Efficient Resource-Constrained Monitoring – Detection of top-k Flows

Jalil Moraney | Supervised By: Prof. Danny Raz

The Problem
Detect the top-k flows in a network while using few counters.

Existing Solutions

1. Sampling:
   • Sample “1 of n packets” or “1 each n ms”
   • Characterize traffic based on sample packets ➔ decreases load
   • Inherently inaccurate
   • Still needs monitoring algorithm

2. Streaming Algorithms:
   • Treat traffic as a stream of packets
   • Process every packet ➔ relatively accurate
   • Per packet operation: either in software or not O(1) operation.

Time Based Approach – “Hash & Split”
• Interval ➔ rounds (say 2) ➔ epochs (say 32)
• Hardware operation at end of epoch
• Previous round results affects current round
  re-allocate counters every epoch

Results (CAIDA ’14 traces)
k and m effect on “Hash & Split” Detection Rate

Future Directions
• Hierarchical Heavy Hitters (HHH) Problem.
• Efficient assignment of monitoring tasks based on Network-wise policy.