Combining Simulation and Emulation for Evaluation of Secure and Resilient Cyber-Physical Systems

Kevin Jin

Department of Computer Science

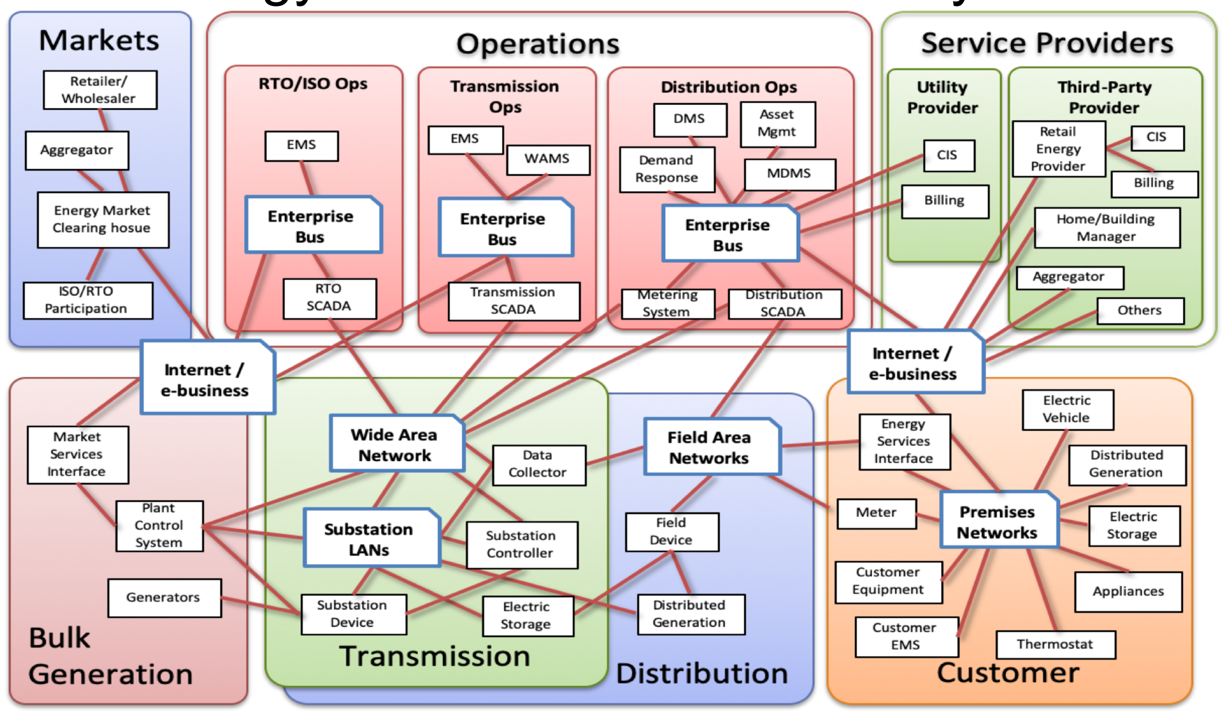
Illinois Institute of Technology

ILLINOIS INSTITUTE OF TECHNOLOGY
College of Science

Cyber-Physical Systems

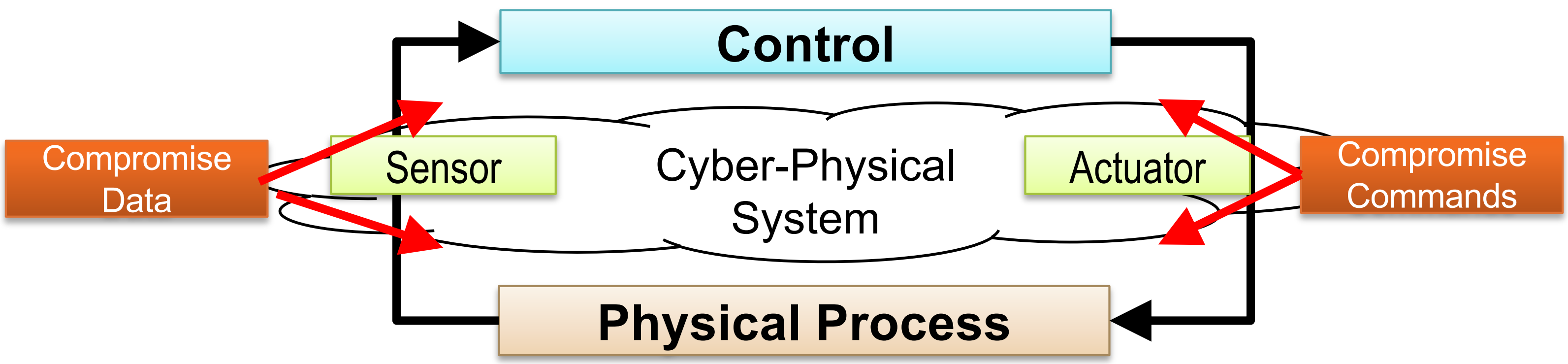
- Control many critical infrastructures
- Increasingly adopt Internet technology to boost control efficiency

More Efficient or More Vulnerable?



Picture source: NIST Framework and Roadmap for Smart Grid Interoperability Standards

Cyber Threats in Power Grids



POLITICS THE WALL STREET JOURNAL.

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say July 23, 2018 7:21 p.m. ET

Blackouts could have been caused after the networks of trusted vendors were easily penetrated

WSJ.com - U.S. regulator says knocking out nine key substations could cause nationwide blackout

THE DAILY SIGNAL

Ukraine Goes Dark: Russia-Attributed Hackers Take Down Power Grid

NATIONAL SECURITY 1 comments

Stuxnet Raises 'Blowback' Risk In Cyberwar

Researchers uncover holes that open power stations to hacking

Hacks could cause power outages and don't need physical access to substations.

Protection of Cyber-Physical Systems

- Commercial off-the-shelf products
  - e.g., firewalls, ids, anti-virus software
- How to enforce system-wide requirements?
  - Resilience, Security, Performance
- How to safely incorporate advanced networking technologies into critical control systems?
  - Real-time operations
  - Large-scale networks
  - Lack of real testbed (unlike the Internet)
- Problem Statement
  - **Develop a scalable and high-fidelity testbed for evaluating cyber effects on the physical system**

Evaluation Methodology

Many options to evaluate cyber-physical systems

Theoretical

Analytical evaluation involves developing models and methods and is a low cost but potentially complex solution

Simulation

Simulation uses models to evaluate systems through virtual time to replicate the outcome of a process. Simulation lacks the fidelity of real systems

Emulation

Emulation replicates the way that a process operates. It may have greater fidelity but physical and scalability limitations.

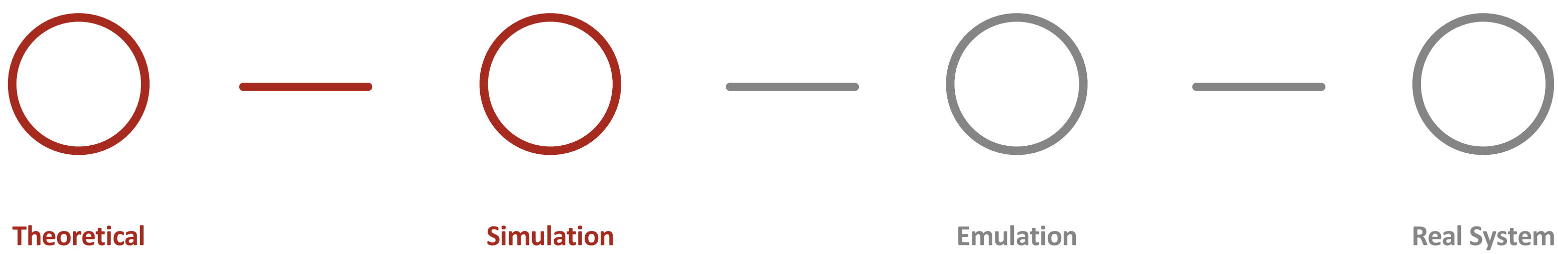
Real System

Real systems are the highest fidelity but have high costs associated with them.

Evaluation Methodology

Theoretical and Analytical

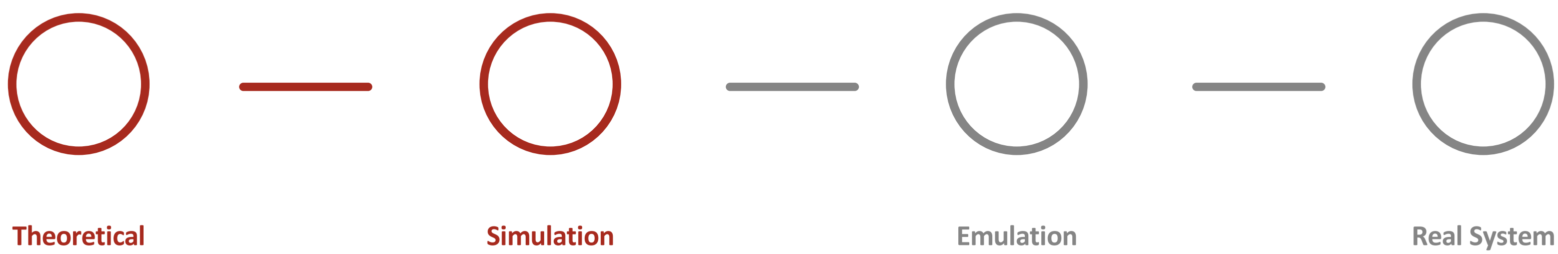
- Algorithms and equations, i.e., Temporal Logic, Hoare Logic, etc.
- Capture the behavior of a system
- Provide closed form solution



Evaluation Methodology

Simulation

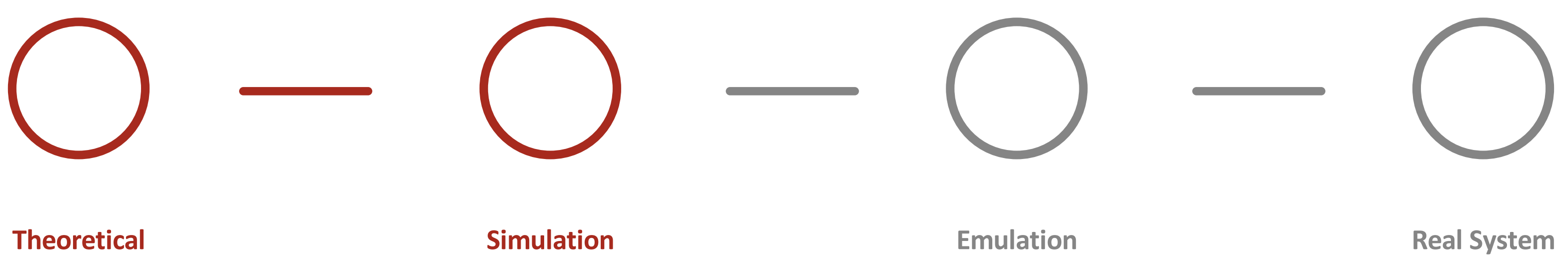
- Execution and interaction of models
- Replicates the results of a process / event
- Executes events to advance clock
- Many types of simulation:
  - Discrete Event, Agent Based, Continuous, Analytical, etc.



Evaluation Methodology

Emulation

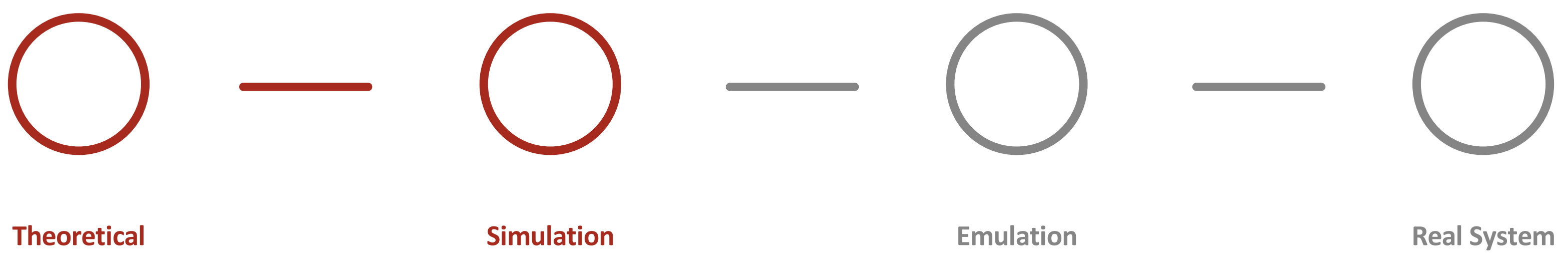
- Replicates behavior of processes
  - i.e., Virtual Machine - run Linux on Windows PC
- Processes execute instructions to advance clocks
- Inherently continuous



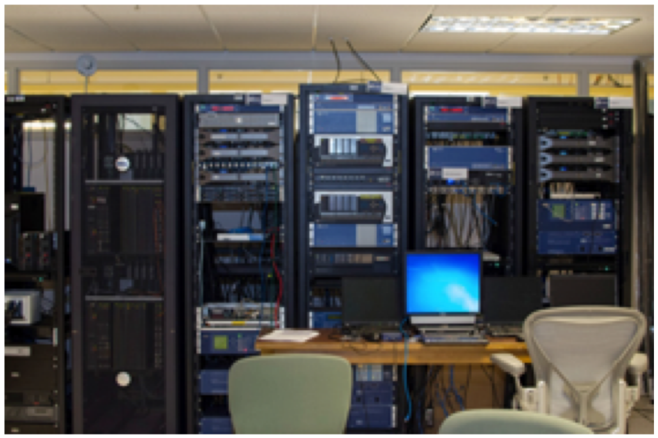
Evaluation Methodology

Real System

- Highest fidelity
- Expensive and impractical



Testbed for Smart Grid Security

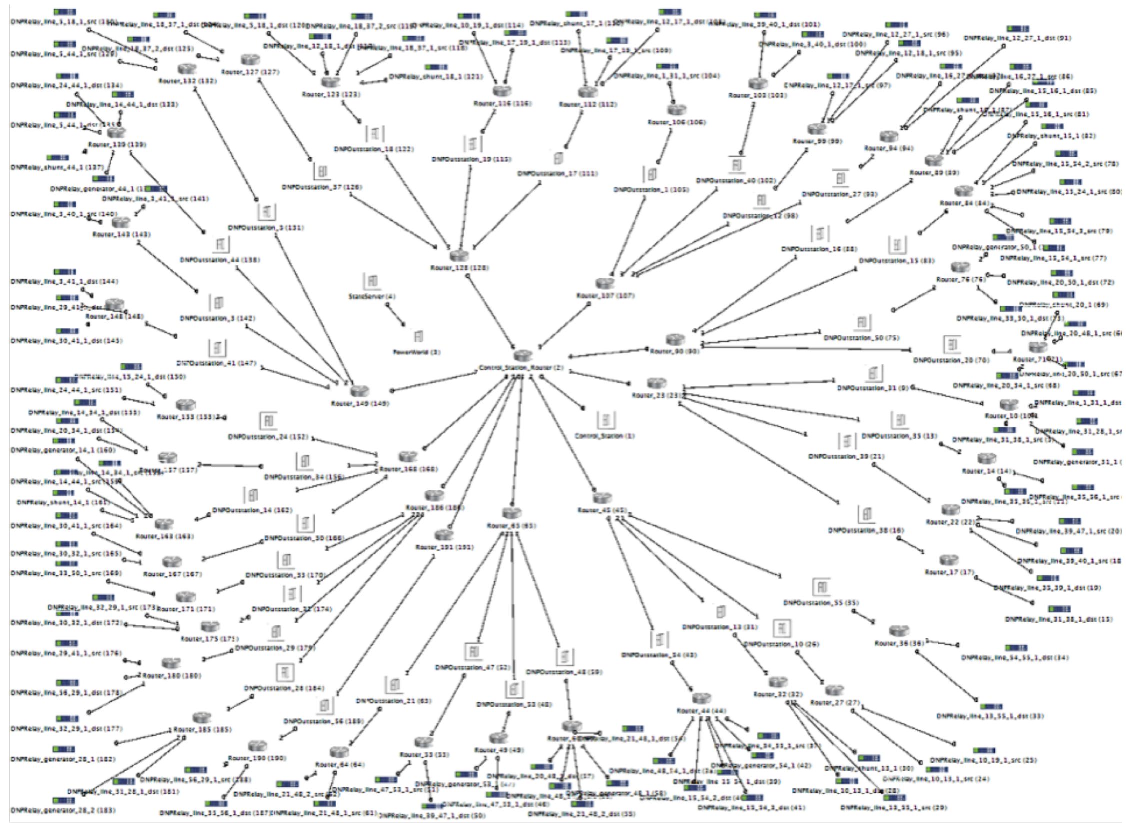


Test Systems in Lab

Security Exercise/Evaluation

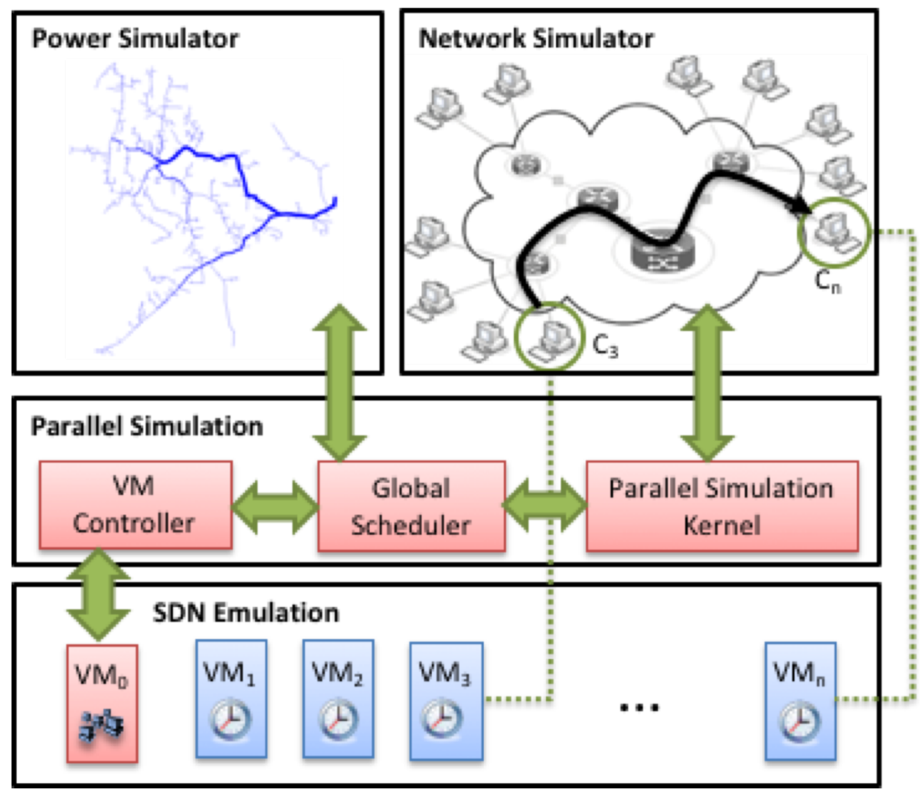
- Scalable
- Flexible
- Controllable
- Reproducible

- No interference with real systems
- Realistic settings



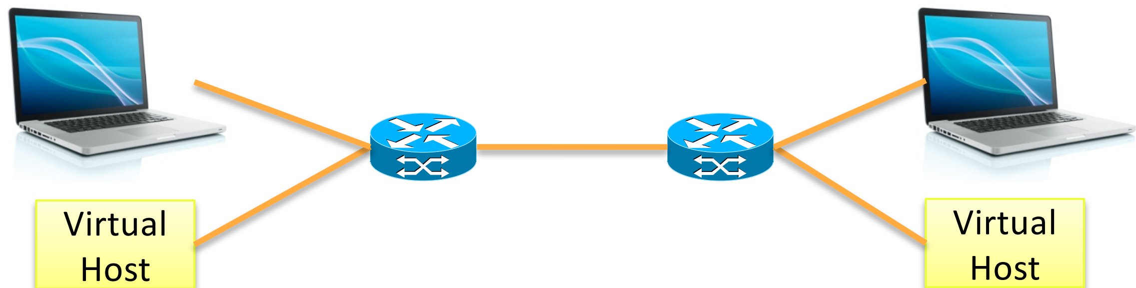
Our Approach – Combining Simulation and Emulation

- Evaluate cyber-physical systems
  - Cyber security
  - Protocol correctness
  - Data collection and evaluation
- Emulate the cyber system
  - Emulate network and compute devices
  - Run real code
- Simulate the physical system
  - Analytical representation of the system
  - Solved offline



[Best paper award, PADS'19], [Best paper finalist, PADS'16]

Network Simulation & Emulation



Emulation – executing "native" software to produce behavior

Simulation – executing model software to produce behavior

Emulation

- High fidelity functional behavior
- Typically tied to "wall-clock" time
- Resource intensive
- Little extra effort needed to include

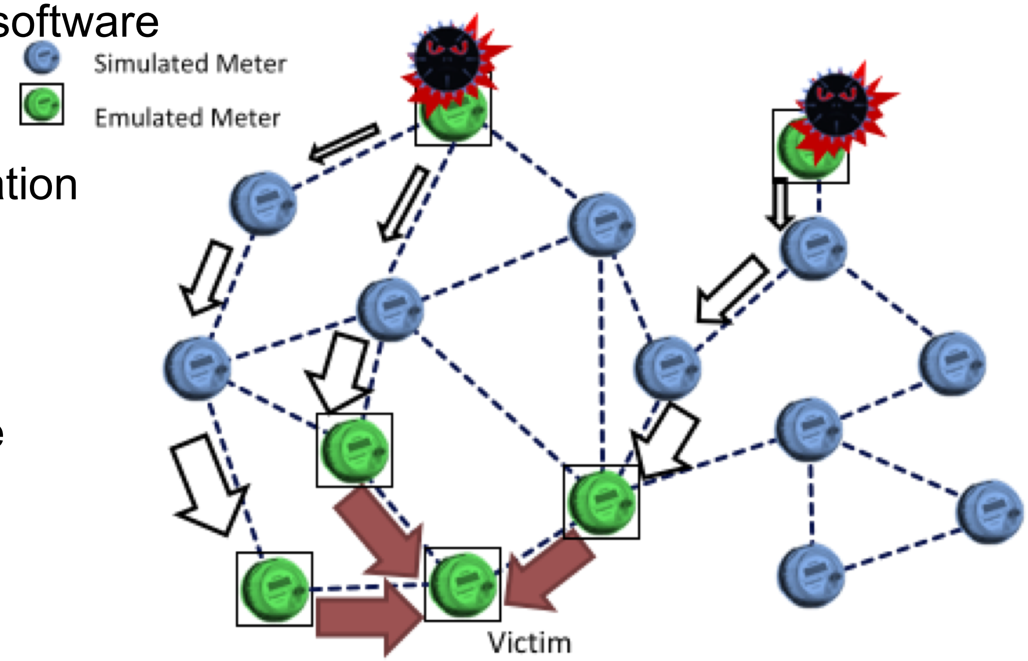
Simulation

- Model abstraction
- May run faster or slower than real-time
- Low(er) memory needs
- Effort needed to develop models

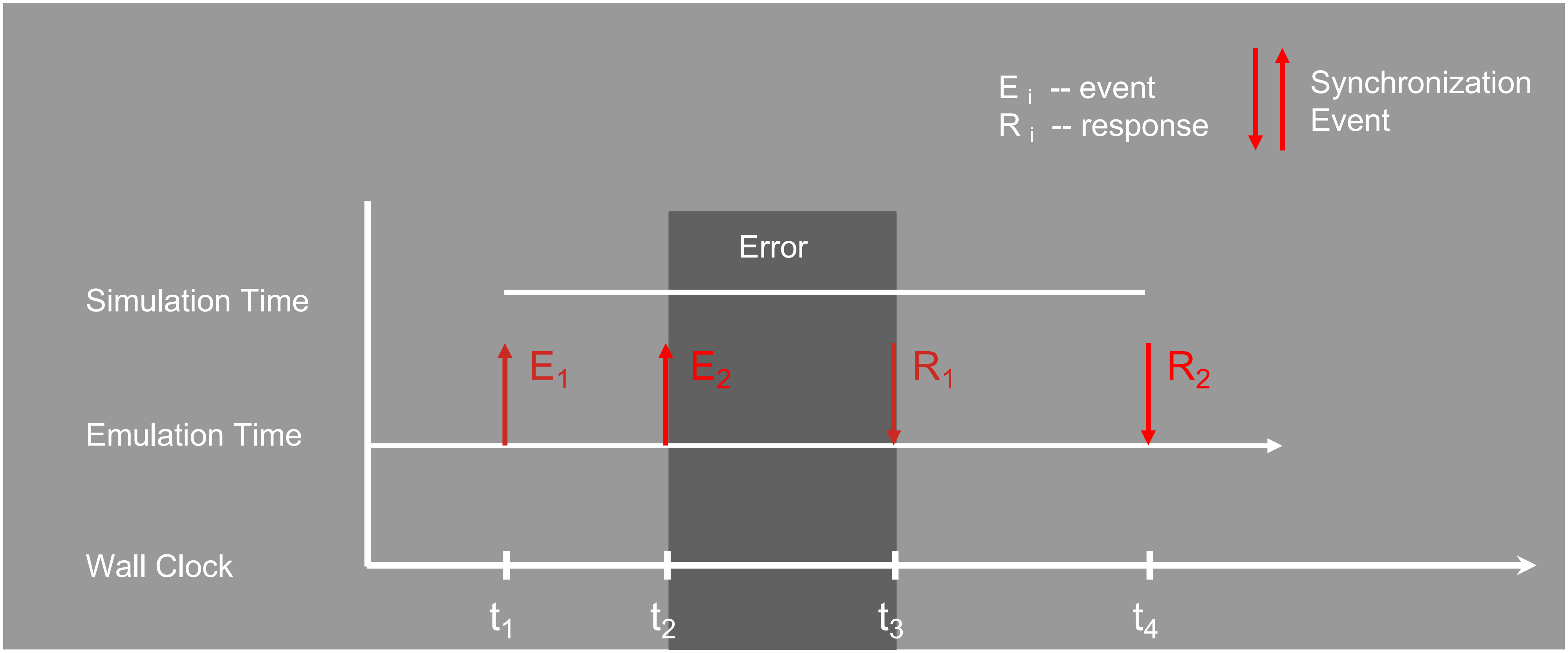
Combining Simulation and Emulation

- Related Work: Power grid and communication network co-simulation
  - FNCS - Transmission, Distribution, Communication
  - EPOCHS - Agent-based commercial software
  - PSLF/ns-2 - proof of concept
  - GECO - global event-driven co-simulation

- Research Challenge: Synchronization
  - Emulation advances in wall-clock time
  - Simulation advances in virtual time



Naive Synchronization - Problem



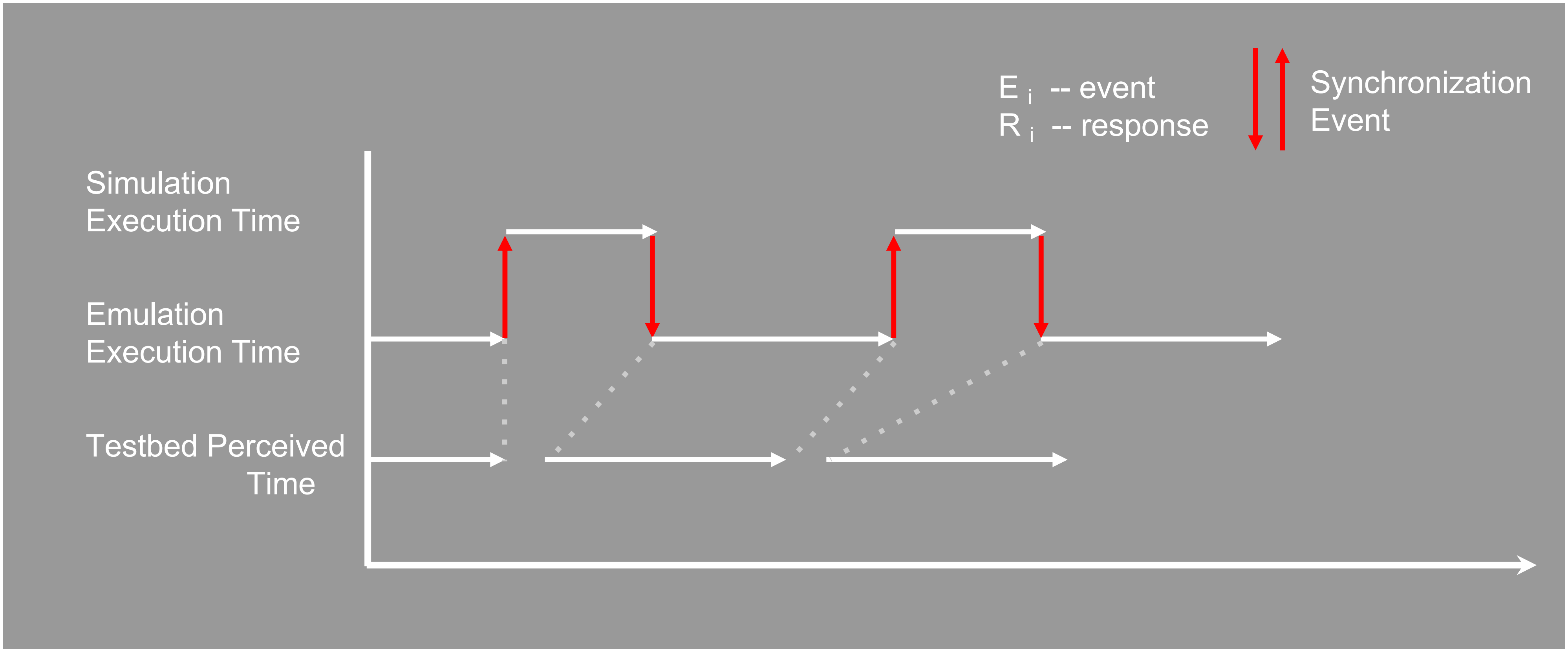
Our Approach: A Virtual Time System in Emulation

- Virtual time provides:
  - Augmented perception of the system clock for a process
- Virtual machines, containers
  - Use virtual time to offset from host's clock
- Emulation experiment reproducibility
  - Use virtual time to schedule processes
- Emulation scalability
  - Virtual time to multiplex resources -- slow down emulator

$$T_{VT} = \frac{T_{wc} - T_s - T_p}{tdf} + T_s$$

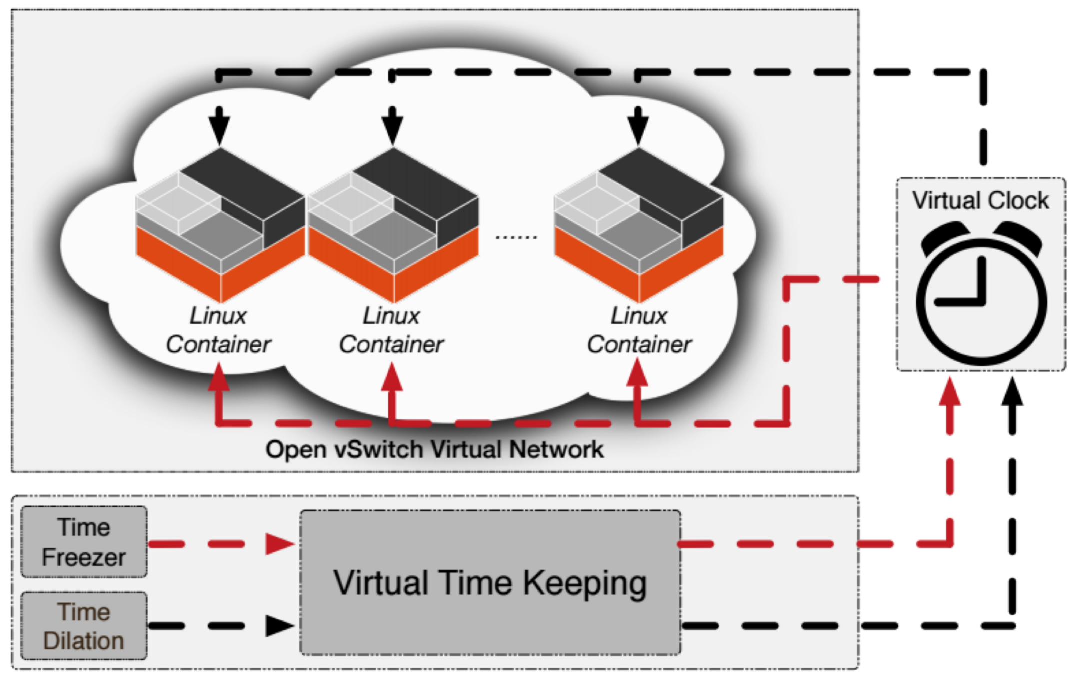
Virtual time	T_{VT}
Wall clock time	T_{wc}
Time process started	T_s
Time process paused for	T_p
Time dilation factor	tdf

Synchronization with Virtual Time



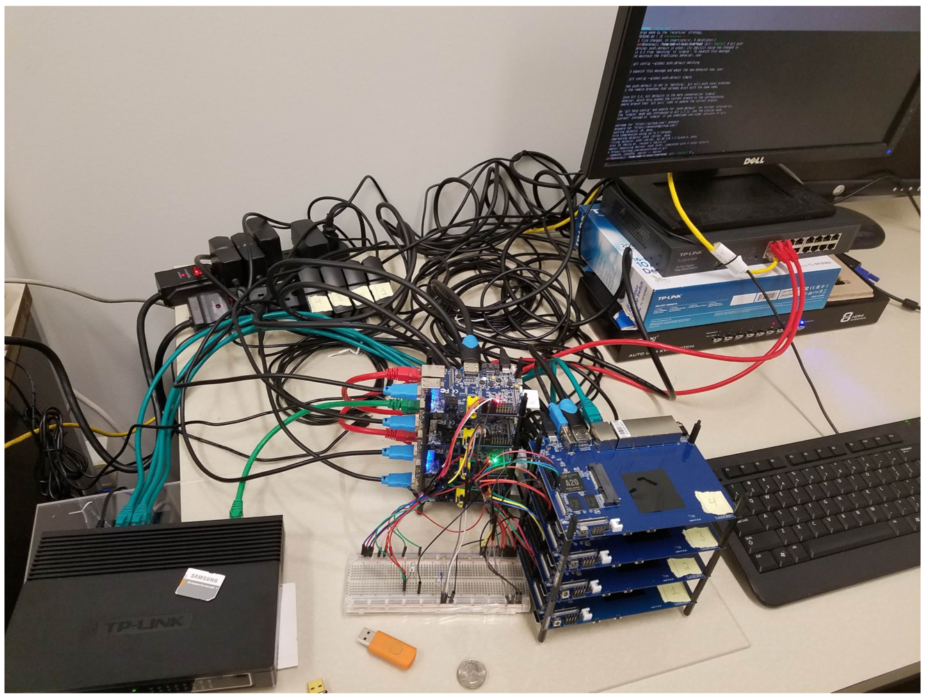
Virtual Time System Design and Implementation

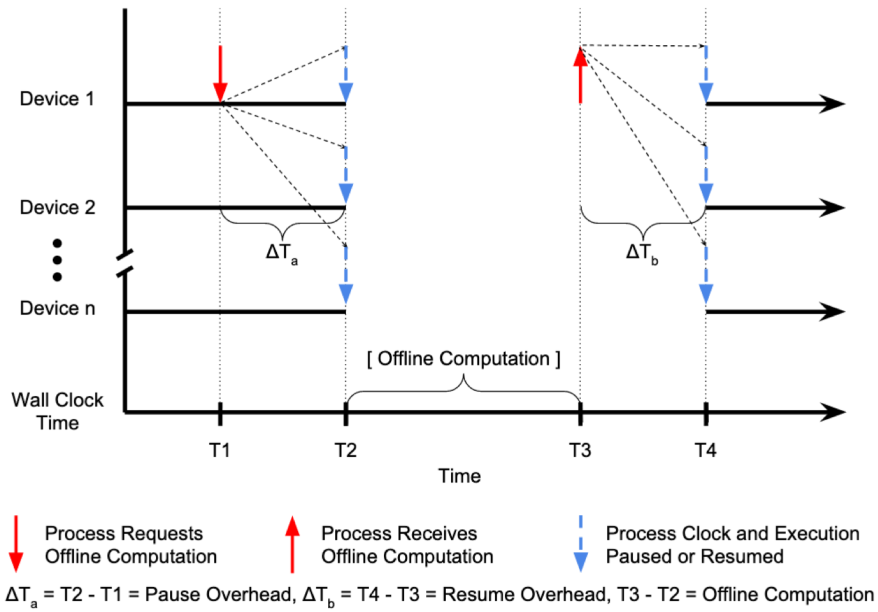
- Each process has a virtual clock managed by the Virtual Time Manager
- Virtual time module allows for
  - Clock Pause/Resume
  - Clock Dilation
- To retrieve virtual time
  - Modify system calls
  - e.g., **`gettimeofday()`**



One Step Further - Distributed Virtual Time

Run across many embedded Linux devices



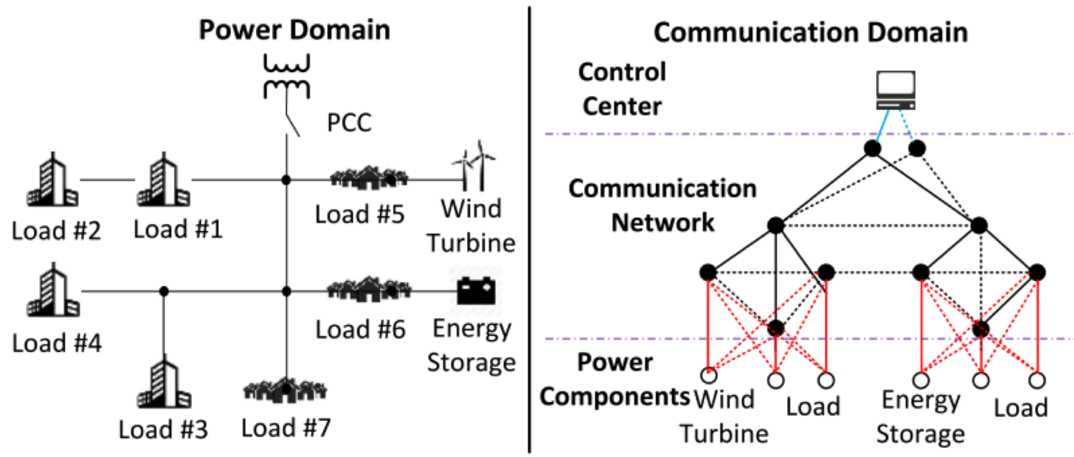


ILLINOIS INSTITUTE OF TECHNOLOGY
College of Science

Case Study I : Cyber-Attack in Power Grid

Model IEEE 13 bus test case in OpenDSS power simulator

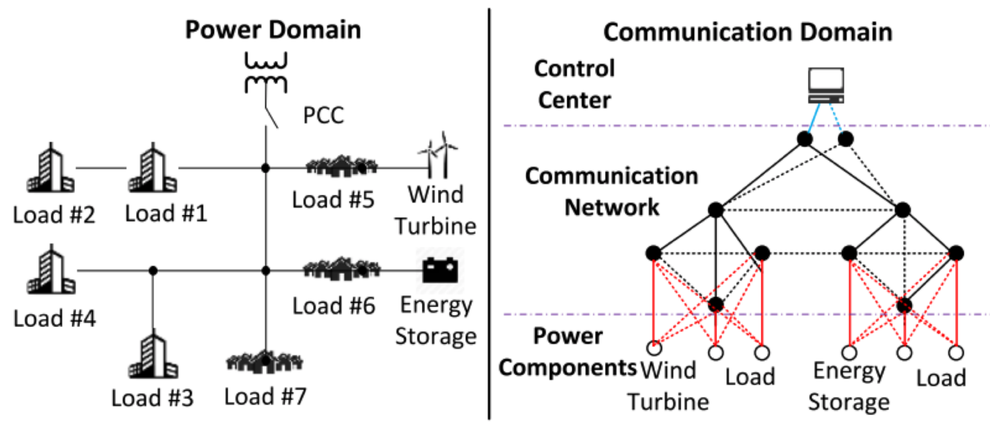
Model communication in Mininet communication network emulator



Case Study I - continued...

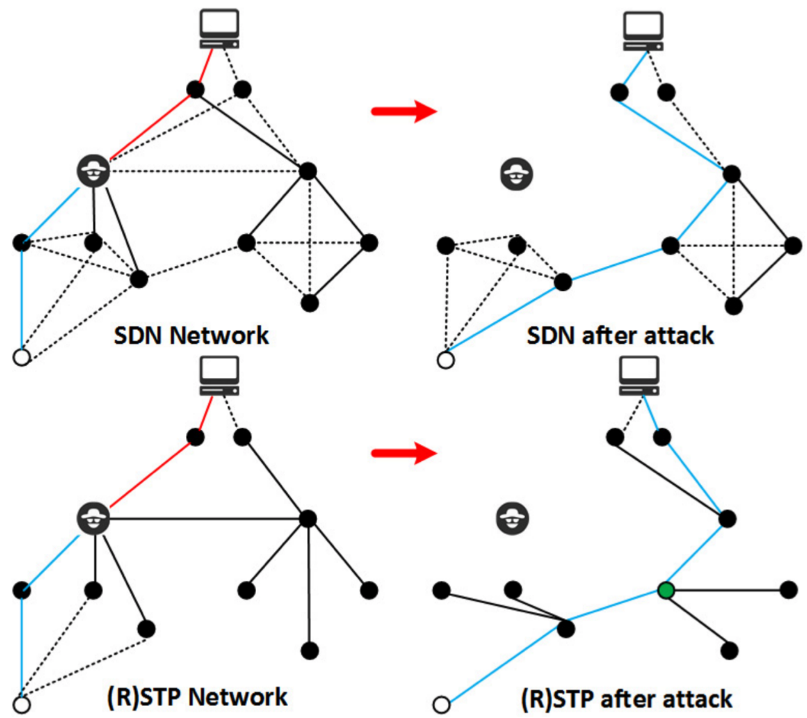
Demand Response application:

- Power consumption and generation needs to be balanced
- The wind turbine generates dynamic power based on weather
- Energy storage device can charge or discharge to balance power
- Control center determines settings for storage device based on sensor readings



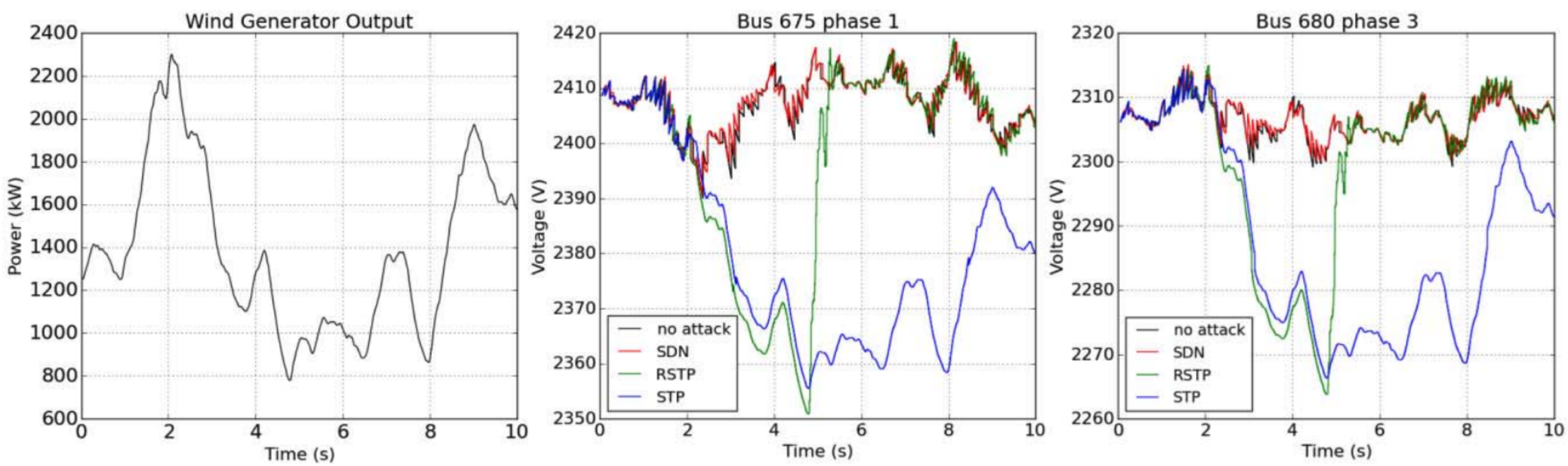
Case Study I - continued...

- Attackers can compromise switches in the communication network
- We evaluate the self-healing nature of the communication network and its effect on the power system
- We evaluate 3 cases:
  - Software-Defined Network (SDN)
  - Spanning Tree Protocol (STP)
  - Rapid Spanning Tree Protocol (RSTP)



Case Study I - continued...

Observation: Centralized network recovery can help to recover from network attacks or outages quicker than standard distributed algorithms



ILLINOIS INSTITUTE OF TECHNOLOGY
College of Science

Conclusion

- Goal: to create a more secure, resilient, and safe cyber-environment for critical cyber-physical systems
- We designed a testbed
  - for evaluating cyber-physical systems
    - Resilience, Security, Performance
  - virtual time system for Linux container
  - synchronization between simulation and emulation systems
  - running across multiple devices

ILLINOIS INSTITUTE OF TECHNOLOGY
College of Science