Ranking flows from sampled traffic

Chadi BARAKAT
INRIA Sophia Antipolis, France

jointly with: Gianluca Iannaccone (Intel Research Cambridge)
Christophe Diot (Thomson Research Paris)

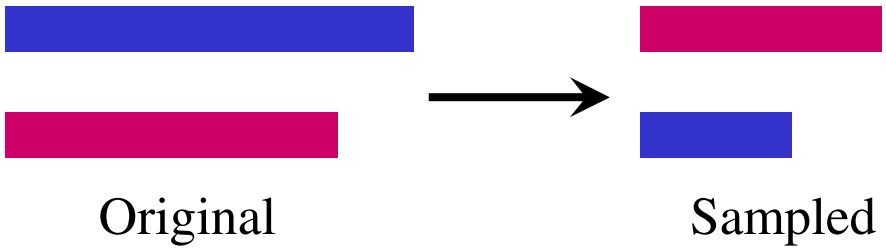
CONEXT 2005
Toulouse, October 27th 2005

Packet sampling and flow information

- Packet sampling is a need at high speed links.
  - Very hard (and expensive) to monitor all packets.
- Principle:
  - Capture a subset of the packets, say for example one packet over T or with some predetermined probability p.
  - Compute the needed information from this subset.
  - Then infer the original information.
- This is fine for total traffic statistics
  - Average rate, variability, correlation, packet size dist, etc.
- But is tricky for information related to flows …

Packet sampling and flow information

- A flow is a set of packets carrying the same information in their headers (5-tuple, IP @ prefix, protocol number, etc).
- Challenges with packet sampling:
  - Most small flows disappear.
    - The number of these flows cannot be recovered except if we know the flow size distribution (which is usually the unknown).
  - Large flows might be split into small flows.
  - The order of flows based on their volumes can change.



State of the art

- The focus was mainly on the inference of general flow information, as the flow size distribution [Duffield et al. 2003, Hohn and Veitch 2003]
  - Problem very hard to solve because of the lack of information on the number of non sampled flows.
  - And because of the large number of operations involved, that require very high numerical precision.
- Few works focus on the detection of large flows (called heavy hitters) from sampled traffic, but without ranking them.
  - What sampling rate is required to detect a flow of size larger than some threshold ? [Mori et al. 2004, Choi et al. 2002]

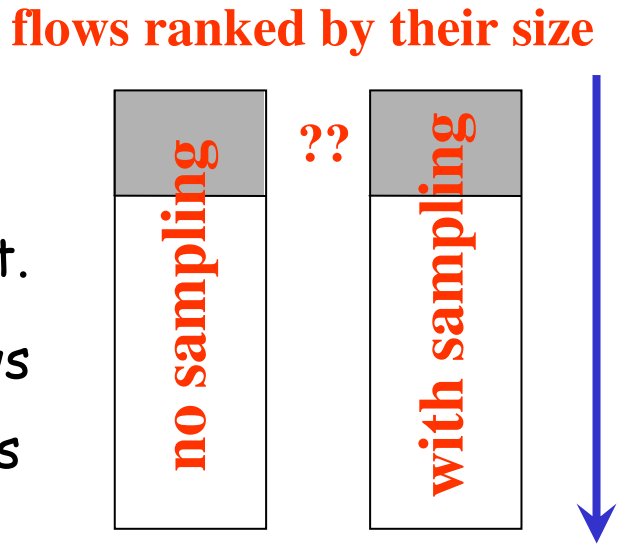
The purpose of our study

- Focus on the largest flows.

  Study their detection and ranking from a sampled traffic.

- **Problem statement:**

  - Rank sampled flows using their sampled sizes.
  - Take the largest " t " flows in the sampled list.
  - Check whether this short list of top " t " flows corresponds to the short list of top " t " flows in the original traffic.



  - As a beginning, we require the two lists to have the same flows in the same order.

Applications

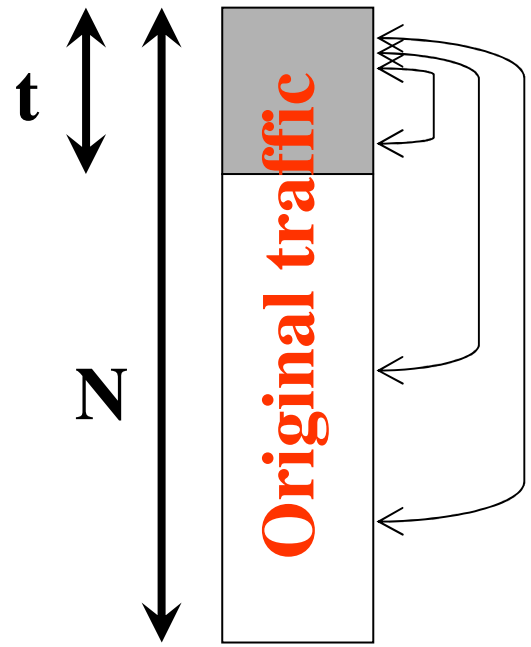
- Diverse potential applications:
  - usage based pricing.
  - anomaly detection.
  - traffic engineering.
  - buffer management.
  - detection of popular prefixes.
  - etc.

Methodology

- Take a packet sampling rate **p** (random sampling).
- Take a certain number of flows (say **N**) whose size follow some distribution (Pareto distribution as an example).
- Compute the error made when ranking the largest " **t** " flows from the sampled traffic.
- Validate the numerical results on real traces.

Performance metric

- We need a metric that can be computed easily and accurately.
- Take a pair of flows, the first one at the top of the original list (before sampling) and the second one anywhere in the list. The total number of these pairs is equal to $(2N-t-1)t/2$.
- After sampling, the two flows of the pair can be either ranked correctly or misranked. Compute the probability of misranking. Let P_m.
- Define our metric as: $P_m \times (2N-t-1)t/2$
  = Total number of misranked flow pairs averaged over all flow size realizations.



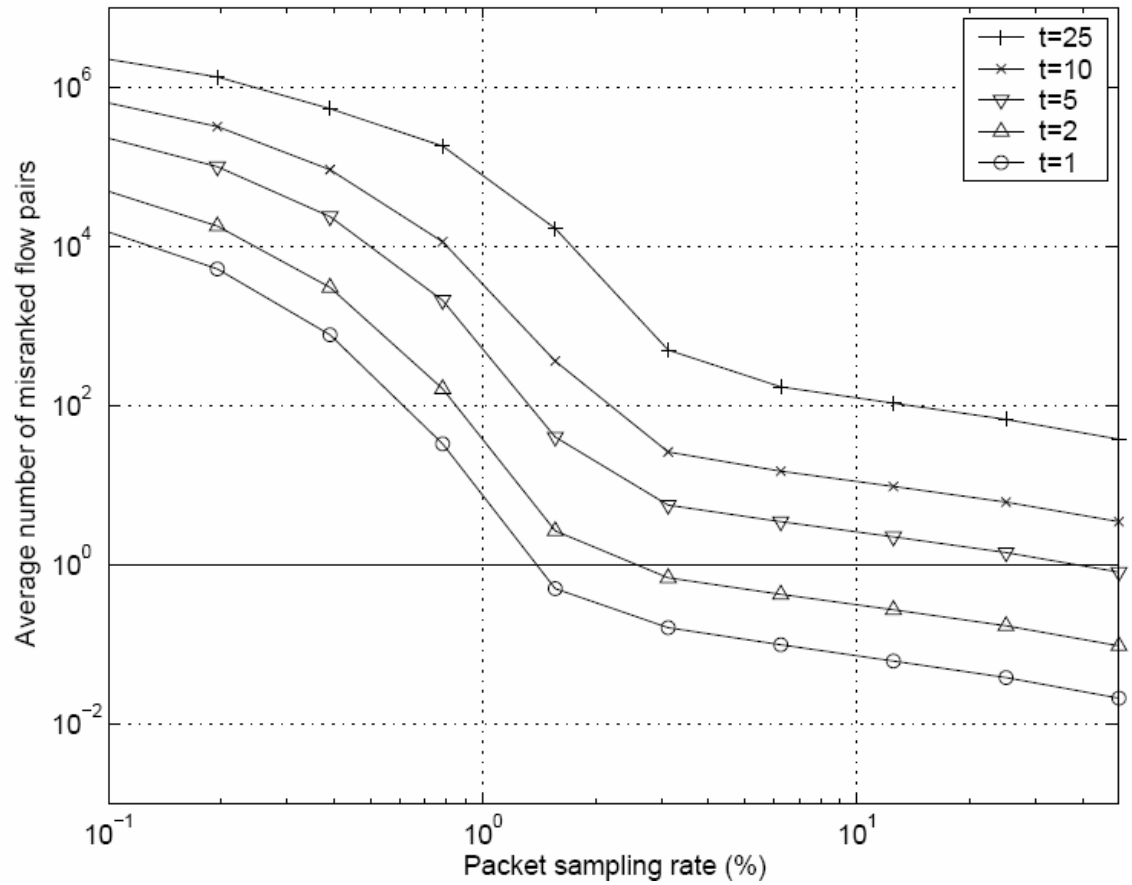
- We deem the ranking acceptable if our metric is smaller than one.

Numerical results

- Model can solve quickly in matlab (few seconds for millions of flows).
- Change the parameters of the model (average flow size, shape of the flow size distribution, etc.) and study how the ranking (after sampling) performs with the sampling rate.
- Parameters of the model extracted from publicly available traces. Flows are TCP connections.

Numerical results
Varying the number of top flows

Parameters calculated from a trace collected on the Abilene Network
1 minute measurement interval



The ranking improves with the sampling rate.

The ranking becomes worse when we consider more flows at the top.

A sampling rate on the order of 1% allows the ranking of the top one or two flows.

As we consider more flows, the required sampling rate increases well above 10%.

Other results

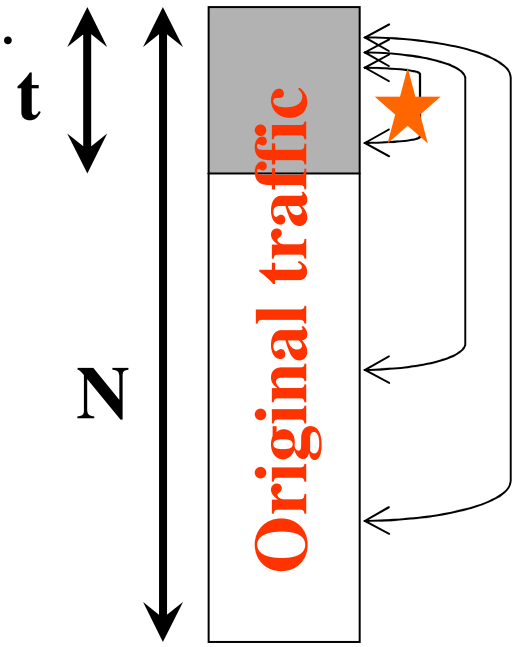
- For low sampling rates, the error scales as 1/p.
- For distributions whose tail decreases fast enough (faster than the square root of the size), the ranking improves with the total number of flows **N**.
- Making flows bigger improves the ranking if the difference of their sizes increases faster than the sqrt of the size.
- The ranking improves when the tail of the flow size distribution becomes heavier.

Being less conservative

From ranking to only detecting

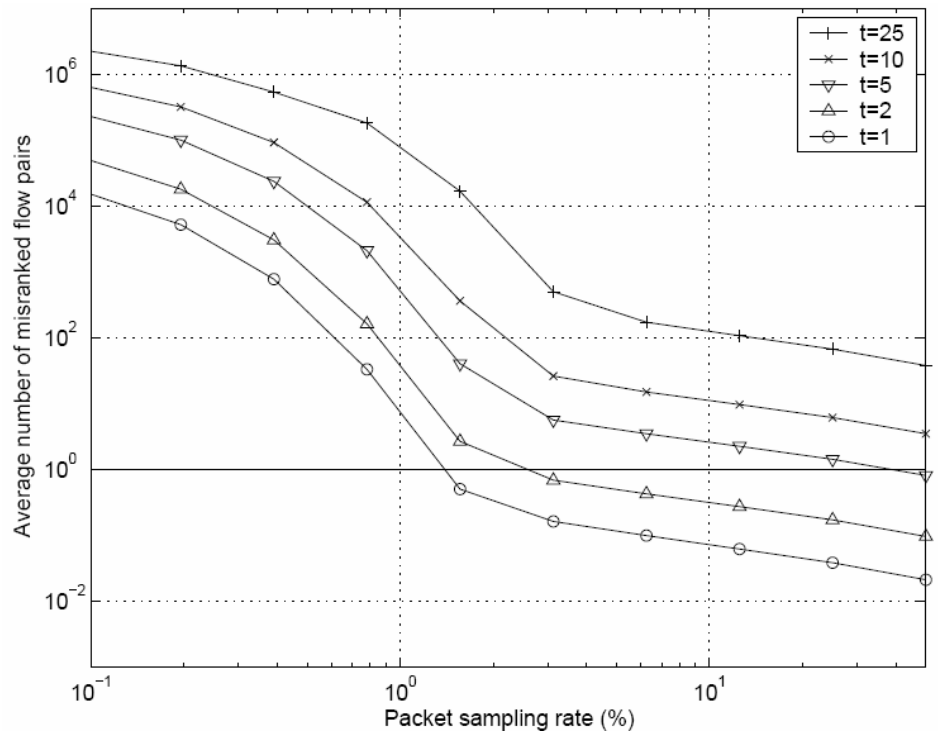
From ranking to only detection

- The order among top flows is no longer important. Only their detection is important.
- The performance metric has to be slightly changed: Average number of misranked flow pairs, where one element of a pair is a top flow and the other element a NON top flow.
- **Conclusion**: the required sampling rate can be reduced by an order of magnitude !

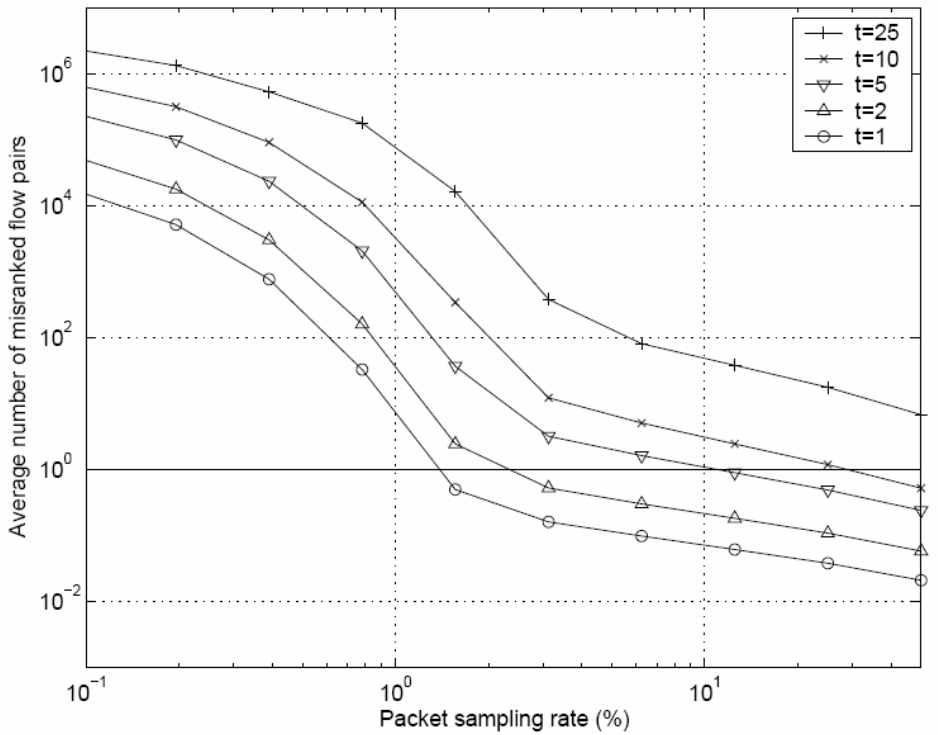


From ranking to only detection

Parameters calculated from a trace collected on the Abilene Network
1 minute measurement interval



Detection and ranking

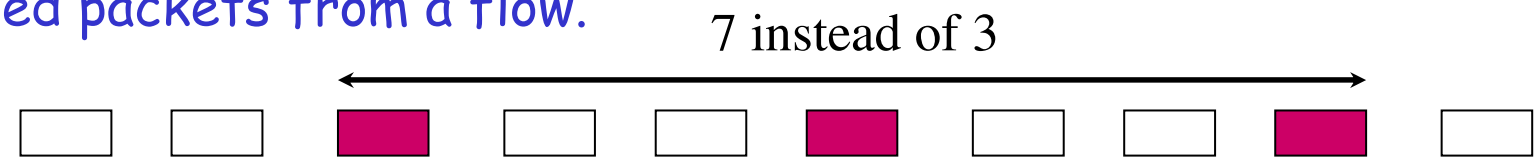


Only detection

Using transport information to improve the ranking: the protocol-aware method

Protocol-aware ranking

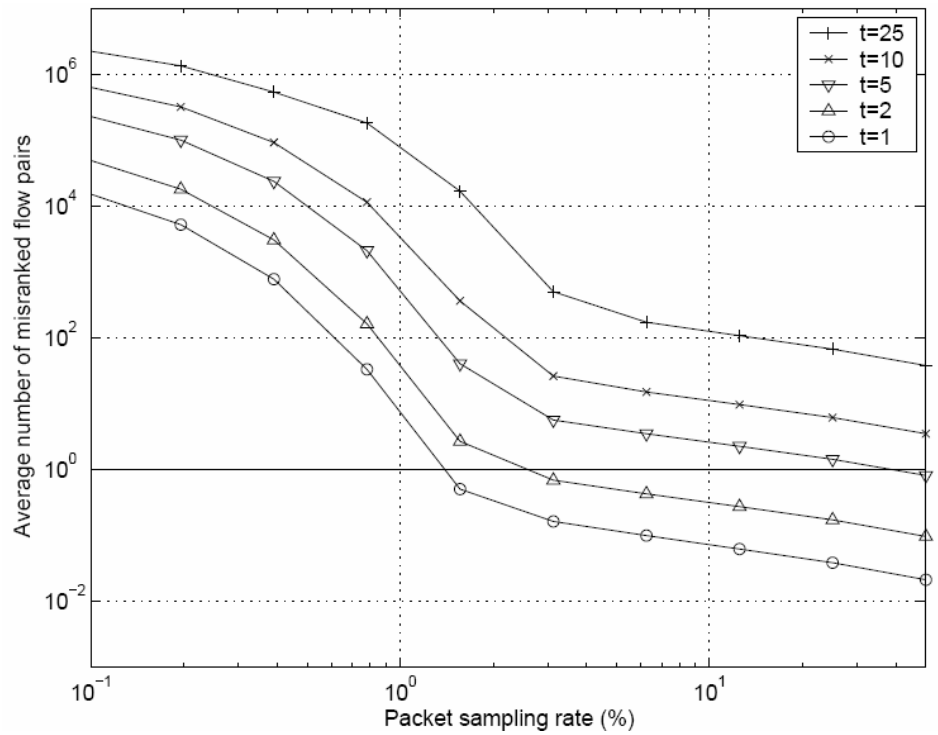
- Consider the sequence number when available in transport header, e.g. TCP sequence number, to get a better estimation of the flow size.
  - Sampled flow size becomes the distance between the fist and last sampled packets from a flow.



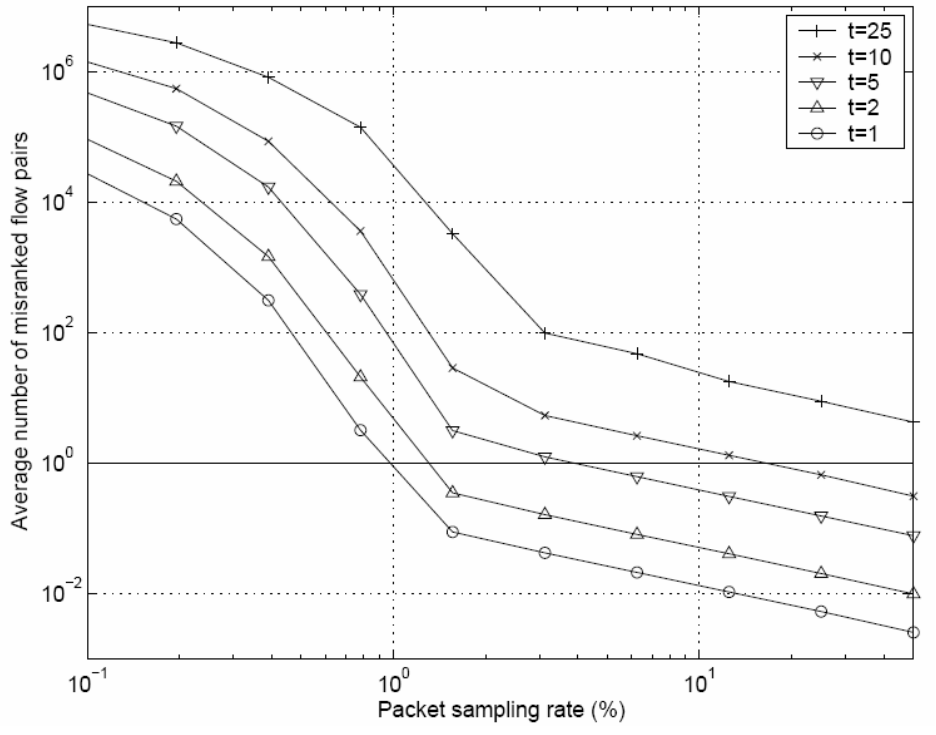
- Our metric for ranking performance remains the same, only the probability to misrank two flows changes.
- **Positive result:** at high sampling rate (above 1%), we get a performance an order of magnitude better.
- **Negative result:** no improvement at low sampling rate …
  - For protocol aware ranking, the error scales as $1/p^2$.
  - Whereas it scales as $1/p \ll 1/p^2$ for the previous method.

Protocol-aware ranking

Parameters calculated from a trace collected on the Abilene Network
1 minute measurement interval



Blind ranking



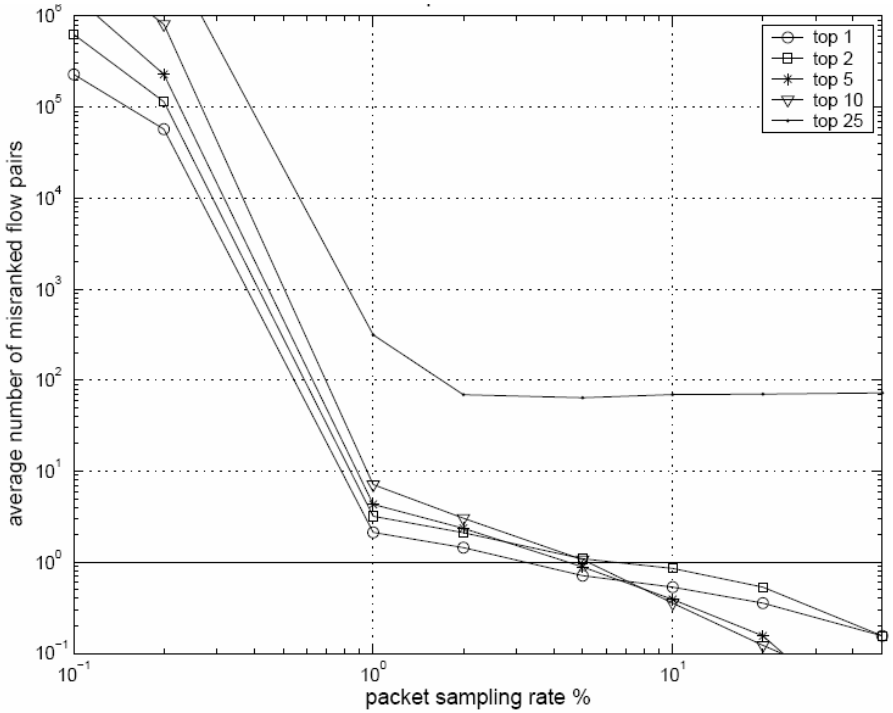
Protocol-aware ranking

More on the protocol-aware ranking

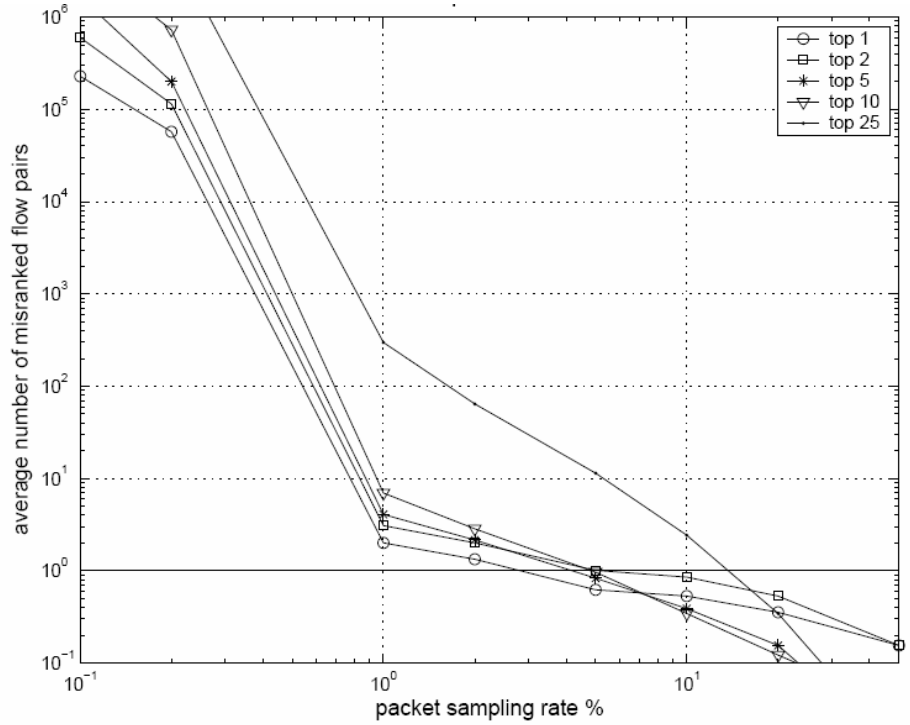
Interesting in general, but

- It only works at the transport level.
- Some flows may experience jumps in the sequence number. These jumps should be detected and not interpreted as non sampled data.
- And there is the problem of losses and retransmissions !!
  - Retransmissions are not counted by this method, however they are considered by the first method.
  - The protocol aware method suits flows defined based on how much data users inject into the network.
  - The previous method suits flows defined based on how much data flows transmit over the network.

An example from a real trace



flow size defined at the network level



flow size defined at the application level

The line t = 25 does not decrease to zero !

Conclusions, perspectives

Main conclusion:

- Detecting and ranking the largest flows from a sampled traffic is not always accurate, except if a high sampling rate is used (order of 10% and even more).

Perspectives:

- Looking for other sampling methods more appropriate for the ranking of the largest flows.
  - Use of data streaming methods.
- Validation with longer traces.