RAINCOAT: RAndomization of Network Communication in Power Grid Cyber INfrastructure to Mislead Attackers

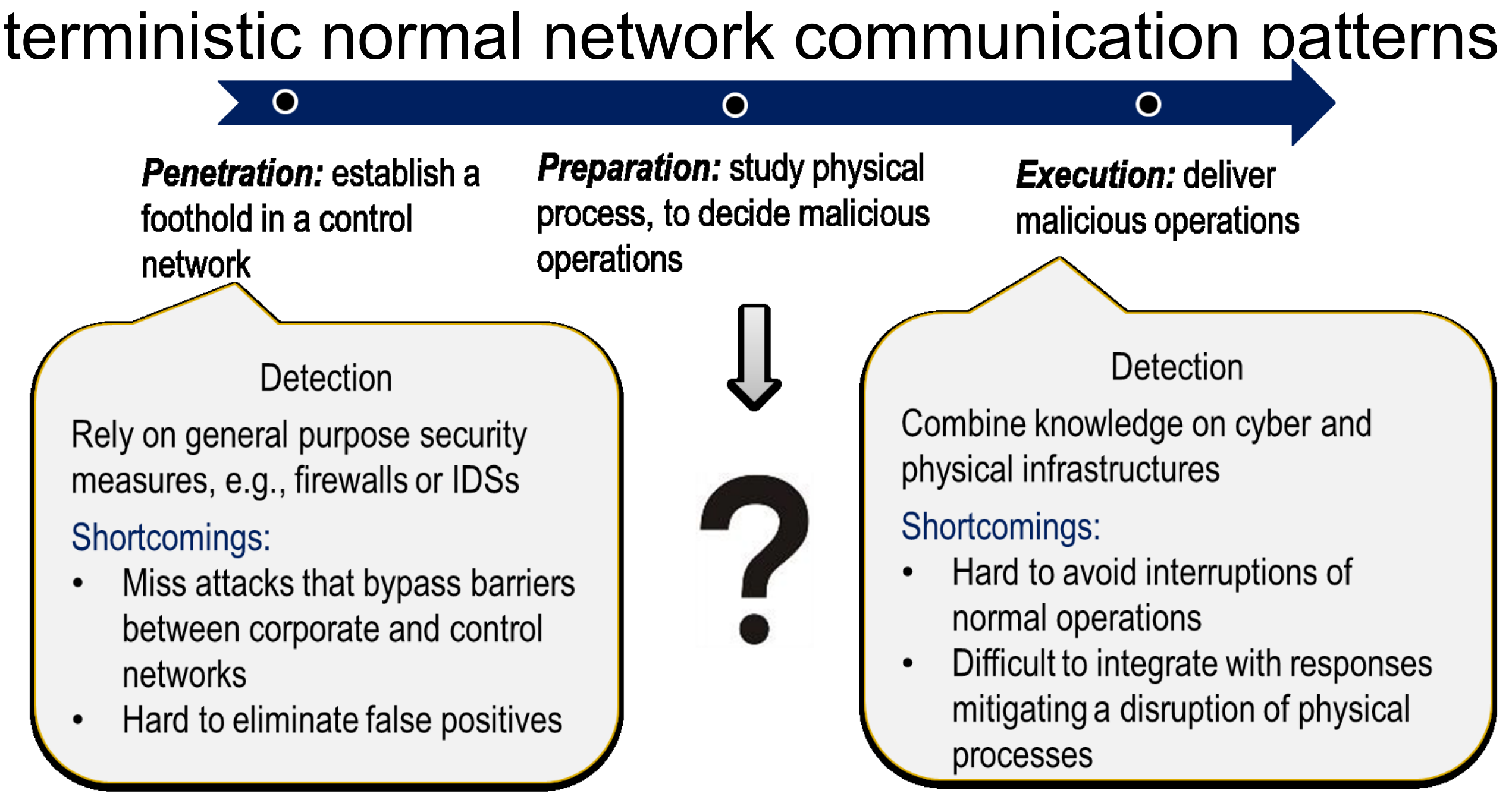
Hui Lin, University of Nevada, Reno (hlin2@unr.edu)

GOALS

- Randomize network connectivity of intelligent electronic devices (IEDs)
  - Increase the unpredictability in control networks
  - Expose attackers when accessing to “off-line” devices
  - Limit information collected by attackers to design attack strategies
- Intelligent spoofing of responses for “off-line” devices
  - Prevent attackers from learning the randomized connectivity
  - Include decoy measurements to mislead attacker
- Implementation
  - Use Software-defined Networking (SDN) to manipulate network flows that deliver power system’s physical operations

CHALLENGE OF DETECTING ATTACKS AT PREPARATION STAGE

- Attackers’ reconnaissance activities introduce little anomaly at the network level
- Passive monitoring of data acquisition:
  - Communication protocols without security protection (e.g., encryption or two-factor authentication)
  - Does not solve all problems
- Active monitoring to scan IEDs
  - Follow deterministic normal network communication patterns



Penetration: establish a foothold in a control network

Preparation: study physical process, to decide malicious operations

Execution: deliver malicious operations

Detection

Rely on general purpose security measures, e.g., firewalls or IDSs

Shortcomings:

- Miss attacks that bypass barriers between corporate and control networks
- Hard to eliminate false positives

?

Detection

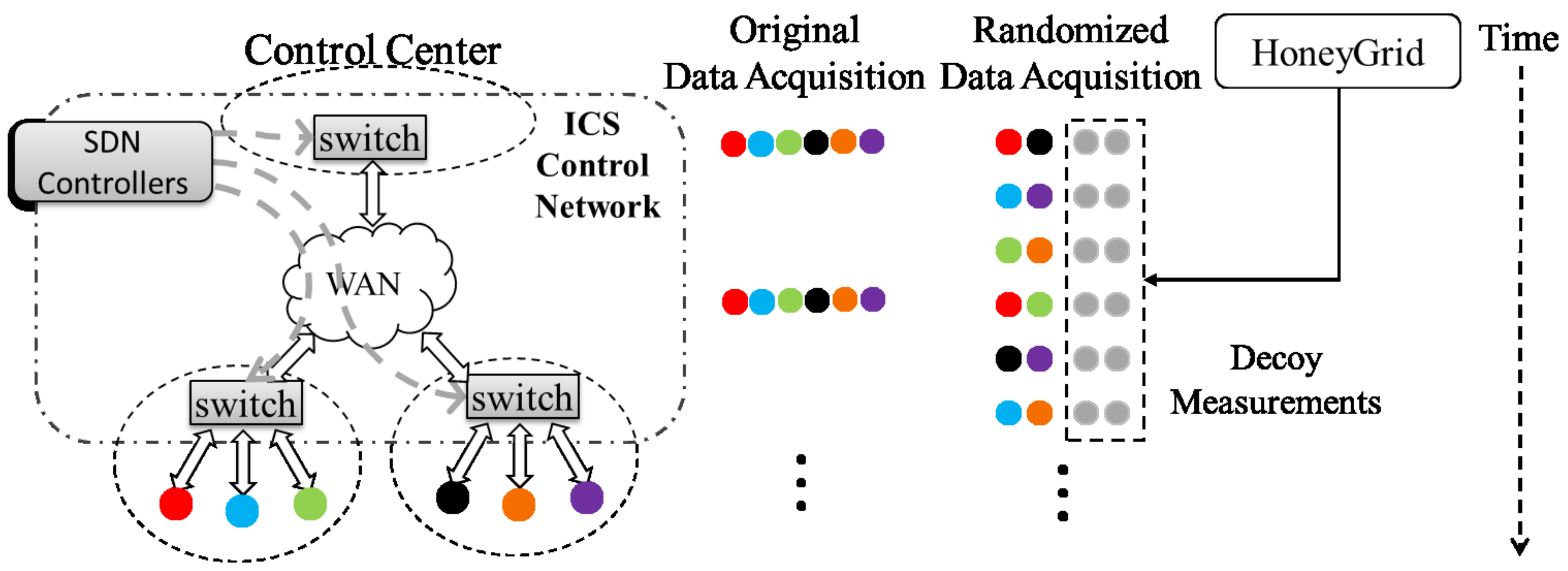
Combine knowledge on cyber and physical infrastructures

Shortcomings:

- Hard to avoid interruptions of normal operations
- Difficult to integrate with responses mitigating a disruption of physical processes

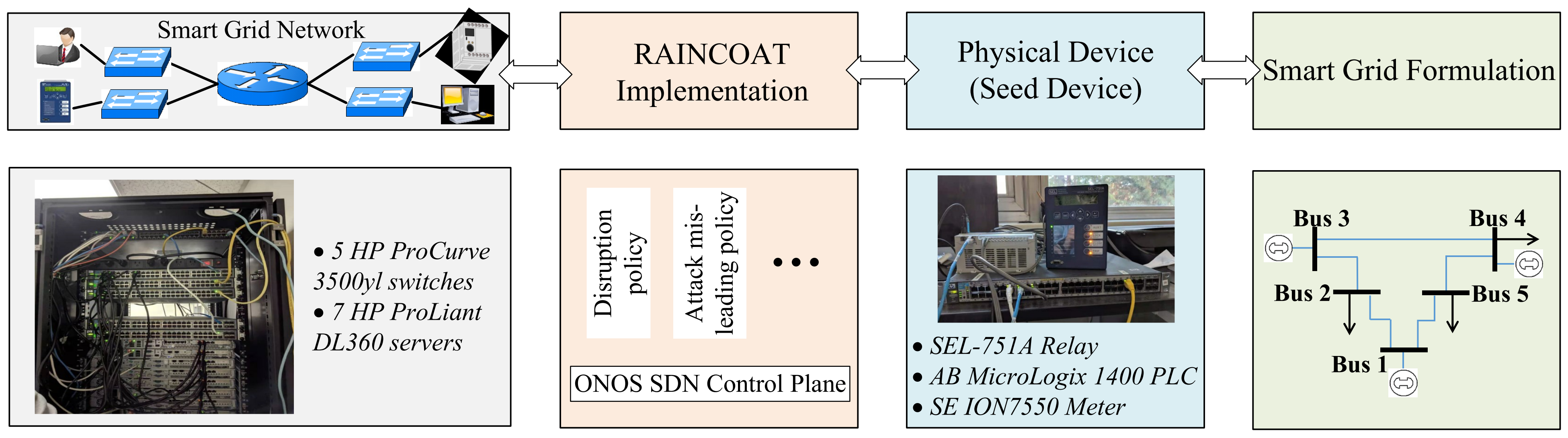
DESIGN OVERVIEW

- Normal data acquisition
  - Periodically collect measurements from all devices
- Divide the acquisition interval into multiple sub-intervals
  - In each sub-interval, collect measurements from randomly selected devices
- Craft decoy measurement: a software simulation of a power system that produces decoy measurements
  - Craft measurements to mislead attackers
  - Follow physical model, e.g., power flow equations have valid solutions
- Procedure
  - To mislead attackers: reverse the order of power flows in decoy measurements
  - To follow physical model: execute state estimator, and use the computed state estimation error to refine measurements



CYBER-PHYSICAL TESTBED

- Construct communication networks based on HP switches
- Use real IEDs from three different vendors
- Simulate power grids in MATPOWER
- Implement RAINCOAT based on ONOS SDN controller

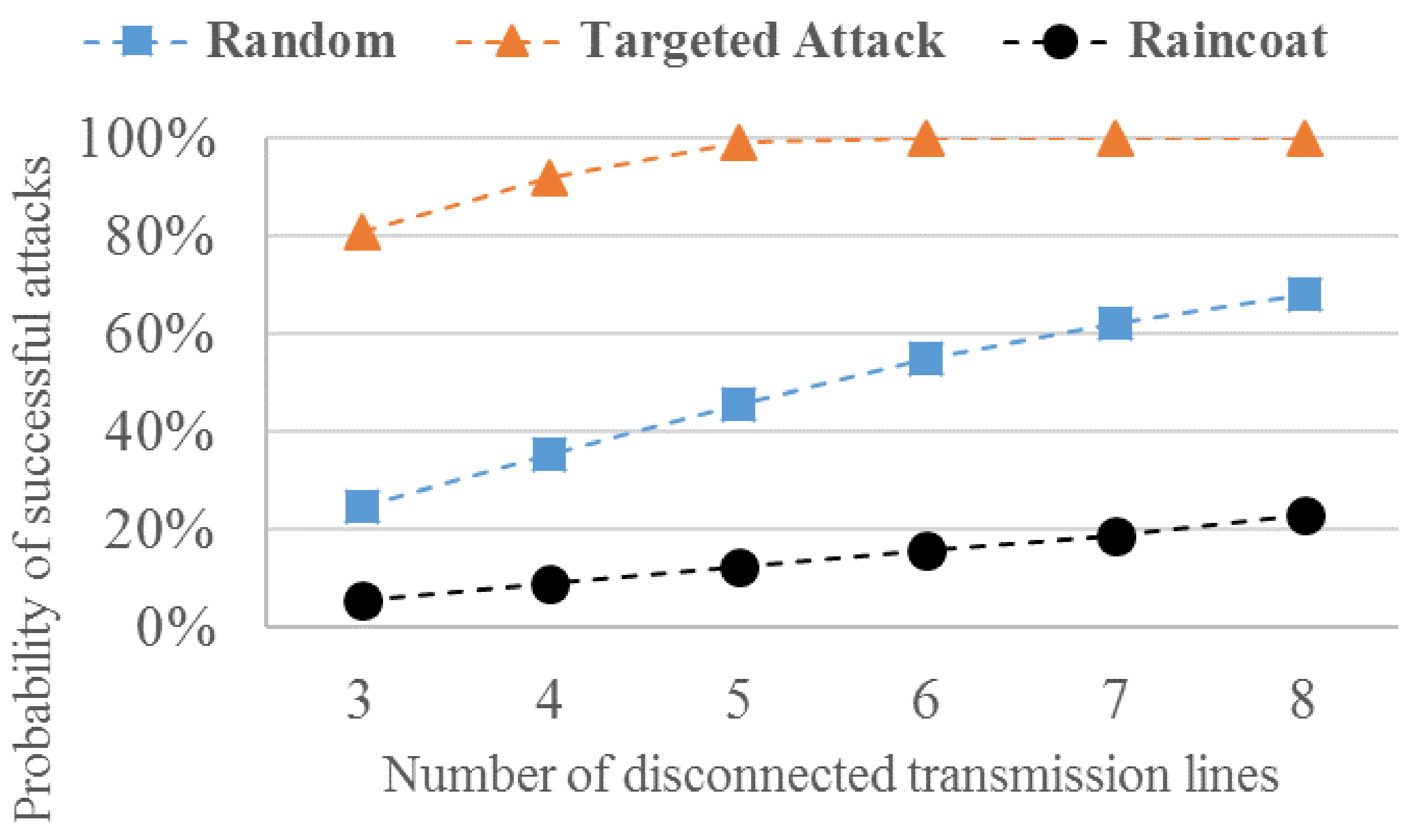


- *5 HP ProCurve 3500yl switches*
- *7 HP ProLiant DL360 servers*

- *SEL-751A Relay*
- *AB MicroLogix 1400 PLC*
- *SE ION7550 Meter*

EVALUATION

- Security evaluation
  - Disconnect multiple transmission lines
  - Successful attacks: at least one remaining transmission line is overloaded
- Random attack (baseline)
  - Attackers have no (or little) knowledge of power system topology and state
  - Challenging to be successful
- Targeted attack
  - Attackers identify critical (e.g., heavy loaded) transmission lines
  - Randomly disconnect critical transmission lines
  - Easy to be successful: more than 70% of successful attacks by disconnect 3 out of 12 critical lines
- Raincoat
  - Attackers identify critical transmission lines in decoy measurements
  - Randomly disconnect false critical transmission lines
  - More challenging than Random attacks, successfully misleading attackers



RTS-96 (IEEE Reliability Test System)

SELECTED PUBLICATIONS

- **Hui Lin**, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "RAINCOAT: RAndomization of Network Communication in Power Grid Cyber INfrastructure to Mislead Attackers,“ *IEEE Transactions on Smart Grid*, September, 2019.
- **Hui Lin**, "SDN-based In-network Honeypot: Preemptively Disrupt and Mislead Attacks in IoT Networks," in *Proceedings of the first International Workshop on Security and Privacy for the Internet-of-Things (IoTSec '18)*, April 17th, 2018.