



ILLINOIS

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

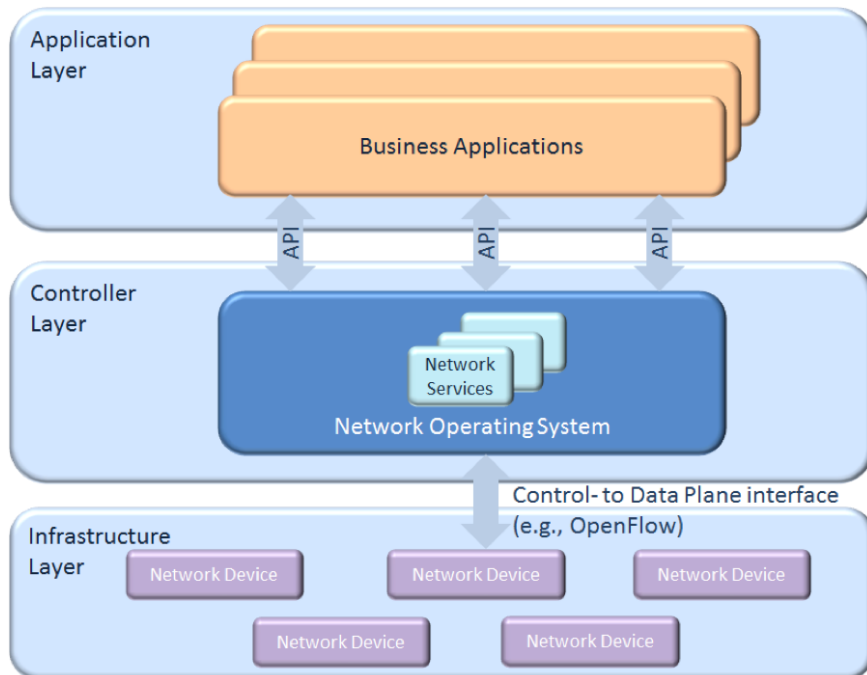


Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges

Xinshu Dong, Hui Lin, Rui Tan,
Ravishankar K. Iyer, Zbigniew Kalbarczyk
Advanced Digital Sciences Center, Singapore
University of Illinois at Urbana Champaign, IL, USA

Zoom In: SDN + Smart Grid

- Software Defined Networking
 - A new networking paradigm
 - Unprecedented flexibility, visibility, and QoS



- Smart Grid
 - Revolutionizing grid operations with ICT technologies
 - Demanding greater performance & resilience in communication channels
- SDN may provide support for communication requirements
- But, will it improve or degrade its *resilience*?

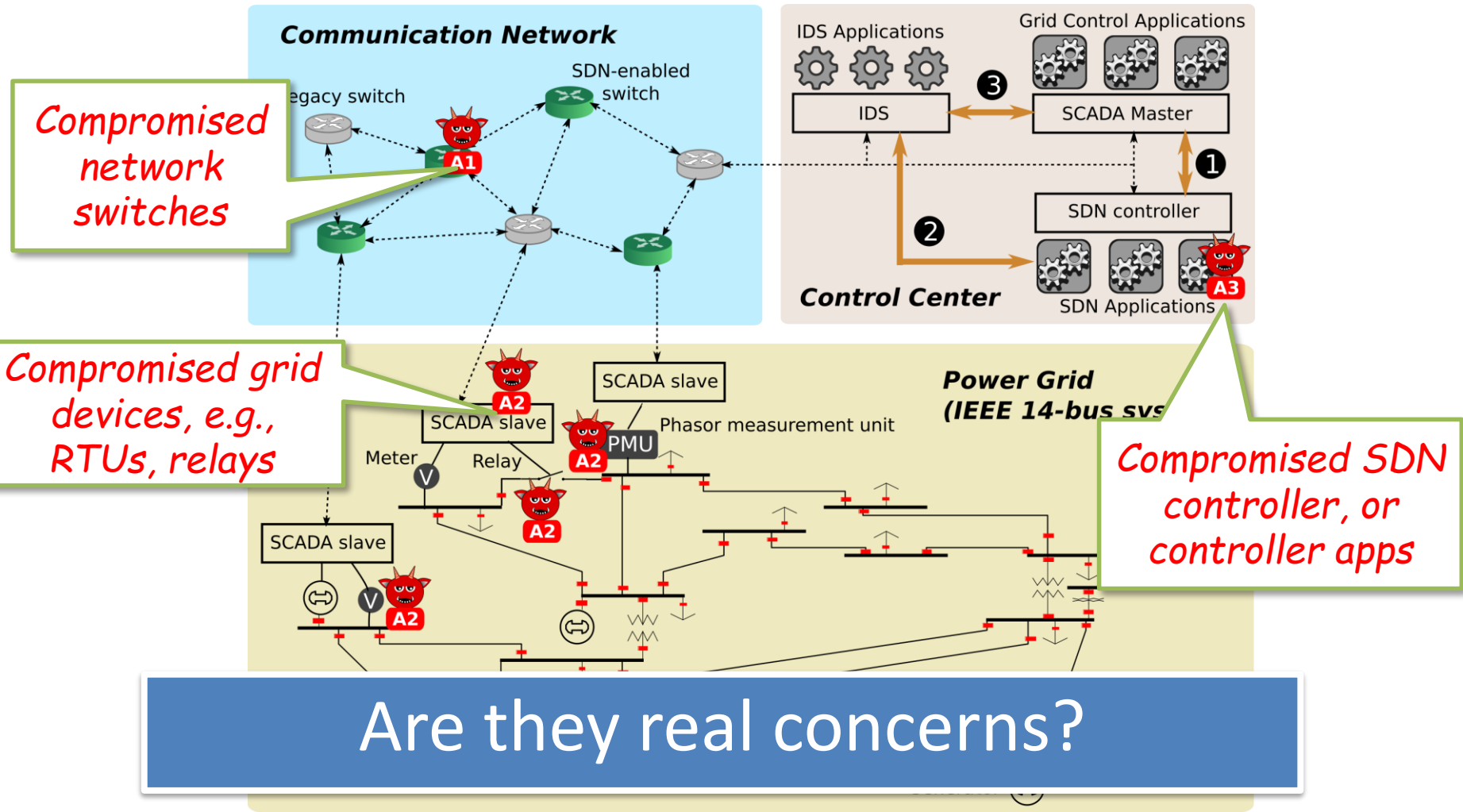
Will SDN Bring Better Resilience to Smart Grid?

- Needless to say its importance...
 - Smart grid: really critical infrastructure
 - Initial moves towards SDN already started
- Opportunities?
- Risks?
- *Can we know it for sure? How?*

This Work: An Initial Attempt

- Initial understanding of the benefits and risks in smart grid resilience with SDN integration
 - Illustrated with examples and analysis
- A testbed proposed to experimentally verify & validate cyber-physical perspectives in applying SDN to smart grid
 - Integrating power system simulation with communication networks
 - Extensible to real power system testbed

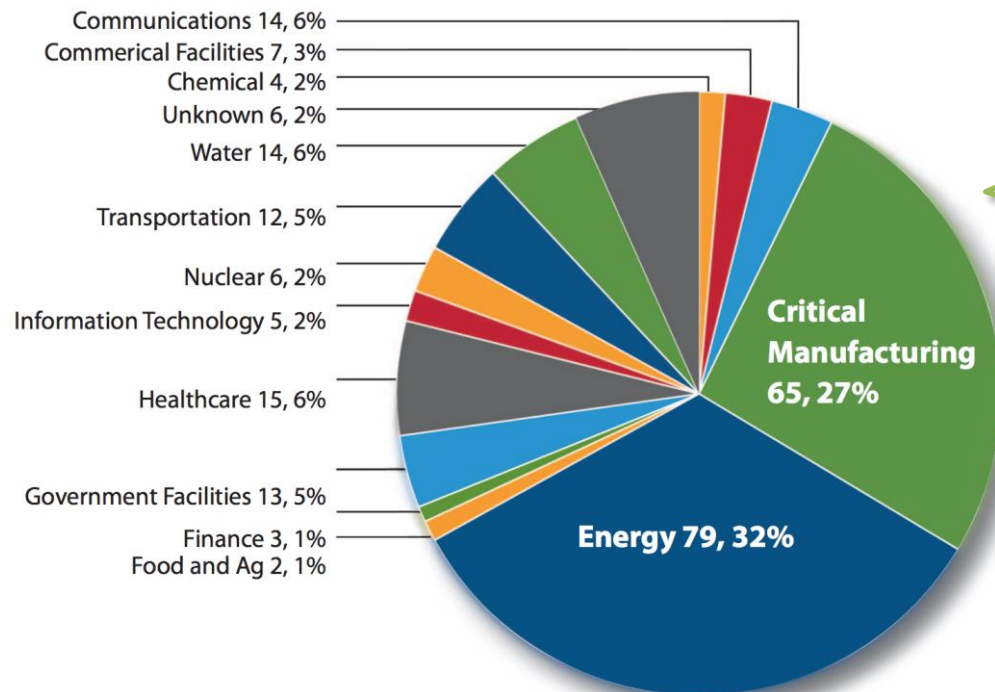
Knowing the Enemies: Prevailing Threats to Smart Grid



Real-World Incidents with Industrial Control Systems

- ICS-CERT report for 09/2014-02/2015

Industrial Control Systems Cyber Emergency Response Team



*A total of 245
incidents
reported*

A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER

Target attack shows danger of remotely accessible HVAC systems

Qualys says about 55,000 Internet-connected heating systems, including one at the Sochi Olympic arena, lack adequate security

Unhappy Workers are Increasingly Behind Security Breaches

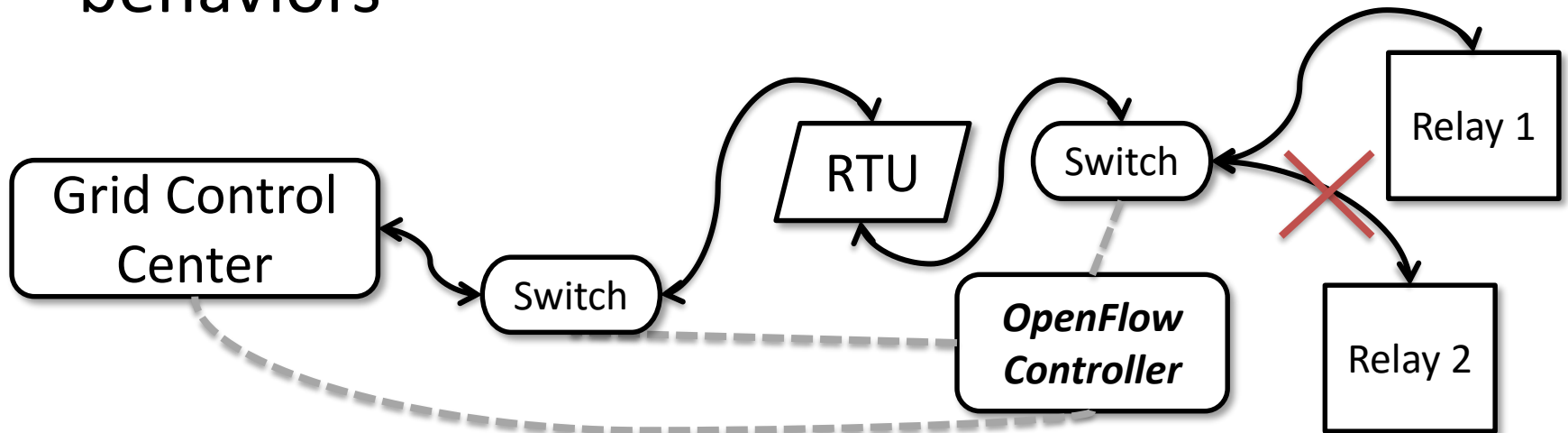
Companies must beware of hackers from within

By KATHY PRETZ 17 March 2015

Greater Resilience?

Opportunities by Example (I)

- Detecting malicious command forwarding behaviors

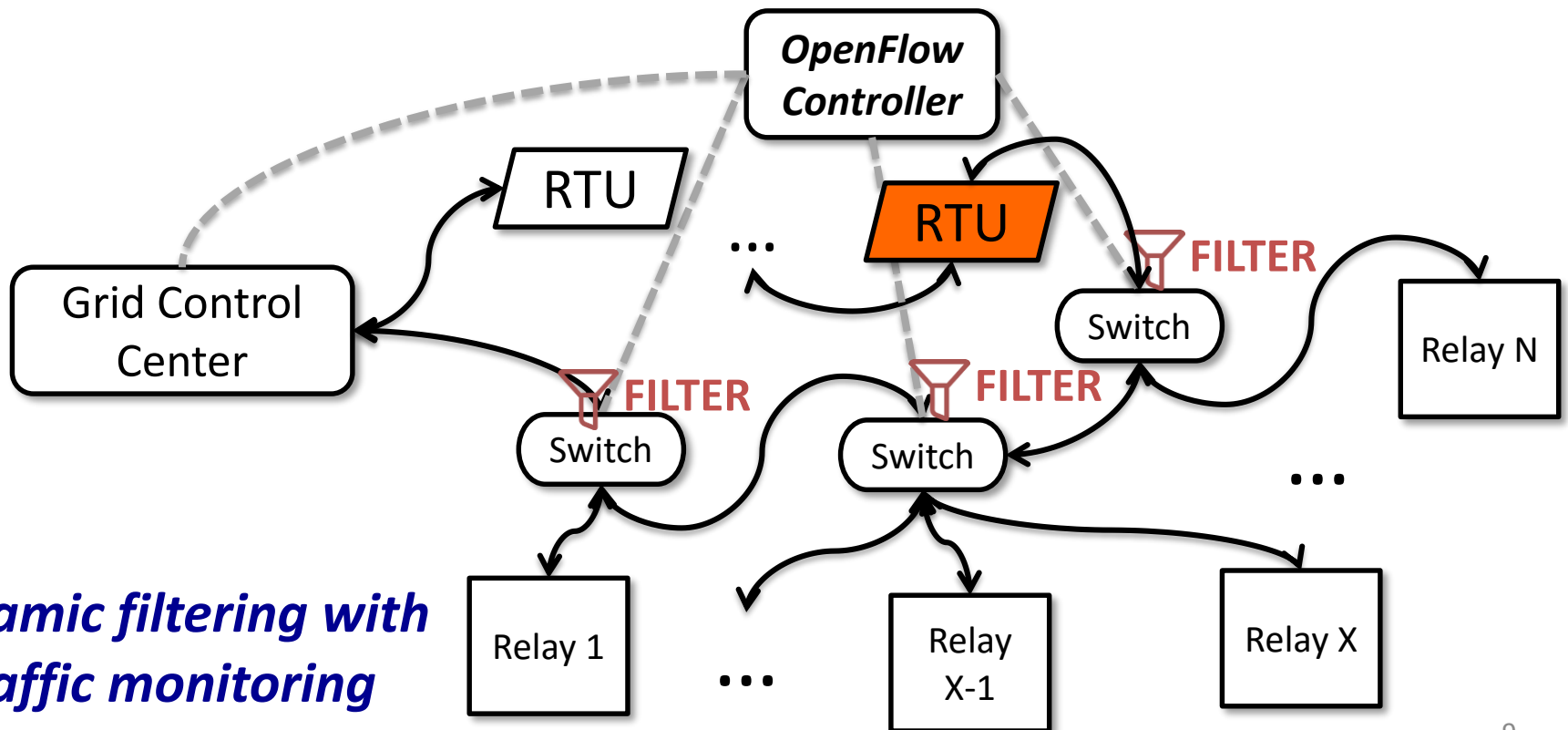


Empowers Control Center to ensure the commands are delivered to the intended control devices.

Greater Resilience?

Opportunities by Example (II)

- Filtering out flooded responses from control and field devices caused by spoofed requests



Greater Resilience?

Opportunities by Example (III)

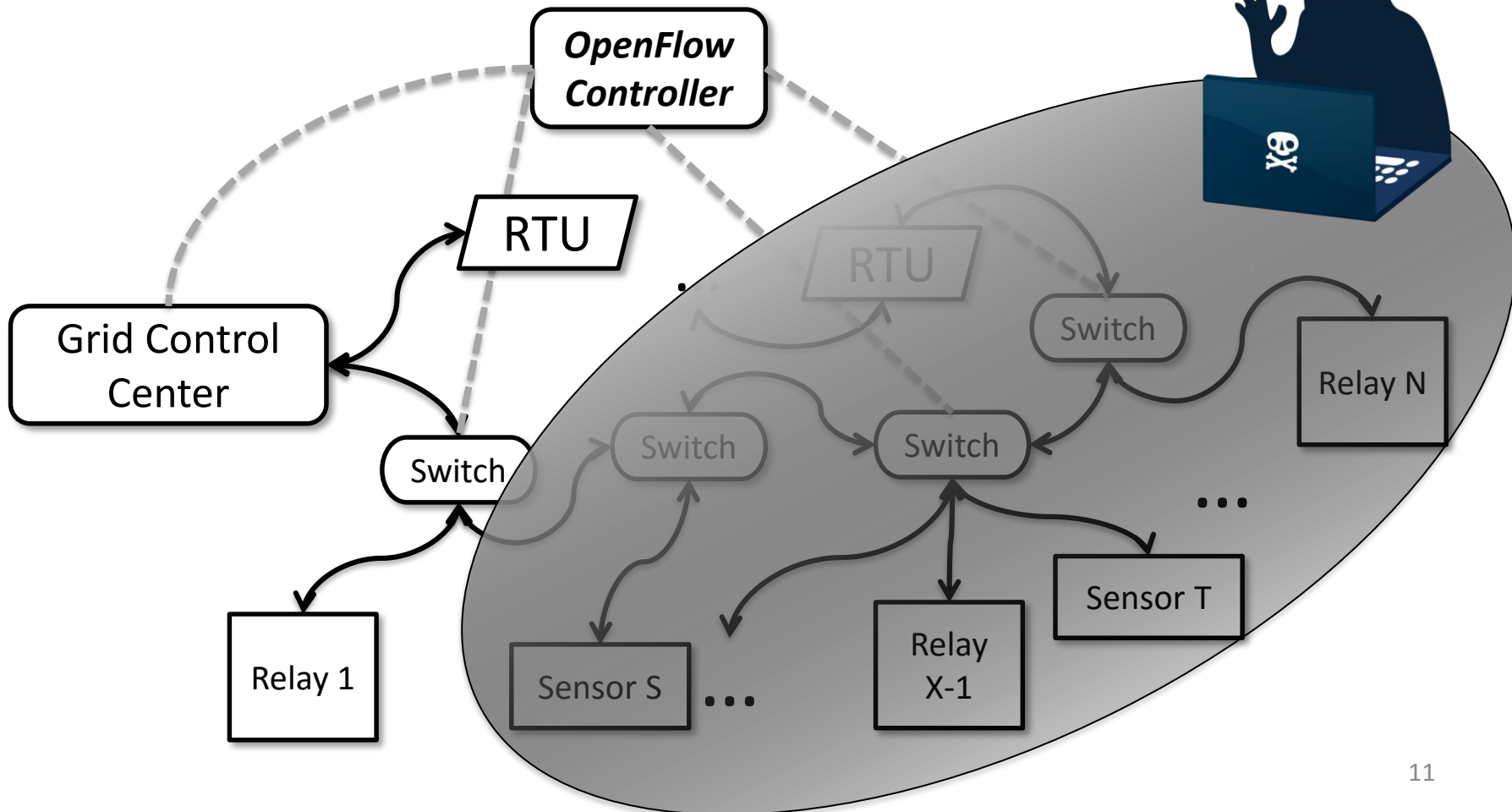
- Subtle, suspicious behaviors in smart grid
 - E.g., packet delays: by surreptitious attacks? Due to transient failures? Unusual but normal bursts of traffic?
 - Difficult to confirm, but highly detrimental to grid operations
- Hot-swapping of public-private network links
 - Trade-offs, between physical isolation and bandwidth
 - Weighing different under catastrophic situations

***SDN can provide a resilient virtual network layer,
with quick and in-phase reset of partial network***

Powerful Tool for Attackers?

Caveats by Example (I)

- Darknets created by *SDN rootkits*



Powerful Tool for Attackers?

Caveats by Example (II)

- Denial-of-Service (DoS) attacks
 - Well studied, still challenging to resolve
 - Grid-specific traffic may allow efficient solutions
- Destructive control commands
 - Will a control command cause delay, congestion, or lack of redundancy that is unacceptable to grid operations?

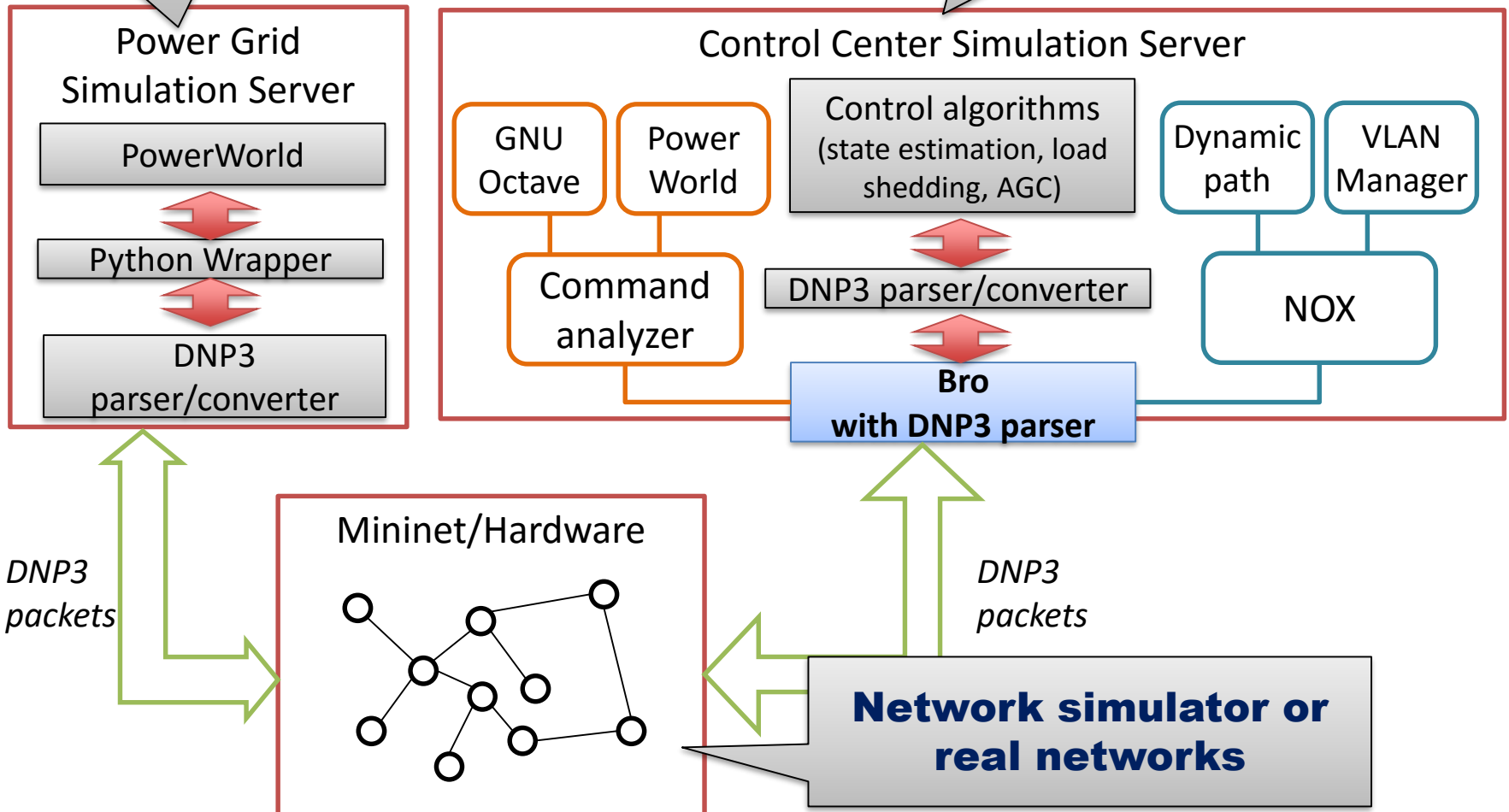
How to Tackle the Dilemma?

- SDN for smart grid
 - Tantalizing opportunities for greater resilience
 - Scaring power could be abused by attackers
- Empirical validation and verification
 - Experiments
 - Tools

High-fidelity power generation & transmission simulator

Proposed Testbed

Simulated control center / SDN controller



What Will Such a Testbed Enable?

- Co-simulation platform to experimentally understand both networking and power system aspects
 - Worst-case estimate of time required to re-establish a virtual network
 - How affordable such delay is to power systems
 - How much bandwidth can be expanded by hotswapping between public/private links
- A platform for developing new tools to quickly validate SDN control commands that can affect power system operations

We're *On Track!*



Conclusion

- Lots of opportunities to build more resilience smart grid communications with SDN
- More research needed for validating how SDN reconfiguration and control will affect grid resilience
 - We are far from being certain
- Testbed building and experimentation as our first step
 - Envision more tools developed to automate the verification and validation phase

Thank you!

- Questions?



Xinshu Dong
xinshu.dong@adsc.com.sg