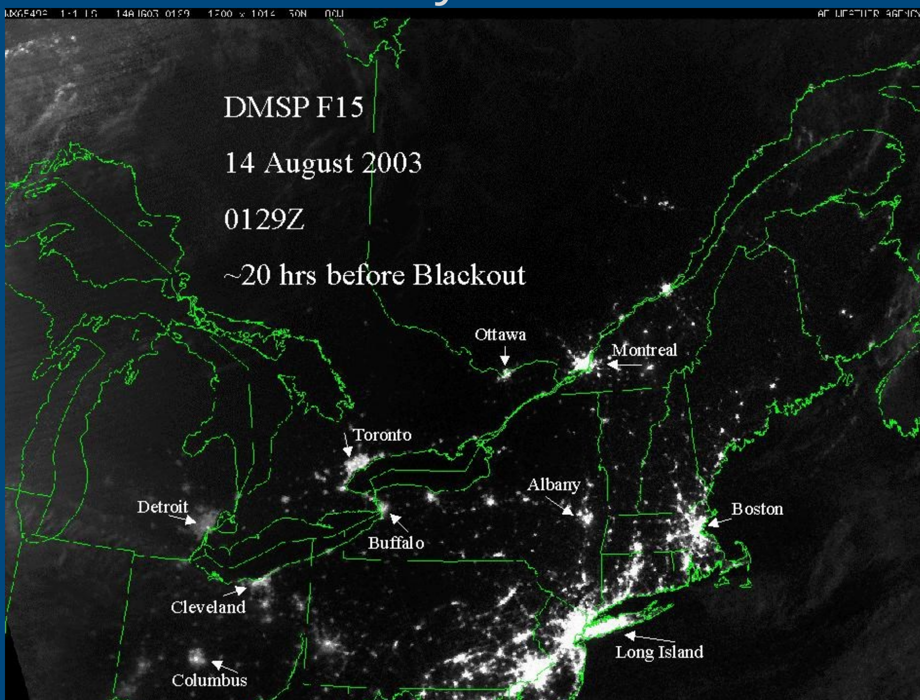
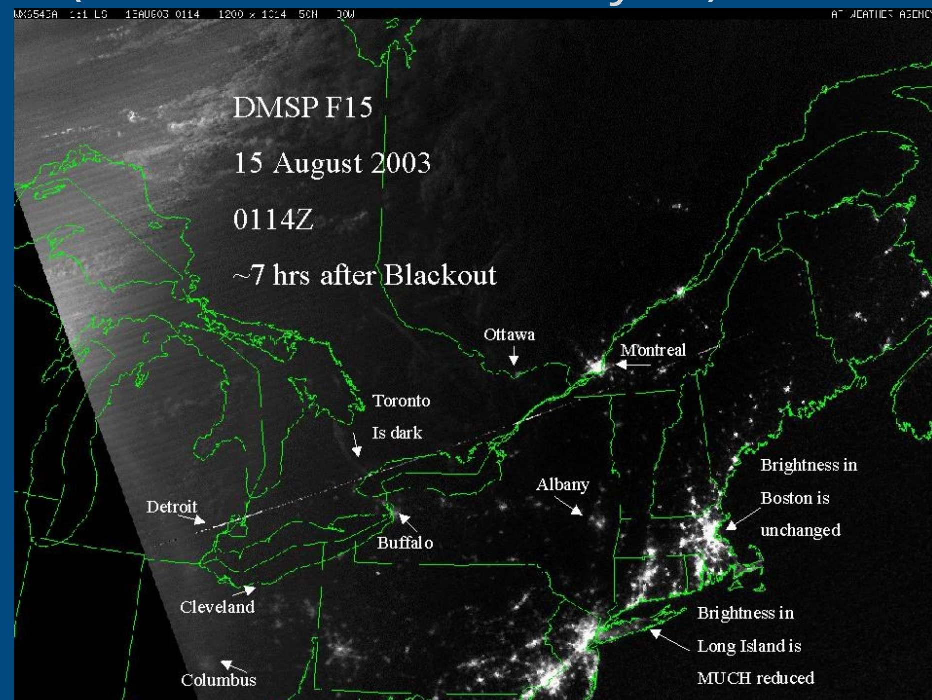
Joint Cyber and Physical Attacks on Power Grids: Graph Theoretical Approaches for Information Recovery

Saleh Soltan[1], Mihalis Yannakakis[2], Gil Zussman[1]
[1]Electrical Engineering, [2]Computer Science
Columbia University, New York, NY

Failures in Power Grids

- Power grids rely on physical infrastructure → Vulnerable to physical attacks/failures
- Failures may cascade → Blackouts (US'03, India'12, Turkey'15)

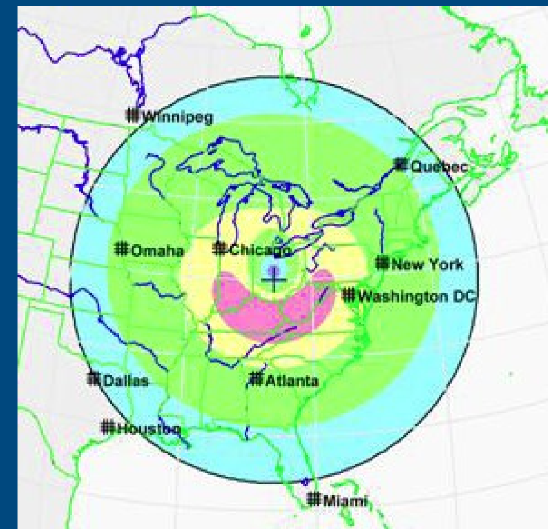




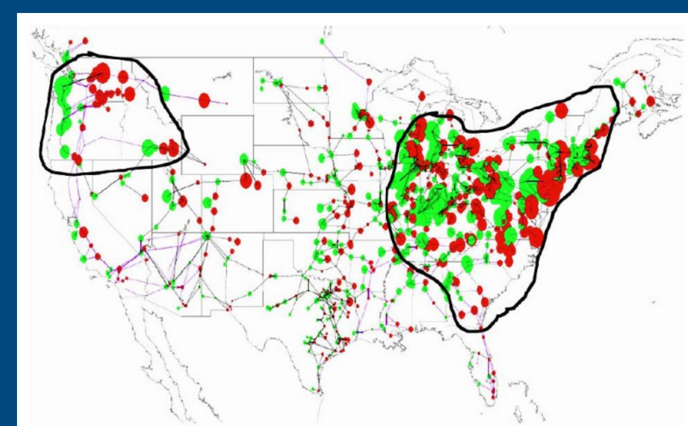
- An attack/failure will have a significant effect on many interdependent systems (communications, transportation, gas, water, etc.)

Physical Attacks/Disasters

- EMP (Electromagnetic Pulse) attack
- Solar Flares - Federal Energy Regulatory Commission (FERC) has recently issued a rule for transmission grid operators to develop a plan to deal with the Geomagnetic disturbances



Source: Report of the Commission to Assess the threat to the United States from Electromagnetic Pulse (EMP) Attack, 2008



FERC, DOE, and DHS, Detailed Technical Report on EMP and Severe Solar Flare Threats to the U.S. Power Grid, 2010

- Other natural disasters
- Physical attacks

Power Grid Attack in San Jose

- “A sniper attack in April 2014 that knocked out an electrical substation near San Jose, Calif., has raised fears that the country's power grid is vulnerable to terrorism. ” –The Wall Street Journal

Shots in the Dark

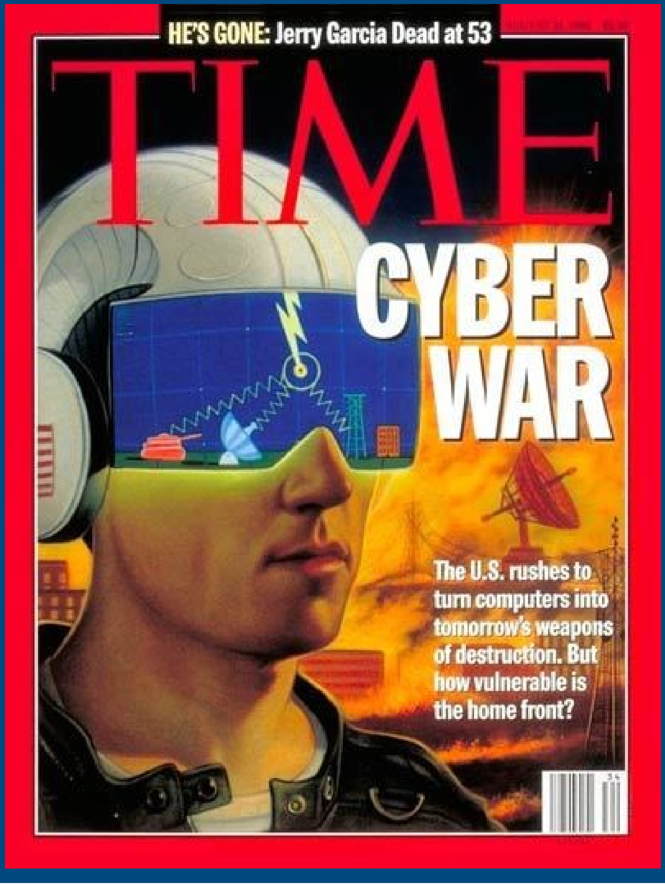
A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1	2	3	4	5	6	7
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can't enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

Cyber Attacks on Control Network

- Federal and industry officials told Congress recently, "The U.S. electrical power grid is vulnerable to cyber and physical attacks that could cause devastating disruptions throughout the country." *The Washington Times 4/16/2014*



Joint cyber and physical attacks

Physical Attack Target

Commands

Data

Cyber Attack Target

Power Grid
Physical Infrastructure

Supervisory Control and Data Acquisition (SCADA) system

Power Flow Equations - DC Approximation

- A power flow is a solution (f, θ) of:

$$\sum_{v \in N(u)} f_{uv} = p_u\,, \qquad \forall\, u \in V$$

$$\frac{\theta_u - \theta_v}{x_{uv}} = f_{uv}, \qquad \forall\, \{u, v\} \in E$$

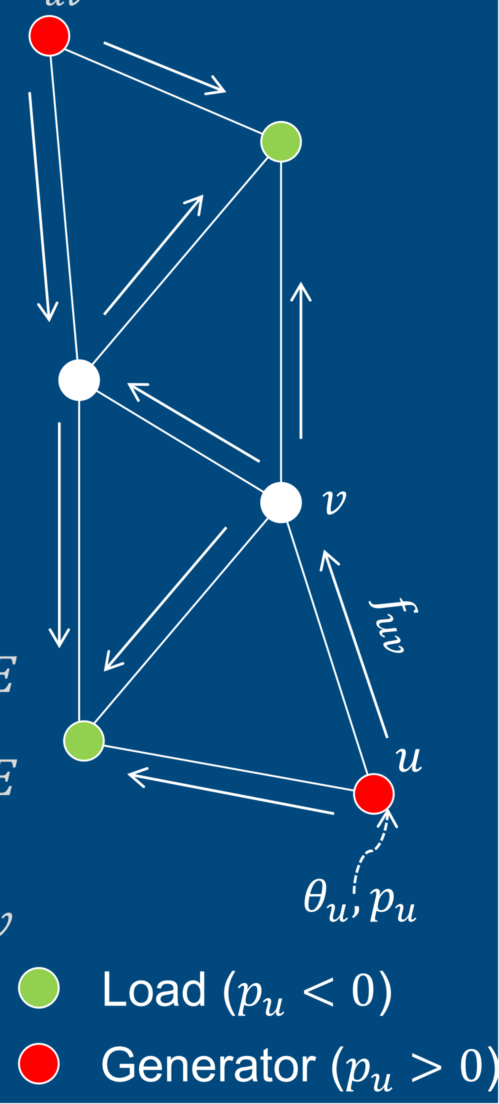
- Matrix form:

$$A\vec{\theta} = \vec{p}$$

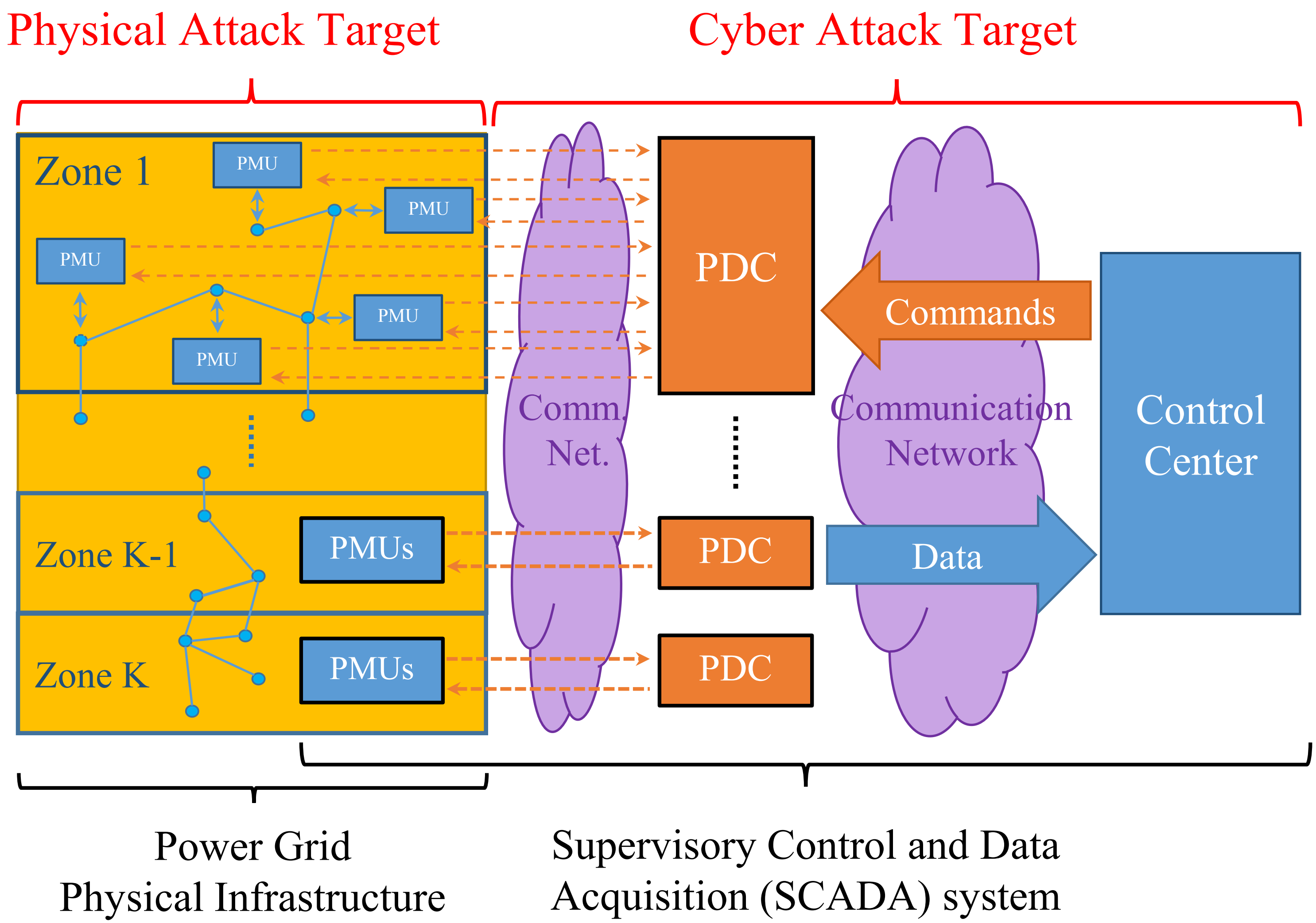
A is the **admittance matrix** of the grid defined as:

$$a_{uv} = \begin{cases} 0, & u \neq v \text{ and } \{u, v\} \notin E \\ -\dfrac{1}{x_{uv}}, & u \neq v \text{ and } \{u, v\} \in E \\ -\displaystyle\sum_{w \in N(u)} a_{vw}\,, & u = v \end{cases}$$

θ_u: Phase Angle
x_{uv}: Reactance



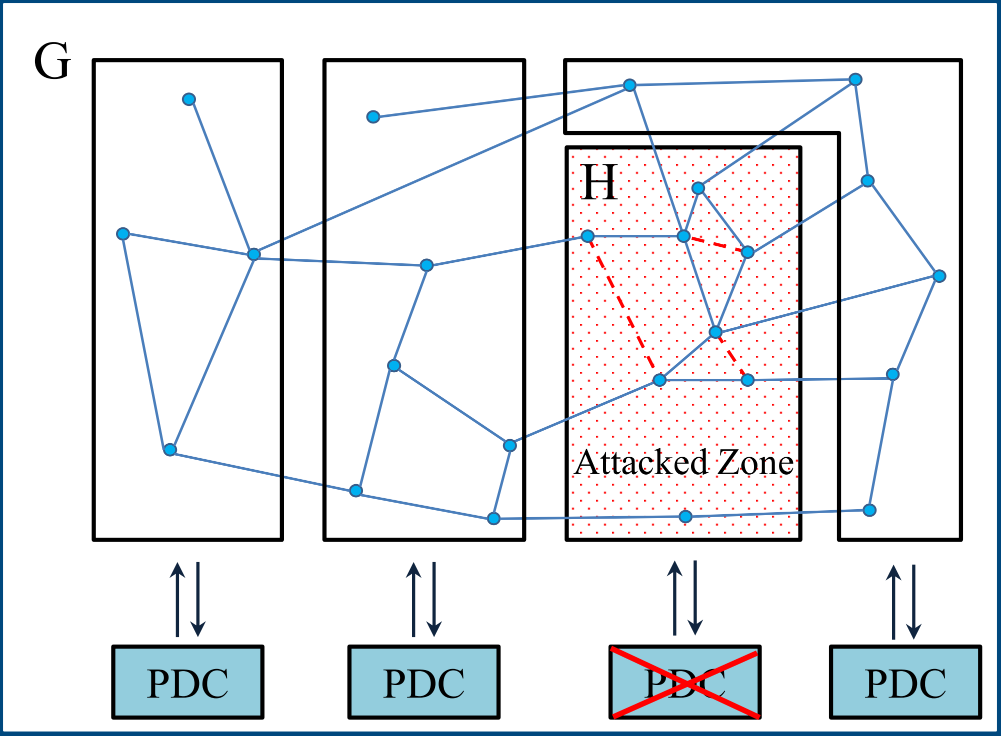
Control Network



PMU: Phasor Measurement Unit
PDC: Phasor Data Concentrators

Attack Model

- An adversary attacks a zone by
  - Disconnecting some edges within the attacked zone (physical attack)
  - Disallowing the information from the PMUs within the zone to reach the control center (cyber attack)
- Use the information available outside of the attacked zone and the information before attack
  - *Recover the phase angles*
  - *Detect the disconnected lines*

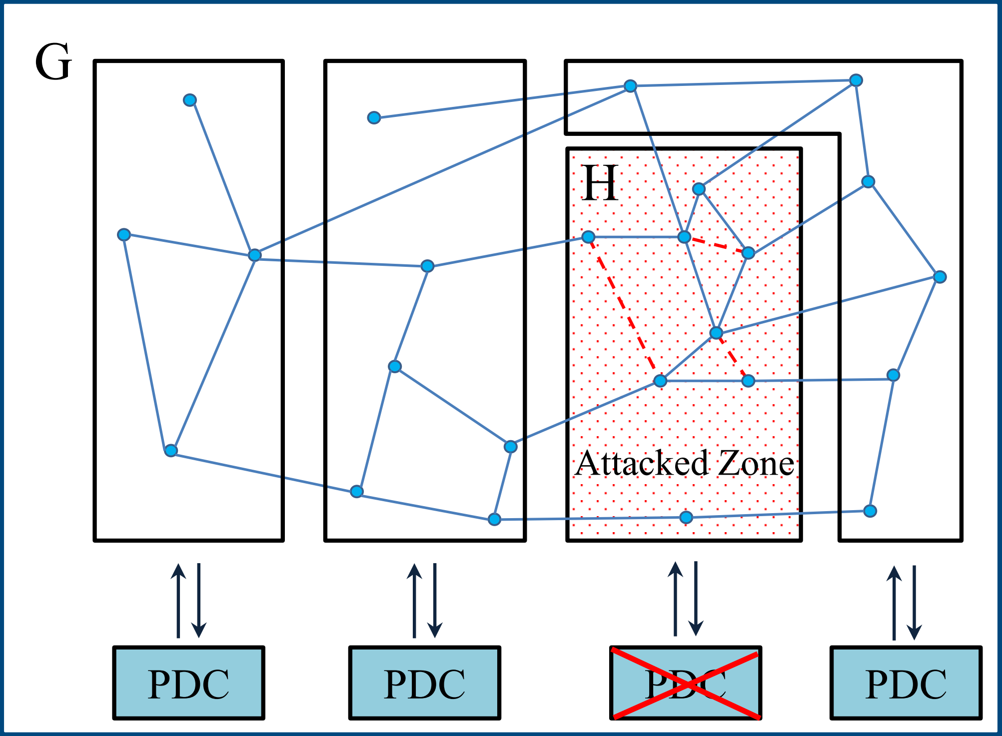


Objectives:

- Identify conditions on zones for which this can be done
  - External Conditions
  - Internal Conditions
- Develop algorithms to partition the network into attack resilient zones

Notation

- H : an induced subgraph of G that represents the attacked zone
- $\overline{H} = G \backslash H$
- $A = \begin{bmatrix} A_{\overline{H}|\overline{H}} & A_{\overline{H}|H} \\ A_{H|\overline{H}} & A_{H|H} \end{bmatrix}$
- $\vec{\theta} = \begin{bmatrix} \vec{\theta}_{\overline{H}} \\ \vec{\theta}_{H} \end{bmatrix}$
- F : Set of failed edges
- O′ : The value of O after an attack



- Our Problem: $\boxed{A\,, \vec{\theta}\,, \vec{\theta}'_{\overline{H}}\,, A'_{\overline{H}|\overline{H}}\,, A'_{\overline{H}|H}}$ ✓

$\boxed{\vec{\theta}'_{H}\,, A'_{H|H}}$ ✗

Related Work

- Vulnerability of networks to attacks was thoroughly studied
  - Percolation Theory and epidemics (Barabasi, Kleinberg, Havlin, etc.)
- Cascading failures in power grid
  - Probabilistic Models (Albert, Buldryev, Stanly, Havlin, etc.)
  - DC power flows (Dobson, Hines, Bienstock, Pinar, etc.)
- Malicious data attacks on the power grid control network
  - False data injection (Sandberg, L. Tong, etc.)
  - Modifying the topology estimate of the grid (L. Tong et. al. 2013)
- Line outage detection from the phase angle measurements
  - Single or double line failures (Tate, Overbye 2009)
  - Heuristic line failure identification in an internal system using the information from an external system (Giannakis et.al. 2012)
  - PMU Location Selection for Line Outage Detection (A. Goldsmith et. al. 2012)

Outline of our approach

Method for
Recovery of phase angles
(External Conditions)

$\vec{\theta}'$

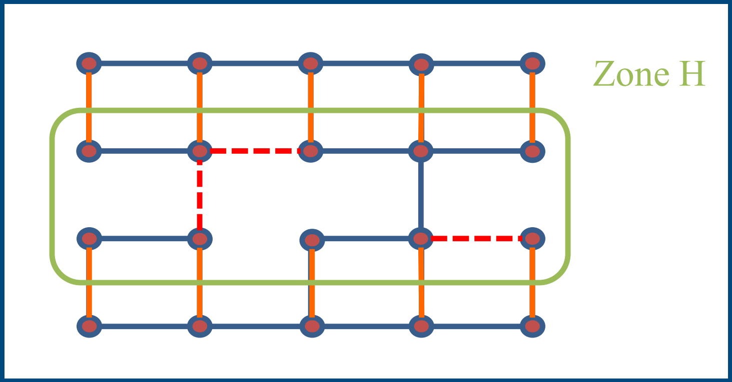
Method for
Failed edges detection
(Internal Conditions)

Method for
Simultaneous
phase angles recovery
and failed edges detection

Less constraints on the graph structure
More constraints on F

Recovery of Phase Angles

- *Theorem.* $\vec{\theta}'_H$ can be recovered after any attack on H, if $A_{\overline{H}|H}$ has linearly independent columns.
- *Corollary.* $\vec{\theta}'_H$ can be recovered almost surely if there is a matching between the nodes inside and outside of H that covers V_H.



- *Idea of the proof.*

$$\begin{cases} A\vec{\theta} = \vec{p} \\ A'\vec{\theta}' = \vec{p} \end{cases} \Rightarrow supp\left(A(\vec{\theta} - \vec{\theta}')\right) \subseteq V_H \Rightarrow A_{\overline{H}|G}(\vec{\theta} - \vec{\theta}') = 0 \Rightarrow$$

$$\Rightarrow \boxed{A_{\overline{H}|H}\vec{\theta}'_H = A_{\overline{H}|G}\vec{\theta} - A_{\overline{H}|\overline{H}}\vec{\theta}'_{\overline{H}}}$$

Outline of our approach

Method for
Recovery of phase angles
(External Conditions)

$\vec{\theta}'$

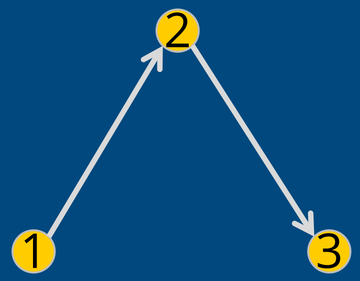
Method for
Failed edges detection
(Internal Conditions)

Incidence Matrix

- Assign an arbitrary orientation to the edges of G
- Denote the set of oriented edges by $\mathrm{E} = \{\epsilon_1, \dots, \epsilon_m\}$
- With this orientation, the (node-edge) incidence matrix of G is denoted by $D \in \mathbb{R}^{n \times m}$ and defined as follows,

$$d_{ij} = \begin{cases} 1, & \text{if } \epsilon_j \text{ is coming out of node } \mathrm{i} \\ -1, & \text{if } \epsilon_j \text{ is going into node } \mathrm{i} \\ 0, & \text{if } \epsilon_j \text{ is not incident to node } \mathrm{i} \end{cases}$$

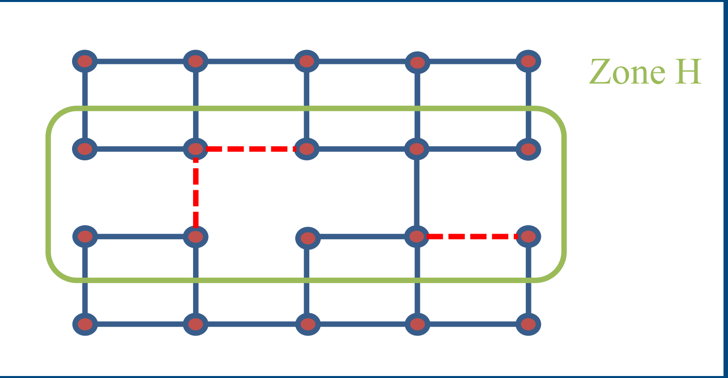
$$D = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix}$$



Detecting Failed Edges

- *Lemma*. There exists a vector $\vec{x} \in \mathbb{R}^{|E_H|}$ such that
$$D_H\vec{x} = A_{H|G}\left(\vec{\theta} - \vec{\theta}'\right)$$
and $supp(\vec{x})$ gives indices of the failed edges.
- *Lemma*. The solution $\vec{x}$ is unique, if and only if H is acyclic.

Failed edges can be detected, if H is acyclic



- The topology can be less restrictive, if we restrict the attack (sparse)

$$\boxed{\min \parallel \vec{x} \parallel_1 \ \ s.t.\ D_H\vec{x} = A_{H|G}(\vec{\theta} - \vec{\theta}')} \qquad (*)$$

- *Lemma*. If H is a cycle and less than half of the edges are failed, then the solution $\vec{x}$ to $(*)$ is unique and $supp(\vec{x})$ gives indices of the failed edges.

Detecting Failed Edges

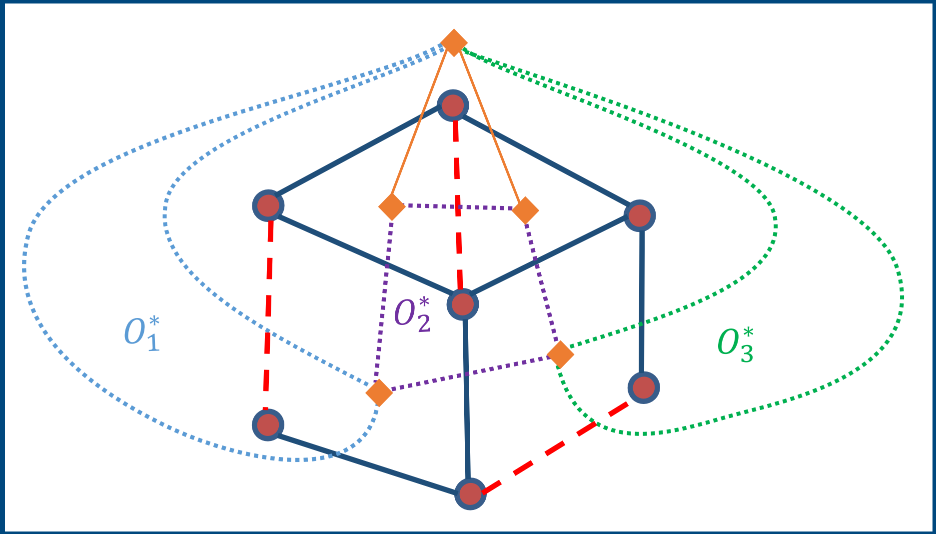
- *Theorem.* In a planar graph H, *the solution* $\vec{x}$ *to*

$$\min \| \vec{x} \|_1 \ \ s.t.\ D_H \vec{x} = A_{H|G}(\vec{\theta} - \vec{\theta}')$$

is unique and $supp(\vec{x})$ gives indices of the failed edges, if the following conditions hold:

(i) for any cycle C in H, $|C \cap F| < |C|/2$,

(ii) F^* can be covered by edge-disjoint cycles in H^*.



Idea of the proof. Faces of the H form a basis for the null-space of D_H

Outline of our approach

Method for
Recovery of phase angles
(External Conditions)

$\vec{\theta}'$

Method for
Failed edges detection
(Internal Conditions)

Method for
Simultaneous
phase angles recovery
and failed edges detection

Simultaneous Phase Angles Recovery and Failed Edges Detection

- *Lemma.* There exist vectors $\vec{x} \in \mathbb{R}^{|E_H|}$ and $\vec{\theta}'_H \in \mathbb{R}^{|V_H|}$ such that

$$D_H\vec{x} = A_{H|G}(\vec{\theta} - \vec{\theta}') \longrightarrow \text{Failed edges detection}$$

$$A_{\overline{H}|G}(\vec{\theta} - \vec{\theta}') = 0 \longrightarrow \text{Phase Angle Recovery}$$

and $supp(\vec{x})$ gives the indices of the failed edges and $\vec{\theta}'_H$ is the vector of the phase angles of the nodes in H.

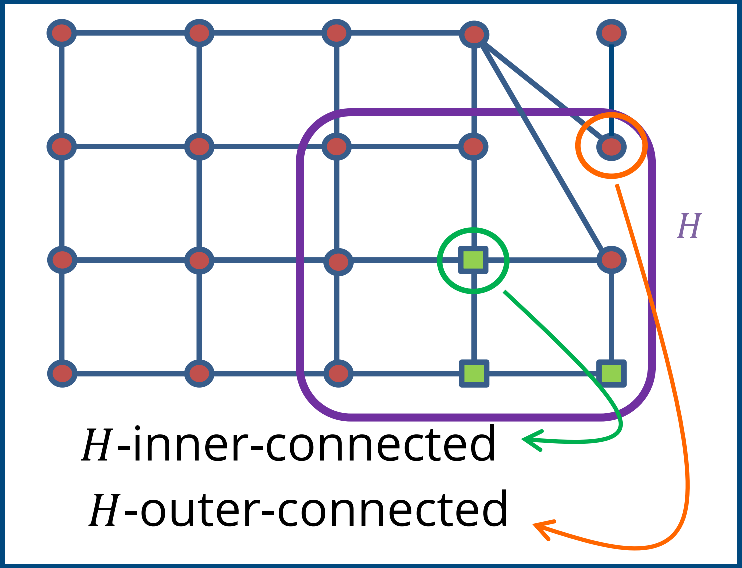
- Solution to the set of equations above is unique if and only if H is acyclic and $A_{\overline{H}|H}$ has linearly independent columns

- Use similar idea to relax the conditions

$$\boxed{\begin{aligned} &\min \| \vec{x} \|_1 \quad s.t. \\ &D_H\vec{x} = A_{H|G}(\vec{\theta} - \vec{\theta}') \\ &A_{\overline{H}|G}(\vec{\theta} - \vec{\theta}') = 0 \end{aligned}} \qquad (**)$$

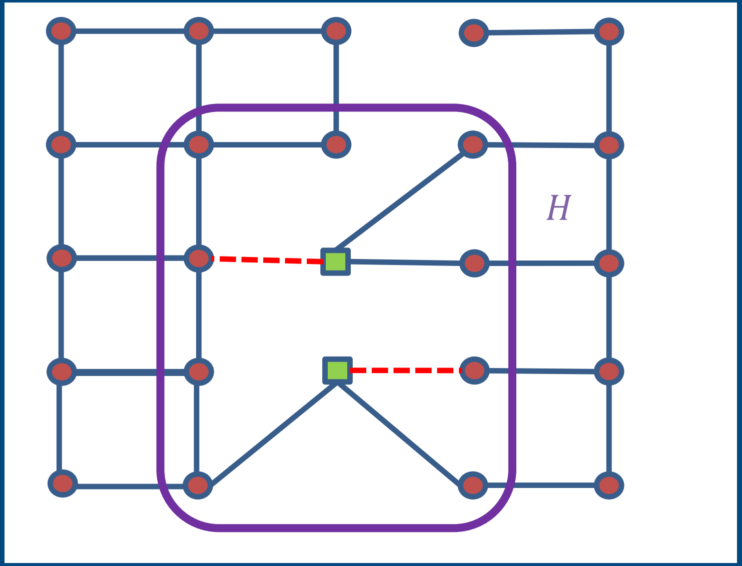
Simultaneous Phase Angles Recovery and Failed Edges Detection

- H-inner-connected nodes V_H^{in}
  H-outer-connected nodes V_H^{out}
- *Lemma.* If v is H-outer-connected, then θ_v' can be computed uniquely.



- *Lemma.* If H is acyclic,
  H-inner-connected nodes form an independent set, and
  $\forall v \in V_H^{\text{in}}, |\partial(v) \cap F| < |\partial(v)|/2$,
  the solution $\vec{x}, \vec{\theta}'$ to $(**)$ is unique.

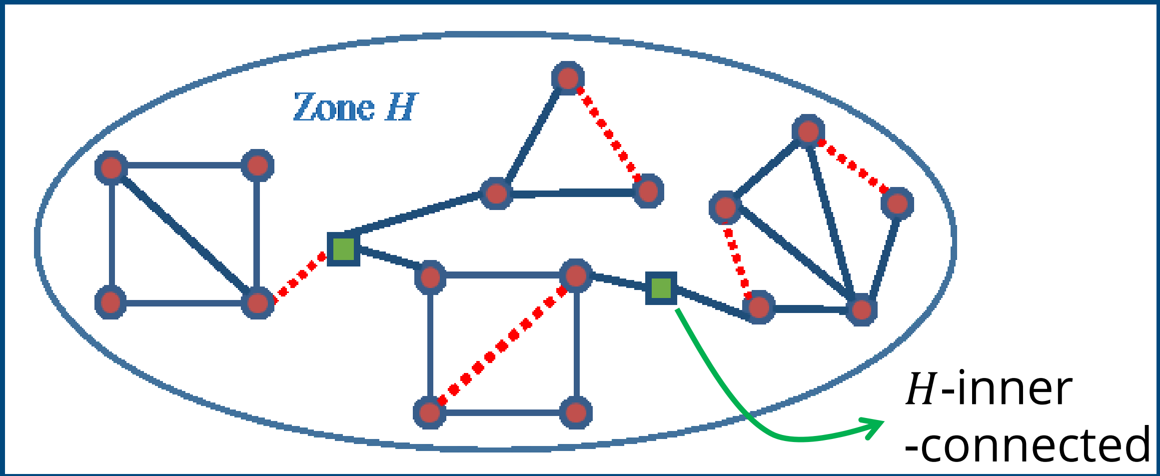
$$\begin{aligned}
&\min \parallel \vec{x} \parallel_1 \;\; s.t. \\
&D_H \vec{x} = A_{H|G}(\vec{\theta} - \vec{\theta}') \\
&A_{\overline{H}|G}(\vec{\theta} - \vec{\theta}') = 0
\end{aligned} \quad (**)$$



$\partial(v)$: the set of edges connected to node v

Simultaneous Phase Angles Recovery and Failed Edges Detection

- *Theorem.* In a planar graph H, the solution $\vec{x}, \vec{\delta}_H$ to $(**)$ is unique with $supp(\vec{x}) = \{i | e_i \in F\}$ and $\vec{\delta}_H = \vec{\theta}_H - \vec{\theta}'_H$, if the following conditions hold:
  (i) $\forall v \in V_H^{\text{in}}, |\partial(v) \cap F| < |\partial(v) \backslash \text{F}|$,
  (ii) for any cycle C in H, $|C \cap F| < |C \backslash \text{F}|$,
  (iii) F^* is H^*-separable,
  (iv) in $A_{\overline{H}|H}$, columns associated with nodes that are not H-inner/outer-connected are linearly independent,
  (v) no cycle in H contains an H-inner connected node,
  (vi) H-inner-connected nodes form an independent set.



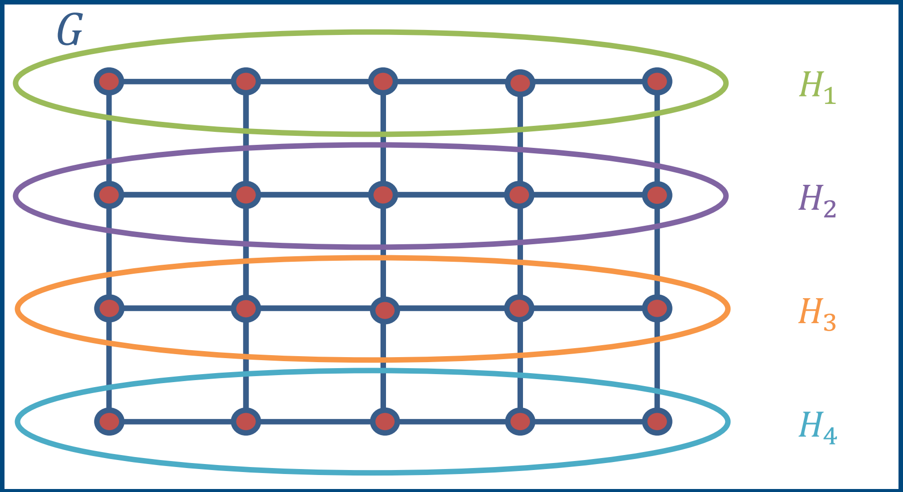
Summary of Results

External conditions	Internal conditions	Attack constraints	Resilience
Matching	Acyclic	None	attack-resilient
Matching	Planar	$\forall$ cycle C, $\lvert C \cap F\rvert < \lvert C \backslash F\rvert$ F^* is H^*-separable	weakly-attack-resilient
Partial matching	Acyclic	$\forall v \in V_H^{\text{in}}$, $\lvert\partial(v) \cap F\rvert < \lvert\partial(v) \backslash F\rvert$	weakly-attack-resilient
Partial matching	Planar No cycle contains an inner-connected-node	$\forall$ cycle C, $\lvert C \cap F\rvert < \lvert C \backslash F\rvert$ $\forall v \in V_H^{\text{in}}$, $\lvert\partial(v) \cap F\rvert < \lvert\partial(v) \backslash F\rvert$ F^* is H^*-separable	weakly-attack-resilient

Divide the graph into attack resilient zones

Minimum Matched-forest Partition

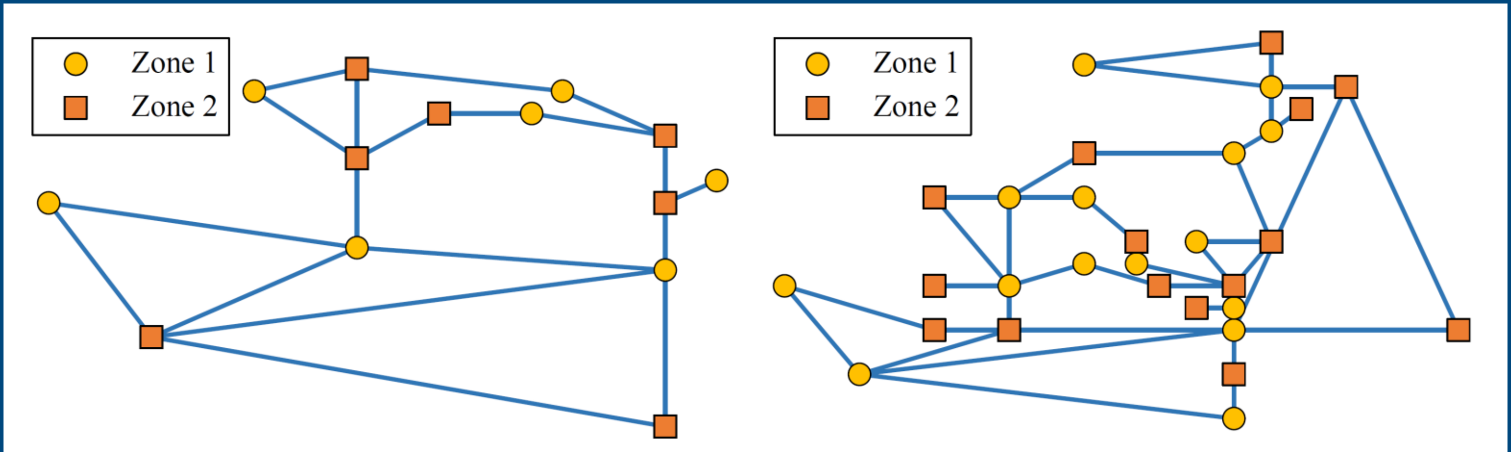
- *Definition.* A *matched-forest* partition of a graph G
  - The subgraph induced by nodes in any partition is acyclic
  - For each partition there is matching between the nodes inside and outside of the partition that covers inside nodes



- *Lemma.* For all $\epsilon > 0$, it is NP-hard to approximate the minimum matched-forest partition of a graph G to within $n^{1-\epsilon}$.

Zone Selection Algorithm

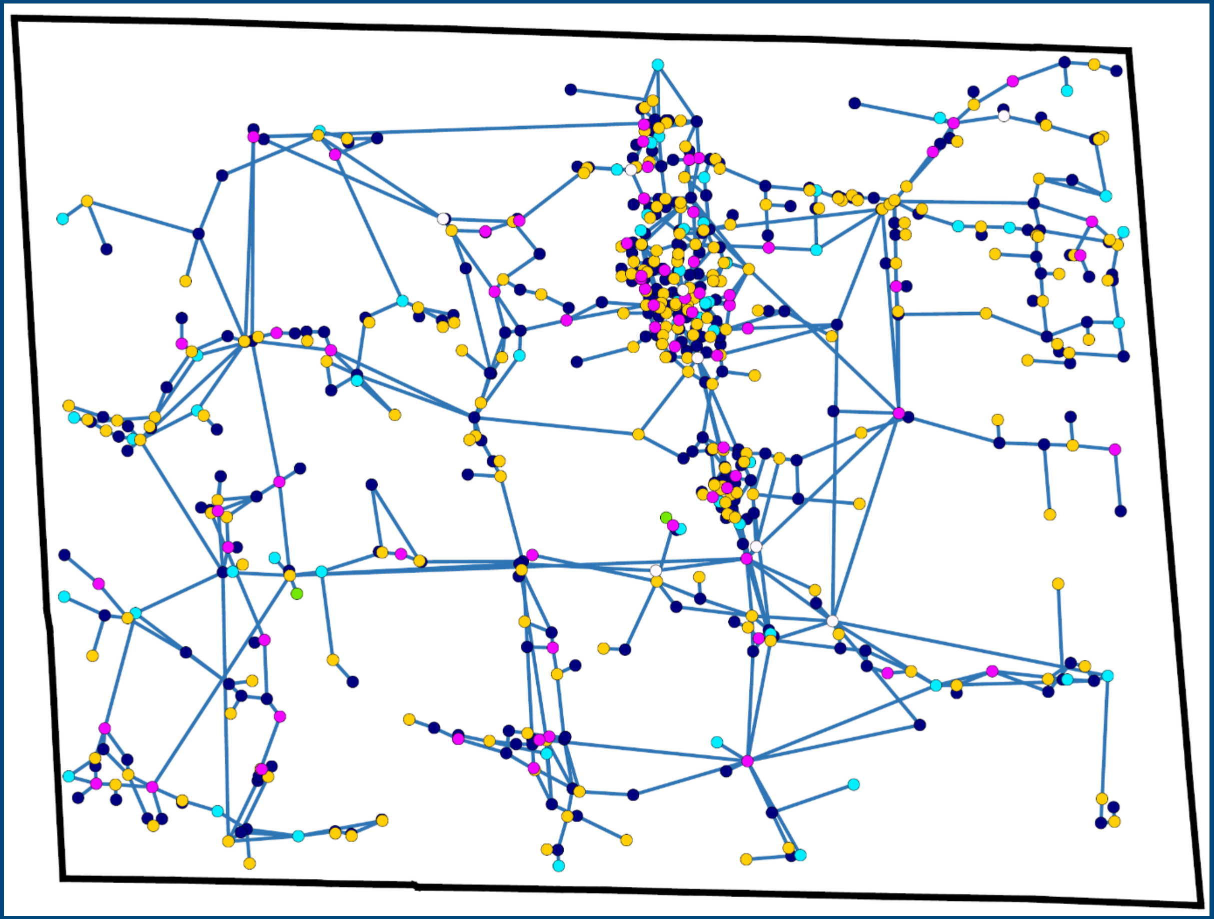
- Zone Selection (ZS) Algorithm is a polynomial time algorithm to find a matched-forest partition of a graph
  - Find the optimal matching cover of G in $O(n^3)$
  - Divide the graphs induced on each matched part into acyclic graphs
- Remark. A planar graph G can be partitioned into at most 3 acyclic subgraphs
- *Lemma.* If G is planar, the ZS Algorithm provides a 6-approximation of the minimum matched-forest partition of G.



(a) IEEE 14 bus (b) IEEE 30 bus

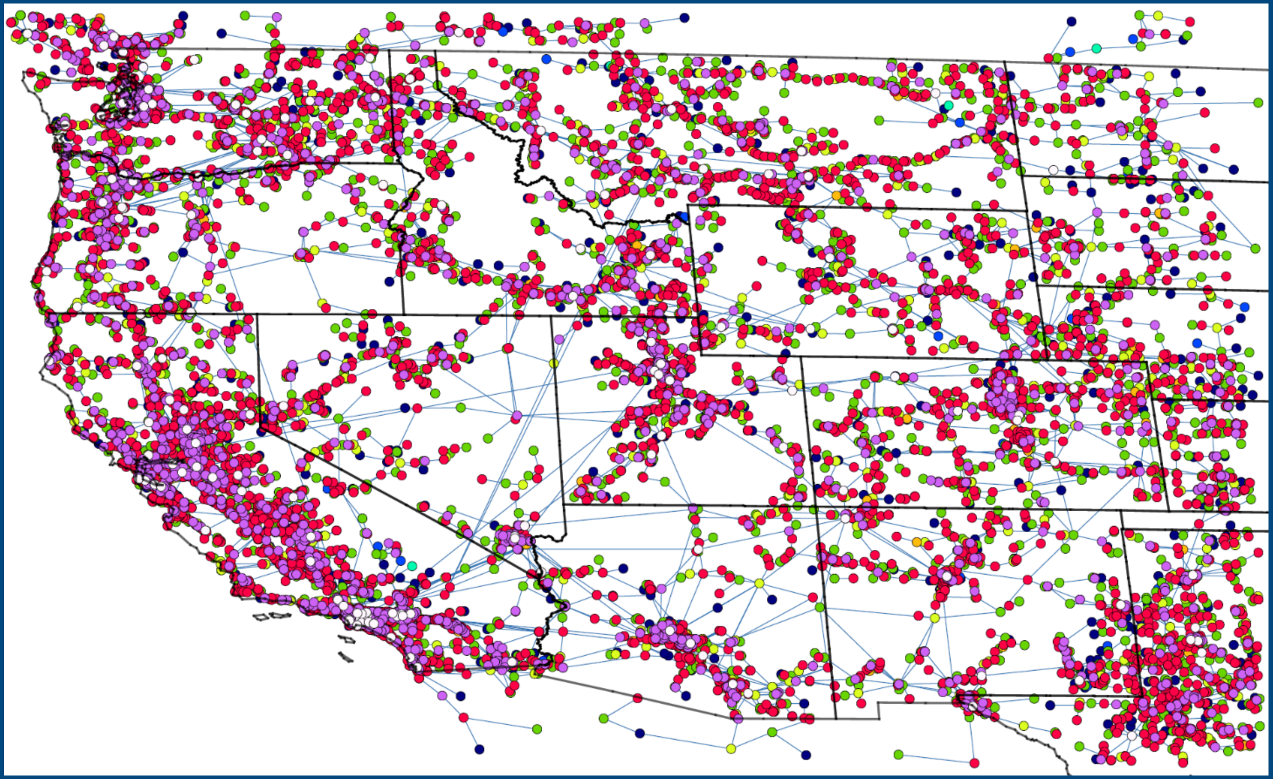
Colorado State Grid

- Partitioning of the Colorado state grid into 6 attack-resilient zones



Western Interconnection

- Partitioning of the U.S. Western Interconnection into 9 attack-resilient zones



- Any subgraph of an attack-resilient zone is also attack-resilient
- The partitions obtained by the ZS Algorithm can be further divided into smaller zones based on geographical constraints

Conclusion

- Provided a new model for joint cyber and physical attacks on power grids
- Developed methods to recover information
- Developed an approximation algorithm for the partitioning the grid into attack-resilient zones

- This is one of the first steps towards understanding the vulnerabilities of power grids to joint cyber and physical attacks and developing methods to mitigate their effects

Thank You!

saleh@ee.columbia.edu

http://wimnet.ee.columbia.edu