PARP: Mislead Physical-Disruption Attacks by Preemptive Anti-Reconnaissance for Power Grids' Cyber-Physical Infrastructures

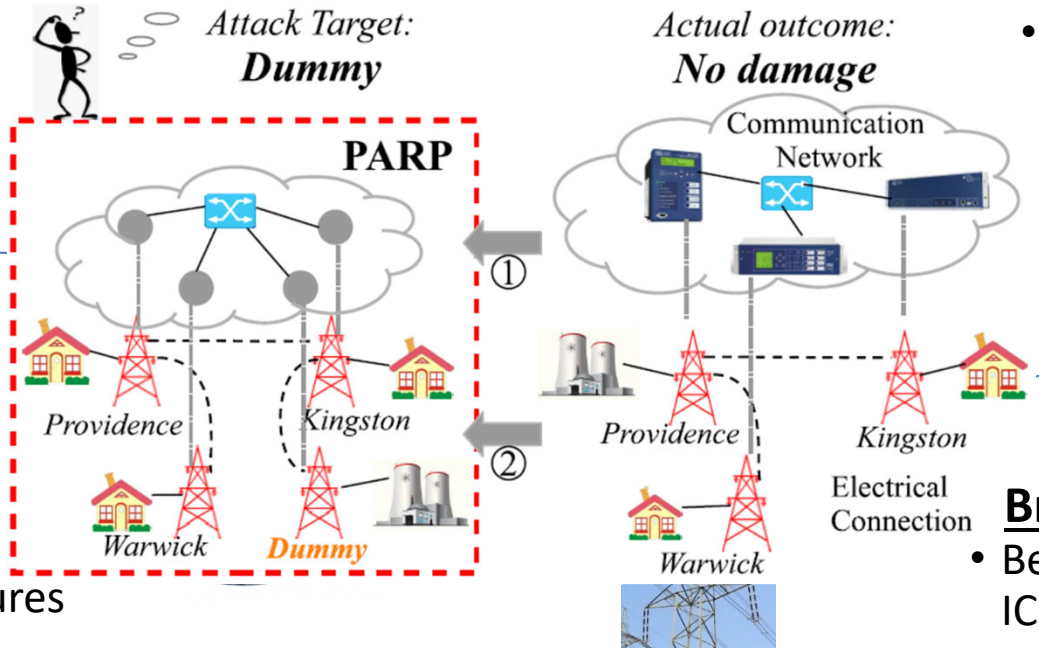
THE UNIVERSITY OF RHODE ISLAND

Challenge:

- Adversaries perform in-depth reconnaissance, leading to irreversible damage
- How to mislead stealthy reconnaissance relying on legitimate operations
- How to craft misleading physical data

Solution:

- PARP, the first Preemptive Anti-Reconnaissance that will mislead adversaries about Power grids' cyber-physical infrastructures
- Technical approaches:
  - Control Function Virtualization (CFV), neutralizing communication pattern that can pinpoint physical device
  - Electrical-Model-Guided Adversarial Generative Networks (EleGAN), crafting decoy physical data conforming to power grids' physical models



Scientific Impact:

- Mislead attacks before malicious activities are launched, removing potential threats in advance
- Covering a wide spectrum of attacks including unknown ones by disrupting reconnaissance on physical data

Broader Impact & Broader Participation:

- Benefit a wide range of ICS environments
- Apply PARP to broader security problems that rely on extensive data for preparation, e.g., attacks driven by AI
- Advance two ICS security courses created and taught by the PI
- Reform hybrid education for existing and future workforce

PI: Hui Lin, huilin@uri.edu
Institution: University of Rhode Island

Award #: 2144513