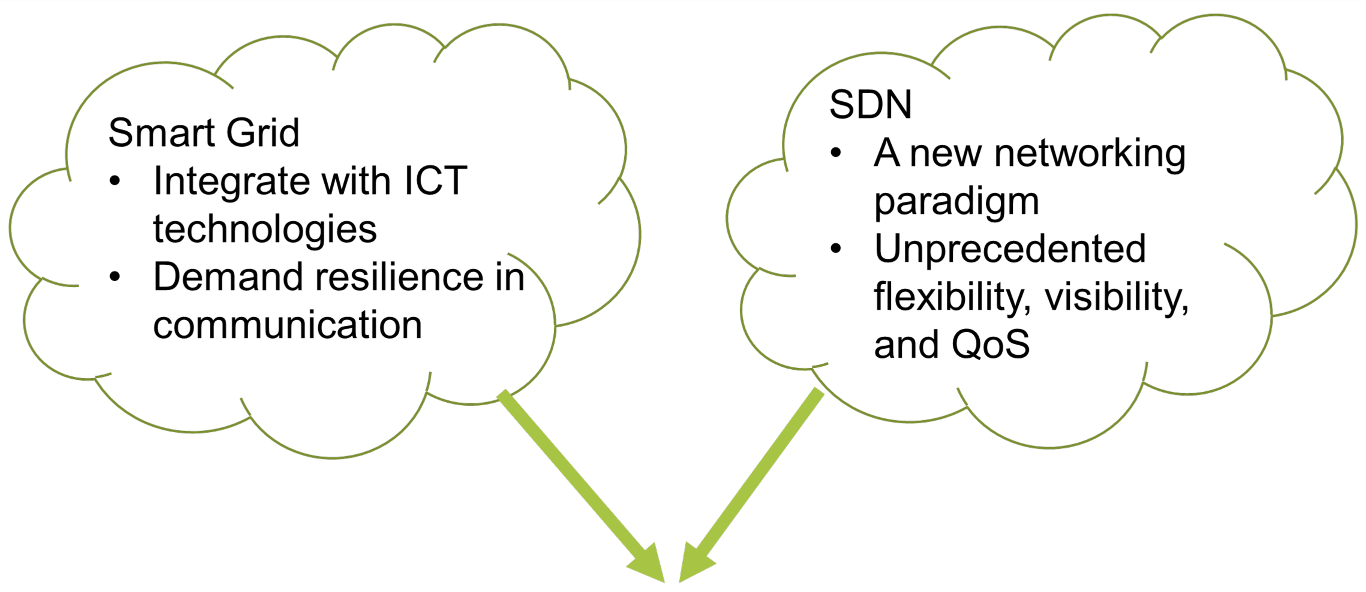
Enhancing Smart Grid Resilience Using Software-Defined Networking

Hui Lin, University of Nevada, Reno (hlin2@unr.edu)

GOALS

- Evaluate the application of software-defined networking (SDN) to smart grids for enhancing system resilience
  – Recover and maintain critical services despite accidental failures and malicious attacks
- Discuss following questions through illustrative examples
  – What are the opportunities for SDN to enhance smart grid resilience
  – What are the security risks that SDN brings to smart grids
  – How do we validate and evaluate attacks or protections?
- Design and develop a testbed that integrates the simulations of both cyber and physical infrastructure of smart grids

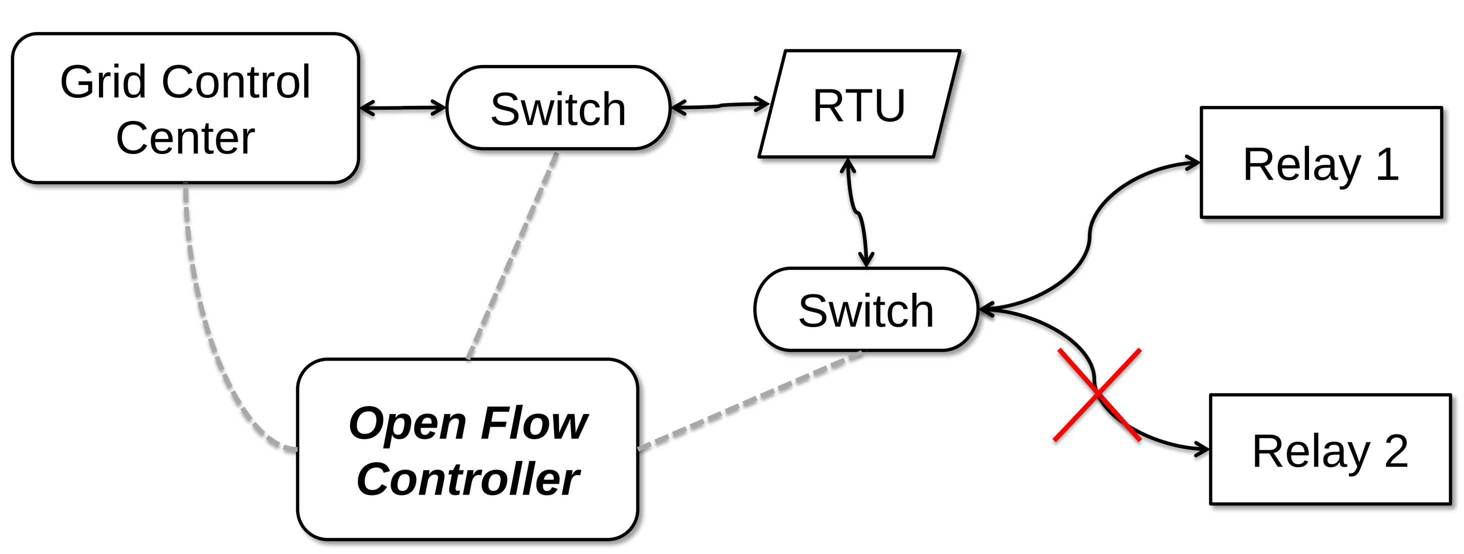
FUNDAMENTAL CHALLENGES



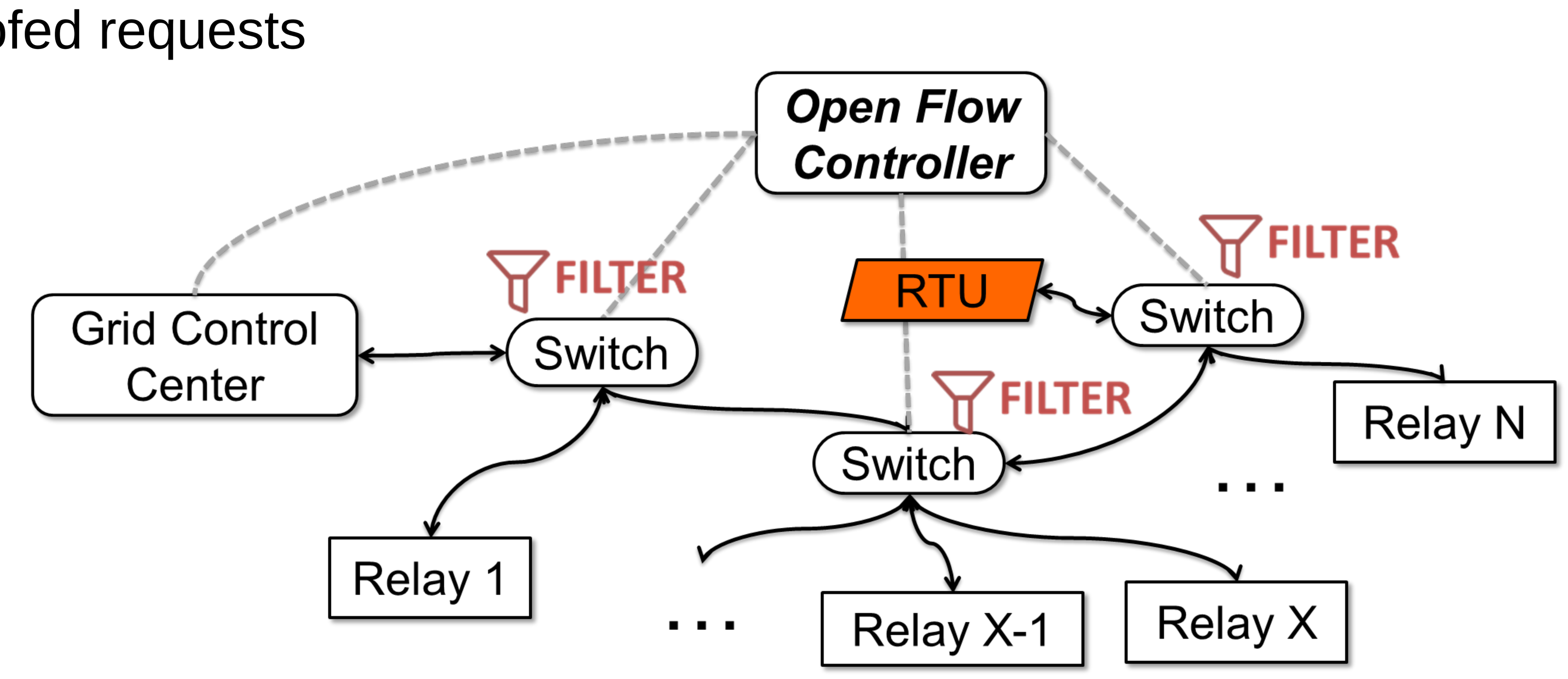
Improve or **Degrade**
Grid Resilience?

OPPORTUNITIES TO IMPROVE GRID RESILIENCE

- Opportunity (1): prevent attackers from compromising commands
  – Ensure correct commands from the control centers being delivered to the intended control devices
  – Monitor actual communication path of the commands



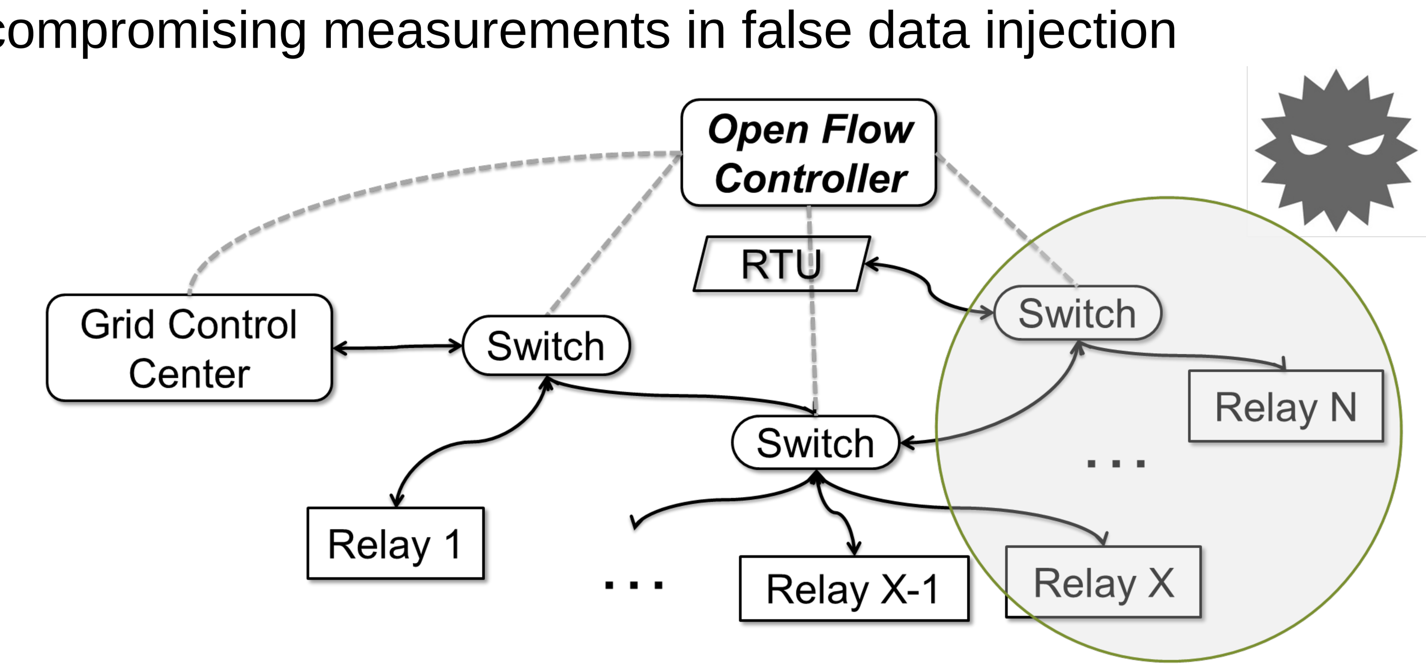
- Opportunity (2): prevent Denial-of-Service attacks
  – Filtering out flooded responses from control and field devices caused by spoofed requests



- Opportunity (3): detect subtle, suspicious behaviors in smart grids
  – 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
- Opportunity (4): isolate devices affected by attacks or accidents
  – Hot-swapping of public-private network links
  – Trade-offs, between physical isolation and bandwidth
  – Weighing different under catastrophic situations

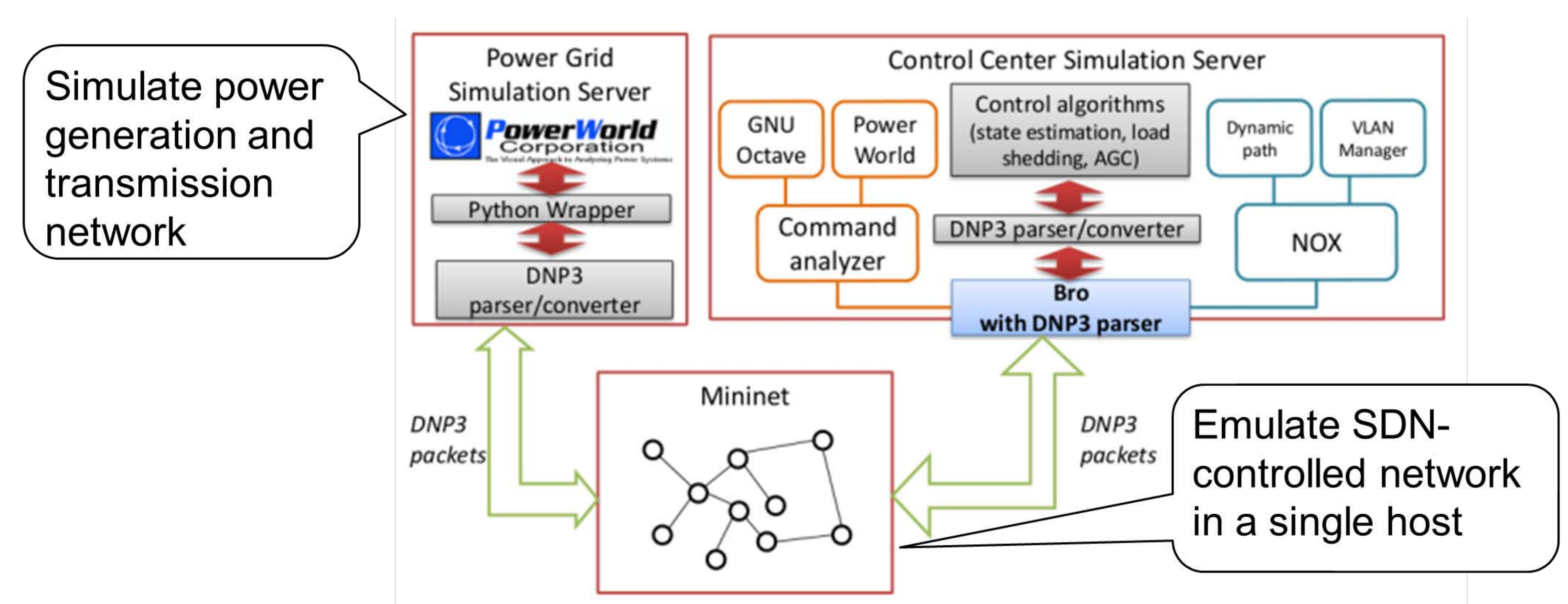
THREATS TO GRID RESILIENCE

- Threat (1): "Darknets" created by SDN rootkits
  – Attackers compromise part of the control plane
  – Manipulate the communications to critical field devices
    - E.g., compromising measurements in false data injection



- Threat (2): Denial-of-Services attacks accelerated by centralized control
  – Well studied, still challenging to resolve
- Threat (3): topology destruction by malicious SDN controller
  – Change the configurations of the communication network
  – Undermine the performance of grid control applications

TESTBED DEVELOPMENT



- Interconnected simulation that integrates both the cyber and physical infrastructure of smart grids
  – Inject faults in simulated communication networks, e.g., Mininet
  – Evaluate physical impacts in transmission networks, e.g., PowerWorld
- Example case
  – Characterize the consequences of such communication latency on automatic generation control (AGC)

FUTURE EFFORTS

- Use simulated testbed for research experiments
  – Evaluate the proposed intrusion detection and response mechanism
- Build testbed in real open flow controllers, switchers instead of simulations
- Evaluate how network activities impact the transient stability of power systems

SELECTED PUBLICATIONS

- Xinshu Dong, **Hui Lin**, Rui Tan, Ravishankar K. Iyer and Zbigniew T. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," in *Proc. CPSS*, ACM, 2015.
- **Hui Lin**, Adam Slagell, Zbigniew Kalbarczyk, Peter W. Sauer, and Ravishankar K. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," in *IEEE Transactions on Smart Grid*, Jan, 2018.