Automated Synthesis Framework for Network Security and Resilience

Matthew Caesar and Kevin Jin

University of Illinois at Urbana-Champaign

University of Arkansas

caesar@illinois.edu,

847-323-2968

We need a science of security

- Practice of doing cyber-security research needs to change
  - Attempts based on reaction to known/imagined threats
  - Too often applied in ad-hoc fashion
- SoS program: move security research beyond ad-hoc reactions
  - Need a principled and rigorous framework
  - Need a *scientific* approach

What is science?

sci·ence *noun* \ˈsī-ən(t)s\

: the systematic study of the structure and behavior of the natural and physical world through observation and experiment

The scientific method

1. Ask a question
2. Formulate a hypothesis
3. Design and conduct an experiment
4. Analyze results

Towards a science of security

- Can we apply the scientific method to the domain of cybersecurity?
  - Challenges: complex, large scale+dynamic environments, many protocols/mechanisms, demanding requirements for accuracy/precision

- Need a new approach

Our project

- Building a rigorous methodology for science of security
  - Techniques for performing/integrating security analyses to automatically and rigorously study hypotheses about end to end security of a network

- Address challenges in applying science to security
  - Leveraging <u>automation</u> to scale and cope with complexity
  - Leveraging <u>rigor</u> for accuracy

- Specific outcome: Resilient network architecture
  - Specific focus: network data flow security

Our approach

Leverage *network synthesis* to automate experiments, apply results

Enables practical uses: deriving patches, automating configuration

Builds upon mathematics (formal logics, formal methods)

Task plan

- **Task 1: Network Control Synthesis**
  - Develop algorithms/systems that perform automated synthesis
  - Automatically derive configurations, patches/fixes
- **Task 2: Network Software Analysis and Modeling**
  - Develop frameworks for writing secure network control programs
  - Joint network/software analysis, integration with network programming languages
- **Task 3: Resilient and Self-healing Network Applications**
  - Self-healing network management
  - Applications to cyber-physical energy systems

Progress Highlights

[Give general overview of progress, # publications, outreach efforts, initiatives]

Built first operational data plane verifier

Technology transfer

- Spawned startup company with multiple active pilots in DoD and commercial sector, sold to VMware Sept 2019
- Ongoing transfers to AT&T, Boeing,

This talk

We will talk about a few particular activities we are doing:

1. Self-driving Service Provider Infrastructures

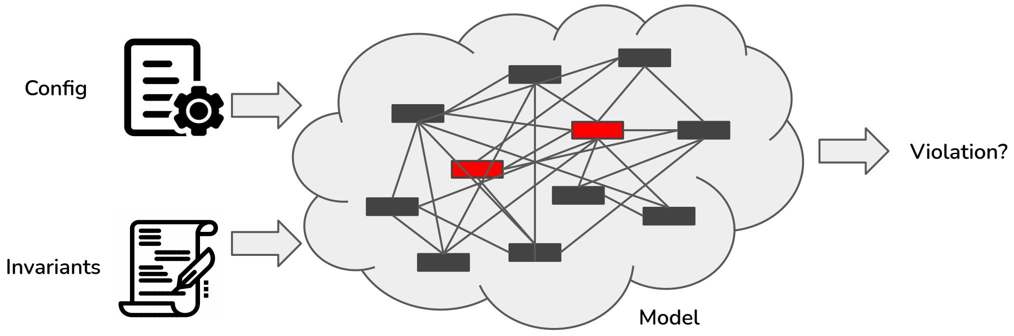
2. Resilient Power Systems

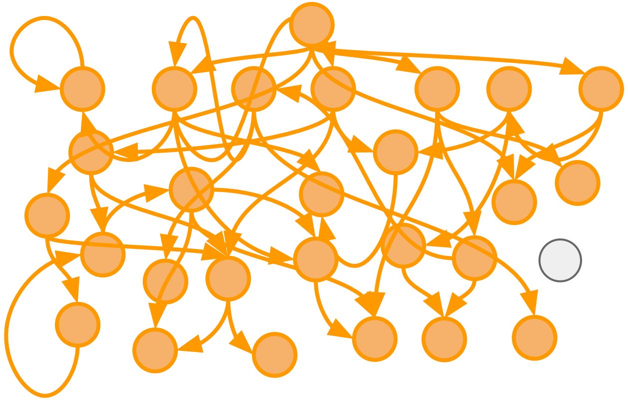
3. Supporting Teaching and Research with Virtualized IoT Systems

Towards Self-Driving Service Provider Infrastructures

One approach: Model-based Verification

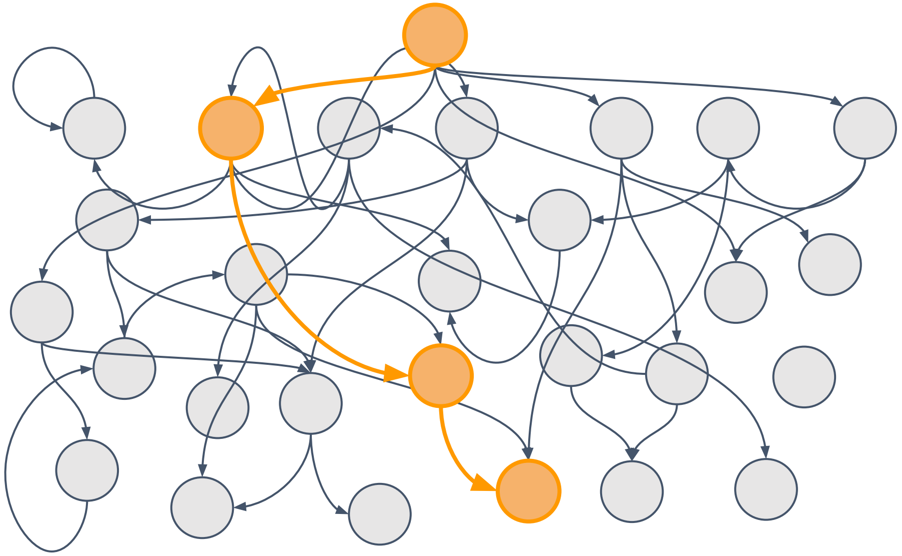
- What is verification?
  - Exhaustively check against all possible states, based on a model of the system.
- Limitations
  - Models can be less accurate compared to running the actual code.
  - Models can be more difficult to understand





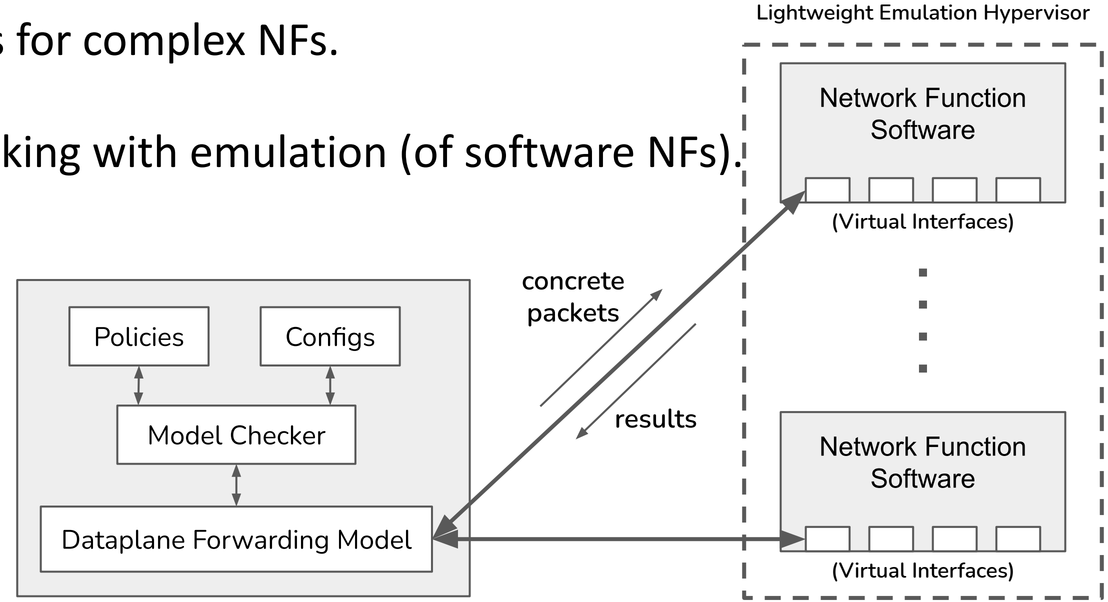
Alternative approach: Emulation testing

- What is emulation testing?
  - Run the actual software in an emulated environment (e.g., VMs).
- Limitation
  - Limited coverage.



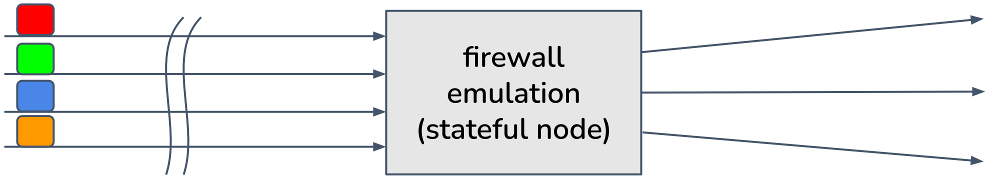
Problem & Solution

- Problem
    - Lack of accurate models for complex NFs.
- Solution
    - Incorporate model checking with emulation (of software NFs).
- Challenges
    - How to emulate?
    - Emulation state tracking.
    - Distribute workload.
    - Multi-connection coord.
    - In-band connection initiation.
    - Drop interpretation.



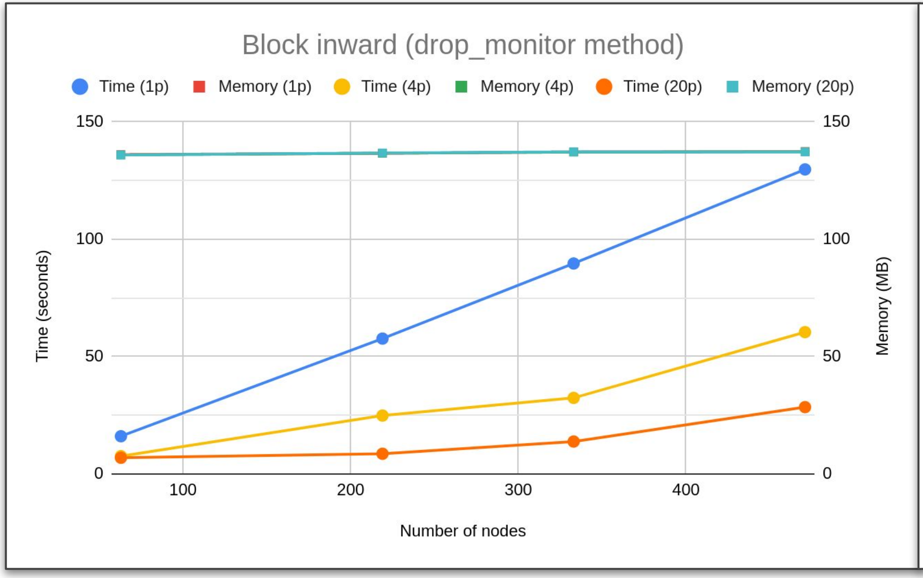
Example Challenge: Multi-connection coordination

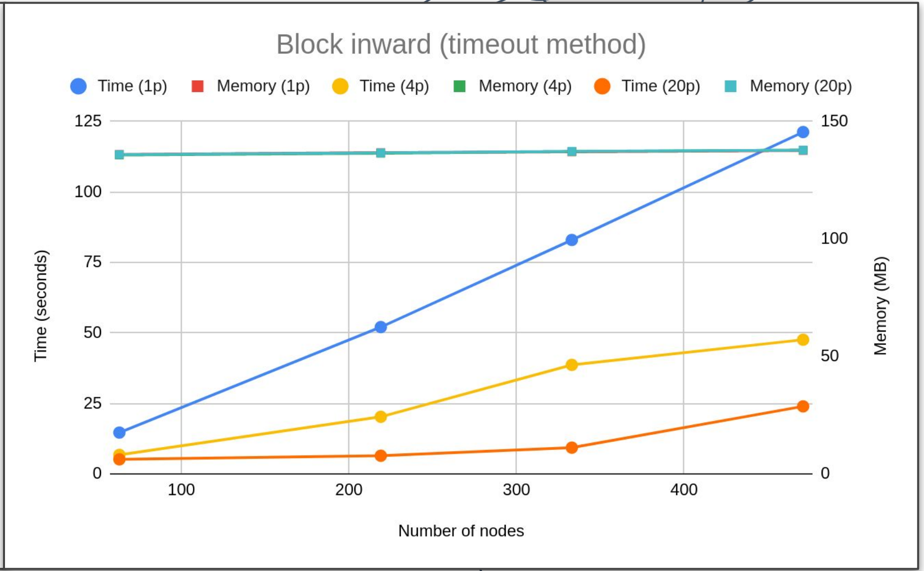
- Partial-order reduction (POR)
  - If any ordering of events (A, B, C) yields the same result, we only test one of them.
    (This preserves completeness.)
- Most of our model is stateless. Apply POR for interleaving connections.
  - Only the orders of packets entering the emulations are relevant.
    i. For now, "emulation instances" ≡ "stateful nodes".
  - POR heuristic (pick arbitrary connection until everyone is entering emulation instances)



Evaluation: Stateful firewalling (time & memory)

Policy: Disallow inward to private subnets.





- Distributing EC workload helps.
- Timeout performs slightly better than the drop_monitor method.
- Approx. linear CPU time & constant memory usage.

Conclusions

Our proof-of-concept system can accurately generate plans for complex tasks

Model checking with emulation techniques to reduce the need for accurate formal models

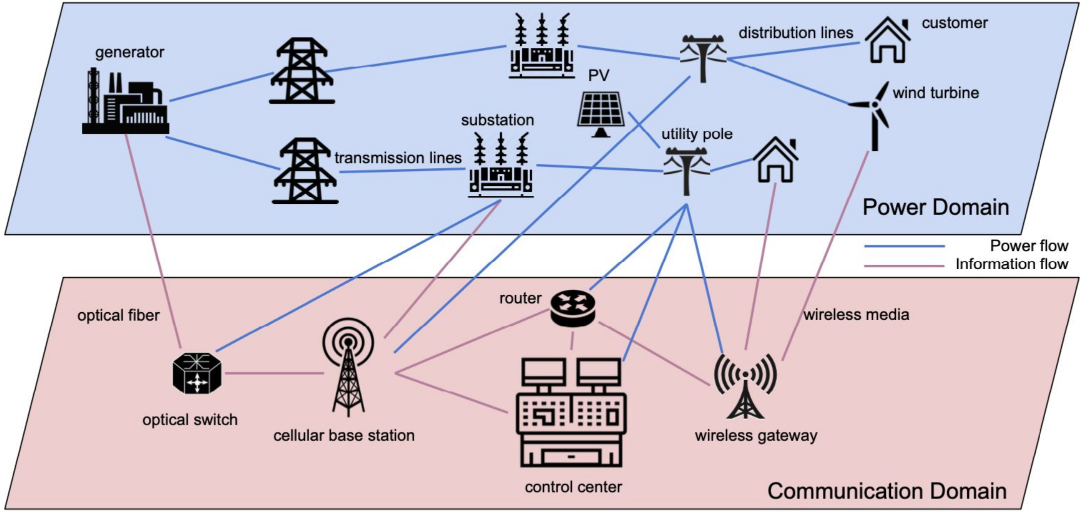
Next steps: domain-specific optimizations, modeling of human actions, integration with (mirrored) AT&T service platform

Towards a Resilient Power Grid with Power-Communication Networks Interdependency Study

Cyber Resilience in Energy Systems

Definition of "Resilience" from Wikipedia

- Computer network — "ability to maintain service in the face of faults"
- Engineering and construction — "ability to respond, absorb, and adapt to, as well as recover in a disruptive event"



Our Approach

- Literature review
  - IET Survey paper 2019
  - Limitations of existing works
    - Only analyzing impact in one direction, i.e., from cyber to power
    - Lacking accurate models of the interdependencies
    - Lacking efforts to address mitigation of and recovery from the failures
- Interdependence modeling and testbed setup
  - DSSNet, combining power simulation and network emulation/hardware
    - ACM SIGSIM-PADS'19, **Best Paper Award**
- Grid resilience applications
  - Self-healing communication network
    - IEEE SmartGridComm'20, **Best Paper Award**
  - Distribution grid restoration
    - IEEE Transactions on Smart Grid [2nd round review]
  - MAD attack detection
    - IEEE Transactions on Smart Grid [In preparation]

Application: Distribution Grid Restoration

- Current restoration takes days or even weeks
  - Hurricane Sandy restoration times
  - PJM: 31 days
  - NYISO: 12 days
  - ISO-NE: 7 days
- Power restoration process
  - Damage assessment
  - Crew dispatch: operation crew, repair crew, …
  - Restoration: energize loads by propagating electricity from substation downwards

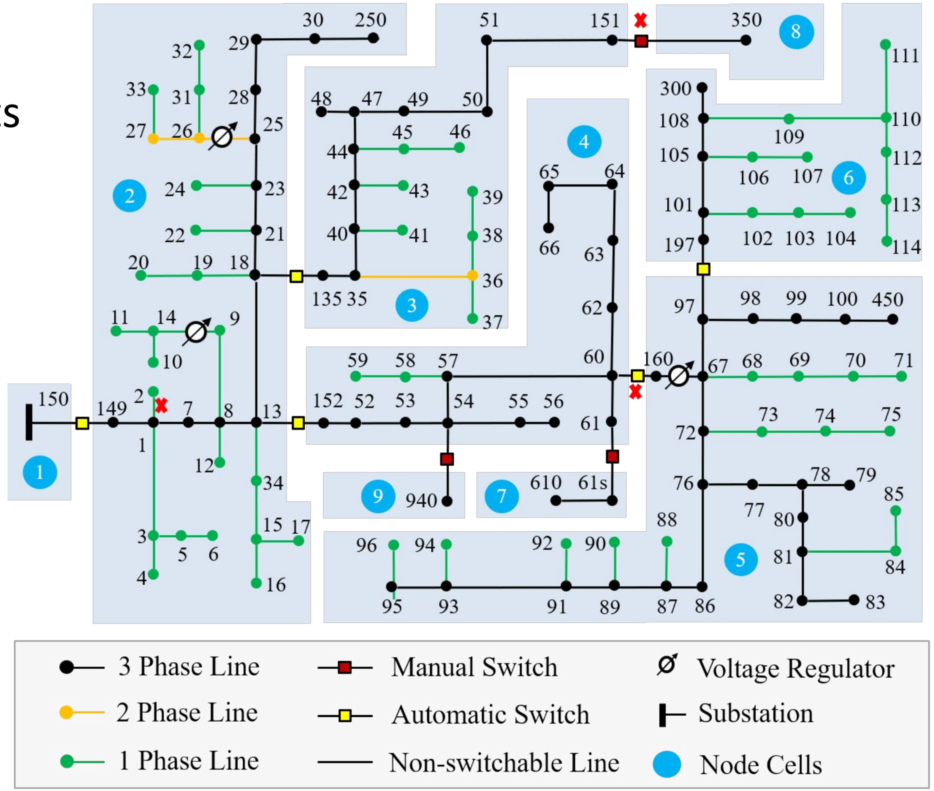
Related works

- Distribution system restoration under natural disasters [1][2]
  - Lack of communication interdependency
- Restoration with communication consideration [3][4]
  - Abstract model that cannot be used directly
- Need an “executable” restoration planning tool for utility companies in face of disasters

[1] Meng, Song, and Wei Sun. "Robust Distribution System Load Restoration with Time-Dependent Cold Load Pickup." *IEEE Transactions on Power Systems* (2020).
[2] Yang, Li-Jun, You Zhao, Chen Wang, Peng Gao, and Jin-Hui Hao. "Resilience-oriented hierarchical service restoration in distribution system considering microgrids." *IEEE Access* 7 (2019): 152729-152743.
[3] Wäfler, Jonas, and Poul E. Heegaard. "Interdependency in smart grid recovery." In *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, pp. 201-207. IEEE, 2015.
[4] Baidya, Prabin M., and Wei Sun. "Effective restoration strategies of interdependent power system and communication network." *The Journal of Engineering* 2017, no. 13 (2017): 1760-1764.

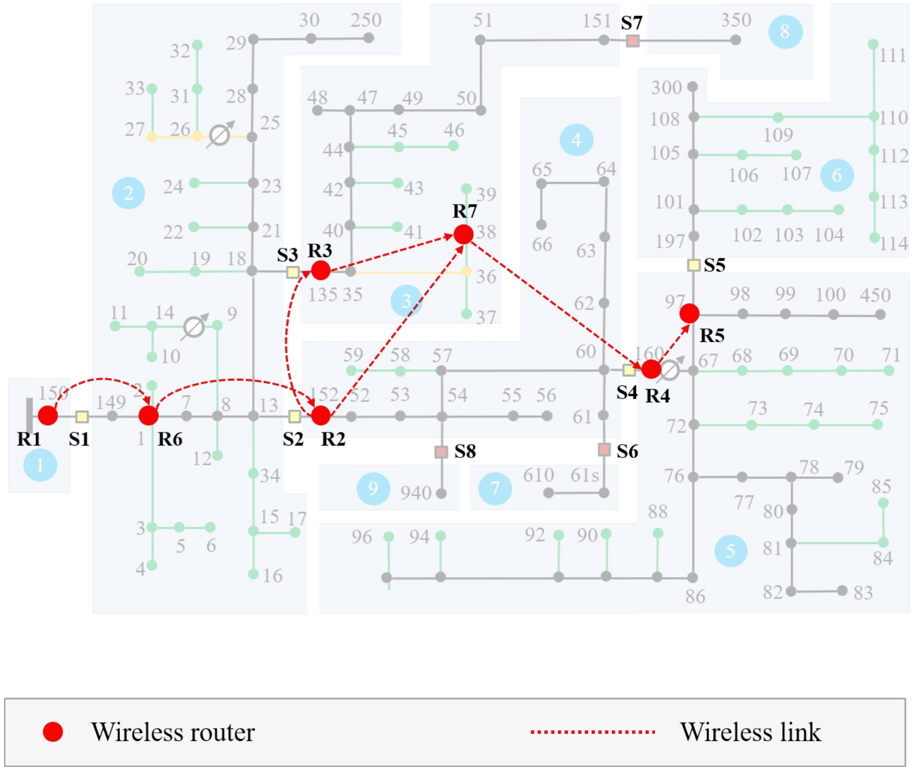
Step 1. Build a two-layer graph model

- Power grid model (e.g. IEEE-123 system)
  - Feeders, branches
  - Manual/automatic switches
  - Node cells (blocks) as energization units



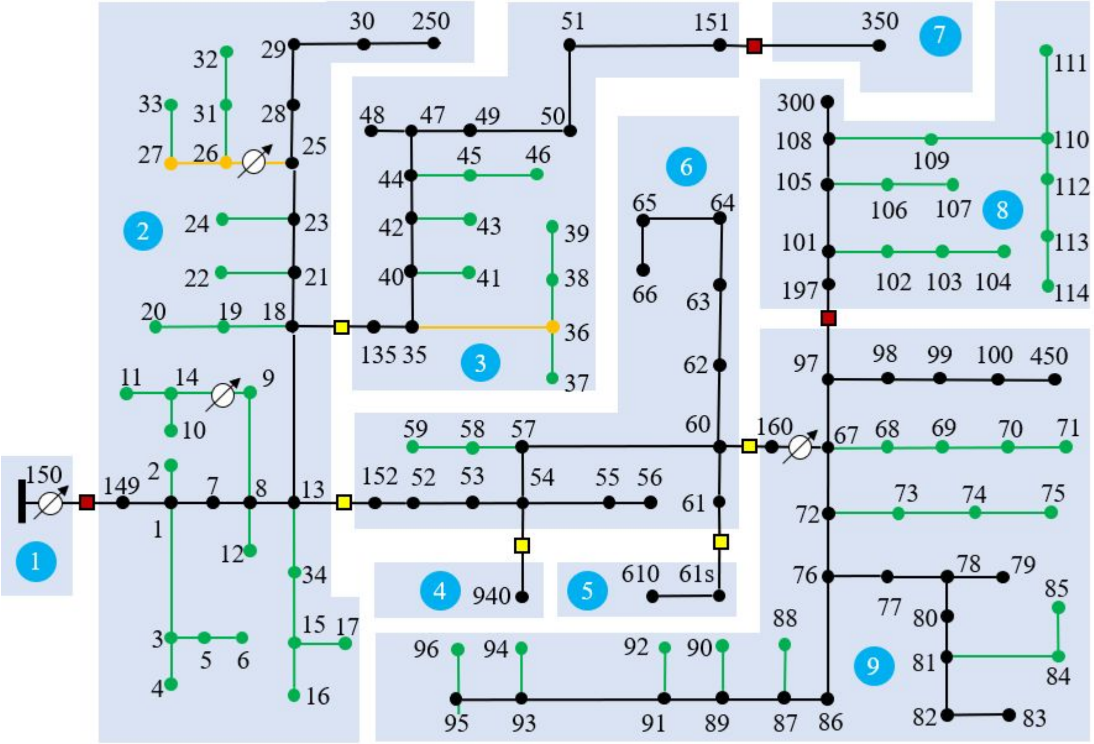
Step 1. Build a two-layer graph model

- Communication overlay (e.g. wireless mesh network)
  - Wireless gateways that control automatic switches
  - Wireless links



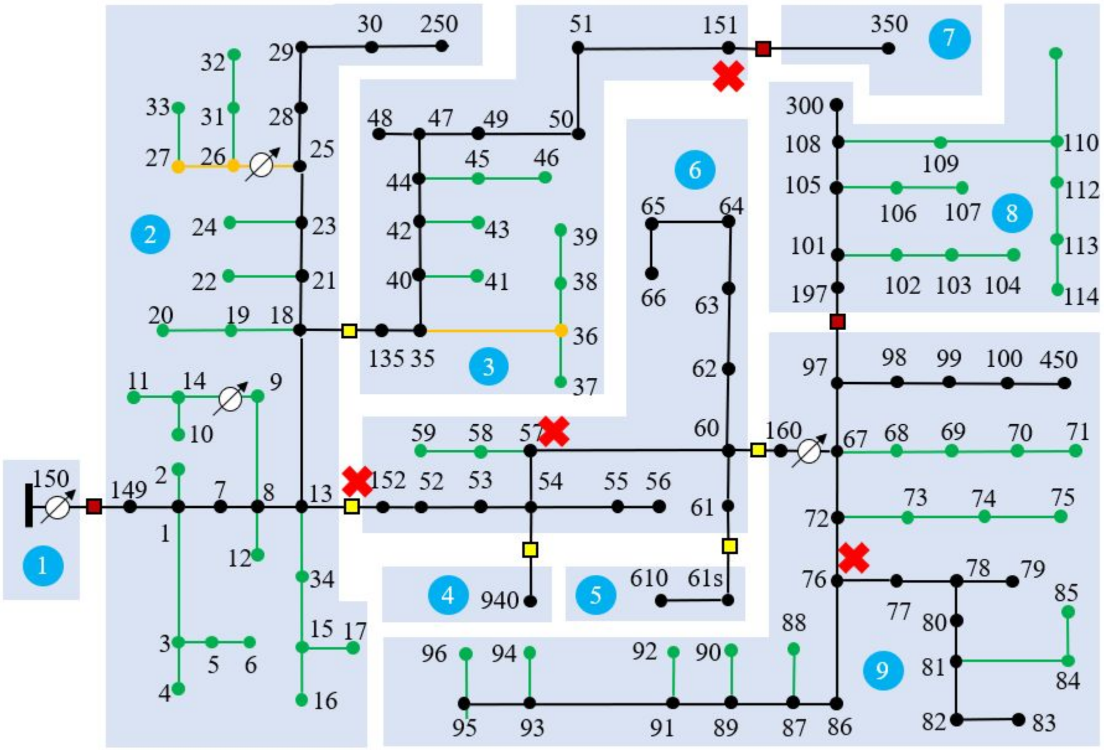
Step 2. Formulate a traveling problem

- All switches are opened automatically to isolate the power failure, forming node blocks



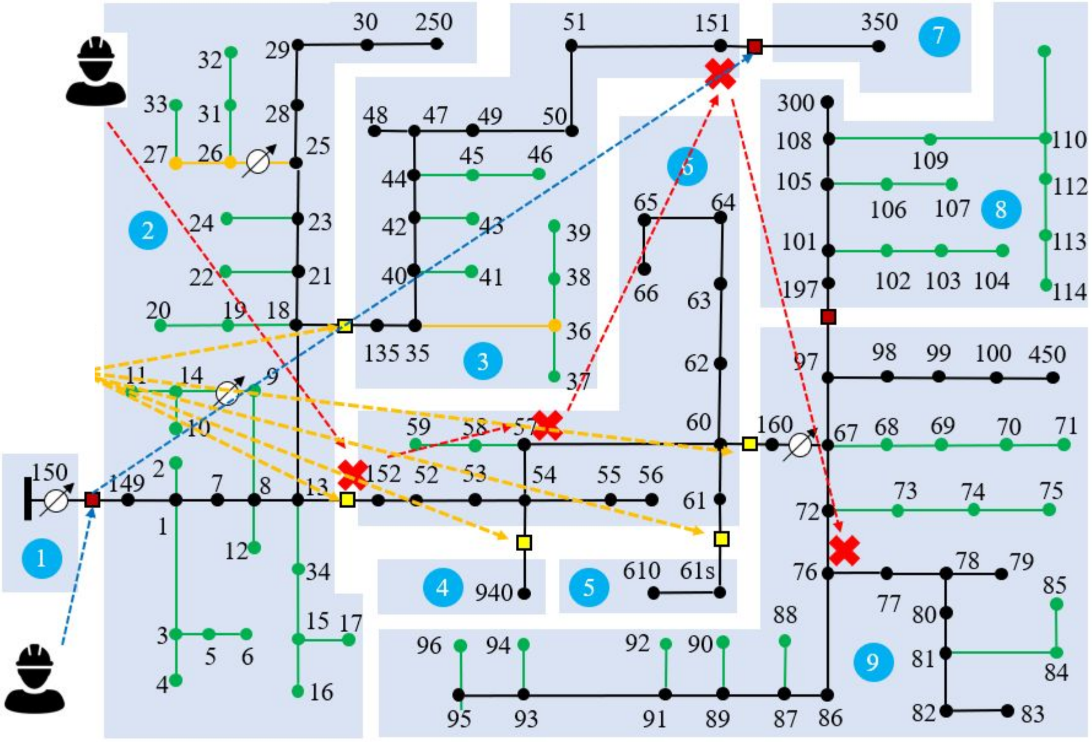
Step 2. Formulate a traveling problem

- All switches are opened automatically to isolate the power failure, forming node blocks
- Identify the damaged components



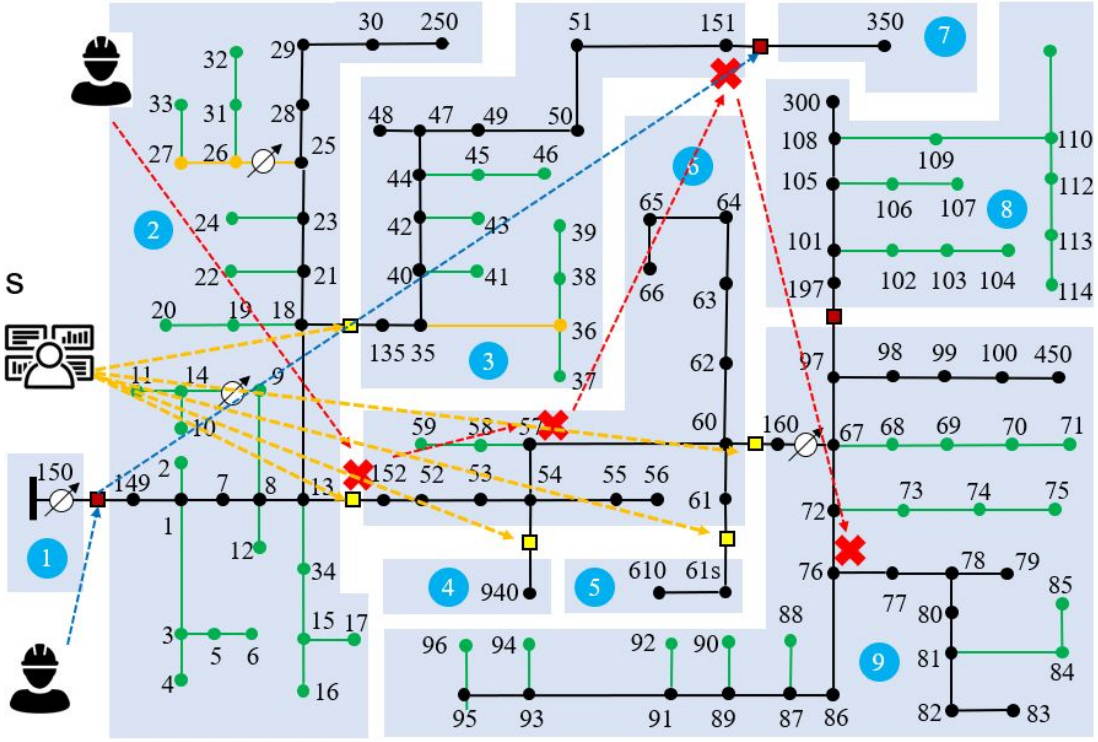
Step 2. Formulate a traveling problem

- All switches are opened automatically to isolate the power failure, forming node blocks
- Identify the damaged components
- Send repair crew to fix the damages
- Send operation crew to operate the switches



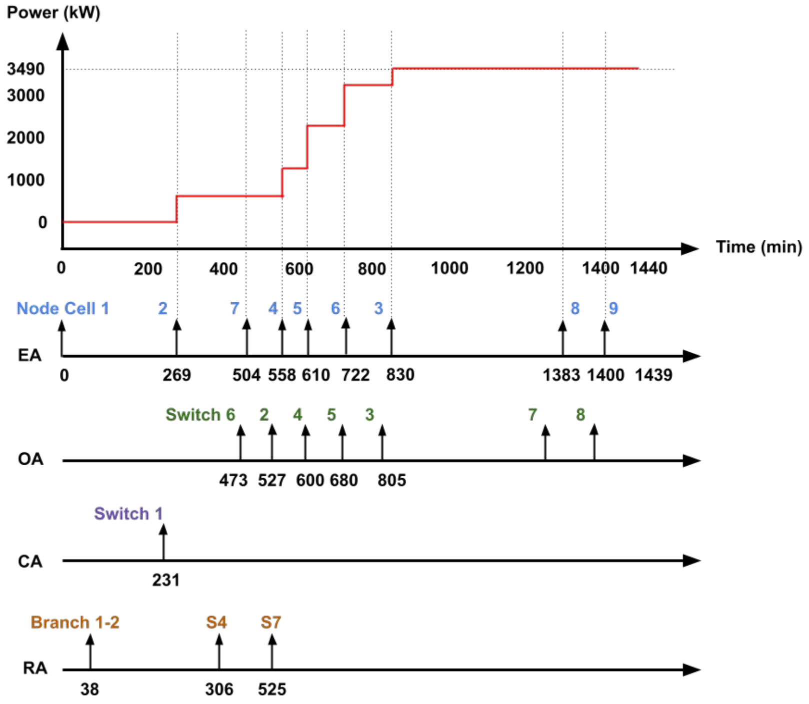
Step 2. Formulate a traveling problem

- All switches are opened automatically to isolate the power failure, forming node blocks
- Identify the damaged components
- Send repair crew to fix the damages
- Send operation crew to operate the switches
- Control center operate the automatic switches remotely



Step 3. Restoration Optimization

- Operation Agent (OA): operating crews that visit and close all the manual switches so that the electricity can flow from an upstream node block to a downstream node block
- Repairing Agent (RA): repair crews that visit multiple damaged components (e.g., damaged loads, switches, and network devices)
- Energization Agent (EA): electricity energization sequence from upstream to downstream node blocks
- Communication Agent (CA): communication flow sequence from one wireless router to another; an automatic switch can only be closed after its associated router has the communication flow



Total restored energy is restored power × duration ("area" of the ladder plot)

Step 3. Restoration Optimization

- Problem formulation
  - Construct *routing matrices* for OA, RA, EA and CA, so that the ***Total restored energy*** is maximized

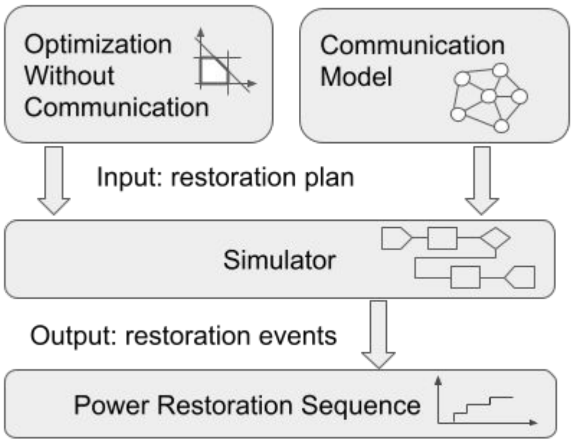
- Constraints:
  - Routing path constraints, power constraints, interdependency constraints

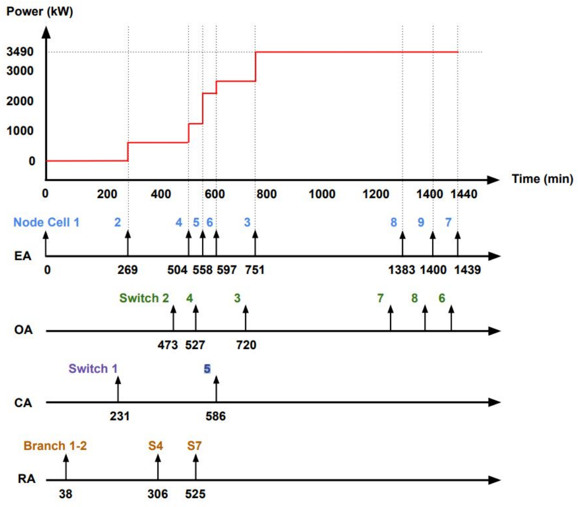
TABLE II: Summary of Interdependent Constraints among Agents

No.	Agents	Constraint
(1)	RA, OA	If a switch is damaged, it needs to be first repaired by RA, then closed by OA.
(2)	RA, EA	If a switch is damaged, node blocks on both ends cannot be energized before it is repaired.
(3)	RA, EA	If a node block contains damaged components, they must be all repaired before energization.
(4)	OA, EA	If EA travels from node block i to j, i is energized either before or after OA closes the switch.
(5)	CA, EA	CA can arrive at a communication node only after EA arrives at the corresponding node block.
(6)	CA, EA	If EA travels through an automatic switch, the switch can be closed only after CA arrives.

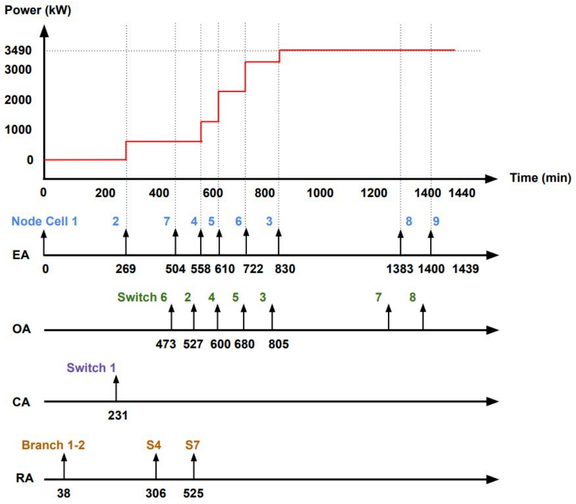
Step 4. Evaluation

- Compare restoration planning with/without interdependency
  - If not coordinate carefully, the utility company has to reroute operation crew to manually operate the remote switches, resulting in *sub-optimal* solutions
- Develop a discrete-event simulator to model such situations
  - Capable to produce the sub-optimal results





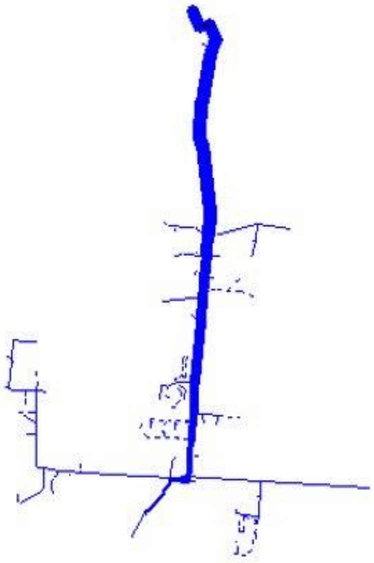
Optimal results from optimization



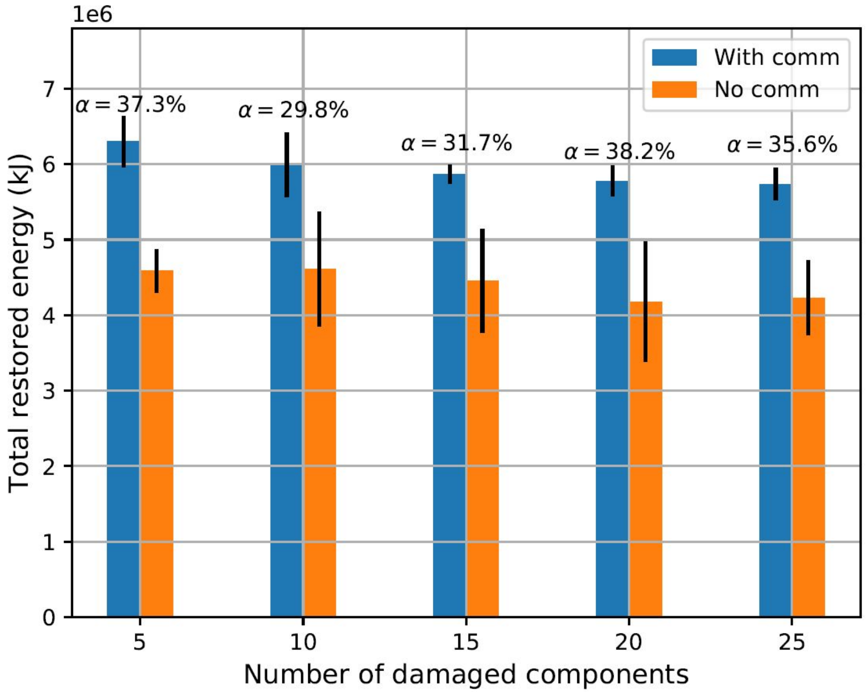
Sub-optimal results from simulation

Step 4. Evaluation

- Ckt7 system for large-scale experiments
  - 2167 buses, 1254 branches, 36 switches



- Total restored energy
  - Increasing number of damages
  - More than 30% improvement



Towards Virtualization of IoT Devices

Motivation: Teaching during the pandemic

Pre-pandemic teaching: focus on real-world experiences

Sudden need to teach online

Can we leverage our research to improve cybersecurity instruction?

A formal methods based platform for cybersecurity education and research

Key approach: expose students to models of devices and interactions

- Leverage our existing research
- Focus: application to IoT

Key missing piece: user interfaces

So we developed:

- UI for building
  - Allows users to drag and drop, and program components
- UI for deployment
  - Implements various environments, e.g., African Savanna

Demo

Conclusions

Building an automated synthesis framework for network security and resilience

Enables new functions: self-driving infrastructures, resilient power grids, teaching and research platforms

Combines formal methods with practical implementations to realize advances in automation, resilience, experimentation, and learning

Contact: caesar@illinois.edu dongjin@uark.edu fanxue2@illinois.edu