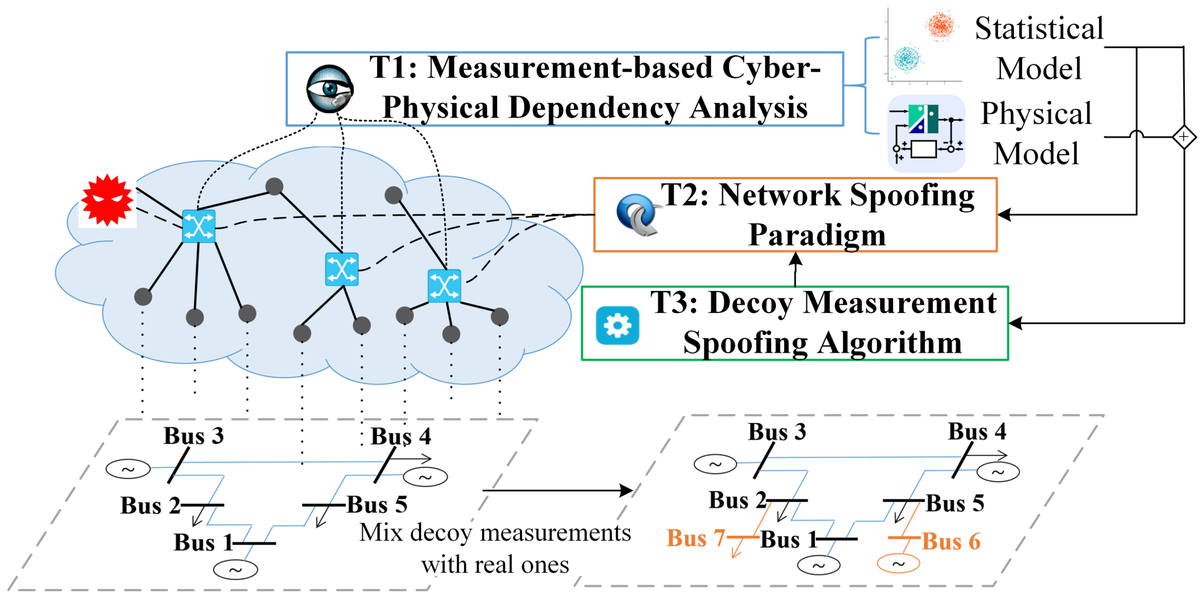
Preempting Physical Damage from Control-related Attacks on Smart Grids' Cyber-physical Infrastructure

Hui Lin: University of Nevada at Reno

OBJECTIVE

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

- Randomize network connectivity of end devices
  - Increase the unpredictability in control network
  - Limit information collected by attackers to design attack strategies
- Intelligently spoof responses for "off-line" devices
  - Include decoy measurements to mislead attackers into designing ineffective attacks



CHALLENGE

- Attackers' reconnaissance activities introduce little anomaly at the network level
- Passive monitoring of data acquisition in smart grids:
  - Communication protocols without security protection
- Active monitoring to scan ICS devices
  - Follow deterministic normal network communication patterns

SCIENTIFIC IMPACT

Preempt damage before malicious activities by injecting intelligently crafted traffic:

- Understand the interdependency between cyber devices and physical components
- Disrupt adversaries' reconnaissance on smart grids' cyber-physical infrastructure.
- Mislead adversaries into designing ineffective attacks
- Develop a cyber-physical testbed integrating real network switches and smart grid simulations

SOLUTION

- Trust 1: measurement-based cyber-physical dependency analysis
  - Correlate events occurred in cyber devices and physical components
- Trust 2: network spoofing paradigm
  - Leverage software-defined networking (SDN) to spoof network traffic following the normal operational logic
  - Follow the normal communication patterns in smart grids, e.g., the specification of the network protocol
- Trust 3: decoy measurement spoofing algorithm
  - Mislead adversaries by presenting a power system different from the one under protection
  - Follow physical model, e.g., power flow equations have valid solutions

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, smart health, 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 an 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