Collaborative Research: FMitF: Track I: Specifying and Verifying Network-wide Properties of Dynamic Data Planes (2219862, 2219863)

PIs: Ratul Mahajan (U Washington), David Walker (Princeton)

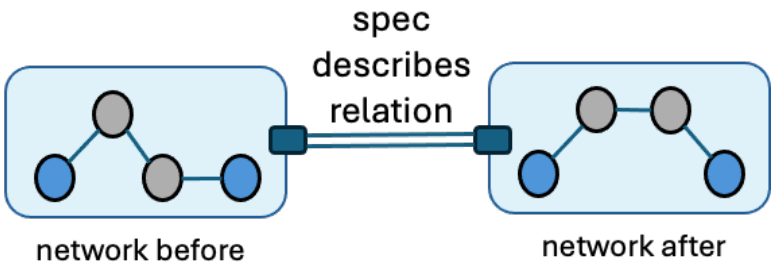
Problem

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

Highlight 1: Relational Verification [SIGCOMM 24]

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)



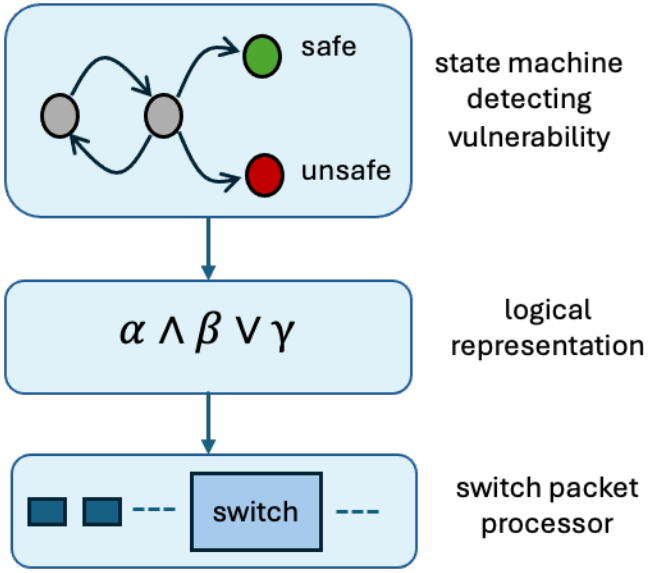
Result: Rela, a new network change specification language and checker based on relations

Result: 97% of high-risk dataplane changes in an industrial network from June 2023-Jan 2024 specified by Rela!

Highlight 2: Synthesizing State Machines [NSDI 24]

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 SMT



Result: A new run-time verification method based on synthesizing state machines using logical techniques

Result: 5x-10x reduction in code vs state-of-the-art!