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

Hui Lin, Zbigniew Kalbarczyk, Ravishankar Iyer

University of Illinois at Urbana-Champaign

Motivation

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

?

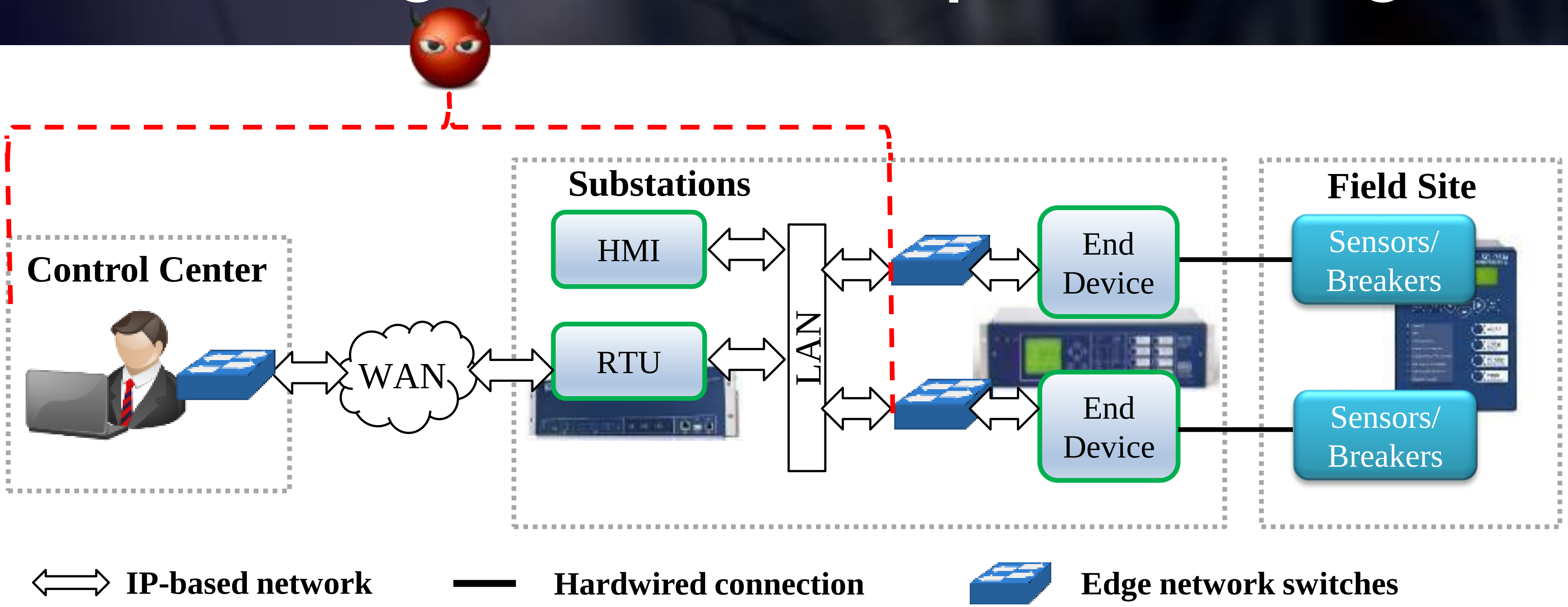
Detection

Combine knowledge on cyber and physical infrastructures

Shortcomings:

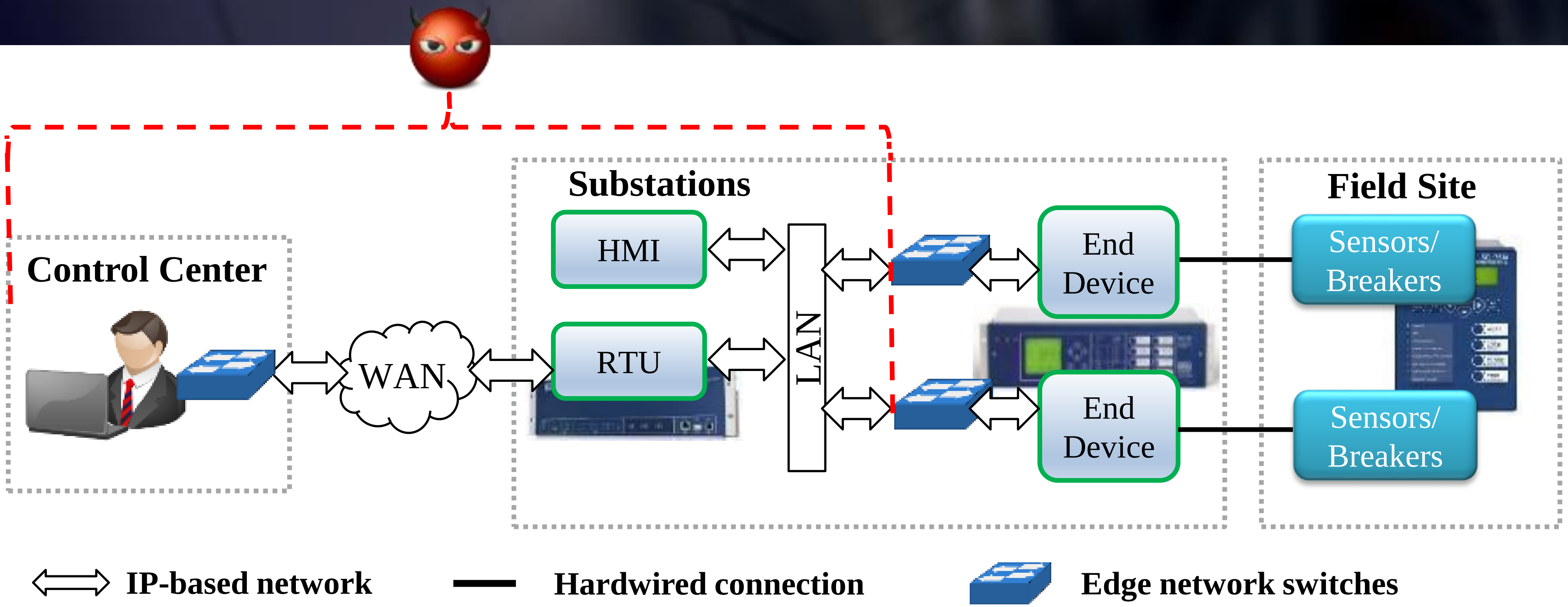
- Hard to avoid interruptions of normal operations
- Difficult to integrate with responses mitigating a disruption of physical processes

Detecting Attacks at Preparation Stage



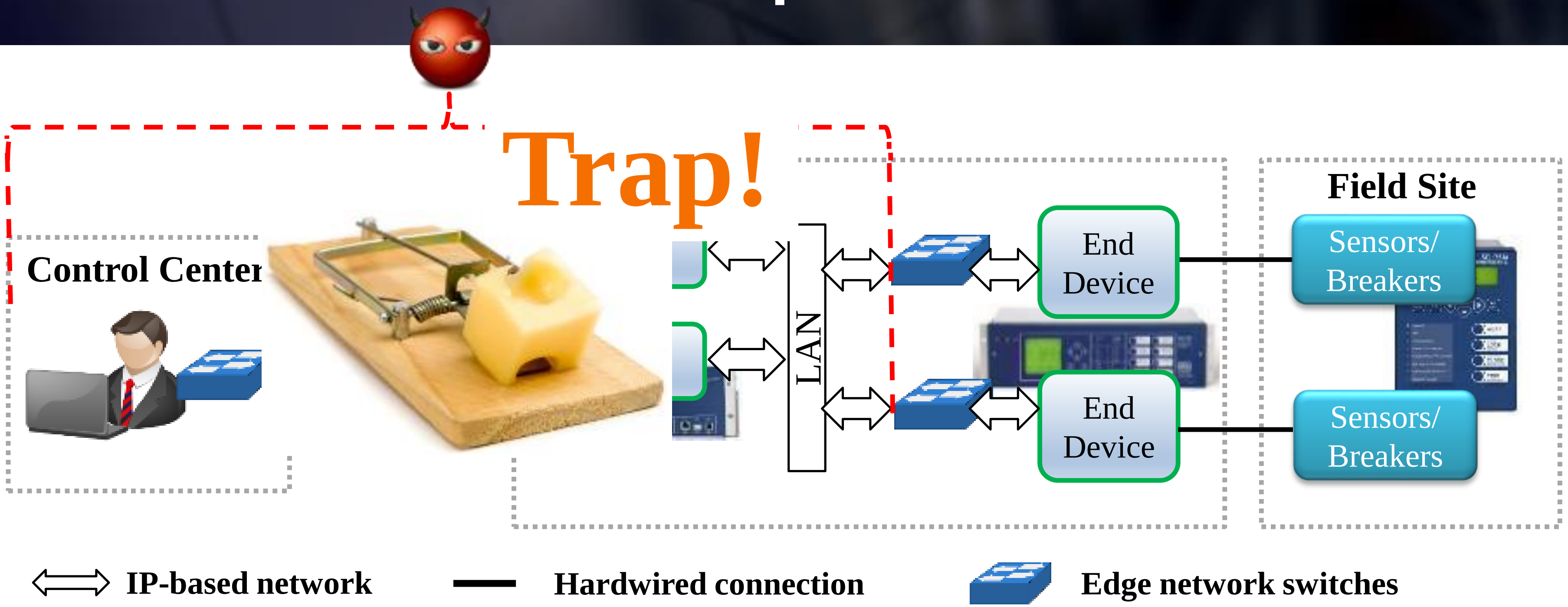
- Attackers' reconnaissance operations introduce little anomaly
  - Monitor measurements to prepare a strategy
- Active monitoring
  - Use legitimate requests to obtain measurements
- Passive monitoring
  - Observe measurements from existing data acquisitions

Threat Model



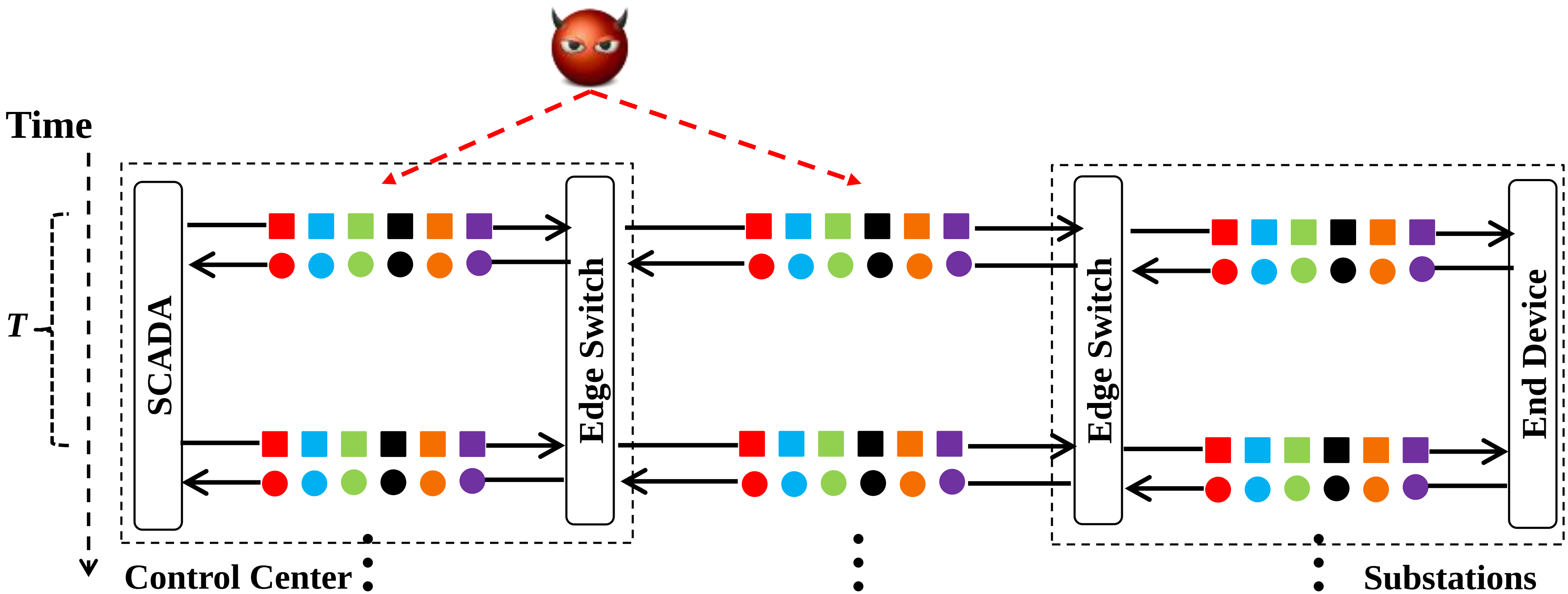
- In *control networks*, attackers can penetrate computing devices on any communication path that connects the control center and end devices
  - e.g., establish footholds in HMI or RTU or laptops connected to WAN
- In *control center*, we trust the integrity of state estimation software
- In *substations*, we assume that attackers cannot physically access end devices, sensors, and breakers
- We trust the integrity of *edge switches*, which are used to manipulate network traffic to disrupt and mislead attacks

What Do We Propose - Raincoat



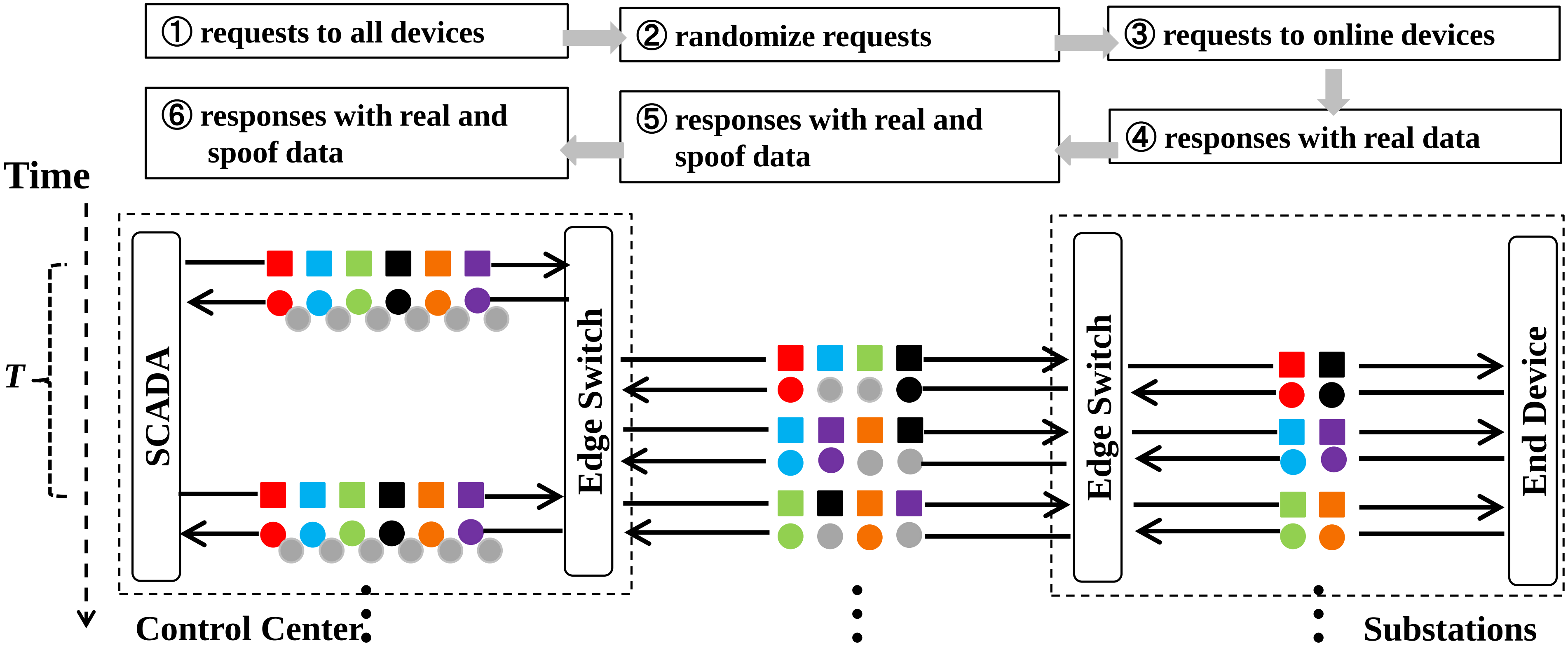
- RAINCOAT: randomize network communication in power grid cyber infrastructure to mislead cyber attackers
  - Disrupt attackers: increase unpredictability in networks
  - Mislead attackers: craft decoy measurements

Normal Periodic Data Acquisition



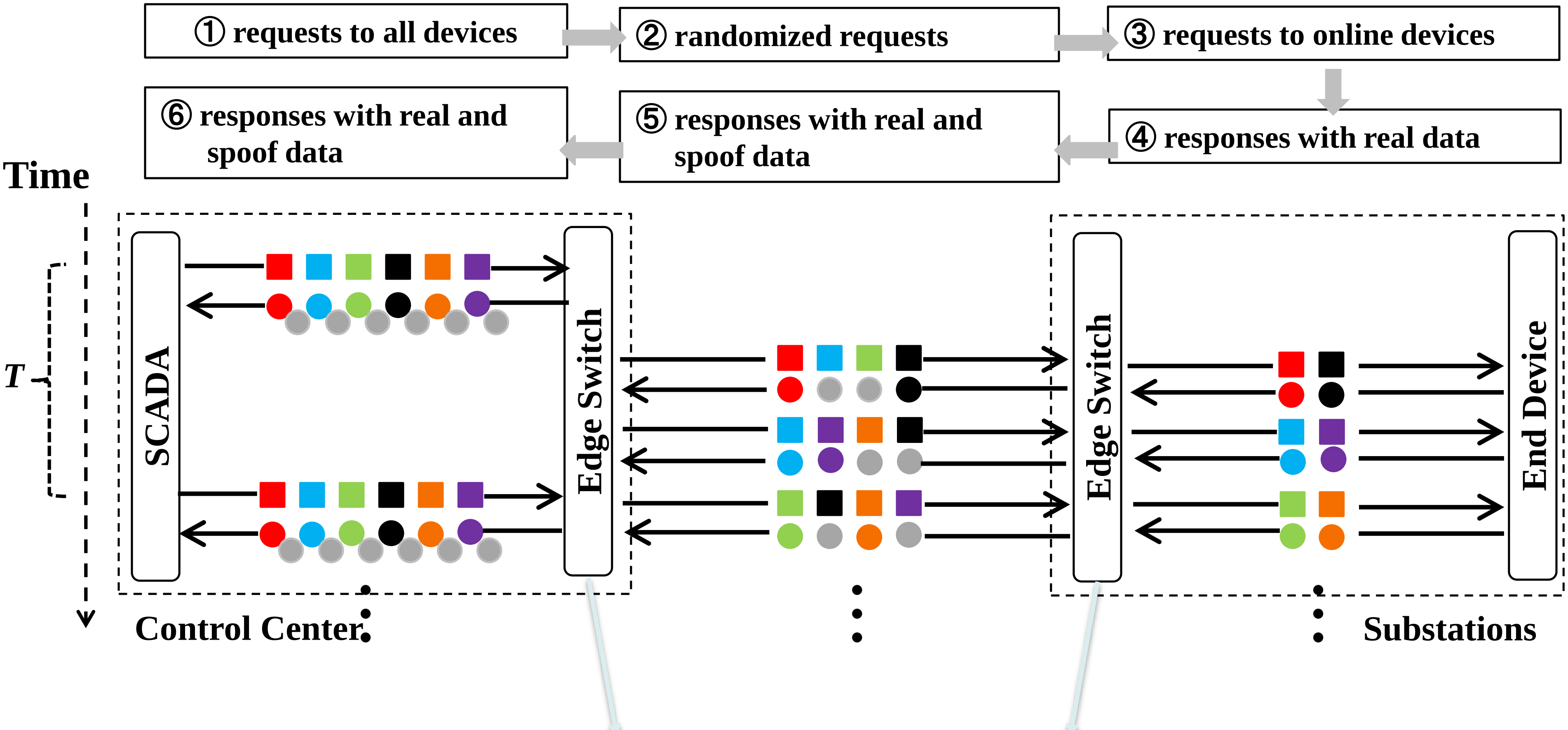
- SCADA master issues data acquisition requests to all end devices periodically
  - *T* ranges from 1 to 10 seconds (based on IEEE Std 1646)

Randomize Data Acquisition



- Objective of Raincoat:
  - Obfuscate attackers with randomized device connectivity and the mix of real and spoofed data
  - Allow system operators collecting measurements from all devices with the same interval

Implementation with SDN



- SDN controller:
  - Randomize data acquisition request
  - Spoof measurements on behalf of off-line devices
- Small changes on existing cyber-physical infrastructure

Craft Decoy Measurements to Mislead Attackers

- Based on decoy measurements, adversaries will not design effective attack strategies
  - In false data injection attacks (FDIA), compromised measurements do not bypass the bad data detection in the state estimation
  - In control-related attacks (CRA), compromised control commands do not lead to physical damage

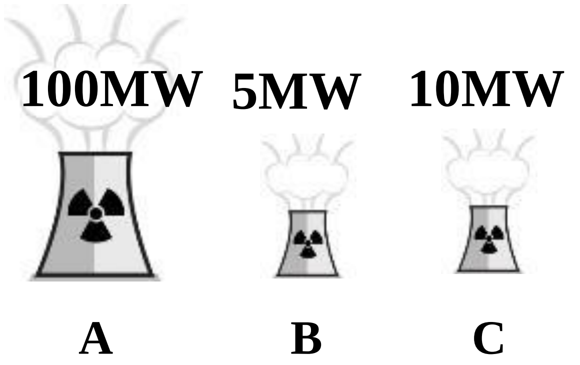
Type	*Preconditions*	*Target*
FDIA	B_{jk}, susceptance of all transmission lines	P_j^G and P_j^L of all substations; P_{jk} of all transmission lines
CRA	P_j^G, Q_j^G, P_j^L, Q_j^L (active/reactive power generation and consumptions) of all substations; P_{jk}, Q_{jk} (active/reactive power flows) of all transmission lines	Control commands that can disconnect transmission lines or substations in a power grid

Procedure to Craft Decoy Measurements

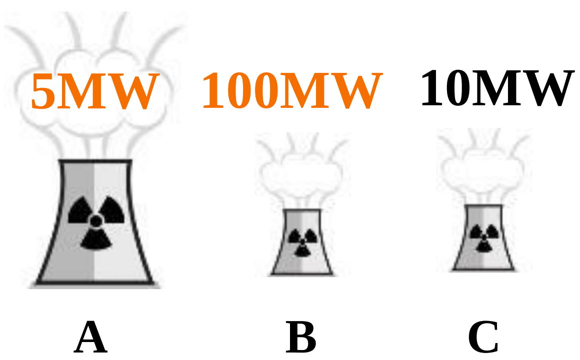
- Step 1: set initial misleading values
  - Step 1.a: mislead FDIAs (false data injection attack)
    - Decide susceptance of all transmission lines
  - Step 1.b: mislead CRAs (control-related attacks)
    - Decide power flows of transmission lines

- Step 2: refine the values based on physical model
  - Iteratively use the results/errors from state estimation to:
    - adjust initial values
    - determine remaining measurements

Step 1: Mislead Control-Related Attacks



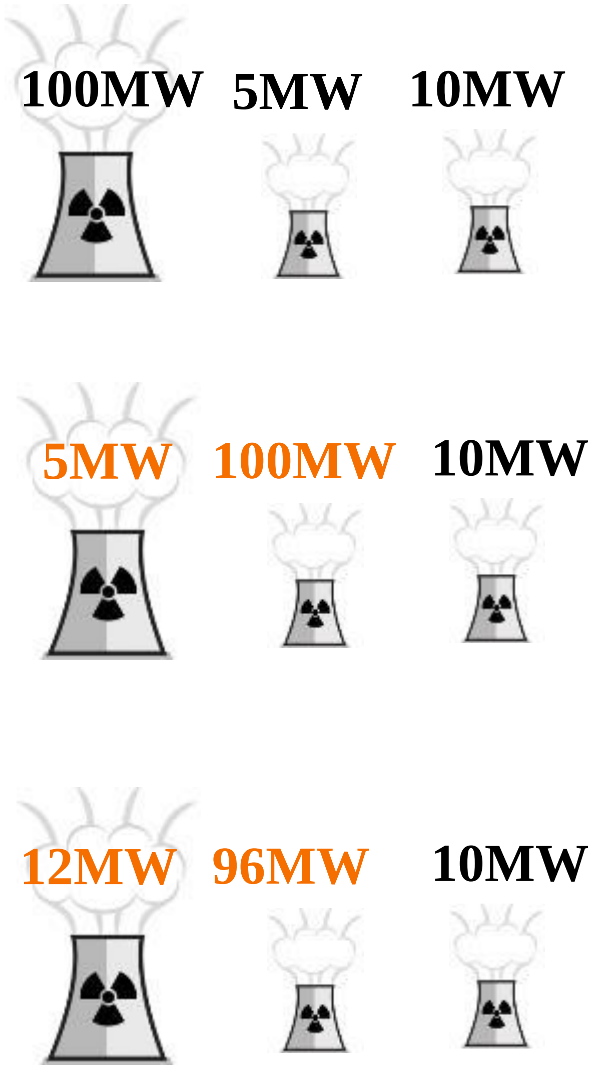
Real Measurements



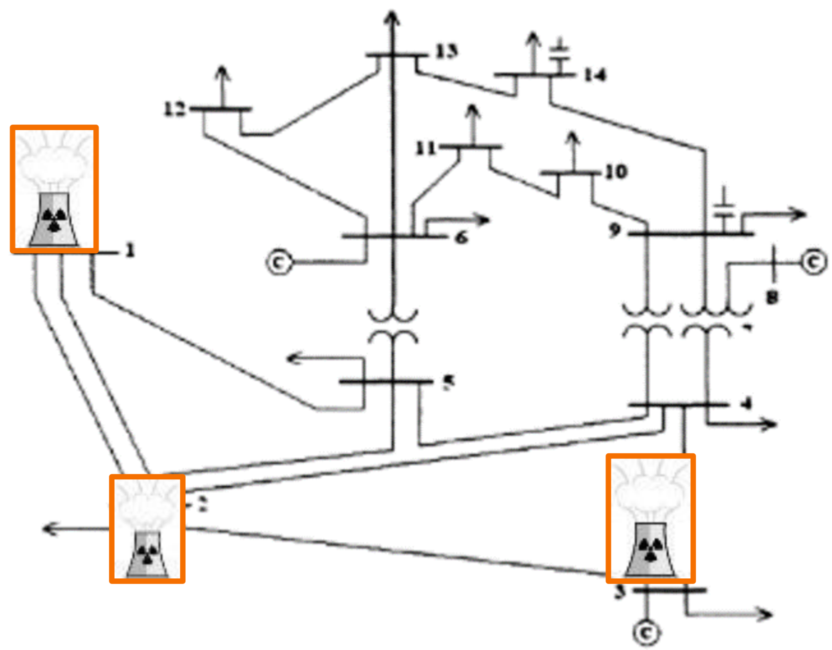
Decoy Measurements

- Attack objective:
  - Use commands to disconnect multiple transmission lines to cause overloading lines
- Attack prerequisite:
  - Identify critical transmission lines, which deliver heavy power flows
- Protection
  - Craft decoy measurements such that attackers always target transmission lines that deliver light power flows

Step 2: Refine Measurements



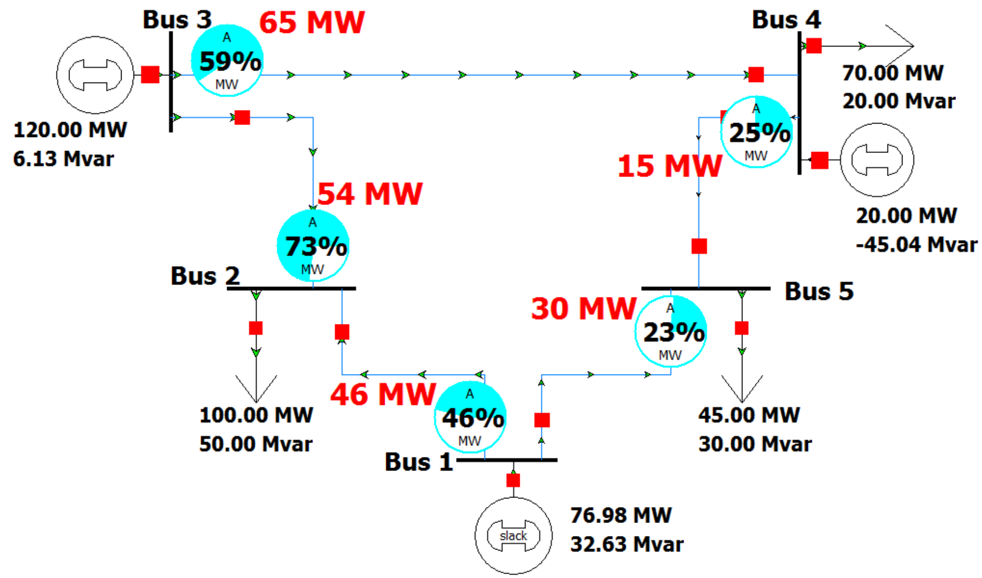
- Adjust measurements based on errors from state estimation
- Repeat until errors become small enough
  - Bypass the bad data detection



Evaluation Setup

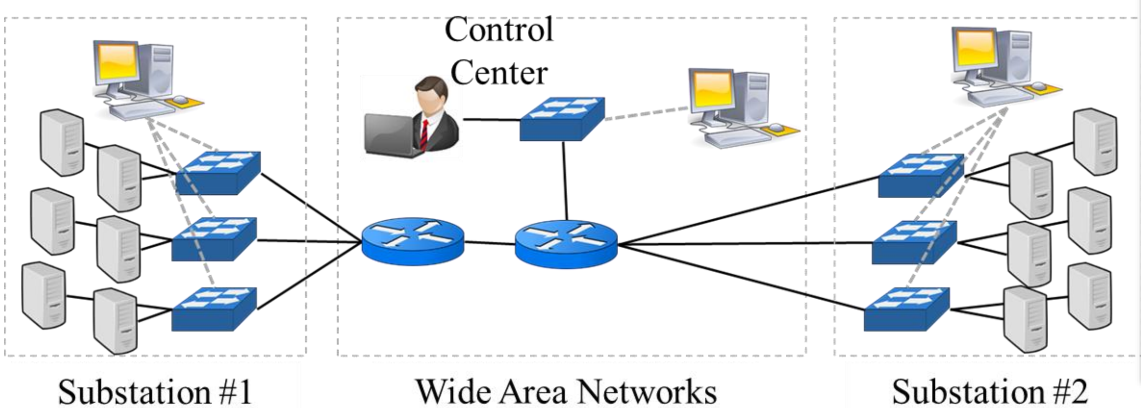
Use Matpower to simulate power systems

- Estimate state after a command is executed



Execute (attack) command transmitted in real networks

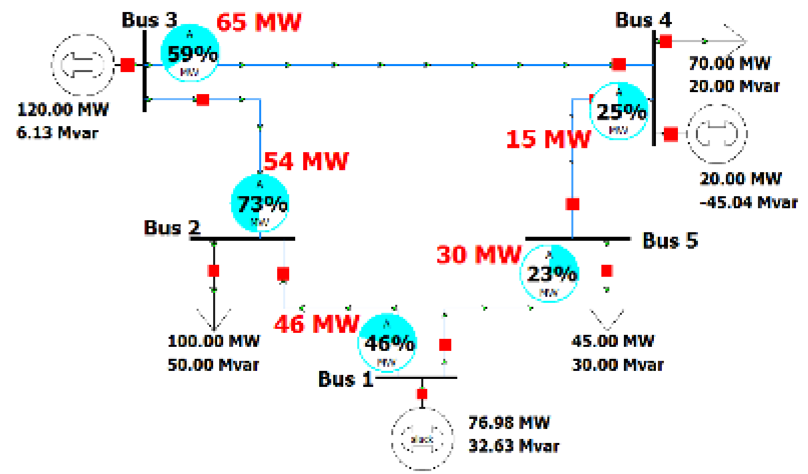
Use power measurements to build network traffic



- Use Geni testbed (including SDN hardware switches) to construct control networks
  - Control center collects measurements or issues commands to end devices

Security Evaluation

- Performed by numerical simulation in Matpower
  - IEEE 24 bus, 30 bus, RTS-96, 286-bus, 405-bus, and 1153-bus systems
- Evaluation of control-related attacks
  - Issue malicious commands that disconnect transmission lines
  - measure the probability of successful attacks
- With Raincoat, the probability of successful attacks is reduced from 70% to 5% (for 1153-buses system)
  - smaller than the probability observed in random attacks

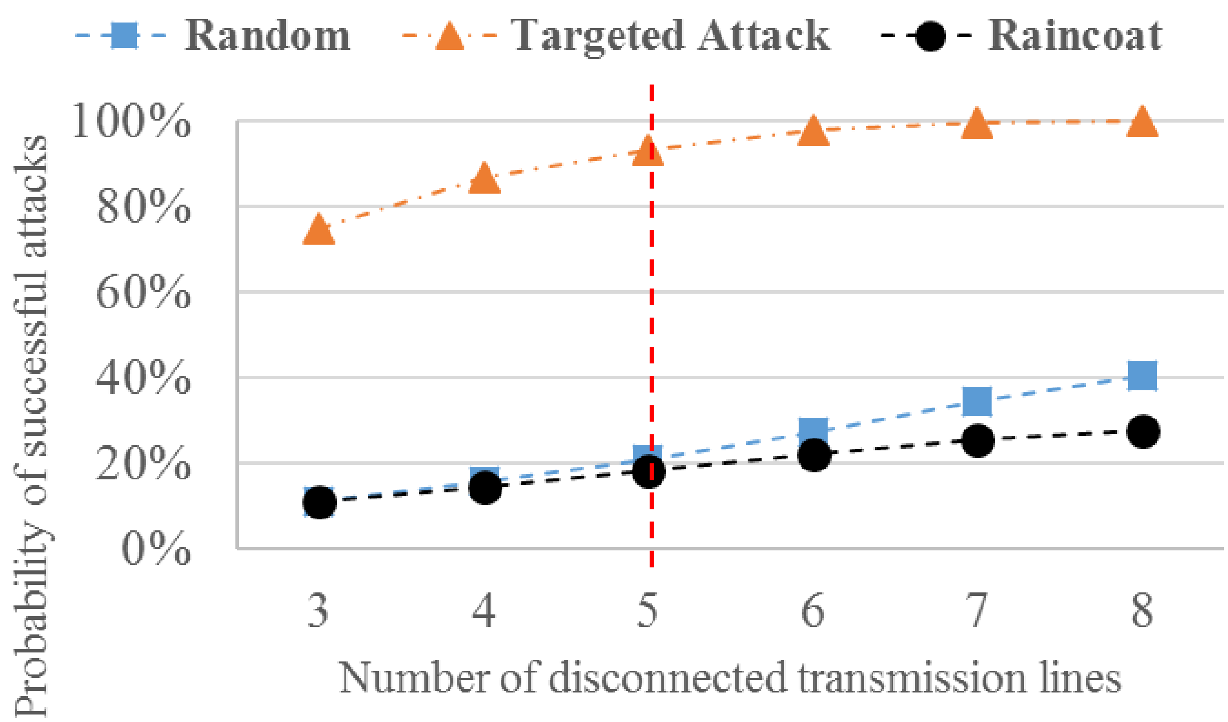


- Evaluation of false-data injection attacks
  - Compromise measurements
  - Measure the probability of successful attacks, which bypass the bad data detection
- With Raincoat, all these evaluated attacks are detected

Evaluation of Control-Related Attacks

- Implement malicious commands that disconnect multiple transmission lines; measure the probability of attacks that cause overloading remaining lines
  - **Targeted attack**
    - Attackers identify critical (e.g., heavy loaded) transmission lines
    - Randomly disconnect critical transmission lines
  - **Raincoat**
    - Attackers identify critical transmission lines from decoy measurements
    - Randomly disconnect false critical transmission lines
  - **Random attack (baseline)**
    - Attackers have no (or little) knowledge of power system topology and state
    - Randomly disconnect transmission lines

Evaluation of Control-Related Attacks

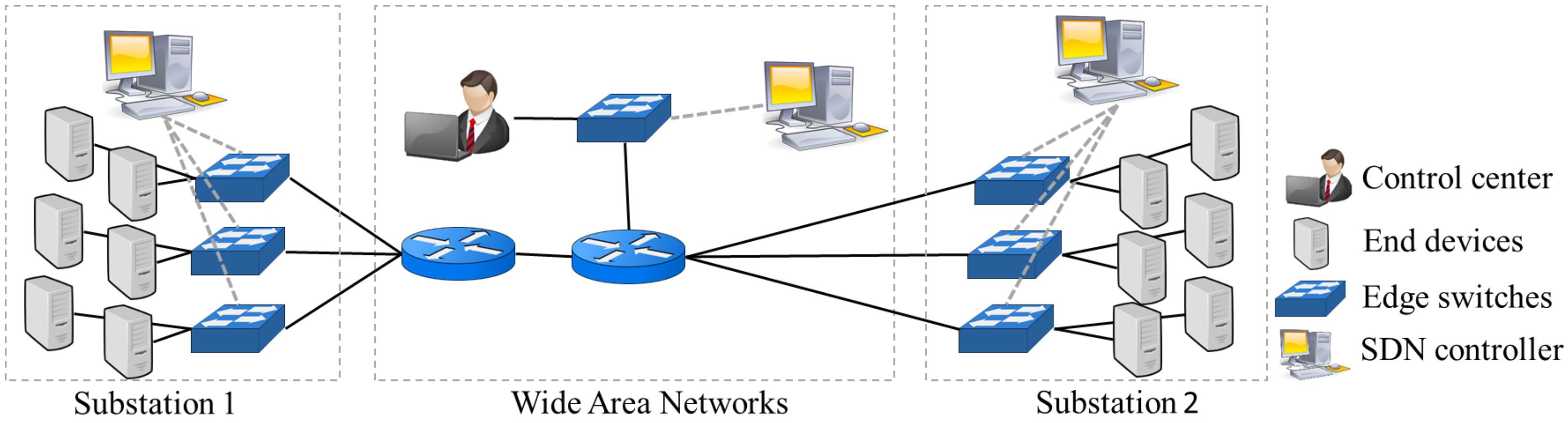


RTS-96; IEEE Reliability Test System, including 73 buses and 120 transmission lines)

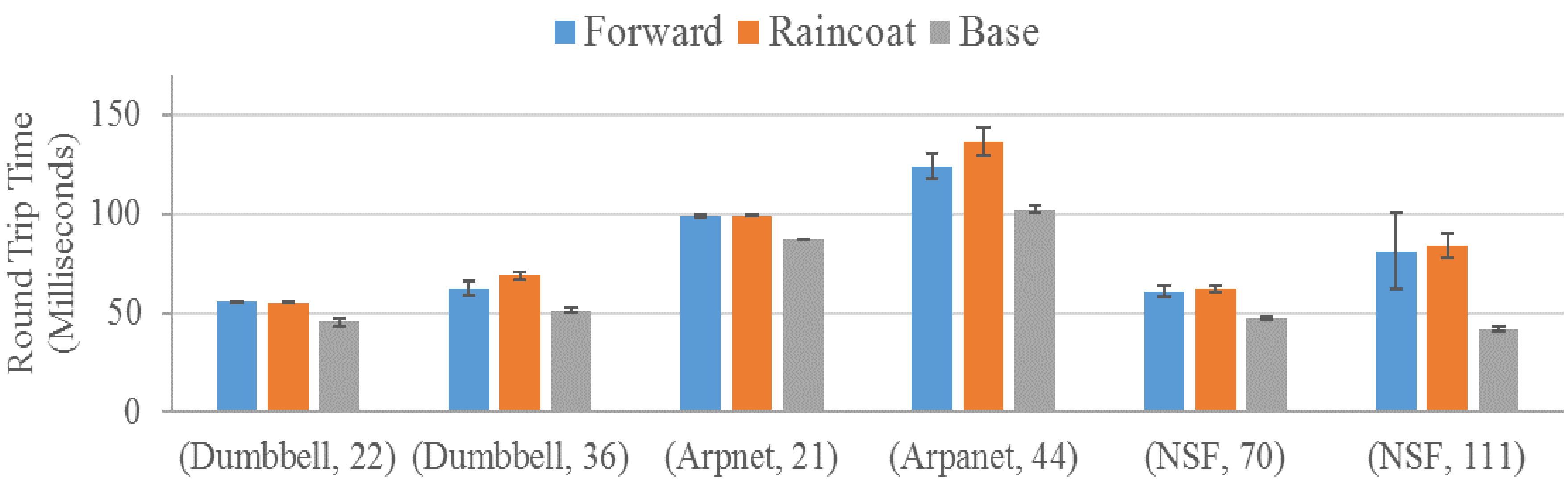
- Probability of successful attacks reduced from 90% (for targeted attack) to below 20% (when using Raincoat)
  - less than for random attacks (attackers have no system knowledge)
- Attack introduces little disturbance even if the malicious command is executed

Performance Evaluation

- Performed in constructed control networks of six different topologies
- Measure the delay of communication caused by Raincoat:
  - Latency between edge switches and SDN controllers
  - Latency of SDN controllers constructing spoofed measurements



Performance Results



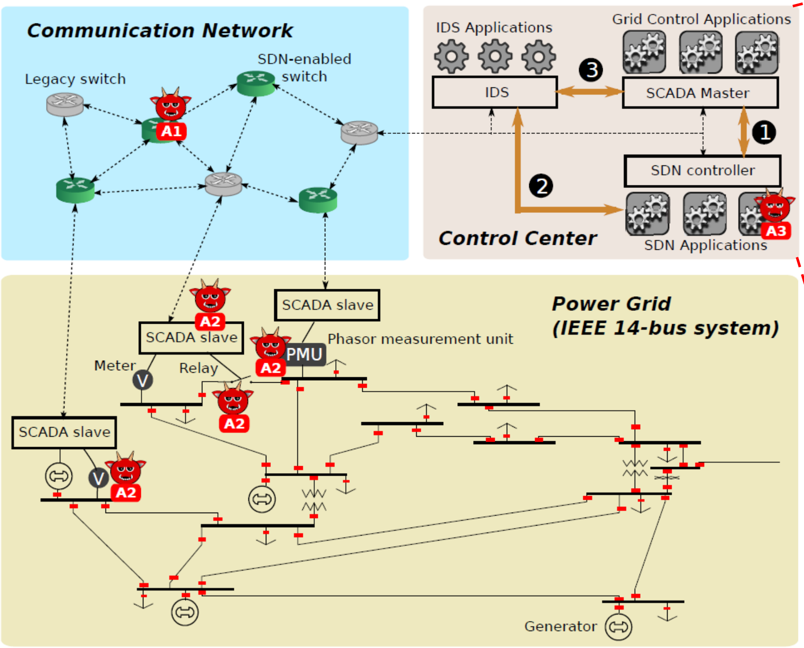
- **Raincoat** introduces less than 6% overhead (on average) as compared with SDN *Forward* flow control mechanisms
- When using Raincoat, the control network still meets the requirement of communication latency (in IEEE Std 1646)

Conclusions

- RAINCOAT: randomizes network communication in power grid cyber infrastructure to mislead cyber attackers
  - Randomize network connectivity of end devices
    - Disrupt adversaries' knowledge to prepare attacks
    - Expose an attacker presence in the system
  - Craft decoy measurements
    - Mislead adversaries' into designing ineffective attacks

- Decoy measurements to mislead attackers into designing:
  - False data injection attacks that **cannot pass the state estimation**
  - Control-related attacks whose **probability of generating physical damage is reduced to less than 5%**

Future Direction



Architecture of an SDN-enabled grid

Research Goals

Integrated Intrusion Detection Framework for SCADA (based on Bro)

Network analyzer for SCADA protocols (DNP3)

RAINCOAT, an SDN-based approach to randomize network communication in Power Grid cyber infrastructure to mislead attackers

- randomize (using SDN) network connectivity of devices in substations to obfuscate system state
- mislead an attacker into designing ineffective attack strategies
- expose an attacker presence in the system

Fast state estimation to detect and mitigate control-related attacks

- combine network monitoring with fast state estimation to predict consequence of malicious commands

Experimental validation of the framework

- use cyber-physical co-simulation testbed
- injection of faults and malicious attacks