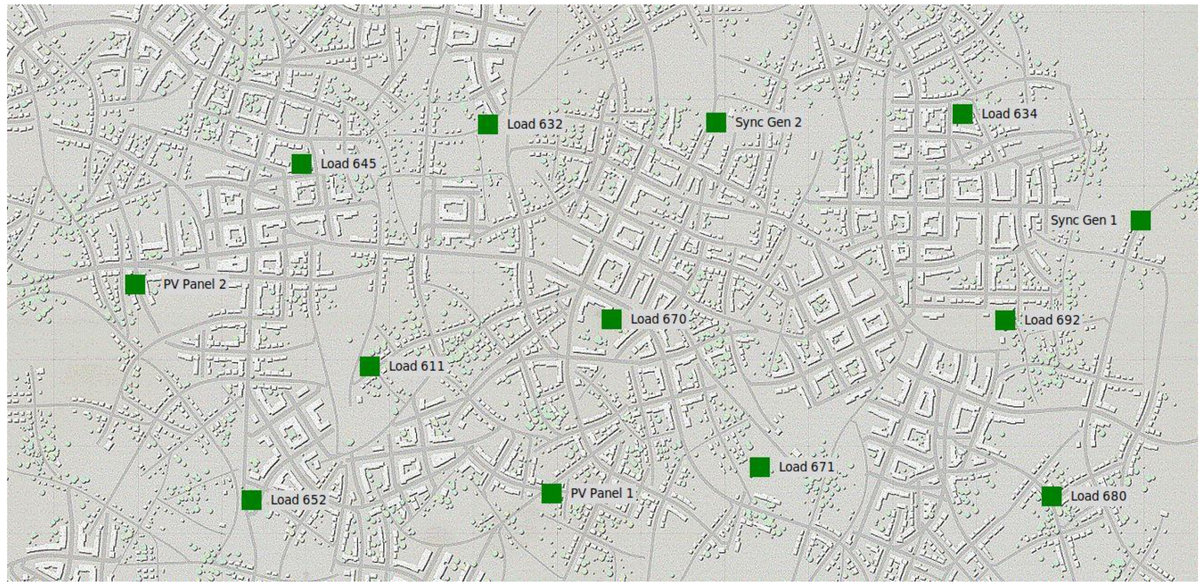
CPS: Small Collaborative Research: CYDER: CYbersecure Distribution systems with power Electronically interfaced Renewables/1837359 /Virginia Tech

Challenge:

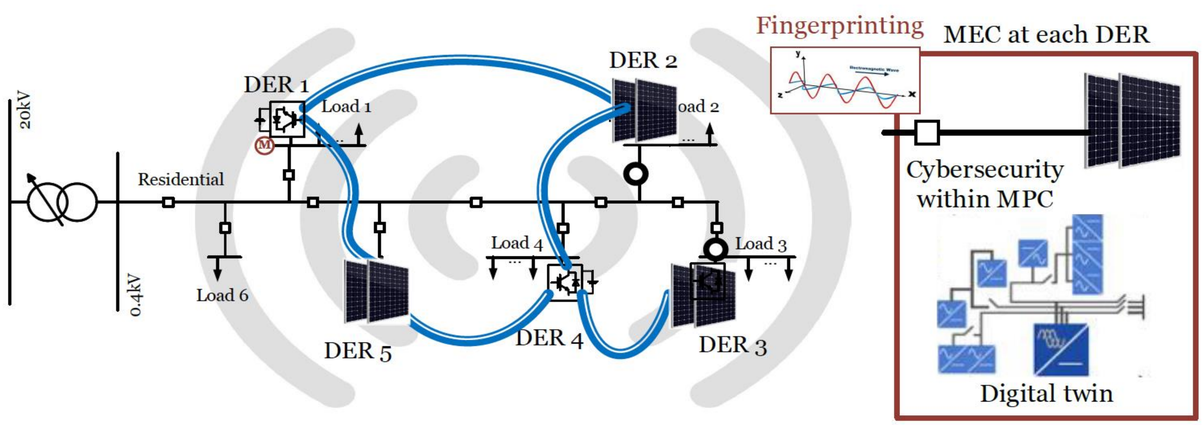
The massive number of grid edge devices, and the increased connectivity exacerbates an already vulnerable nature of the distribution system. At present, certain limitations restrict the variety of cybersecurity detection and/or prevention techniques that may be applied. Furthermore, malicious attacks can be coordinated to disrupt critical electricity service and damage the society and economy.



Solution:

A new methodology based on distributed intelligence to enable generation and load agents to share cyber information for decision making by each agent. Key innovations include:

- –Node-stationed network-based IDS (NIDS)
- –Effective decentralized correlation technique
- –Efficient consensus protocol for mitigation
- –A coordinated control strategy for IBRs



Scientific Impact:

The algorithm is significant in its ability to correlate attacks and predict the targets of a coordinated cyberattack in real-time, and in a decentralized mechanism, using a cyber-physical metric.

Broader Impact:

- A female URM PhD student recruited for the project
- It contributes to security and resilience of the electricity infrastructure.
- Testbed is being used in a new experiential learning program on utility system cybersecurity

NSF 1837359 – Chen-Ching Liu, Ali Mehrizi-Sani, Jennifer Appiah-Kubi, Ardavan Mohammadhassani