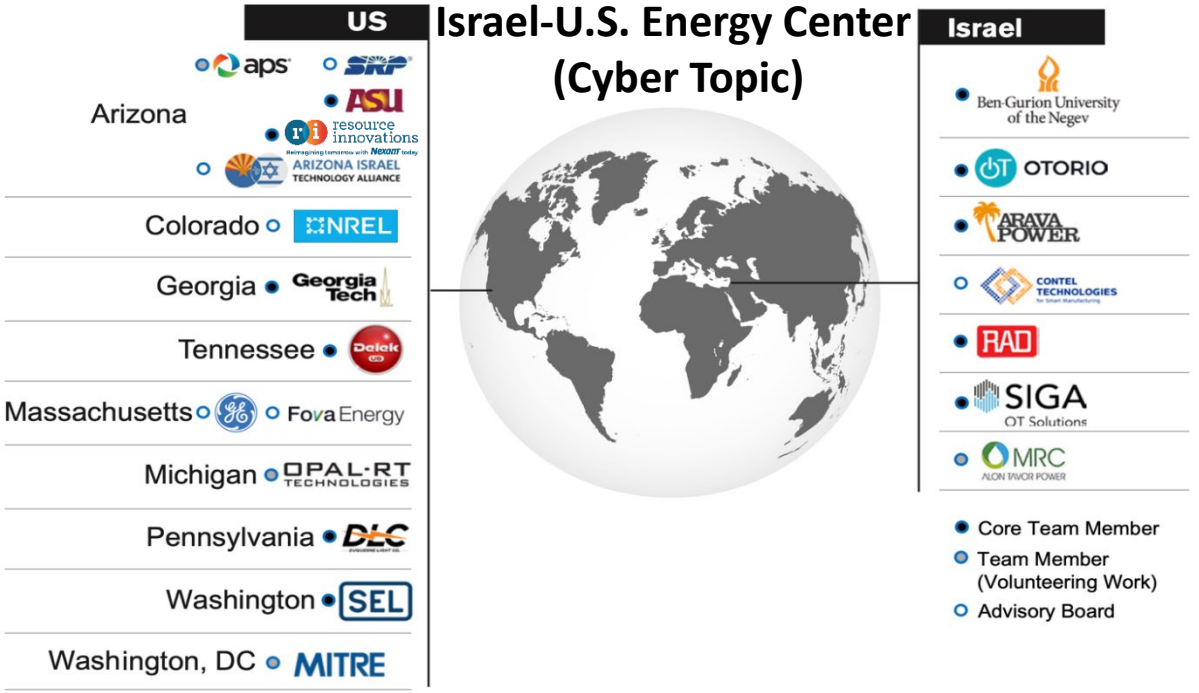
Task 1: Topology Identification for Cyber Security

Yang Weng, Bilal Saleem, and Haoran Li

Arizona State University

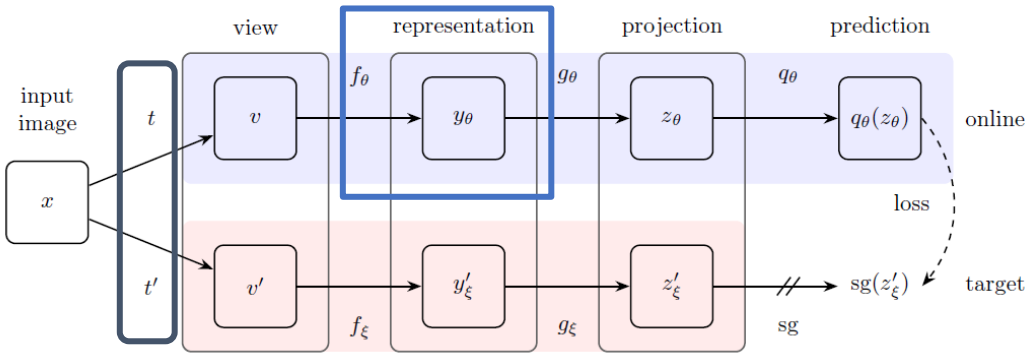
Aug 9, 2022



Motivation: Cyber-Security Application

System Information Identification

Use these learned features for downstream Tasks, e.g., classification



Power system measurements

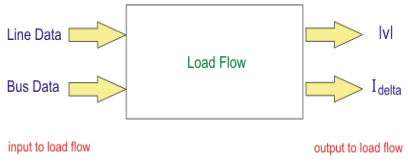
Loss Function for System Info:

$$\mathcal{L}_{\theta,\xi} \triangleq \left\| \overline{q_\theta}(z_\theta) - \overline{z}'_\xi \right\|_2^2$$

Idea: use this as a score for compatibility

Requirements

Hosting Capacity Analysis



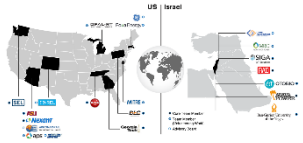
Load Flow Analysis

Expensive Solution

Field Validation of Conductors

Costly

Past Work and Problem Definition



- In the past, we generated simulated data related to
  - System observability
  - Communication delay
  - Change point (Fig. shown on right)
  - PMU data (Voltage Angle)

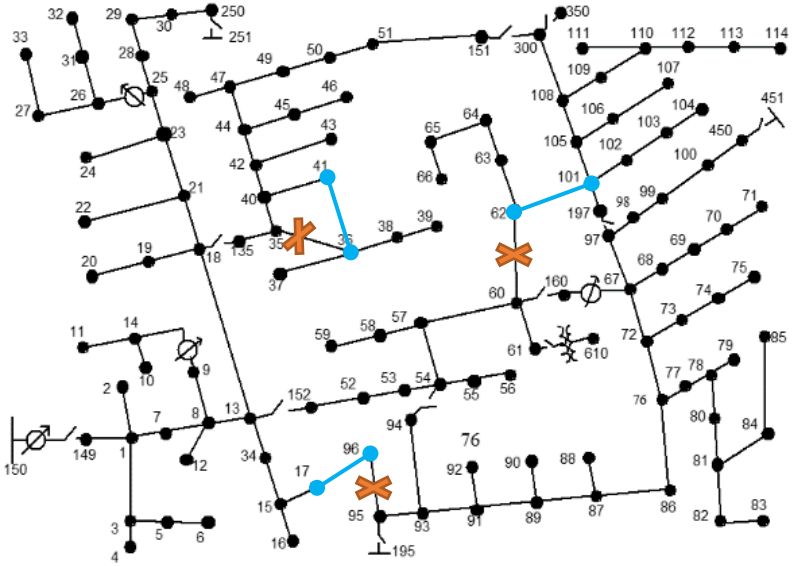


Figure: Modified IEEE-123 bus data

- Using the available data, find out which smart meters are connected to which transformer

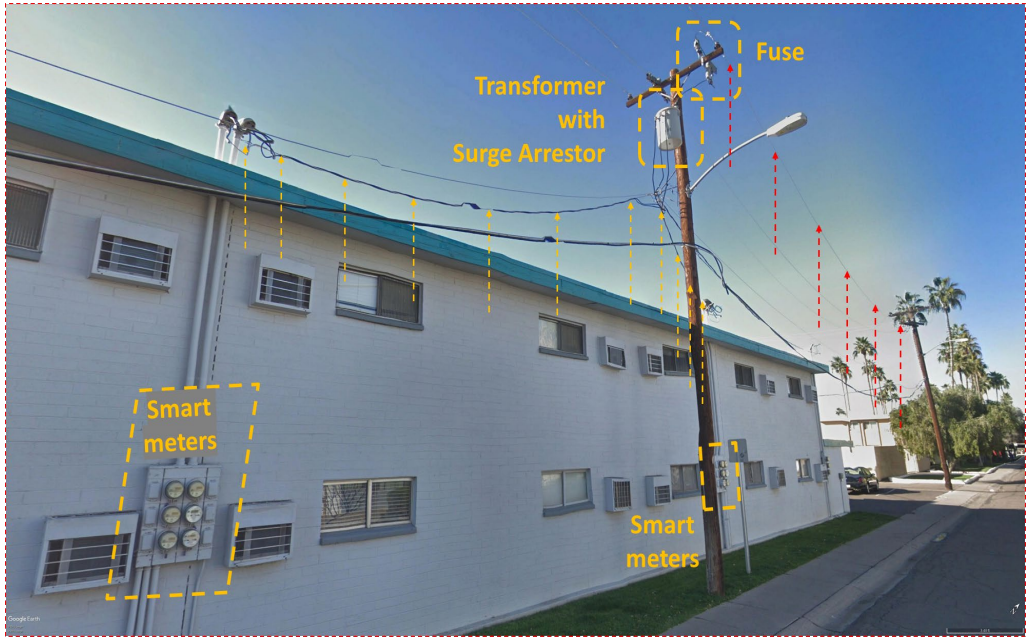
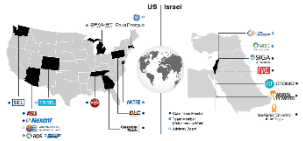


Figure: Problematic Places

Underground Lines and Transformers



- Determining transformer affiliation through **Google Maps** becomes **impossible**

Figure: A pad mounted transformer for underground distribution.

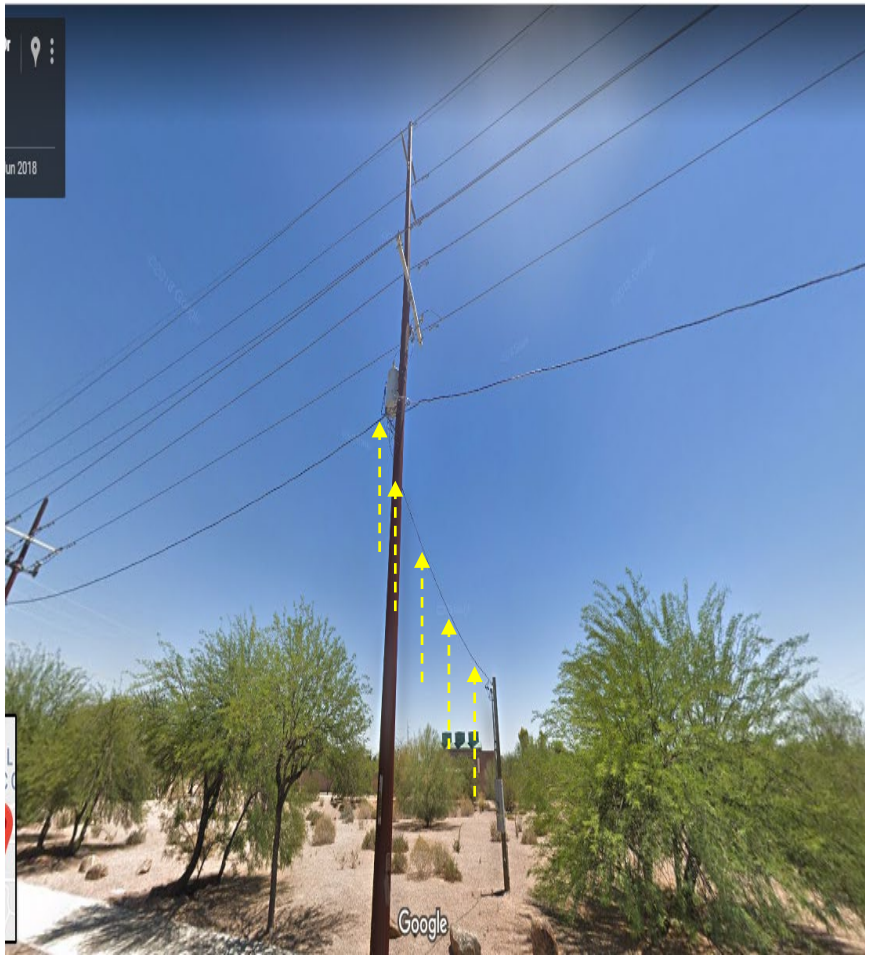


Figure: An overhead line going underground.

Transformer Association in Distribution Grids

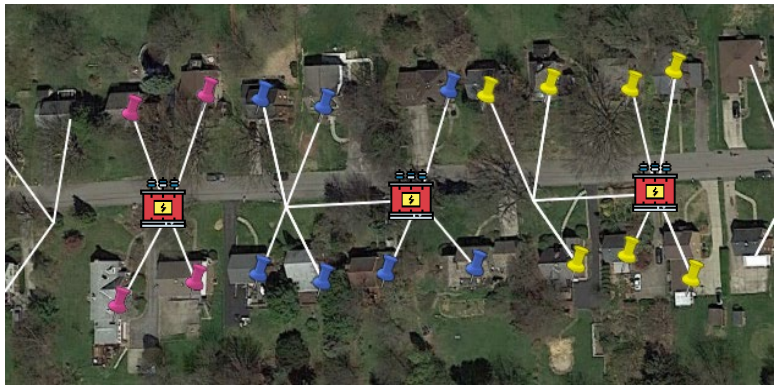
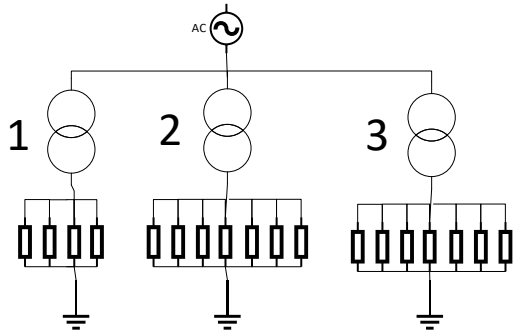


Figure: Actual Topology



Schematic of the above test case.

Transformer Voltage Drop

Similar Meter Voltages

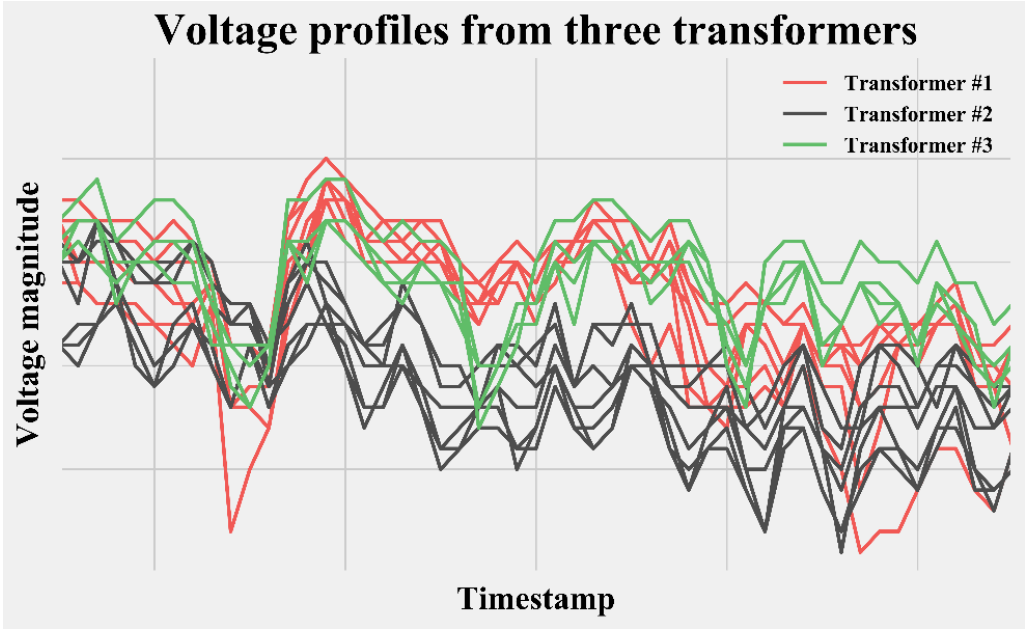
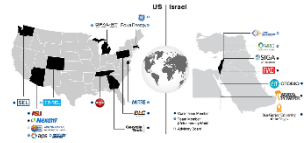
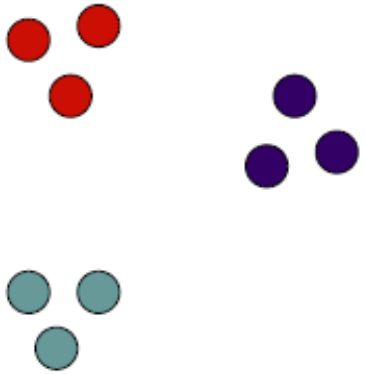


Figure: Smart Meter Voltage Data

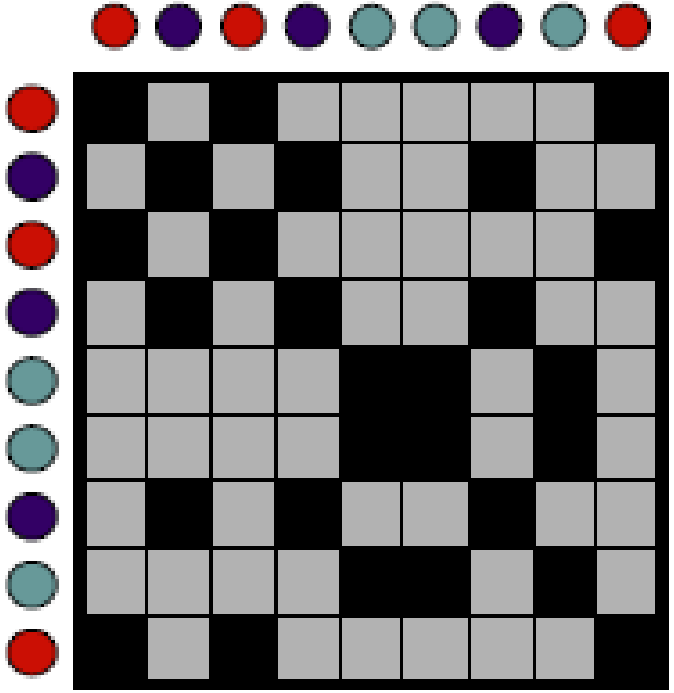
Spectral Clustering Mathematical Formulation



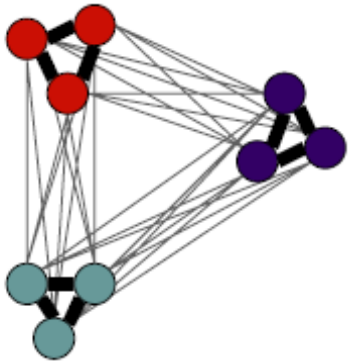
Data from Smart Meters



Similarity Matrix



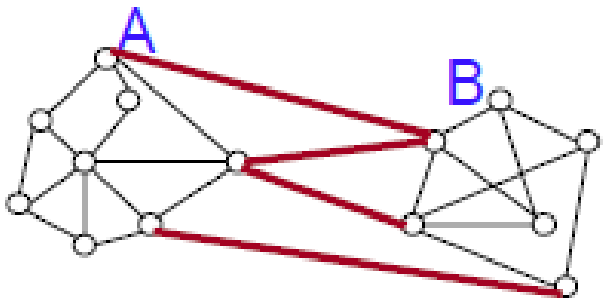
Similarity Graph



Spectral Clustering Mathematical Formulation

$$cut(A,B) \coloneqq \sum_{i \in A, j \in B} w_{ij}$$

$$Q(A,B) = cut(A,B)\left(\frac{1}{weight(A)} + \frac{1}{weight(B)}\right)$$



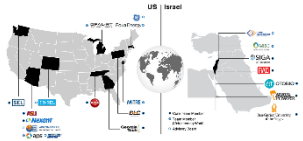
$$\min Q(A,B) = \min \frac{q^T L q}{q^T W q}, \qquad \text{subject to } q^T W e = 0, q \neq 0$$

$$q_i = \begin{cases} \frac{1}{vol(A)} & if\ i \in A \\ -\frac{1}{vol(B)} & if\ i \in B \end{cases}$$

Is solved when q is the eigenvector corresponding to the 2nd smallest eigenvalue λ_2 of the generalized eigenvalue problem,

$$\boldsymbol{L}z = \lambda \boldsymbol{W} z$$

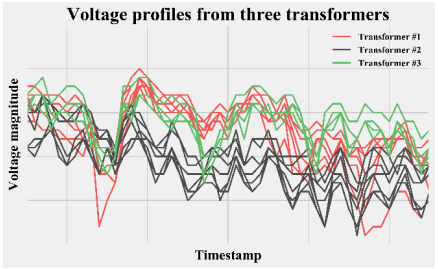
Spectral Clustering Mathematical Formulation

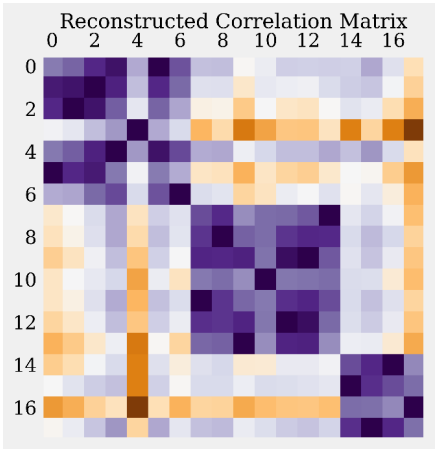


1. Given the similarity matrix A, compute the first k eigenvectors $v_1, \ldots, v_k$
2. Build the matrix $V \in \mathbb{R}^{n.k}$ with the eigenvectors as columns

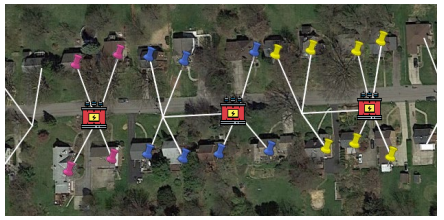
	v_1	v_2	v_3
Z_1	v_{11}	v_{12}	v_{13}
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Z_n	v_{n1}	v_{n2}	v_{n3}

3. Run the K-means algorithm on the k-dimensional data $\boldsymbol{Z}$ to obtain the desired k-way multi-partitioning.
4. Results:

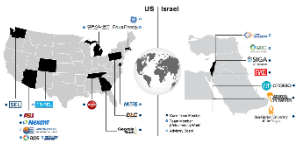


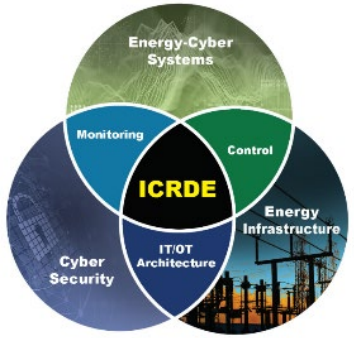


Transformer Association Reconstructed 100%!



Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-based Centralized Defence and Edge Resilience





Theme 1: Cyber-Physical System (CPS) Data Preparation

- **Project 1**: Physical Processes as Cybersecurity Assets
  - **T1: Realization of advanced energy management applications**
  - **T2**: Digital representation of physical processes and operational process modelling
    - **T3**: Data collection and aggregation
- **Project 2**: Knowledge Base Establishment and Representation Learning of Threats
  - **T4**: Multi-level threat intelligence knowledge base (MITRE)
    - **T5**: Adversarial mimicking (Theoretic)
    - **T6**: Threat hunting (Actively learning)

Theme 2: Data Analytics for Monitoring

- **Project 3**: Cyber Attacks Detection of IT/OT Architecture
  - **T7**: Malware threats mitigation (Smart enemy? Reduce probing and plan)
  - **T8**: Detect event mimicking attacks
    - **T10**: Multilayer anomaly detection (Uncertainty)
    - **T9**: False Data Injection (Physical Embedding)
  - **T11**: AI-based intrusion detection (Engage operator)
  - **T12**: Explainable cyber-AI analytics (Metric + Temporal)

Theme 3: Control and Validation

- **Project 4**: Cyber Resilience and Robustness for Control Actions
  - **T13**: Firmware verification (Edge)
  - **T14**: Attack tolerance (Insensitive to the attack)
  - **T15**: Self healing and auto-remediation (Optimization)
    - **T16**: RL control for CPS (Advise Sys Operator)
- **Project 5**: Future-Proof Architectures
  - **T17**: ICS security by design
  - **T18**: Hardware in the loop