A new paradigm for network simulations; model-checking meets event simulation

Taghrid Samak[1], Adel El-Atawy[2], Dan Gunter[1]

1 Lawrence Berkeley National Laboratory

2 Google Inc.

The Model

Unified model

- Set theory
- Boolean representation

Model-checking

- States and transitions
- Property verification

Problem Evolution

Single firewall analysis

- Anomalies, misconfigurations, etc

Packet decision for a single policy

- Optimization, rule caching, rule reordering, etc.
- Firewall "gray-box" testing

Policy equivalence

- NP-Hard, but easy !!!

Multi-firewall anomaly analysis

Multi-device/type analysis

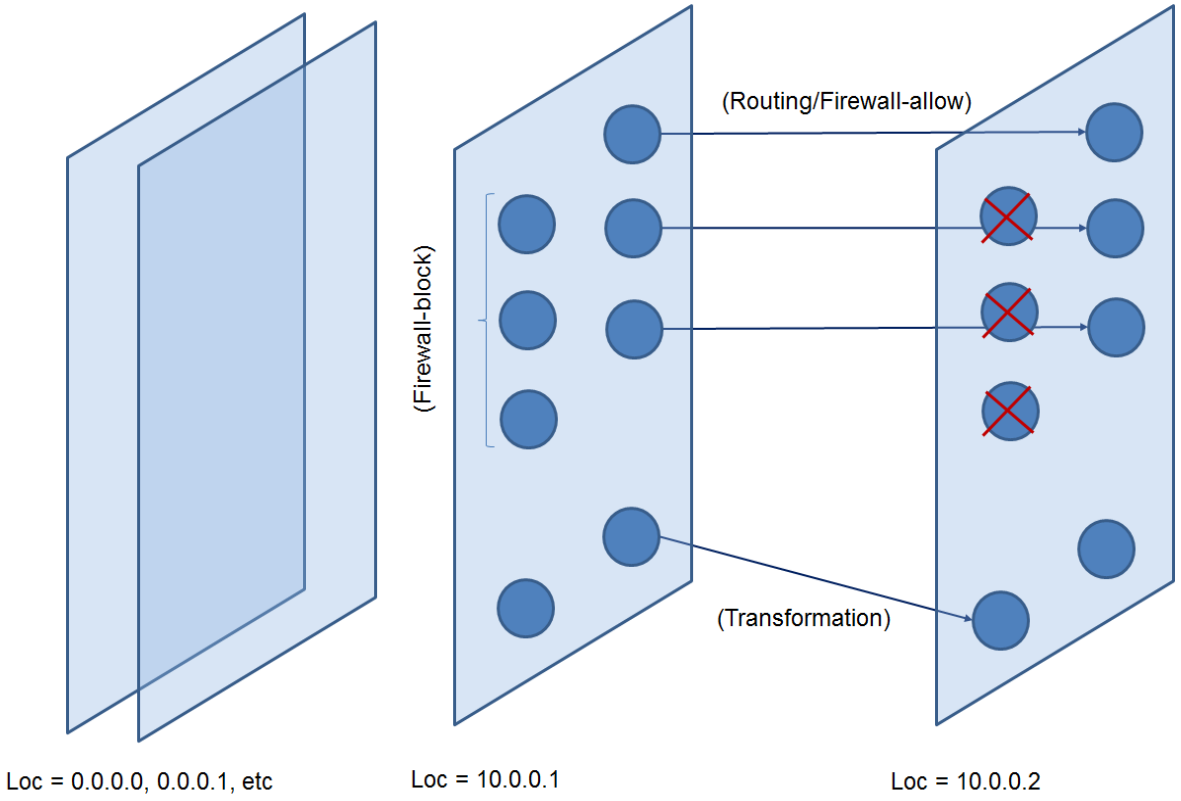
- Model checking on the device-level (BDD+CTL)
- Model checking on the rule level (SAT+LTL)

Multi-device/type with QoS analysis

Network Model

Transitions represent valid moves from a state to state according to device definition, and policies in place.

“Most” states have a single outgoing edge (i.e., deterministic state machine).



Closing the Gap

Model-checking steps as events

Simulating multiple scenarios simultaneously

What-if scenarios

Application-centered design

Future Directions

Parallel model-checking platforms

Parameter selection and tuning

Decentralization of the simulation

Probabilistic modeling

Data-driven verification

Discussion!