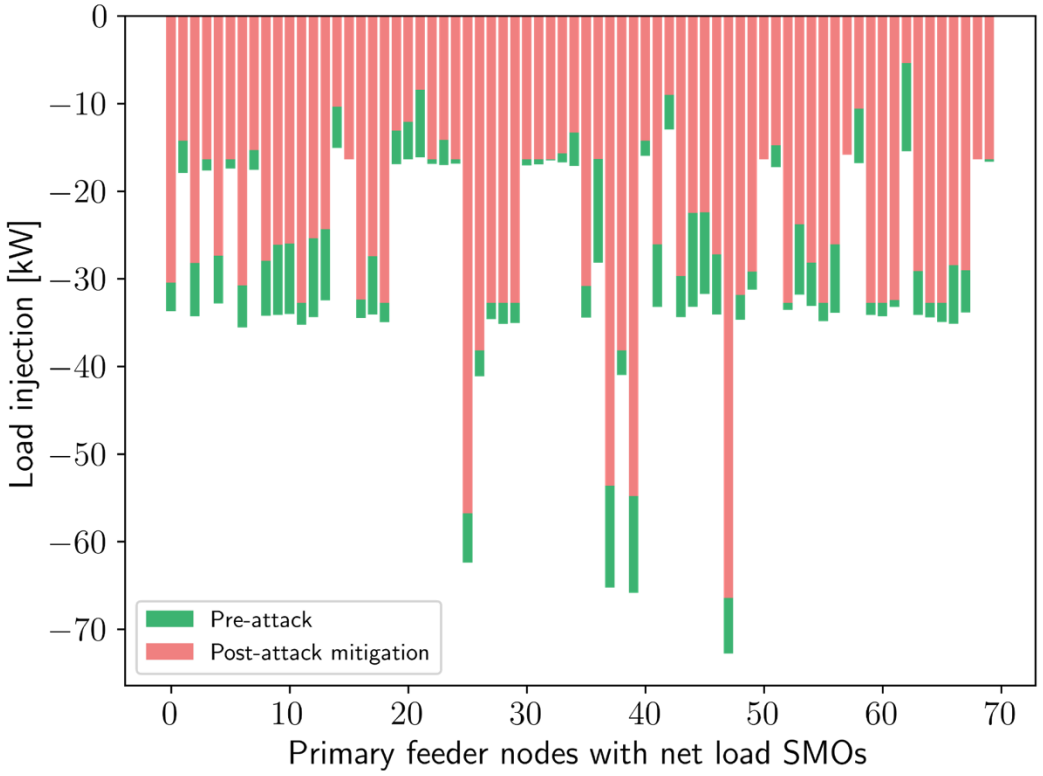
- 4 generators attacked: At nodes 25, 40, 81, 94
  - Physical outage → All drop to zero (641 kW generation loss)
  - Cyber attack → Communication with Market Operator compromised
- Leverage available upward flexibility of remaining generator at SMO 67
- Increase in generator output is limited by power flow/network constraints

Leverage load flexibility to fully resolve attack

In addition to utilizing extra generation flexibility, we also need to shift/curtail some of the remaining flexible loads

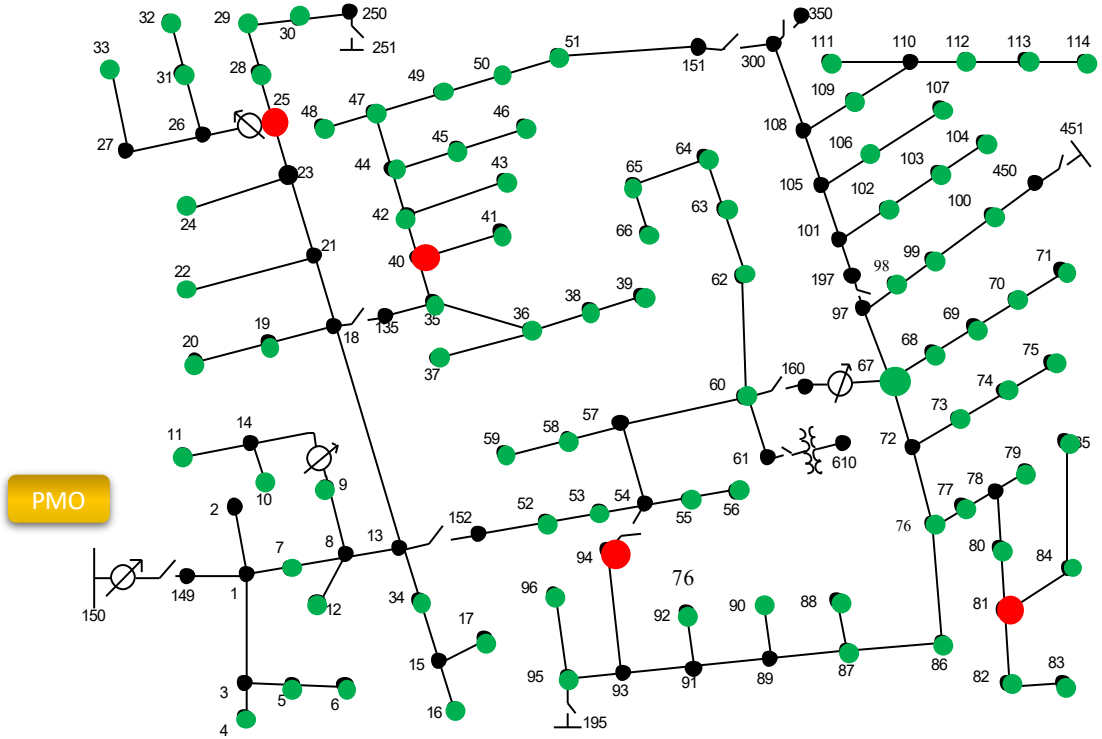


Generation flexibility



Demand response flexibility

Large-scale attack mitigation summary



1. A total of 641 kW generation loss
2. PMO alerts other trustable PMAs/SMOs to redispatch their generation assets
3. Trustable PMAs/SMOs will curtail flexible loads to respond & mitigate attack
4. SMOs redispatch SMAs who provide correct setpoints
5. Total import from the main grid stays at the same level

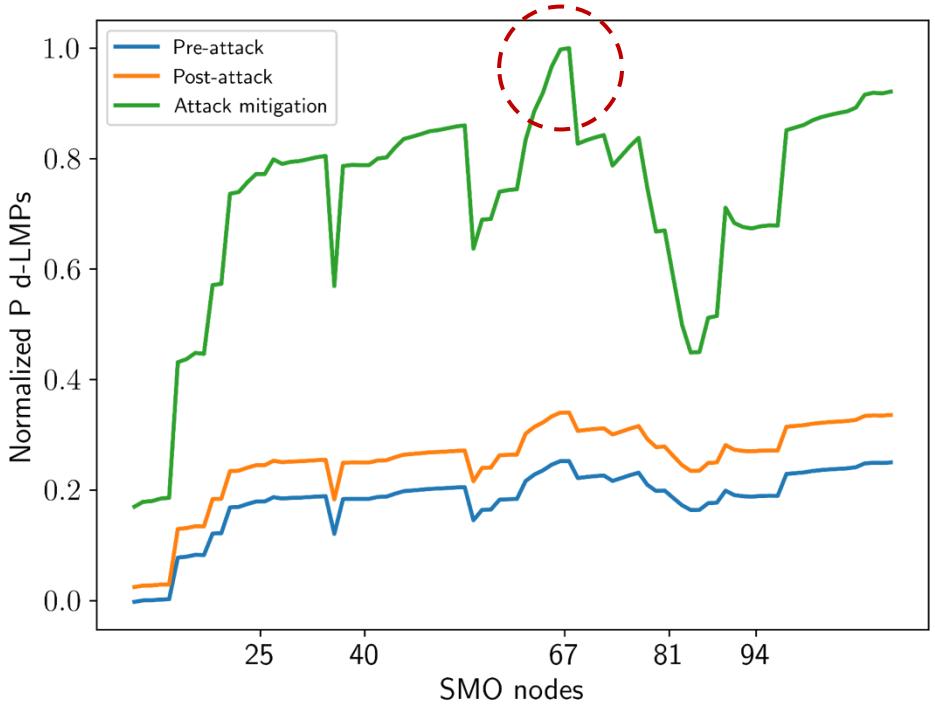
82 flexible load nodes respond

: Attacked Nodes

: Trustable EUREICA-Nodes

Large scale attack system impacts

	Pre-attack	Post-attack	Attack mitigation
Power import from main grid [kW]	1,325	1,821 (+37.4%)	1,328
Total cost [$]	10,752	11,500 (+7%)	14,156 (+31.7%)
Total load [kW]	2,064	2,023 (-0.02%)	1,775 (-14%)



1. Loss of **641 kW** of local generation
2. Without mitigation, this would lead to a large increase in power import of **600 kW**
3. Mitigation 1st utilizes upward flexibility to increase local generation by **284 kW**
4. Then curtails flexible loads by **307 kW**
5. Mitigation minimizes extra power import to only 3 kW
6. Mitigation comes at an increased cost to PMO
   → Need to compensate resources for their flexibility

Conclusions & future work

- First work to leverage electricity markets to provide resilience against cyber-physical attacks on the grid
- Applied a novel hierarchical local electricity market structure to coordinate distributed energy resources
- Modify optimization objective function coefficients to re-dispatch markets and successfully mitigate disruption attacks
- Reduce extra power imports → Minimize reliance on external main grid
- Locally mitigate distribution system attacks → Prevents effects on transmission
- Future work
  - Adapt our framework for other types of attacks e.g. deception, disclosure
  - Extend to other types of meshed, unbalanced distribution grids
  - Consider even larger, more distributed attacks

aac LAB