CRII: CPS: Data-Driven Cascading Failure Abstraction and Vulnerability Analysis in Cyber-Physical Systems

PI: Xiang Li (xli8@scu.edu) , Santa Clara University

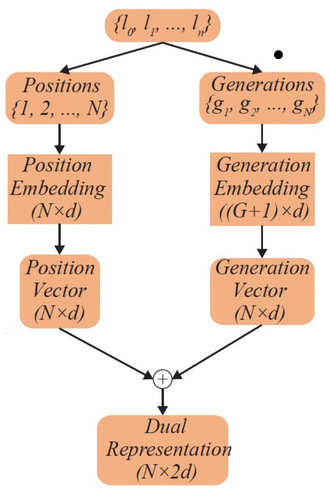
https://www.nsf.gov/awardsearch/showAward?AWD_ID=1948550

Challenge:

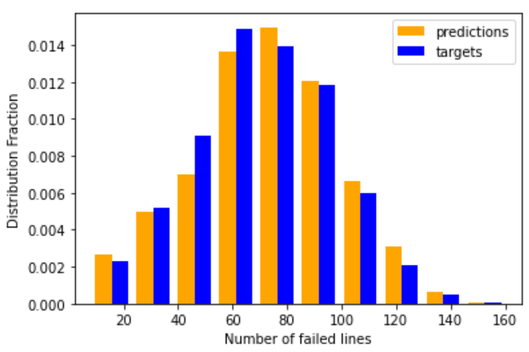
- Correlations between CPS components are crucial for cascading failure understanding and describing complicated CPS cascading failures with simpler models, yet the existing methods cannot accurately reveal them.
- In diffusion based cascading failure models derived with correlations, diffusion maximization and mitigation problems are both #P-Hard.

Solution:

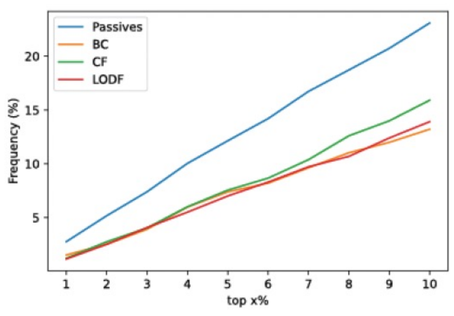
- Trained *the first Transformer based models* to predict CPS cascading failure with high accuracy.
  - Use initial failures to predict all components failed in the cascade.
    - *Encoder-decoder model with component ids as input/target: f1 score of 0.77 for predicting status of all components .*
    - *Good at estimating overall cascade size.*
  - *Use initial failures to predict components failed in each round of the cascade.*
    - *Encoder-only model with dual representation of cascade as training data: f1 score of 0.99 when predicting failed lines.*
    - *Revealed correlation using the attention mechanism.*



Dual representation

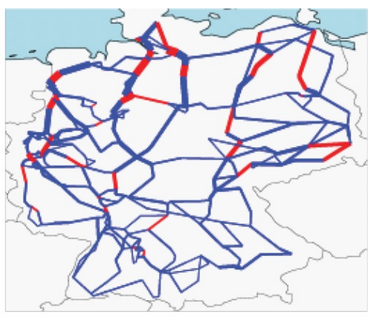


Cascade Size Prediction

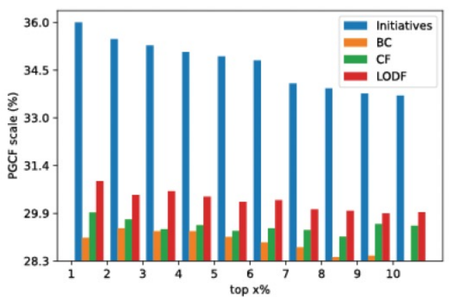


Performance of Top Passives

***Initiatives**: the components that their own failure are more likely to trigger others' failure.*
***Passives**: the components that are easy to fail because others' failure*



Top Initiatives in the German Power Network



Performance of Top Initiatives

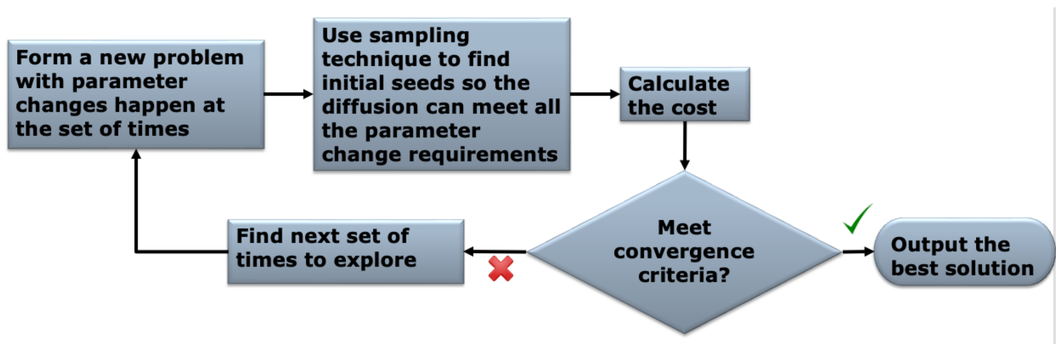
Broader Impact:

- Better understanding of cascading failures will help enhancing CPS security

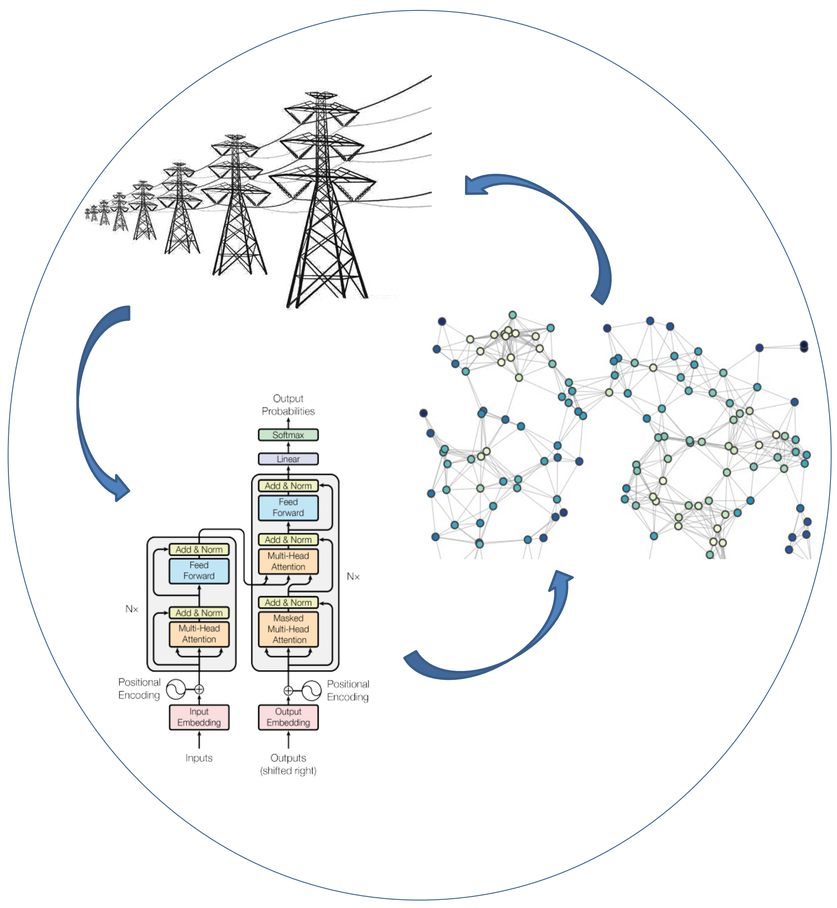
Scientific Impact:

- Using Transformer to predict cascading failures can be helpful to simplify any complicated cascading process in CPS.
- A new method to use the attention mechanism to reveal the correlation of components. It is further extended to identify the most critical components in cascading failure.
- The developed sampling methods in large-scale networks can be extended to other diffusion maximization and mitigation problems in various networks.

- Built simpler cascading failure models using the learned correlations.
- Developed *new* efficient sampling algorithms for both diffusion maximization and mitigation problems.
  - A ***dynamic*** algorithm for diffusion maximization, the cascade model parameters may change during diffusion propagation
  - An ***adaptive*** algorithm for diffusion maximization, making decisions based on the current status of the cascades.
  - An **novel** line blocking algorithm for diffusion mitigation, with an adaptive reachability calculation algorithm for estimating the impact of blocking lines.



The dynamic algorithm



Broader Impact:

- Research opportunities for high school students and students from underrepresented groups
- Senior design project opportunities
- Disseminated research results to high school and undergraduate students in workshops and seminars