Automating SDN Policy Composition — A Database Perspective

Anduo Wang
Temple University

Jason Croft
University of Illinois Urbana-Champaign

motivation

forming a correct modular composition is still challenging, relies on human operators for
- understanding of module internals
- inter-module interactions depending on traffic context
- automating SDN composition with database reasoning

example input (modules \(fw\), \(lb\), \(rt\))

\[ \text{clients} \{ H_1, H_2 \} \]
\[ \text{firewall} \{ FW \} \]
\[ \text{load balancer} \{ LB \} \]
\[ \text{servers} \{ S_1, S_2 \} \]

\(fw\), firewall blocks traffic from/to \(H_2\)
\(lb\), load balancer directs \(H_1\) traffic from/to \(S_1\)
\(rt\), routing between \(H_1\) and \(S\)

a manual composition

\(fw\) filters client traffic before \(lb\) and \(rt\)
\(lb\) restores returning traffic’s public address before \(lb, rt\)

\[ \text{if}_e (ec, lb_1, lb_2) \text{ where } \begin{align*}
lb_1 & = src=H_1 \land dst=S_1 \land pt=1 \\
lb_2 & = src=S_1 \land dst=H_1 \land src=pt=1
\end{align*} \]

correctness criterion

a composite is correct if it preserves semantics of member modules

stratified dependency graph

- compute for each module \(x\) a stratification number \(sn(x)\)
  \[ sn(x) = \max\{(sn(y) \mid y \text{ is a parent of } x \text{ in } D) \} + 1 \]

- modules with equal \(sn\) are composed in parallel
- modules with unequal \(sn\) are composed sequentially

\[ \forall u,v,y \in D, sn(u) = sn(v) + 1 = sn(x) = sn(y) \]

compute for each module \(x\) a stratification number

- modules with equal \(sn\) are composed in parallel
- modules with unequal \(sn\) are composed sequentially

\[ \forall u,v,y \in D, sn(u) = sn(v) + 1 = sn(x) = sn(y) \]

dependency synthesis

- model SDN modules as database query/update
- a control loop of (check, repair)

behavioral dependency
- \(x\) depends on \(y\) \(\langle x \rightarrow y \rangle\) if
- \(x\) can violate \(y\) invariant and trigger \(y\) action

database irrelevance reasoning
- update \(\Delta_x\) is relevant to query \(i_x\) if \(\Delta_x \land i_x\) is SAT
- \(\Delta_y\) is irrelevant to \(i_x\) if \(\Delta_y \land i_x\) is UNSAT

reasoning for \(lb_2 \rightarrow fw\)

\[ \theta[S, H_1] = S = S \land H_1 = H_1 \text{ is SAT} \]

- reachability \(\_S, H_1\)
- reachability \(\_S, H_1\)

- reachability \(\_S, H_1\)

Acknowledgment

This material is based upon work supported by the NSF Grant CNS 1657285

http://ravel-net.org/