FMitF Track I

# Specifying and Verifying Network-wide Properties of Dynamic Data Planes

https://www.cs.princeton.edu/~dpw/grants/nsf-fmitf-2219862.html

**Ratul Mahajan**
Univ. of Washington

**David Walker**
Princeton University

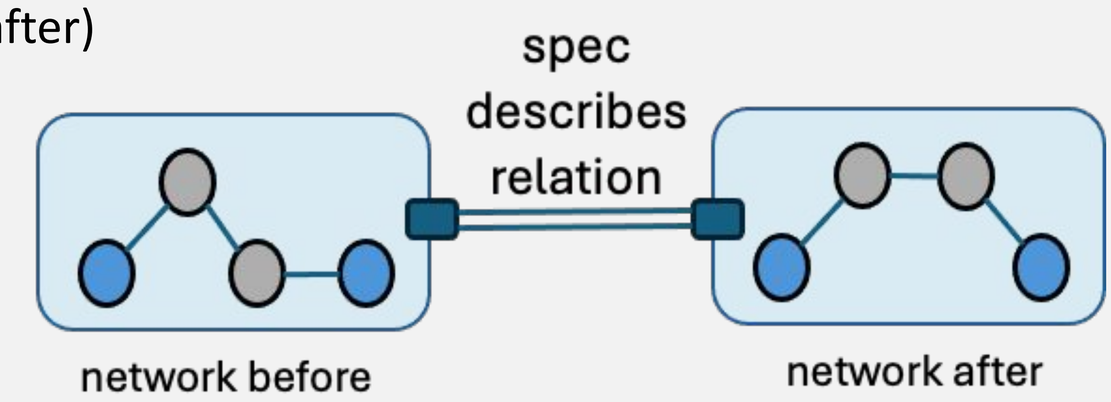
## Problem

**Networks must change**: To add capacity, to patch security holes, to balance load, to react to the environment, etc
**But every change is risky**: Most network outages arise due to changes with unexpected consequences

### Network change validation via relational verification

**Context:** Creating accurate specifications for changes to large networks is impossible the "usual" way because "normal" specs are way too big. But we can't verify changes are correct without specifications!

**Key idea:** Specs about changes should be *relations*--properties of pairs of networks (before and after)




**Solution:** Rela, a network change specification language and checker based on relations

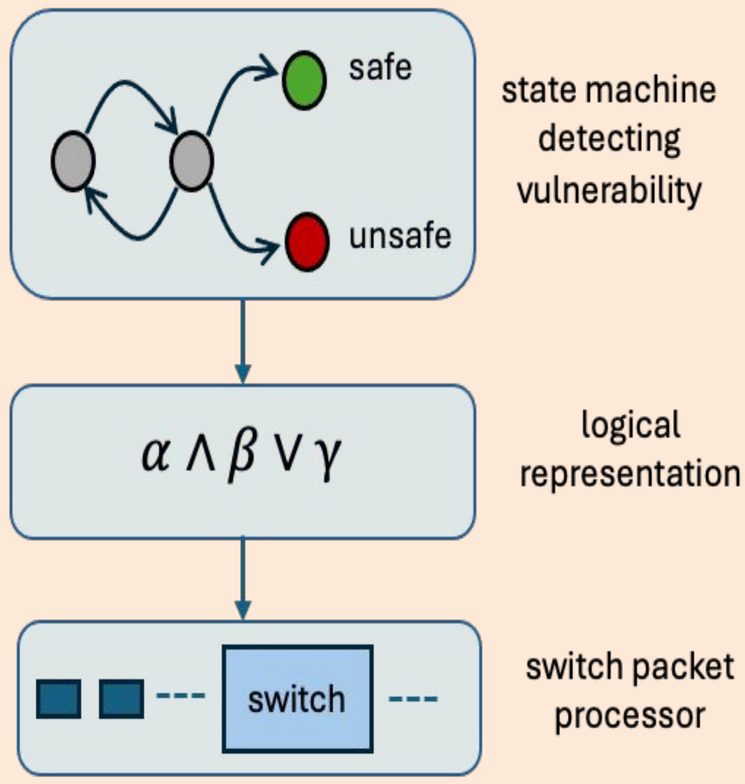
```
// Example: All traffic on link a1 must move to a2
spec change_link = { a1 : replace (a1, a2); }
```

**Result:** 93% of high-risk data plane changes in a global backbone network can be specified by Rela in 10 lines.

### Network monitoring via state machine synthesis

**Context:** Detecting problems often involves monitoring sequences of events. Implementing such monitors by hand is hard due to switch hardware constraints.

**Key idea** Synthesize monitor implementation using logic




**Solution:** A run-time verification method based on synthesizing state machines using logical techniques

**Result:** 5x-10x reduction in program code vs SOTA

## Broader Impact

**Field deployment:** Rela is deployed at a large cloud provider where it validates all complex changes
**Selected publications:**
- Relational Network Verification, *ACM SIGCOMM 2024.*
- Sequence Abstractions for Flexible, Line-Rate Network Monitoring, *USENIX NSDI 2024.*

**Open source software:**
- Rela: https://github.com/alibaba/rela
- Lucid and FLM: https://github.com/PrincetonUniversity/lucid/

**Outreach**
- Talks at Amazon, ACM SIGCOMM FMANO workshop, and APNet
- Blog: https://netverify.fun/network-change-verification-even-for-networks-without-specifications/