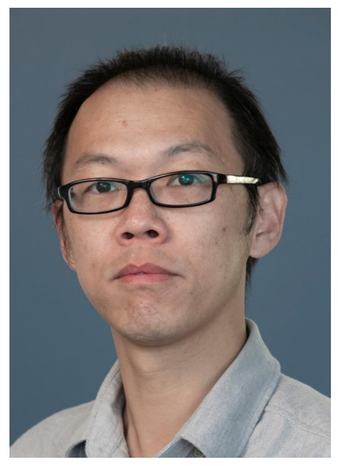
PARP: Mislead Physical-Disruption Attacks by Preemptive Anti-Reconnaissance for Power Grids' Cyber-Physical Infrastructures



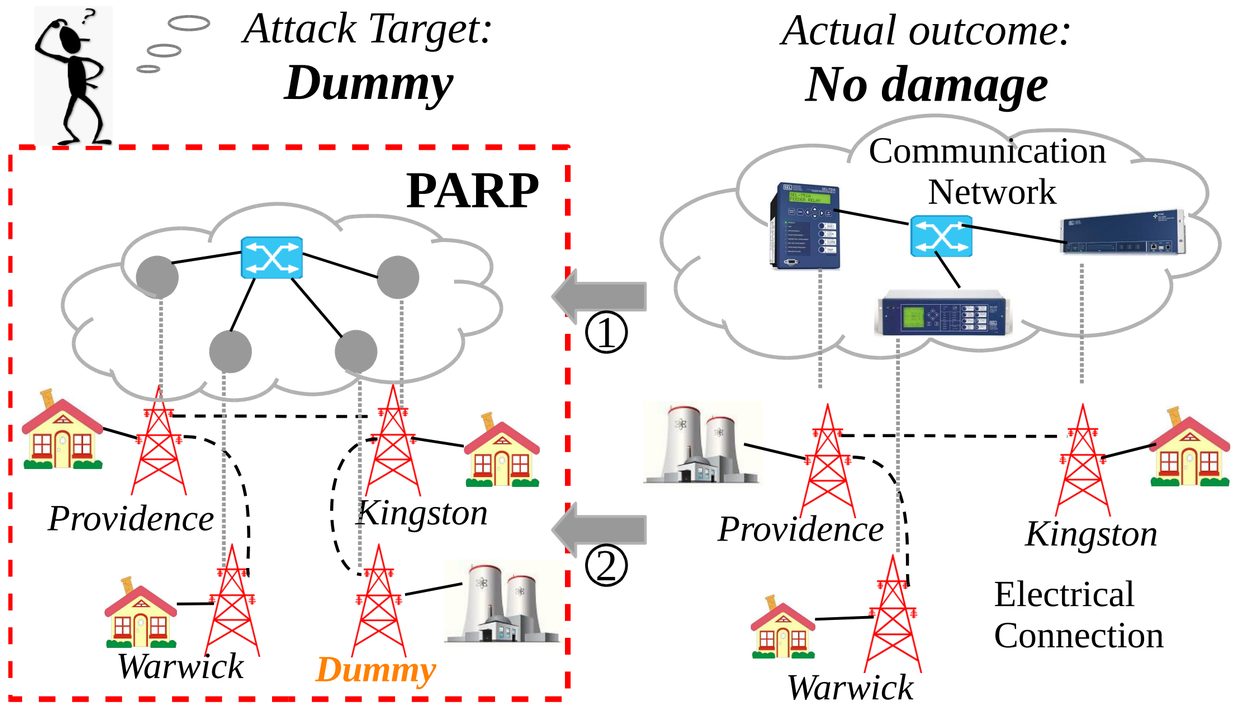
PI: Hui Lin, University of Rhode Island

https://www.nsf.gov/awardsearch/showAward?AWD_ID=2144513

OBJECTIVE

Disrupt/mislead attackers' reconnaissance to cause physical damage in smart grids

- Physical function virtualization
  - Follow the actual implementation of network stacks and system invariants
- Decoy data construction
  - Conform to power grids' physical model



CHALLENGE

- How to mislead stealthy reconnaissance relying on legitimate operations
  - Mimicking systems often poorly follows a complete system specification
  - Simulations do not conform with proprietary implementation
- How to craft misleading physical data
  - Existing honeypot projects do not model physical processes

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

SOLUTION

Thrust 1: Physical function virtualization

- Construct virtual node templates including basic configuration
- Build profile of seed devices, including actual network stack implementation and system invariants
- Create packet hooking component, tailoring application payload at runtime

Thrust 2: Decoy data construction

- Take the physical topology and actual measurements as inputs
- Adjust gradient descent procedure of state estimation to inject new measurements
- Make the combination of decoy and actual data conform to physical model

BROADER IMPACT (RESEARCH)

- Apply to other cyber-physical systems (CPS) by instrumenting their network infrastructure
- Spoof measurements based on other CPSs' physical model
- Example CPSs include: Internet of things, vehicle communication, and smart transportation

BROADER IMPACT (EDUCATION)

- Create and enhance a new special topic course on CPS security
- Integrate the topic in other security and network courses
- Serve as a project for department or college-level activities, e.g., Hackathon

BROADER IMPACT (INDUSTRIAL)

- Search the opportunity to integrate the implementation in utility environment
- Collect real measurements to understand the state-of-the-art configurations of modern CPSs
- Obtain feedback from engineers on the proposed moving target defense mechanisms