Network Measurements and Sampling

Nick Duffield, Carsten Lund, and Mikkel Thorup

AT&T Labs-Research, Florham Park, NJ
IP Network

The Edge of Network

Links

Routers
Some Questions that are hard to answer about IP networks

- Given a hotspot, how do we change network configuration to fix the problem.
  - What exactly is the problem? Type of traffic?
- Traffic usage. Which applications are using the network?
- How do we design an efficient network?
  - Where do the traffic want to go?
Traffic Matrix Construction

- **Traffic Matrix**
  - Point to Point Demands
  - Point to Multi-Point Demands
    - Needed to model in networks with multi-homing and peering. (e.g., ISPs etc.)

- **Input for many tasks**
  - Network Design
  - Reroute traffic
  - Failure analysis
  - OSFP weight optimization (Thorup et al.)
Measurement Options

- SNMP
  - Counting packets on interfaces
- Packet sniffers/Probes
  - Whole packet header/contents
- Flow measurements
  - Router support
  - Network-wide measurements
- Packet sampling (sFlow)
- Trajectory sampling
- Etc.
Traffic Matrix: SNMP based methods

- Network Tomography
  - From link measurement determine traffic matrix, using temporal correlations.

- Network Tomogravity
  - Starts with a model of the traffic matrix from edge measurements.
  - Uses internal measurements to find a consistent solutions that is close to the traffic matrix that the model predicted.
Traffic Matrix: Flow based methods.

- Detailed measurement where the traffic enter and determine from the destination IP address, where the traffic will exit the network
  - Need Prefix level routing information to determine the exit point
Traffic Matrix: Method Comparison

- **SNMP based**
  - Less accurate
  - Harder to deal with multi-point destinations
    - Tomography do not.
    - Tomogravity do try to model it.
  - Measurement instrumentation/gathering is standard.

- **Flow based**
  - More accurate
  - Deal with the multi-point destinations
  - Measurement instrumentation/gathering is not standard.
  - Need to deal with huge amount of detailed measurements
Outline of the rest of the talk

- **Context**
  - What are Flows?
  - Measurement Infrastructure

- The main idea
  - Size dependent sampling
  - Optimal sampling

- How do this compare to size independent sampling?

- Billing application
IP Flow Abstraction

- **IP flow abstraction**
  - set of packets identified with “same” address, ports, etc.
  - packets that are “close” together in time

- **IP flow summaries**
  - reports of measured flows from routers
    - flow identifiers, total packets/bytes, start and end times

- Several flow definitions in commercial use
Collection System

Routers

Flow Collectors

Central Server

Flow Data
Aggregate Data
Resources in the Measurement System
Measure/Export All Traffic Flows?

- Flow volumes
  - one OC48 (2.4 Gbps Trunk) ⇒ several GB flow summaries per hour

- Cost
  - network resources for transmission
  - storage-processing at the collection system
Flow Sampling?

- **Sampling**
  - statisticians reflex action to large datasets

- **Export selected flows**
  - reduce transmission/storage/processing costs

- **Sufficiently accurate?**
  - Depends on application.
    - Traffic Engineering (where do traffic flow)
    - Traffic Analysis (application usage, etc.)
    - Billing
      - risk of overcharging (⇒ irate customers)
      - risk of undercharging (⇒ irate shareholders)
Packet Sampling and Flow Sampling

- **Packet Sampling**
  - when router can’t form flows at line rate
    - scaling at a single router

- **Flow sampling**
  - managing volume of flow statistics
    - scaling across downstream measurement infrastructure

- **Complementary**
  - could combine
    - e.g. 1 in N packet sampling + flow sampling
Usage Estimation

- Each flow $i$ has
  - "size" $x_i$
    - bytes or packets
  - "color" $c_i$
    - combination of IP address, port, ToS etc that maps to billable stream (= customer + billing class)

- Goal
  - to estimate total usage $X(c)$ in each color $c$

$$X(c) = \sum_{i: c_i = c} x_i$$
Basic Ideas

- **Match sampling method to flow characteristics**
  - high fraction of traffic found in small fraction of long flows
    - sample long flows more frequently than short flows
      - large contributions to usage more reliably estimated

- **Show how to relate sampling and accuracy**
  - simple rules to achieve desired accuracy
Size independent flow sampling bad

- Sample 1 in N flows
  - estimate total bytes by N times sampled bytes

- Problem:
  - long flow lengths
    - estimate sensitive to inclusion or omission of a single large flow
Size dependent flow sampling

- Sample flow summary of size $x$ with prob. $p(x)$
- Estimate usage $X$ by

$$X' = \sum_{\text{sampled flows}} \frac{x}{p(x)}$$

  - boost up size $x$ by factor $1/p(x)$ in estimate $X'$
    - compensate against chance of being sampled

- Chose $p(x)$ to be increasing in $x$
  - longer flows more likely to be sampled
  - compare size independent sampling: $p(x) = 1/N$
Statistical Properties

- Fixed set of flow sizes \{x_1, x_2, \ldots, x_n\}
  - we only consider randomness of sampling

- \(X'\) is unbiased estimator of actual usage \(X = \Sigma_i x_i\)
  - \(\Rightarrow X' = X\): averaging over all possible samplings
  - holds for all probability functions \(p(x)\)

Proof:

- \(X' = \Sigma_i w_i x_i / p(x_i)\)
  - \(w_i\) random variable
    - \(w_i = 1\) with prob. \(p(x_i)\), 0 otherwise
  - \(\Rightarrow w_i = p(x_i)\) hence \(\Rightarrow X' = \Rightarrow \Sigma_i w_i x_i / p(x_i) = \Sigma_i x_i = X\)
What is best choice of $p(x)$?

- Trade-off accuracy vs. number of samples
- Express trade-off through cost function
  - $\text{cost} = \text{variance}(X') + z^2 \text{average number of samples}$
    - parameter $z$: relative importance of variance vs. # samples
- Which choice of $p(x)$ minimizes cost?
  - $p_z(x) = \min \{ 1, x/z \}$
    - flows with size $\geq z$: always selected
    - flows with size $< z$: selected with prob. proportional to their size
- Trade-off
  - smaller $z$
    - more samples, lower variance
  - larger $z$
    - fewer samples, higher variance
- Will call sampling with $p_z(x)$ “optimal”
Optimal vs. size independent sampling

- NetFlow traces
  - 1000’s cable users, 1 week
- Color flows
  - by customer-side IP address c
- Compare
  - 1 in N sampling
  - optimal sampling
    - same average sampling rate
- Measure of accuracy
  - weighted mean relative error
    \[
    \frac{\sum_c |X'(c) - X(c)|}{\sum_c X(c)}
    \]
- Heavy tailed flow size distribution is our friend!
  - allows more accurate encoding of usage information
Charging and Sampling Error

- **Optimal sampling**
  - no sampling error for flows larger than \( z \)

- **Exploit in charging scheme**
  - fixed charge for small usage
  - usage sensitive charge only for usage above insensitivity level \( L \)

- **Charge according to estimated usage**
  \[
  f(X'(c)) = a + b \max\{ L, X'(c) \}
  \]
  - coefficients \( a, b \) and level \( L \) could depend on color \( c \)

- **Only usage above \( L \) needs reliable estimation**
Accuracy and Parameter Choice

- **Given target accuracy**
  - relate sampling threshold $z$ to level $L$

- **Theorem**
  - $\text{Variance}(X') \leq z X$ (tight bound)
  - now assume: $z \leq \varepsilon^2 L$
    - Std.Dev. $X' \leq \varepsilon X$ if $X \geq L$
      - bound sampling error of estimated usage $> L$
    - Std.Dev. $f(X') \leq \varepsilon f(X)$
      - bound error of charge based on estimated usage

- **Bounds hold for any flow sizes \{x_i\}**
  - no assumption on flow size distribution
    - just choose $z \leq \varepsilon^2 L$
Example

- **Target parameters**
  - $L = 10^7, \varepsilon = 10\% \Rightarrow z = 10^5$

- **Scatter plot**
  - ratio estimated/actual usage vs. actual usage
    - each color $c$
  - observe better estimation of higher usage

- **Want to avoid**
  - ratio $> 1+\varepsilon = 1.1$
    - and
      - usage $> L = 10^7$

- **Less than 1 in 1000 “bad” points**
Compensating variance for mean

- **Aim:**
  - reduce chance of overestimating usage

- **Method:**
  - theorem gave bound: \( \text{Var}(X') \leq zX \)
  - anticipate upwards variations in \( X' \) by subtracting off multiples of std. dev.
    - charge according to
      \[
      X_s' = X' - s\sqrt{zX'}
      \]
  - again: no assumptions on flow size distribution
Example: s=1

- Scatter pushed down:
  - no points with ratio $>1.1$ and usage $> 10^7$
- Drawback
  - more unbillable usage
    - when $X'_s < X$
- Small unbillable usage for heavy users
  - ratio $\rightarrow 1$
  - $\text{Std.Dev.}(X')/X'$ vanishes as $X$ grows
Example: $s=2$

- Scatter pushed down further:
  - no points with ratio > 1

- Trade off
  - unbillable usage vs. overestimation

<table>
<thead>
<tr>
<th>$s$</th>
<th>unbill. bytes</th>
<th>$X'<em>s &gt; X</em>?$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-0.1%</td>
<td>50%</td>
</tr>
<tr>
<td>1</td>
<td>3.1%</td>
<td>3%</td>
</tr>
<tr>
<td>2</td>
<td>6.2%</td>
<td>0%</td>
</tr>
</tbody>
</table>
How to reduce unbillable usage?

- Make sampling more accurate
  - reduce $z$
- For unbillable fraction $< \eta$
  - chose $s \cdot z \leq \eta^2 L$
- Example:
  - $s = 2$, $\eta = 10\%$
  - reduce $z$
    - from $10^5$ to $10^4$
- Alternative
  - increase coefficient $a$ in charge $f(X)$ to cover costs
Tension between accuracy and volume

- **Want to reduce** $z$
  - better accuracy, less unbillable usage

- **Drawback**
  - increased sample volume

- **Solution**
  - make billing period longer instead
    - usage roughly proportional to billing period
    - allows increased charge insensitivity level $L$
  - sampling production rate controlled by threshold $z$
    - rate $r \sum_x f(x)p_z(x)$
      - flow arrival rate $r$, fraction $f(x)$ of flows size $x$

- **Need only** $z = \varepsilon^2 L$
  - larger $L$ allows smaller error $\varepsilon$ for given $z$
Summary

- **Size dependent optimal sampling**
  - preferentially sample large flows
  - more accurate usage estimates for given sample volume
  - sample flow of size $x$ with probability $p_z(x)$

- **Charging from measured usage $X'$**
  - charge $f(X') = a + b \max\{L, X'\}$
  - fixed charge for usage below insensitivity level $L$
  - only need to reliably estimate usage above $L$

- **Sampling/charging accuracy**
  - choose $z = \varepsilon^2 L$ to get standard error $\varepsilon$

- **Variance compensation**
  - replace $X'$ by $X'_s = X' - \sqrt{zX'}$

- **Longer billing cycle**
  - increases $L$, better accuracy ($\varepsilon$) at given sampling rate ($z$)
Papers