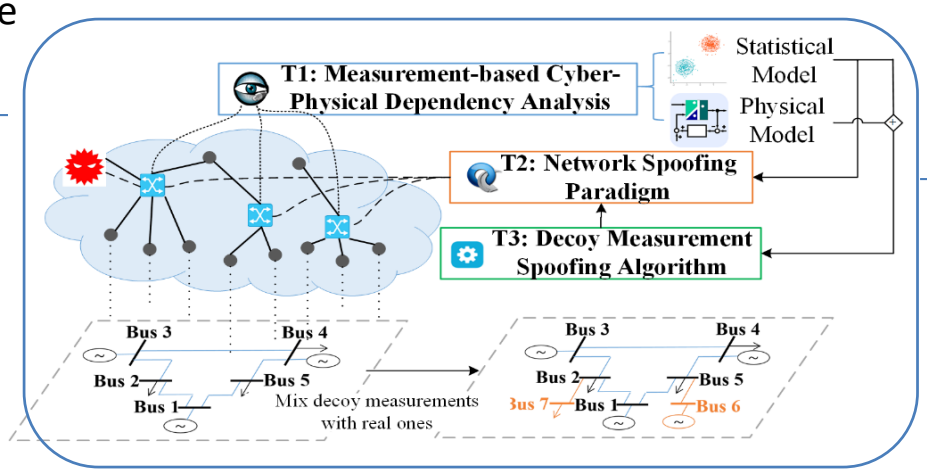
Preempting Physical Damage from Control-related Attacks on Smart Grids' Cyber-physical Infrastructure

Challenge:

- Preventing physical damage of attacks in smart grid is difficult based on passive detections
- Detecting reconnaissance activities can cause false alerts

Solution:

disrupt/mislead attackers' reconnaissance before physical damage



- Trust 1: measurement-based cyber-physical dependency analysis
- Trust 2: network spoofing paradigm
  - Leverage software-defined networking (SDN) to spoof network traffic following the normal operational logic
- Trust 3: decoy measurement spoofing algorithm
  - Mislead adversaries by presenting a power system different from the one under protection

Scientific Impact:

preempt damage before malicious activities by injecting intelligently crafted traffic:

- Disrupt adversaries' reconnaissance on smart grids' cyber-physical infrastructure
- Mislead adversaries into designing ineffective attacks

Broader Impact:

- Apply to other cyber-physical systems by instrumenting their network infrastructure
- Outreach to real utility environment
- Create and enhance a new course on CPS Security
- Integrate CPS security in other security and network courses

PI: Hui Lin, hlin2@unr.edu
Institution: University of Nevada at at Reno

Award #: 1850377