Advanced Networking Technology for Energy Delivery Systems

RAINCOAT: Randomized Network Communication in Power Grid Cyber Infrastructure to Mislead Cyber Attackers

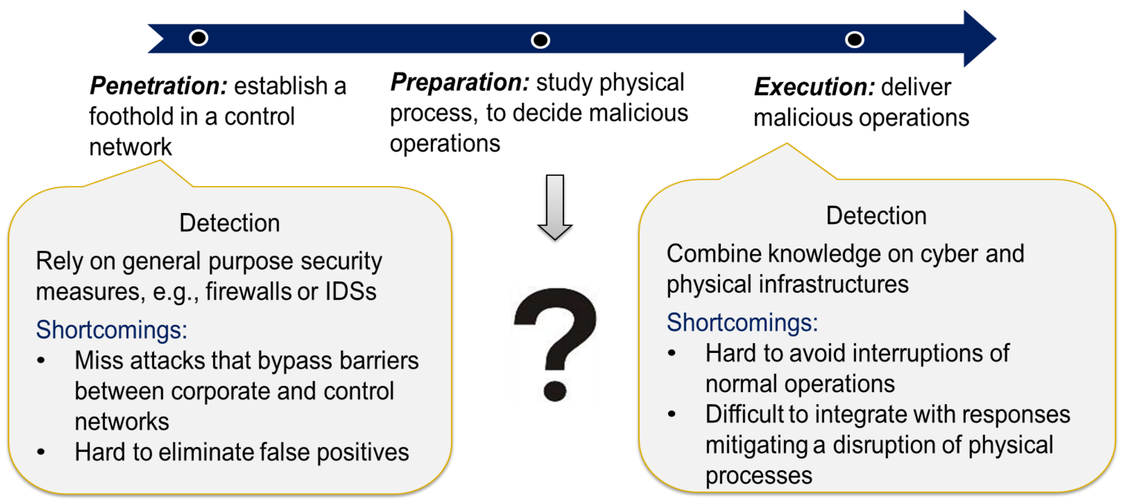
Hui Lin, Zbigniew Kalbarczyk, Ravishankar K. Iyer

GOALS

- Develop and demonstrate Raincoat, an SDN-based approach to continuously mislead an attacker into designing ineffective attack strategies.
  - Randomize network connectivity of physical devices in the power grid to increase the unpredictability in control networks.
  - Expose attacker's presence in the system and prevent system damage.
- Explore integration of Raincoat approach with an adaptive intrusion detection system such as Bro.
- Validate the approach, on a cyber-physical testbed which integrates the simulation of SDN-based communication network and power grid.
- Support *Roadmap* strategies to "Develop and Implement New Protective Measures to Reduce Risk" and "Sustain Security Improvements."

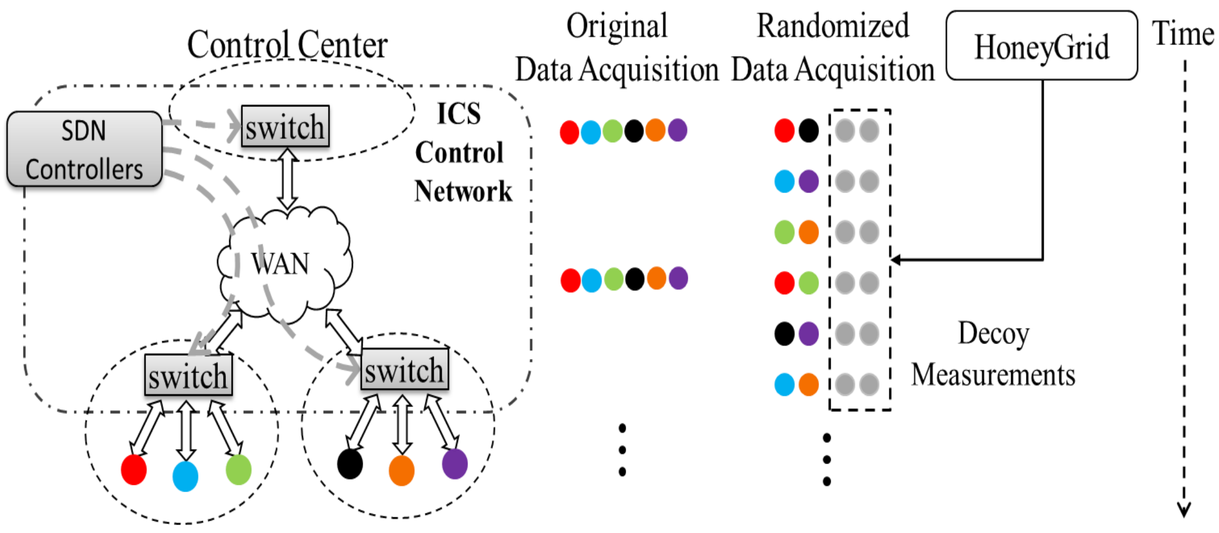
CHALLENGE OF DETECTING ATTACKS AT PREPARATION STAGE

- Attackers' reconnaissance activities introduce few to no visible traces of malicious activity.
- *Passive monitoring* of data acquisition in ICSs:
  - Communication protocols without security protection
- *Active monitoring* to scan ICS devices
  - Follow deterministic normal network communication patterns



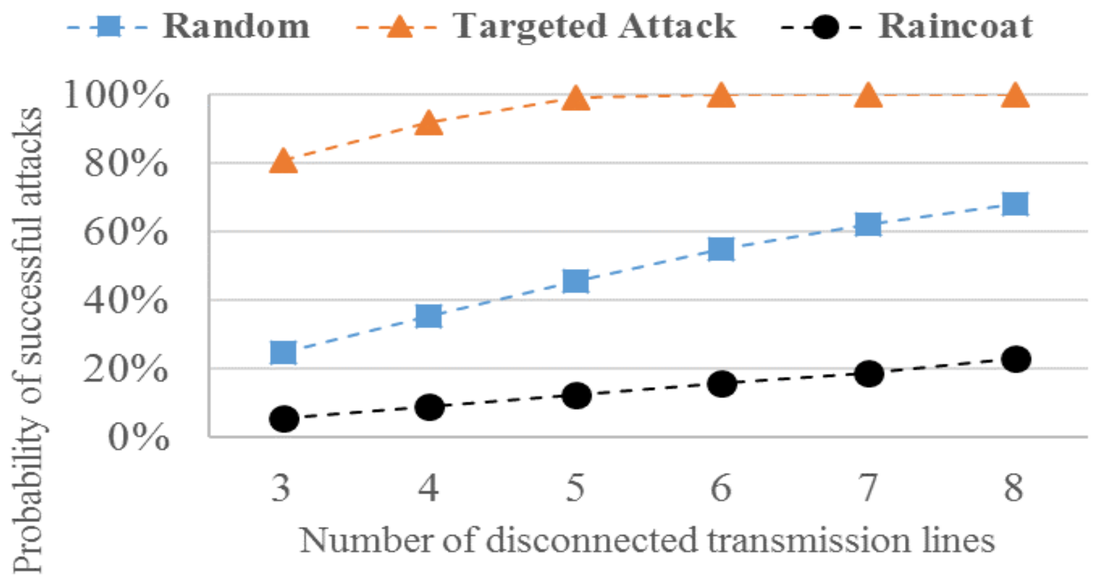
RESEARCH PLAN

- Develop SDN-based approach (called Raincoat) to manipulate network connectivity of devices in the power grid to continuously mislead an attacker into deriving ineffective attack strategies.
  - *Divide data acquisition interval into multiple sub-intervals.*
    - In each sub-interval, collect measurements from randomly selected devices (i.e., *on-line devices*).
    - Keep remaining devices off-line (i.e., no network connectivity).
  - *Use a software simulation of a power system to produce decoy measurements.*
    - Follow physical model.
    - Use real measurements from *on-line* devices.
    - Craft measurements from *off-line* devices.
- Integrate the developed approach (algorithm) with an existing SDN controller.
- Evaluate the ability of Raincoat to reduce the probability of successful attacks on simulated power grid networks.
- Evaluate implications of accidental failures and malicious attacks in the SDN-based infrastructure.



RESEARCH RESULTS

- Raincoat implementation and evaluation against: *false data injection attacks* and *control related attacks*
- Target systems
  - IEEE 24-bus, IEEE 30-bus, IEEE RTS-96 , and power systems representing three areas of Polish 400-, 220-, and 110-kV networks, namely a 286-bus, a 406-bus, and an 1153-bus systems.
- Attack scenarios:
  - *Random attack (baseline)*
    - Attackers have no (or little) knowledge of power system topology and state
    - Randomly disconnect transmission lines
  - *Targeted attack*
    - Attackers identify critical (e.g., heavy loaded) transmission lines
    - Randomly disconnect critical transmission lines
  - *Raincoat*
    - Attackers identify critical transmission lines based on decoy measurements
    - Randomly disconnect false critical transmission lines that are controlled by online devices



Probability of successful attacks (at least one transmission line is overloaded) for IEEE RTS-96 system

- Results
  - Relatively easy to achieve successful *targeted attack*
    - More than 70% of successful attacks achieve success by disconnecting 3 out of 120 transmission lines.
  - Hard to achieve successful attacks using *random* strategy
  - *Raincoat* reduces probability of successful attack below the level of the random attack.
    - Successfully hides real system state and actual device connectivity to mislead attackers into designing inefficient strategies.

INTERACTION WITH OTHER PROJECTS

- Visit Galvin Microgrid at Illinois Institute of Technology to initiate collaboration.
  - Collect real measurements related to operations at power systems' distribution networks.
- Collaborate with the Advanced Digital Sciences Center (ADSC)
  - Under the project *Towards a Resilient Smart Power Grid: A Testbed for Design, Analysis, and Validation of Power Grid Systems*

FUTURE EFFORTS

- Randomize networks that include data acquisition with short collection period, e.g., PMU measurement collection.
  - Prioritize measurements that experience big changes.
  - Randomize measurements for other devices.
- Evaluate implications of accidental failures and malicious attacks in the SDN-based infrastructure.
- Integrate the proposed approach with an adaptive intrusion detection system (e.g., Bro) to support detection and response to attacks against SDN based networks.

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY