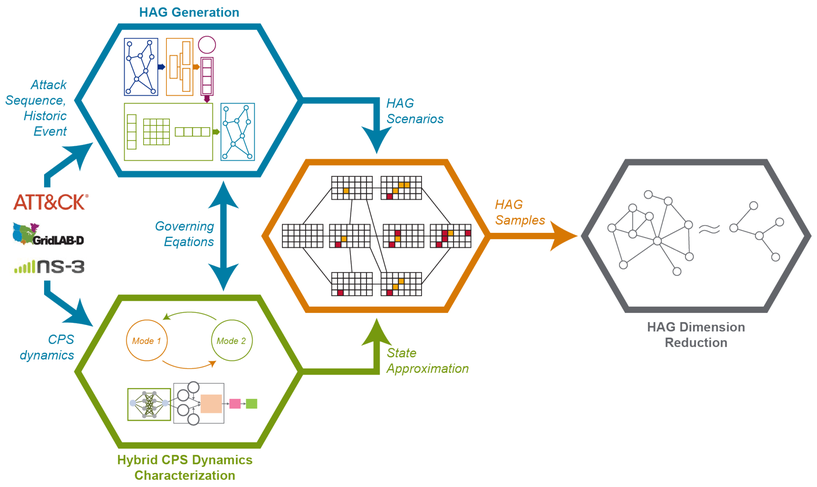
HAGEN: Efficient Hybrid Attack Graph Generation for Cyber-Physical System Resilience Experimentation | Thrust 1

Sumit Purohit, Arnab Bhattacharya, Omer Subasi, Ashutosh Dutta, Oceane Bel, Cimone Wright-Hamor, Aowabin Rahman



OBJECTIVE

To develop novel theory and algorithms to generate hybrid attack graphs (HAGs) for cyber-physical system (CPS) resilience experimentation at desired scale and speed.

- Characterize hybrid CPS dynamics across scale with sparse data
  - Physics-informed learning of CPS dynamics across scale with sparse simulated data (e.g., GridLAB-D, NS3)
- Leverage hybrid dynamics to generate credible course-of-action HAGs
  - Temporal generative models to produce HAG scenarios bootstrapped with MITRE ATT&CK and industrial control system kill chain information
- Perform dimension reduction of HAGs for edge test case experimentation
  - Property-preserving, multi-layer graph sampling and classification algorithms via distributed computing architectures

ACHIEVEMENTS

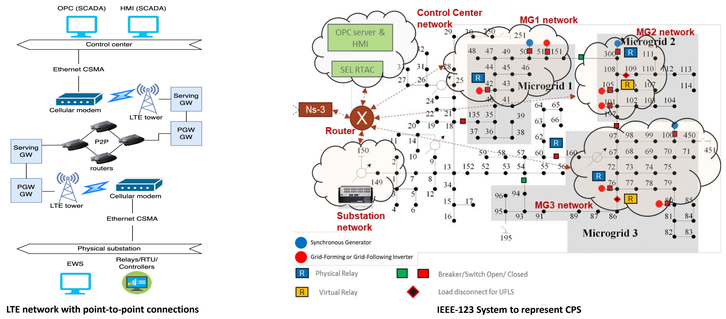
- Dutta, A., Purohit, S., Bhattacharya, A., and Bel, O. (2022, May). “Cyber Attack Sequences Generation for Electric Power Grid.” In 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES) (pp. 1-6). IEEE.
- “Impact-Driven Sampling Strategies for Hybrid Attack Graphs.” [Submitted to International Symposium on Technologies for Homeland Security (IEEE-HST)].
- “Mathematical Modeling of Secure Energy Systems (MMOSES).” [Submitted to Advanced Scientific Computing Research MMICCS DE-FOA-0002704].
- Special issue on “Scalable Graph Neural Networks: Theory & Practice,” *Parallel Computing*.

APPROACH

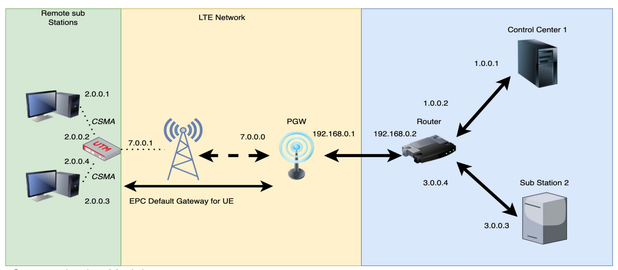
- Hybrid attack graphs provide a flexible and efficient approach to generate attack sequences for a CPS
  - CPS state and dynamics are represented as nodes and adversary tactics, and physical actions are represented as edges that cause the system to change from one state to another

Co-Simulating Microgrid and Communication

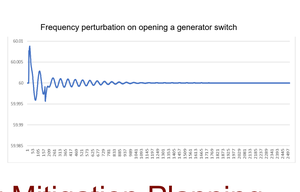
- Co-design of CPS-emulation platforms and data generation for a system of interest with different scenarios and faults
- Algorithm development to train generative and physics-informed learning models

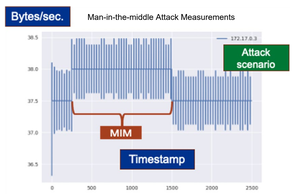


NS-3 GridLAB-D HELICS PyG



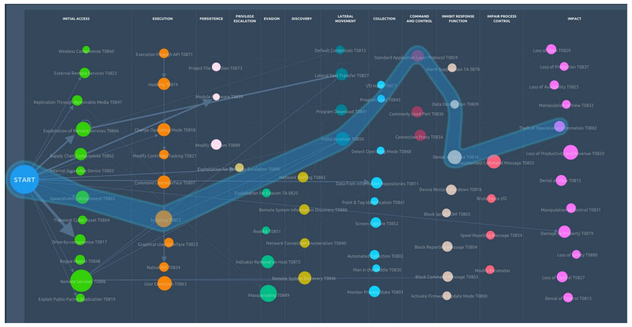
Communication Model

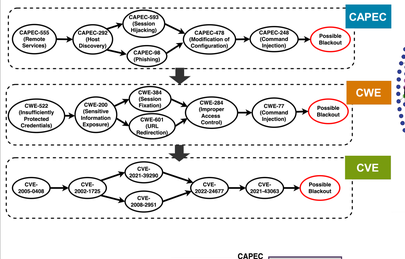




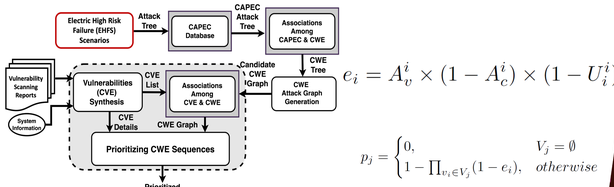
Risk Mitigation Planning

- Generate feasible attack sequences for a specific system and identify key weaknesses



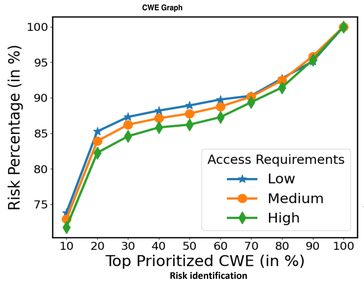


Attack Knowledge Graph



$$e_i = A_v^i \times (1 - A_c^i) \times (1 - U_i^i)$$

$$p_j = \begin{cases} 0, & V_j = \emptyset \\ 1 - \prod_{v_i \in V_j} (1 - e_i), & otherwise \end{cases}$$



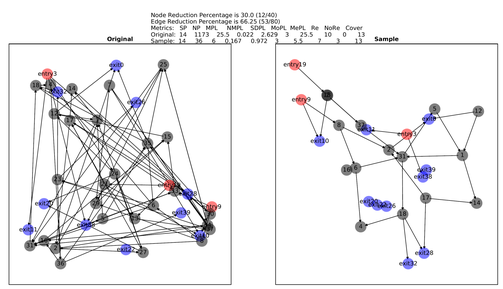
$$P_k = \prod_{w_j \in \mathcal{L}_k} p_j$$

$$R_x = \frac{R(W) - R(W - X)}{R(W)}$$

$$R(W) = (1 - \prod_{k \in \mathcal{L}} (1 - P_l)) \times I_m$$

Scalability of HAG Generation

- “Coverage”-based node sampling
- Weakness-driven (CWE) approach



U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

8/17/2022 | PNNL-SA-175005

Pacific Northwest NATIONAL LABORATORY
www.pnnl.gov