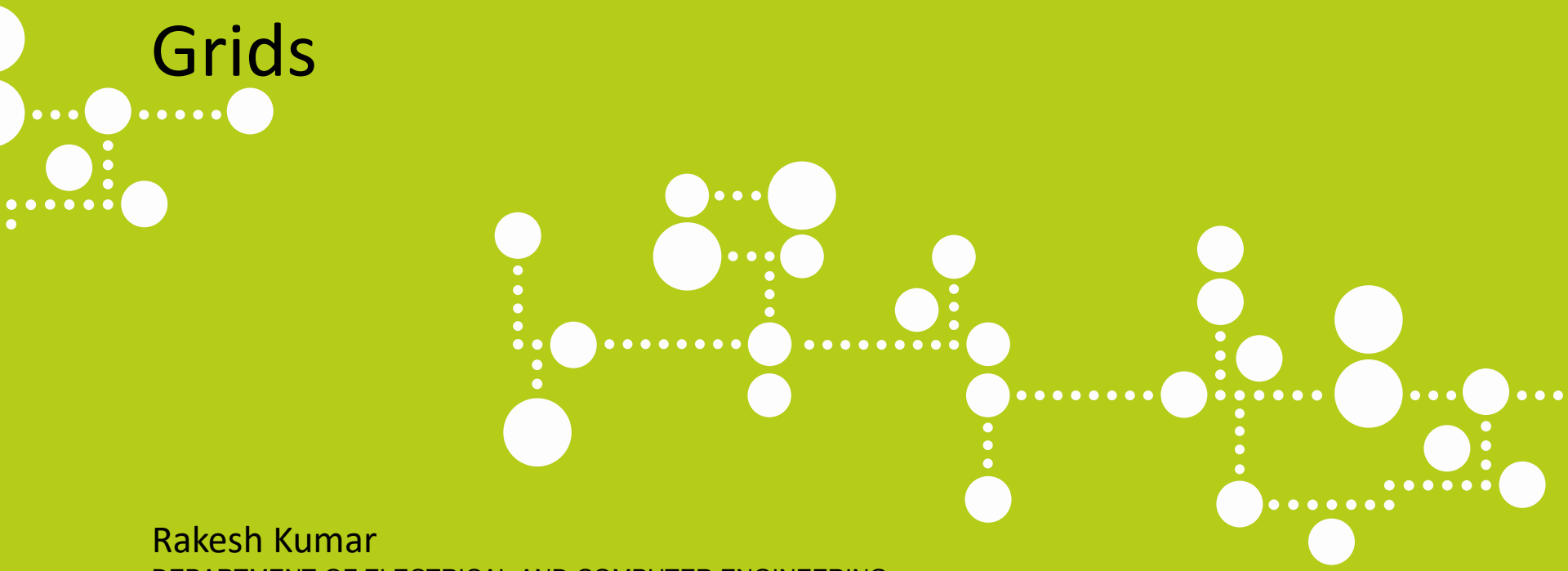
Validating Security and Resiliency in Software Defined Networks for Smart Grids



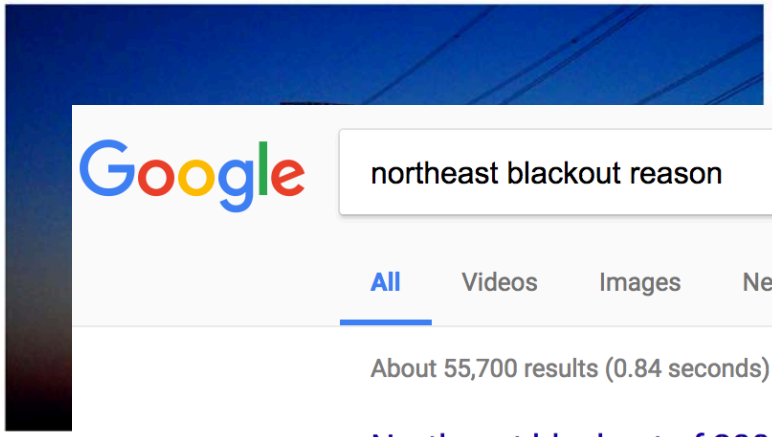
Rakesh Kumar
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
UNIVERSITY OF ILLINOIS, URBANA-CHAMPAIGN

Motivation

RUSSIA

The Ukrainian Power Grid Was Hacked Again

KZ KIM ZETTER
Jan 10 2017, 9:07am



Google northeast blackout reason

All Videos Images News Shopping More Settings Tools

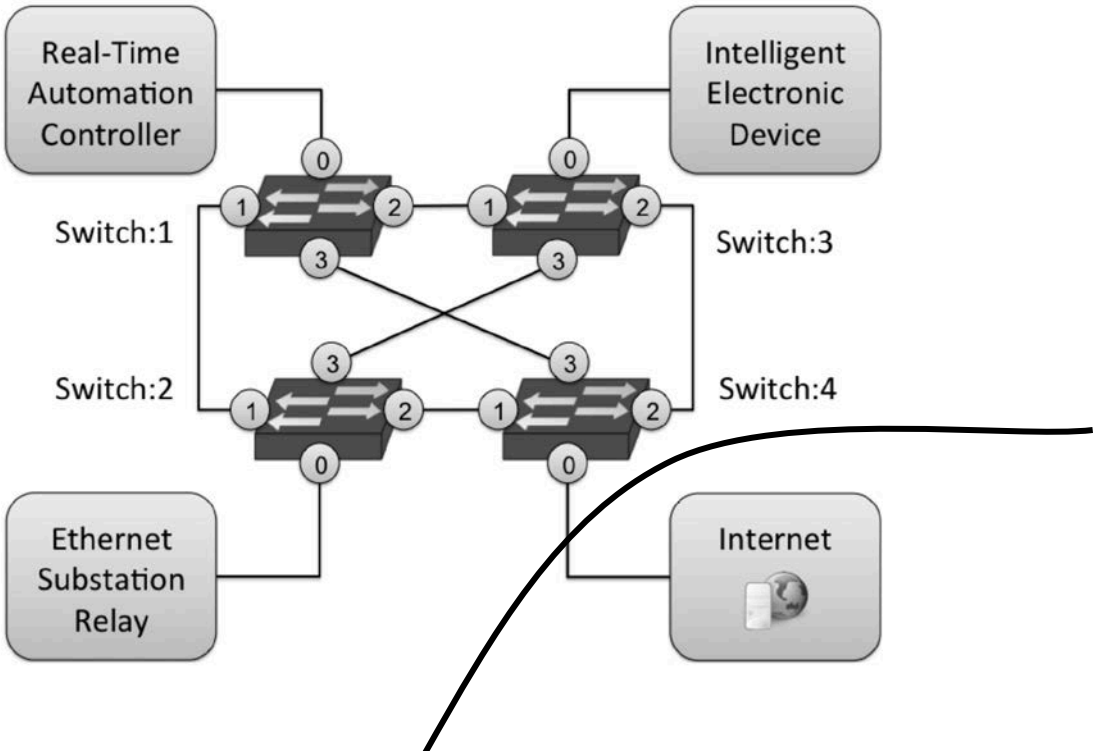
About 55,700 results (0.84 seconds)

Northeast blackout of 2003 - Wikipedia
https://en.wikipedia.org/wiki/Northeast_blackout_of_2003
Jump to **Causes** - **Causes**[edit]. Satellite imagery of the **Northeastern** United States taken before and during the **blackout**.
Northeast blackout of 1965 · Race condition · 1999 Southern Brazil blackout

Expe
cybe

Security: Access Control

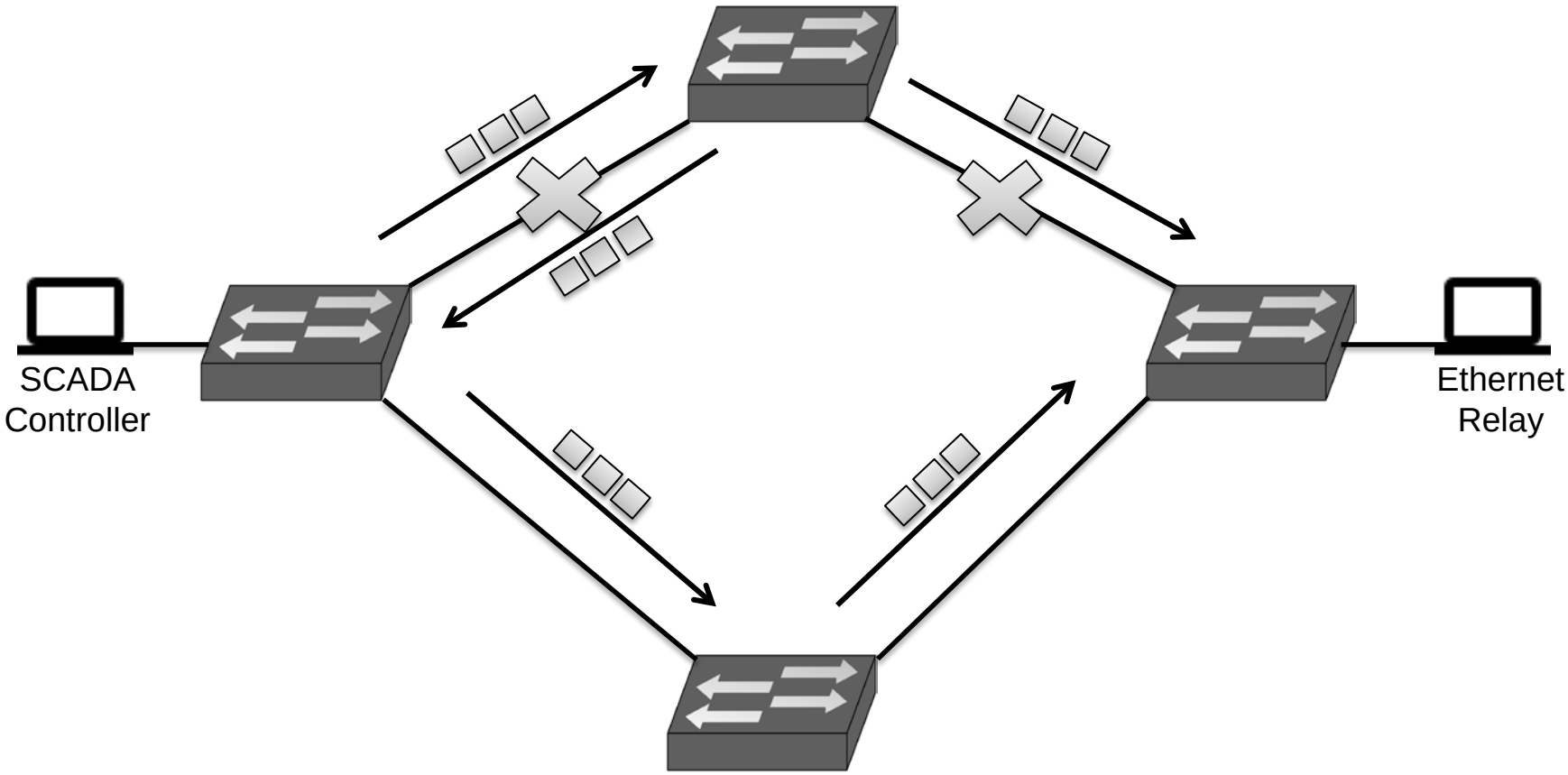
- In United States, power utilities are required to follow NERC CIP Standards.
  - Utilities are periodically audited to secure their Electronic Security Perimeter (ESP)



Resiliency: Link/Device failure

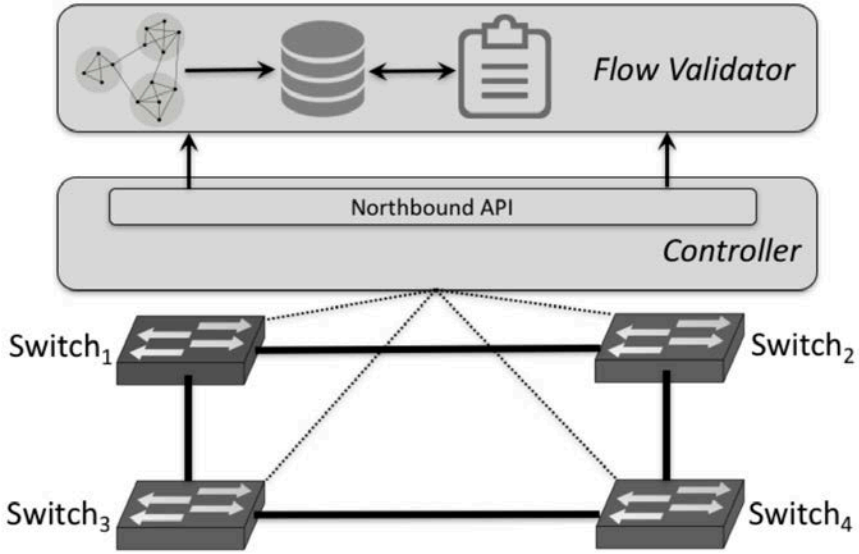
- Upon failure, ask the SDN controller for flow rules
  - Applications may not tolerate the delays incurred
- Flow rules that anticipate failures and take corrective actions to provide *seamless resilience*
  - Fast Failover Mechanism: Designed for small, predictable latency

Resiliency: Illustration

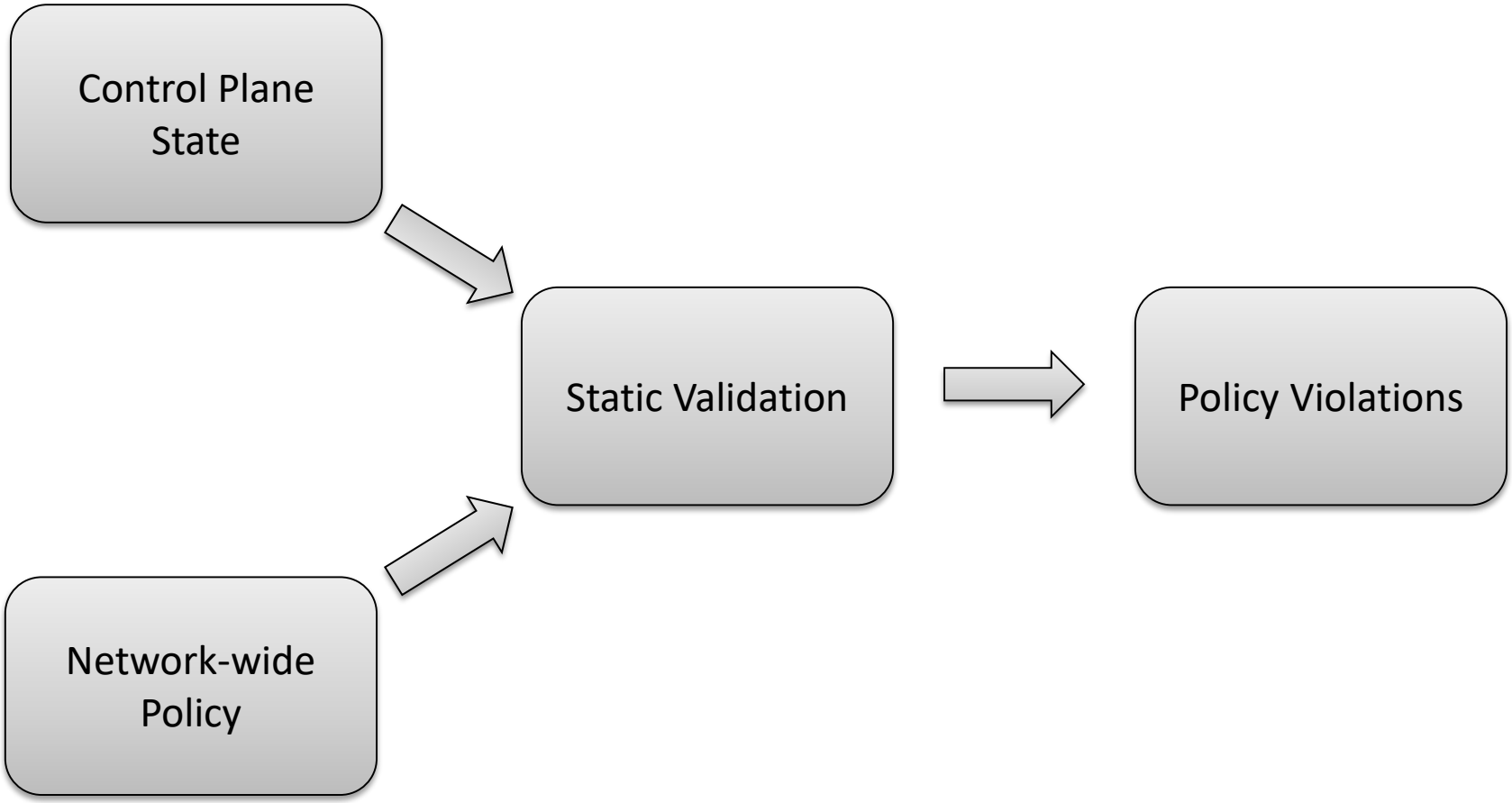


Software Defined Networking (SDN)

- Logically centralized Control Plane State at *Controller*
- Standardized Data Plane in *Switches* and Switch-Controller communication protocol.
- Controller's *Northbound* API enables exhaustive validation.



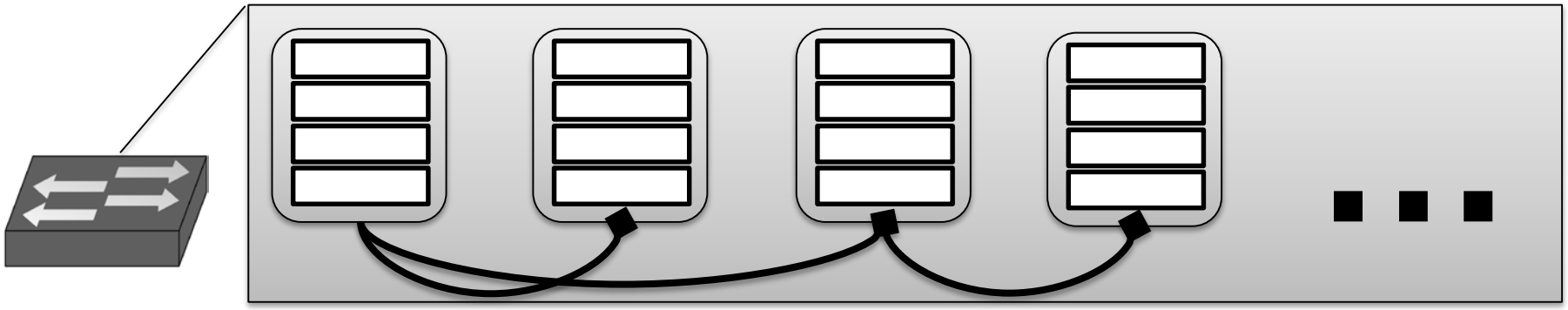
Validation using the SDN Architecture



Rest of the talk:

- Life of a packet
- Resilient Routing Policy (RRP) Specification
- Model
- Design
- Evaluation
- Conclusion and Future Work

Life of a Packet in an OpenFlow 1.x switch

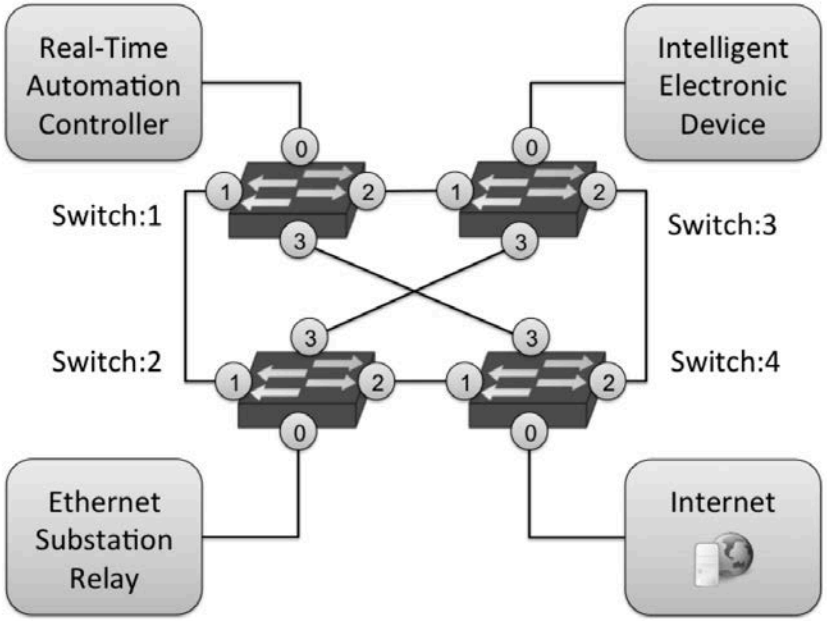


- Flow Table Pipeline
- Flow Rule
  - Match
  - Instructions
    - Single port output, packet header modifications
    - Fast Failover Output: $\{p_1, p_2, p_3 \ldots\}$

Resilient Routing Policy (RRP) Specification

- Zones: Set of ports
- Traffic Set: Packet header field values
- Failure Events: Specific set of link/switch failures
- Constraints: Desired properties, such as:
  - Connectivity
  - Isolation
  - Path Length
  - Link Avoidance

RRP Example



$$z_1 = \{p_{1,0}\} \qquad z_3 = \{p_{4,0}\}$$
$$z_2 = \{p_{2,0}, p_{3,0}\}$$
$$v_1 = \{[-\infty, +\infty]\} \qquad v_2 = \{[443, 443]\}$$
$$t_1 = \{(i_1, v_1) \dots (i_d, v_1)\} \qquad t_2 = \{(i_1, v_2), (i_1, v_1) \dots (i_d, v_1)\}$$
$$c_1 = \{C, L_3\} \qquad c_2 = \{C, A_{\{l_{3,4}\}}\}$$

$$e_1 = \{(l_{1,3}), (l_{3,4}), (l_{4,2}), (l_{2,1}), (l_{1,4}), (l_{2,3})\}$$

$$s_1 = (z_2, z_1, t_1, c_1, e_1) \qquad s_2 = (z_3, z_1, t_2, c_2, \emptyset)$$

$$P = \{s_1, s_2\}$$

The policy specifies that:

- ESR and IED are connected to the RTAC even when any single link fails by a path that traverses no more than three switches in the topology.
- The path of HTTPS traffic from the internet to the RTAC must not cross the link between Switch:3 and Switch:4.

Model

- **Efficiency:** Emphasis on having the capability to perform incremental computation as events occur in the network
- **Composition:** Model for the structure of the network on different levels of abstraction (i.e. switch and network-level)
- **Explicit Representation:** Model for the traffic (set of packet headers) that flows on the network

Port Graph

- The state (topology + configuration) of the SDN is modeled as a directed graph.
- Nodes model places of interest, e.g.
  - Ingress, Egress nodes for physical ports
  - Nodes representing each table
- Each edge *(p, s)* models the transfer of traffic, it has:
  - Edge Filter: *EF(p, s)*
  - Modifications

Admitted Traffic Set (ATS)

- $ATS_{(p,\ d)}$ is the set of packet headers that an SDN is able to carry from node *p* to node *d*.
- $T_{(p,\ d,\ s)}$ is the set of packets that are carried from port *p* to destination *d*, via its successor *s*, thus:

$$T_{p,d,s} = EF_{(p,s)} \cap ATS_{s,d}$$

$$ATS_{p,d} = \bigcup_{s} T_{p,d,s}$$

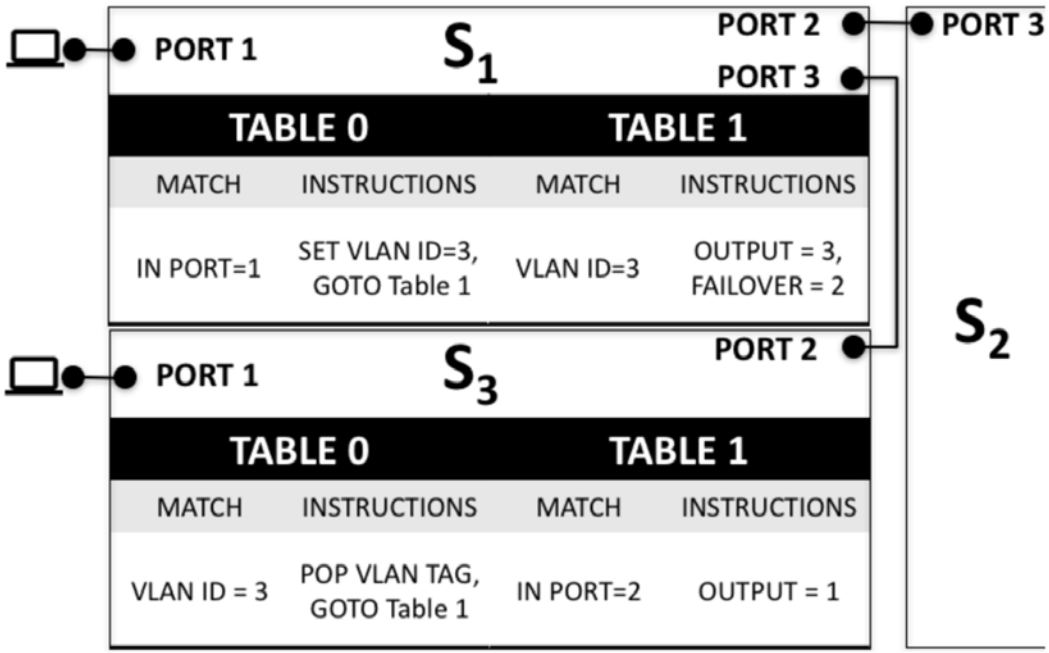
- Incremental analysis made possible by comparing ATS before and after an event:

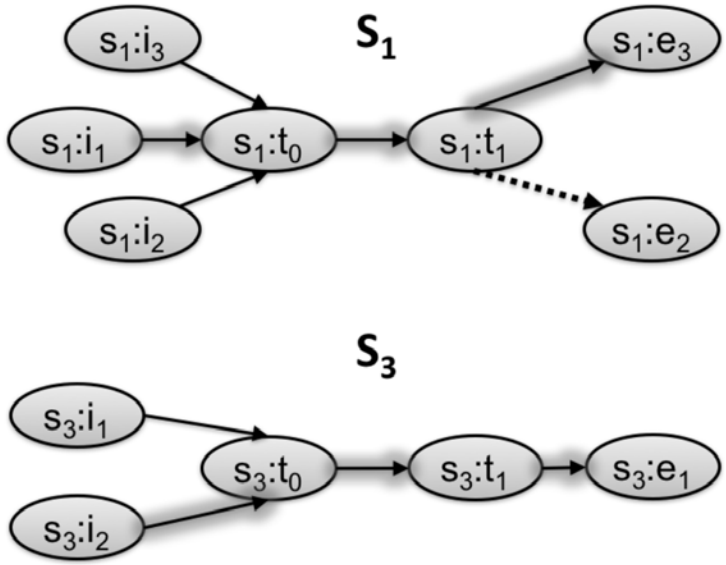
$$ATS'_{c,d} \subseteq \mathrm{ATS}_{c,d} \ \ \& \ \mathrm{ATS}_{c,d} \subseteq \mathrm{ATS}'_{c,d}$$

Design

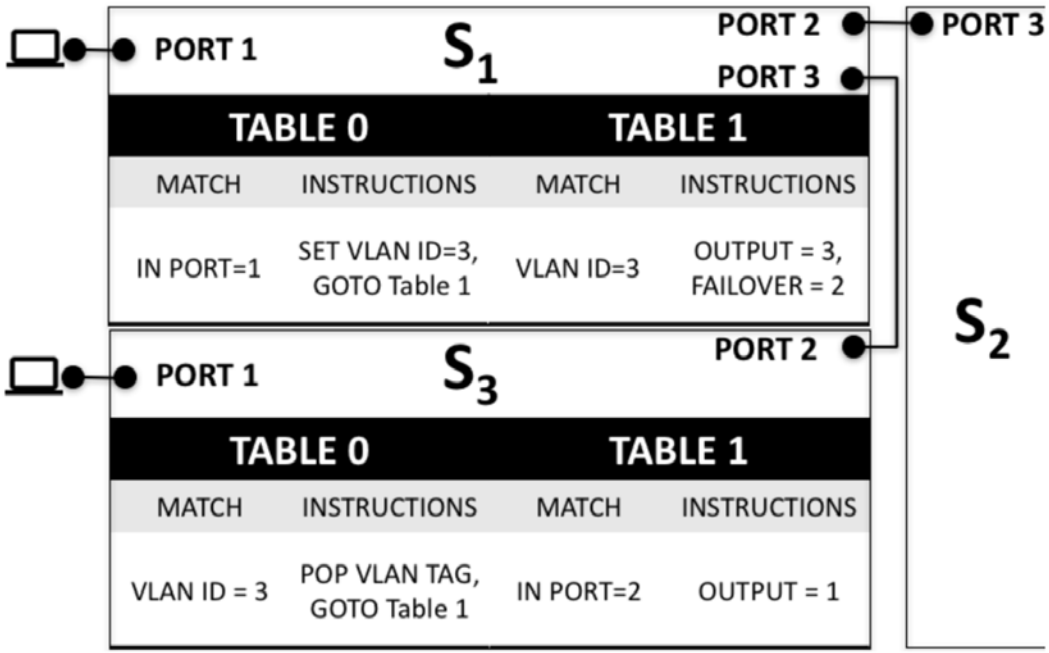
- First, construction of port graphs
- Computation of $ATS_{(p, d)}$ for all *p, d* using a reverse DFS on the port graphs.
- Each edge in the port graph has a flag that represents whether the edge is active based on the current state of the network.

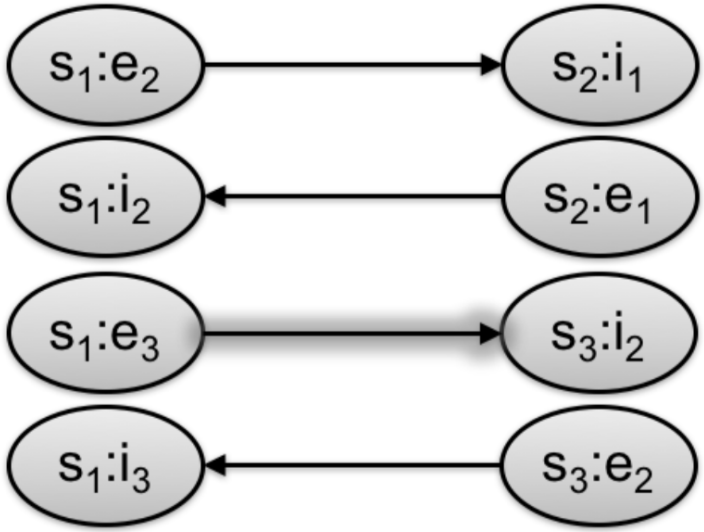
Constructing Switch Port Graphs



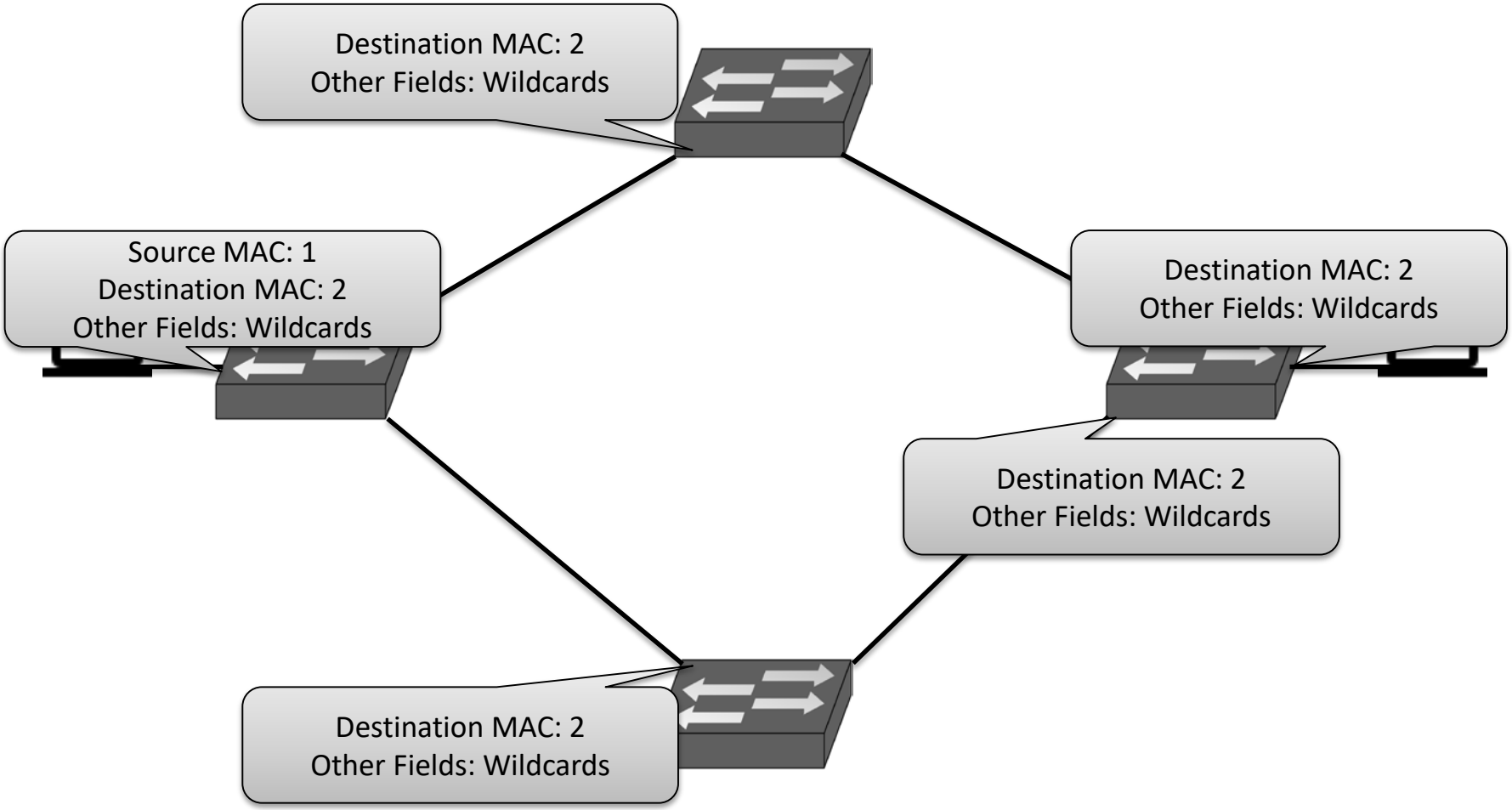


Constructing Network Port Graph





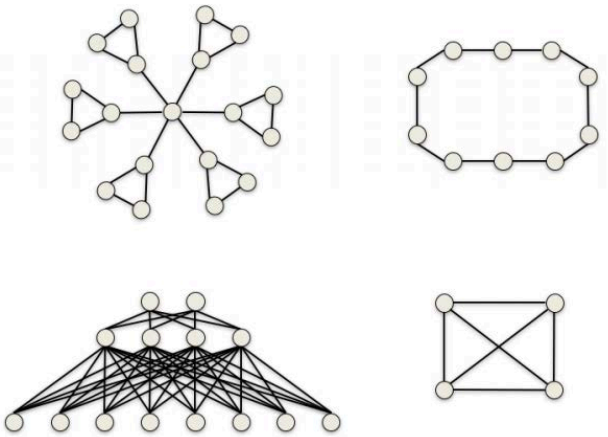
Initializing $ATS_{(p, d)}$



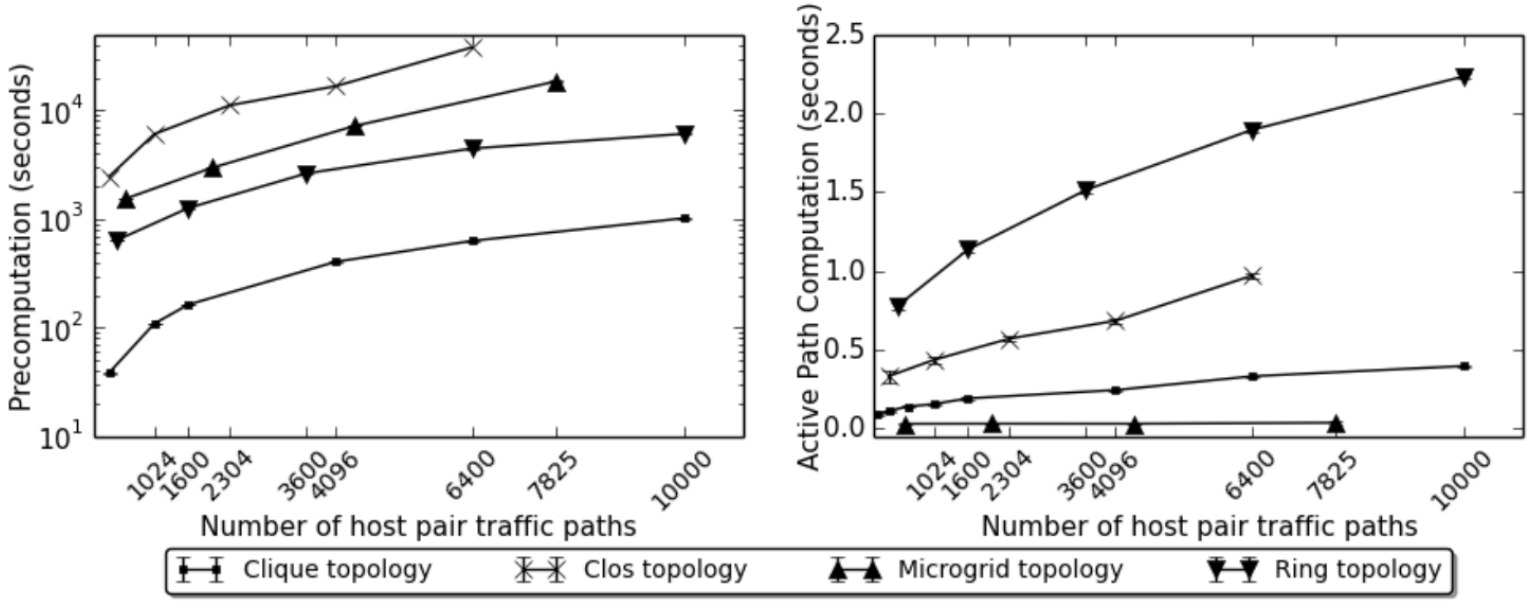
Evaluation Setup

- Experiments performed on a machine running `mininet` and Ryu:
  - Two processor cores at 3.3 GHz
  - 16 GB RAM.
- Ten iterations of each analysis

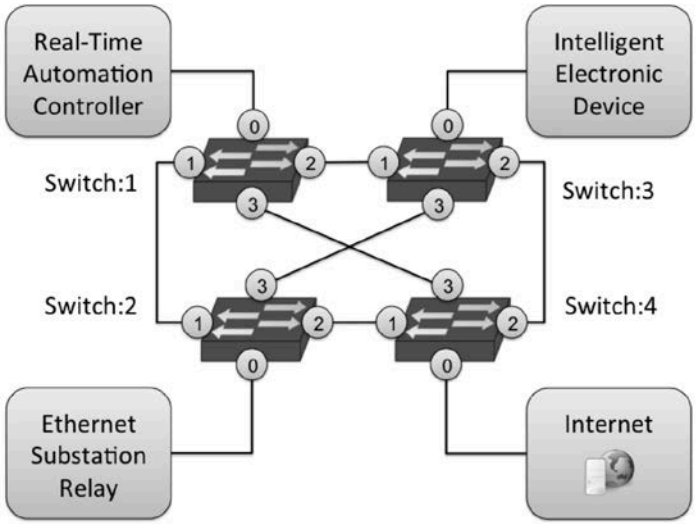
Microbenchmark

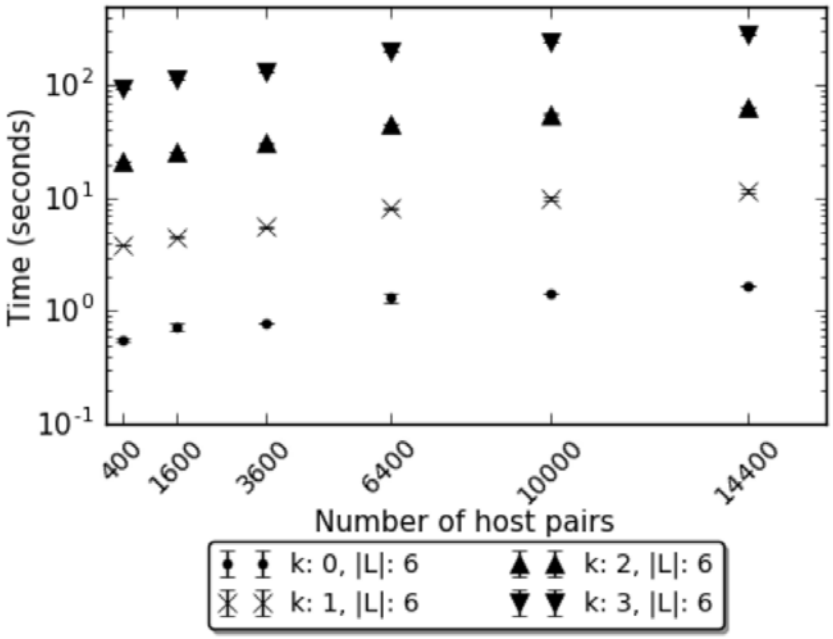


- Flow rules that fast-failover synthesized to sustain failure of a single link
- Policy requires that the path lengths be less than the diameter of the network



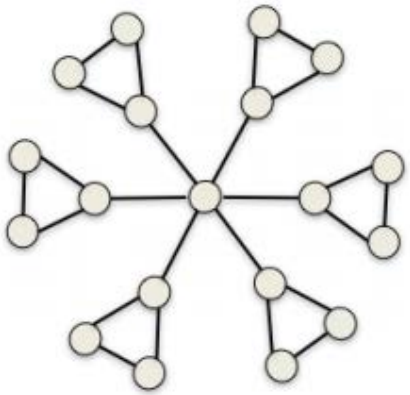
Resilience in a substation network

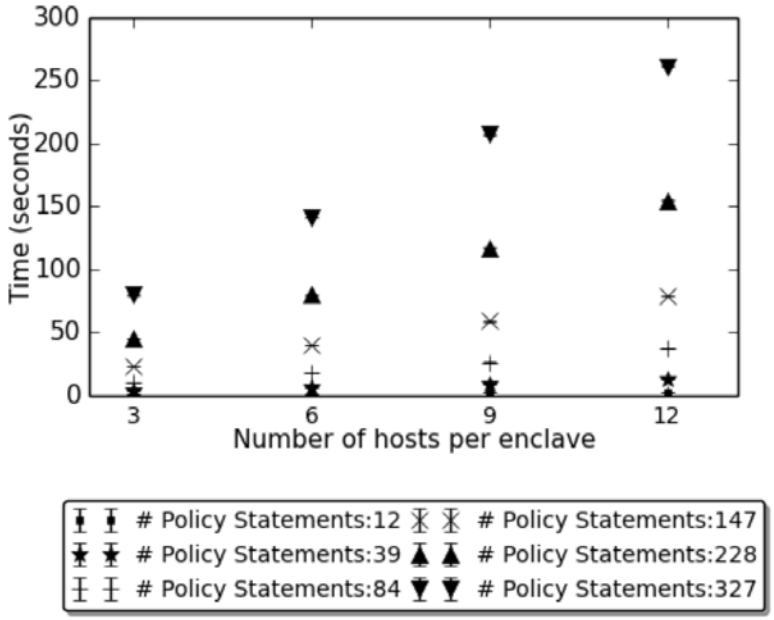




- Same policy as described previously, except the zone sizes keep increasing now

Security for interconnected microgrids





- Six microgrids connecting to a control center
- Network divided in 19 enclaves and a single functional domain
- Policy: Communication only possible within an enclave or functional domain

Conclusion

- A framework for validating resiliency requirements for an SDN by performing exhaustive packet flow analysis
- Model, design of data structures
- Incremental Computation technique provides computational gains
- Scales for larger topology sizes