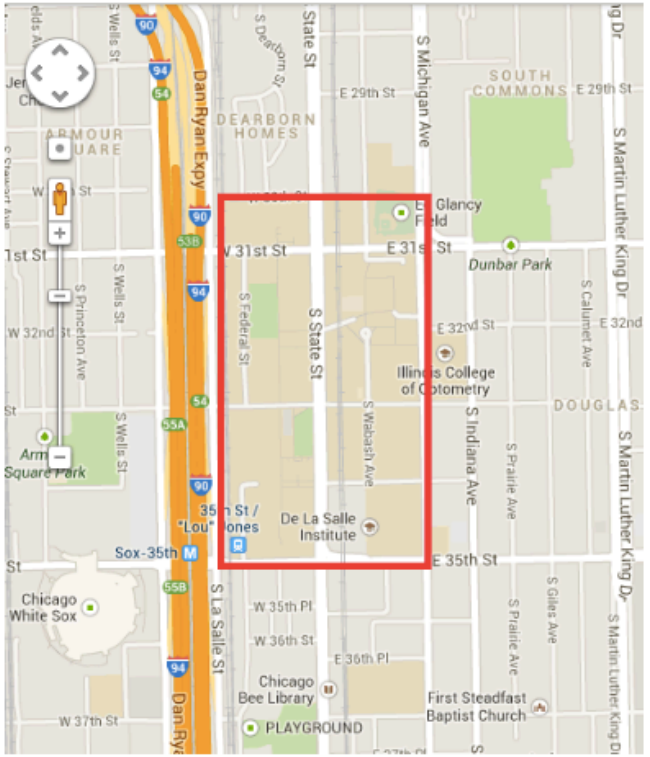
Enabling a Cyber-Resilient and Secure Energy Infrastructure with Software-Defined Networking



Dong (Kevin) Jin

Department of Computer Science

Illinois Institute of Technology

SoS Lablet/R2 Monthly Meeting, Jan 2017

ILLINOIS INSTITUTE OF TECHNOLOGY

Part of the SoS Lablet with

- David Nicol

- Bill Sanders

- Matthew Caesar

- Brighten Godfrey

Project Progress

Publications in the current quarter (Oct – Dec 2016)

- Jiaqi Yan and Dong Jin. "A Lightweight Container-based Virtual Time System for Software-defined Network Emulation," Journal of Simulation, November 2016
- Xin Liu and Dong Jin. "ConVenus: Congestion Verification of Network Updates in Software-defined Networks." Winter Simulation Conference (WSC), December 2016
- Ning Liu, Adnan Haider, Dong Jin and Xian-He Sun. "A Modeling and Simulation of Extreme-Scale Fat-Tree Networks for HPC Systems and Data Centers," ACM Transactions on Modeling and Computer Simulation (TOMACS), December 2016

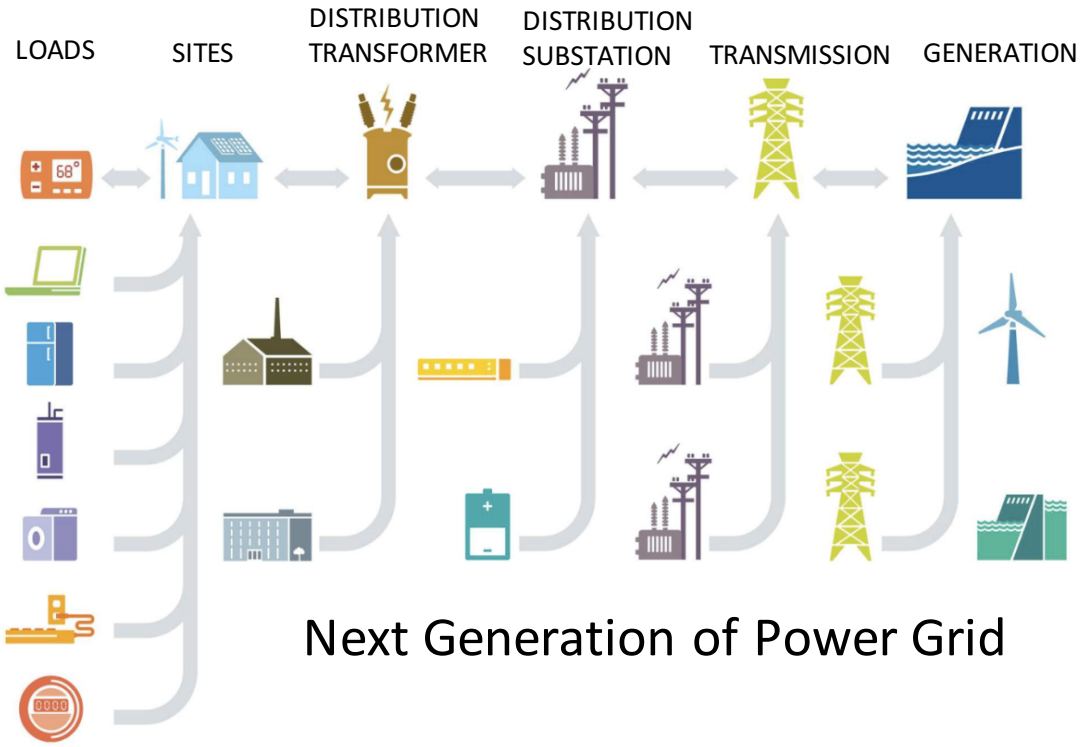
Project Progress

Paper submitted in the current quarter (Oct – Dec 2016)

- Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour, Cheol Won Lee and Jong Cheol Moon. "Towards a Resilient and Secure Microgrid Using Software-Defined Networking," IEEE Transactions on Smart Grid, Special section on Smart Grid Cyber-Physical Security (Second round review)
- Christopher Hannon, Jiaqi Yan, Dong Jin, Chen Chen, and Jianhui Wang. "Combining Simulation and Emulation Systems for Smart Grid Planning and Evaluation," ACM Transactions on Modeling and Computer Simulation (TOMACS)
- Christopher Hannon, Dong Jin, Chen Chen, and Jianhui Wang, "Ultimate Forwarding Resilience in OpenFlow Networks," ACM SIGCOMM Symposium on SDN Research 2016

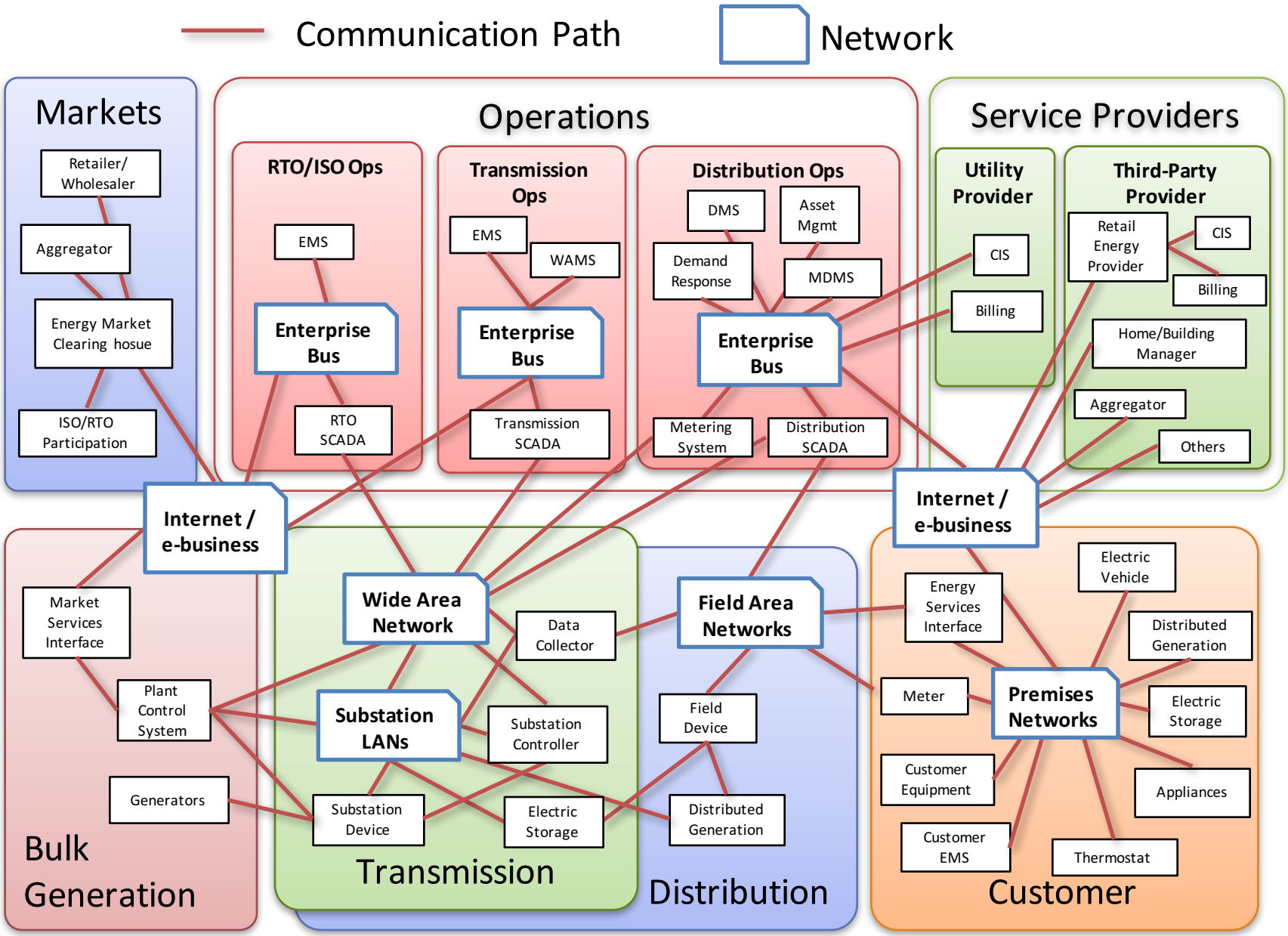
Industrial Control Systems (ICS)

- 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



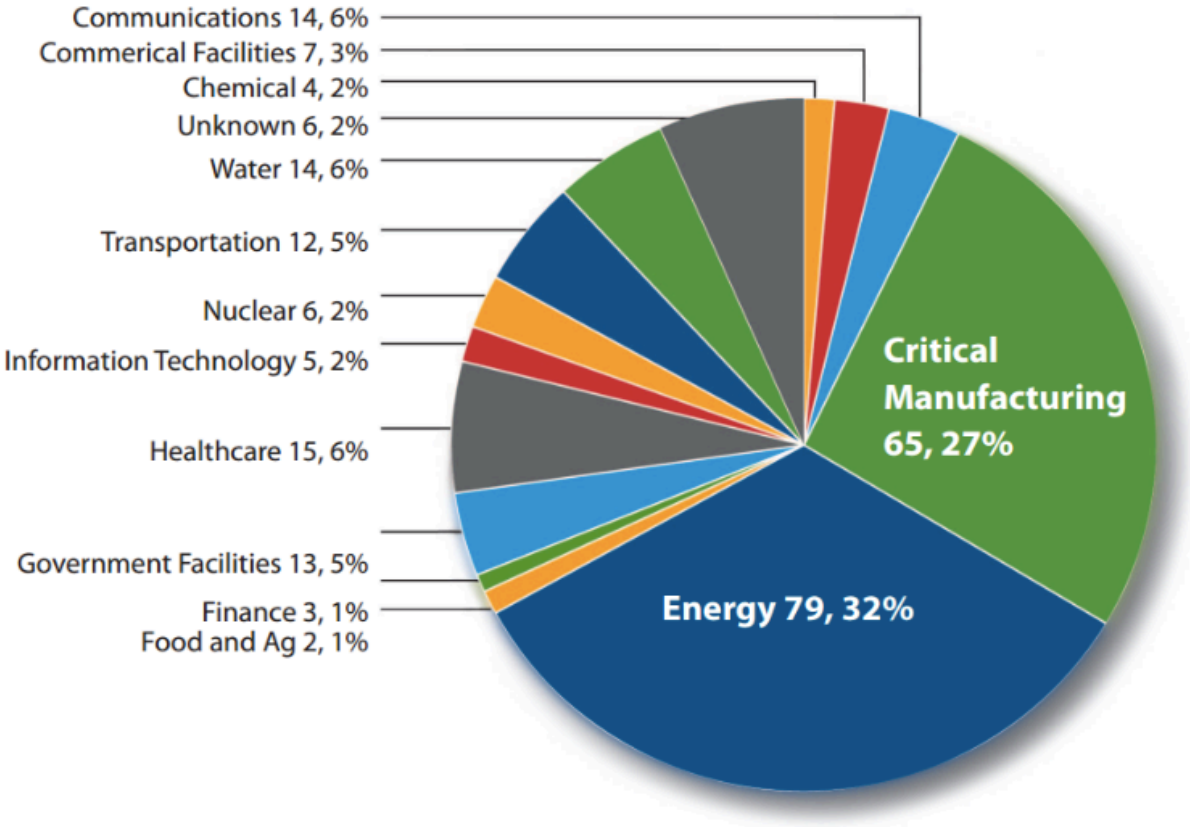
Next Generation of Power Grid

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

Ukraine Power Grid Cyber Attack

- 80,000 residents in western Ukraine
- 6 hours, 134 MW power lost in Dec 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?

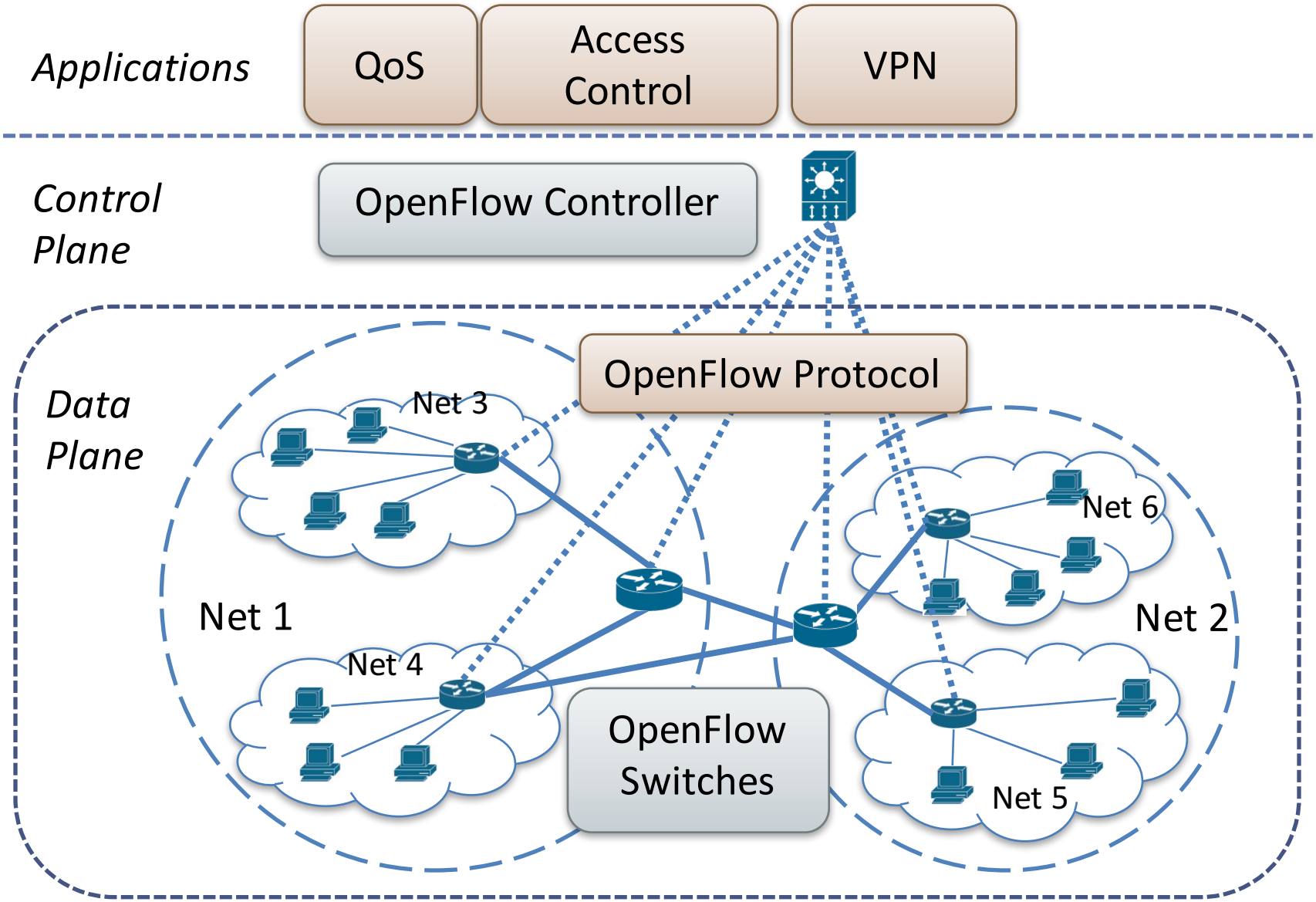
Problem Statement

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

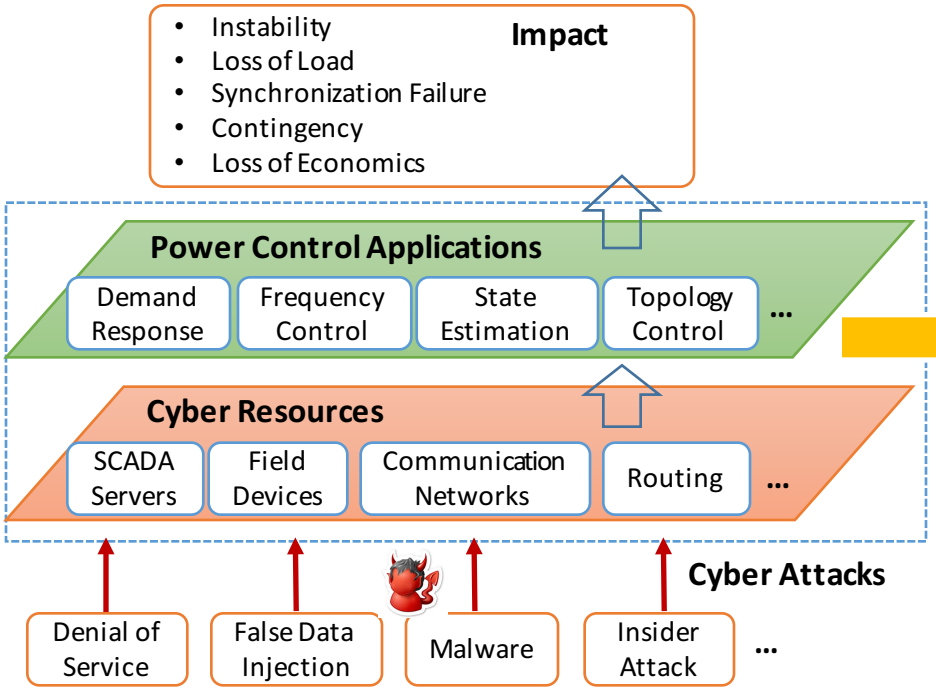
ICS – industrial control system

SDN – software-defined networking

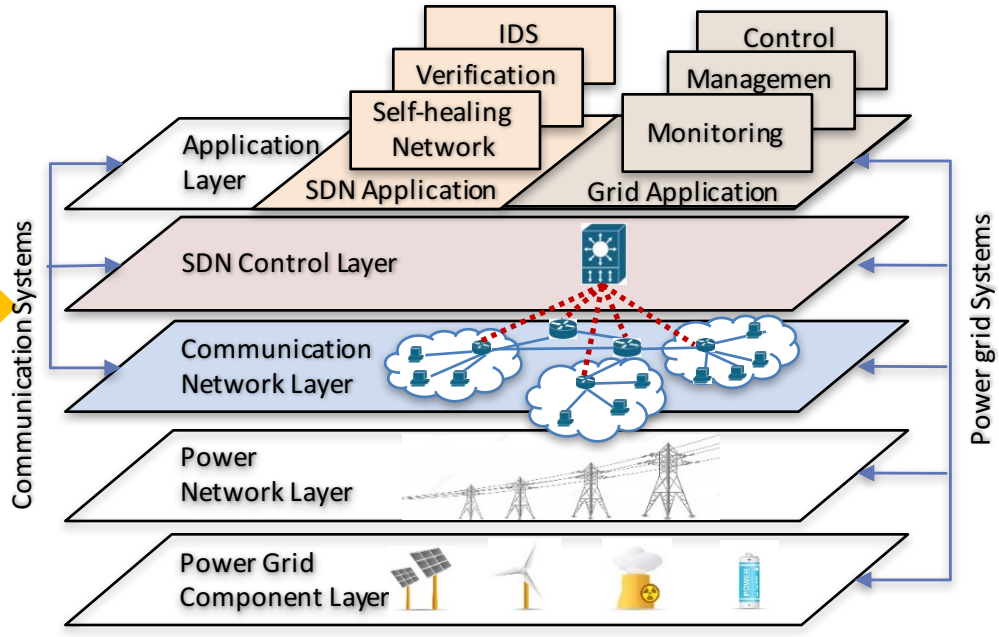
SDN Architecture



An SDN-Enabled Power Grid



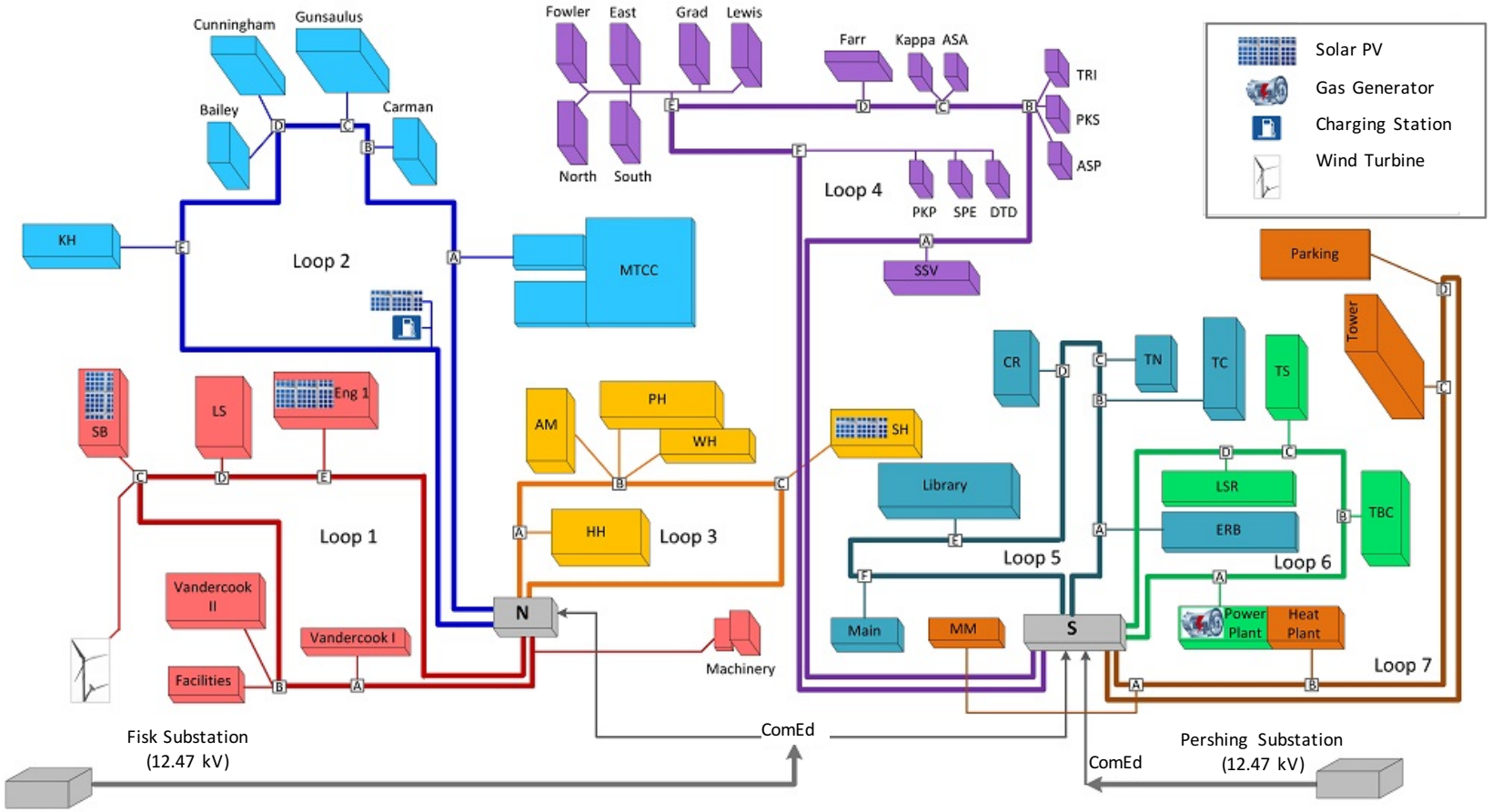
Current Power Grid: Potential Cyber Attacks and Their Implications



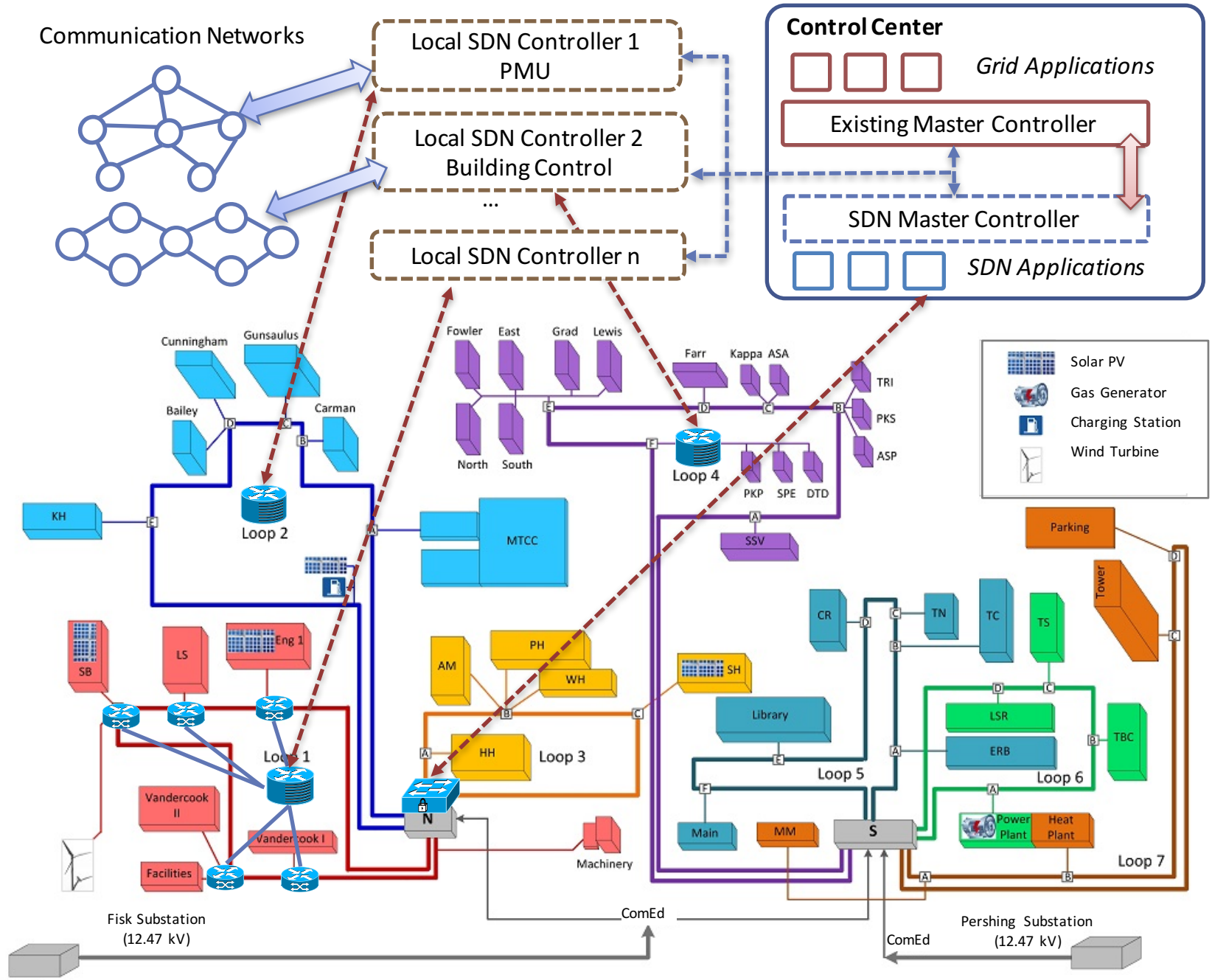
Future SDN-enabled Power Grid: A Cyber-Attack-Resilient Platform

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
Fowler
East
Grad
Lewis
North
South
Farr
Kappa
ASA
TRI
PKS
ASP
PKP
SPE
DTD
Loop 4
KH
Loop 2
MTCC
SSV
Parking
Tower
CR
TN
TC
TS
SB
LS
Eng 1
AM
PH
WH
SH
Library
LSR
ERB
TBC
HH
Loop 3
Loop 5
Loop 6
Loop 1
Vandercook II
Vandercook I
Facilities
N
Machinery
Main
MM
S
Power Plant
Heat Plant
Loop 7
Fisk Substation
(12.47 kV)
ComEd
ComEd
Pershing Substation
(12.47 kV)

Transition to an SDN-Enabled Microgrid

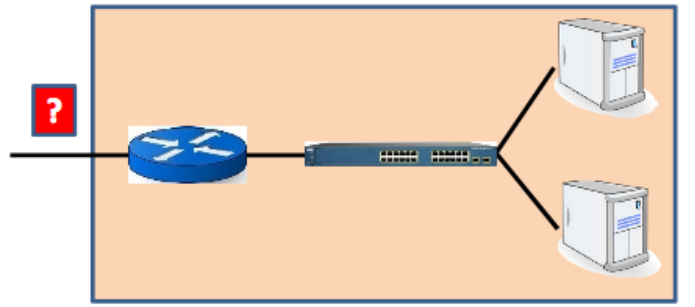
- SDN-based Applications
  - Real-time Verification
  - Self-healing PMU
- Hybrid Testbed
  - SDN emulation + Power Distribution System Simulation

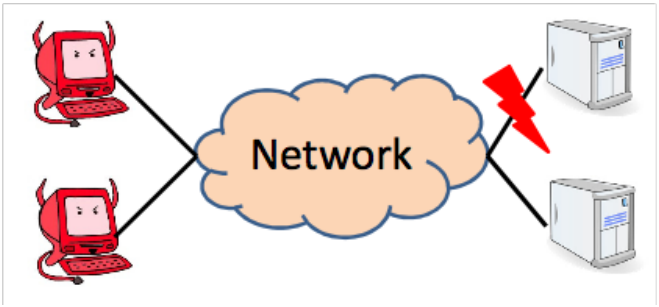
Application 1: Network Verification – Motivation

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

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

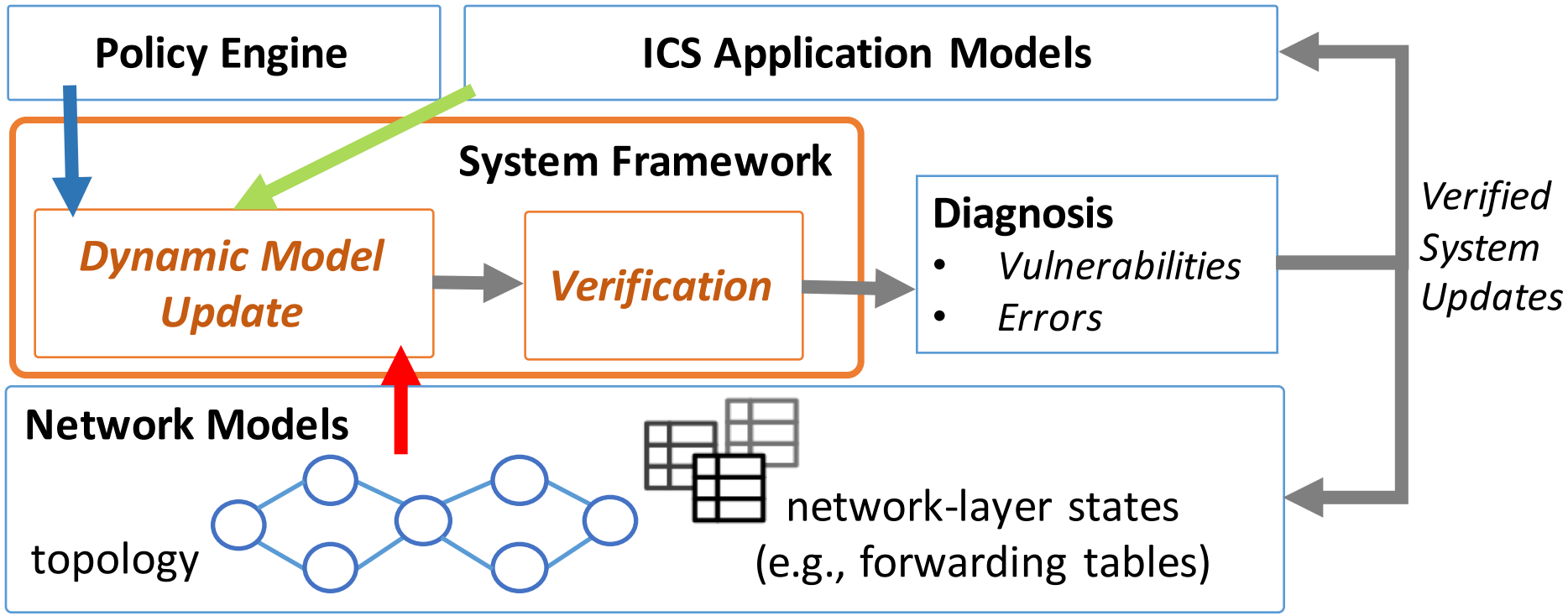
- Unauthorized access
- Unavailable critical services
- System performance drop
  - Instability
  - Loss of load
  - Synchronization Failure
- …





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

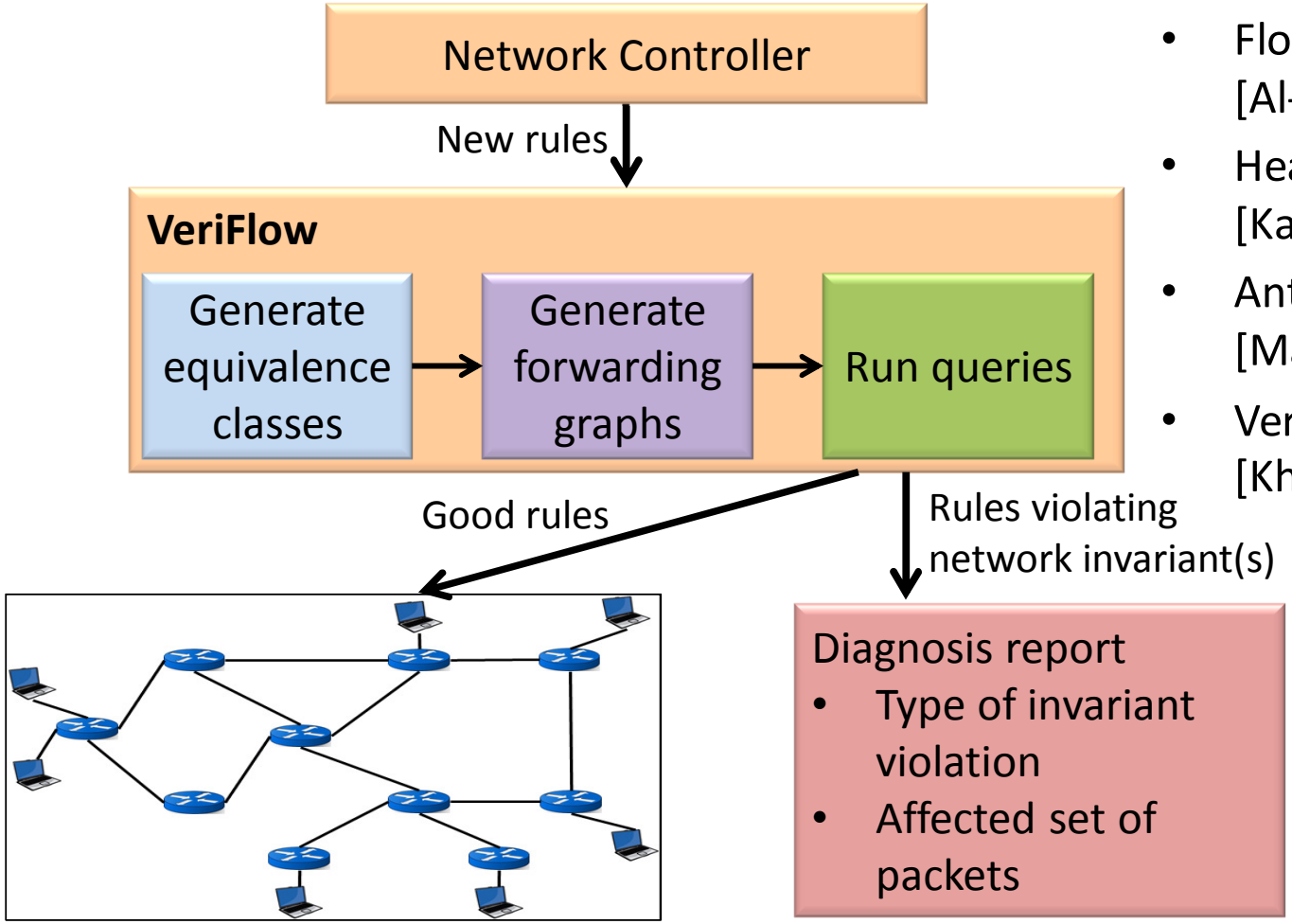


Dynamic Network Data (topology, forwarding tables …)

Dynamic Application Data (control updates …)

User-specified Policy (security, performance …)

Network-Layer Verification



Prior Work

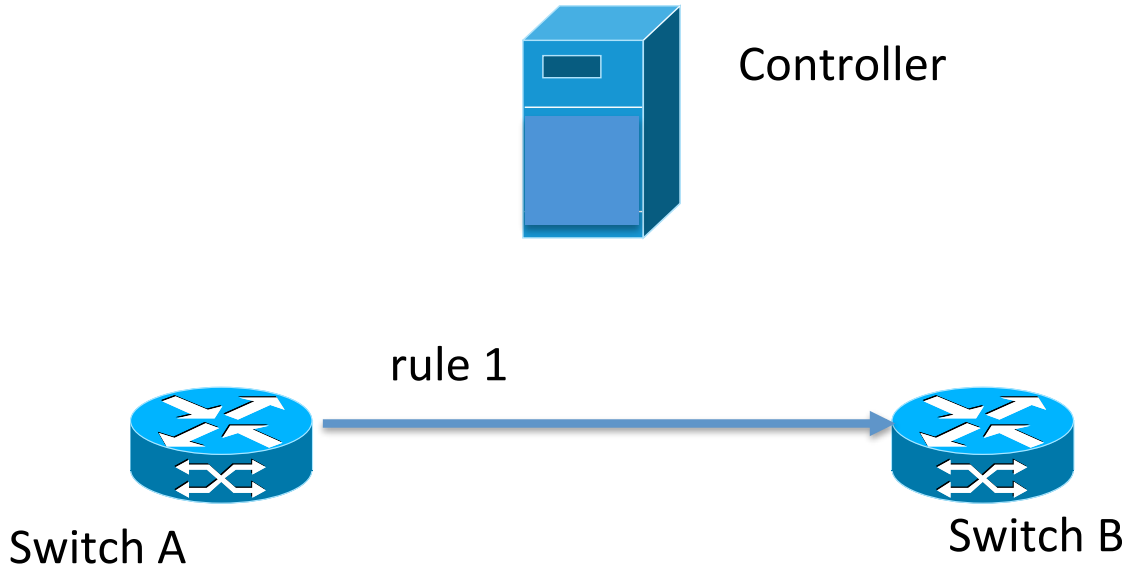
- FlowChecker [Al-Shaer et al.,SafeConfig2010]
- HeaderSpaceAnalysis [Kazemian et al.,NSDI2012]
- Anteater [Mai et al.,SIGCOMM2011]
- VeriFlow [Khurshid et al., NSDI2012]

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

Challenges — Timing Uncertainty

Old config: Switch A => Switch B

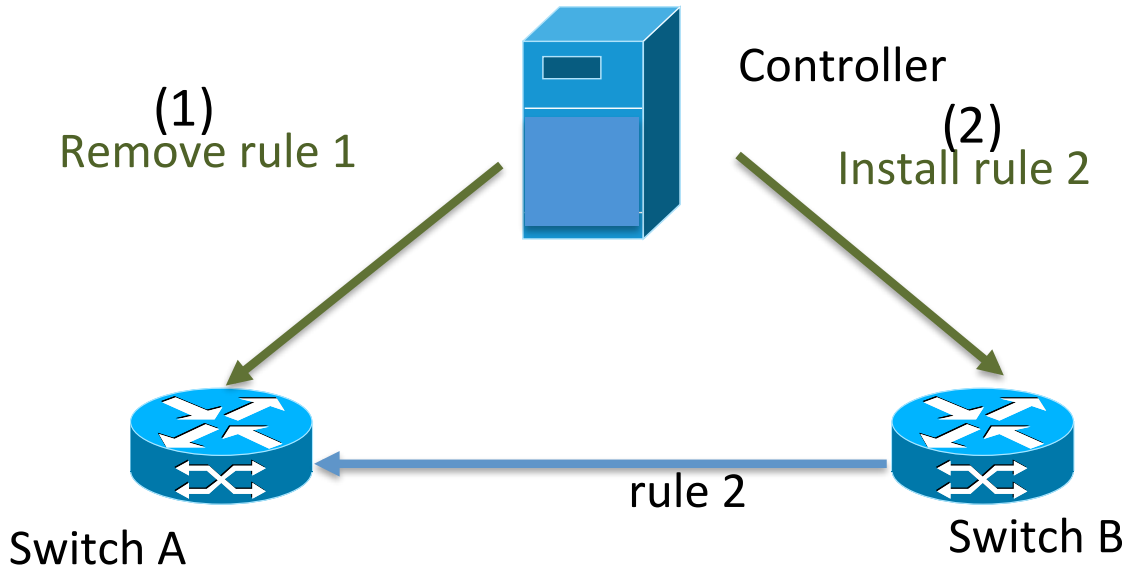
New config: Switch B => Switch A



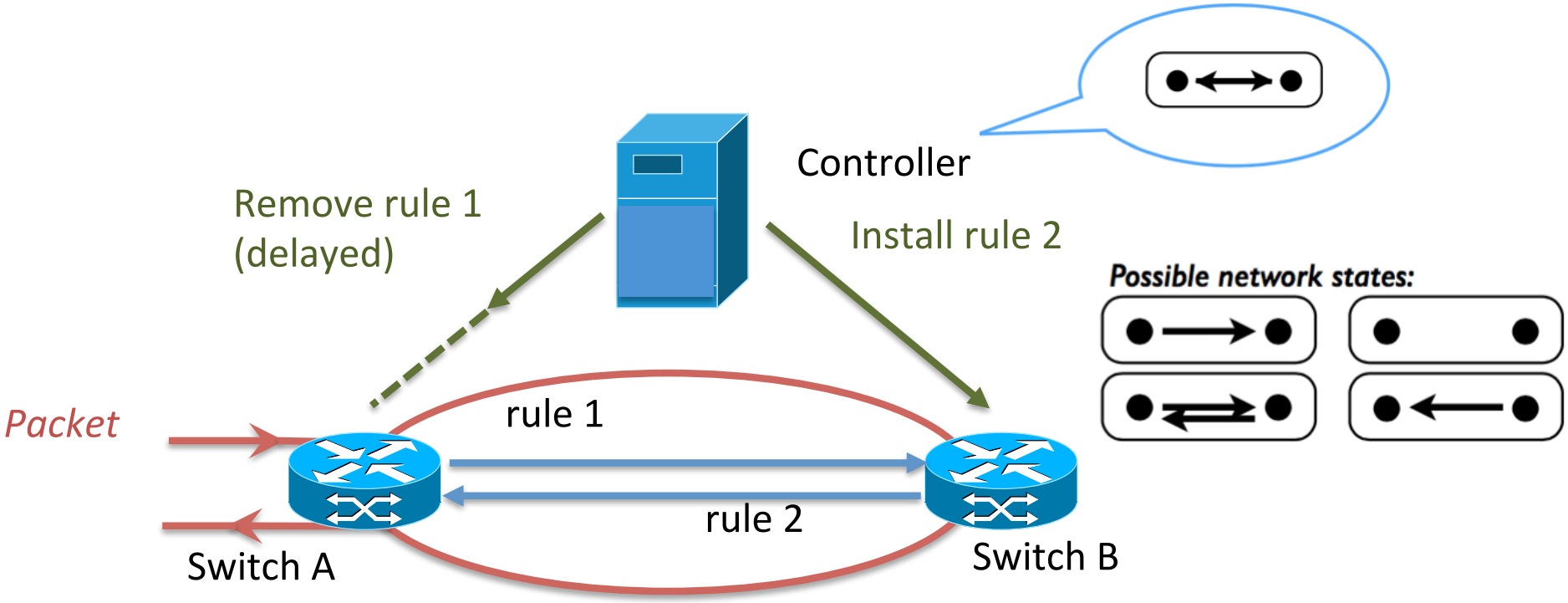
Challenges — Timing Uncertainty

Old config: Switch A => Switch B

New config: Switch B => Switch A



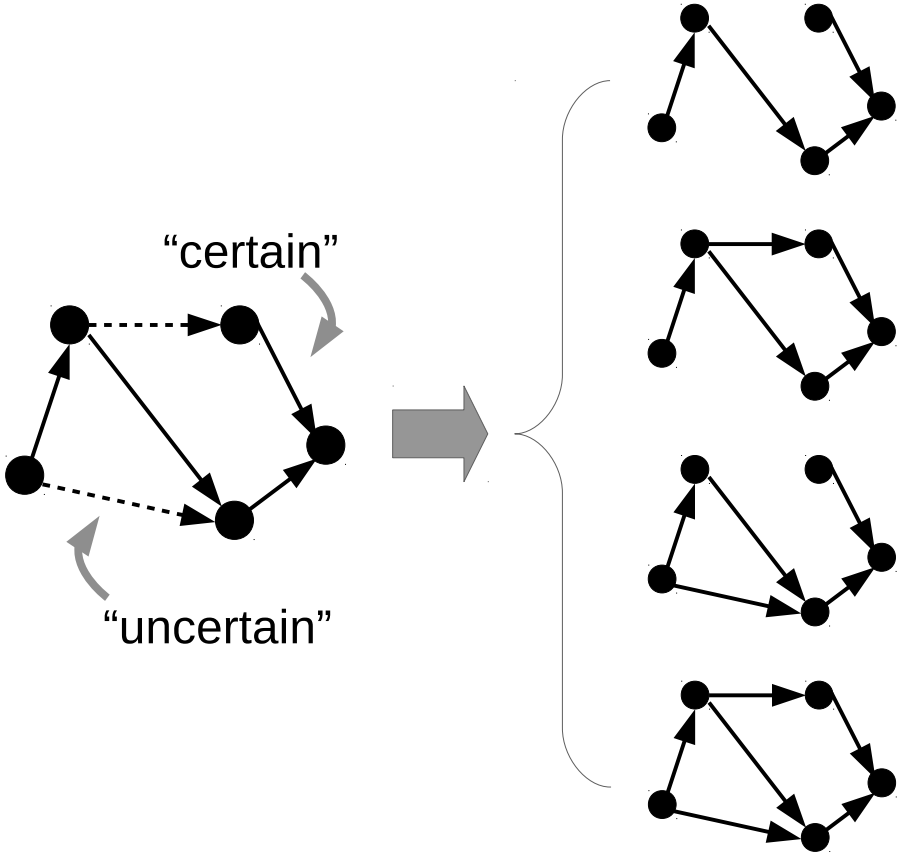
Challenges — Timing Uncertainty



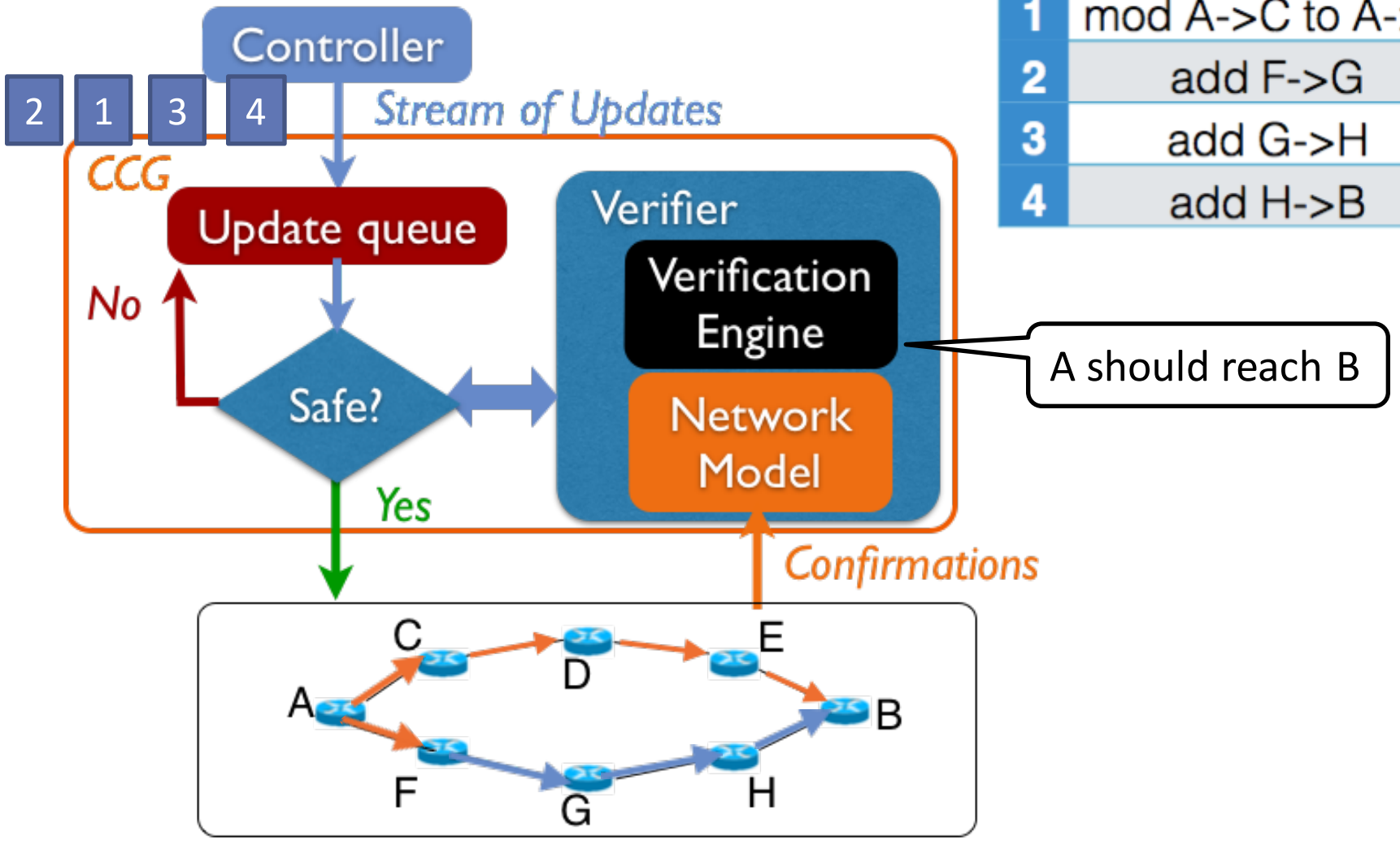
Loop-freedom Violation

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

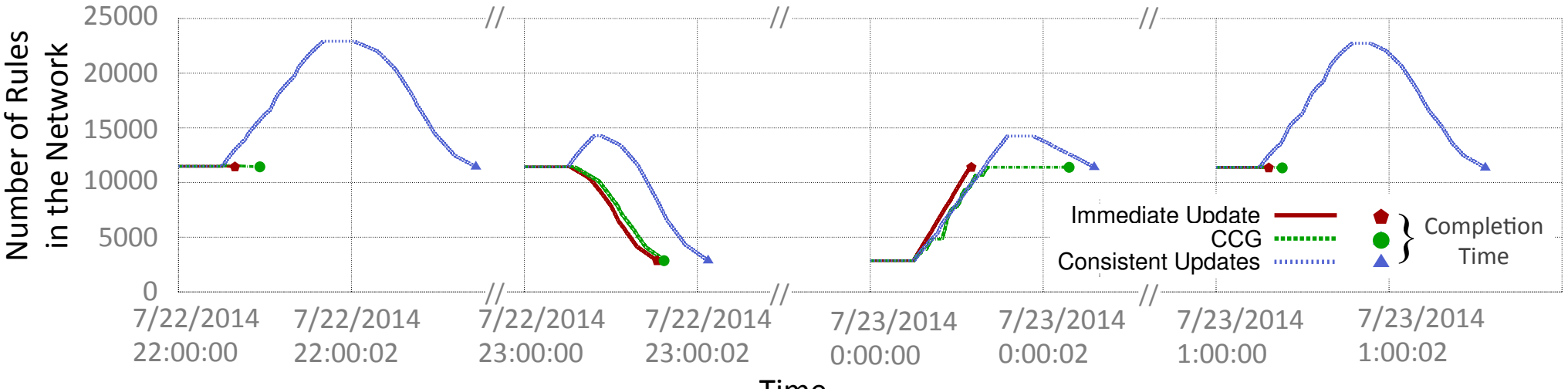
Enforcing dynamic correctness with heuristically maximized parallelism

OK, but…

Can the system "deadlock"?

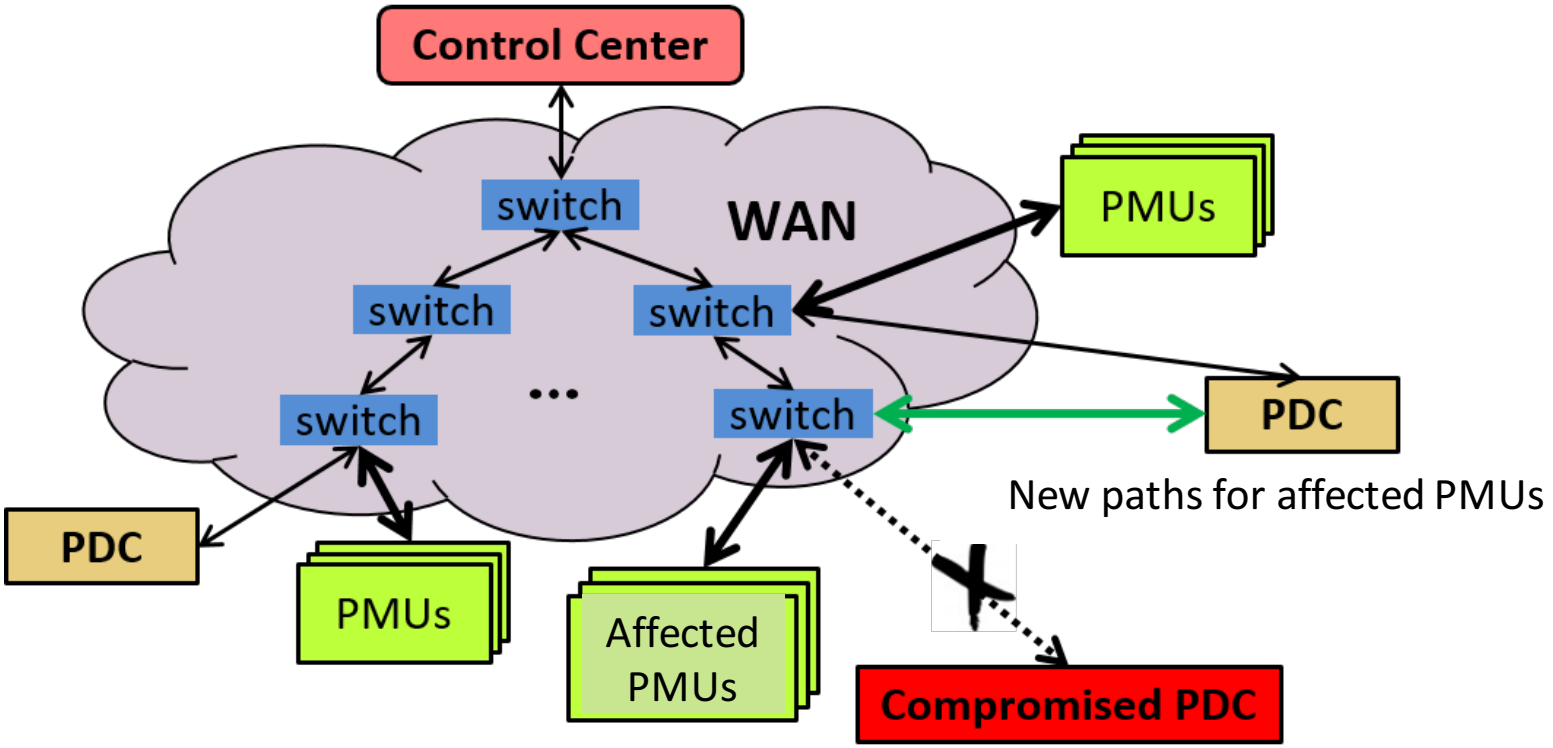
- Proved classes of networks that never deadlock
- Experimentally rare in practice!
- Last resort: heavyweight "fallback" like consistent updates [Reitblatt et al, SIGCOMM 2012]

Is it fast?



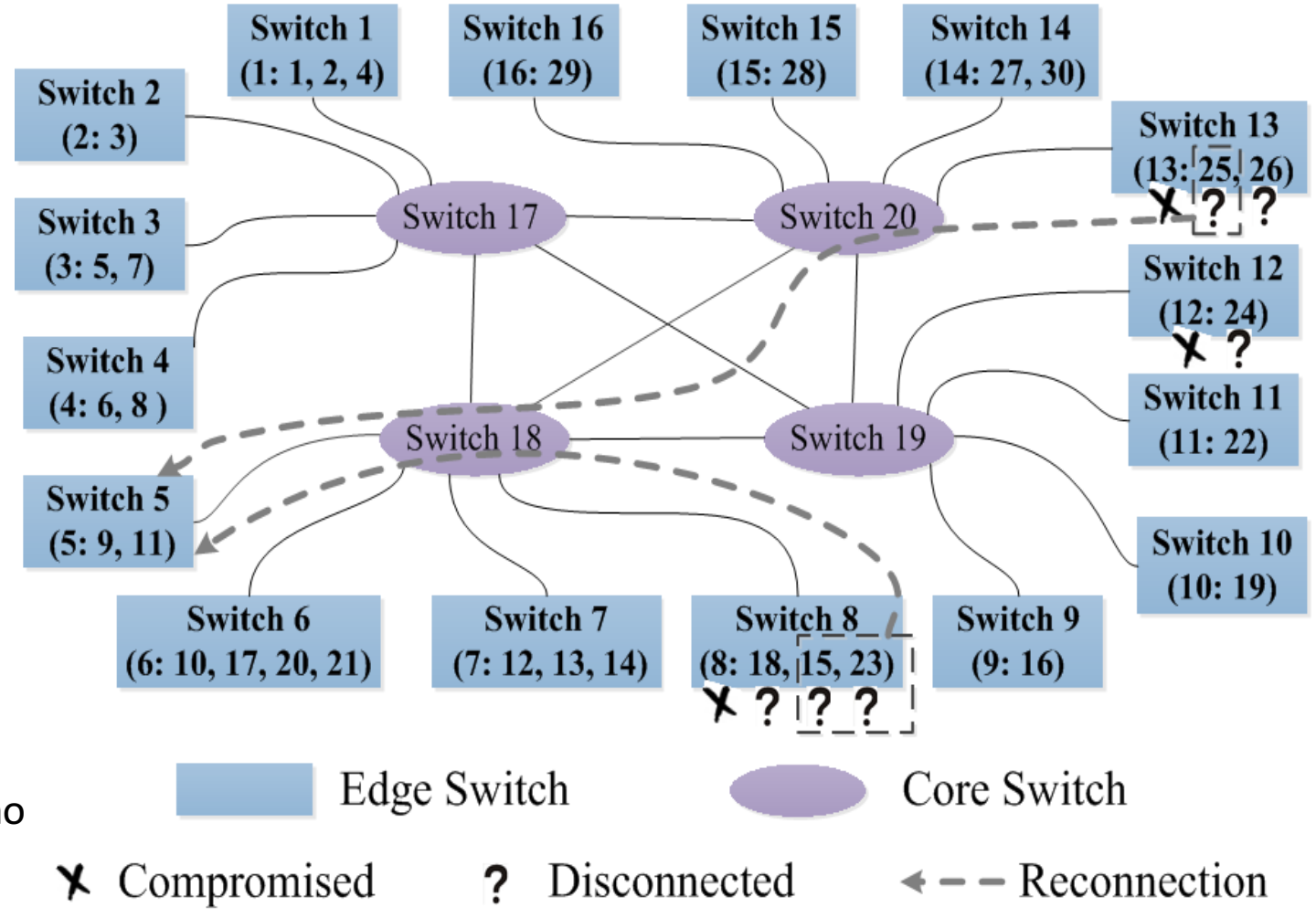
Slide borrowed from Brighten Godfrey, TSS Seminar, Sep 2015

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



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

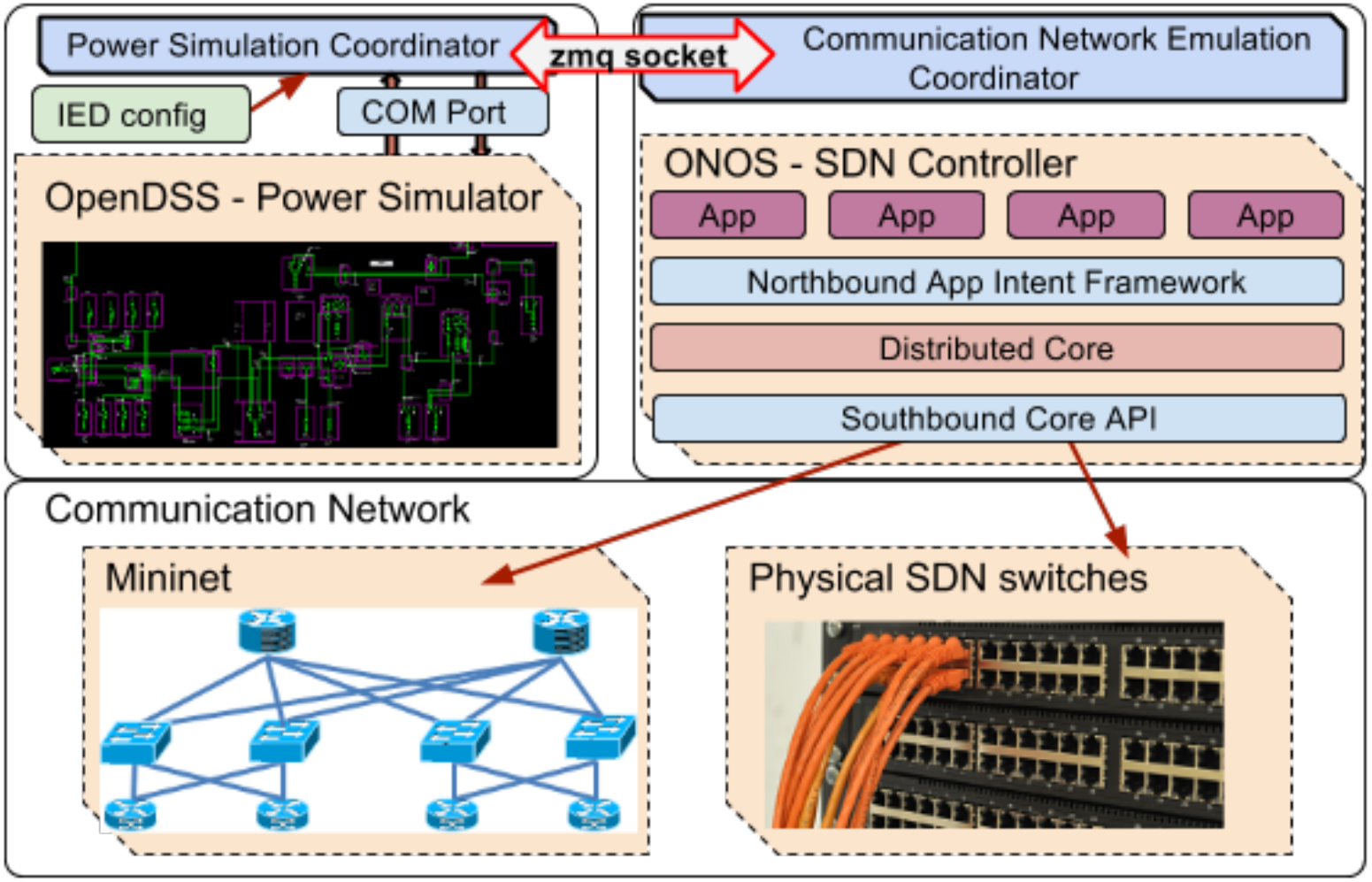
Self-Healing Phasor Measurement Unit (PMU) Networks



Video Demo

Self-healing Scheme on PMU Network for IEEE 30-bus System

A Hybrid Testing Platform



Power Distribution System Simulation + SDN-based Network Emulation

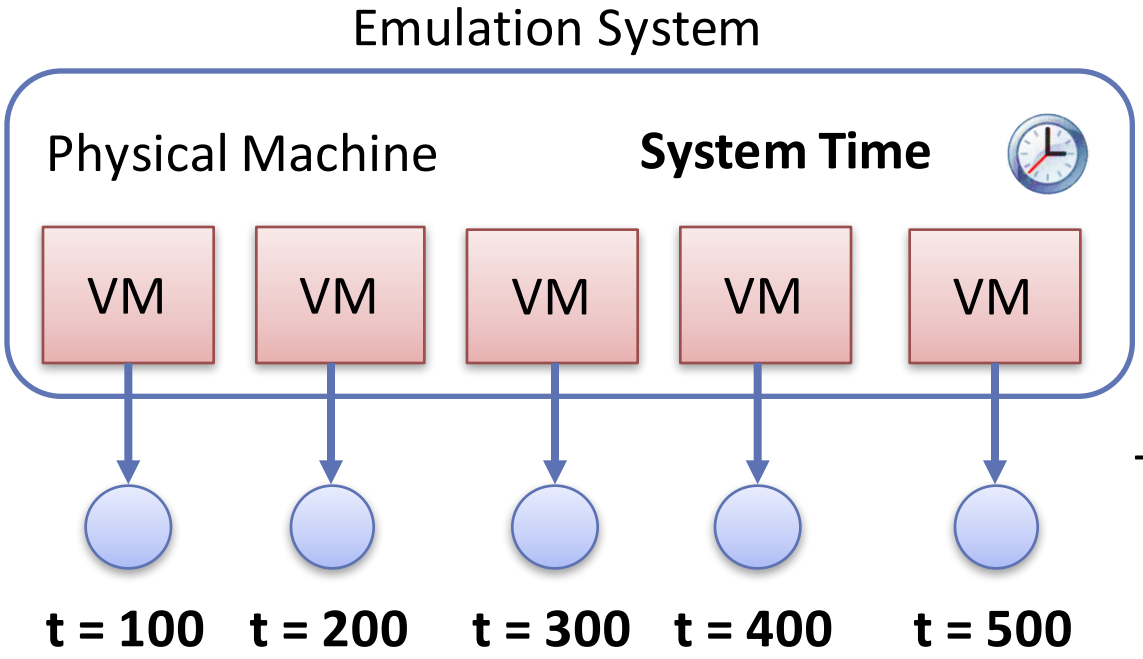
A Hybrid Testing Platform

- 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

Integration Emulation & Simulation

Issue: Temporal Fidelity in emulation

ordinary emulators embedded in real-time, but simulators speak in virtual time



VM - Virtual Machine

Time Slice – System Execution Unit

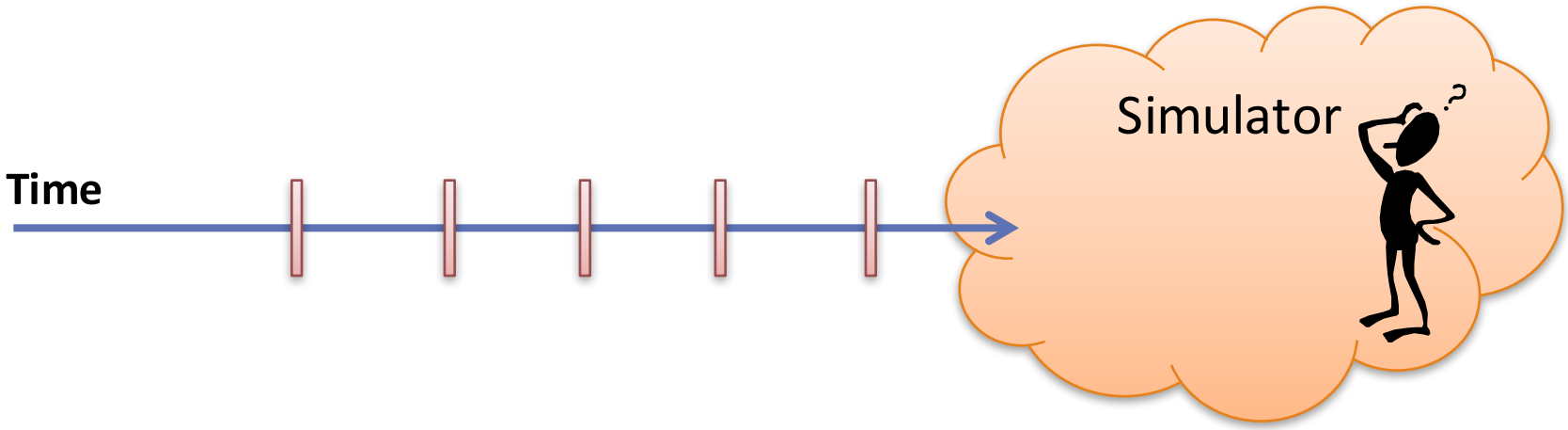
e.g., Time Slice = 100 µs

Integration Emulation & Simulation

Suppose the medium is shared access…

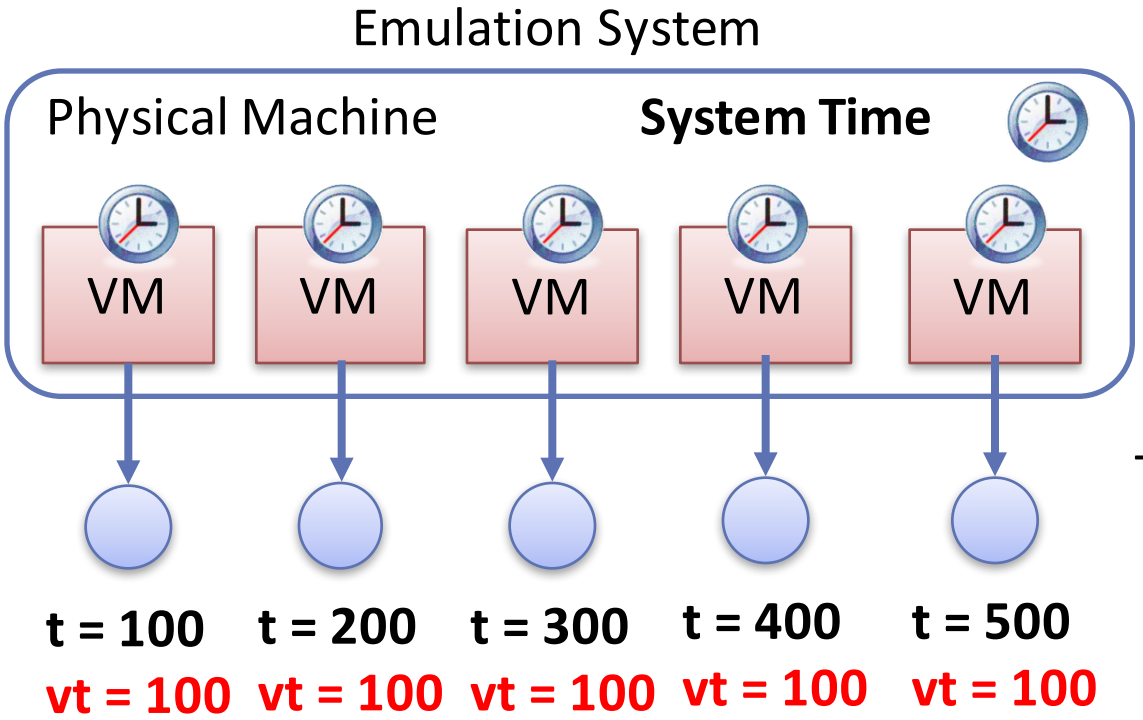
Suppose the packets all join the same queue….

Wrong behaviors due to the emulator's serialization of the time



Our approach: Virtual Time in Emulation

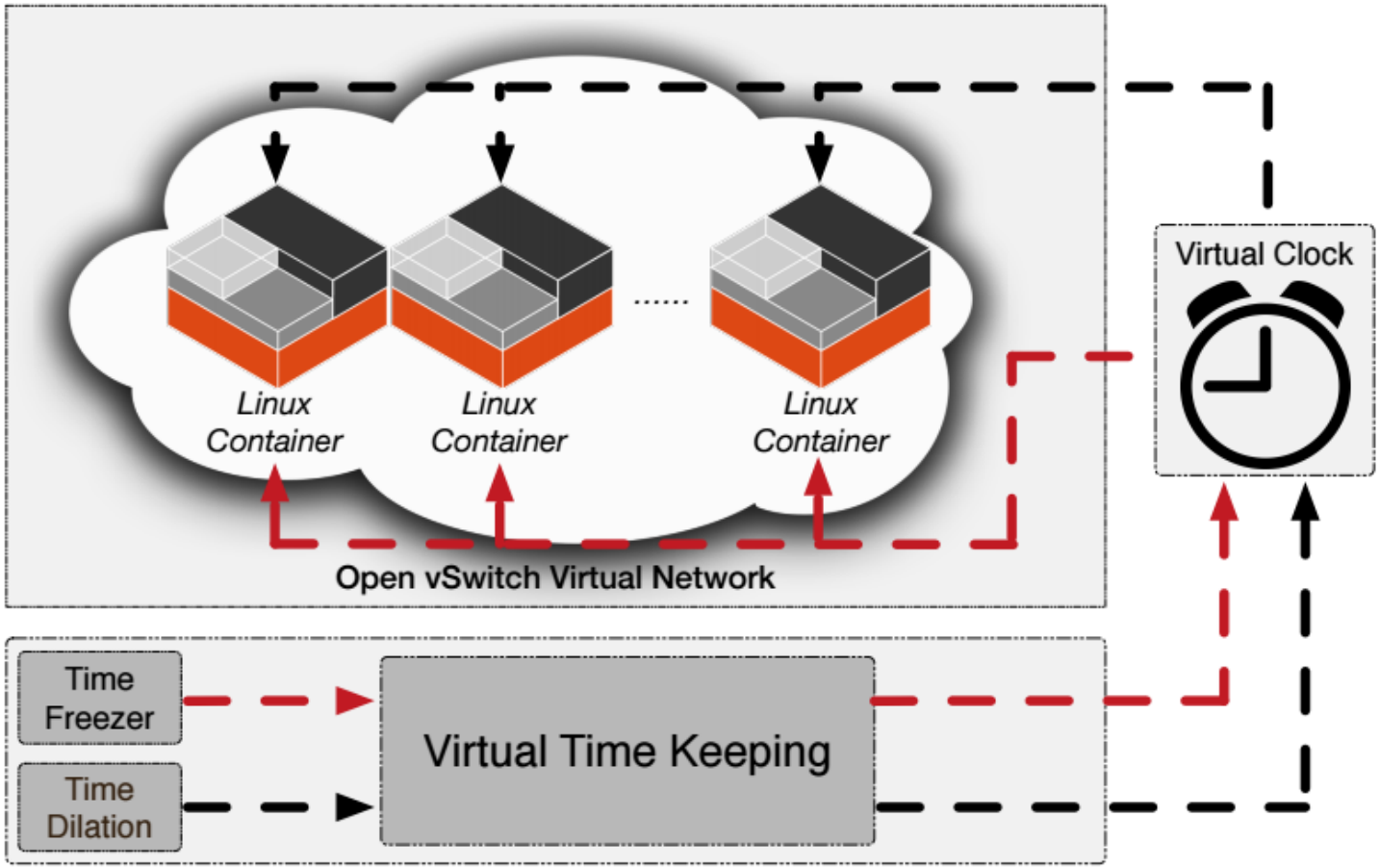
When the emulator is embedded in **virtual time**, time stamps on messages are closer to reality



VM - Virtual Machine

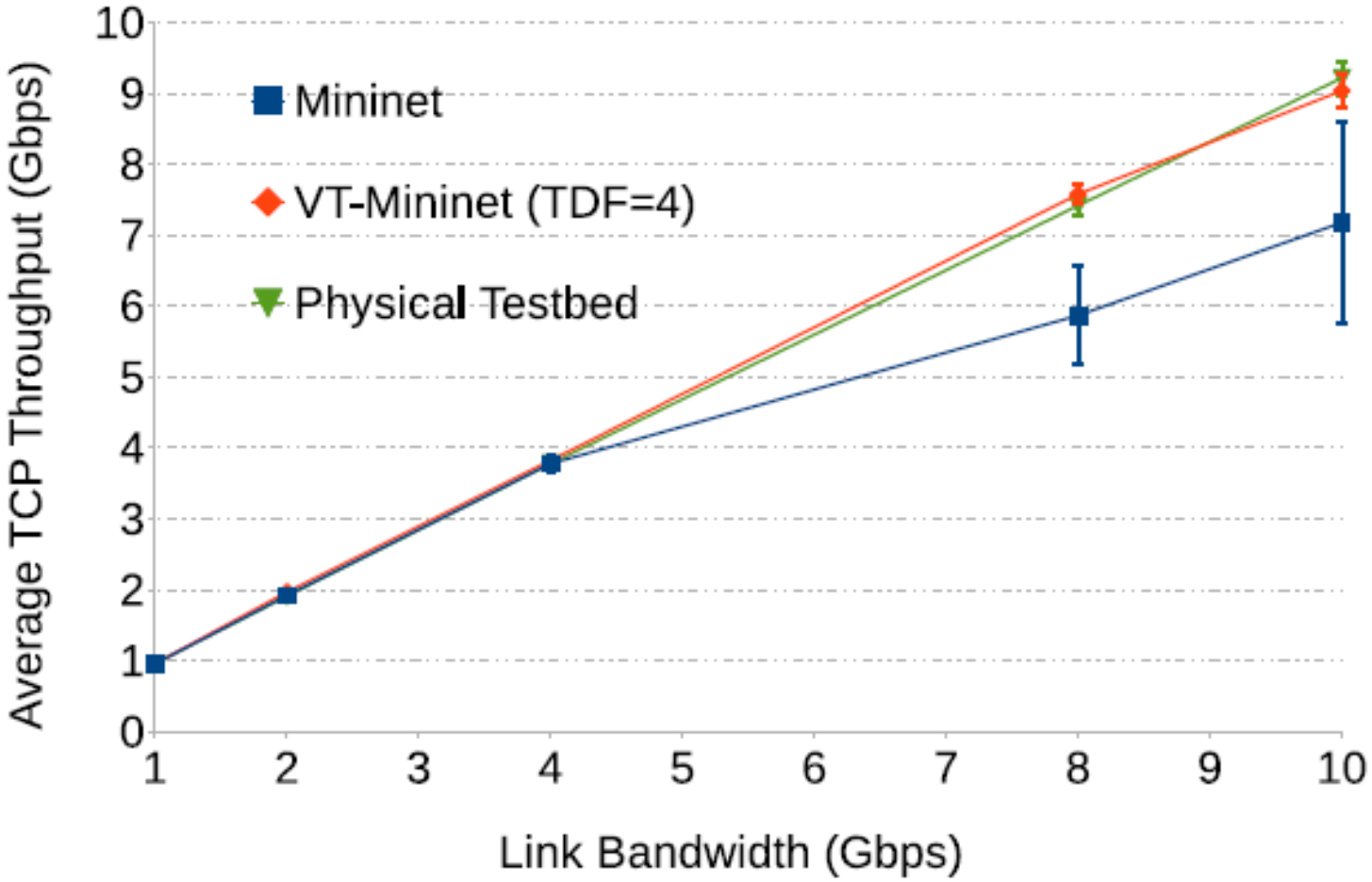
Time Slice – System Execution Unit
e.g., Time Slice = 100 µs

Virtual Time System Architecture for a Container-based Network Emulator

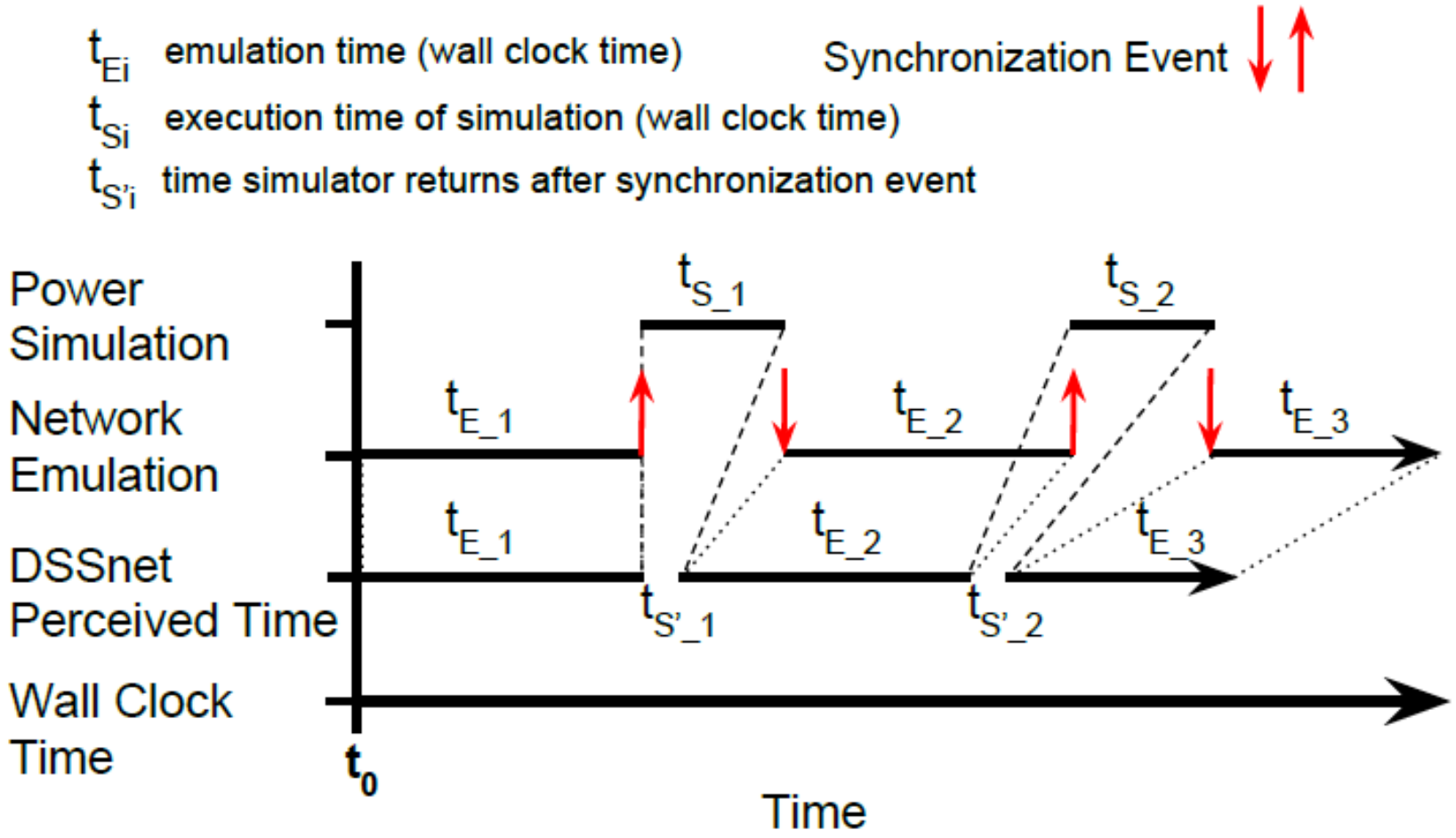


Source code: https://github.com/littlepretty/VirtualTimeForMininet

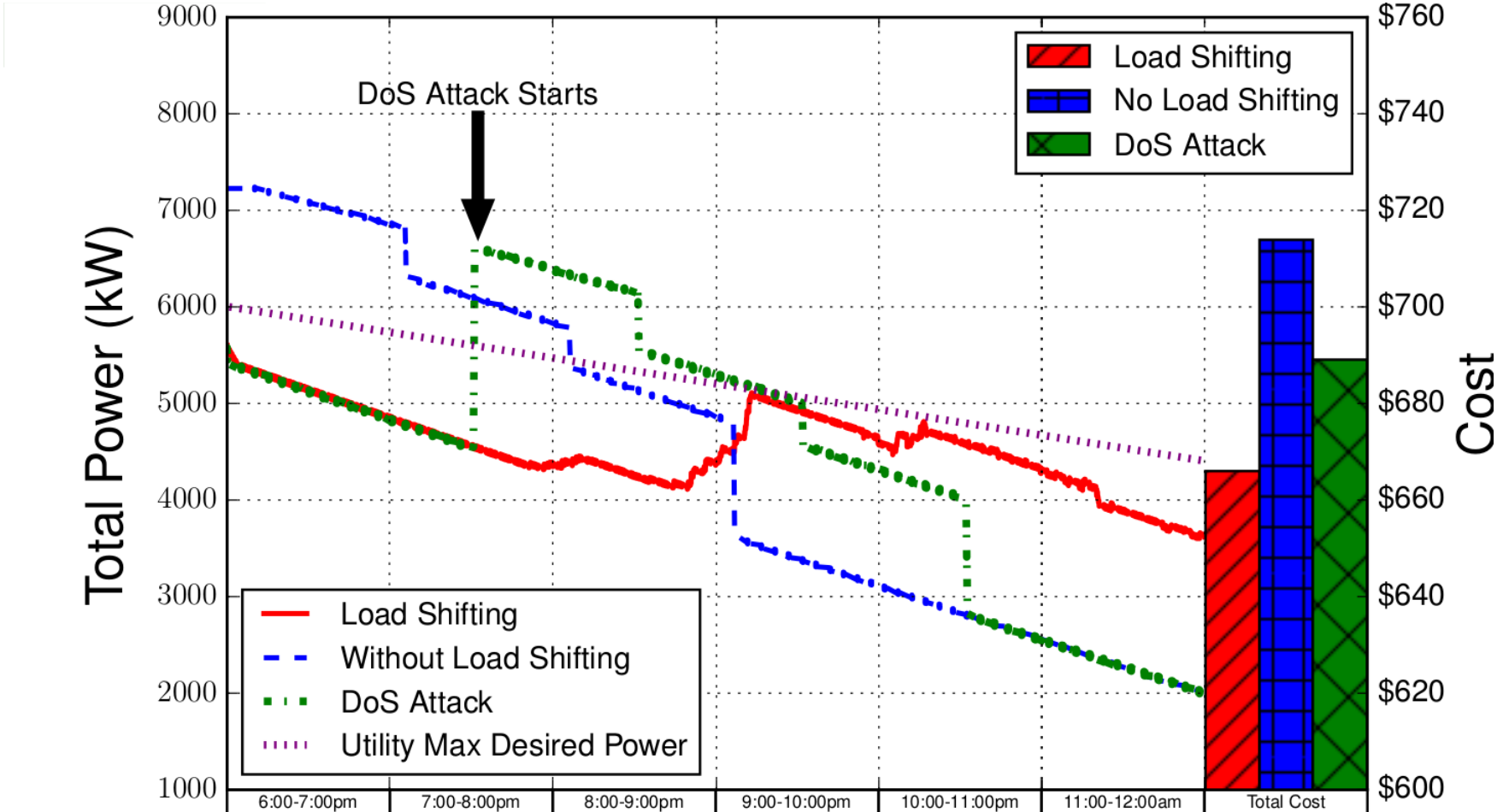
Virtual Time to Emulation Fidelity Enhancement



Virtual Time for Simulation/Emulation Synchronization



DSSNet Use Case



	6:00-7:00pm	7:00-8:00pm	8:00-9:00pm	9:00-10:00pm	10:00-11:00pm	11:00-12:00am	Total Cost
Avg Price (cents/kWh)	3.15	2.9	2.75	2.3	1.9	1.4	2.40(Avg)
Load Shifting (USD)	158.62	130.57	115.27	112.65	91.41	57.51	666.01
No Load Shifting (USD)	217.15	177.34	143.98	86.85	55.95	32.39	713.66
DoS Attack (USD)	158.62	161.85	153.56	114.26	67.89	32.39	688.57

Future Work

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


Thank you