Flow-state dependent packet selection techniques

Click icon to add photo

Ram (Ramki) Krishnan– Brocade Communications

Ning So – Tata Communications

Changes from IETF 86 (1)

- Positioning -- incorporate suggestions from WG chair (Juergen Quittek)
  - Expand on flow-state dependent packet selection techniques discussed in flow selection (http://datatracker.ietf.org/doc/draft-ietf-ipfix-flow-selection-te) and RFC5475.

Changes from IETF 86 (2)

- Various flow state dependent packet selection techniques from different papers
  - Sample and hold
  - Multistage Filters
  - Rotating conservative counting Bloom filters with periodic decay
- Value proposition of the above techniques
  - Prefer large flows over small flows – address flow cache scalability and avoid high CPU utilization

Terminology:
-- Large flow(s): long-lived large flow(s)
-- Small flow(s): long-lived small flow(s) and short-lived small/large flow(s)

Changes from IETF 86 (3)

- Common elements of Information model (additions to flow selection draft)
  - largeFlowObservationInterval
  - largeFlowBandwidthThreshold
- Corresponding IANA Information Elements

Terminology:
-- Large flow(s): long-lived large flow(s)
-- Small flow(s): long-lived small flow(s) and short-lived small/large flow(s)

Material from IETF 86

- Practical Application of flow state dependent packet selection techniques
    - Behavioral Security Threat Detection, for e.g. DDOS attacks, with minimal sampling overhead – details below
- Large Flow Classification
    - Recognized large flows can be broadly classified as
    - Well behaved (steady rate) large flows, e.g. video streams; Bursty (fluctuating rate) large flows e.g. peer-to-peer traffic
    - The large flows can be optionally sampled
- Small Flow Processing
    - Sample small flows (excluding the large flows) at a normal rate using PSAMP protocol.
    - Examine small flows for determining behavioral security threats like DDOS attacks for e.g. SYN floods, Scanning attacks etc.

Terminology:
-- Large flow(s): long-lived large flow(s)
-- Small flow(s): long-lived small flow(s) and short-lived small/large flow(s)

NEXT STEPS

- Adopt as a work item in IPFIX working group
  - Complements flow-state dependent packet selection techniques discussed in flow selection (http://datatracker.ietf.org/doc/draft-ietf-ipfix-flow-selectio) and RFC5475
  - Operator Interest
  - Vendor Interest
  - Interest from IPFIXERs (Salvatore D'Antonio et al.)