FSR: Formal Analysis & Implementation Toolkit for Safe Inter-domain Routing

Wenchao Zhou
University of Pennsylvania

Collaboration work with Anduo Wang, Yiqing Ren, Limin Jia, Alexander J.T. Gurney, Boon Thau Loo and Jennifer Rexford
Introduction

- Today’s Internet routing system (BGP) does not guarantee convergence (safety)
  - Policy configuration largely affect the behavior of BGP
  - Oscillations cause serious performance disruption

- Limitations of current approaches
  - Formal theories: Manual proofs or counter-examples
  - Distributed implementation: Simulations for study protocol overhead and transient behavior during protocol execution

- Goal of FVR: Bridging the formal theories and distributed implementation
Architecture (10,000 feet)

- Input: policy configurations (as algebra)
  - Examples: Gao-Rexford guideline [SIGMETRICS 00], hop-count
- Formal side: Safety analysis results
- Practical side: Distributed implementation
Policy as Routing Algebra

- **An abstract structure** \( \langle \Sigma, L, <, \oplus \rangle \)
  - \( \Sigma, L \) describe route and link attributes
  - \( \oplus \) specifies how to compute new routes
  - \( < \) determines how to compare routes

- **Gao-Rexford Guideline**

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Algebra instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Sigma )</td>
<td>Business relationship: customer, peer, provider</td>
</tr>
<tr>
<td>L</td>
<td>Business relationship between neighboring ASes</td>
</tr>
<tr>
<td>&lt;</td>
<td>Prefer customer (C) over peer(R) / provider(P)</td>
</tr>
<tr>
<td>( \oplus )</td>
<td>How a new route attribute depends on existing routes and links; and whether a node exports/imports certain classes of routes</td>
</tr>
</tbody>
</table>
Contribution #1: Reduction from safety analysis to SMT solving

- Strict monotonicity (SM) implies safety [SIGCOMM 03, 05]
- Convert policy configuration into Yices (SMT solver) constraints
- Check if the constraints are satisfiable
Contribution #1: Reduction from safety analysis to SMT solving

Output: Safety analysis result

- SAT – automatically generated proofs
- UNSAT – an unsatisfiable core (pinpoint configuration errors)
Contribution #2: Provably correct distributed implementation

- Generalized path vector + policy configuration
- Generation of *Declarative Networking* program [SIGCOMM 05]
- Correctness proof for the policy -> NDlog translation
Demo: GR + HopCount
Demo: GR + HopCount
Demo: GR (wrong) + HopCount
Demo: Pinpoint Mis-configuration
Summary

- Bridging formal theories and implementation
  - Unified policy specifications (based on routing algebra)
  - Automated safety analysis (reduced to constraint solving)
  - Provably correct distributed implementations
Thank you...

FSR: Formal Analysis & Implementation Toolkit for Safe Inter-domain Routing

http://netdb.cis.upenn.edu/fvr/