Monitoring significant traffic on networks

Motivation

- help operators understand how the network is used and allocate resources efficiently
- implement monitoring tool using routers already in the network, so "network elements monitor themselves"

What the CS department’s network operator want to know about the network traffic...

- 40% is Alice downloading files from x.ac.edu
- 10% is the small Systems group browsing the web
- 10% is Alice’s mother in the Systems group browsing the web.

Related work

assumes specialized hardware that can make new rules for every incoming packet, or call the control plane to prune insignificant prefixes every 100 packets...

but we’re constrained to:
- fetching counts, making new rules only as frequently as every 10 seconds (~10K packets)
- available hardware

so we relax the tight accuracy bounds...

Concise but complete summary

Maps well to hardware...

Results

Evaluation Setup
- 2 sets of packet traces from high-speed links
- Monitoring interval: 50 seconds
- Threshold: 10%

Fast discovery
- for constant traffic, takes 2.5-10 seconds to find IBH

Fast adaptation
- for changing traffic, takes 14-100 seconds, interval until number of new IBH per interval drops to 1/10 (one to actual value)

Fewer rules - 5 times as much power saved
- Even after most powerful, we use at most 64

From here

extend to multidimensional
- actually implement on OpenFlow
- look for better algorithms
- use machine learning to identify likely heavy hitters early

My internship...

exciting, enlightening first research experience
- cutting-edge network monitoring
- make the best of what's there
- network research, OpenFlow

A big thank you to my mentor Professor Jennifer Rexford, my office-mate Alex Fabrikant and my PEI co-intern Dana Butnaris! 
Monitoring significant traffic on networks

-Lavanya Jose

Advised by Professor Jen Rexford, Computer Science, Princeton University
Motivation

- help operators understand how the network is used- and allocate resources efficiently

- Implement monitoring tool using routers already in the network, so "network elements monitor themselves"
What the CS department's network operator want to know about the network traffic.

- 40% is Alice downloading files from xyz.edu
- 10% is the small Graphics group browsing the web
- 10% is Alice's mates in the Systems group browsing the web.
How we could help the operator ...

store all raw data - expensive to collect, and even process (for us!)

choose cautiously what to store for a concise but complete summary
concise but complete summary

- heavy hitters (000*, 100*)
- heavy hitter prefixes
- hhh (000*, 01*, 100*, 1*)
maps well to hardware...

<table>
<thead>
<tr>
<th>Prefix</th>
<th># packets seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>000*</td>
<td>35</td>
</tr>
<tr>
<td>.01*</td>
<td>10</td>
</tr>
<tr>
<td>100*</td>
<td>40</td>
</tr>
<tr>
<td>1*</td>
<td>10</td>
</tr>
</tbody>
</table>
related work

assumes specialized hardware that can make new rules for every incoming packet, or call the control plane to prune insignificant prefixes every 100 packets...
so they can provide tight accuracy bounds

but we're constrained to

- fetching counts, making new rules only as frequently as every 10 seconds (~10K packets)
- available hardware
so we relax the tight accuracy bounds...
method
EaC with similar setting but monitors all heavy hitter prefixes (in orange), we monitor just the HHH kids (in green), and readjust
Results
Evaluation Setup:
2 sets of packet traces from hi-speed links
Monitoring Interval: 10 seconds
Threshold: 10%

Fast discovery
for constant traffic takes 4-5 ten-second intervals to find HHH

Fast adaptation
for changing traffic takes 12-14 ten second intervals until number of new HHH per interval drops to 2-3 (close to actual value)

Fewer rules- 5 times as much power saved
EaC uses at most 320 rules, we use at most 64
From here

extend to multidimensional
actually implement on OpenFlow
look for still better algorithms
use machine learning to identify likely heavy hitters early
My internship...

exciting, enlightening first research experience
cutting-edge network monitoring
make the best of what's there
network research, OpenFlow
IW
A big thank you to my mentor Professor Jennifer Rexford, my office-mate Alex Fabrikant and my PEI co-intern Dana Butnariu!