vCRIB: Virtualized Rule Management in the Cloud
Masoud Moshref, Minlan Yu, Abhishek Sharma, Ramesh Govindan
Department of EE/Computer Engineering Group

Motivation: Cloud rule management is hard
- Many fine-grained rules for various management tasks (e.g., access control, customized routing)
- Need to manage rules at both switches and hosts

<table>
<thead>
<tr>
<th>Position</th>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Complex rules</td>
<td>CPU usage → decrease revenue</td>
</tr>
<tr>
<td></td>
<td>Knowledge of VMs</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Optimized HW</td>
<td>Limited TCAM size</td>
</tr>
<tr>
<td></td>
<td>Knowledge of network</td>
<td></td>
</tr>
</tbody>
</table>

Overlapping Rules
S1: SrcIP=10.0.0.0/16, DstIP=10.0.0.0/16, Rate limit
S2: SrcIP=10.0.0.0/8, DstIP=10.0.0.0/8, Deny
- Loading/removal dependency of overlapping rules
- Solution: Partition the space

Resource Assignment
- Constraints
  - CPU
  - Memory
  - Functionality
- Goal
  - Traffic
  - Cost

Partition and Placement
- Handling overlapping rules with partitions
  - BSP Tree:
    - Recursively cut the space and create the tree
    - Stop when the number of rules reach the total network memory
    - Trade-off between balance and split rules for the position of cut: F=α×max_{p}S(p) + (1−α)×N.
- Placing partitions with resource constraints
  - DFS Branch and Bound: Place the largest unassigned partition on the position with minimum traffic overhead

Evaluation Results
- vCRIB is efficient in placing rules using provided resources
  - Larger network capacity → Smaller partitions
  - Smaller partitions → more flexibility in placement → less traffic overhead
  - Aggregatable source IP addresses for VMs on each hypervisor (Agg setting) → less traffic overhead

moshrefj@usc.edu