Challenges for Using Sampled Traffic Measurements

Nick Duffield
AT&T Labs Research, Florham Park
http://www.research.att.com/info/duffield

Collaboration with Carsten Lund, Mikkel Thorup
Setting

- Traffic measurements are increasingly sampled
  - Resource constraints of measurement infrastructure
  - Ever-increasing traffic speed, volumes
- Measurement-based applications
  - Increasingly need fine-grained traffic characterization
    - provisioning: by customer, routing prefix, OD pair, application port
    - traffic characterization, security: fine time granularity
- Problem
  - Can these applications work effectively with sampled data?
- Rephrase
  - Can we better match sampling techniques to applications?
An Measurement Infrastructure and Resource Constraints

- Routers
  - Limited resources for packet measurement operations

- Bandwidth
  - Need to avoid (excessive) loss of measurement data in transmission

- Memory
  - Avoid overflow of caches for aggregation (e.g. formation/aggregation of flow statistics)

- Disk Storage
  - Cost to store large volumes of historical data; need fast retrieval for queries

- All these constraints easier to meet if some form of data reduction is employed
Why Sample?

- Statistician’s reflex:
  - Sample! Usually simple to implement, quick to execute
  - Allows retention of fine grained detail
    - Compare other data reduction methods: aggregation, filtering
  - Maintains ability to satisfy ad-hoc queries
    - No need to predefine aggregations

- Questions
  - What is the best sampling strategy given the data, applications?
  - How does one form estimates of traffic for applications?
  - What are trade-offs between sampling rate and estimation accuracy?
  - How to attribute accuracy to usage estimates?
  - How to dimension the measurement infrastructure?

- This talk: understand the limitations of simple sampling methods
  - Simple = uniform, independent
Sampling Practice and Proposals

- Sampling at router: select substream of packets for measurement
  - Router reports on each selected packet: sFlow, Trajectory Sampling
  - Router reports summaries of packet substream: Sampled NetFlow
  - Router samples of flow cache instantiations: Sample and Hold
  - Router sampling capabilities under standardization in psamp@IETF

- Sampling in collectors and warehouse
  - Size-dependent selection of flow records: Smart Sampling
Data, Applications and Sampling

- Elementary events: packet headers, flow records
- Many applications require measures of usage as input
  - usage metrics: e.g. #bytes, #packets, #flows
  - aggregation classes dependent of application
  - class = e.g. per host, customer, prefix, port, OD pair, time period
- Variable level of detail
  - e.g. total bytes vs. frequencies of bytes per flow
- With sampling
  - Aim to estimate metrics for original traffic from samples
Two types of metric estimation

- **Estimation from single events**
  - estimated metric = sampled metric / sampling probability
  - example: packet sampling with probability $p$
    - estimated original byte rate = byte rate in sampled packets / $p$
  - estimator variance
    - characterize estimation error through sampling variance

- **Estimation from multiple events**
  - Example: traffic flow = multiple packet event
  - Estimation of original traffic characteristics from sampled NetFlow
    - e.g. weight of traffic in long flows vs. short flows
Internet Traffic Flows

- Internet flows
  - set of packets with common property, observed in some time period
- Common property
  - key: built from header fields (e.g. src/dst address, TCP/UDP ports)
- Flow termination criteria
  - interpacket (inactive) timeout
  - protocol signals (e.g. TCP FIN, RST)
  - ageing (active timeout), flushing, ...
- Flow summaries
  - reports of measured flows exported from routers
  - E.g., flow key, flow packets/bytes, first/last packet time, router state
- Measured flow semantics
  - artificial, may capture appl. transactions if good start/termination criteria
Estimation from Sampled Flow Records

Sampling completed flow records within the collection infrastructure
Impact of Sampling Strategy

- Aims:
  - Estimation of metrics per class: #bytes, #packets, #flows

- Uniform sampling (1 in N flow records)?
  - Unbiased estimates: estimated metric = N * sampled metric

- Estimator variance highly dependent on metric under study
  - #flows OK: Standard Error $\sim N^{1/2}$
  - flow length distribution OK: pointwise standard error $\sim N^{1/2}$
  - #packets: Standard Error $\sim N^{1/2}$ $\text{RMS}(\text{length})/\text{Mean}(\text{length})$
  - #bytes: Standard Error $\sim N^{1/2}$ $\text{RMS}(\text{bytes})/\text{Mean}(\text{bytes})$

- Empirical fact
  - heavy tailed distribution of bytes, packets per flow

- Unbounded variance of byte, packet estimates
  - Metrics highly sensitive to random omission of single large flow
Uniform flow sampling statistically 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

![Graph showing the relationship between flow packets and log tail probability]
Estimation of Bytes, Packet Usage

- Each flow record \( i \) includes:
  - size \( x_i \):
    - bytes or packets
  - key \( c_i \) (distinguishing common property of packets of flow \( i \))

- Goal
  - estimate usage \( X(c) \) for each key \( c \) of interest during some period.
  - or over aggregates of keys (also denote by \( c \))

\[
X(c) = \sum_{i: c_i = c} x_i
\]
Size dependent flow sampling

- High fraction of traffic found in small fraction of long flows
  - sample long flows more frequently when estimating bytes, packets
  - large contributions to usage more reliably estimated
- Sample flow summary of size x with prob. p(x)
- Estimate usage X by
  \[ X' = \sum_{\text{sampled flows}} \frac{x}{p(x)} \]
- X’ unbiased estimate of X
- Chose p(x) to be increasing in x
  - longer flows more likely to be sampled
  - compare size independent (uniform, 1 in N) sampling: p(x) = 1/N
What is best choice of p(x) for size estimation?

- Claim: big reduction in Var(X') by careful choice of p(x)
- Trade-off accuracy vs. number of samples
- Express trade-off through cost function
  - For a given probability function p(x) write cost
  - $C_z(p) = \text{Var}(X') + z^2$ average number of samples
  - Parameter $z$: relative importance of variance vs. # samples
- Aim: choose p(x) so as to minimize cost
- Role of flow sizes in the minimization
  - Treat flow sizes $x_i$ as fixed
  - Do not try to exploit any statistical properties of flow sizes
    - robust w.r.t. variations flow size distribution
What is best choice of \( p(x) \) for size estimation?

- Theorem: minimum cost \( p \)
  - for any fixed set of flow sizes \( \{x_1, x_2, \ldots, x_n\} \)
  - assume independent sampling
    - OK since flow sizes fixed
  - \( C_z(p) \geq C_z(p_z) \) where \( p_z(x) = \min \{ 1, x/z \} \)

- Comment
  - 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 \( p_z \) “optimal”
Accuracy: optimal vs. uniform sampling

- NetFlow traces
  - 1000’s users, 1 week
- Aggregate flow keys
  - by user-side IP address $c$
- Compare
  - 1 in N uniform 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
Do Charging and Sampling Mix?

- **Usage sensitive charging**
  - charge based on sampled network usage

- **Is sampled usage reliable enough?**
  - risk of overcharging or undercharging

- **Approach**
  - manage sampling error through charging scheme
  - make charging **insensitive** to small usage
  - sampling error for small usage not reflected in charge to user

- **Trade-off**
  - allow small consistent undercount to reduce risk of overcharge
Charging and Sampling Error

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

- 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 key \( c \)

- Only usage above \( L \) needs reliable estimation
Estimation Accuracy and Threshold Choice

- Given target accuracy $\varepsilon$
  - relate sampling threshold $z$ to insensitivity level $L$

- Theorem:
  - Std. Error of Charge $\leq \varepsilon$, provided $z \leq \varepsilon^2 L$

- Generality
  - no assumption on flow size distribution

- Applicability
  - $z$ probably governed by target sampling rate
  - $L$ can be increased proportional to billing period
  - Hence for any target error $\varepsilon$ can realize $z \leq \varepsilon^2 L$
- 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:**
  - can prove: $\text{Variance}(X') \leq z \times X$
  - anticipate upwards variations in $X'$ by subtracting off multiples of std. dev.
  - charge according to

\[
X_s' = X' - s\sqrt{zX'}
\]
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
  - estimate/actual usage → 1
  - Std.Dev.(\( X' \))/\( X' \) vanishes as \( X \) grows

Charge insensitive to usage: sampling error has no effect on charge.
Example: $s=2$

- Scatter pushed down further
  - no points with estimated $X'_s >$ actual $X$

- Trade off
  - unbillable usage vs. overestimation

<table>
<thead>
<tr>
<th>$s$</th>
<th>unbill. bytes</th>
<th>$X'_s &gt; X$?</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>

Charge insensitive to usage: sampling error has no effect on charge
Sampling Flow Records: Summary

- Coupling between sampling strategy and estimation problems
- Uniform sampling of for #flows, flow distribution
  - Long flow pathologies if estimating #bytes, #packets
- Smart sampling
  - Optimal trade-off of sample volume and byte estimation variance
- Generalizations
  - More sophisticated cost functions embody extended application aims
  - Sampling under hard constraints on number of samples
- Pricing
  - Match pricing and sampling schemes
  - Usage based charged largely insensitive to sampling error
  - Trade off small but consistent underbilling against sampling error
Estimation of Original Flow Statistics from Sampled NetFlow Records
How to infer flow properties of original packet stream from flows of the sampled packet stream?
Consider Simple Instance of Problem

- A set of original traffic flows
  - \( f_i = \text{absolute frequency of flows comprising } i \text{ packets} \)

- Sampling
  - Packets are sampled independently with probability \( 1/N \)

- Data
  - Sampled NetFlow: flows formed from sampled packet stream.
  - \( g_i = \text{absolute frequency of number of sampled flows with } i \text{ packets} \)

- Problem
  - Estimate the \( f_i \) from the \( g_i \)
Large N and Short Flows: Challenge

- Value for N?
  - N could be 10’s, 100’s, even 1000’s

- Short Flows: hard
  - Flows shorter than N typically see only 1 packet sampled, at most
  - Detail in length distribution of short flows is washed out by sampling
  - Observed predominance short flows in traffic

- Extreme example: consider 2 cases: both comprising 2 million packets
  - Case 1: 2,000,000 original flows of length 1
  - Case 2: 1,000,000 original flows of length 2
  - Packet sampling 1 in N = 10,000 packets,
  - Average # sampled flows of length 1: in both cases 200 (nearest integer)
  - Probability to obtain any 2 packet sampled flows in case 2: about 1%
Long Flows: Easier

- Flows of length $iN$ (i small integer or larger)
  - streaming, filesharing, VoIP, 100’s or 1000’s packets per flow
- Poisson effect: very likely that roughly $i$ packets are sampled
  - Mean $= i$, variance $\approx i$
- Simple Scaling Inference
  - Attribute original flow of length $Ni$ to each sampled flow of length $i$:
    - $f_{Ni} = g_i$
- Experiment:
  - Sampling probability $1/N = 1/10$
  - Plot joint frequency of original and sampled flow lengths
- Coarse agreement, at least
  - Larger frequencies clustered near:
    - Original length $= N \times$ Sampled Length
Limitations of Simple Scaling

- Lack of smoothness
  - Inferred original distribution concentrated on multiples of $N$
  - Actual distributions not sharp, even at small multiples of $N$
- Lack of detail at short lengths
  - Shortest inferred length is $N$
- Fails to register flows that evade sampling:
  - $\# \text{ estimated original flows} = \# \text{ sampled flows}$
- Biased in favor of longer flows
  - Longer flows have greater chance to be sampled

Frequency of original, sampled flow lengths, $N = 10$
Difficult to Exploit the Average Behavior

- Average Sampling
  - Mean number of i-packet flows obtained from sampling j-packet flow:
    \[
    \text{binomial probability } B(j, i) = \binom{j}{i} N^{-i} (1-N^{-1})^{j-i}
    \]

- Express average frequencies \(E[g_i]\) of sampled flows in terms of \(f_i\)
  \[
  E[g_i] = \sum_{j \geq i} f_j B(j, i)
  \]

- Relationship is invertible when original flow length is bounded...
  \[
  f_i = \sum_{j \geq i} E[g_j] B(j, i) (-N)^{j+i}
  \]

- ...but unstable: coefficients in grow with length as power law in \(N\)

- Estimate by using actual measured frequencies \(g_i\) in place of \(E[g_i]\)?
  - Unbiased, but doomed to failure because of high variance;
  - Would need very accurate measurements of longer length frequencies
Challenges and Inference Methods

- **Short Flows**
  - Must accept lack of detail in inferred frequencies of short flows
  - Think of as smoothing over a distribution of original frequencies
    - those that are consistent with the measured flow length
  - **Converse:**
    - inferred distribution probably not statistically indistinguishable from true

- **Long Flows:**
  - Simple scaling increasingly accurate at long length
    - See also Hohn and Veitch, IMC 2003

- **Extended Simple Scaling**
  - Take account of flows that evade sampling,
  - Extract available detail for low length frequencies

- **Maximum Likelihood Estimation**
  - Smoothing comes for free
  - Can transparently incorporate estimation of #flows that are not sampled
Extended Simple Scaling: Missing Flows

- Some original flows evade sampling altogether
- First step: estimate number of missed flows
  - Trick: use statistics of SYN flows (TCP flows only)
  - Assumption: 1 SYN packet per TCP flow
  - Data: $g_{i}^{\text{SYN}} = \text{frequency of sampled flows with } i \text { packets, including SYN}$
- Theorem:
  - $g_{0} = (N-1) g_{1}^{\text{SYN}}$ is unbiased estimator of frequency of unsampled flows
- Estimate total number of original flows
  - $g_{0} + \sum_{i \geq 1} g_{i}$ is unbiased estimate of $\sum_{i \geq 1} f_{i}$
- How to distribute this estimated number over original lengths?
Extended Simple Scaling: Longer Flows

- **Aim:**
  - distribute inferred mass over original flow lengths

- **Spread mass** $g_i$ **uniformly** on interval width $N$ centered on $N_i$
  - preserves number of flows
    - consistent with unbiased estimation of total #flows
  - mean length of flows (nearly) scales by $N$
    - inverts average sampling behavior

- **Piecewise uniform distribution reflects lack of knowledge**
Extended Simple Scaling: Shorter Flows

- How to spread mass $g_0$ (estimated #flows not sampled)?
  - No sensible way to simply scale length (sampled length = 0!)

- Instead:
  - Try to estimate some detail in distribution of shorter flows

- Suppose largest original frequency is $f_L$ for some $L < N$, with $f_L \gg$ other $f_i$

\[
\frac{E[g_0]}{E[g_1]} \approx \frac{(N-1)}{L}
\]

- Consequence: if data obeys $g_0 > g_1$,
  - estimate dominant length $L$ by $(N-1) \frac{g_1}{g_0}$

- More refined argument spreads $g_0 + g_1$ over two low lying intervals
Extended Simple Scaling: Sample Results

- Trace: 10M packets collected at campus LAN during 300 minutes

- Peak distribution localized within lengths < 10, even for large N

- Discrepancy measure:
  - Weighted Mean Relative Difference = \[ \frac{2 \sum_i |f_i(\text{actual}) - f_i(\text{est})|}{\sum_i (f_i(\text{actual}) - f_i(\text{est}))} \]
  - Dominated by differences in largest frequencies
  - WMRD less than 20% for N = 10, 30, 100
Maximum Likelihood Estimation: Setup

- Treat original frequencies $f_i$ as parameters to be estimated
  - $f_i$ viewed as average frequencies arising from distribution of original lengths
  - $f_i / \Sigma f_i = \text{probability for original flow to have length } i$
- Compute probability $P(\{f_i\})$ to obtain sampled flow frequencies $g_i$
  - As function of the parameters $f_i$
- MLE: estimate by finding parameters $f_i$ that maximize $P(\{f_i\})$
- Good statistical properties in general
  - Consistent (= converges to true value as amount of data grows)
  - Efficient (= minimal variance w.r.t a class of estimators)
- Drawbacks
  - Can be difficult to calculate in practice
    - Previous inverted average is stationary point but generally non-physical
  - Resort to iterative methods: EM algorithm
Maximum Likelihood Estimation: Sample Results

- Trace: 37M packets collected at OC3 campus link
- Extract HTTP and DNS components (modulo port number abuse)

Discrepancy (WMRD) after 1,000 iterations
- \( N = 10 \): HTTP 54%, DNS 16%
- \( N = 100 \): HTTP 60%, DNS 37%

Increasing iterations appears to reduce WMRD
Largest discrepancy we found: WMRD 10% or less in other data, even at \( N = 100 \)
- Was this data unusually bad? HTTP peak at length 5, smoothed out in estimation
## Comparison of the Estimators

<table>
<thead>
<tr>
<th></th>
<th>Extended Simple Scaling</th>
<th>Maximum Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applicable to Traffic</strong></td>
<td>TCP only</td>
<td>All</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>No clear winner, but better control of total number of flows</td>
<td></td>
</tr>
<tr>
<td><strong>Computation</strong></td>
<td>$O(\max{N, j_{\max}})$</td>
<td>$O(i_{\max}^2)$ setup</td>
</tr>
<tr>
<td></td>
<td>No iteration</td>
<td>$O(i_{\max}j_{\max})$ per iteration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use simple scaling for longer flows</td>
</tr>
<tr>
<td><strong>Drawbacks</strong></td>
<td>Throw away most of sampled flows (those no SYN present).</td>
<td>Slow Convergence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Criterion for Termination</td>
</tr>
</tbody>
</table>
Inferring Flow Distributions: Summary

- Independent packet sampling model
  - Inference inherently difficult due to washing out of low length detail
  - Reasonable recovery of smoothed length distributions (N<100)

- Other sampling strategies?
  - Potential scope for dependent sampling methods
  - Preferentially pick out shorter flows?

- Converse Approach
  - Sample and Hold (Estan and Varghese, Sigcomm 2002)
    - Different aim: report on long flows, suppress reports on shorter flows
  - Packet sampling to preferentially pick out longer flows
    - Random choice to instantiate each potential new flow cache entry
    - Small flows may be missed, long flows more likely to be measured
    - Not generally possible to construct unbiased metric estimators
Summary and Outlook

- Limitations of independent sampling
  - For estimating multi-packet events
  - Potential scope for dependent packet sampling?

- Limitations of uniform sampling
  - For estimating usage from highly skewed flow distributions

- Need to match sampling strategies to estimation goals
  - Non uniform sampling for estimating byte usage from flow records
  - Flow cache sampling (sample and hold) to focus on long flows
References


- See also: http://www.research.att.com/~duffield/pubs