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

Dong (Kevin) Jin

ILLINOIS INSTITUTE OF TECHNOLOGY

Who am I?

- CS faculty, Ph.D., University of Illinois at Urbana-Champaign (UIUC), http://cs.iit.edu/~djin/
- Research: cyber-security, networking, cyber-physical system security, simulation & modeling
- Industrial experience at Los Alamos National Lab, IBM, Motorola
- I like designing/building/deploying large-scale software systems that are grounded in strong theoretical principles

Master of Cyber Security Program

- New CS master degree started at Fall 2019
- What is unique?
  - **From theory to practice**
    - Data and information security
    - Network and system security
    - Software security
- Why join us?
  - IIT is a Center of Academic Excellence in Information Assurance Education (CAE/IAE) designated by the National Security Agency
  - CS
    - Multi-millions of federal/industrial research grants in cyber security
    - A very strong team in the cyber security research and education
- How to join?
  - https://science.iit.edu/programs/graduate/master-cybersecurity-mcybcode
  - Also available to co-terminal students

Master of Cyber Security Program

Research Areas and Projects

S3F/S3FNet

Science of Security Systems

Looking for strong and self-motivated students to work together!

Smart Grid Security

Software-Defined Networking

More Details: http://cs.iit.edu/~djin/research/index.html

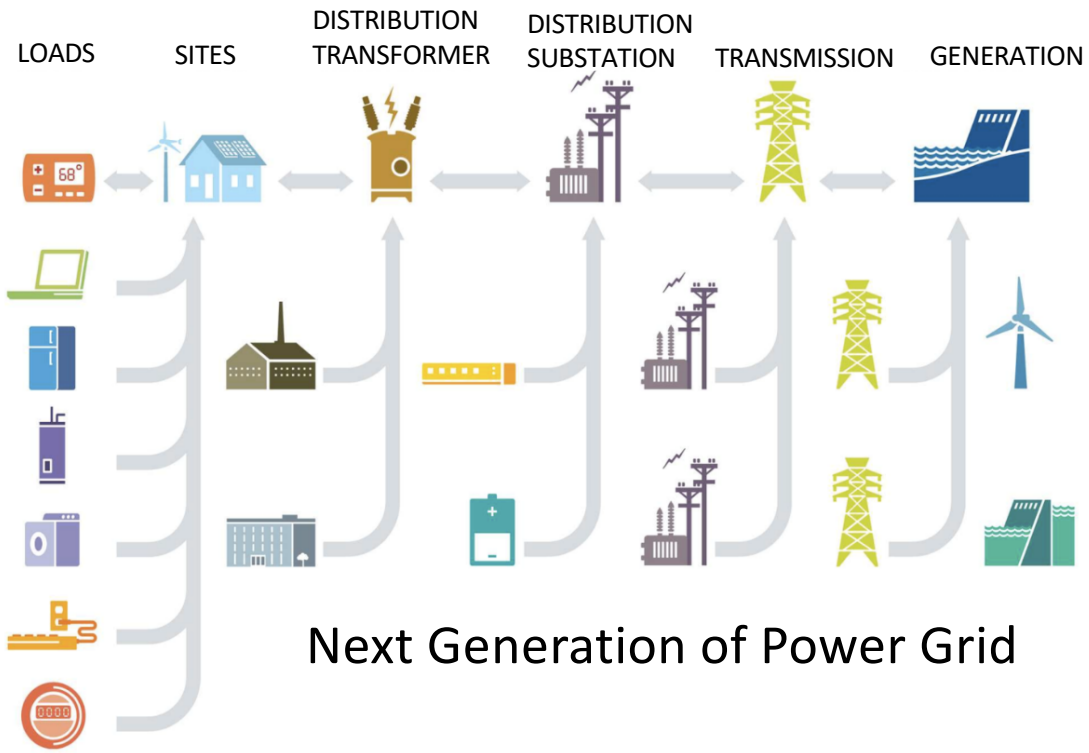
How to Get Involved in Our Research

- For all students, excellent performance in
  - CS 458 Information Security
  - CS 558 Advanced Computer Security (Semester-long project)
  - CSP 544 System and Network Security (Hands-on Labs) – new in Spring 2020
- Master students
  - CS 597 (Research Project), semester-long projects for credits
  - CS 591 (Master thesis), typically two-semester commitment
- Undergraduate students
  - CS 497 (undergraduate research) with me, semester-long projects for credits

More Details: http://cs.iit.edu/~djin/research/opening.html

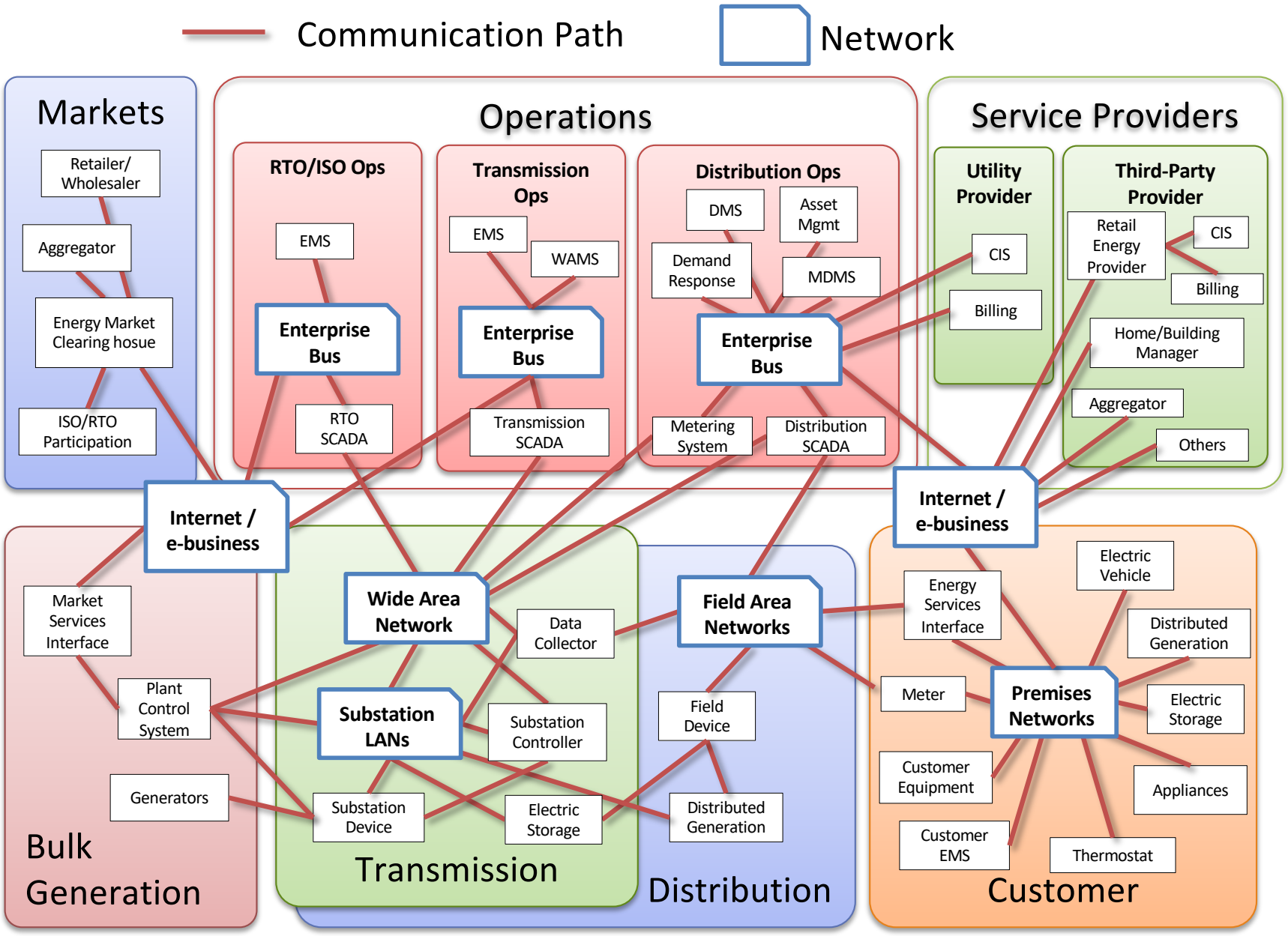
Industrial Control Systems (ICS)

- Control many critical infrastructures
- Modern ICSes increasingly adopt Internet technology to boost control efficiency



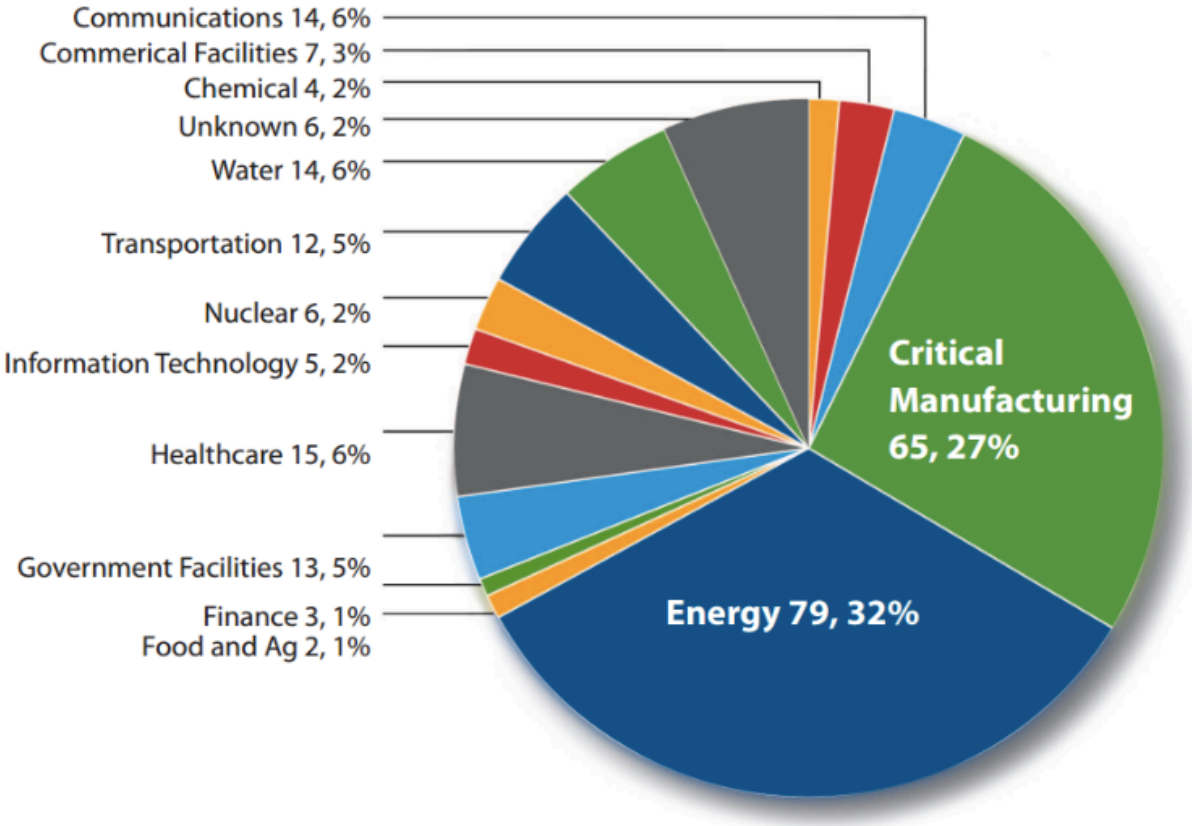
Next Generation of Power Grid

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

- 230,000 residents in western Ukraine
- 6 hours, 73 MW power lost in Dec 2015

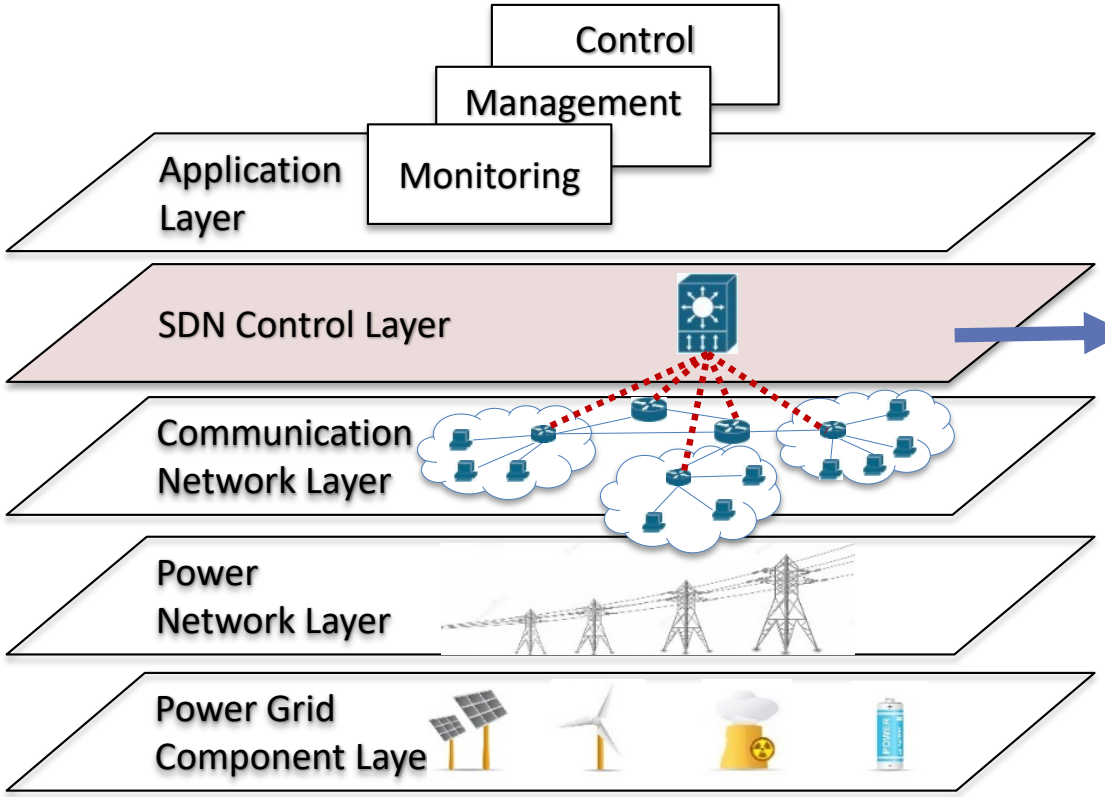
Picture source: 1. National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT Monitor Sep 2014 – Feb 2015
2. http://dailysignal.com/2016/01/13/ukraine-goes-dark-russia-attributed-hackers-take-down-power-grid/

ILLINOIS INSTITUTE OF TECHNOLOGY

Protection of Industrial Control Systems

- Commercial off-the-shelf products
  - e.g., firewalls, anti-virus software
  - fine-grained protection at single device only
- How to check system-wide requirements?
  - Security (e.g., access control)
  - Performance (e.g., end-to-end delay)
- How to safely incorporate existing networking technologies into control systems?
  - Real time operations
  - Large-scale networks
  - Lack of real testbed (unlike Internet)

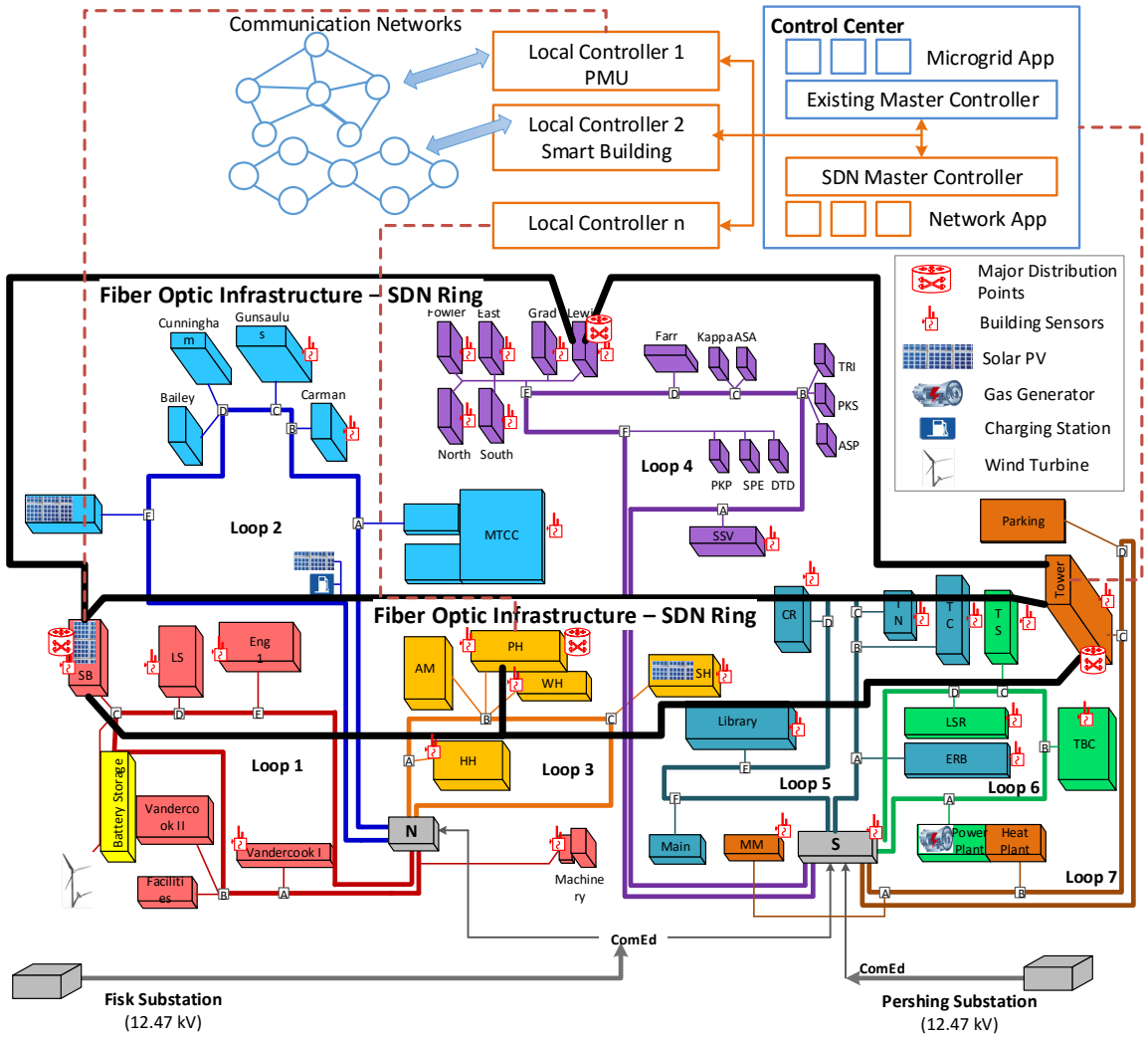
Our Work: Enable a Secure and Resilient ICS in Microgrid with SDN



Contribution I
A novel SDN architecture in microgrid

ICS – industrial control system
SDN – software-defined networking

Transition to an SDN-Enabled Microgrid

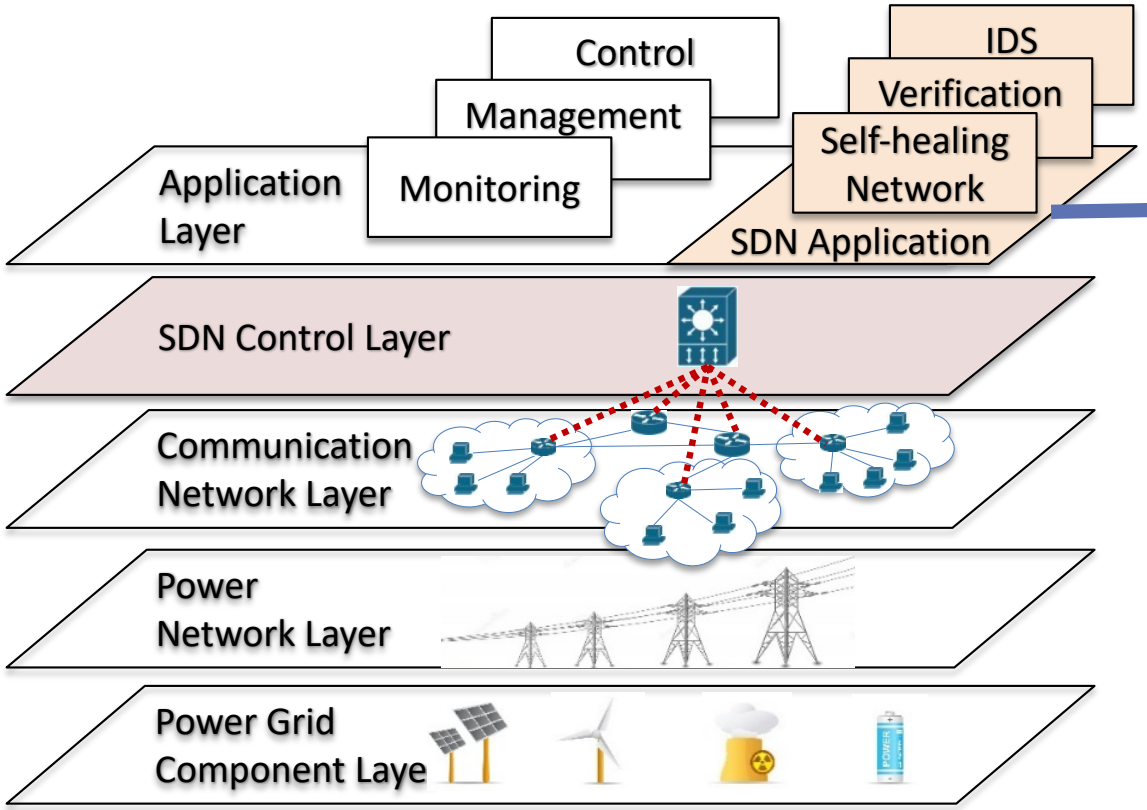


- Facility
  - DOE-funded IIT Microgrid
  - First Cluster of Microgrids in US
  - SDN deployment
- Big data available
  - Processing
  - Storage
  - Analytics

Simulation Testbed -> Living Lab

In-house research idea -> Real system deployment

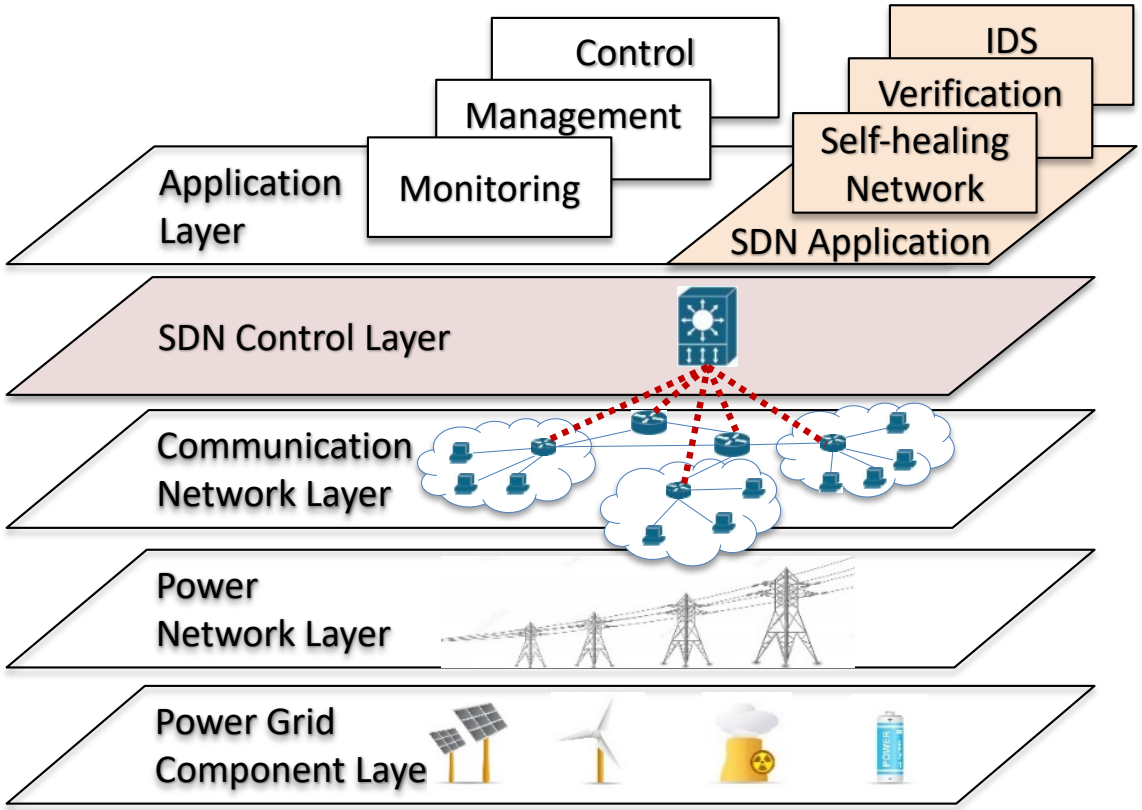
Our Work: Enable a Secure and Resilient ICS in Microgrid with SDN



Contribution II
Innovative SDN-based security applications

ICS – industrial control system
SDN – software-defined networking

Our Work: Enable a Secure and Resilient ICS in Microgrid with SDN



Contribution III
SDN-enabled microgrid testbed

- Parallel Simulation (scalability)
- Virtual-Machine-based Emulation (fidelity)

ICS – industrial control system
SDN – software-defined networking

Outline

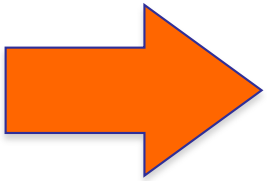
- SDN Background
- Applications
  - Network Verification[1]
  - Self-healing PMU system [2]
- Testing and Evaluation Platform[3]

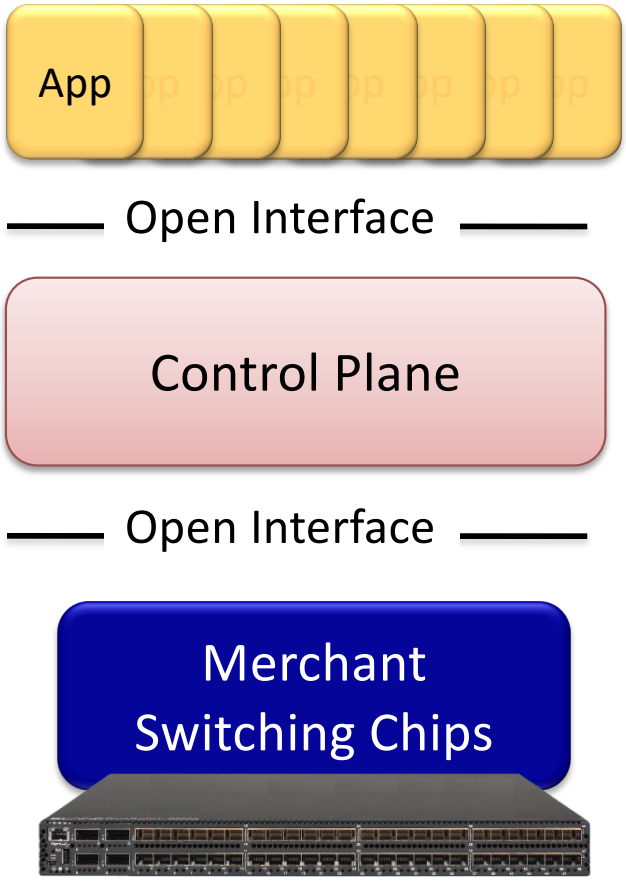
[1] Wenxuan Zhou, Dong Jin, Jason Croft, Matthew Caesar, and Brighten Godfrey. "*Enforcing Customizable Consistency Properties in Software-Defined Networks.*" **USENIX NSDI**

[2] Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour and Cheol Won Lee. *"Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking."* **IEEE Transactions on Smart Grid**

[3] Christopher Hannon, Jiaqi Yan and Dong Jin. *"DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation."* **ACM SIGSIM-PADS (Best Paper Finalist)**

SDN Background





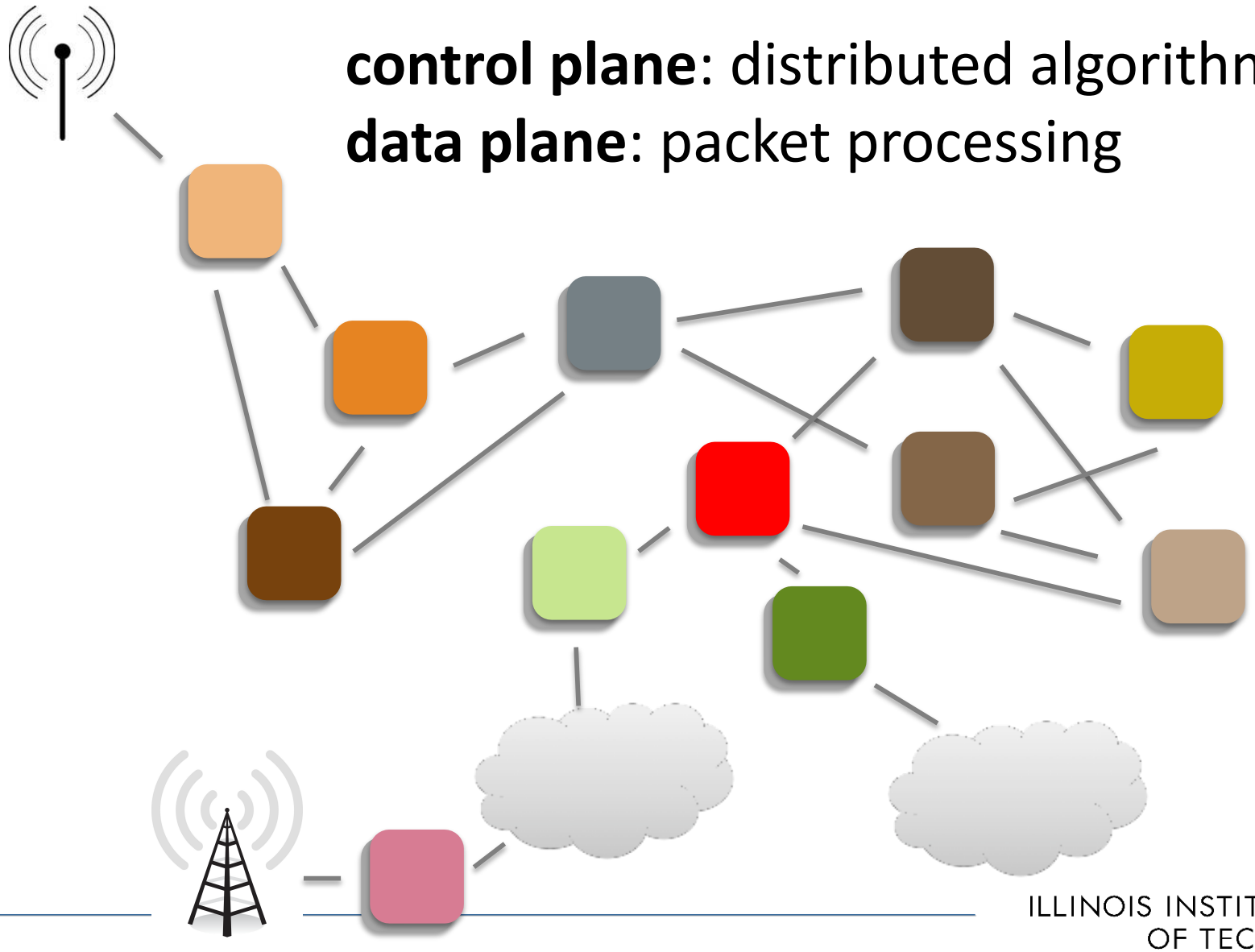
Closed, proprietary
Slow innovation

Open interfaces
Rapid innovation

Picture Source: Nick McKeown, Open Networking Summit 2012

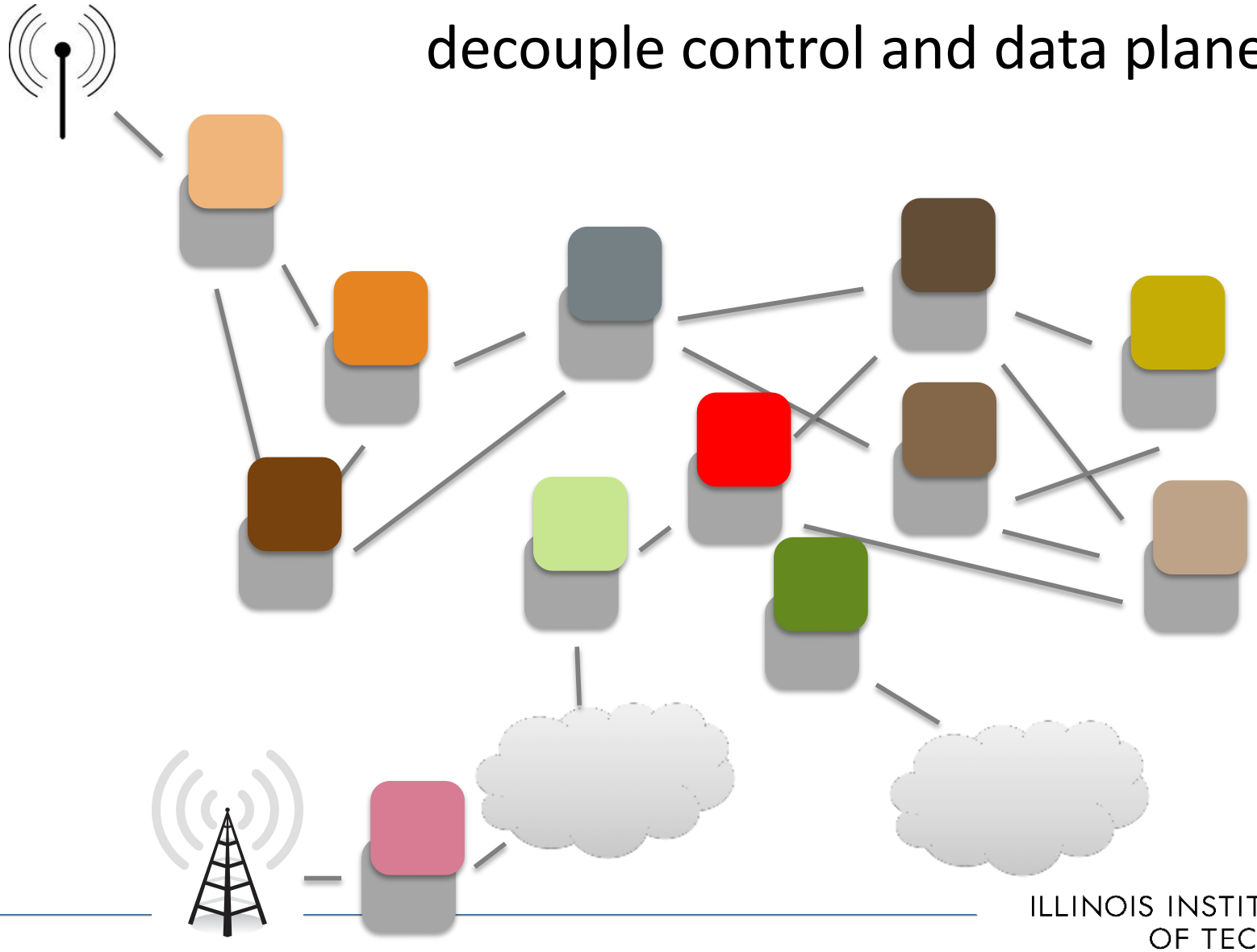
Software Defined Networks

control plane: distributed algorithms
data plane: packet processing



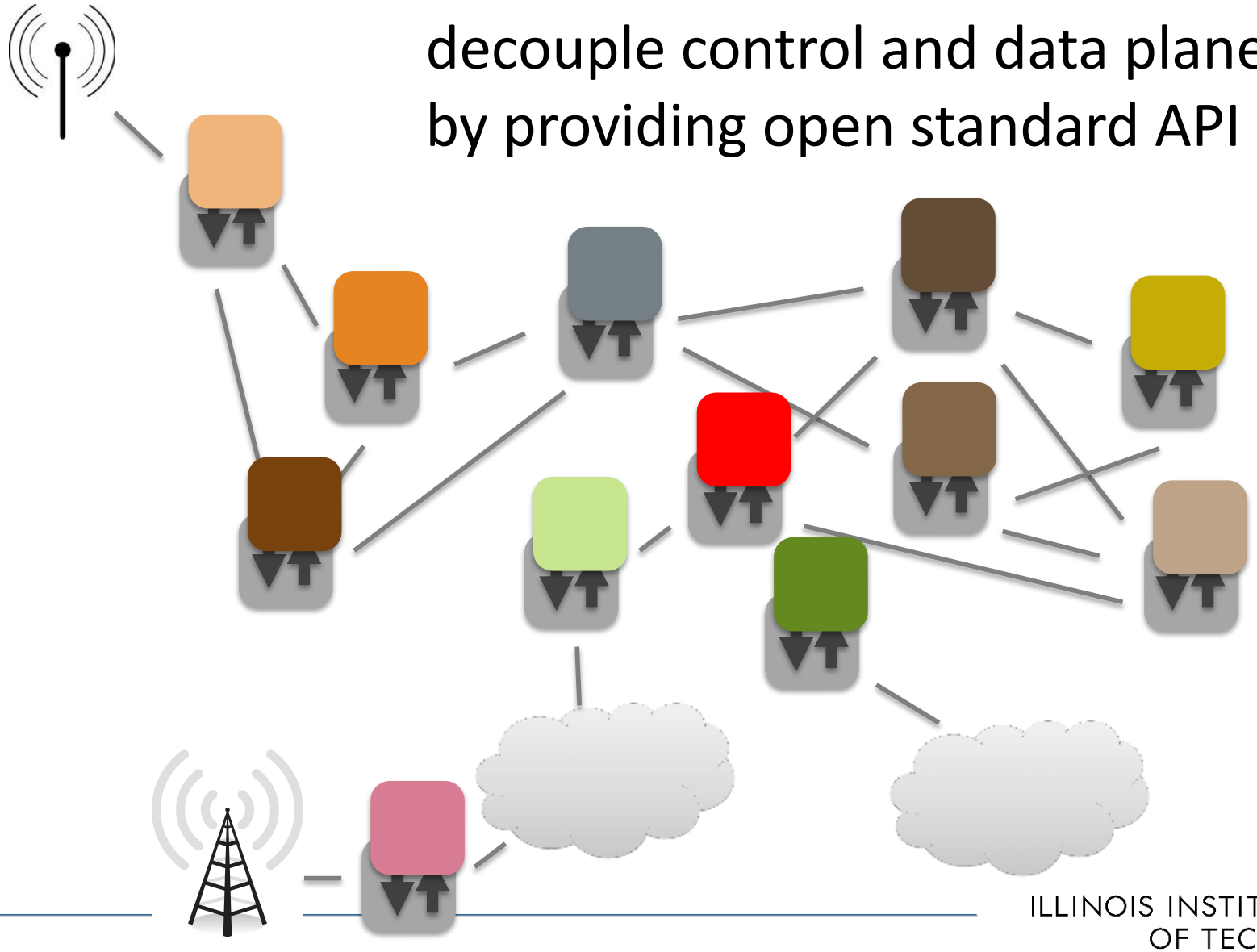
Software Defined Networks

decouple control and data planes

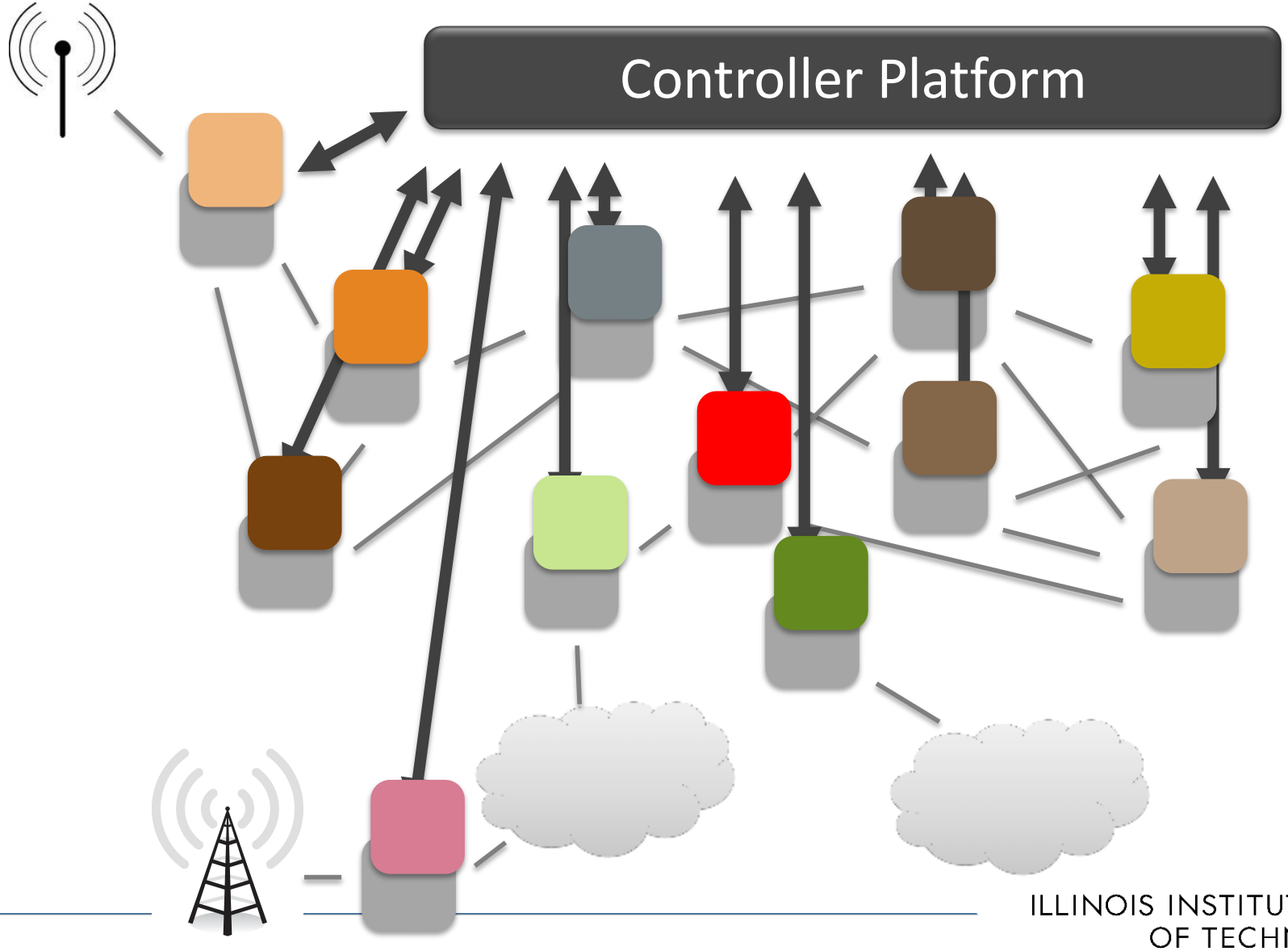


Software Defined Networks

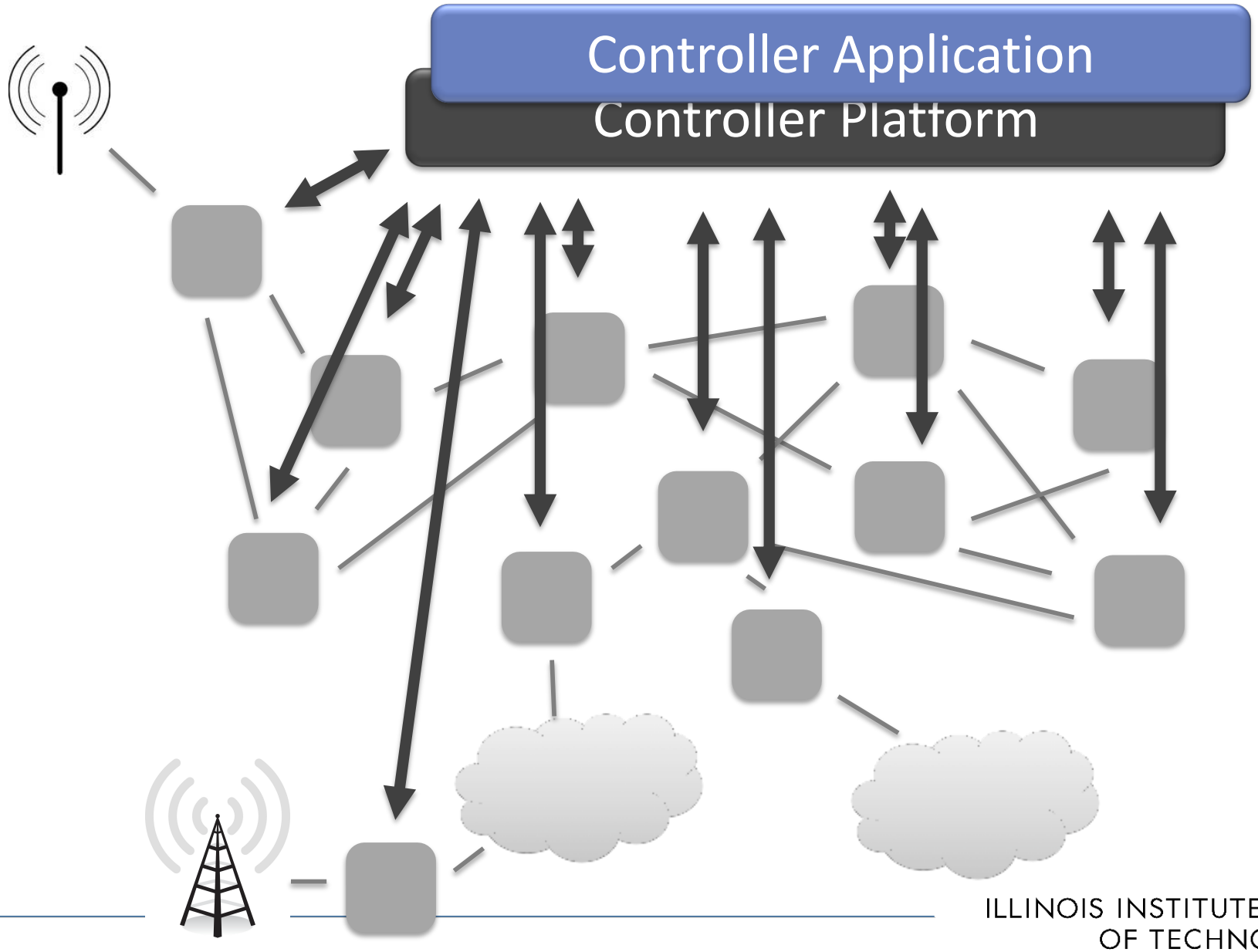
decouple control and data planes
by providing open standard API



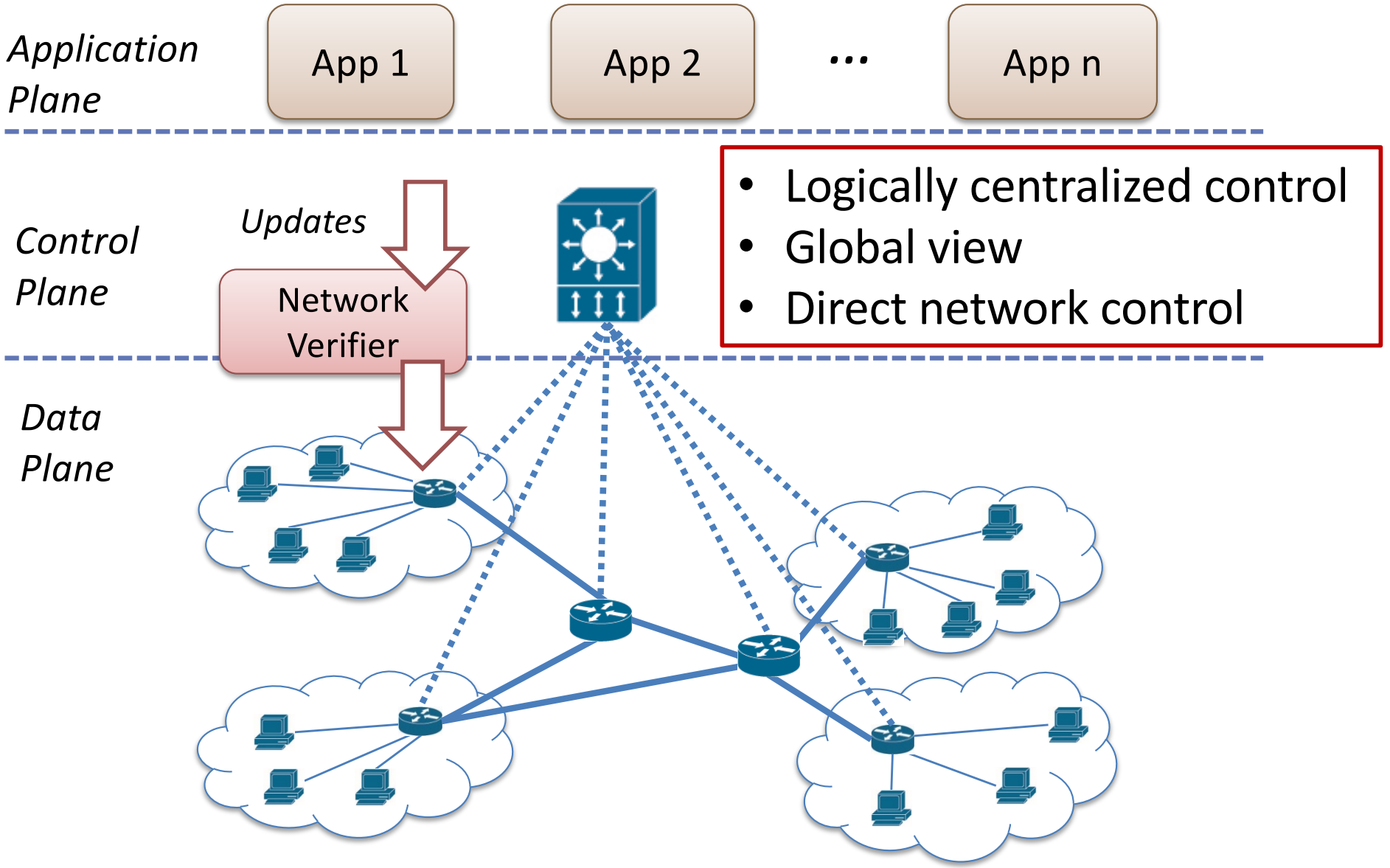
(Logically) Centralized Controller



Protocols ➔ Applications



SDN Architecture



Outline

- SDN Background
- Applications
  - Network Verification[1]
  - Self-healing PMU system [2]
- Testing and Evaluation Platform[3]

[1] Wenxuan Zhou, Dong Jin, Jason Croft, Matthew Caesar, and Brighten Godfrey. "*Enforcing Customizable Consistency Properties in Software-Defined Networks.*" **USENIX NSDI**

[2] Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour and Cheol Won Lee. *"Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking."* **IEEE Transactions on Smart Grid**

[3] Christopher Hannon, Jiaqi Yan and Dong Jin. *"DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation."* **ACM SIGSIM-PADS (Best Paper Finalist)**

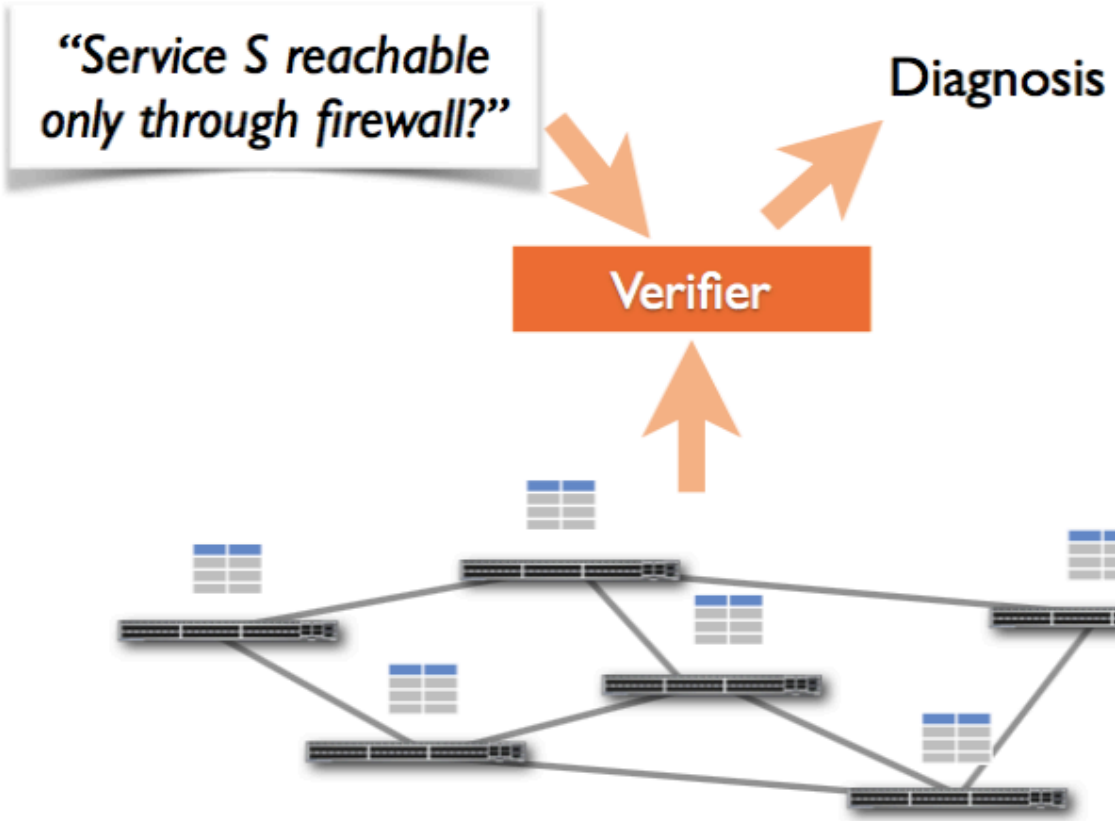
Network Verification - Motivation

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

82%
concerned that changes would cause problems with existing functionality

Survey of network operators: [Kim, Reich, Gupta, Shahbaz, Feamster, Clark, USENIX NSDI 2015]

Network Verification



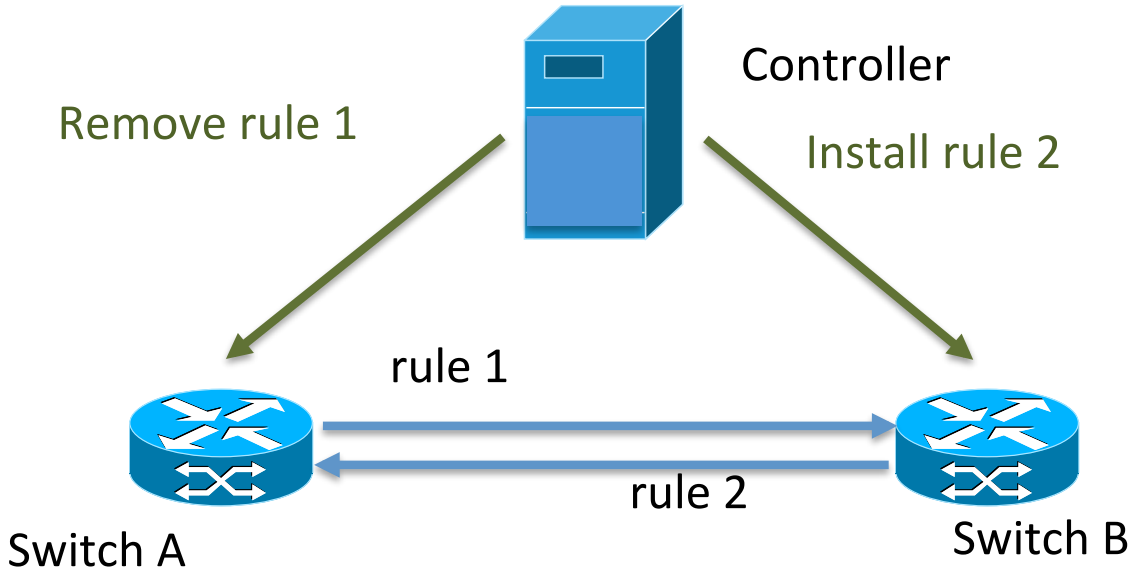
Prior Work

- Static network snapshot analysis
  - Klee [2008]
  - Anteater [2011]
- Dynamic verification
  - FlowChecker [2011]
  - VeriFlow [2012]
  - HSA [2012]
  - Sphinx [2015]

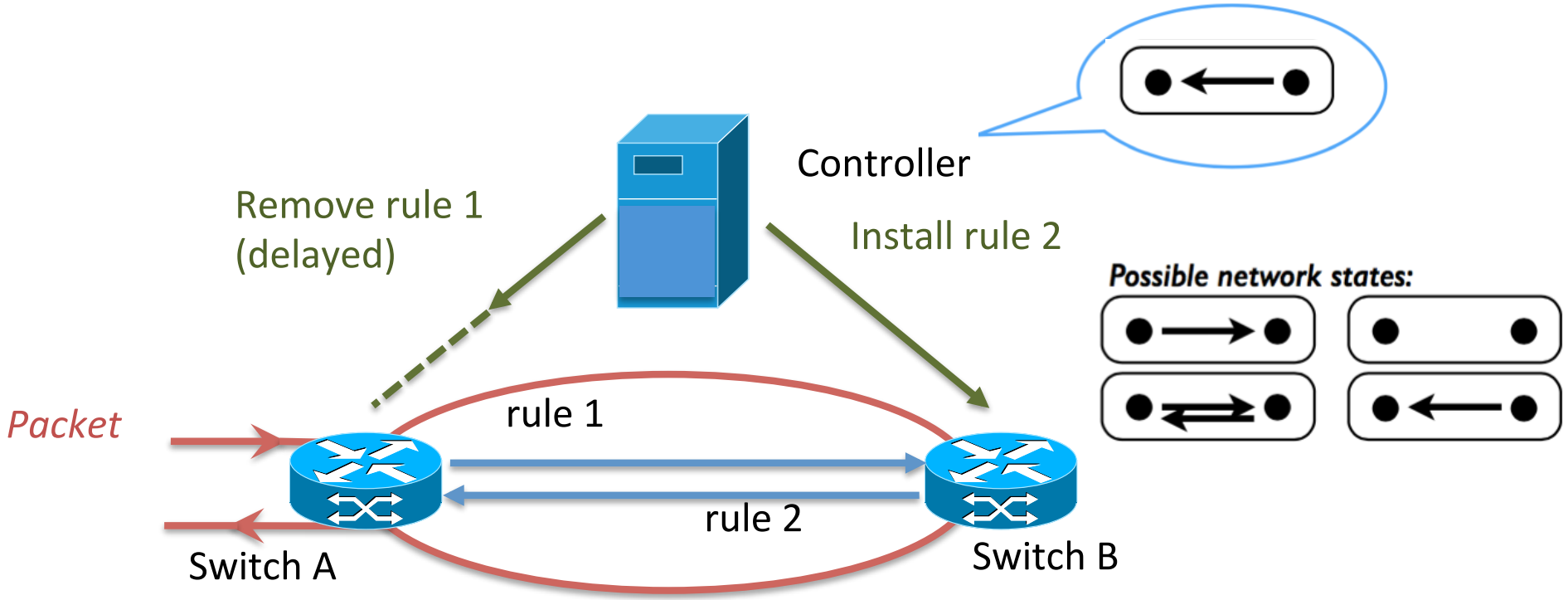
Challenge: Timing Uncertainty

Old config: A => B (rule 1)

New config: B => A (rule 2)



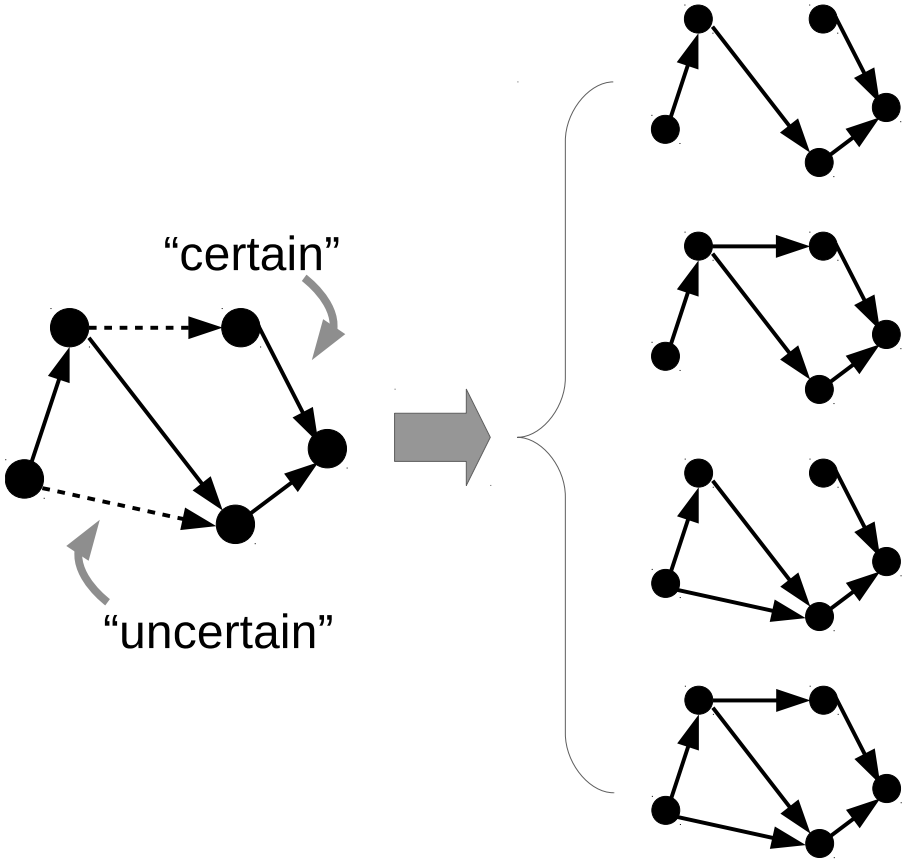
Challenge: Timing Uncertainty



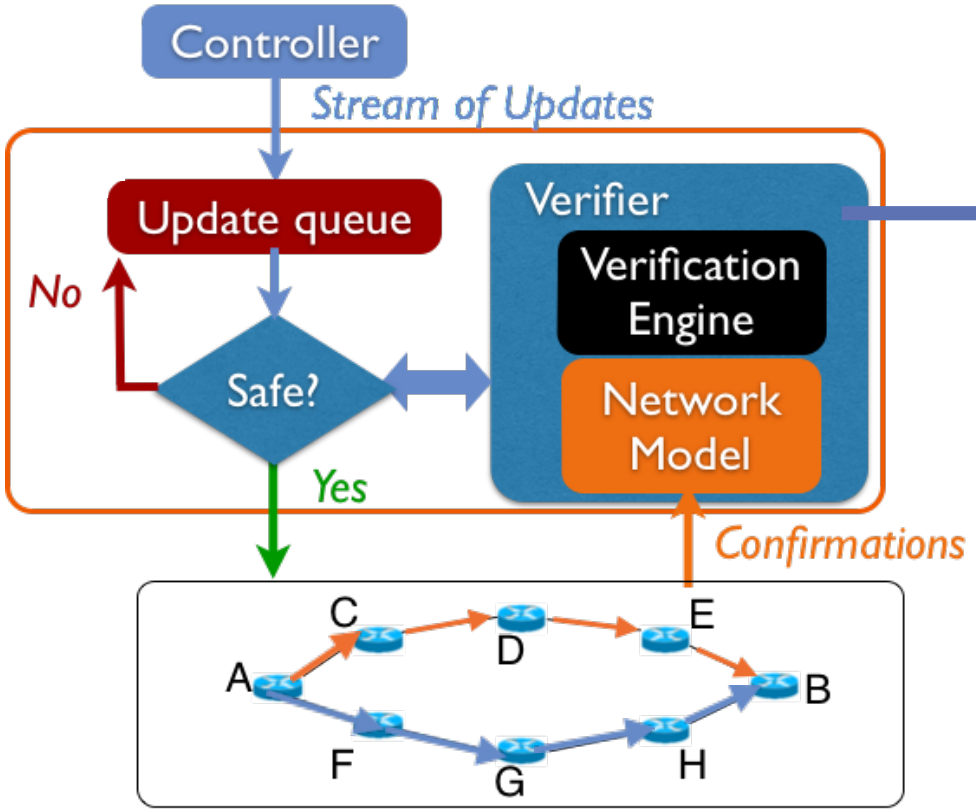
Loop-freedom Violation

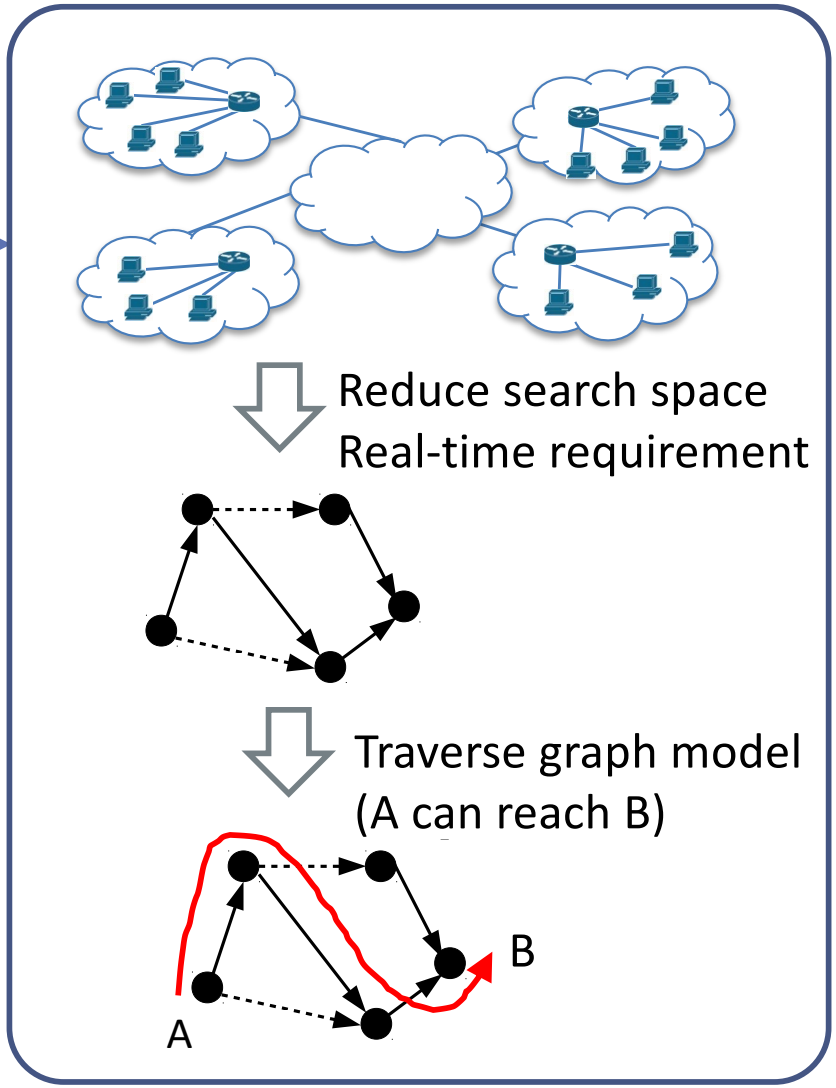
Uncertainty-aware Modeling

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

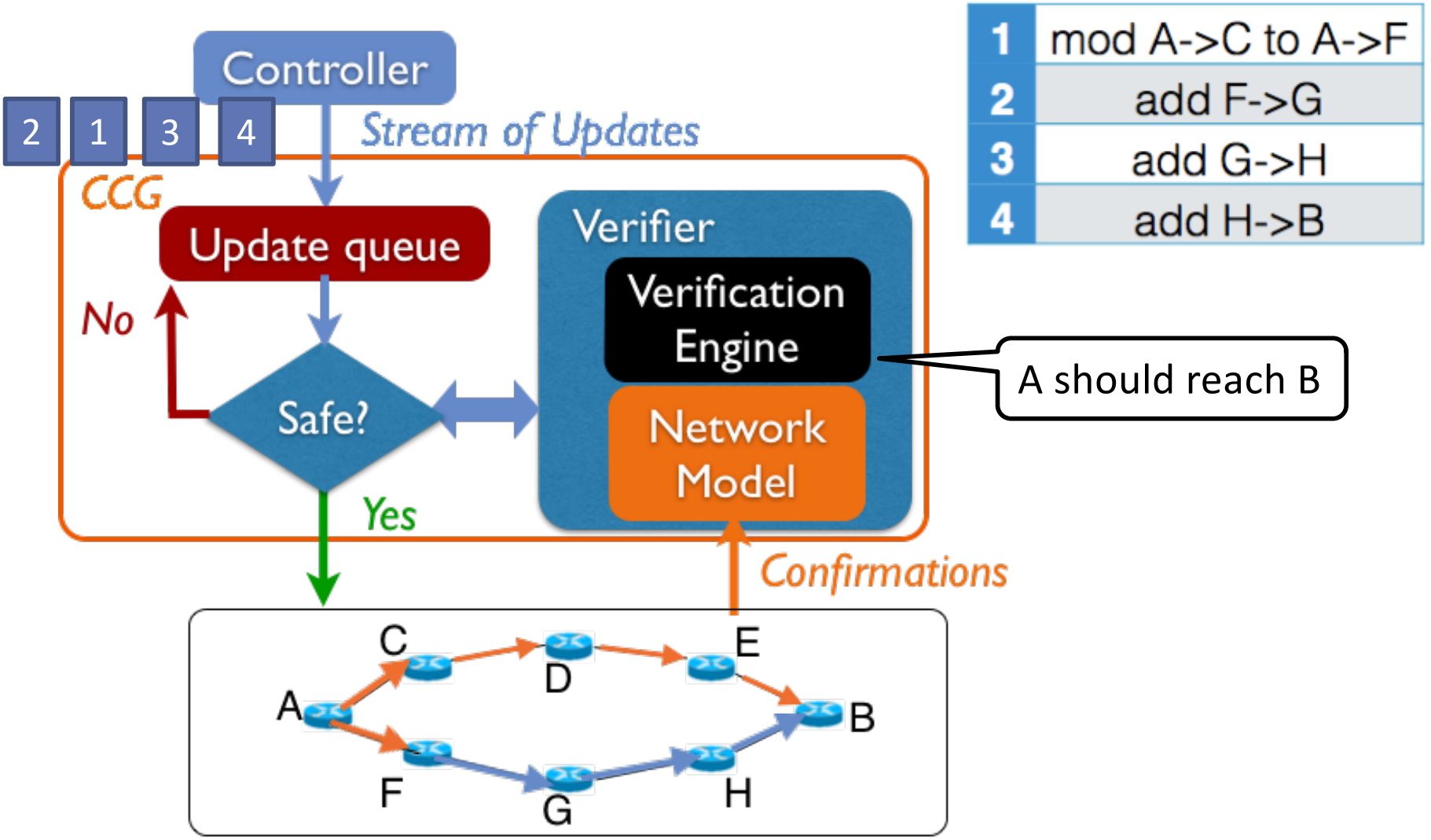


SDN-based Verification System





SDN-based Verification System



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

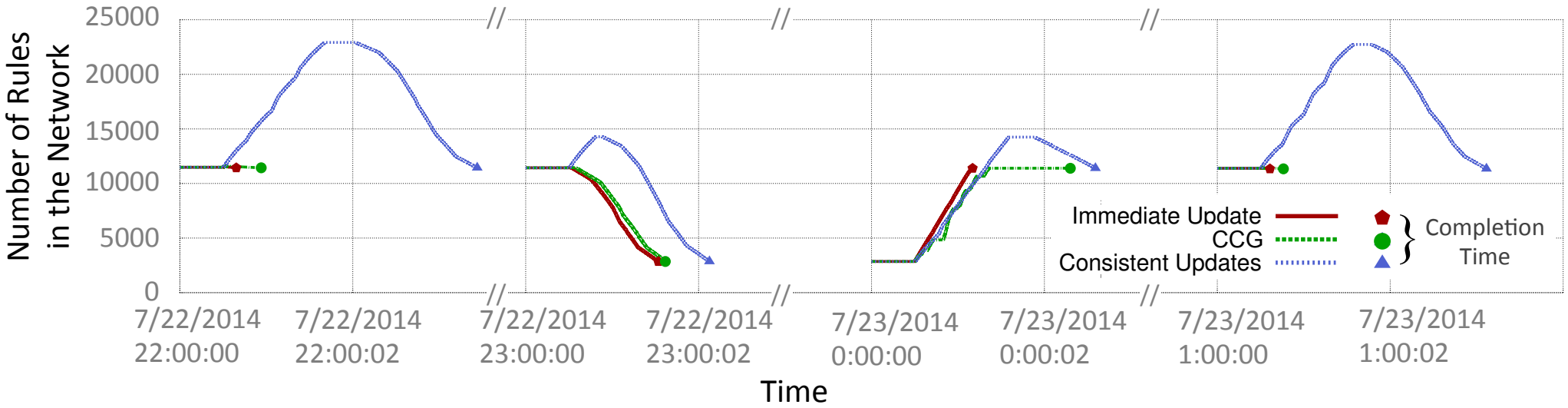
Enforcing dynamic correctness with heuristically maximized parallelism

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?



Outline

- SDN Background
- Applications
  - Network Verification[1]
  - Self-healing PMU system [2]
- Testing and Evaluation Platform[3]

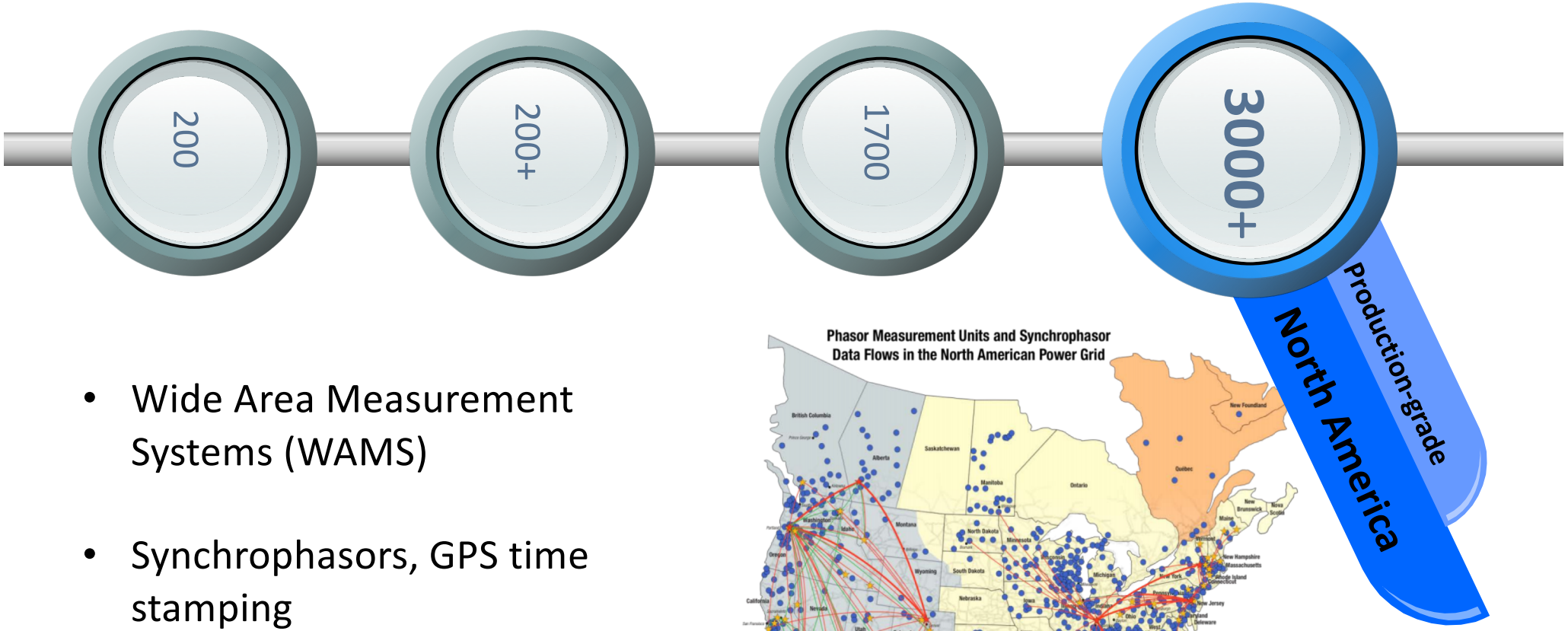
[1] Wenxuan Zhou, Dong Jin, Jason Croft, Matthew Caesar, and Brighten Godfrey. *"Enforcing Customizable Consistency Properties in Software-Defined Networks."* **USENIX NSDI**

[2] Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour and Cheol Won Lee. *"Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking."* **IEEE Transactions on Smart Grid**

[3] Christopher Hannon, Jiaqi Yan and Dong Jin. *"DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation."* **ACM SIGSIM-PADS (Best Paper Finalist)**

Self-healing PMU Network

2007 → 2009 → 2014 → By **2019**



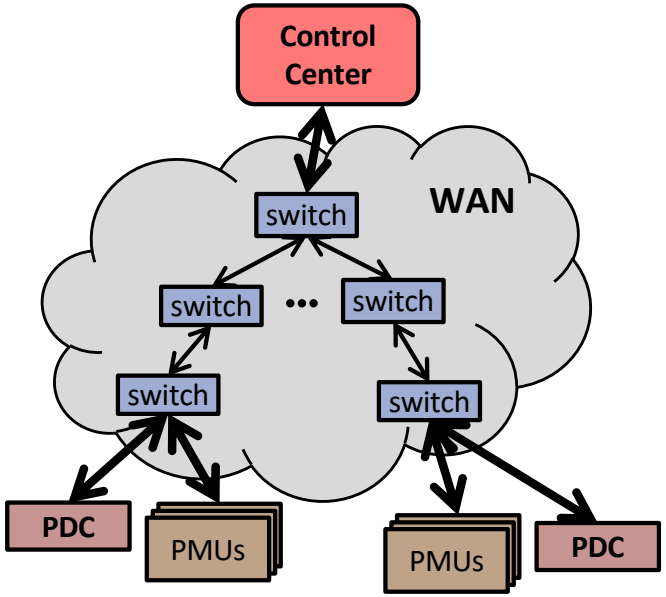
- Wide Area Measurement Systems (WAMS)
- Synchrophasors, GPS time stamping

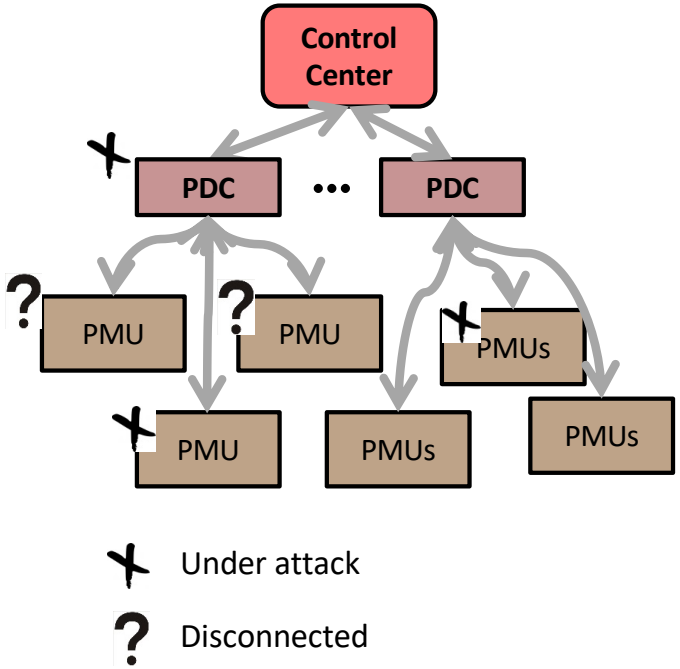
PMUphasor measurement unit

Source: https://www.naspi.org/sites

Challenges

- High volume of measurement data
- Network architecture – no standard yet
- Cyber-attacks and human errors
  - e.g., denial-of-service, man-in-the-middle attacks [1][2]





PMU phasor measurement unit
PDC phasor data concentrator

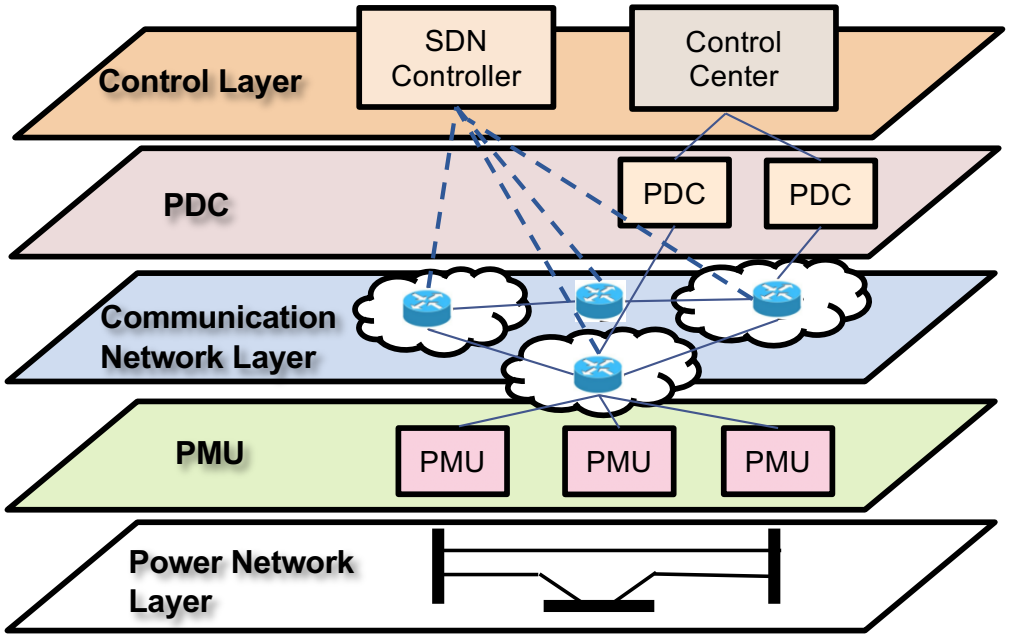
- Lose system observability
- Affect state estimation

[1] C. Beasley, G. K. Venayagamoorthy, and R. Brooks. Cyber security evaluation of synchrophasors in a power system.
[2] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, R. King, M. Freund, and V. Madani. Cybersecurity risk testing of substation phasor measurement units and phasor data concentrators.

Self-healing PMU network

- Objectives
  - Recover power system observability
  - Isolate compromised devices; re-connect uncompromised devices
  - Fast recovery speed
  - Easy and inexpensive deployment
- Contributions
  - An SDN-based architecture
  - Global-optimized self-healing solution
  - A working prototype system with good system performance

Self-healing PMU network



Self-healing PMU Infrastructure

```
vagrant@jessie: ~/yfq
File  Edit  View  Search  Terminal  Help
vagrant@jessie:~/yfq$ sudo python ieee30bus.py

*** Adding Routers:
R1 R2 R6 R9 R10 R12 R15 R18 R25 R27 R100

*** Adding FibbingControllers:
c1
*** Creating network
*** Adding hosts:
D1 D2 D3 D4 D5 D6 D7 D8 D9 D10 u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16 u17 u18 u19 u20 u21 u22 u25
u26 u27 u28 u29 u30
*** Adding switches:

*** Adding links:
(1.00Mbit) (1.00Mbit) (D1, R6) (1.00Mbit) (1.00Mbit) (D2, R12) (1.00Mbit) (1.00Mbit) (D3, R10) (1.00Mbit) (1.00Mbi
t) (D4, R25) (1.00Mbit) (1.00Mbit) (D4, R25) (1.00Mbit) (1.00Mbit) (D5, R1) (1.00Mbit) (1.00Mbit) (D6, R15) (1.00M
bit) (1.00Mbit) (D7, R27) (1.00Mbit) (1.00Mbit) (D8, R2) (1.00Mbit) (1.00Mbit) (D9, R9) (1.00Mbit) (1.00Mbit) (D10
, R18) (1.00Mbit) (1.00Mbit) (R1, R15) (1.00Mbit) (1.00Mbit) (R1, R100) (1.00Mbit) (1.00Mbit) (R2, R9) (1.00Mbit)
(1.00Mbit) (R2, R100) (1.00Mbit) (1.00Mbit) (R6, R12) (1.00Mbit) (1.00Mbit) (R6, R100) (1.00Mbit) (1.00Mbit) (R9,
R18) (1.00Mbit) (1.00Mbit) (R9, R100) (1.00Mbit) (1.00Mbit) (R10, R25) (1.00Mbit) (1.00Mbit) (R10, R100) (1.00Mbit
) (1.00Mbit) (R12, R10) (1.00Mbit) (1.00Mbit) (R12, R100) (1.00Mbit) (1.00Mbit) (R15, R27) (1.00Mbit) (1.00Mbit) (
R15, R100) (1.00Mbit) (1.00Mbit) (R18, R6) (1.00Mbit) (1.00Mbit) (R18, R100) (1.00Mbit) (1.00Mbit) (R25, R1) (1.00
Mbit) (1.00Mbit) (R25, R100) (1.00Mbit) (1.00Mbit) (R27, R2) (1.00Mbit) (1.00Mbit) (R27, R100) (1.00Mbit) (1.00Mbi
t) (c1, R18) (1.00Mbit) (1.00Mbit) (u1, R1) (1.00Mbit) (1.00Mbit) (u2, R6) (1.00Mbit) (1.00Mbit) (u3, R1) (1.00Mbi
t) (1.00Mbit) (u4, R12) (1.00Mbit) (1.00Mbit) (u5, R2) (1.00Mbit) (1.00Mbit) (u6, R6) (1.00Mbit) (1.00Mbit) (u7, R
6) (1.00Mbit) (1.00Mbit) (u8, R6) (1.00Mbit) (1.00Mbit) (u9, R9) (1.00Mbit) (1.00Mbit) (u9, R9) (1.00Mbit) (1.00Mb
it) (u10, R6) (1.00Mbit) (1.00Mbit) (u11, R9) (1.00Mbit) (1.00Mbit) (u12, R12) (1.00Mbit) (1.00Mbit) (u13, R12) (1
.00Mbit) (1.00Mbit) (u13, R15) (1.00Mbit) (1.00Mbit) (u13, R15) (1.00Mbit) (1.00Mbit) (u14, R12) (1.00Mbit) (1.00M
bit) (u14, R25) (1.00Mbit) (1.00Mbit) (u15, R15) (1.00Mbit) (1.00Mbit) (u16, R12) (1.00Mbit) (1.00Mbit) (u17, R10)
 (1.00Mbit) (1.00Mbit) (u18, R15) (1.00Mbit) (1.00Mbit) (u19, R18) (1.00Mbit) (1.00Mbit) (u20, R10) (1.00Mbit) (1.
00Mbit) (u21, R10) (1.00Mbit) (1.00Mbit) (u22, R10) (1.00Mbit) (1.00Mbit) (u25, R27) (1.00Mbit) (1.00Mbit) (u26, R
25) (1.00Mbit) (1.00Mbit) (u27, R27) (1.00Mbit) (1.00Mbit) (u28, R6) (1.00Mbit) (1.00Mbit) (u29, R27) (1.00Mbit) (
1.00Mbit) (u30, R27)
*** Configuring hosts
D1 D2 D3 D4 D5 D6 D7 D8 D9 D10 u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16 u17 u18 u19 u20 u21 u22 u25
u26 u27 u28 u29 u30
*** Found 64 broadcast domains
*** Allocating primary IPs
*** Allocating private router IPs
*** Starting 11 routers
R1 R2 R6 R9 R10 R12 R15 R18 R25 R27 R100
*** Setting default host routes
D1 via R6, D2 via R12, D3 via R10, D4 via R25, D5 via R1, D6 via R15, D7 via R27, D8 via R2, D9 via R9, D10 via R1
8, u1 via R1, u2 via R6, u3 via R1, u4 via R12, u5 via R2, u6 via R6, u7 via R6, u8 via R6, u9 via R9, u10 via R6,
 u11 via R9, u12 via R12, u13 via R15, u14 via R12, u15 via R15, u16 via R12, u17 via R10, u18 via R15, u19 via R1
8, u20 via R10, u21 via R10, u22 via R10, u25 via R27, u26 via R25, u27 via R27, u28 via R6, u29 via R27, u30 via
R27,
*** Starting controller
c1 Starting southbound controller for  c1

*** Starting 0 switches

*** Starting CLI:
mininet>
```

PMU network layer creation

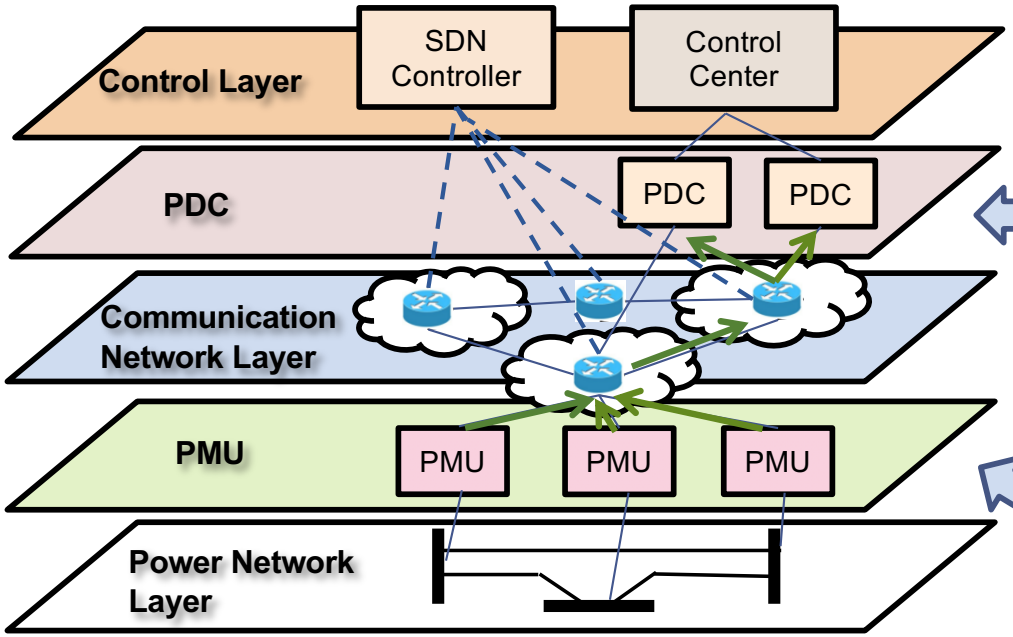
System models

Graph $G_p(B, L_p)$ power transmission network

$G_c(U \cup D \cup R, L_c)$ IP-based PMU network

B - set of buses; L_p - set of transmission lines ; U - set of PMUs
D - set of PDC; R - set of router; L_c - set of links

Self-healing PMU network



PMU Properties	
PMU Server Details	
UDP Port	6000
TCP Port	6001
PMU Configuration Details	
PMU ID	10
Station Name	test
Number of Phasors	3
Number of Analog	0
Digital Status Word	0
Data Rate	30
Format Word	1
Configuration Count	0
CFG Frame Size	114

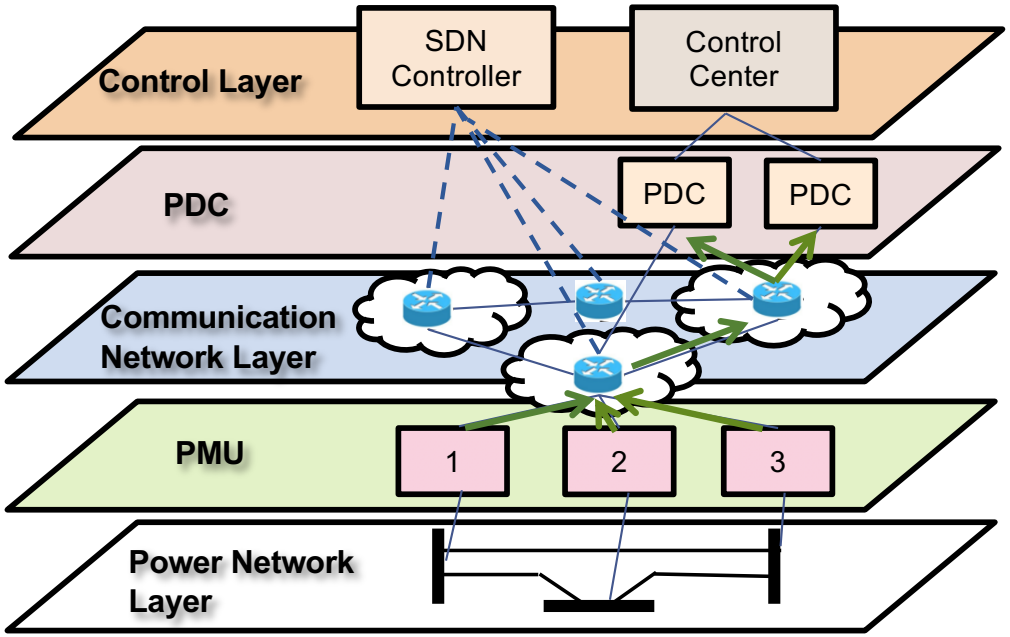
Observability function of bus i $O_i = \sum a_{i,j} p_j$

where $a_{i,j}$ defines the bus connectivity

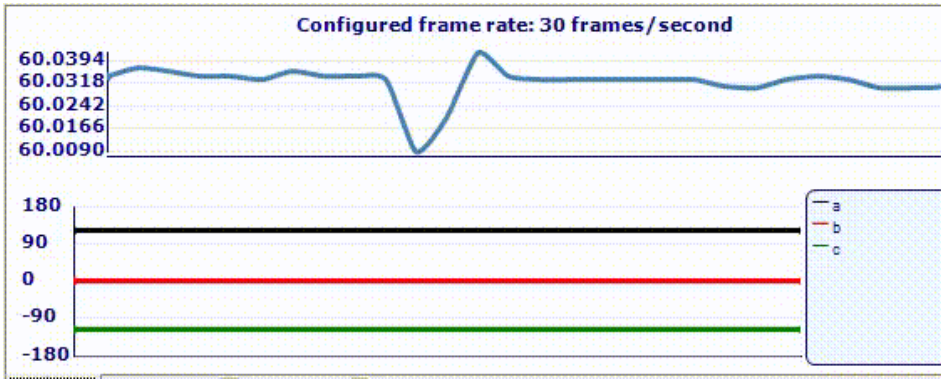
$$a_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 1 & \text{if } i \neq j \text{ and bus } i \text{ and bus } j \text{ are connected} \\ 0 & \text{otherwise} \end{cases}$$

PMU/PDC application layer creation

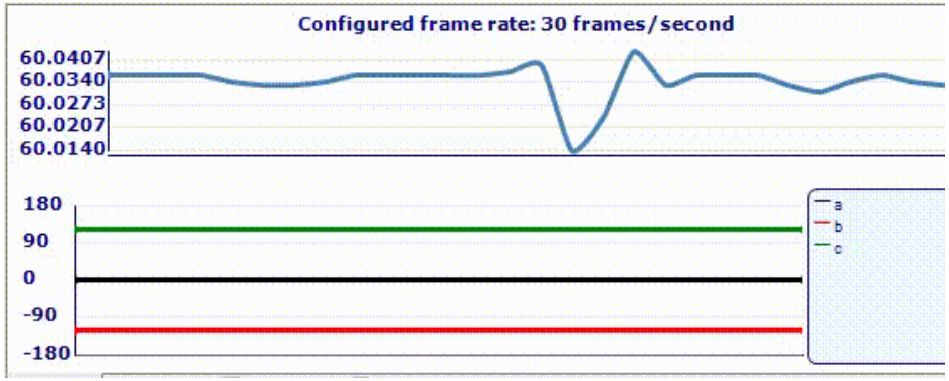
Self-healing PMU network



Control Center Monitoring System

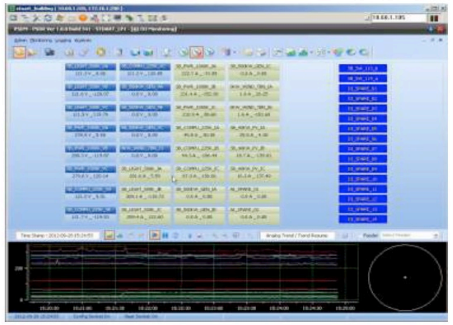


PMU3

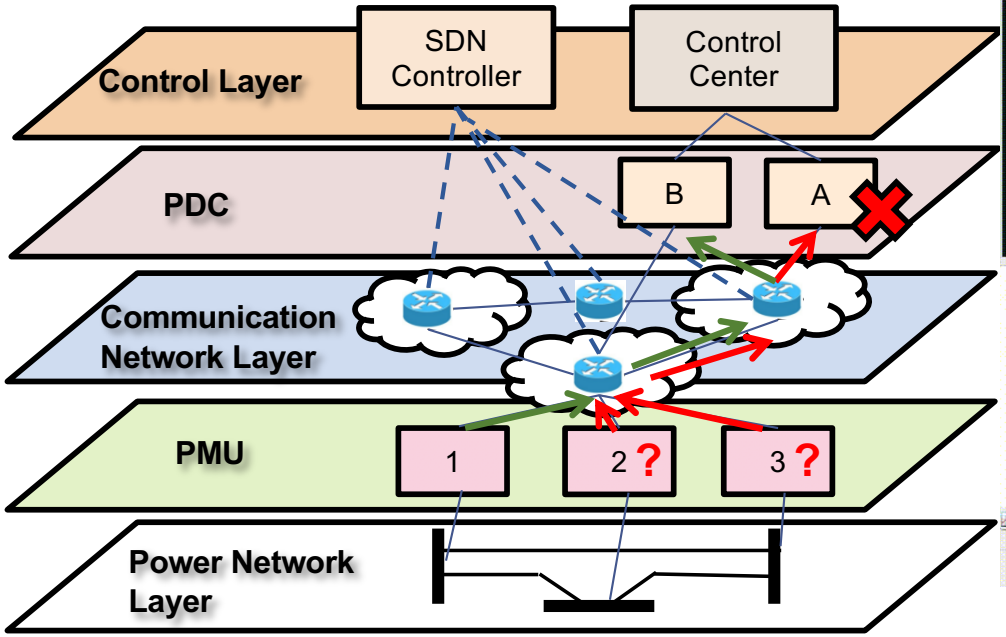


PMU1

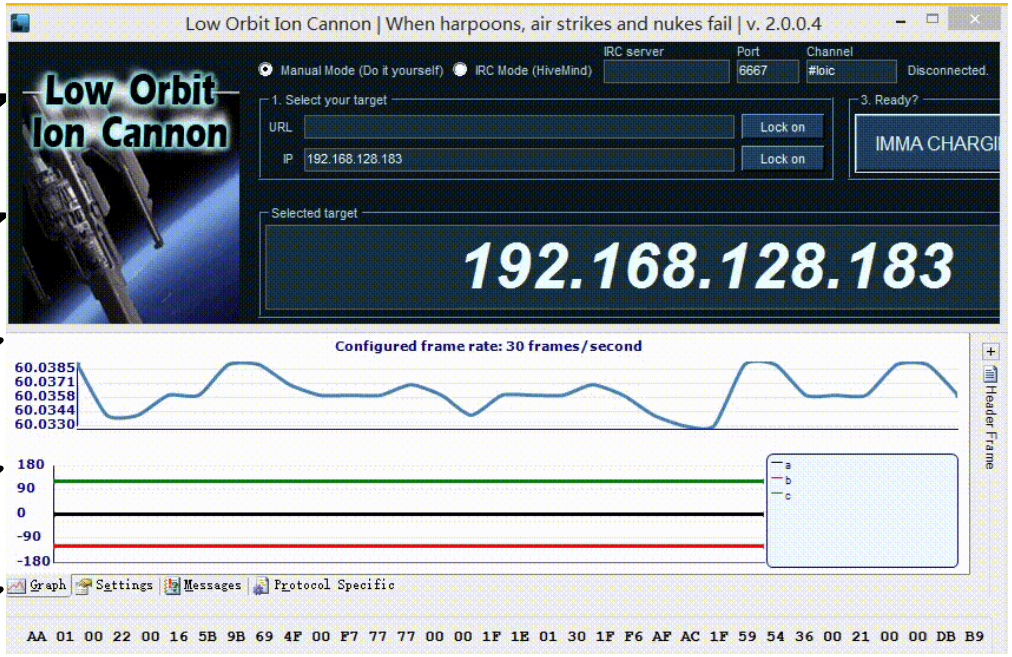
Real Data Collected from IIT Distribution System PMU network



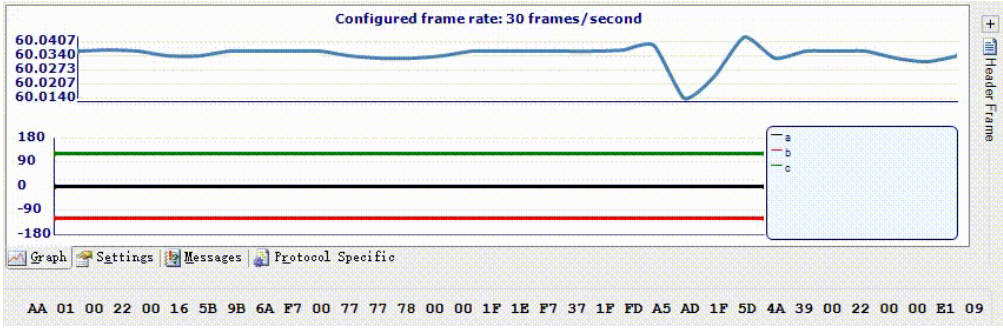
Self-healing PMU network



PDC A stop functioning under a cyber-attack

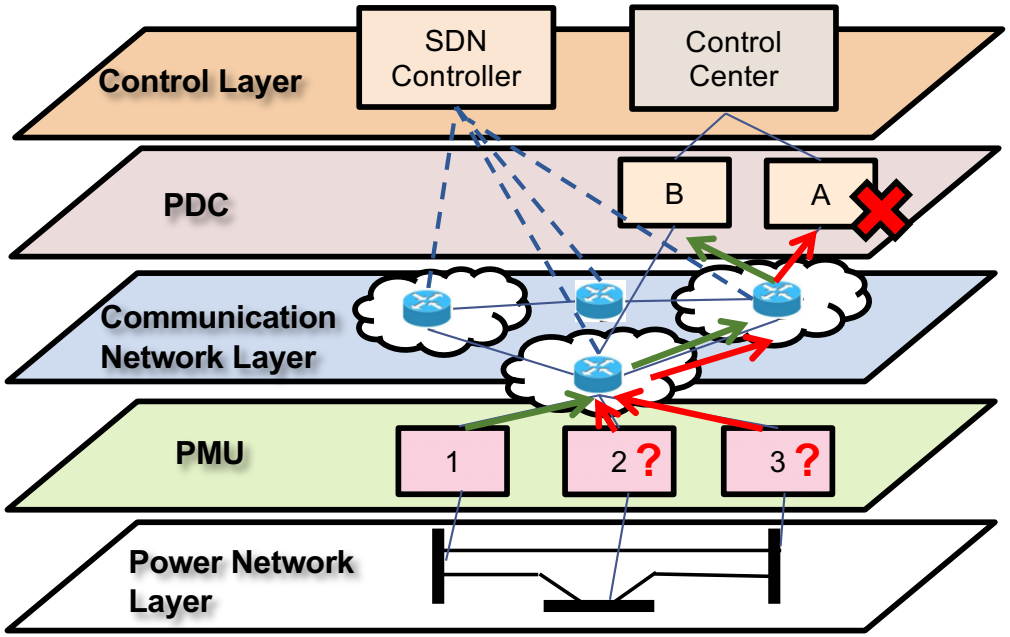


PMU3



PMU1

Self-healing PMU network



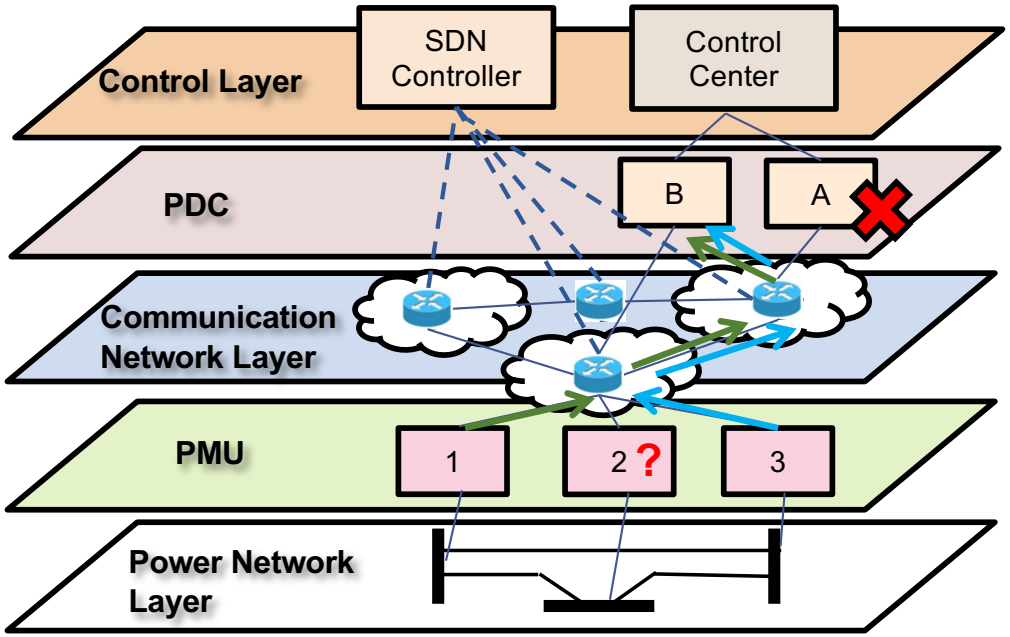
Constraints

- PDC connection space constraints
- Congestion freedom constraints
- Rule capacity constraints

Objective: quickly restore system power observability

Stage I	minimize # of reconnected PMUs
Stage II	minimize # of new rules on SDN switches

Self-healing PMU network



Constraints

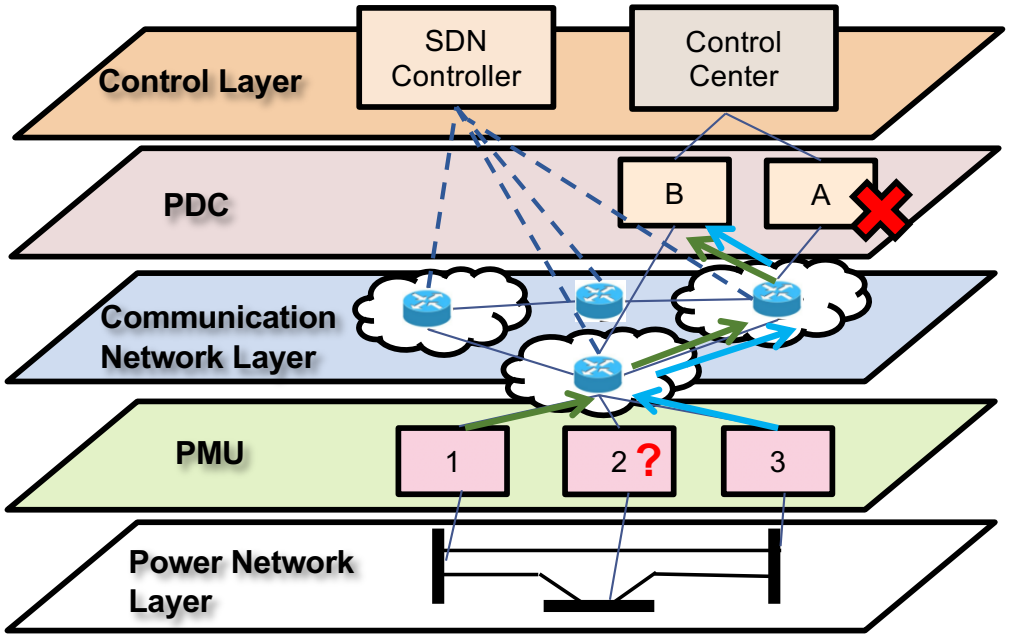
- PDC connection space constraints
- Congestion freedom constraints
- Rule capacity constraints

Objective: quickly restore system power observability

Stage I	minimize # of reconnected PMUs
Stage II	minimize # of new rules on SDN switches

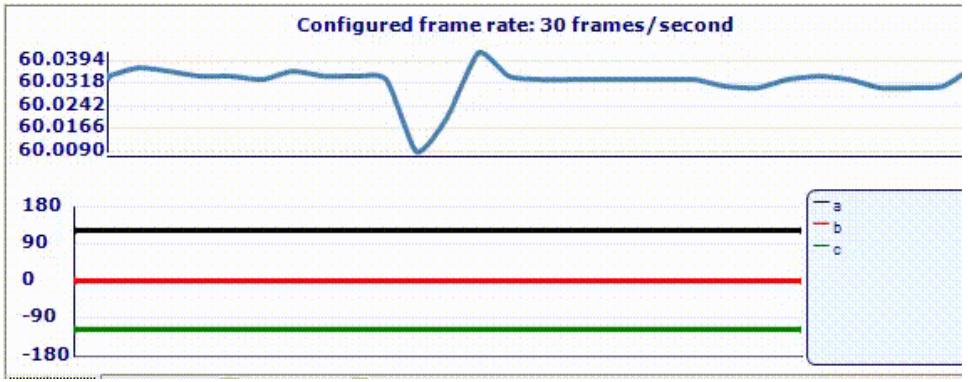
```
----------------Start solving stage 1----------------------
==================== stage 1 solution ======================
=====
[Pair(pmu='u10', pdc='d10'), Pair(pmu='u21', pdc='d5'), Pair(
pmu='u22', pdc='d9')]



----------------Start solving stage 2----------------------
==================== stage 2 solution ======================
=====
{Pair(pmu='u22', pdc='d9'): ['u22', 'r10', 'r12', 'r6', 'r18'
, 'r9', 'd9'], Pair(pmu='u10', pdc='d10'): ['u10', 'r9', 'r18
', 'd10'], Pair(pmu='u21', pdc='d5'): ['u21', 'r10', 'r25', '
r1', 'd5']}



==================== shortest paths ========================
======
{Pair(pmu='u22', pdc='d9'): ['u22', 'r10', 'r12', 'r6', 'r18'
, 'r9', 'd9'], Pair(pmu='u10', pdc='d10'): ['u10', 'r6', 'r18
', 'd10'], Pair(pmu='u21', pdc='d5'): ['u21', 'r10', 'r25', '
r1', 'd5']}
```

Self-healing PMU network

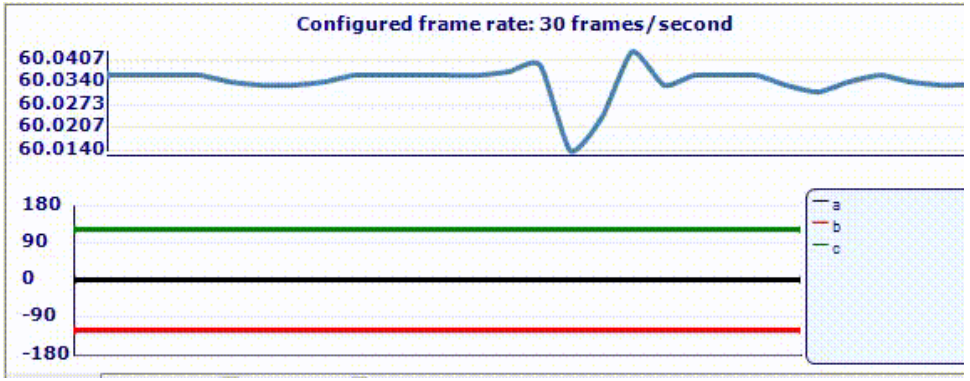


Constraints

- PDC connection space constraints
- Congestion freedom constraints
- Rule capacity constraints



PMU3 - reconnected



PMU1

Objective: quickly restore system power observability

Stage I minimize # of reconnected PMUs

Stage II minimize # of new rules on SDN switches

Outline

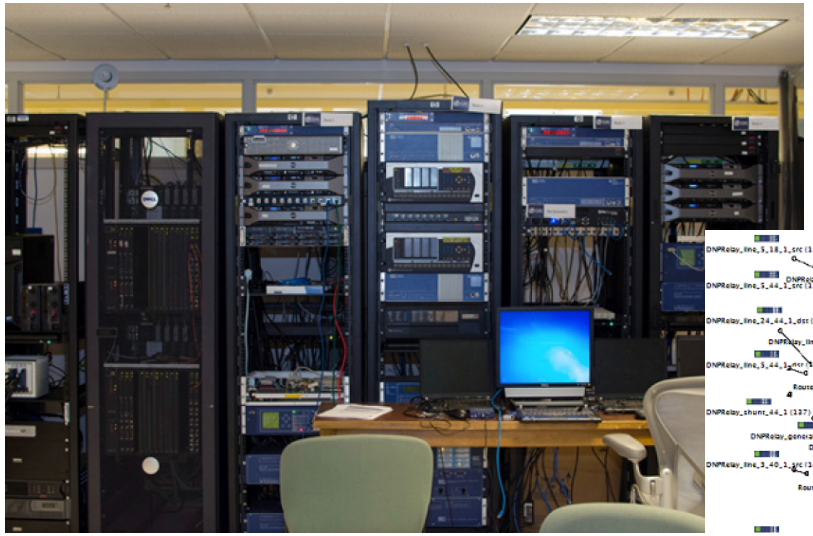
- SDN Background
- Applications
  - Network Verification[1]
  - Self-healing PMU system [2]
- Testing and Evaluation Platform[3]

[1] Wenxuan Zhou, Dong Jin, Jason Croft, Matthew Caesar, and Brighten Godfrey. *"Enforcing Customizable Consistency Properties in Software-Defined Networks."* **USENIX NSDI**

[2] Dong Jin, Zhiyi Li, Christopher Hannon, Chen Chen, Jianhui Wang, Mohammad Shahidehpour and Cheol Won Lee. *"Towards a Cyber Resilient and Secure Microgrid Using Software-Defined Networking."* **IEEE Transactions on Smart Grid**

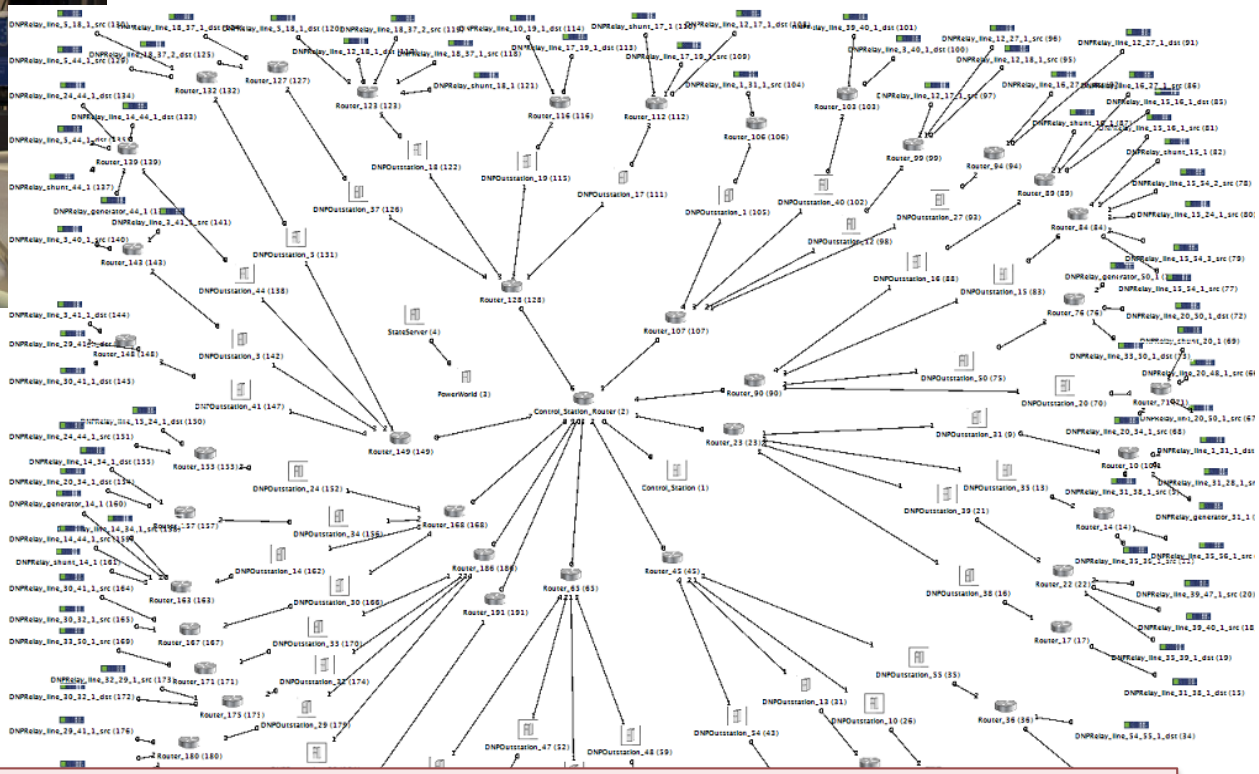
[3] Christopher Hannon, Jiaqi Yan and Dong Jin. *"DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation."* **ACM SIGSIM-PADS (Best Paper Finalist)**

Testbed for Smart Grid Security



Test Systems in Lab

- No interference with real systems
- Realistic settings

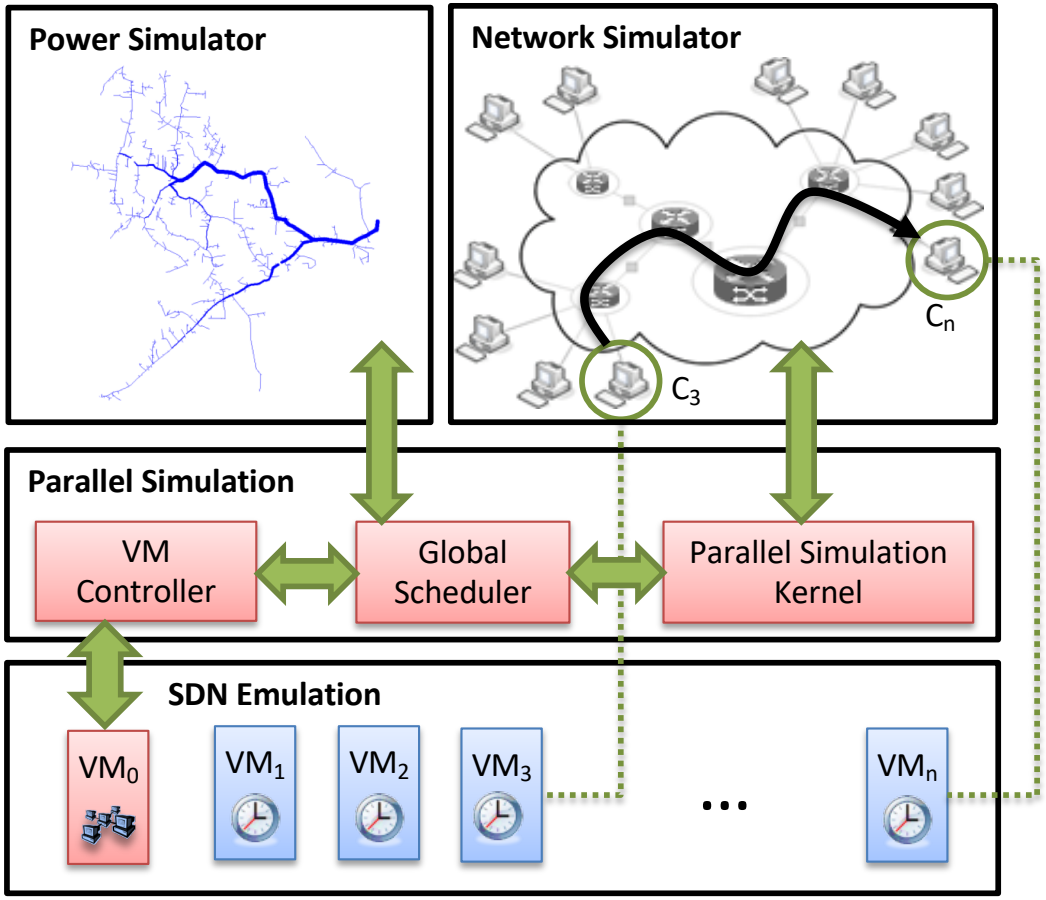


Security Exercise/Evaluation

- Scalable
- Flexible
- Controllable
- Reproducible

A Large-scale, High-fidelity Simulation/Emulation Testbed

Testbed Design



Parallel Simulation/Emulation Testbed

[Best paper award, PADS'12], [Best paper finalist, PADS'16]

- SDN Emulation
  - lightweight virtual machine
  - unmodified code execution
  - virtual time system
- Parallel Simulation Engine
  - 1 million nodes
- Simulation
  - S3FNet: communication network
  - OpenDSS: power distribution system
- Using by
  - IBM Research
  - Boeing
  - Argonne National Lab

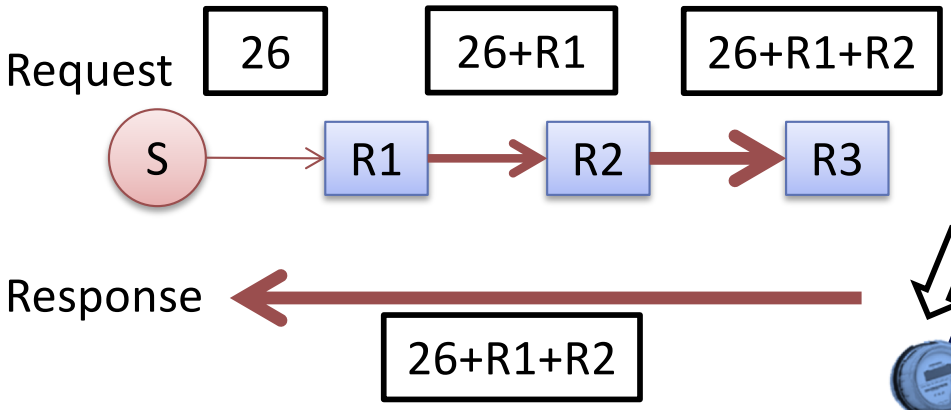
Cyber-security Evaluation

Extensively utilize the testbed to evaluate cyber-attacks

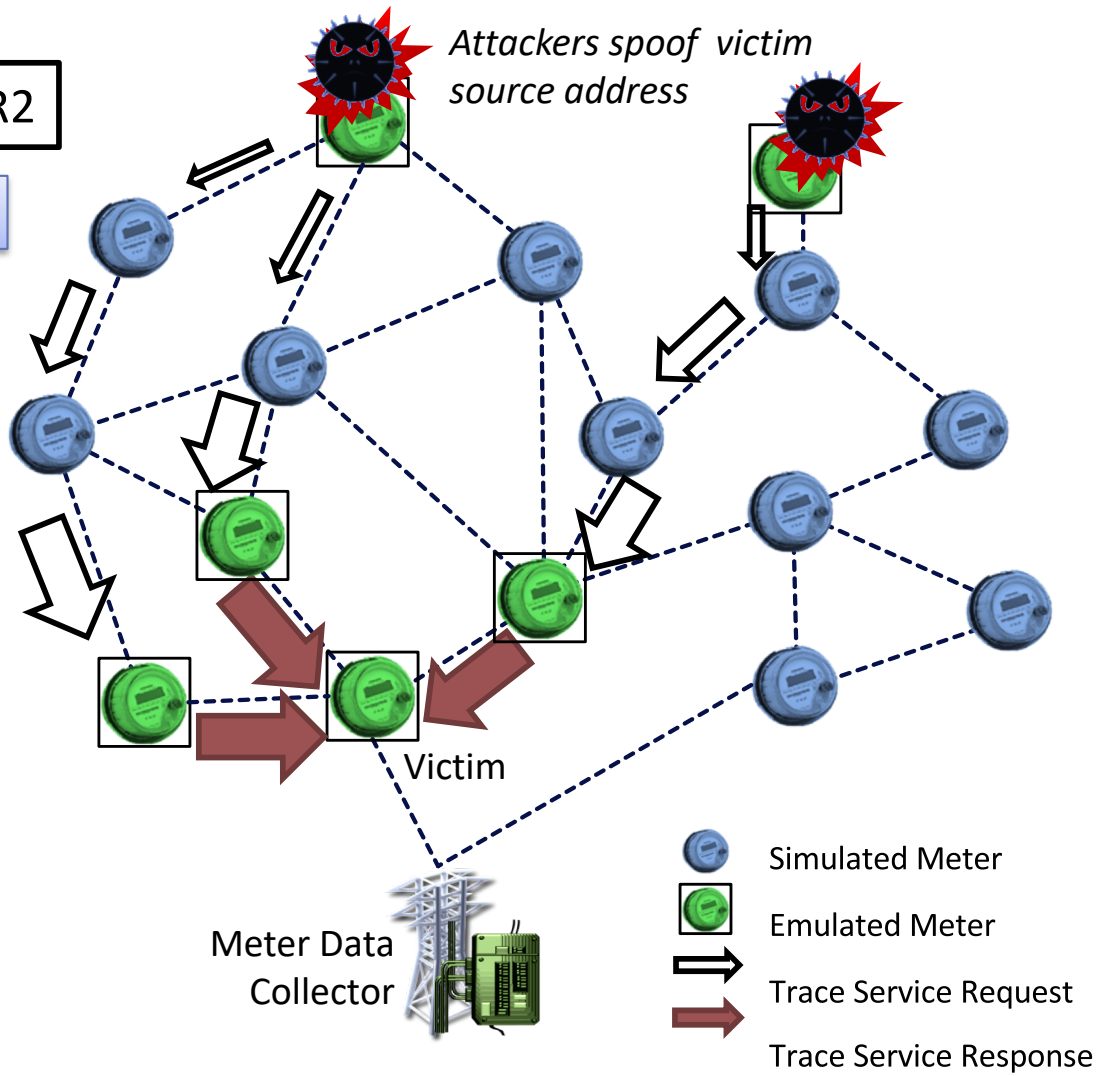
- Power grid control network
  - supervisory control and data acquisition (SCADA)
- Wide area monitoring
  - Phasor measurement unit (PMU)
- Advanced metering infrastructure (AMI)
  - Demand response
  - Load disaggregation
- Transactive control networks

Use Case: DDoS Attack in Smart Meter Networks

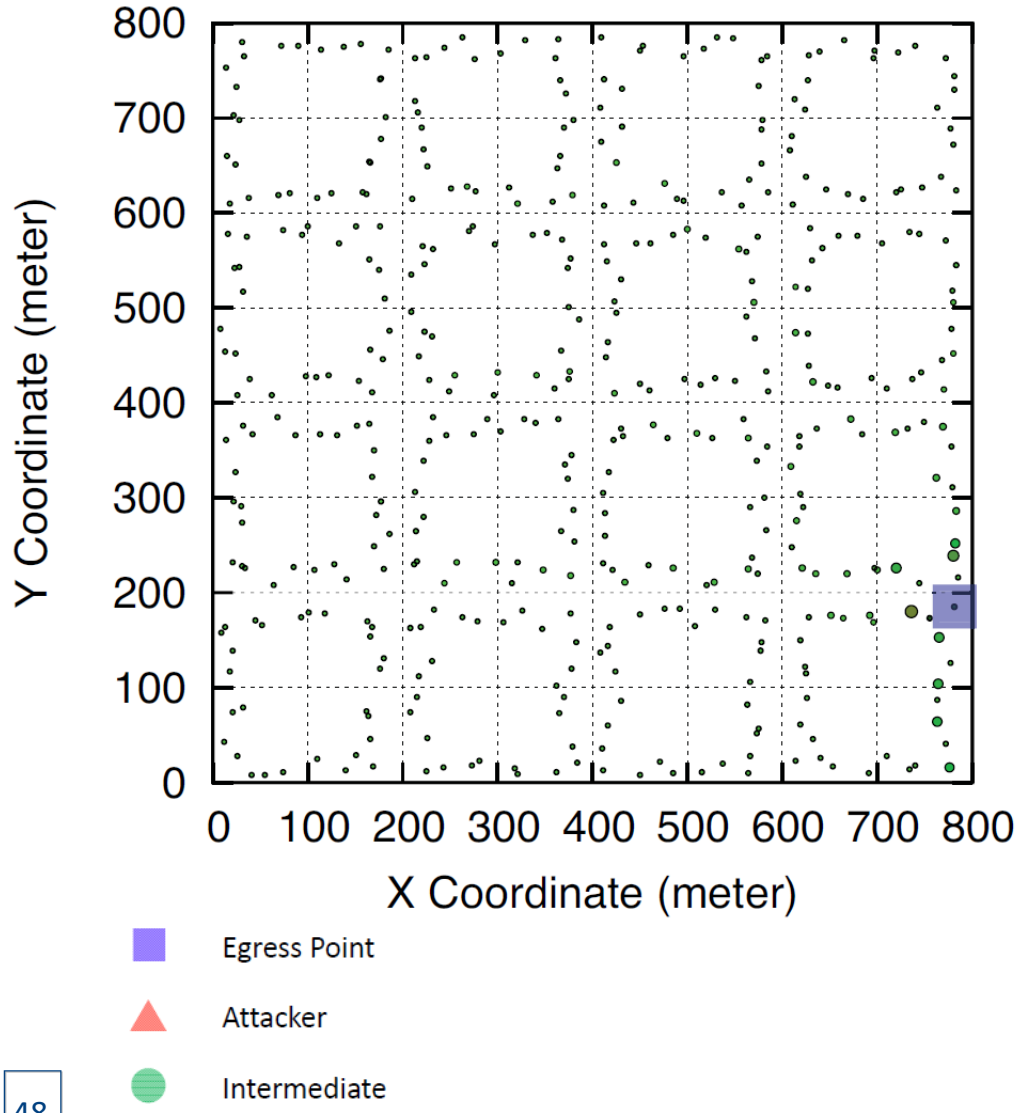
C12.22 Trace Service



- Amplification
  - Increased volume of traffic
- Reflection
  - Spoofed source address (the victim's address)

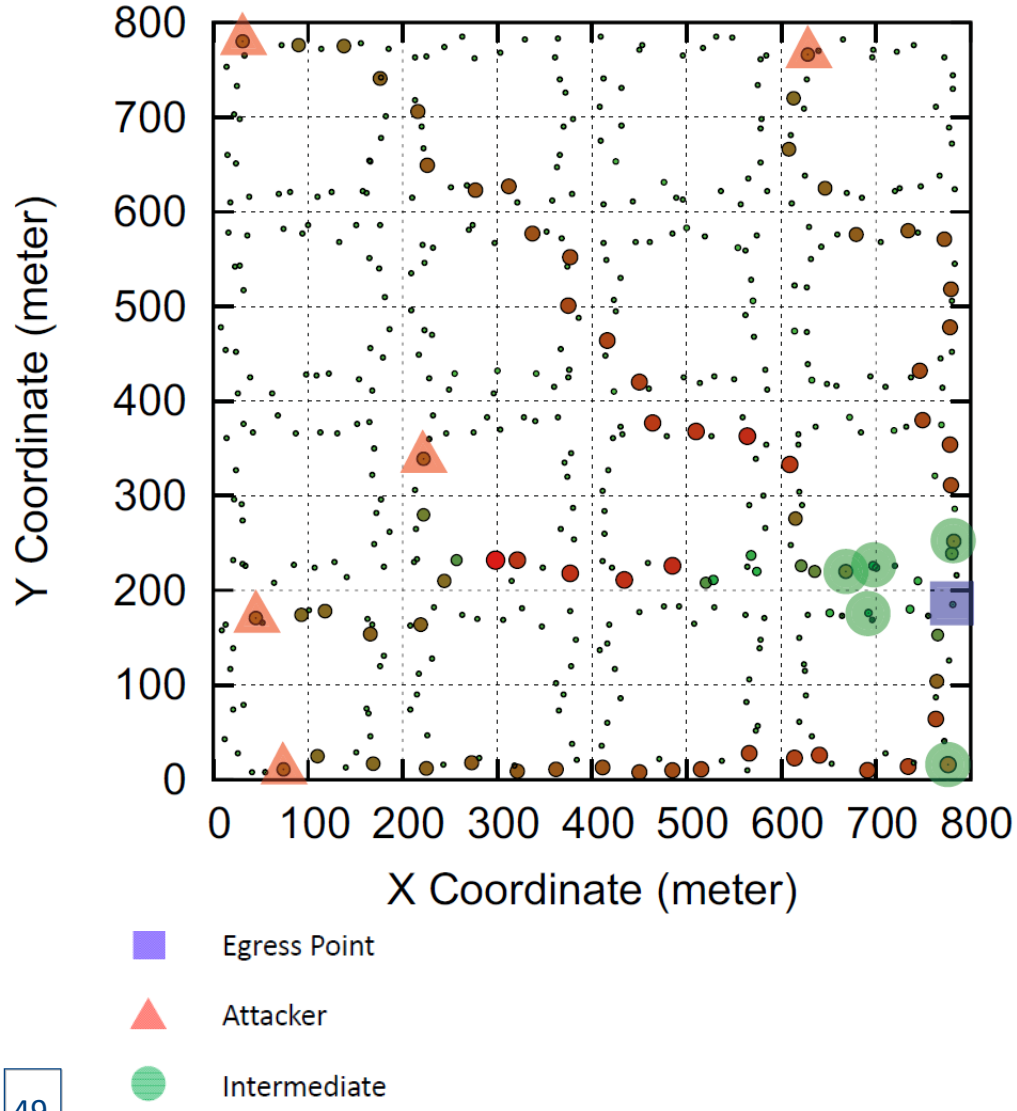


Attacking Experiment



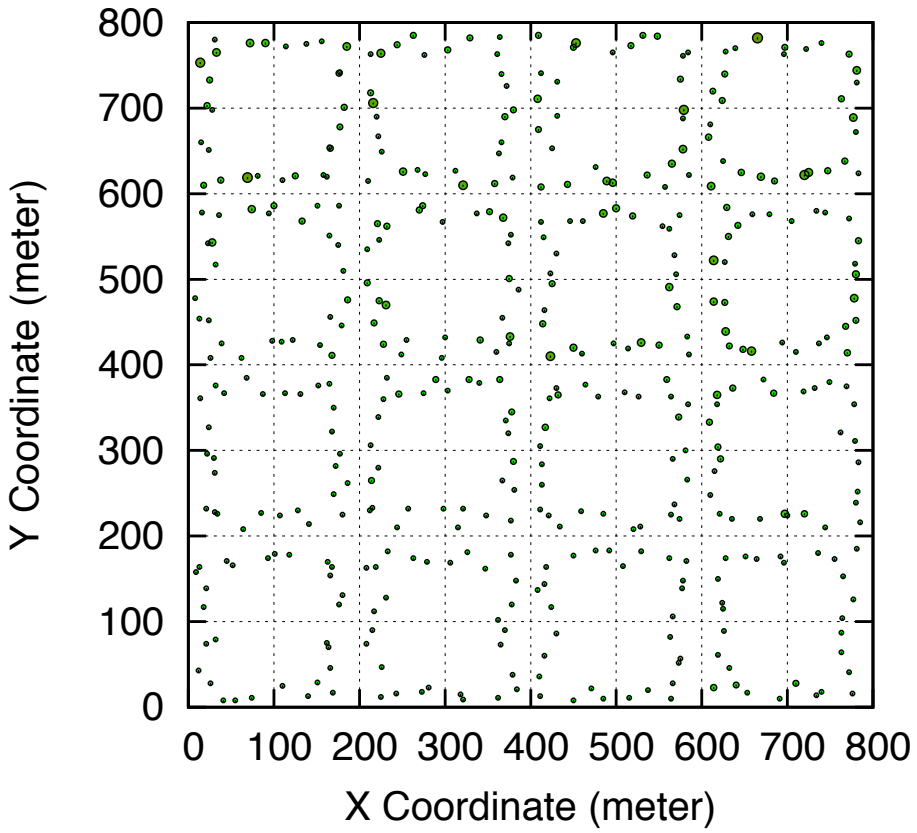
- 4x4 blocks, 448 meters
- ZigBee wireless network, 1 Mb/s bandwidth

Attacking Experiment

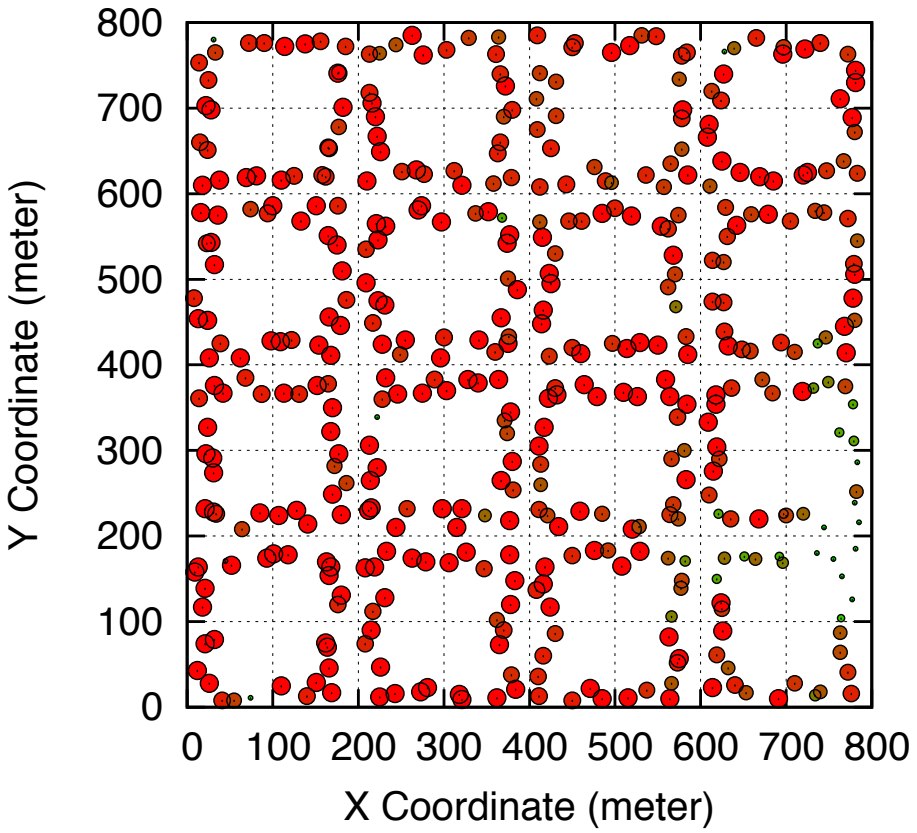


- 4x4 blocks, 448 meters
- ZigBee wireless network, 1 Mb/s bandwidth
- 5 attackers
- Victim: the single egress point (meter gateway)

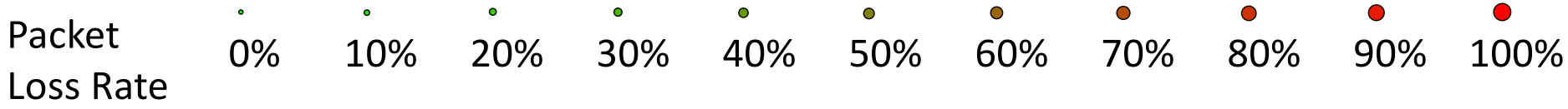
Experimental Results – Packet Loss



Normal



Under DDoS Attack



Conclusion

- Goal: To build a more secure, resilient, and safe cyber-environment for industrial control systems
- Enable a cyber secure and resilient ICS in microgrid with SDN
  - A novel SDN architecture in microgrid
  - Innovative SDN-based security applications
  - Microgrid testbed using parallel simulation and virtual-machine-based emulation


Thank you!


DSSnet: A Smart Grid Modeling Platform
Combining Electrical Power Distribution
System Simulation and Software
Defined Networking Emulation
DELL