Using traffic snapshots to detect DDoS attacks
From state-of-the-art approaches to the industry

Gilles Roudière [1] *(PhD student)*
Philippe Owezarski [1], François Devienne [2] *(Supervisors)*

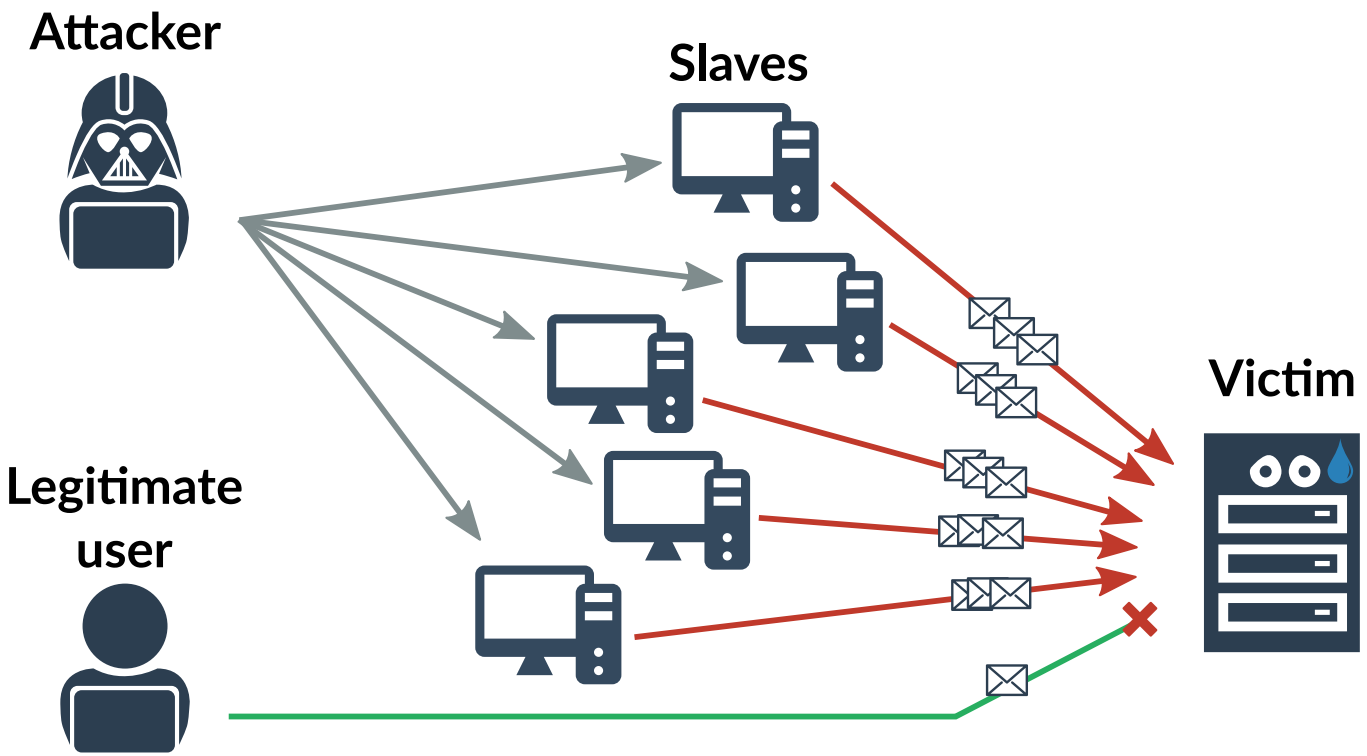
[1] LAAS-CNRS, {gilles.roudiere, philippe.owezarski}@laas.fr
[2] Border 6, francois.devienne@border6.com

18th May 2018

In partnership with: border 6

What are DDoS attacks ?

Distributed Denial of Service Attacks (DDoS):



What are DDoS attacks ?

Major impact:

- May cause a **total paralysis** of the targeted services.

Numerous:

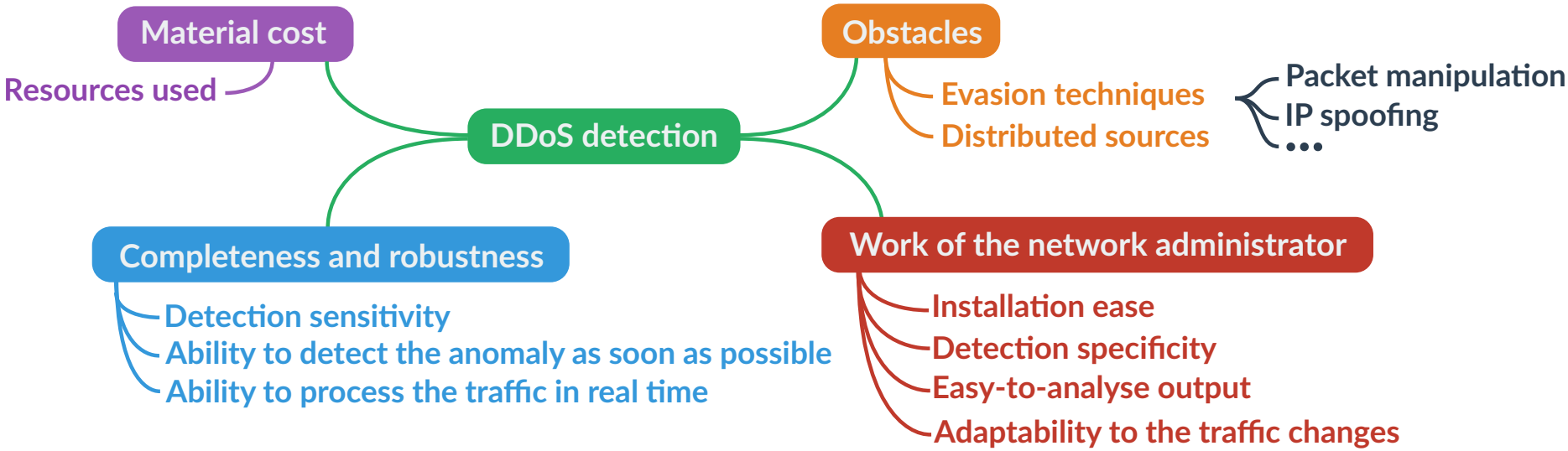
- **84%** of companies underwent at least one in 2016. (including 18% that suffer at least one a month)

Costly:

- 63% of companies estimate the cost of the unavailability of their services to more than **$100000/h**,
- In average, an attack costs **$2.5 millions**.

(Source: Neustar, 2017)

Building an efficient detector

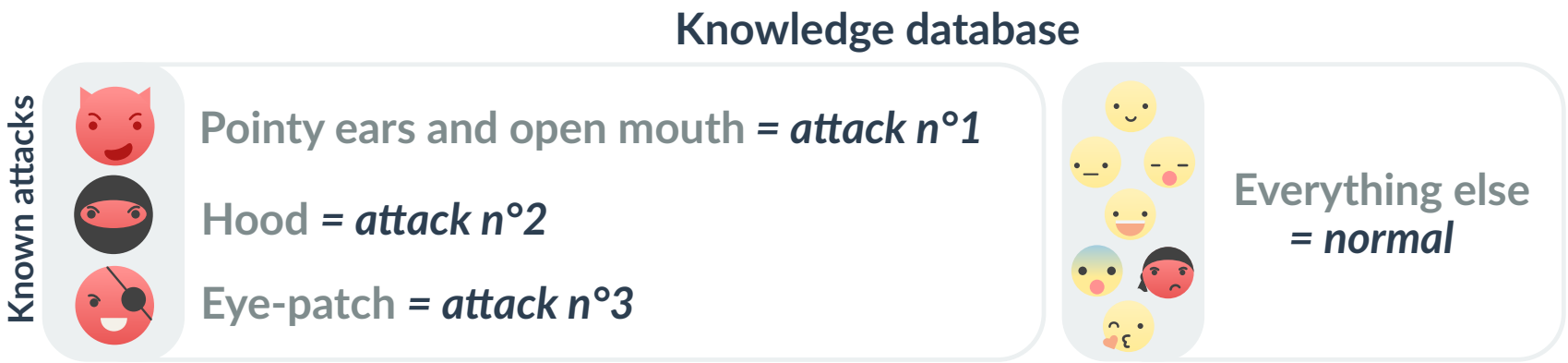


Building an efficient detector

- Limited remaining computational resources,
- Sampled traffic,
- Detection on the victim side,
- Detection at the network level.

How to detect attacks ?

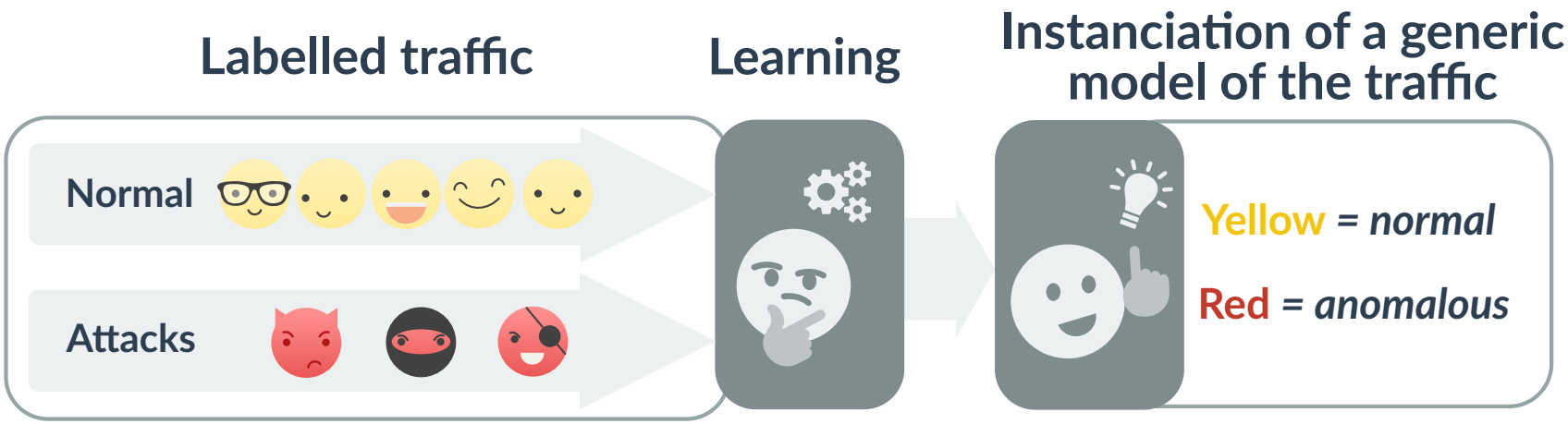
The basics: Knowledge-based approaches.



- ✓ Efficient detection of known attacks,
- ✓ Provides exhaustive diagnosis information,
- ✗ Traffic signatures are hard to create,
- ✗ Do not detect unknown anomalies.

How to detect attacks ?

The wizard of math's : supervised approaches.

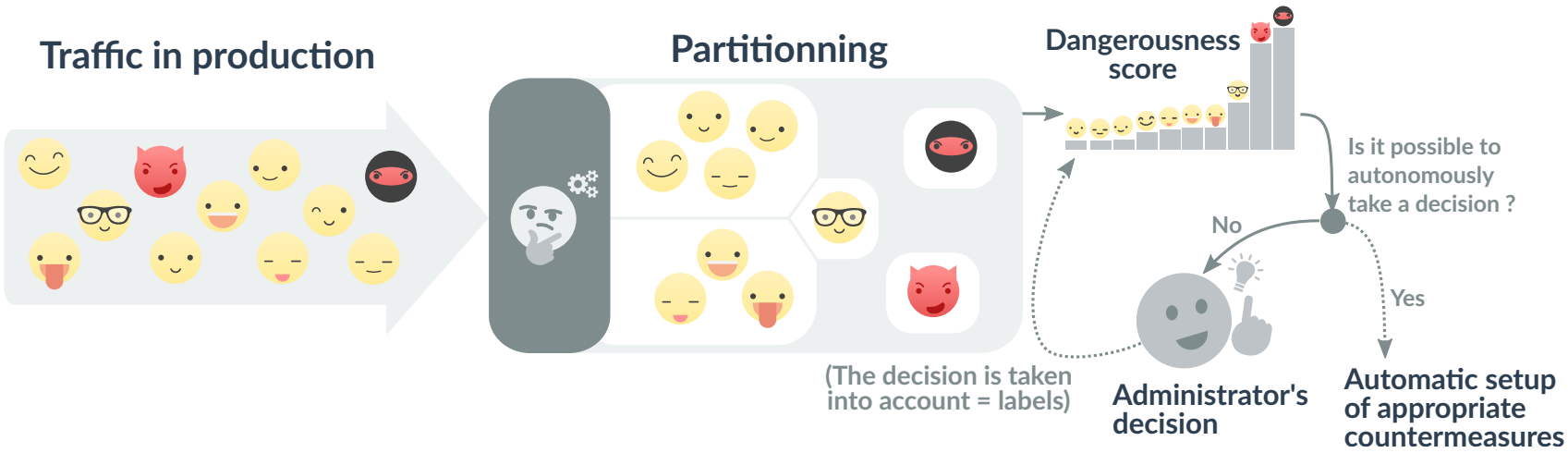


- ✓ Can detect unknown anomalies,
- ✓ Can be trained again if the traffic evolves,

- ✗ Building a model of the traffic is complex,
- ✗ Needs a representative labelled dataset...
- ✗ ...which needs to be rebuilt when the traffic evolves.

How to detect attacks ?

The future of anomaly detection: unsupervised approaches.



- ✓ Need from little to no intervention from the network administrator, autonomous in most cases,
- ✓ Can detect unknown anomalies,
- ✓ Autonomously extract the distinctive features of each traffic class ⇒ Can automatically produce filtering rules,

- ✗ May need a lot of computing power depending on the algorithm used and the input data.

Unsupervised detection: the workflow

- The anomaly detector spots an unusual behavior

If the anomaly seems very dangerous:

- The detector filters the unusual traffic, applying automatically the mitigation rules.

else:

- The detector asks the network administrator's feedback first,
- The network administrator analyses the provided results and make a decision,
- If the traffic should be blocked, the detector applies the mitigation rules.

Autonomous Algorithm for Traffic Anomaly Characterization
A new algorithm, tested and free to implement.

G. Roudière, P. Owezarski, "A Lightweight Snapshot-Based DDoS Detector"
CNSM'2017, 13th International Conference on Network and Service Management

The full paper, with all the algorithm details, is freely available at:
`https://hal.laas.fr/hal-01676810`

-

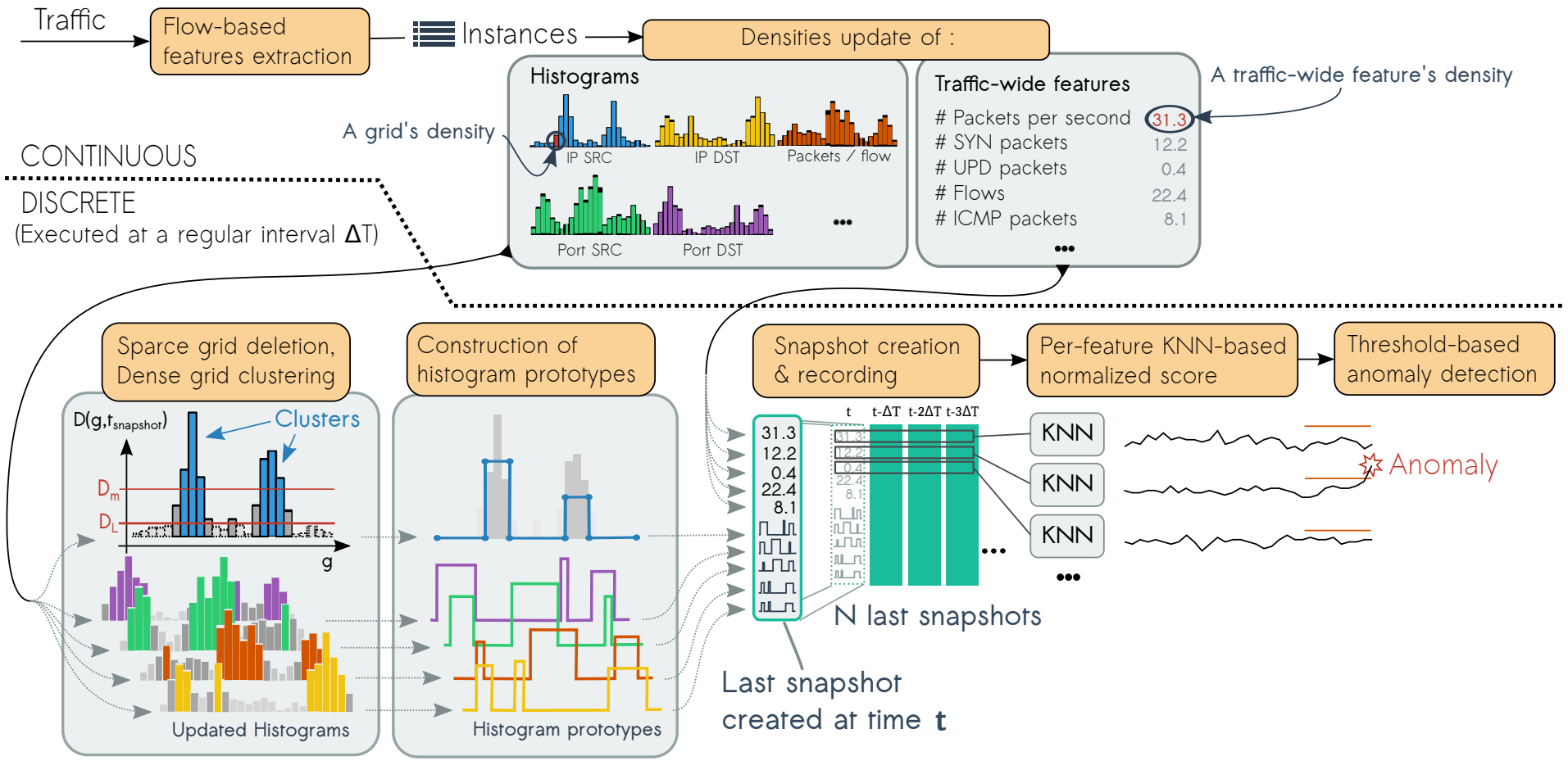
Hopefully soon to be published: G. Roudière, P. Owezarski, "Evaluating the Impact of Traffic Sampling on AATAC's DDoS Detection" *ACM SIGCOMM Workshop on Traffic Measurements for Cybersecurity (WTMC 2018)*

AATAC

An algorithm solving industrial problems:

- Fully **autonomous**, detection,
- **Lightweight**,
- Able to operate over **sampled traffic**,
- Simplifying the analysis stage, producing **easy to understand results**,
- **Focus on DDoS attacks**, but able to detect other kind of anomalies.
- **Compatible with industrial technologies**: IPFix of Sflow.

AATAC


Traffic
Flow-based features extraction
Instances
Densities update of :
Histograms
IP SRC
IP DST
Packets / flow
Port SRC
Port DST
A grid's density
Traffic-wide features
Packets per second 31.3
SYN packets 12.2
UPD packets 0.4
Flows 22.4
ICMP packets 8.1
A traffic-wide feature's density
CONTINUOUS
DISCRETE
(Executed at a regular interval ΔT)
Sparce grid deletion, Dense grid clustering
Construction of histogram prototypes
Snapshot creation & recording
Per-feature KNN-based normalized score
Threshold-based anomaly detection
D(g,t_snapshot)
Clusters
D_m
D_L
g
Updated Histograms
Histogram prototypes
31.3
12.2
0.4
22.4
8.1
t
t-ΔT
t-2ΔT
t-3ΔT
KNN
KNN
KNN
Anomaly
N last snapshots
Last snapshot created at time t

AATAC: Output analysis

⇒ The last N snapshots can be plotted as a video of the traffic evolution when the anomaly occurs. It outputs basic signatures too.

Evaluation: Detection quality

SynthONTS:

- 13 anomalies generated by emulation,
- then included into real traces.

Results:

Best operation point:

True positive rate:	0.83
False positive rate:	0.0013

- The detection stays good with most parameter changes,
- Less than 1 second to detect the attack.

Evaluation: Real time operation

Real traces:
- Mainly web traffic,
- Including a real DDoS attack,
- Captured within the network of a Border 6's client.

Results:

N	Continuous (Calculation time for 1s of traffic)	Discrete (Calculation time in milliseconds)
100	0.20	0.029
1000	0.20	0.028
5000	0.21	0.030

On a 3.00GHz Intel Xeon CPU (E5-2623 v3)

Evaluation: Comparison with other tools

	Algorithm type	Real-time capability	Detection
Ours	Unsupervised	-	10 / 13
FastNetMon	Signatures	3× slower	6 / 13 et 1 FP
ORUNADA	Unsupervised	10× slower	13 / 13

Evaluation: Sampled traffic

Count-based sampling

- 3 sampling techniques,
- Sample more packets when the traffic increases,
- Showed good and stable performances.

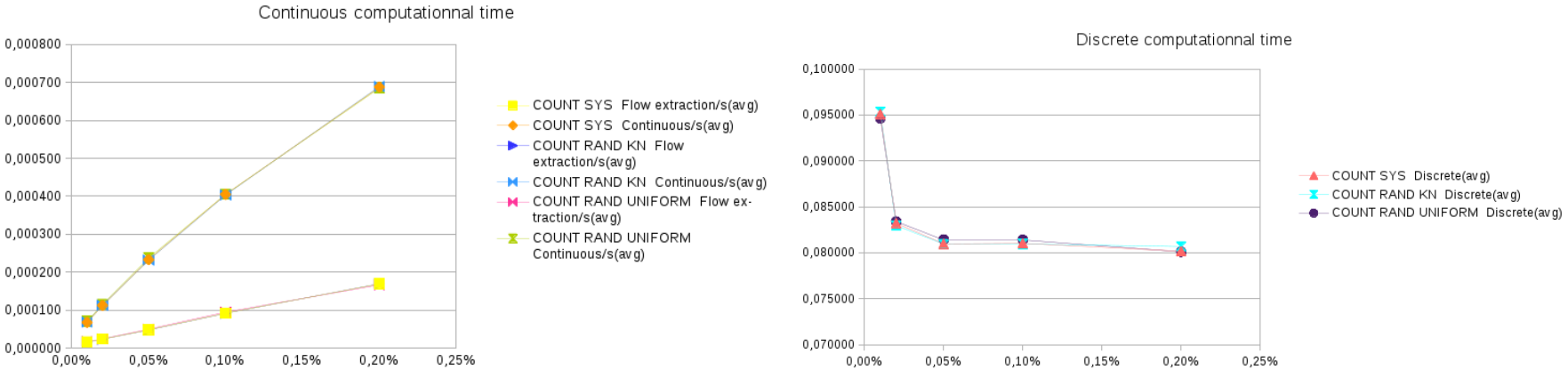
Time-based sampling

- 2 sampling techniques,
- Feed the detector with a steady input rate,
- Showed very good performances at higher rates.

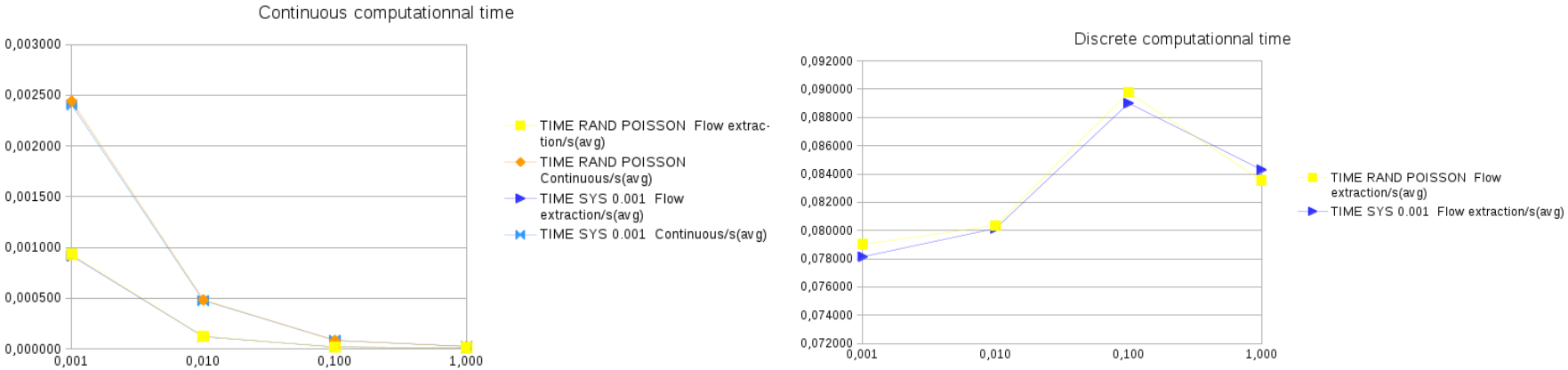
The sampling has little to no impact on the detection efficiency.

Evaluation: Sampled traffic

Count-based



Time-based



Conclusion and future works

A detection which is:

- Efficient,
- Robust and real-time,
- Autonomous,
- Able to operate over sampled traffic,
- Producing easy to interpret results.

Future works:

- Autonomous creation of better traffic signatures,
- Improve the characterization of the traffic by using reinforcement techniques.

Thank you!
Any question ?