Use of Sketches in DPP for DDoS and Monitoring

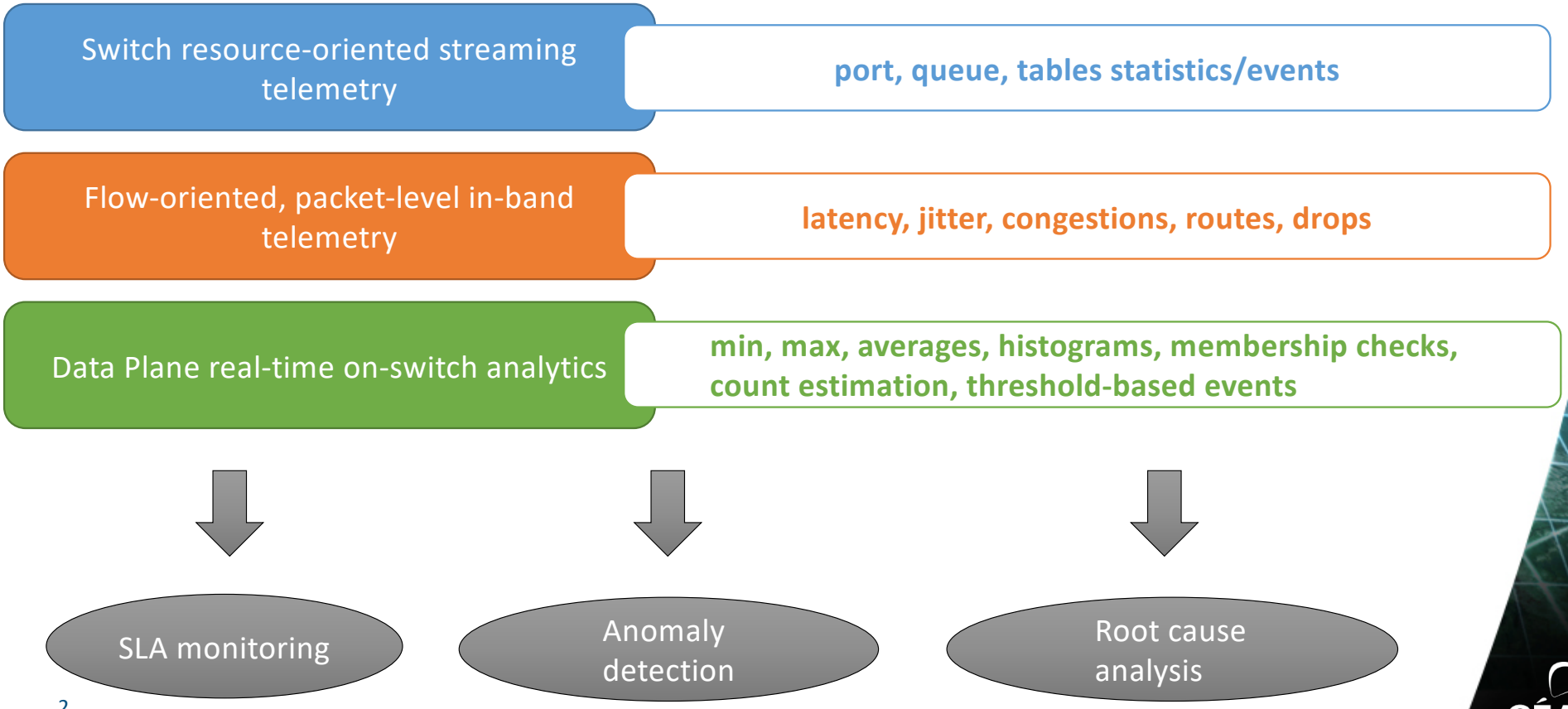
Data plane real-time analytics for the network visibility

Damian Parniewicz (PSNC), Damu Ding (FBK), Federico Pederzolli (FBK)
WP6 T1 Data Plane Programming

Telemetry and Big Data Workshop
10th November 2020

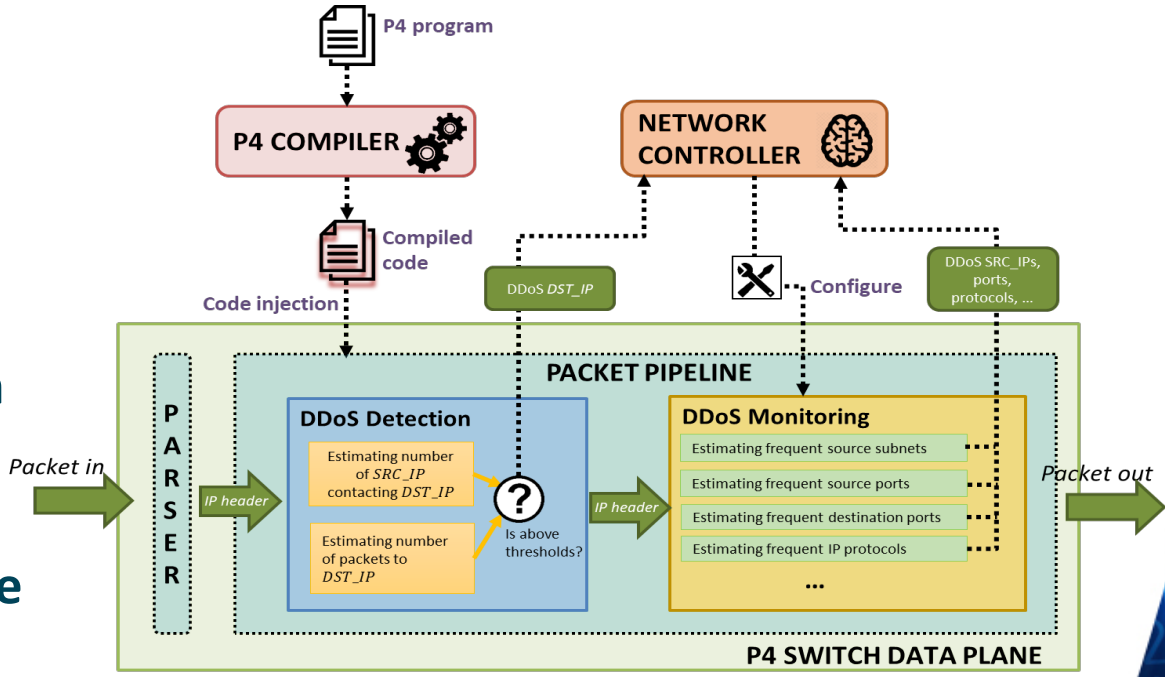
www.geant.org

Evolution and complementarity in the network monitoring

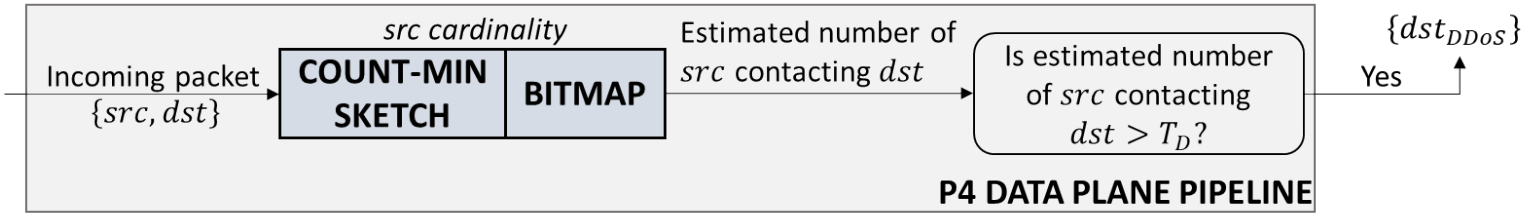


Analytics in Data Plane for simple DDoS detection and DDoS traffic monitoring

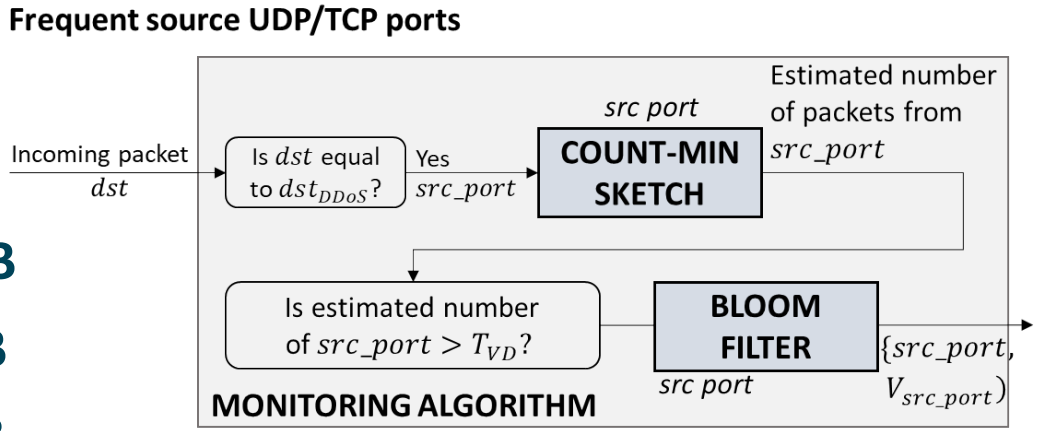
- Very fast detection (< 1sec) based on thresholds of IP destinations in packets
- Measured at boundaries of NRENs/ GÉANT network
- Providing detailed information about the DDoS attack characteristics
- Possibility of almost immediate mitigation of the attack
- About 400-800 KB of switch memory required



Sketch structures used in our P4 anti-DDoS algorithms

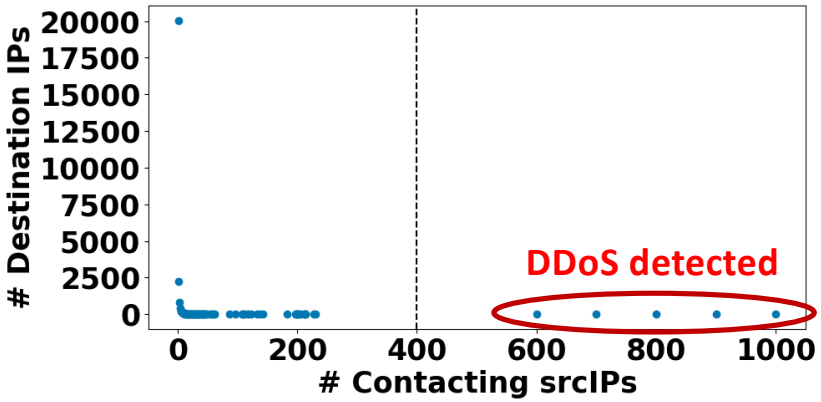


- **Sketch-based strategy for volumetric DDoS attack detection**
- **IPv4 cardinality sketch: 400 KB**
- **port frequency sketch: 34.6KB**
- **port membership sketch: 1.08 KB**



Accuracy tests and performance tests

Synthetic traffic *(with simulated DDoS)*



- Tested with CAIDA UCSD Anonymized Internet Traces Dataset + simulated DDoS traffic
  - ~491K packets, ~28K flows per a second

- 10G performance tests with iperf generated traffic
  - Testbed limitations visible

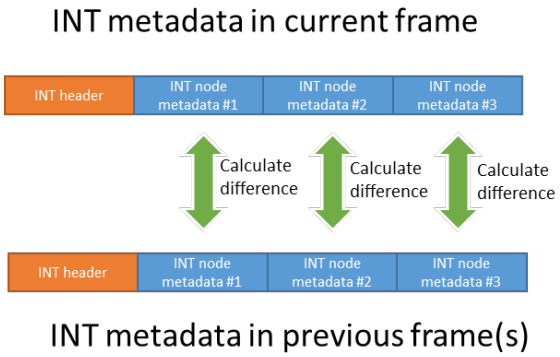
iPerf bandwidth: **10 Gbps**

L4 Protocol	Datagram/ Segment size	Packet loss (No loss)	Throughput (Bottleneck: CPU server)	Average Packet processing time
UDP	500 bytes	0%	1.03 Gbps	393 ns
UDP	1000 bytes	0%	1.95 Gbps	390 ns
UDP	1470 bytes	0%	2.87 Gbps	389 ns
UDP	3000 bytes	0%	5.45 Gbps	396 ns
UDP	6000 bytes	0%	9.62 Gbps	392 ns
UDP	9000 bytes	0%	9.67 Gbps	392 ns
TCP	64 Kbytes	-	9.05 Gbps	392 ns
TCP	128 Kbytes	-	9.41 Gbps	389 ns

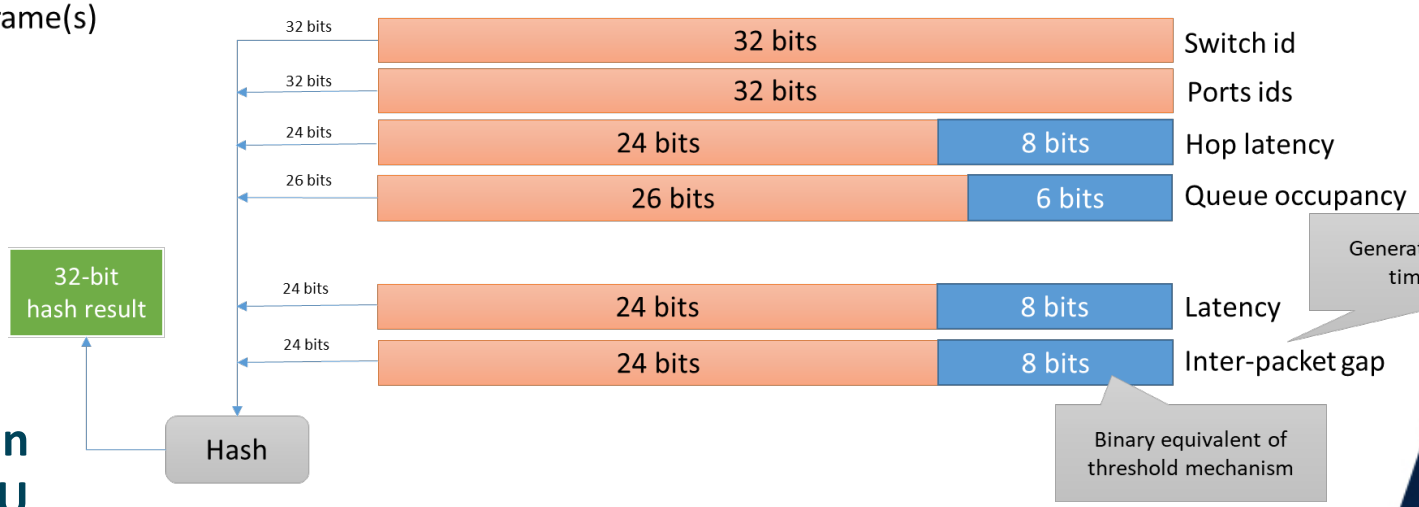
Data plane sketches drawbacks/problems

- Requires proper pre-configuration to be effective
  - Sketch parameters have a large impact on the quality of their estimations
- A sketch instance is a single purpose entity
  - For multiple concurrent data plane analytics more sketches are required
- Lack of resources for additional data plane analytics in current Barefoot Tofino based switches
  - Available packet pipeline processing stages fully utilized for switching functionalities and currently implemented sketches
- More complex sketches not possible in P4
  - Limited resources to implement very complex packet processing
  - Lack of arithmetic operations such as division or logaritmic operations requires creative solutions

Data plane INT analytics (not sketch-based)



- **Divide INT metadata fields into two parts:**
  - **bits which should be constant for some time**
  - **bits which may change without triggering a new INT report**



Hash operation can save a lot of ALU operations

Conclusions

- Data Plane programming is now available to "users" and will enrich our monitoring toolset
- No single silver bullet for network visibility
  - Focus on „information that matters” because switch resources are scarce and Big Data infrastructure is costly

- Data Plane real-time analytics can be used for:
  - Generating global and scalable accurate statistics
  - Detecting outliers and reacting in near real-time
  - Complementing switch’s other telemetry capabilities
  - Data Plane processing may greatly reduce requirements on the network analytics infrastructure

Thank you

Any questions?

damianp@man.poznan.pl
ding@fbk.eu
fpederzolli@fbk.eu

www.geant.org

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

The scientific work is published for the realization of the international project co-financed by Polish Ministry of Science and Higher Education in the years 2019 - 2022 from financial resources of the programme entitled "PMW"; Agreement No. 5023/H2020/2019/2