Towards a Secure and Resilient Industrial Control System with Software-Defined Networking

Dong (Kevin) Jin

Department of Computer Science

Illinois Institute of Technology

TSS/SoS Seminar, March 15, 2016

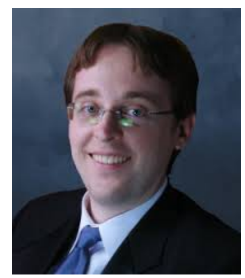
ILLINOIS INSTITUTE OF TECHNOLOGY

Part of the SoS Lablet with

- David Nicol

- Bill Sanders

- Matthew Caesar



- Brighten Godfrey

Work with …

Wenxuan Zhou Jason Croft

Matthew Caesar Brighten Godfrey

Christopher Hannon Jiaqi Yan

Hui Lin Chen Chen

Jianhui Wang Junjian Qi

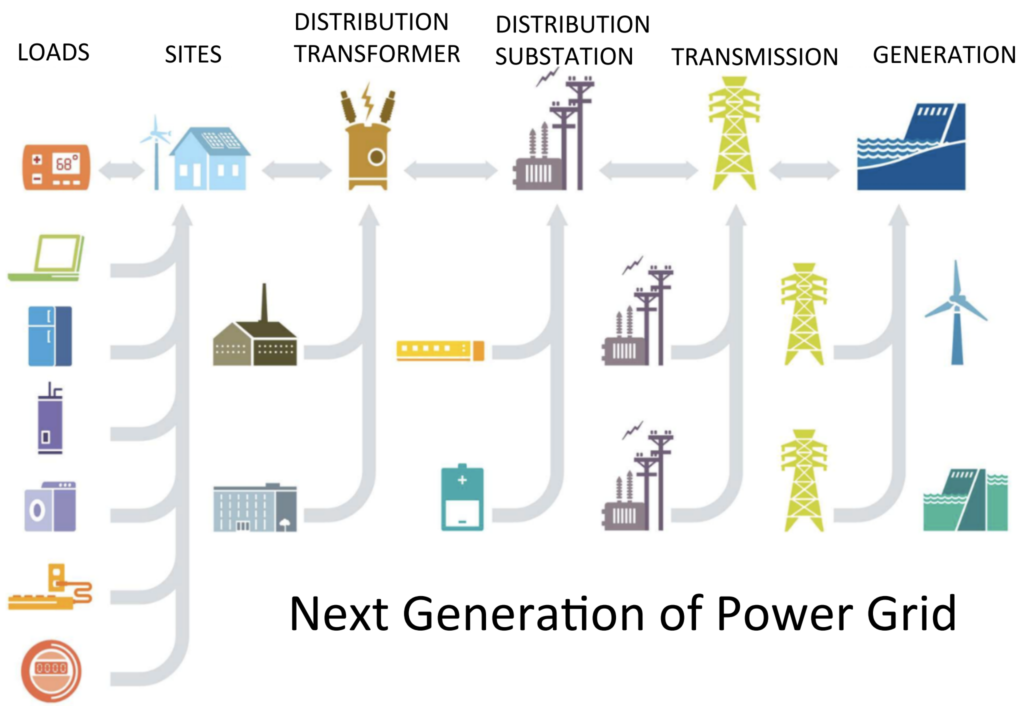
Zhiyi Li Mohammad Shahidehpour

References to papers in this talk

- Wenxuan Zhou, Dong Jin, Jason Croft, Matthew Caesar, and Brighten Godfrey. "Enforcing Customizable Consistency Properties in Software-Defined Networks." NSDI, 2015
- Christopher Hannon, Jiaqi Yan and Dong Jin. "DSSnet: A Microgrid Modeling Platform with Electrical Power Distribution System Simulation and Software Defined Networking Emulation." ACM SIGSIM PADS 2016 (to appear)
- Hui Lin, Chen Chen, Jianhui Wang, Junjian Qi and Dong Jin. "Self-Healing Attack-Resilient PMU Network for Power System Operation." IEEE Transactions on Smart Grid (submitted)
- Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour. "Towards A Resilient and Secure Microgrid Using Software-Defined Networking." IEEE Transactions on Smart Grid, Special Issue on Smart Grid Cyber-Physical Security (submitted)

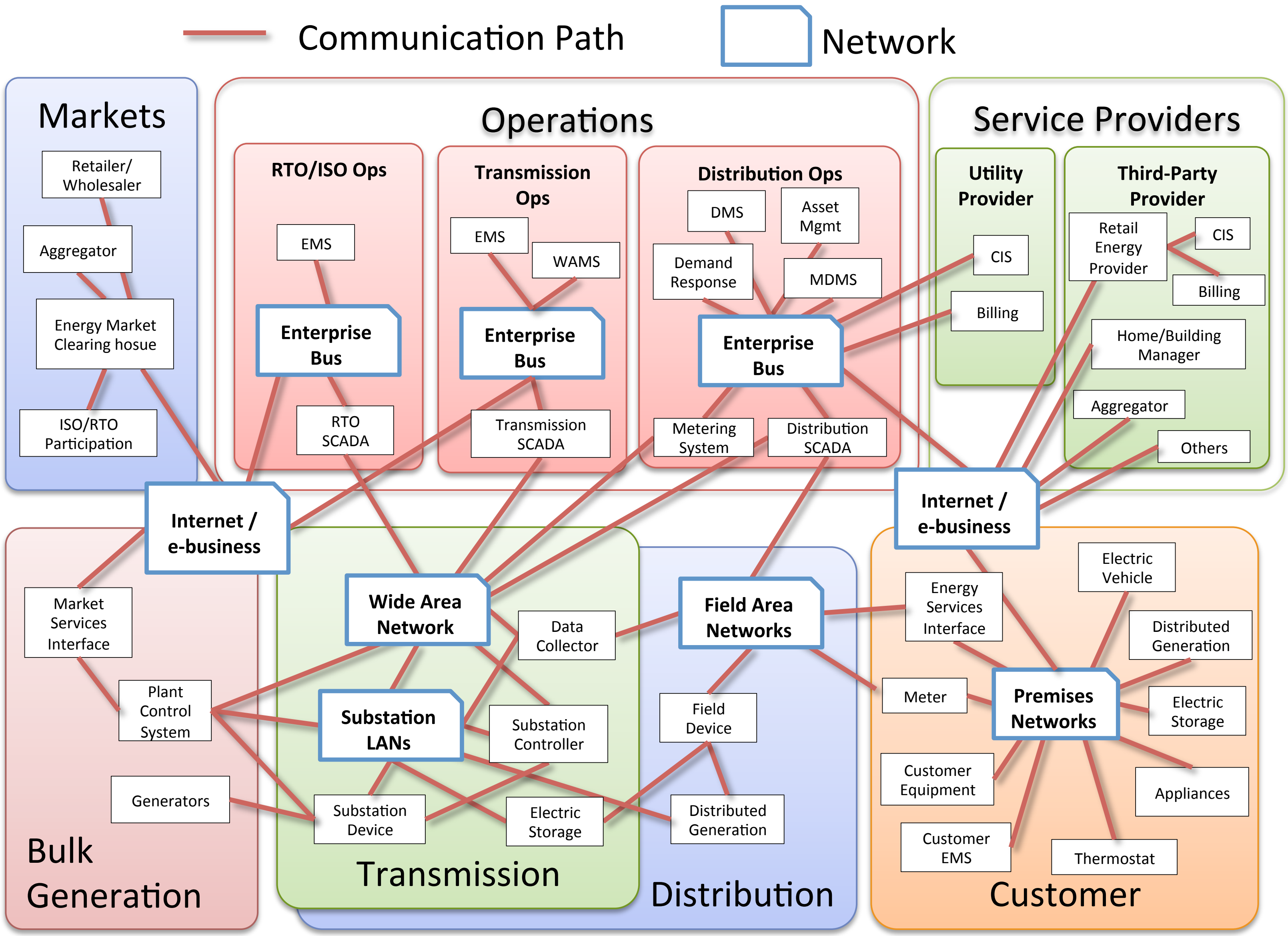
Industrial Control Systems (ICS)

- Control many critical infrastructures
  - e.g., power grids, gas and oil distribution networks, wastewater treatment, transportation systems …
- Modern ICSes increasingly adopt Internet technology to boost control efficiency, e.g., smart grid



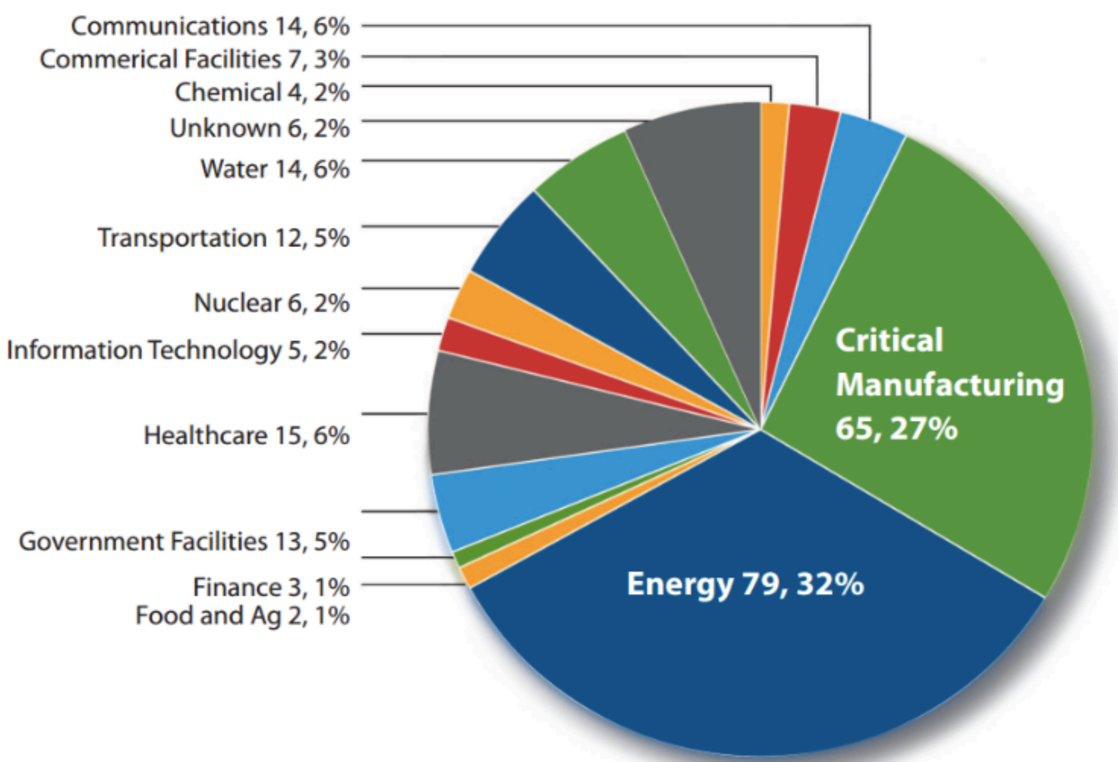
Next Generation of Power Grid

More Efficient or More Vulnerable?



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

Cyber Threats in Power Grids



- 245 incidents, reported by ICS-CERT
- 32% in energy sector
- 80,000 residents in western Ukraine
- 6 hours, lost power on Dec 23, 2015

THE DAILY SIGNAL SEARCH

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

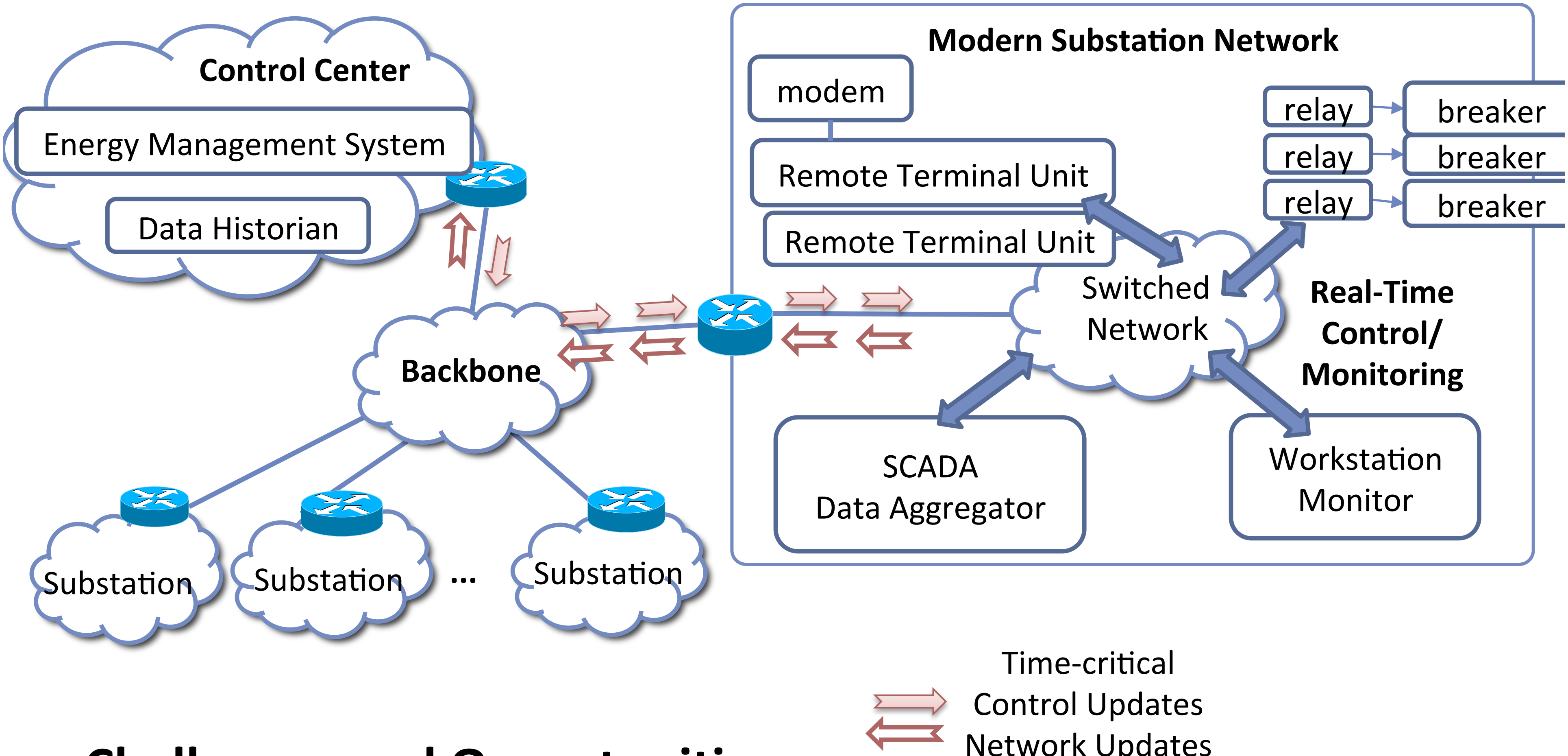
Riley Walters / January 13, 2016 / 1 comments

Picture source: 1. National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT Monitor Sep 2014 – Feb 2015
2. http://dailysignal.com/2016/01/13/ukraine-goes-dark-russia-attributed-hackers-take-down-power-grid/

Protection of Industrial Control Systems

- Commercial of-the-shelf products
  - e.g., firewalls, antivirus software
  - fine-grained protection at single device only
- How to check system-wide requirements
  - Security policy (e.g., access control)
  - Performance requirement (e.g., end-to-end delay)
- How to safely incorporate existing networking technologies in control system infrastructures?

A Representative Smart Grid Control Network



Challenges and Opportunities

Differences and Similarities

A Utility Control Network

An Enterprise Network

Similarities

- black hole avoidance
- loop mitigation
- fast convergence speeds
- priority control
- multiple services on a single physical channel
- ...

Differences

- strictly defined forwarding paths
- end-to-end performance guarantee
- system-wide visualization
- real-time monitoring
- a deny-by-default security model
- ...

Problem Statement

- Minimize the gaps with an SDN-enabled communication architecture for ICS
- Create innovative applications for ICS security and resiliency
  - Real-time network verification
  - Self-healing network management
  - Context-aware intrusion detection
  - Many more ...

ICS – industrial control system

SDN – software-defined networking

SDN Architecture

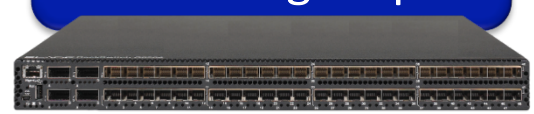
App | App | App | App | App | App | App | App

Open Interface

Control Plane or Control Plane or Control Plane

Open Interface

Merchant Switching Chips

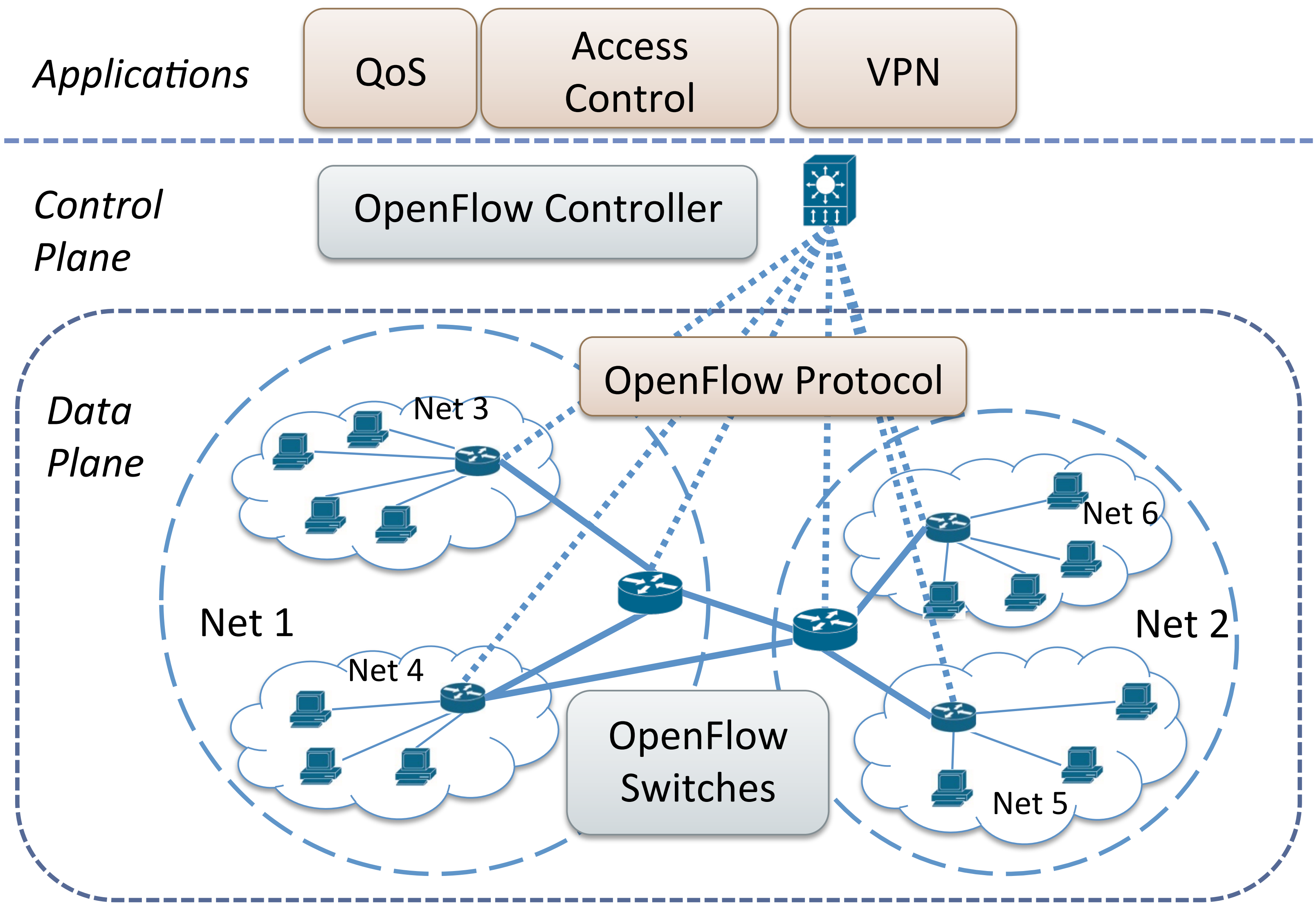


Vertically integrated
Closed, proprietary
Slow innovation

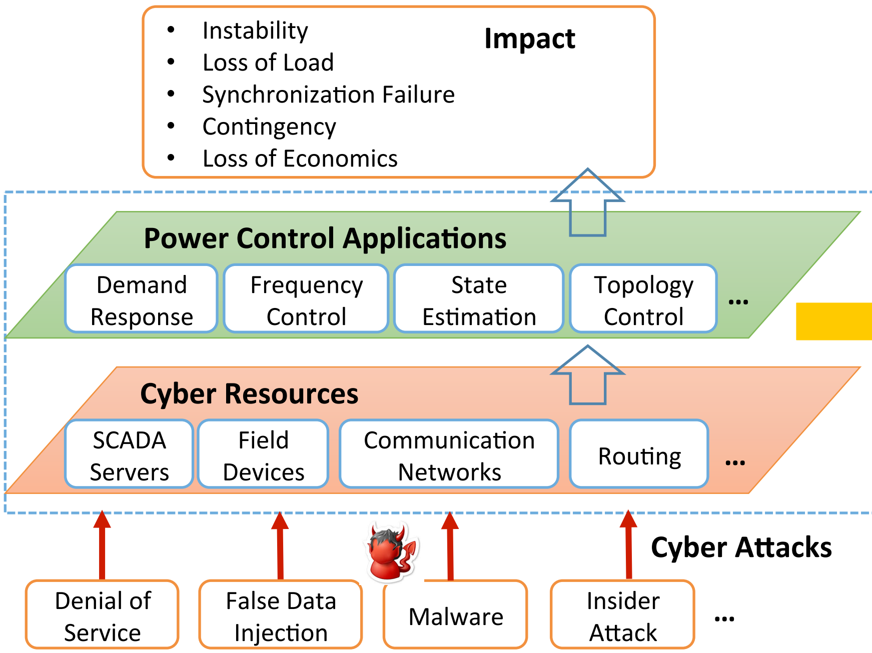
Horizontal
Open interfaces
Rapid innovation

Source: Nick McKeown, Open Networking Summit 2012

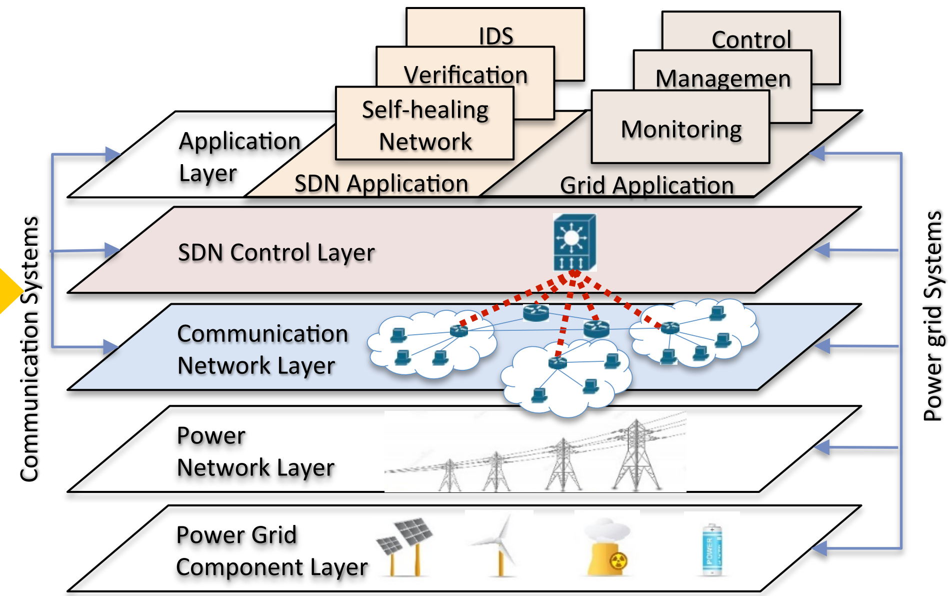
SDN Architecture - Continue



An SDN-Enabled Power Grid



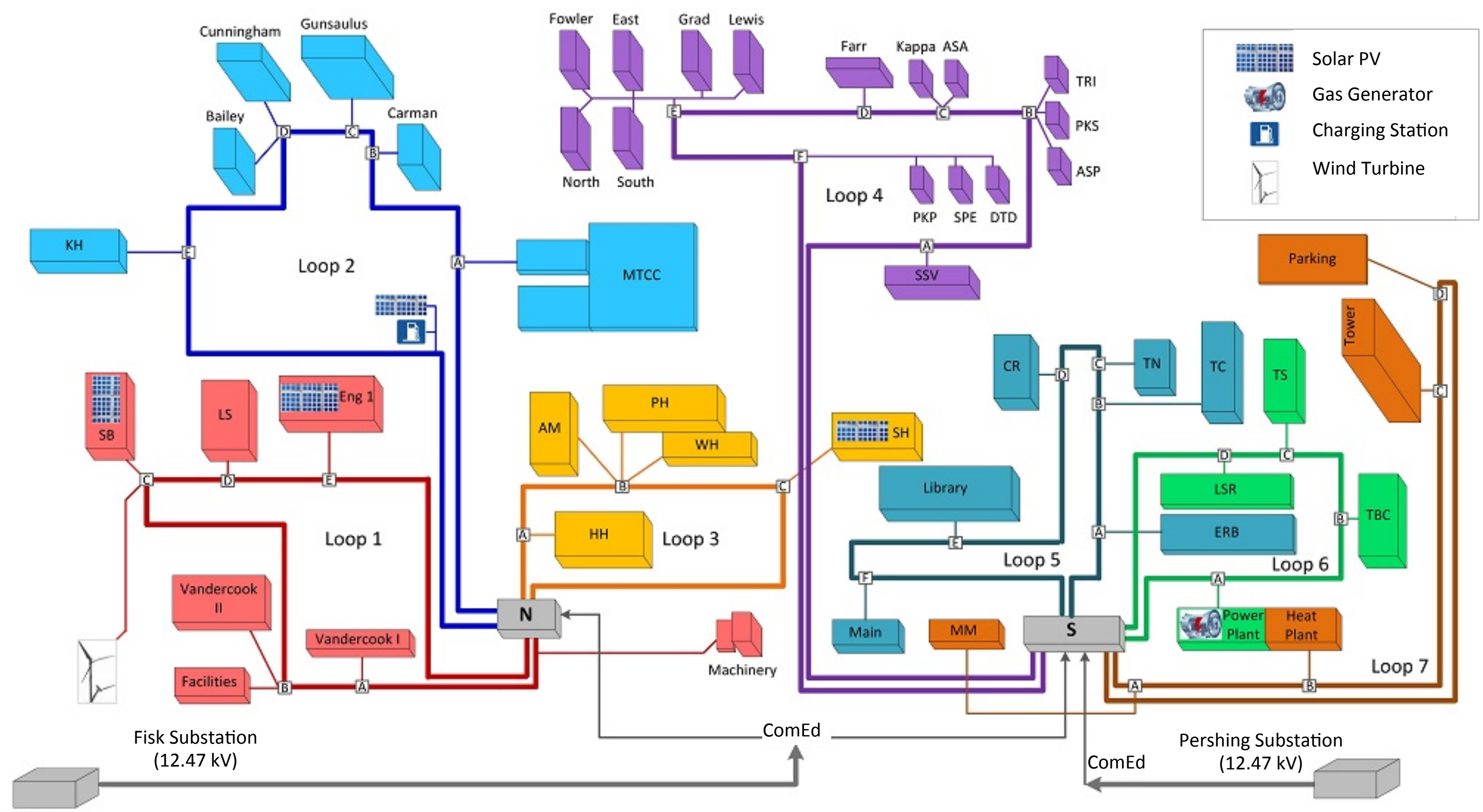
Current Power Grid: Potential Cyber Attacks and Their Implications



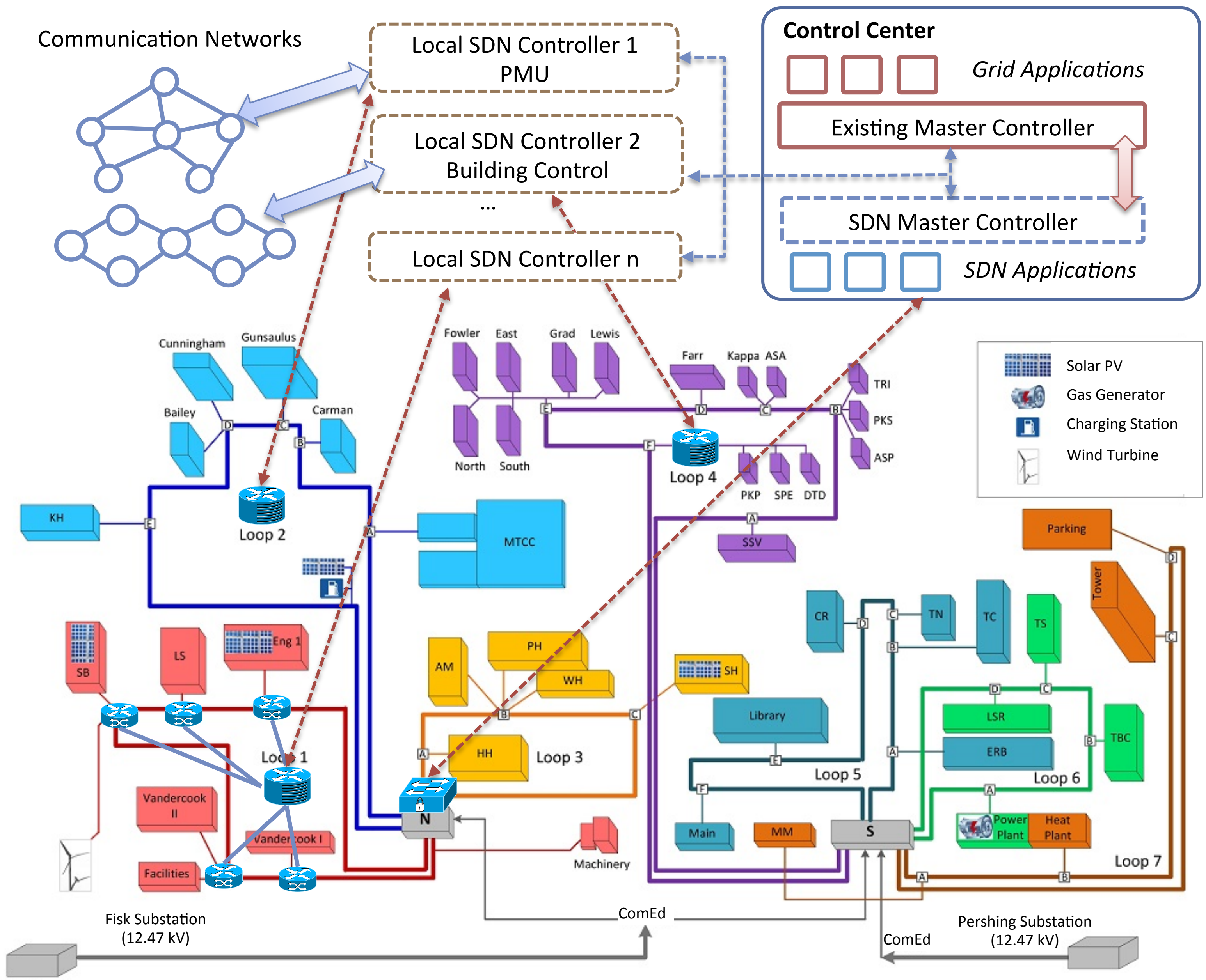
Future SDN-enabled Power Grid: A Cyber-Attack-Resilient Platform

Transition to an SDN-Enabled IIT Microgrid

- Real-time reconfiguration of power distribution assets
- Real-time islanding of critical loads
- Real-time optimization of power supply resources



ILLINOIS INSTITUTE OF TECHNOLOGY



Communication Networks
Local SDN Controller 1
PMU
Local SDN Controller 2
Building Control
...
Local SDN Controller n
Control Center
Grid Applications
Existing Master Controller
SDN Master Controller
SDN Applications
Solar PV
Gas Generator
Charging Station
Wind Turbine
Cunningham
Gunsaulus
Bailey
Carman
KH
Loop 2
MTCC
Fowler
East
Grad
Lewis
North
South
Farr
Kappa
ASA
TRI
PKS
ASP
Loop 4
PKP
SPE
DTD
SSV
Parking
Tower
CR
TN
TC
TS
SB
LS
Eng 1
AM
PH
WH
SH
Library
LSR
ERB
TBC
Loop 1
HH
Loop 3
Loop 5
Loop 6
Vandercook II
Vandercook I
Facilities
N
Machinery
Main
MM
S
Power Plant
Heat Plant
Loop 7
ComEd
Fisk Substation
(12.47 kV)
Pershing Substation
(12.47 kV)

Transition to an SDN-Enabled Microgrid

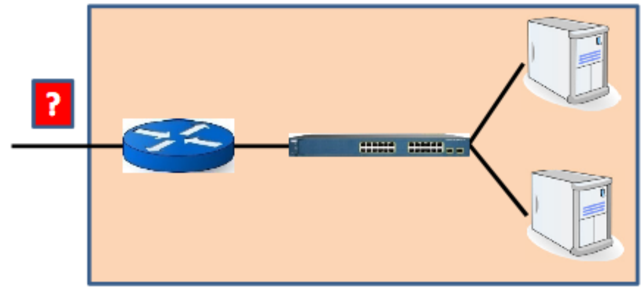
- SDN-based Applications
  – Real-time Verification
  – Self-healing PMU
- Hybrid Testbed
  – SDN emulation + Power Distribution System Simulation

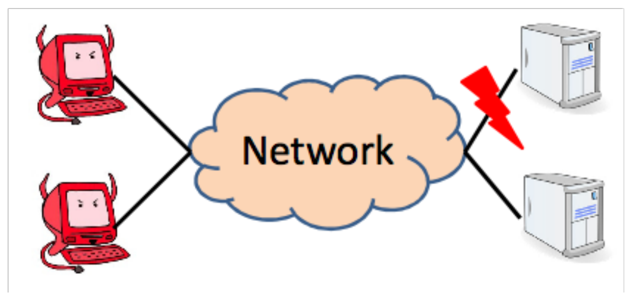
Application 1: Network Verification – Motivation

89% of operators never sure that config changes are bug-free[1]

82% concerned that changes would cause problems with existing functionality[1]

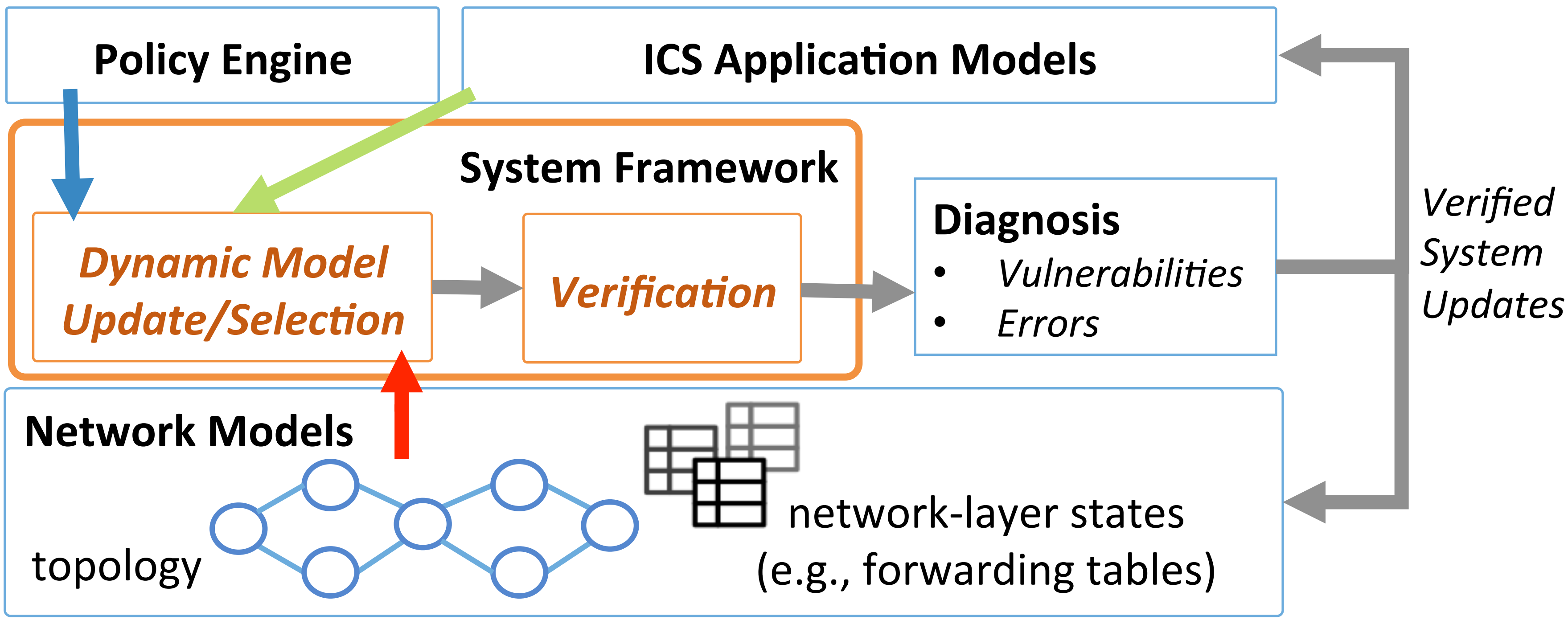
- Unauthorized access
- Unavailable critical services
- System performance drop
  - Instability
  - Loss of load
  - Synchronization Failure
- …





1. Survey of network operators: [Kim, Reich, Gupta, Shahbaz, Feamster, Clark, USENIX NSDI 2015]
2. Pictures borrowed from VeriFlow slides [Khurshid, Zou, Zhou, Caesar, Godfrey NSDI 2013]

Verification System Design



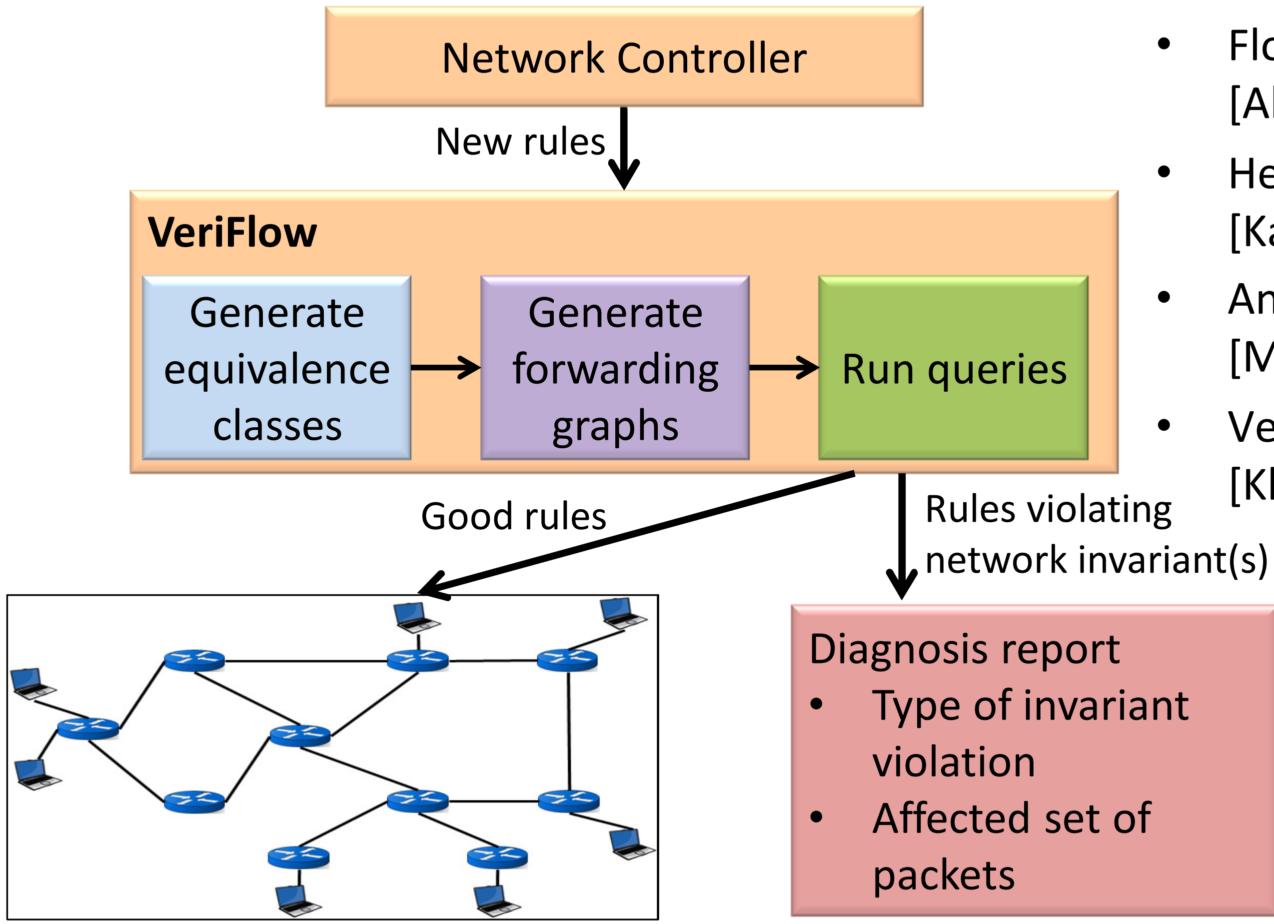
Dynamic Network Data (topology, forwarding tables …)

Dynamic Application Data (control updates …)

User-specified Policy (security, performance …)

ILLINOIS INSTITUTE OF TECHNOLOGY

Network-Layer Verification



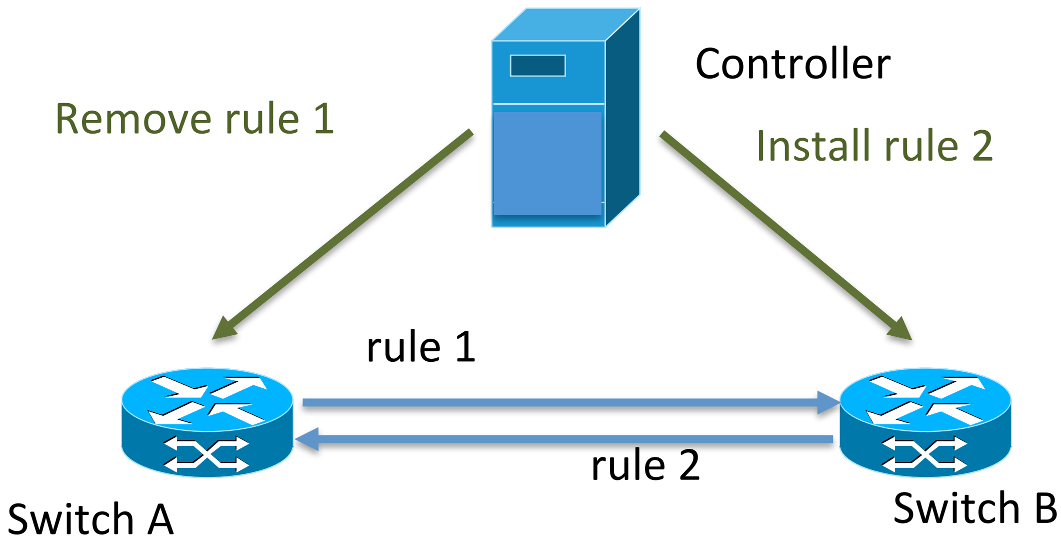
Prior Work

- FlowChecker [Al-Shaer et al.,SafeConfig2010]
- HeaderSpaceAnalysis [Kazemian et al.,NSDI2012]
- Anteater [Mai et al.,SIGCOMM2011]
- VeriFlow [Khurshid et al., NSDI2012]

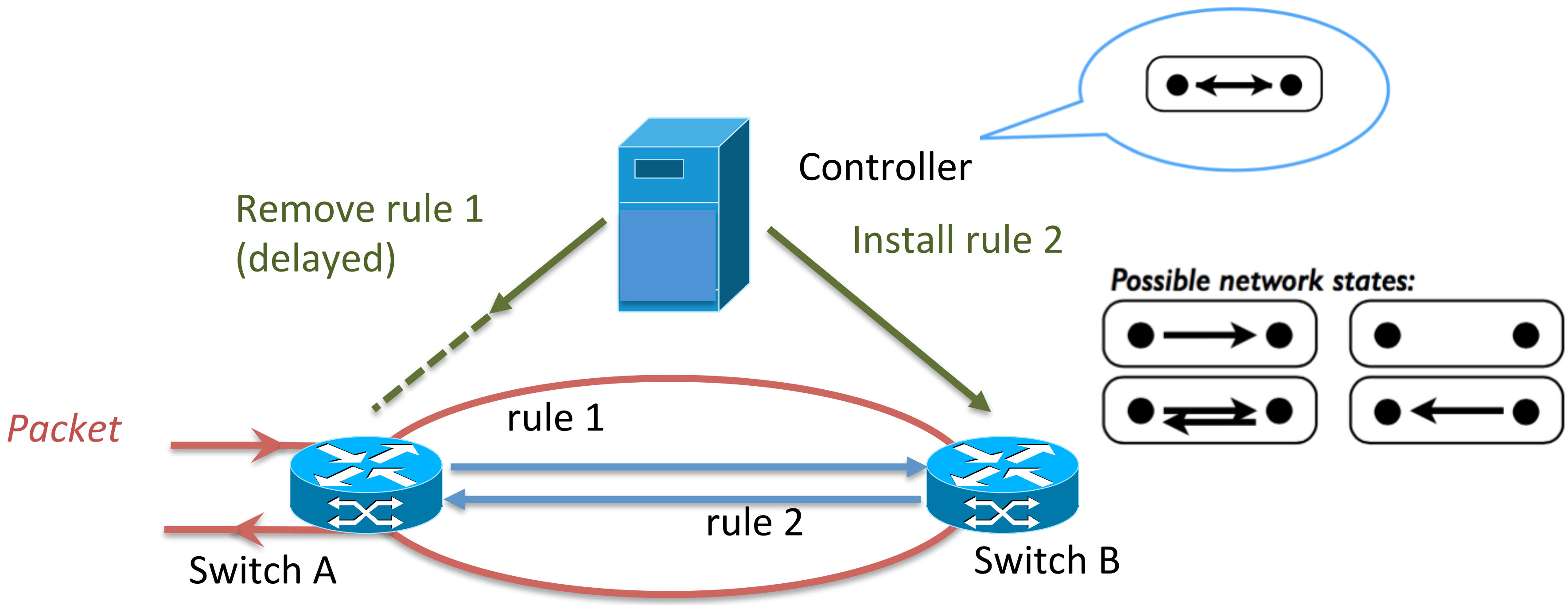
Pictures borrowed from VeriFlow slides [Khurshid, Zou, Zhou, Caesar, Godfrey NSDI 2013]

Challenges — Timing Uncertainty

Network devices are asynchronous and distributed in nature



Challenges — Timing Uncertainty

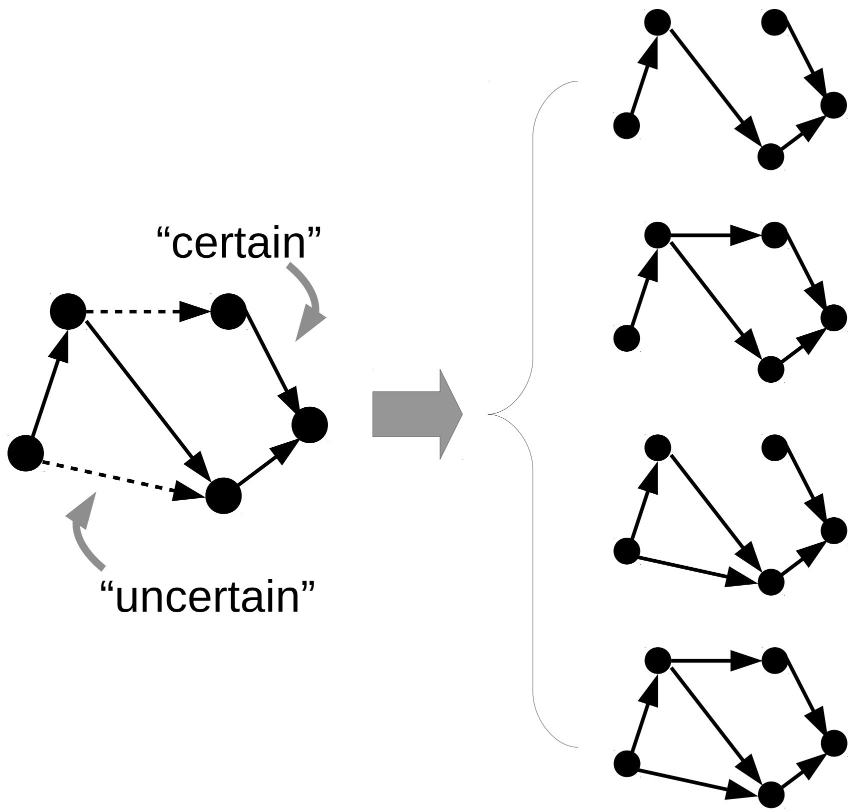


Loop-freedom Violation

ILLINOIS INSTITUTE OF TECHNOLOGY

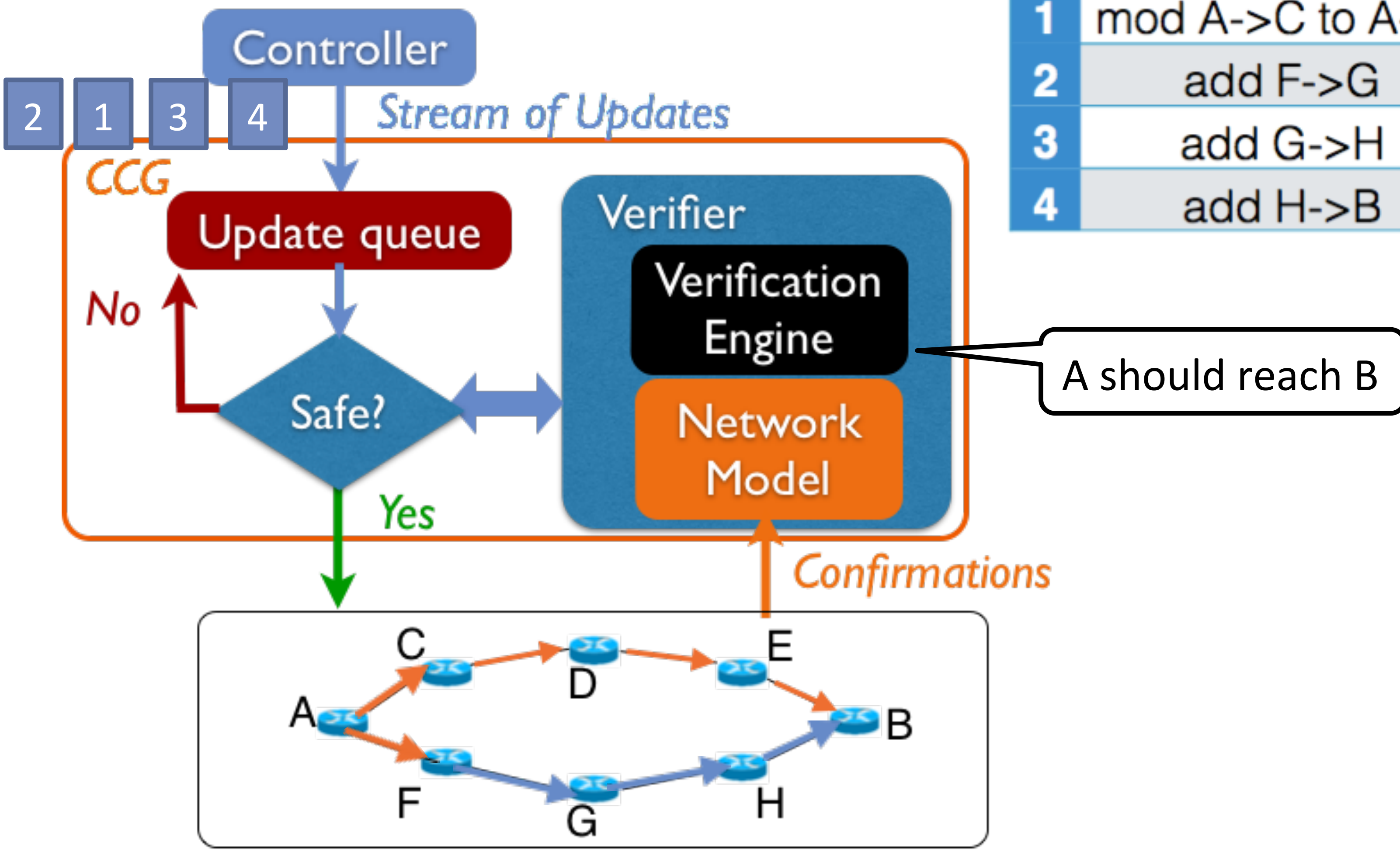
Uncertainty-aware Modeling

- Naively, represent every possible network state O(2^n)
- Uncertain graph: represent all possible combinations



Update synthesis via verification

1	mod A->C to A->F
2	add F->G
3	add G->H
4	add H->B



Enforcing dynamic correctness with heuristically maximized parallelism

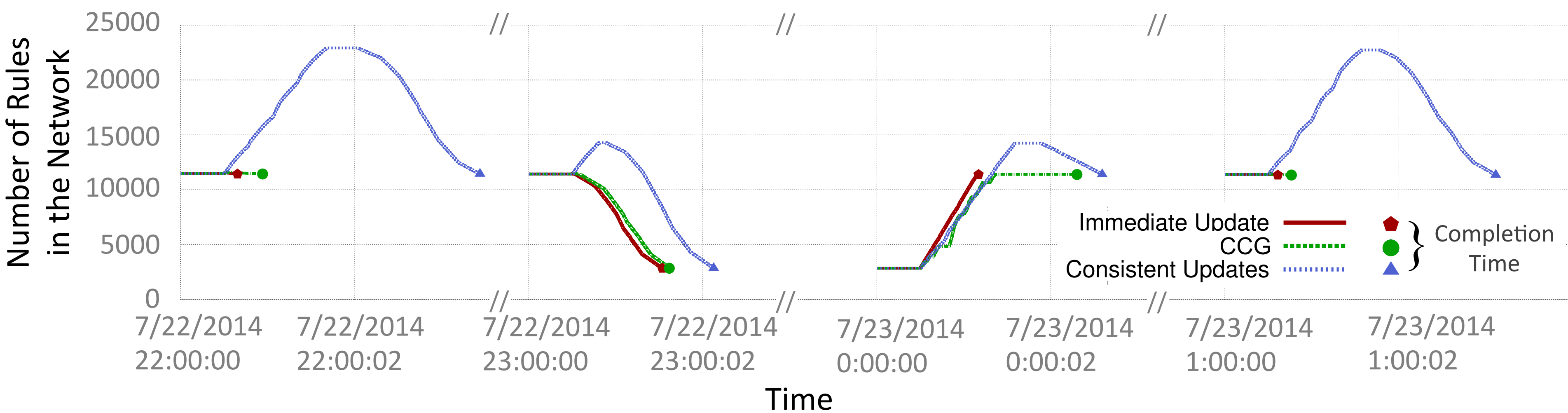
Slide borrowed from Wenxuan Zhou, “CCG” NSDI 2015

OK, but…

Can the system "deadlock"?

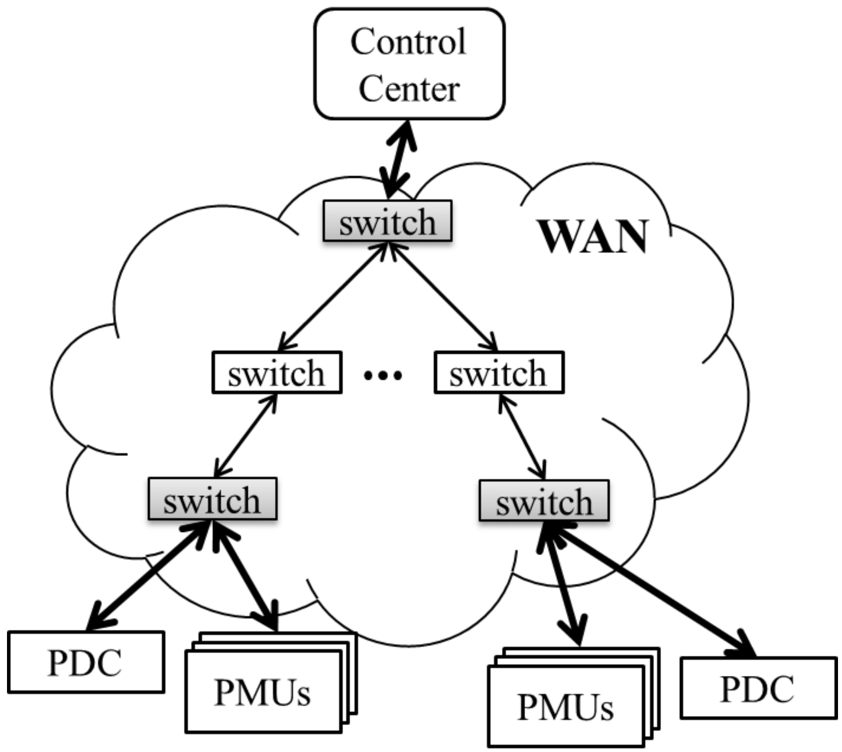
- Proved classes of networks that never deadlock
- Experimentally rare in practice!
- Last resort: heavyweight "fallback" like consistent updates [Reitblatt et al, SIGCOMM 2012]

Is it fast?

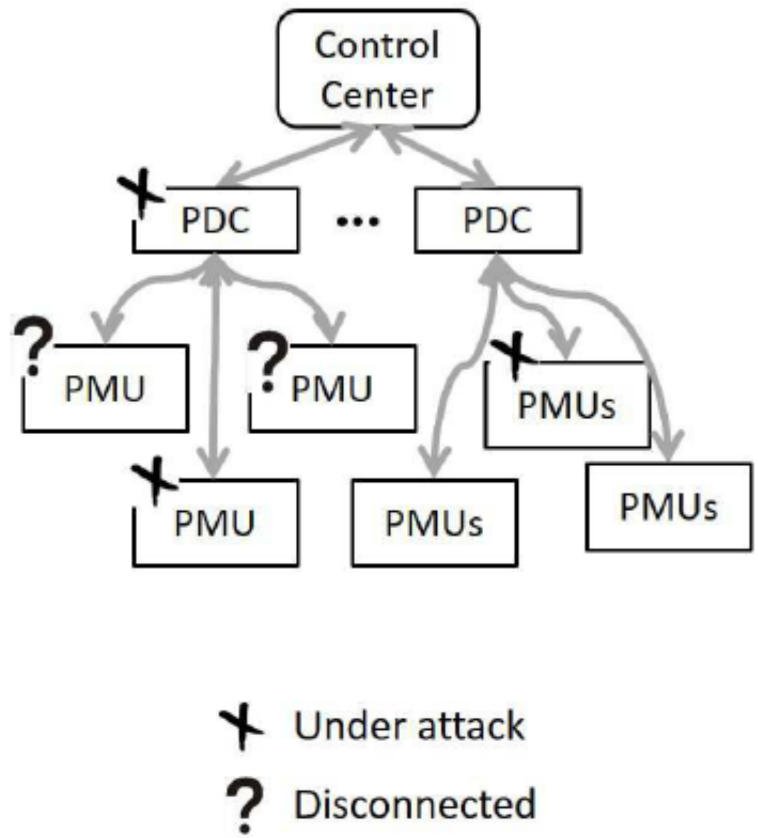


Slide borrowed from Brighten Godfrey, TSS Seminar, Sep 2015

Application 2: Self-Healing Phasor Measurement Unit (PMU) Networks



Integration of A Communication Network and A PMU Network

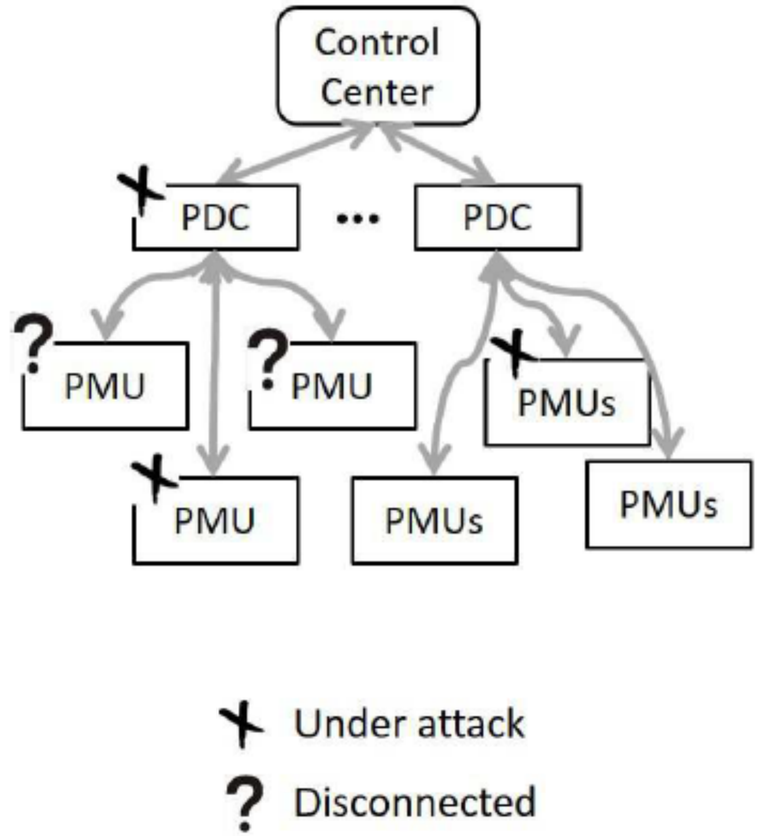


ILLINOIS INSTITUTE OF TECHNOLOGY

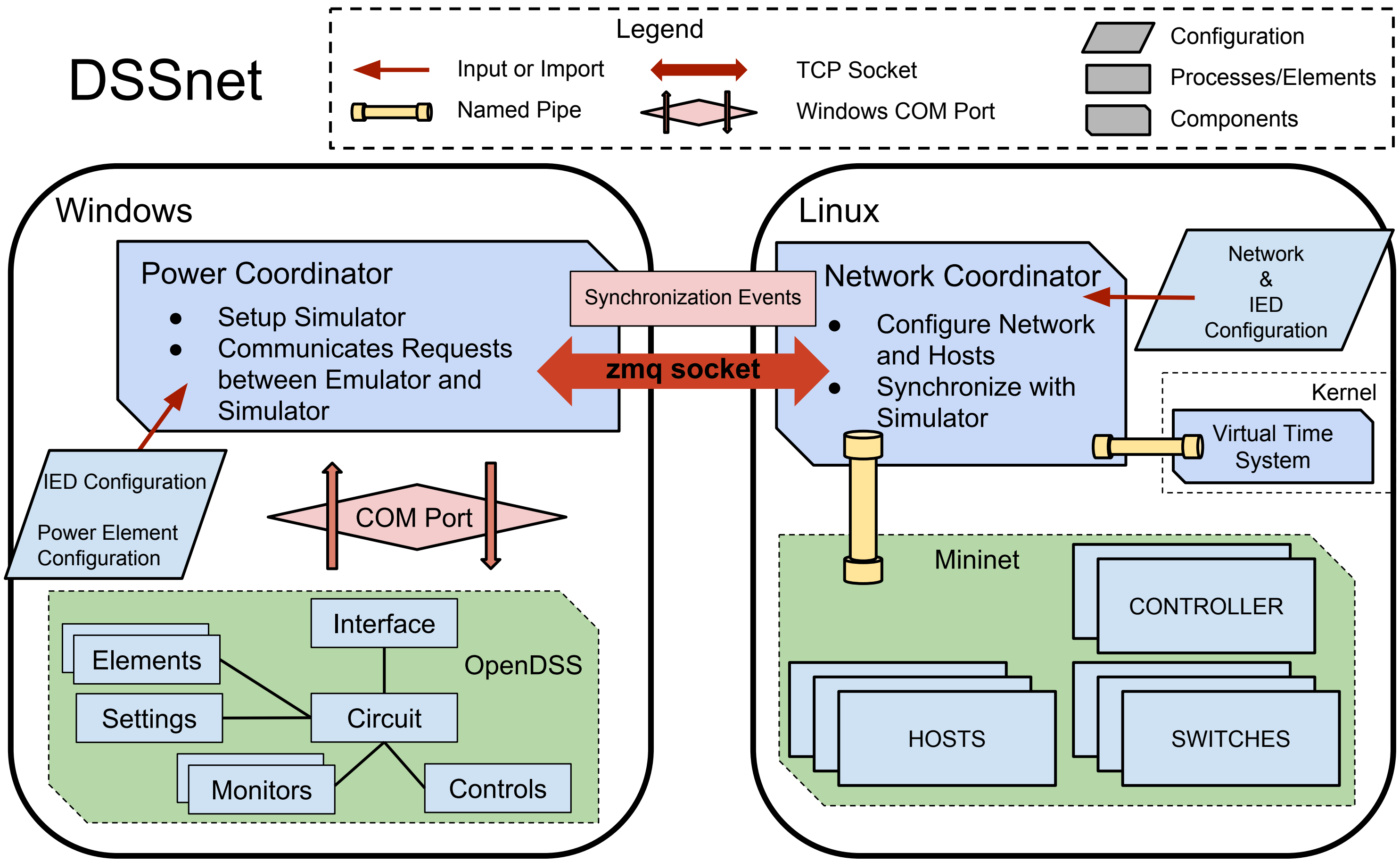
Self-Healing PMU Networks

- Isolate compromised devices
- "Self-heal" the network by quickly re-establishing routes
  - To restore power system observability
  - Using an integer linear program model

Video Demo



A Hybrid Testing Platform



Power Distribution System Simulation + SDN-based Network Emulation

ILLINOIS INSTITUTE OF TECHNOLOGY

A Hybrid Testing Platform

- Challenges
  - Temporal fidelity in network emulation
  - Synchronization between two sub-systems
    - Emulation – executing "native" software to produce behavior in wall-clock time
    - Simulation – executing model software to produce behavior in virtual time

Our approach: Virtual Time

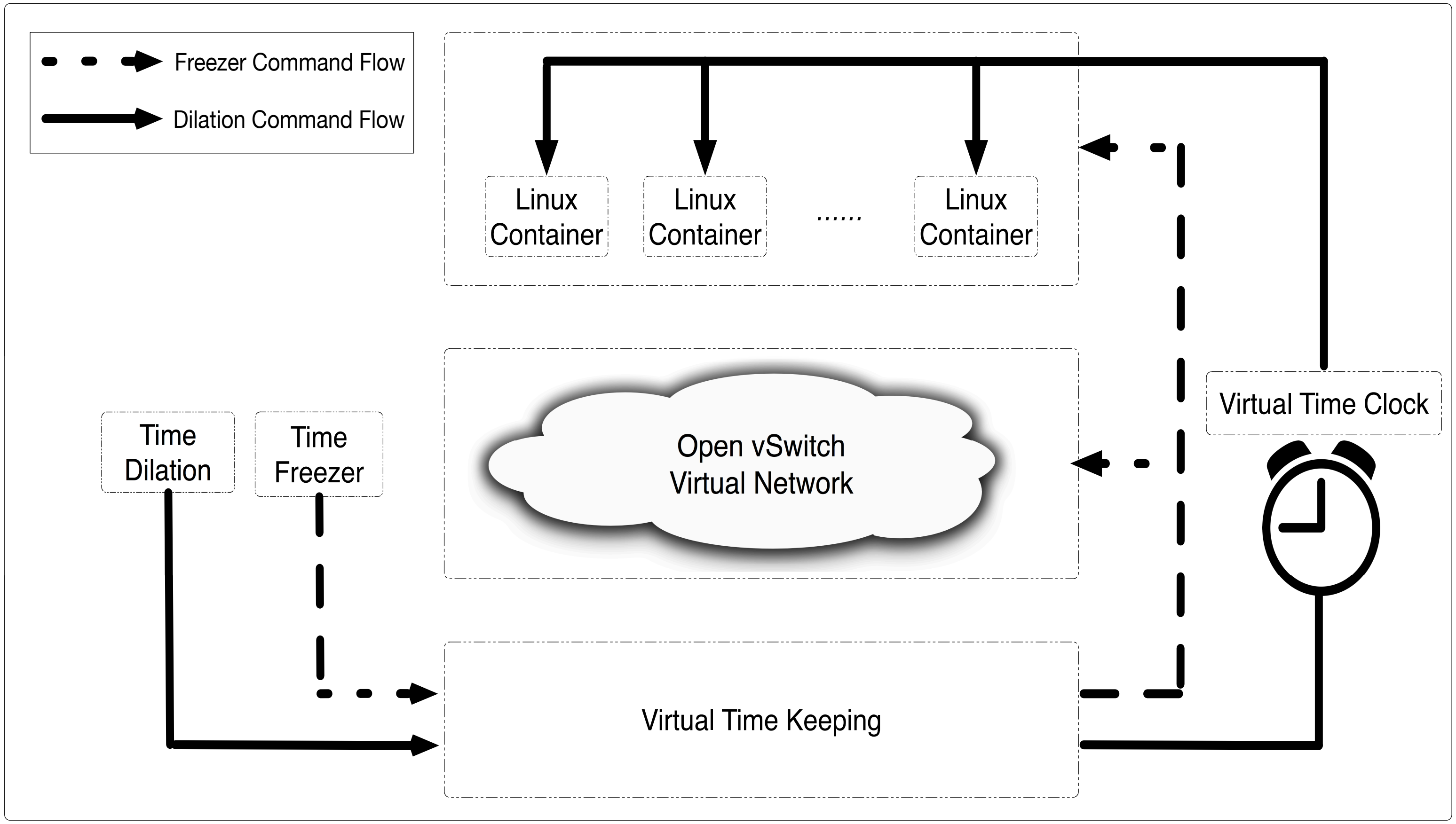
- Key idea: trade execution time with fidelity
- Time dilation factor (TDF) [Gupta, 2011]

$$= \frac{time\ passing\ rate\ in\ the\ physical\ world}{time\ passing\ rate\ in\ a\ VM's\ perception\ of\ time}$$

- TDF = 10
  - 10 seconds in real time <=> 1 second in a time-dilated emulated host
  - a 100 Mbps link is scaled to a 1 Gbps link

D. Gupta, K. V. Vishwanath, et al. "Diecast:Testing distributed systems with an accurate scale model". ACM Transactions on Computer Systems,29(2):1–48, 2011

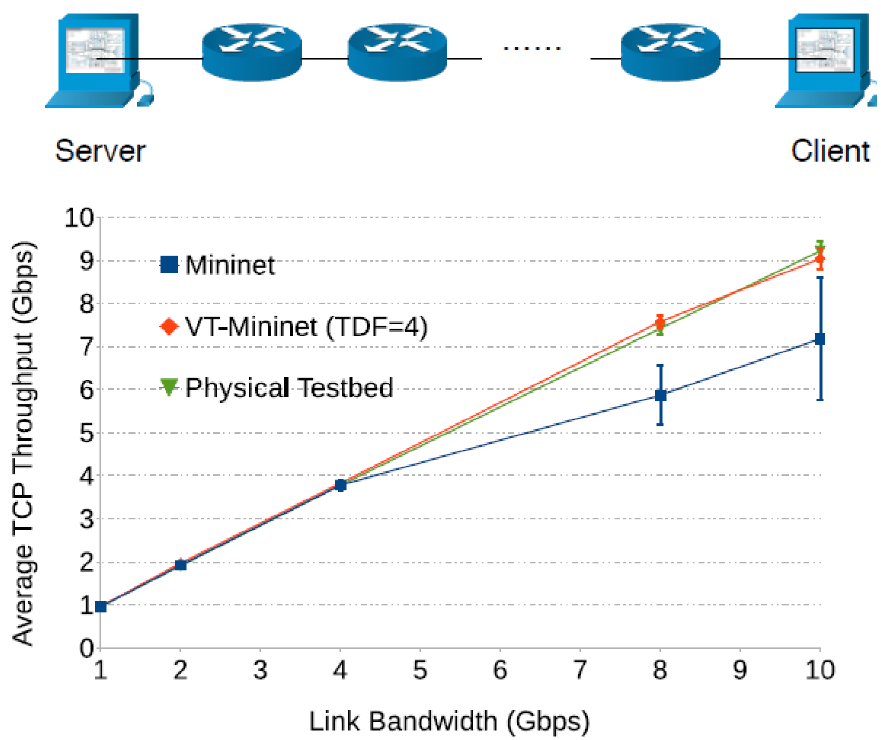
Virtual Time System Architecture for a Container-based Network Emulator



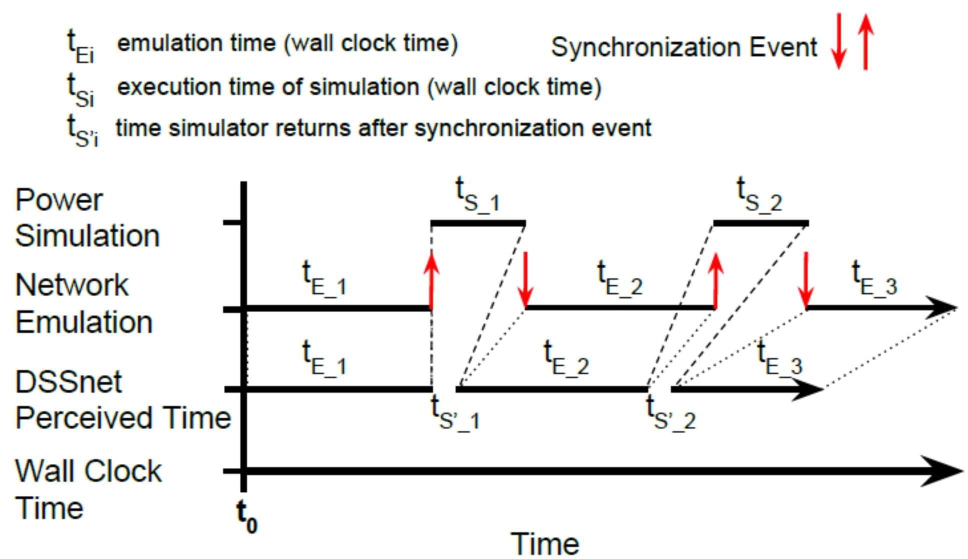
Source code: https://github.com/littlepretty/VirtualTimeForMininet

Virtual Time is Useful

1. Emulation Fidelity Enhancement



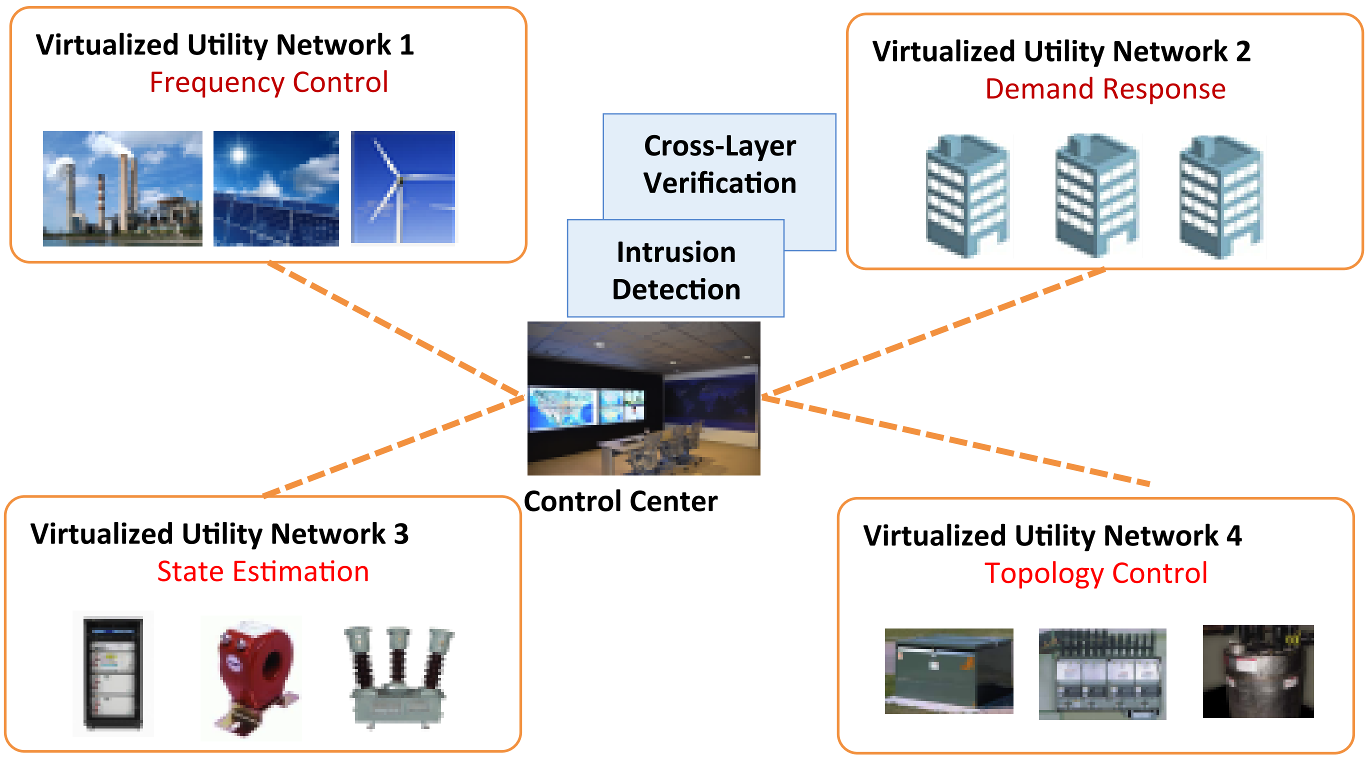
2. Simulation/Emulation Synchronization



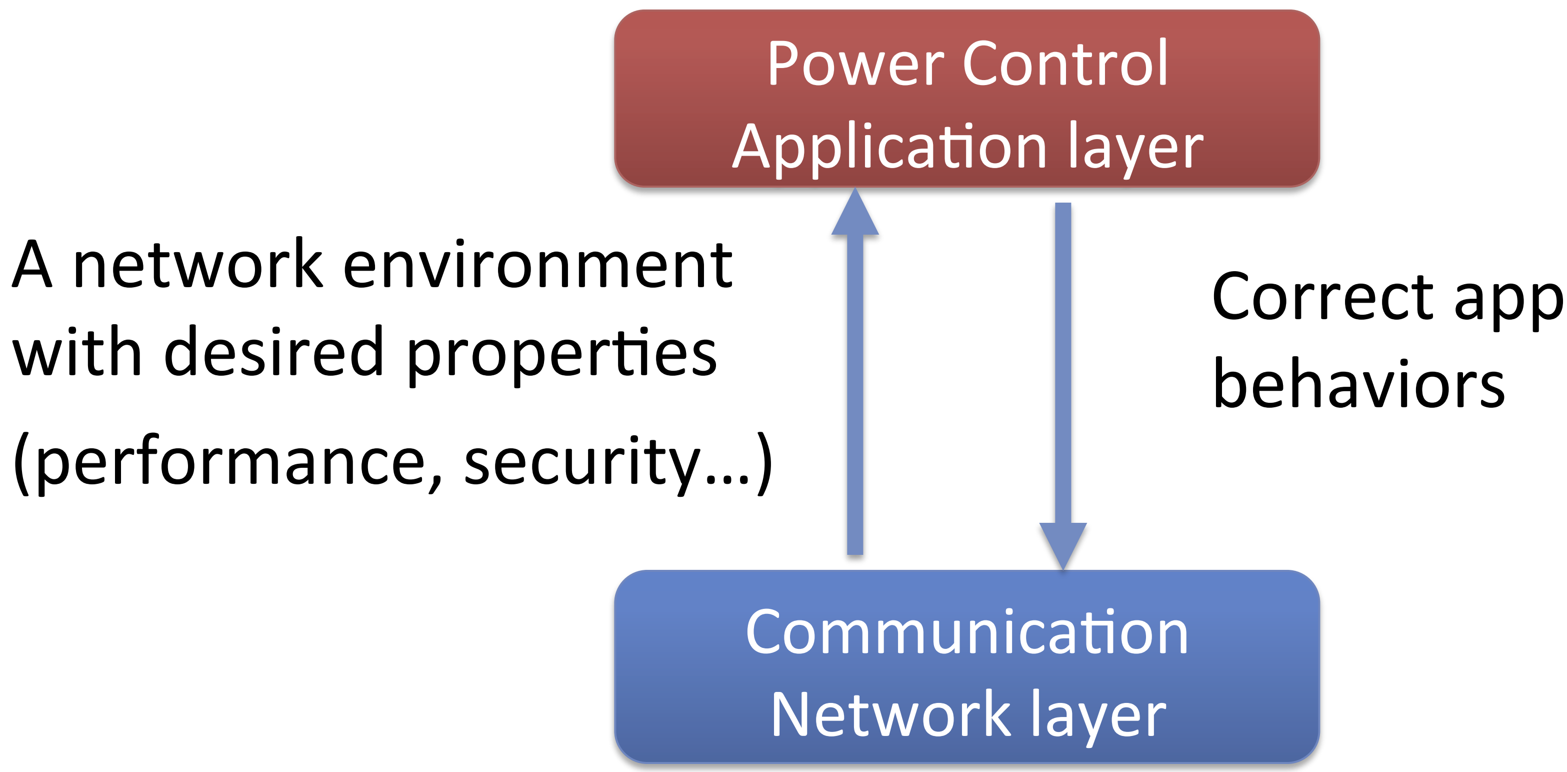
Future Work

- More applications
  - e.g., Specification-based Intrusion Detection
- Network layer → Application layer and Cross-layer verification
- In-house research idea → Real system deployment
  - IIT Microgrid
  - First Cluster of Microgrids in US (12MW IIT + 10MW Bronzeville)

Specification-based Intrusion Detection



Cross-layer Verification




Thank you