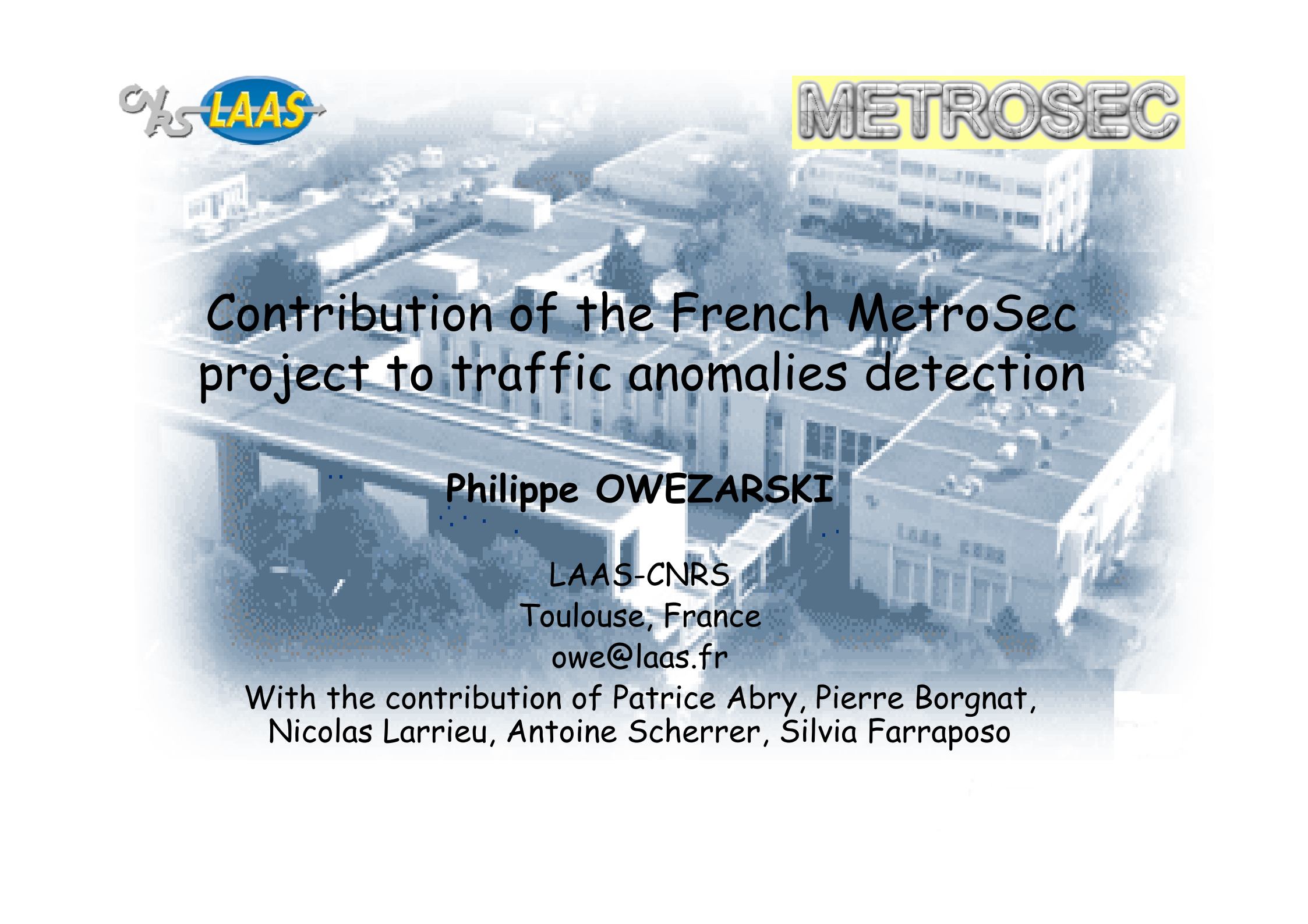


Contribution of the French MetroSec project to traffic anomalies detection

Philippe OWEZARSKI

LAAS-CNRS
Toulouse, France
owe@laas.fr

With the contribution of Patrice Abry, Pierre Borgnat, Nicolas Larrieu, Antoine Scherrer, Silvia Farraposo

Outline

- Traffic characteristics and IDS
- A non Gaussian and long memory model for Internet traffic with anomalies
- Model validation with traffic traces (with and without anomalies)
- Anomalies/DDoS attacks detection
  - With the non Gaussian and long memory model
  - Using deltoids
- Ongoing and Future work

Motivation

- Traffic anomalies (on a link)
  - One or several occurrencies that change the way traffic is flowing in the network
- Consequences
  - Performance decrease
  - QoS degradation

Existing work

- Several projects on traffic anomalies detection arised in the past
  - They rely in general on simple statistics on traffic characteristics
    - But they lack by a bad knowledge on traffic characteristics

      →Limited efficiency

Known traffic characteristics

- Non Gaussian, non Poisson statistics
- Long Range Dependence (LRD), Strong correlations
- Traffic can look different according to the granularity of observation

- And…

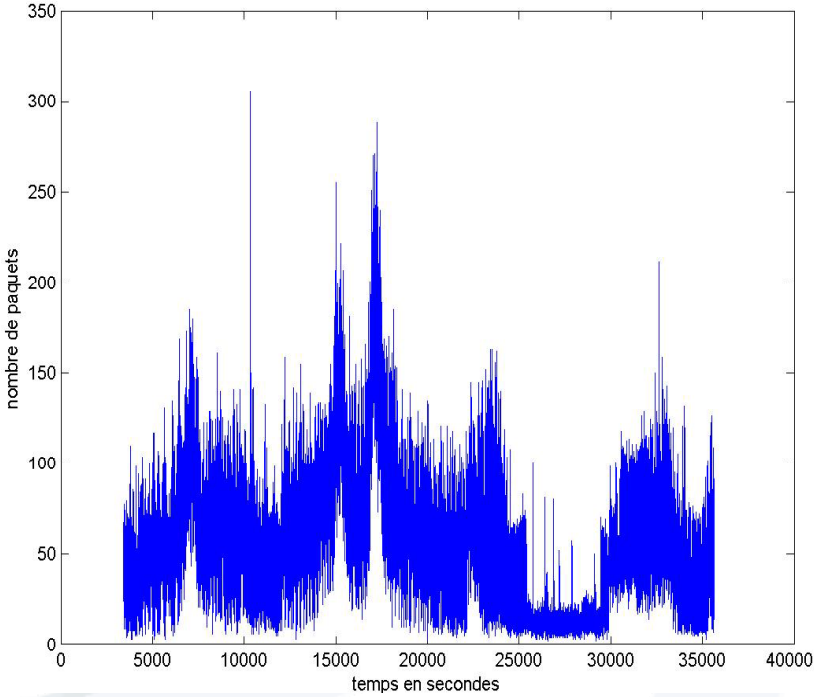
  …**Traffic is highly variable !**

Profile based IDS issues

Traffic profiles in IDS do not consider such variability

False positive rate is high

→ Impossible to fix reliable thresholds



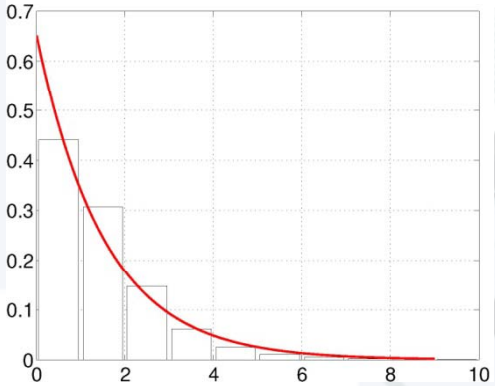
Temporal evolution of the number of TCP/SYN packets

A traffic profile cannot be based only on some averages (non Gaussian)

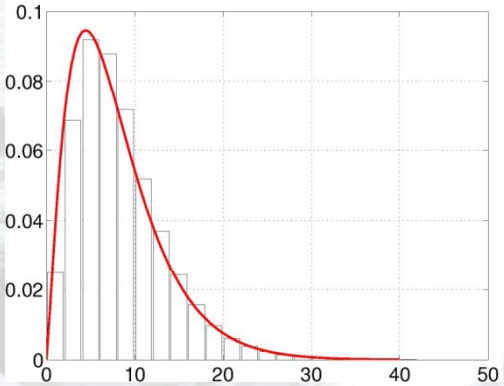
→ High level statistics are required

Marginal laws

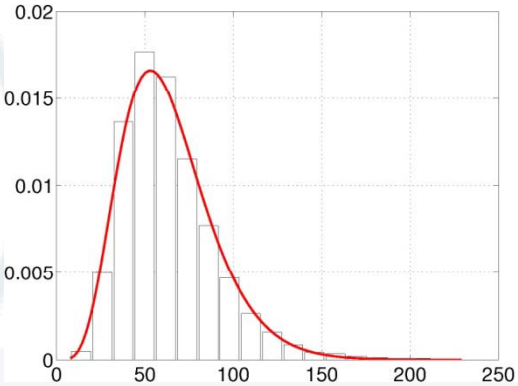
- Distributions of empirical probabilities LBL-TCP-3



Δ=4ms



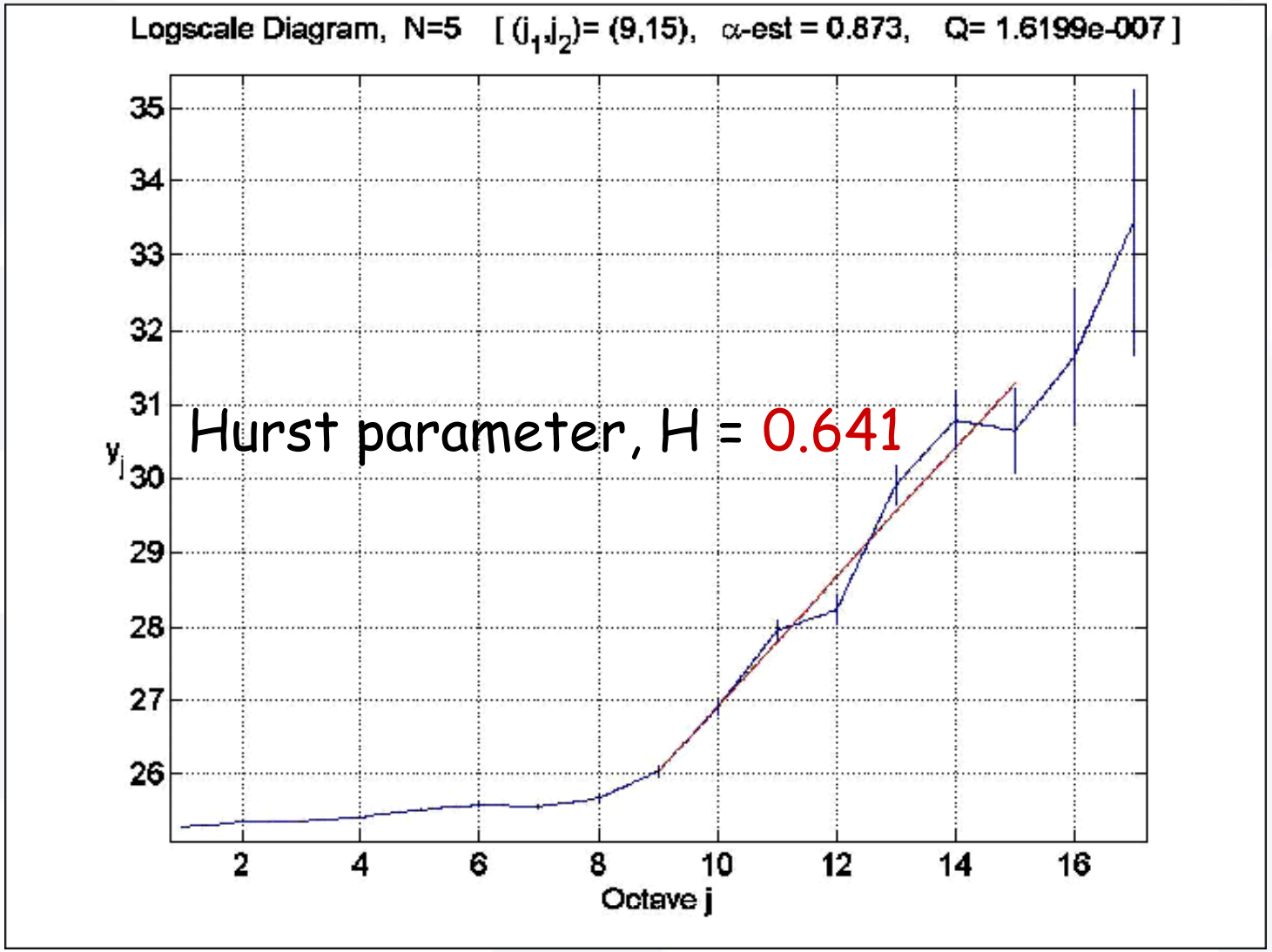
Δ=32ms



Δ=256ms

- Poisson model? Exponential law? Gaussian?
- What aggregation level to select?

Traffic Correlation (SRD and LRD)



What model for a non Gaussian and long memory process ?

Non Gaussian with LRD model

Joint modelling of 1st and 2nd orders statistics

- Packet aggregated count process: $X_\Delta(k)$

$X_\Delta(k)$ = #pkt during $[k\Delta, (k+1)\Delta]$

or

- Bytes aggregated count process: $W_\Delta(k)$

$W_\Delta(k)$ = #bytes during $[k\Delta, (k+1)\Delta]$

- 1st. PDFs of marginals as gamma laws

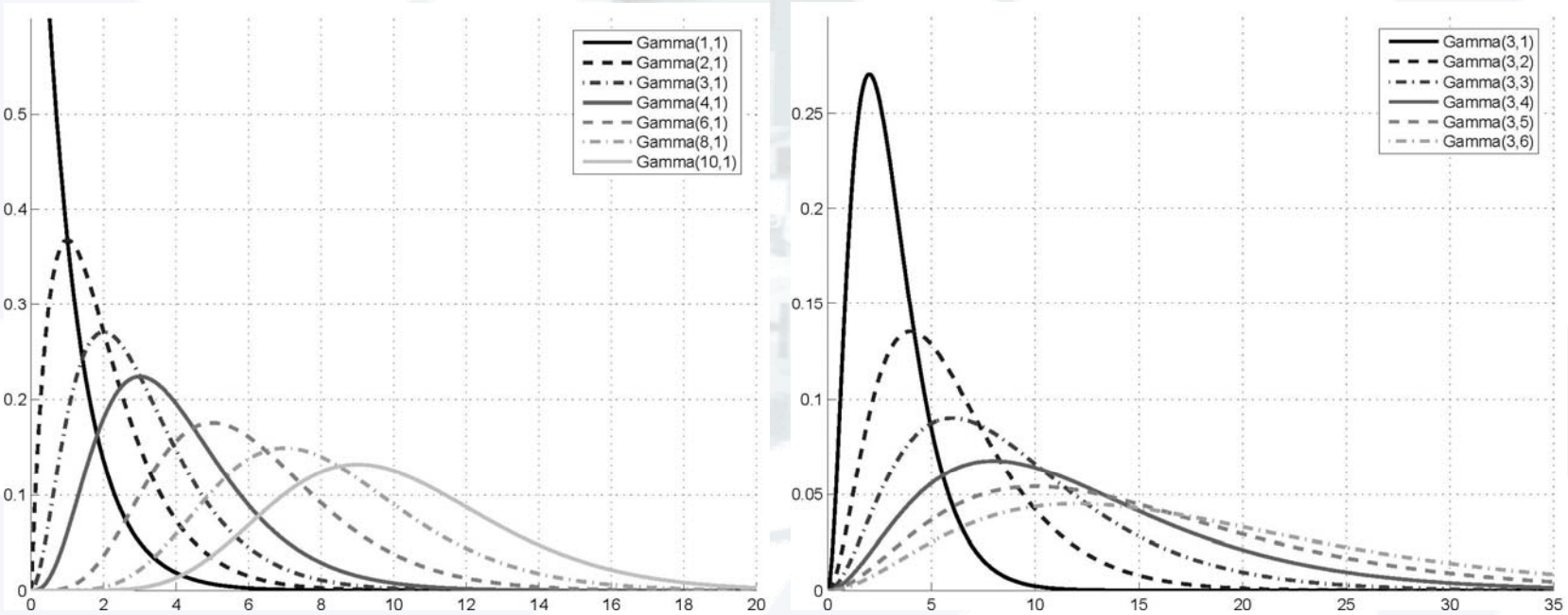
Note: one fit for each Δ

- 2nd. Covariance (or spectrum) with LRD

Covariance of a farima model

Gamma distributions

$$\Gamma_{\alpha,\beta}(x) = \frac{1}{\beta\Gamma(\alpha)}\left(\frac{x}{\beta}\right)^{\alpha-1}\exp\left(-\frac{x}{\beta}\right)$$



Shape parameter α : can model from Gaussian to exponential ;

$1/\alpha \approx$ distance to Gaussian

Scale parameter β : multiplicative factor

Long memory from a farima model

- Long range dependence

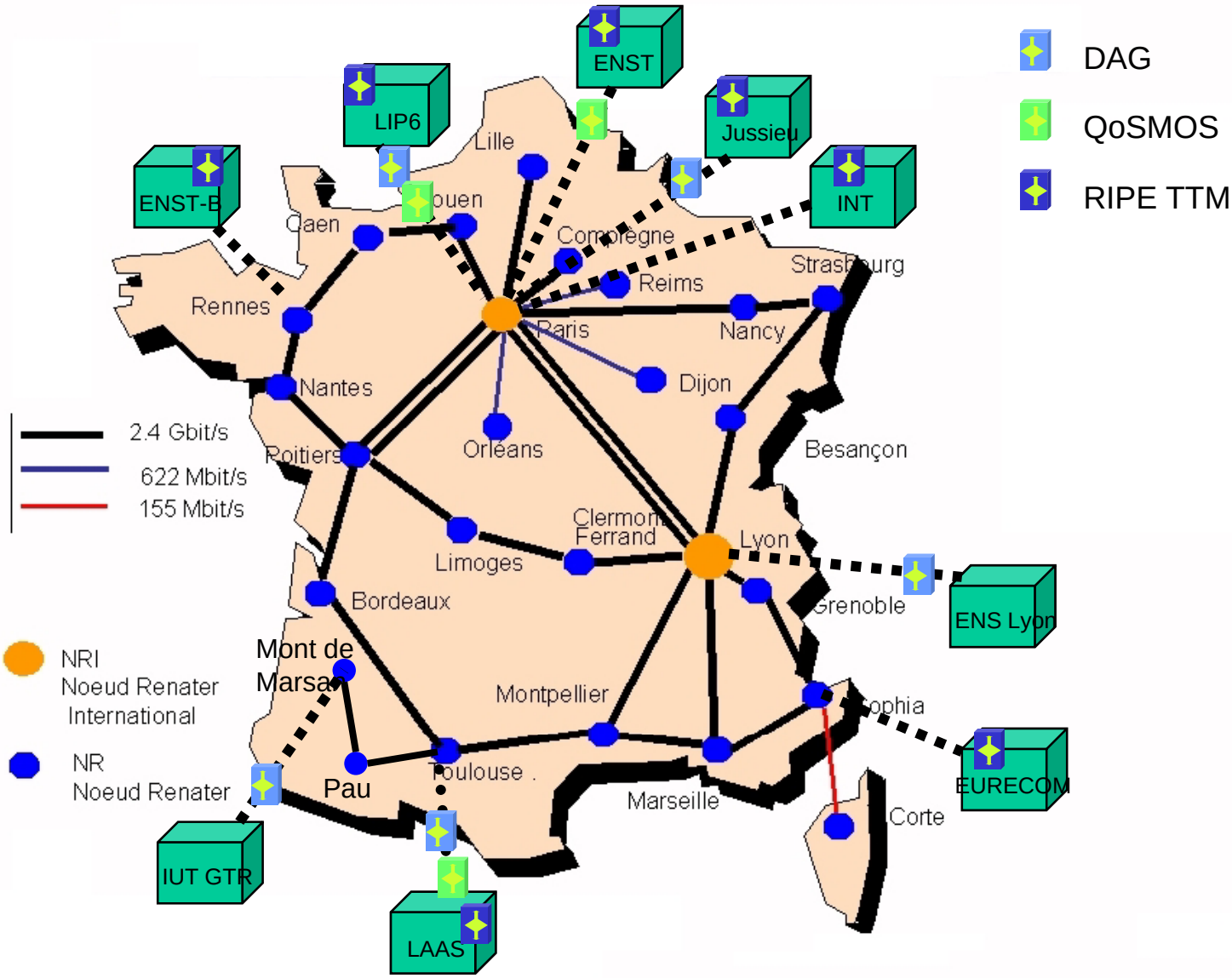
  covariance is a non-summable power-law → spectrum $f_{X_\Delta}(\nu)$:

  $f_{X_\Delta}(\nu) \sim C|\nu|^{-\gamma}$, $|\nu| \to 0$, with $0<\gamma<1$

- Farima = fractionnaly integrated ARMA
  1. Fractional integration with parameter d→LRD with $\gamma=2d$
  2. Short range correlation of an ARMA(1, 1)
     →parameters θ, ϕ

$$f_{X_\Delta}(\nu) = \sigma_\varepsilon^2 \left|1-e^{-i2\pi\nu}\right|^{-2d} \frac{\left|1-\theta e^{-i2\pi\nu}\right|^2}{\left|1-\phi e^{-i2\pi\nu}\right|^2}$$

Monitoring platform



Traces for validation

Data	Date (start time)	T (s)	Network link	# Pkts (10^6)	IAT (ms)	Repository
PAUG	1989-08-29(11:25)	2620	LAN(100BaseT)	1	2.6	ita.ee.lbl.gov/index.html
LBL-TCP-3	1994-01-20(14:10)	7200	WAN(100BaseT)	1.7	4	ita.ee.lbl.gov/index.html
AUCK-IV	2001-04-02(13:00)	10800	WAN(OC3)	9	1.2	wand.cs.xaikato.ac.nz/wand/wits
CAIDA	2002-08-14(10:00)	600	Backbone(OC48)	65	0.01	www.caida.org/analysis/workload/oc48/
UNC	2003-04-06(16:00)	3600	WAN(100BaseT)	4.6	0.8	www-dirt.cs.unc.edu/ts
METROSEC-ref1	2004-12-09(18:30)	5000	LAN(100BaseT)	3.9	1.5	www.laas.fr/METROSEC
METROSEC-ref2	2004-12-10(02:00)	9000	LAN(100BaseT)	2.1	4.3	www.laas.fr/METROSEC
METROSEC-DDoS	2004-12-09(20:00)	9000	LAN(100BaseT)	6.9	1.3	www.laas.fr/METROSEC
METROSEC-FC	2005-04-14(14:30)	1800	LAN(100BaseT)	3.7	0.48	www.laas.fr/METROSEC

Traffic traces with anomalies

- TAuckland traces – NLANR project
- and
- MétroSec traces

Anomaly	Quantity	Tool	Intensity
Flash crowd	4	Server web	34% - 71%
DDoS	4	Hping	28% - 99%
	10	Iperf	15% - 58%
	3	Trinoo	7% - 87%
	9	TFN2K	4% - 92%
	12	TFN2K Modifié	1% - 4%

$\Gamma_{\alpha,\beta}$ – farima (ϕ, d, θ) model validation

- **Parameters estimation:**
  - **1st order:** Instead of the usual moment based technique which estimates μ and σ^2, we use maximum likelihood based estimates for α and β.
  - **2nd order: LRD** (long memory) estimated with a multi-resolution analysis, characterized by ***d***, the long memory parameter measured on an aggregation range Δ for which the log scale diagram is linear.

    From this wavelet base estimation of d, we perform a fractional derivation of X_Δ. This removes the long memory from the process so that only the ARMA component is left. ϕ and θ are easy to estimate with an iterative procedure based on the **Gauss-Newton** algorithm.

$\Gamma_{\alpha,\beta}$ – farima (ϕ, d, θ) model validation

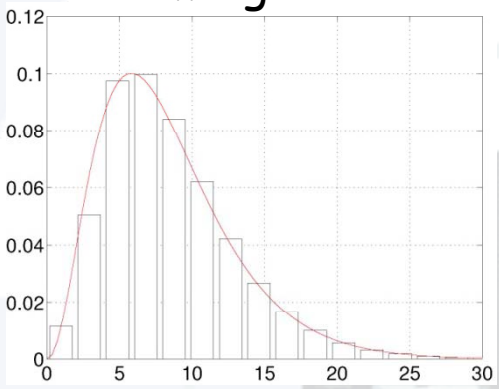
- To assess the validity of the model with actual traffic traces, we made a comparative analysis of :
  - Actual traces time series
  - $\Gamma_{\alpha,\beta}$ – farima (ϕ, d, θ) time series produced by a numerical generator designed for this purpose

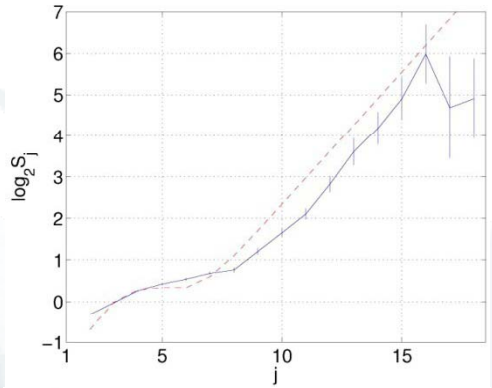
AUCK-IV: $\Gamma_{\alpha,\beta}$ – farima (ϕ, d, θ) fits

marginals

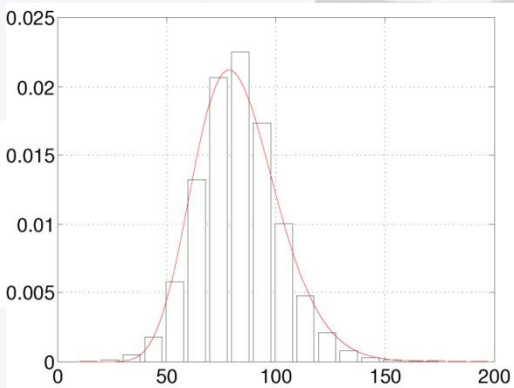
covariances

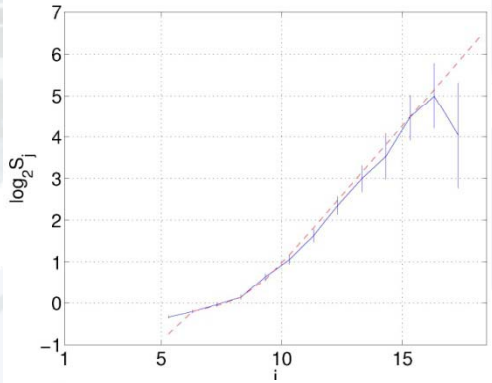
Δ=10ms



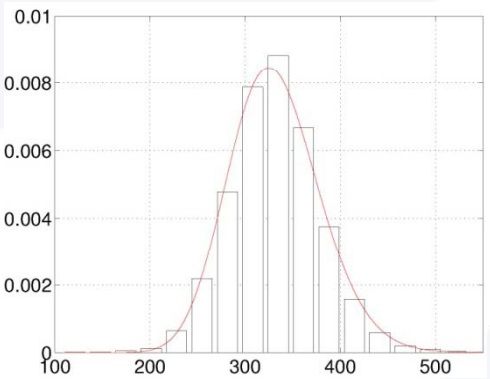


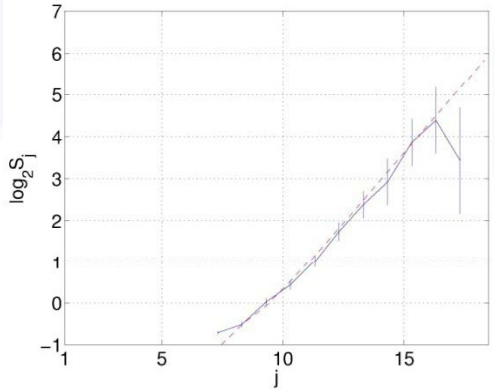
Δ=100ms





Δ=400ms





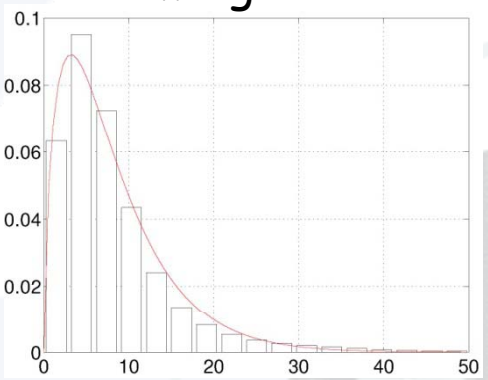
j=1 corresponds to 10 ms

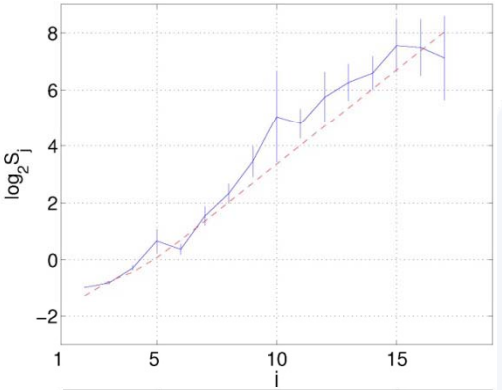
METROSEC-ref1: $\Gamma_{\alpha,\beta}$ – farima (ϕ, d, θ) fits

marginals

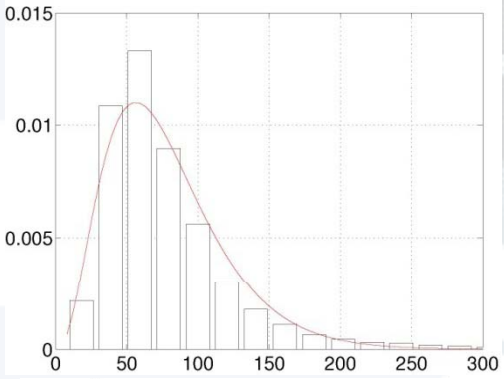
covariances

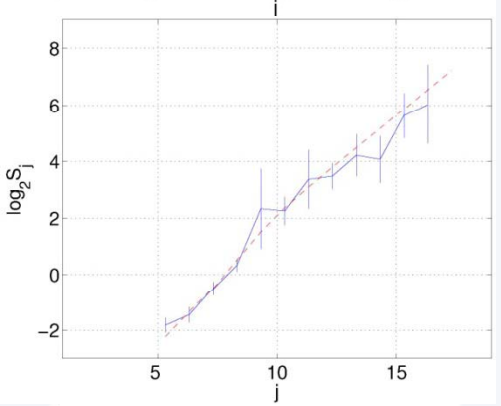
Δ=10ms



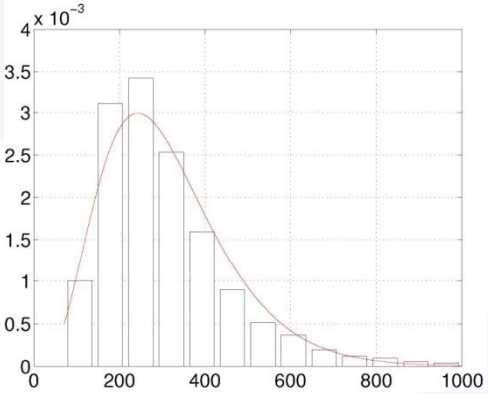


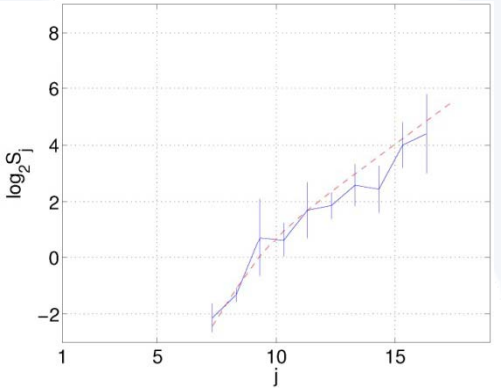
Δ=100ms





Δ=400ms





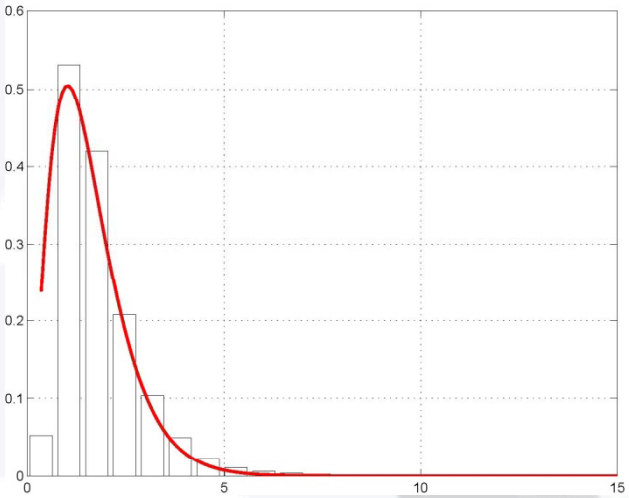
j=1 corresponds to 10 ms

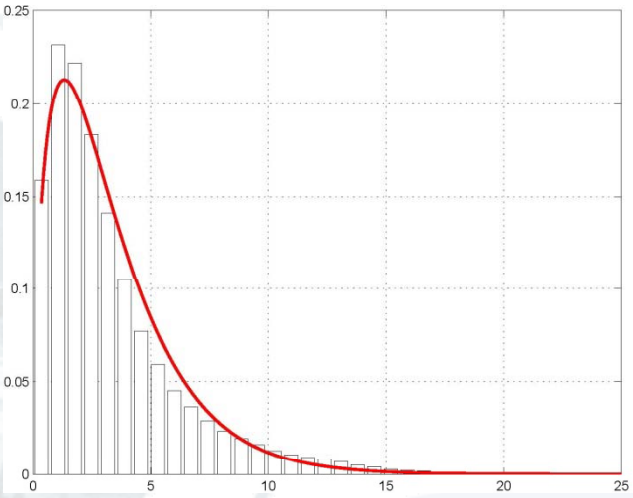
METROSEC-DDoS & FC: $\Gamma_{\alpha,\beta}$ marginals fits

DDoS attack

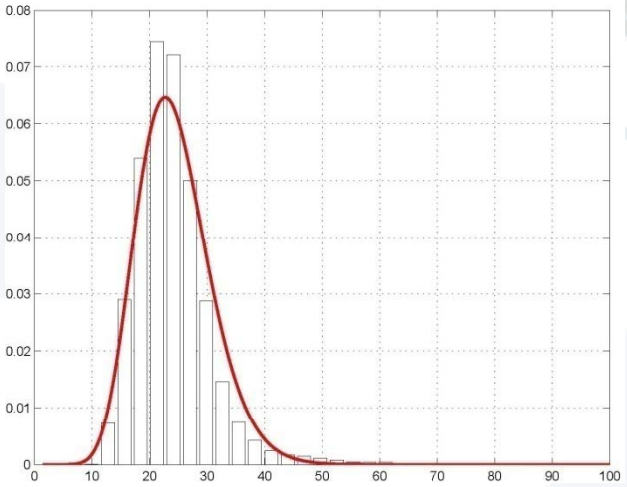
Flash crowd

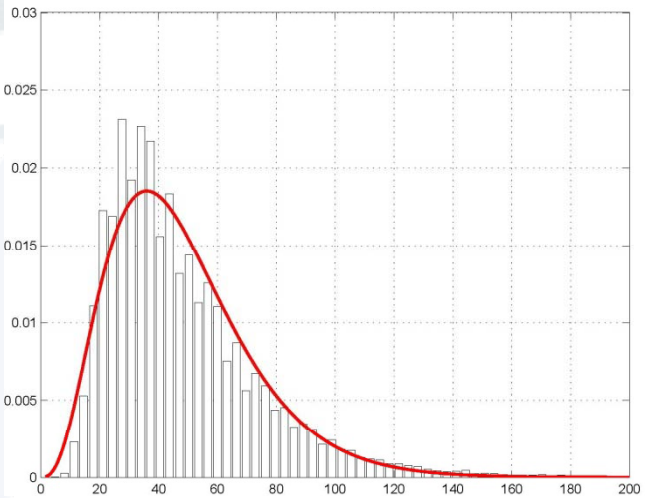
Δ=2ms





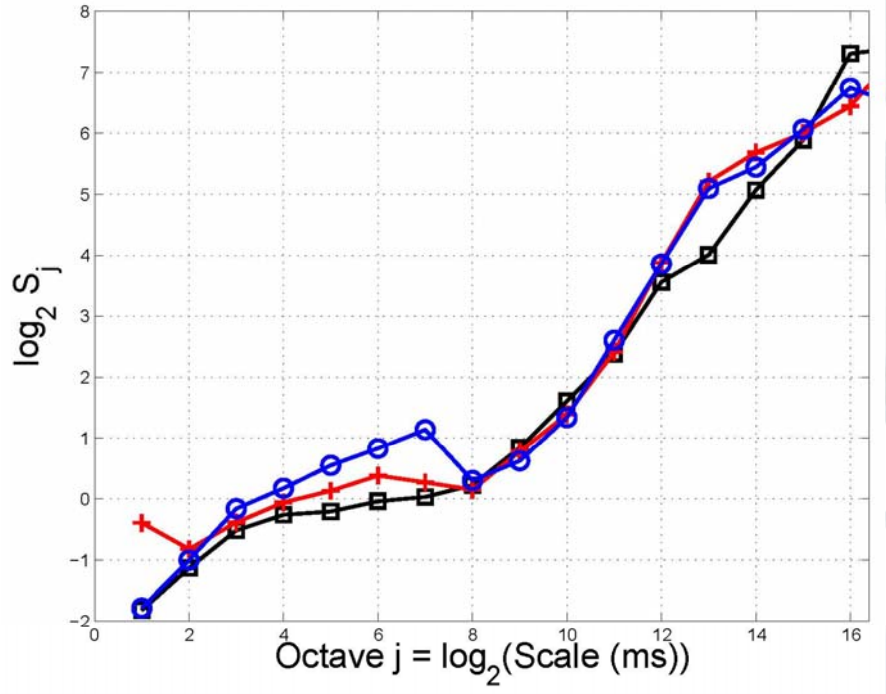
Δ=32ms



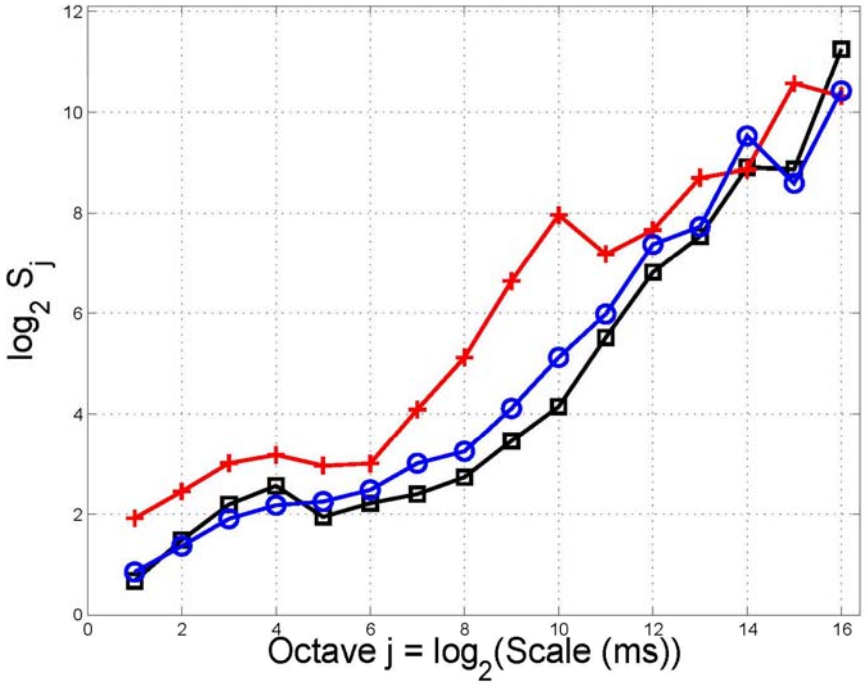


Logscale diagrams for METROSEC-DDoS & FC

DDoS



Flash Crowd



During
After
Before

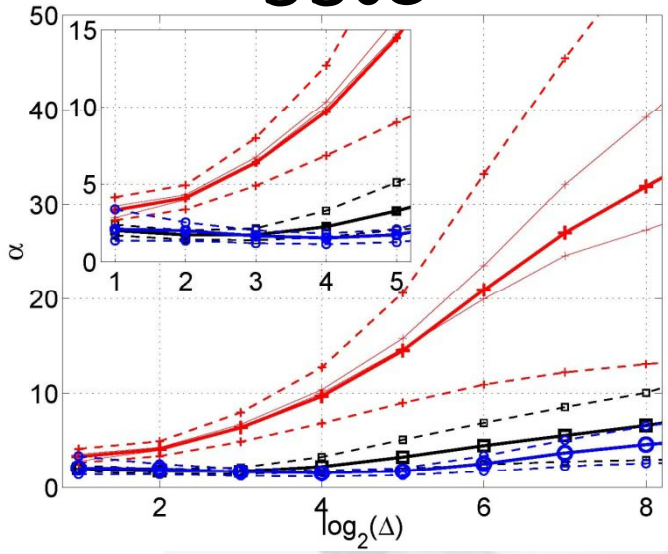
Estimated α and β as a function of $\log_2\Delta$

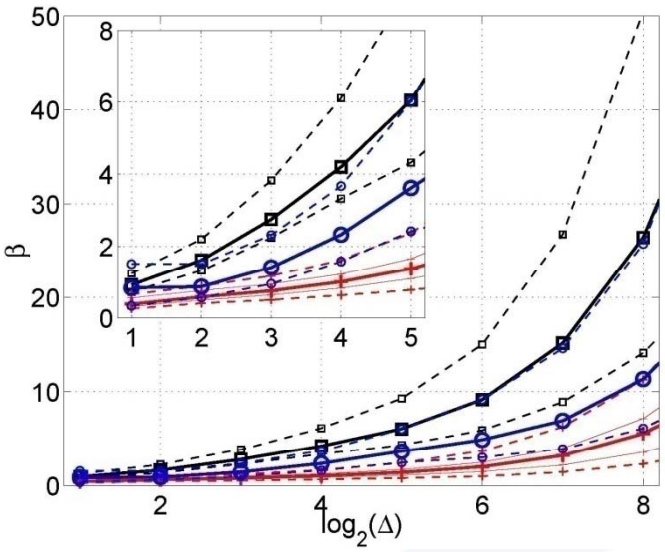
During
After
Before

α

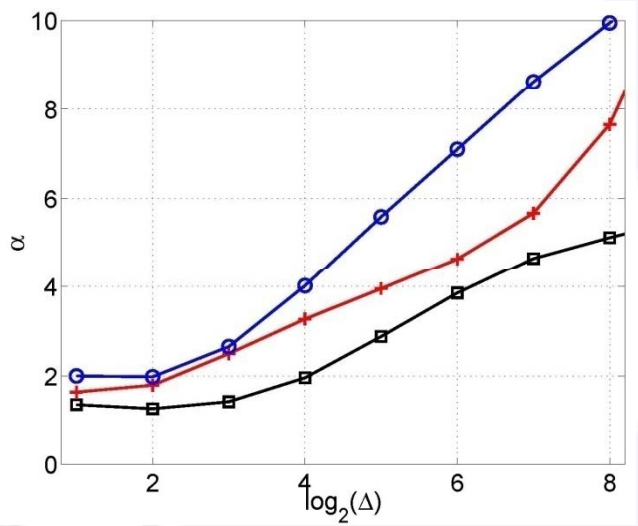
β

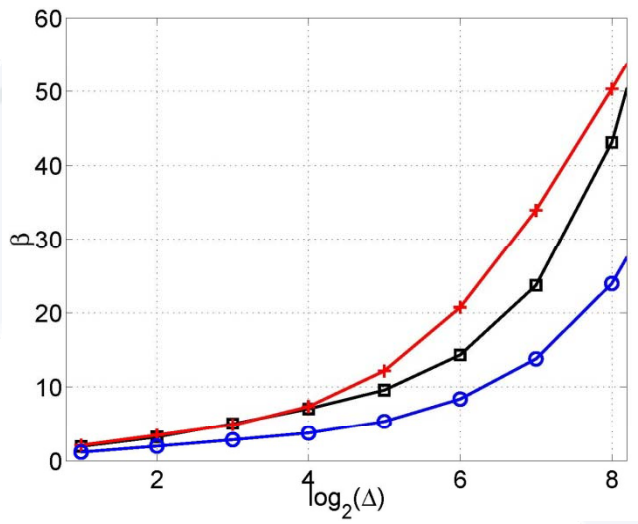
DDoS





Flash Crowd





DDoS impact on traffic

- α = shape parameter, $1/\alpha$ quantifies the gap with a Gaussian law
- β = scale parameter → decreases during DDoS attack

➔DDoS attack accelerates the convergence towards a Gaussian distribution of traces, and decreases the fluctuation scale around the average traffic

Partial conclusion

- Model for characterizing Internet traffic which works with and without anomalies
- Some parameters change differently in the presence of a legitimate (flash crowd) or illegitimate (DDoS) anomaly

➔How to use such model for an efficient and robust profile based IDS?

Detection principles

- Select a reference window
- Segment the trace into sliding windows of duration T
- For a window at time I:
  - Aggregated trace at scales $\Delta=2j$, $j=1,\ldots,J$
  - Estimation of parameters : $\alpha_\Delta(I)$, $\beta_\Delta(I)$
  - Compute the distance to the reference, between I and R: D(I)
  - Selection of a threshold λ:
    - if $D(I) \geq \lambda$, $\Rightarrow$ anomaly

Selection of the best distance (Basseville 89)

- Quadratic distance on parameters

$$D_\alpha(I) = \frac{1}{j}\sum_{j=1}^{J}(\alpha_{2j}(I) - \alpha_{2j}(R))^2$$

$$D_\beta(I) = \frac{1}{J}\sum_{j=1}^{J}(\beta_{2j}(I) - \beta_{2j}(R))^2$$

- Divergence of Kullback-Leibler; p1 and p2 are 2 p.d.f.

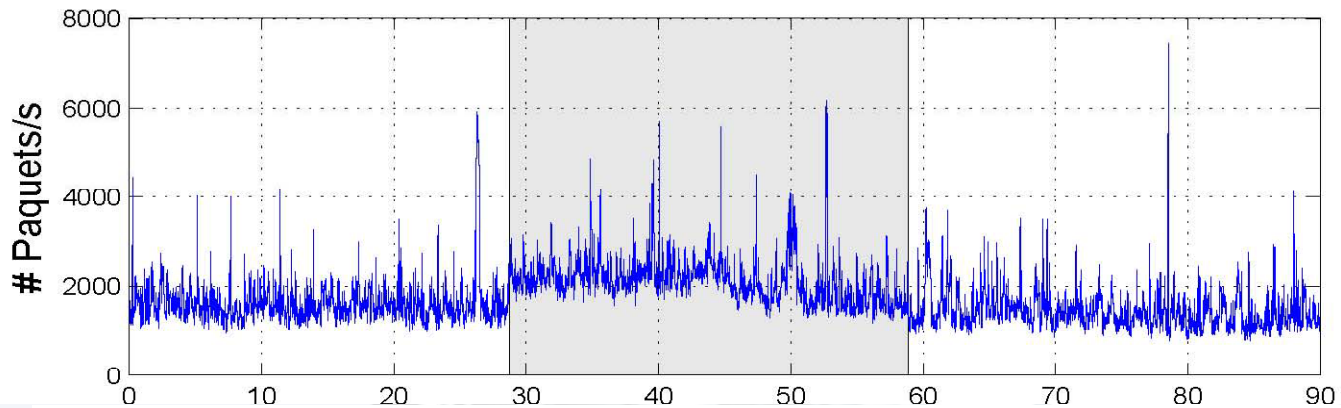
$$DK(p_1, p_2) = \int (p_1(x) - p_2(x))(\ln p_1(x) - \ln p_2(x))dx$$

giving a distance with one or two scales:

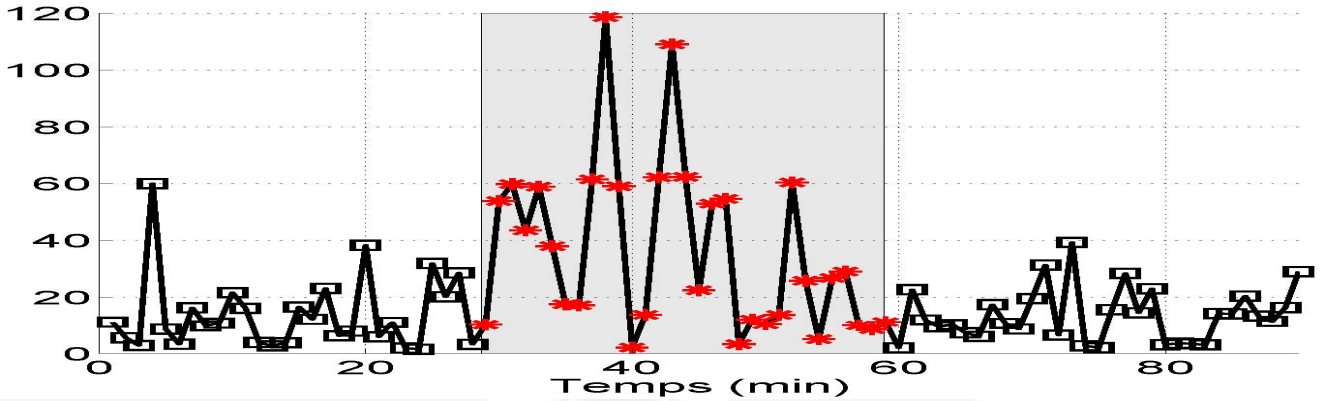
$$K_{\Delta}^{(1D)}(I) = DK(p_{\Delta,I}, p_{\Delta,R})$$

$$K_{\Delta,\Delta'}^{(2D)}(I) = DK(p_{\Delta,\Delta',I}, p_{\Delta,\Delta',R})$$

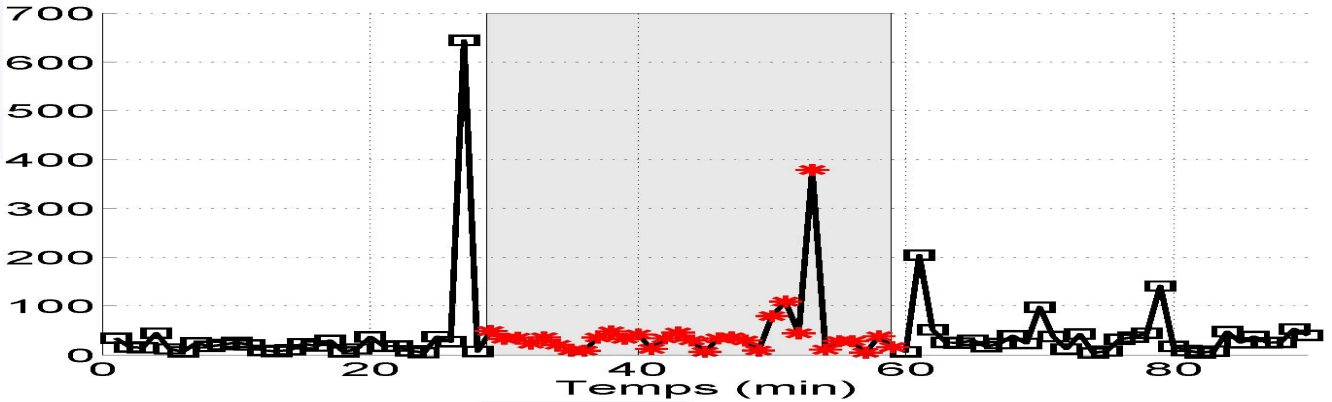
Ex. 1 : Denial of Service attack



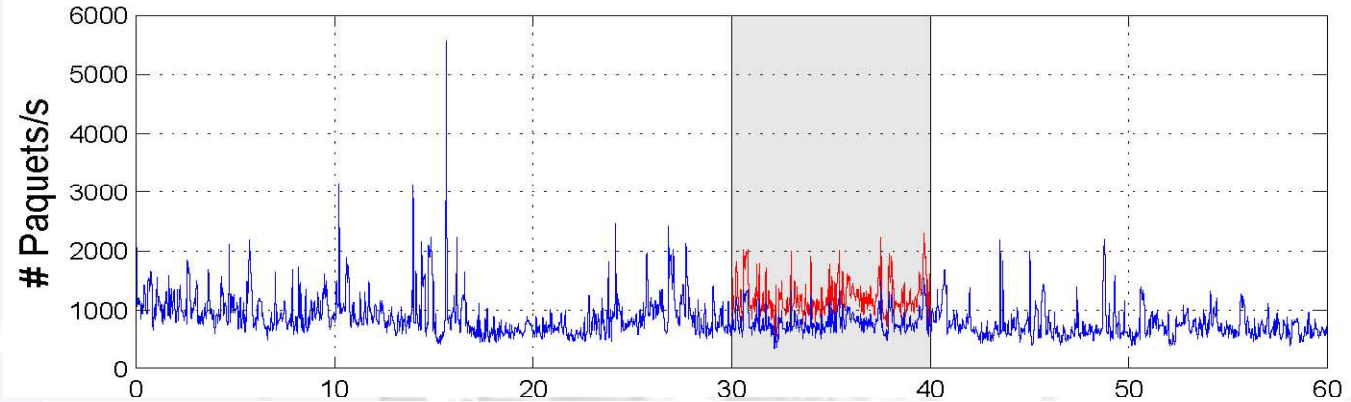
$D_\alpha(I)$



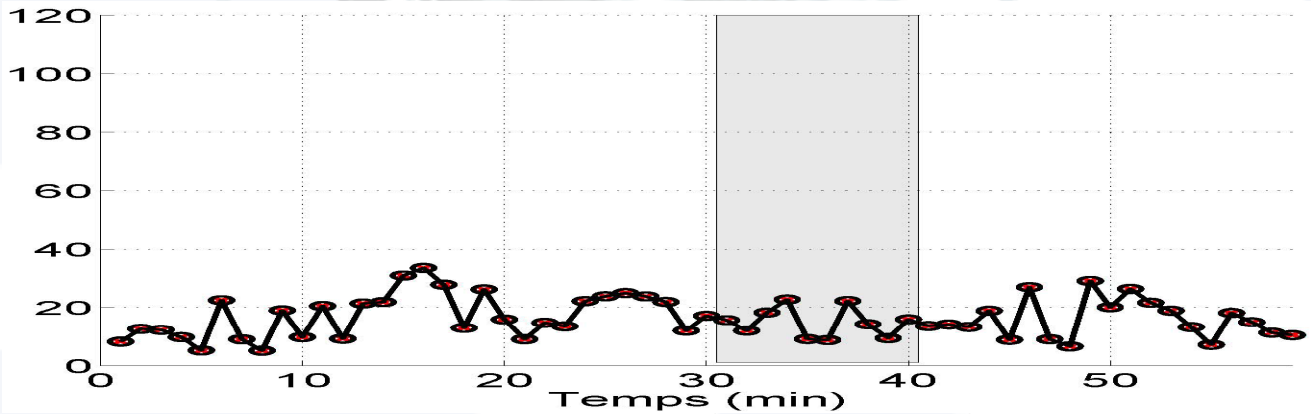
$D_\beta(I)$



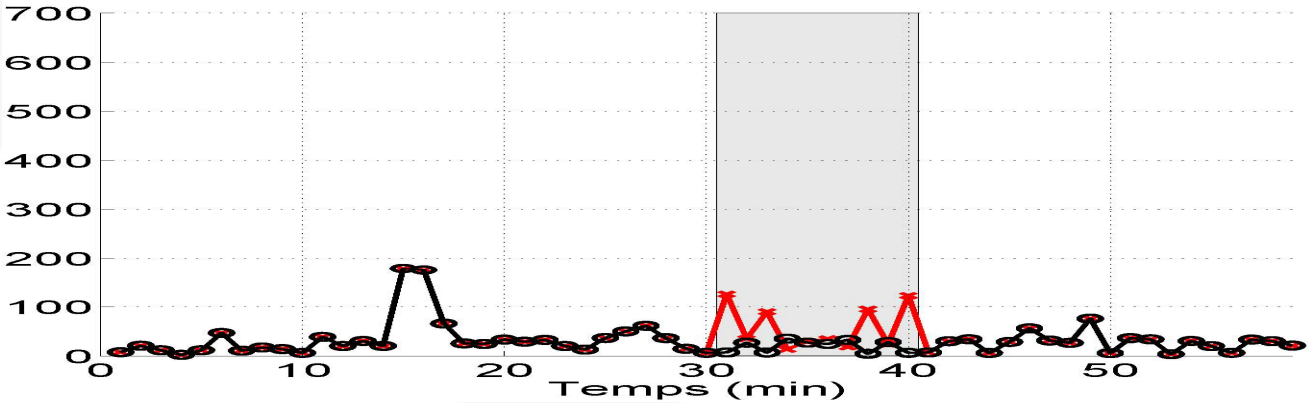
Ex. 2: Multiplicative increase of traffic



$D_\alpha(I)$

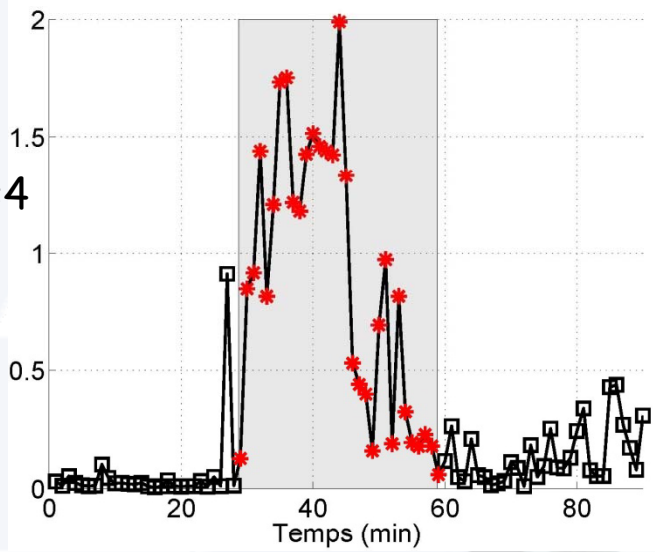


$D_\beta(I)$

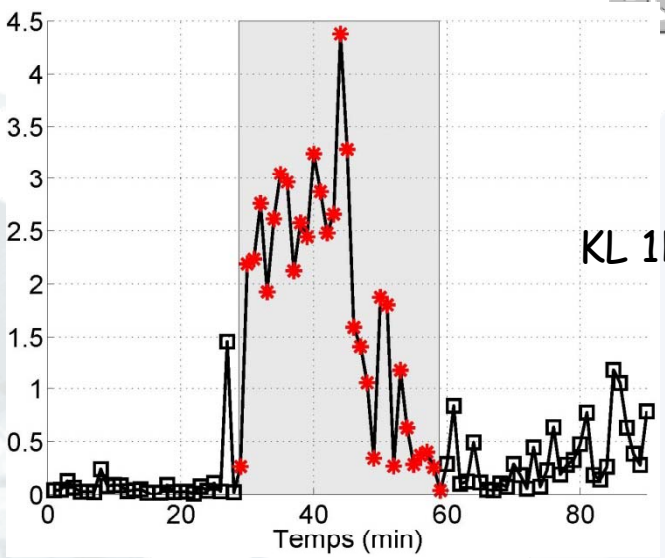


Ex. 3: Comparison between distances

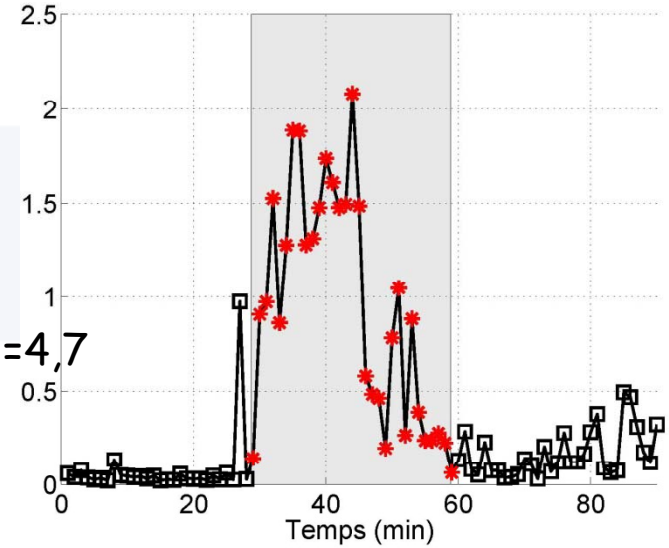
KL 1D, j=4



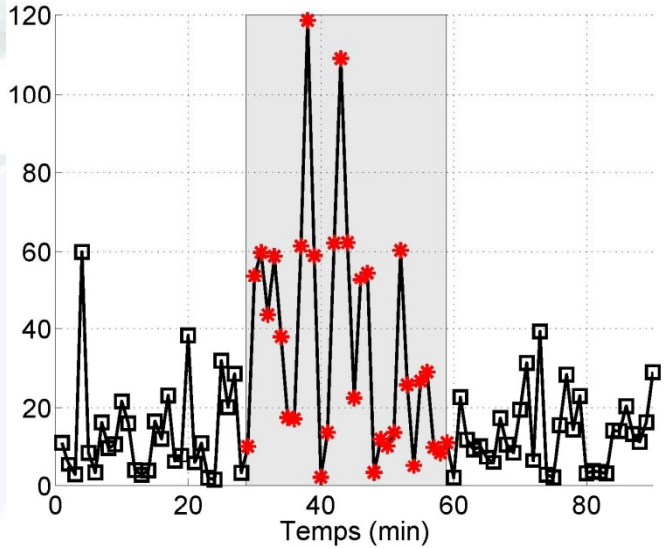
KL 1D, j=7



KL 2D, j=4,7

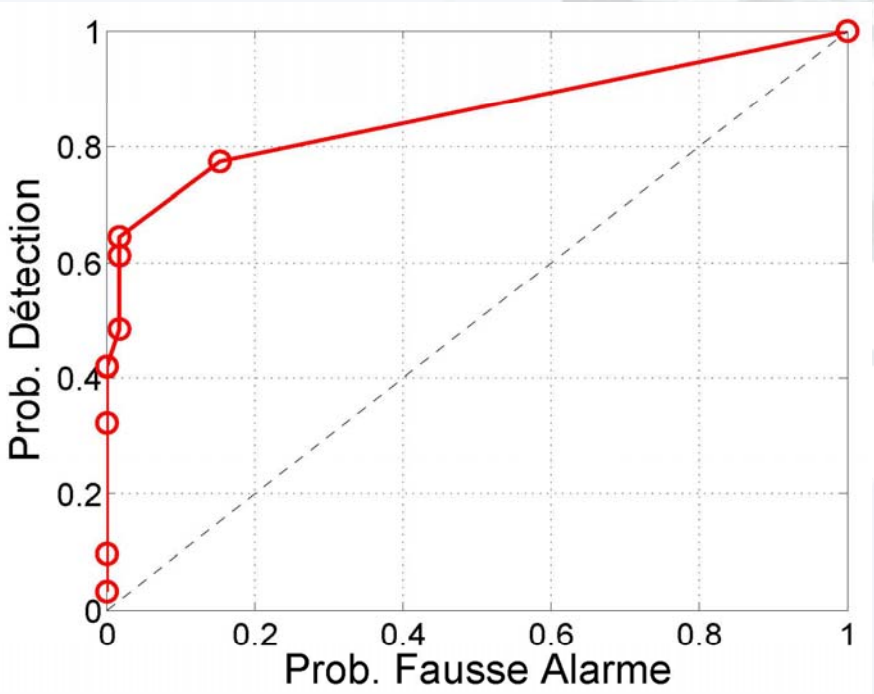


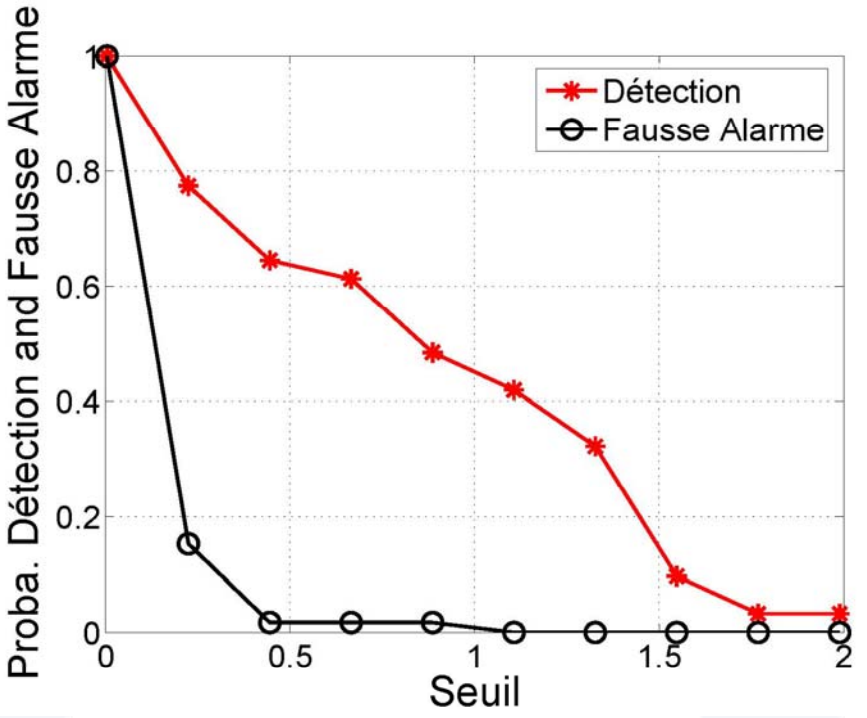
D_α



Statistical performance: ROC curves

- ROC curves: detection probability according to the fixed probability of false alarms
- $P_D=f(P_{FA})$ or $P_D=f(\lambda)$, $P_{FA}=f(\lambda)$





Conclusion on anomalies/attacks detection

- Parameters of the $\Gamma_{\alpha,\beta}$ - farima (ϕ, d, θ) model change differently depending on the type of anomaly
- Kullback- Leibler distance allows a robust detection of attacks, even when they represent less than 1% of the traffic (and is not sensitive to an artificial increase of the amount of traffic)

➔BUT: it is not possible with this method to identify anomaly constituting packets / flows

Objectives

- Define an approach to
  - Detect
  - Classify
  - Identify

  traffic anomalies (One or more occurrences that change the normal flowing of data over a network)
- Define a signature for each traffic anomaly, based on "simple" parameters

→must be easy to handled by network administrators

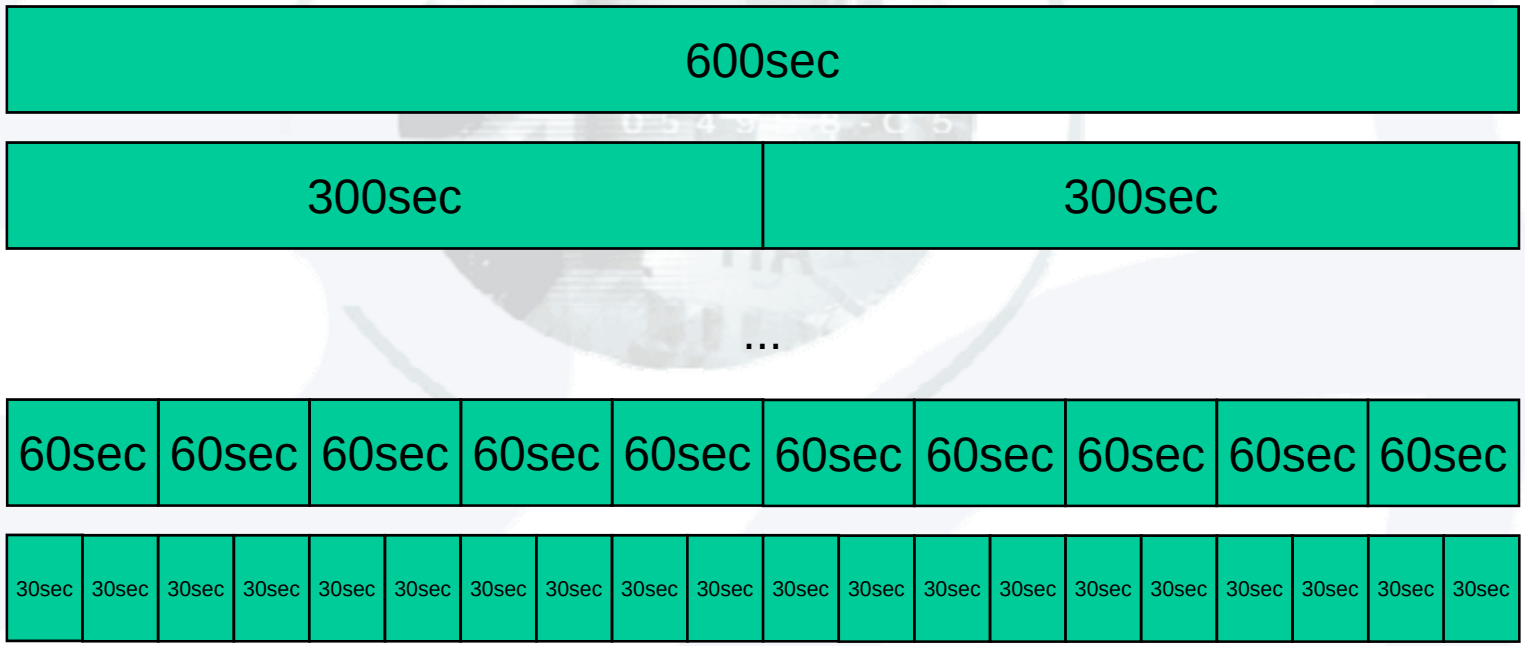
→must permit the design of IPS

The NAD Algorithm …

- Multi-scale concept
- Tomography-based concept
- Generic multi-criteria
  - Uses simple mathematical functions, as volume parameters, to detect anomalous flows
    - Number of packets per unit of time
    - Number of bytes per unit of time
    - Number of new flows per unit of time
  - Uses IP features (addresses and ports) to identify the anomalies

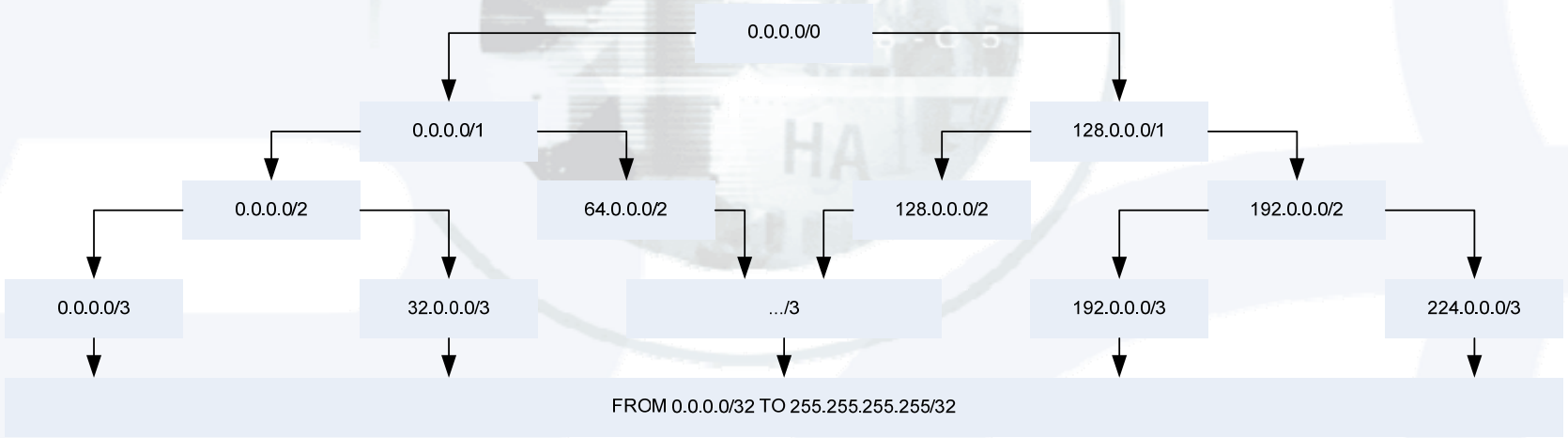
The NAD Algorithm ...(2)

Multi-Scale



The NAD Algorithm ...(3)

Tomography



Formal Definition

- To detect an anomaly it must be responsible for a significant variation in one of the parameters

  → deltoid based method

Let, X = {x1,x2,...,xn}, xi = #{packet | byte | flows} and packet

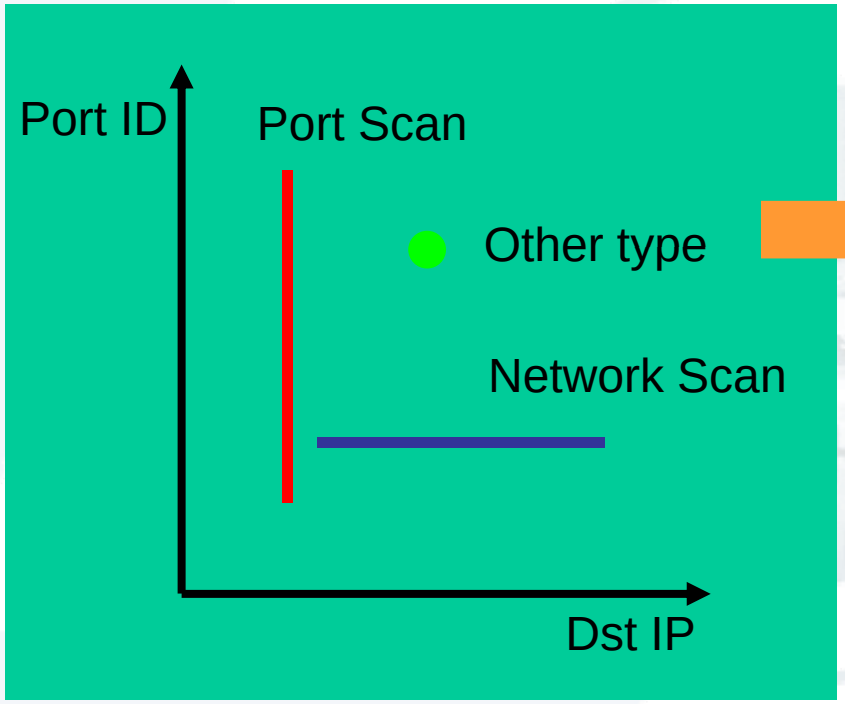
$$\Delta = time\_granularity$$

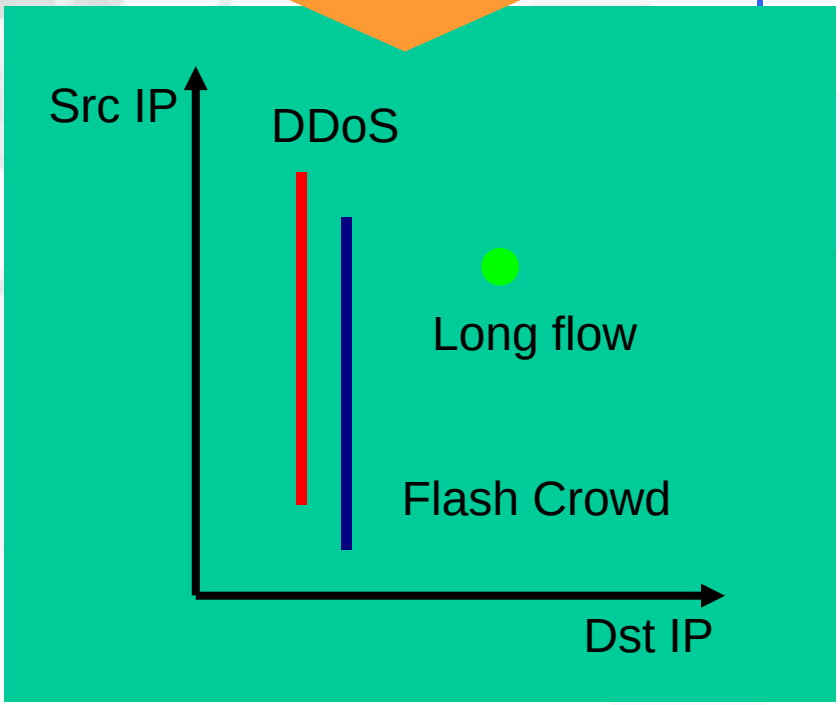
$$X = \{x_1, x_2, ..., x_n\}, x_i = \{\#\ packets\ |\#\ bytes\ |\#\ flows\}/\Delta$$

$$P = \{p_1, p_2, ..., p_{n-1}\}, p_i = x_{i+1} - x_i$$

$$\begin{cases} pi \geq E(p) + k\sigma, select \\ pi < E(p) + k\sigma, reject \end{cases}$$

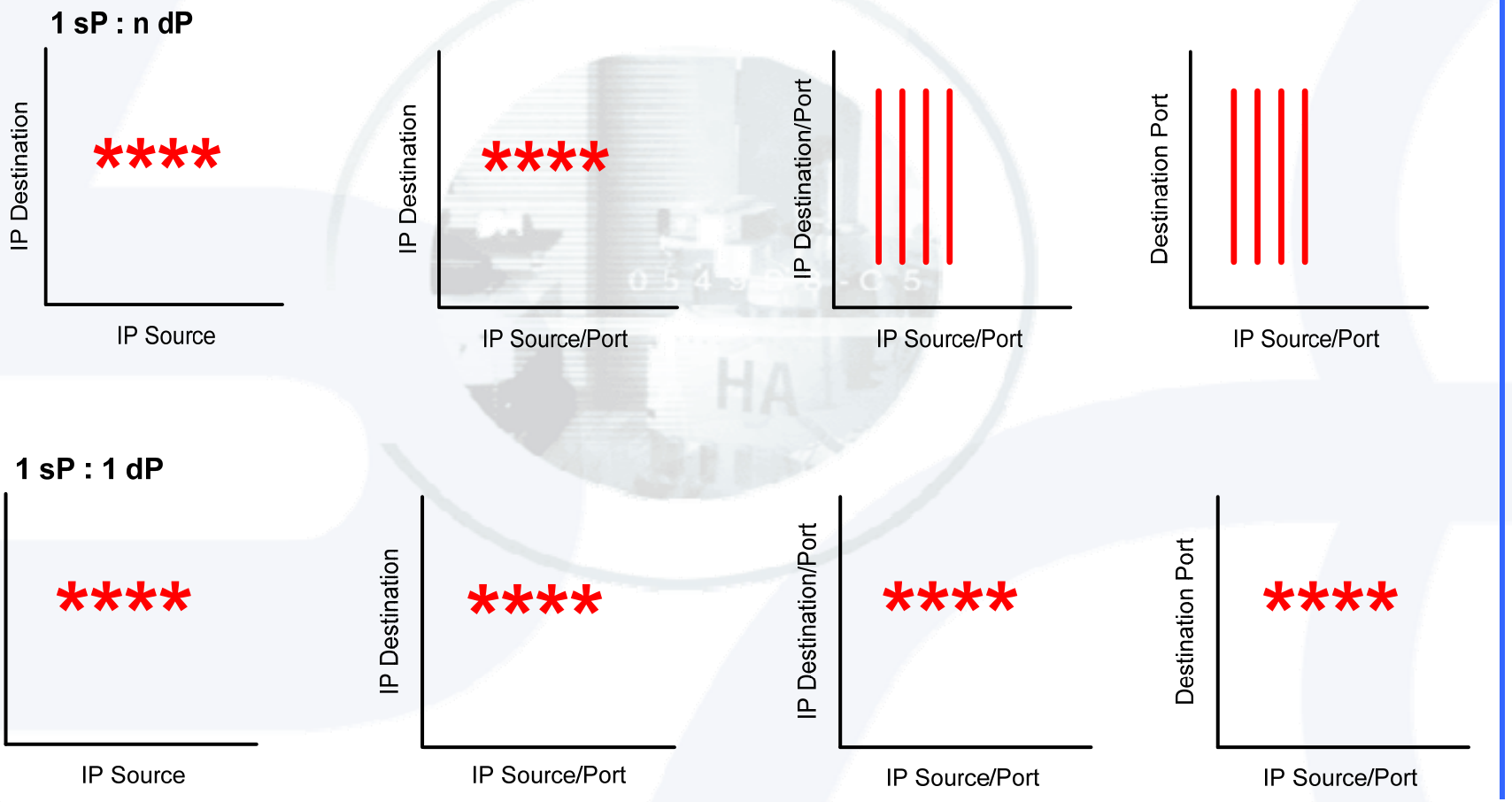
Some Types of Anomalies



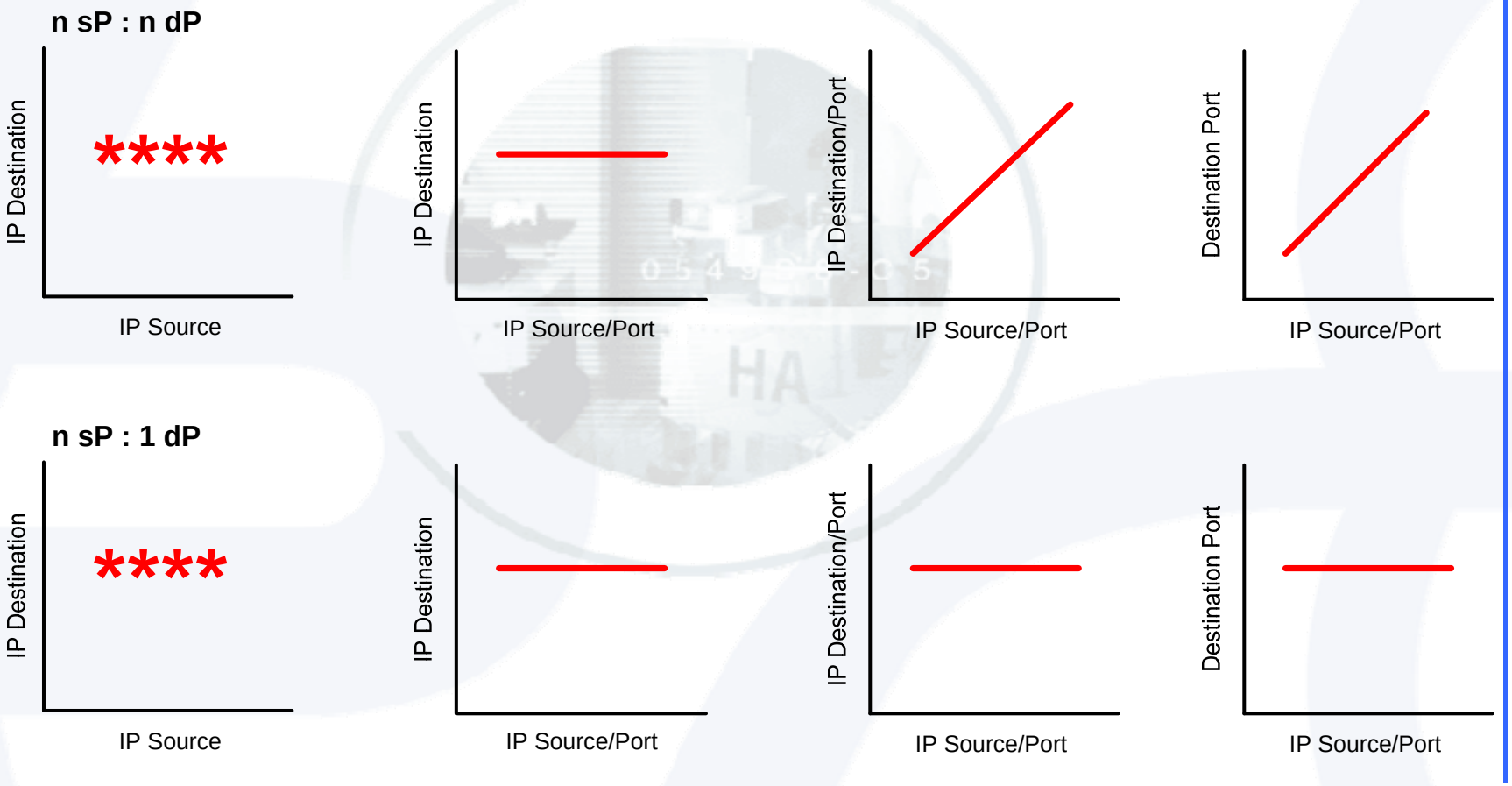


The distribution of points in plots can give a clue about the type of anomaly!

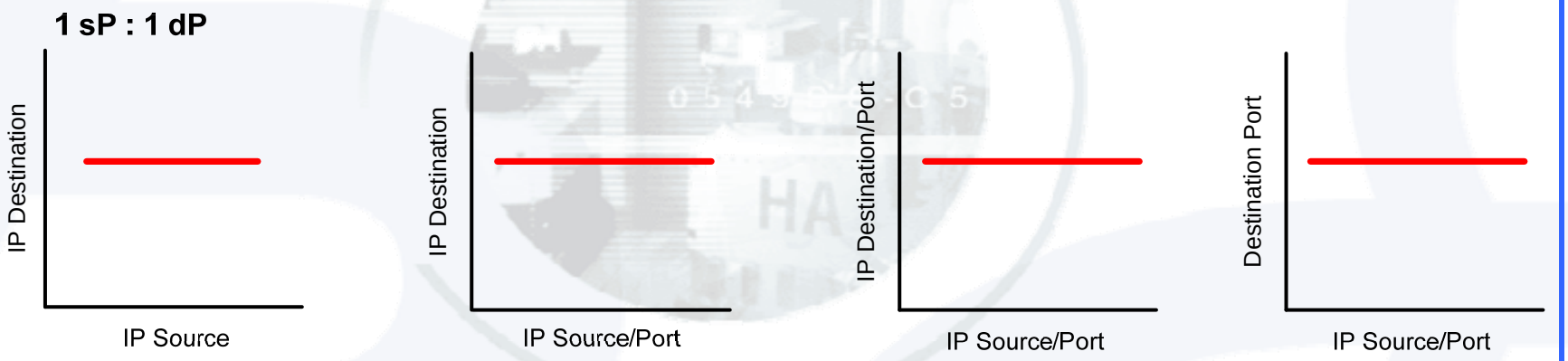
DDoS : N attackers → 1 target



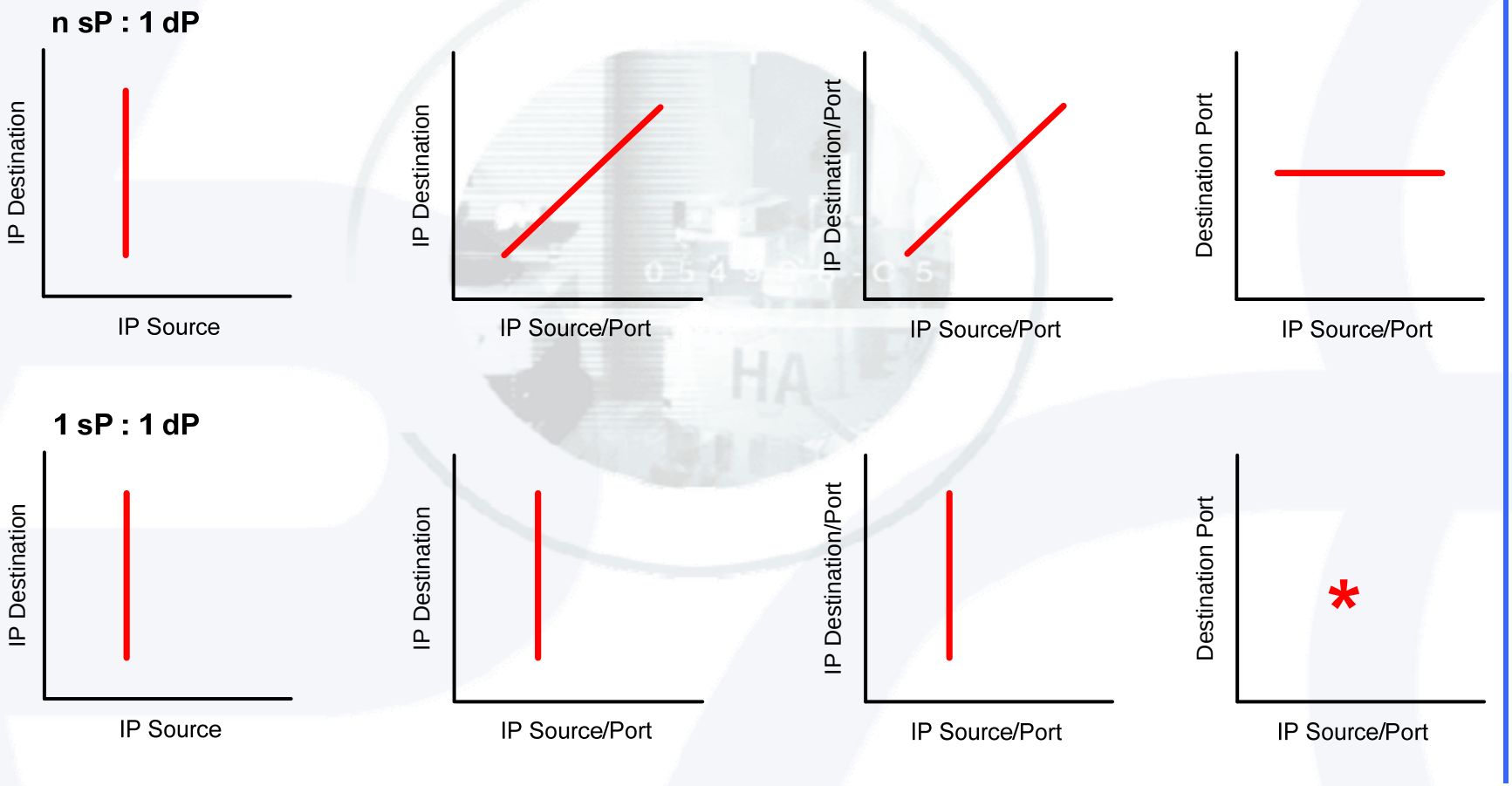
DDoS: N attackers → 1 target (cnd)



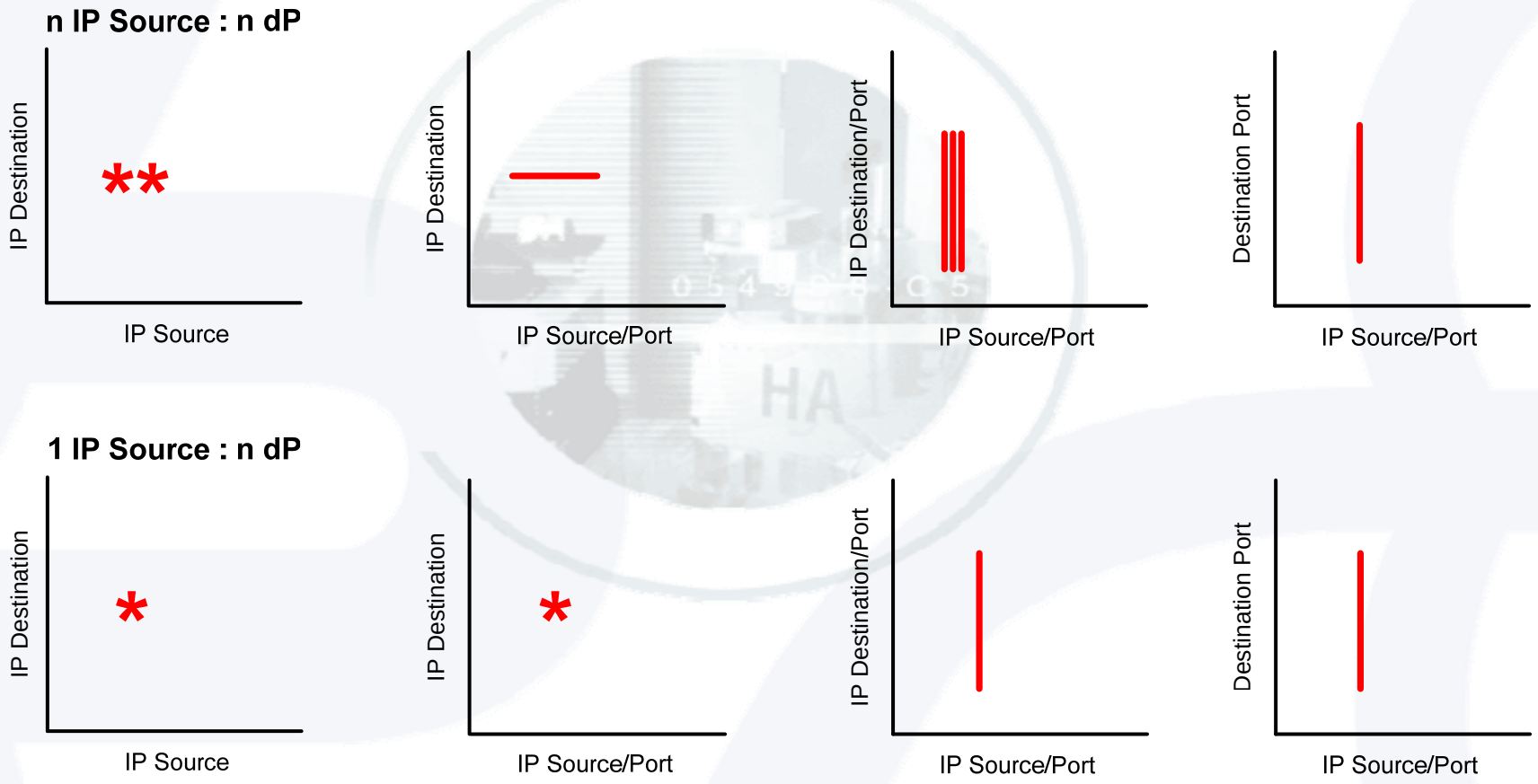
Flash crowd


1 sP : 1 dP
IP Destination
IP Source
IP Destination
IP Source/Port
IP Destination/Port
IP Source/Port
Destination Port
IP Source/Port

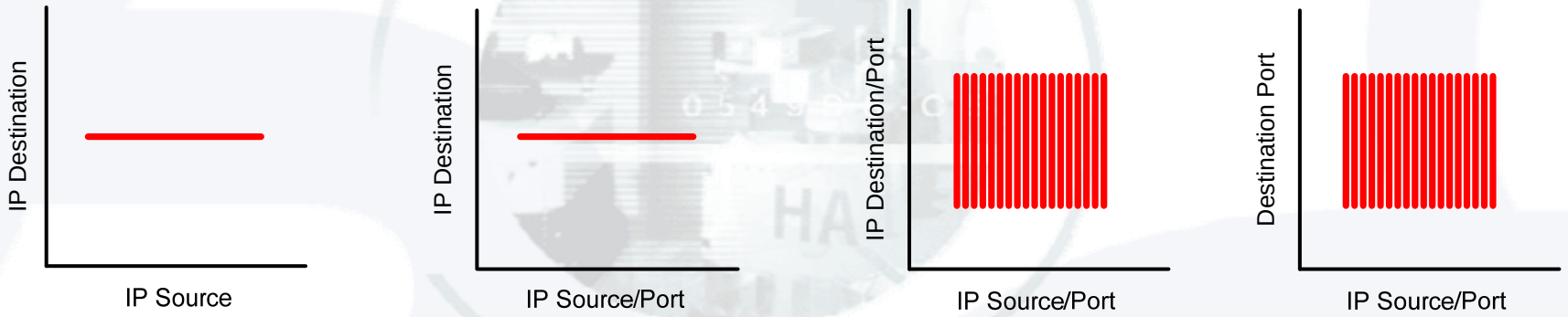
Network scan



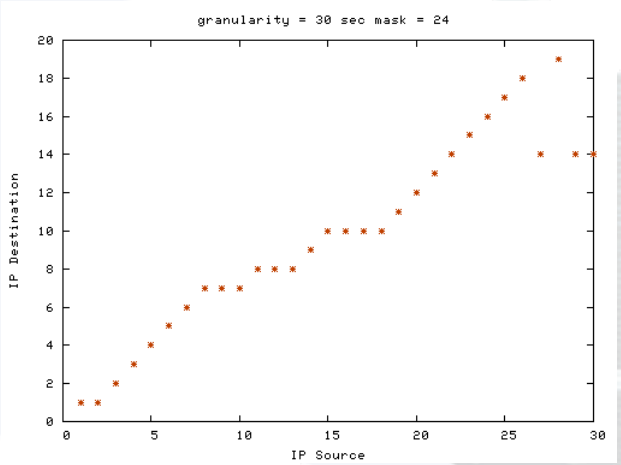
Ports scan

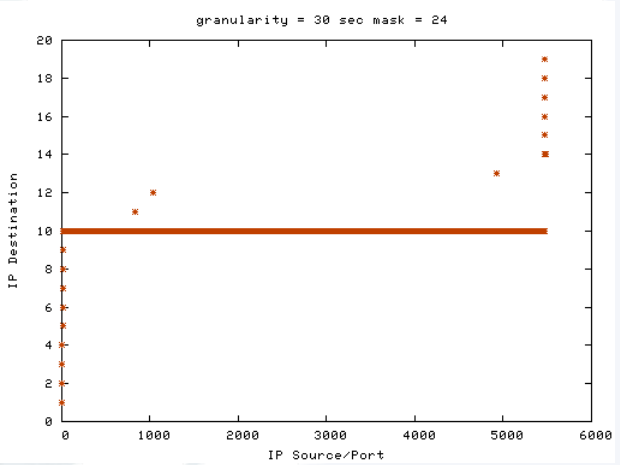

n IP Source : n dP
IP Destination
IP Source
IP Source/Port
IP Destination/Port
Destination Port
1 IP Source : n dP

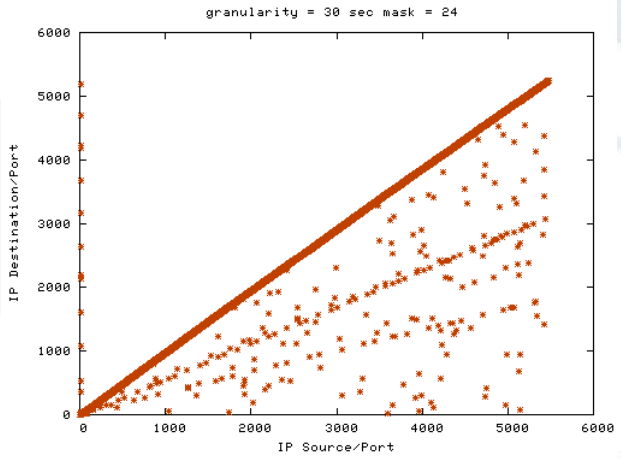
Brute force attack

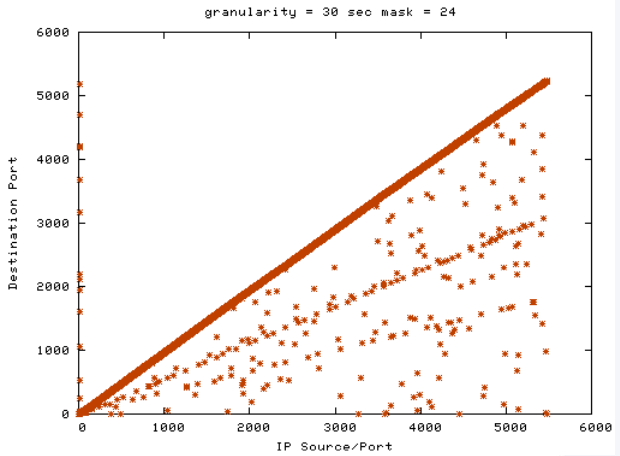


DDoS example

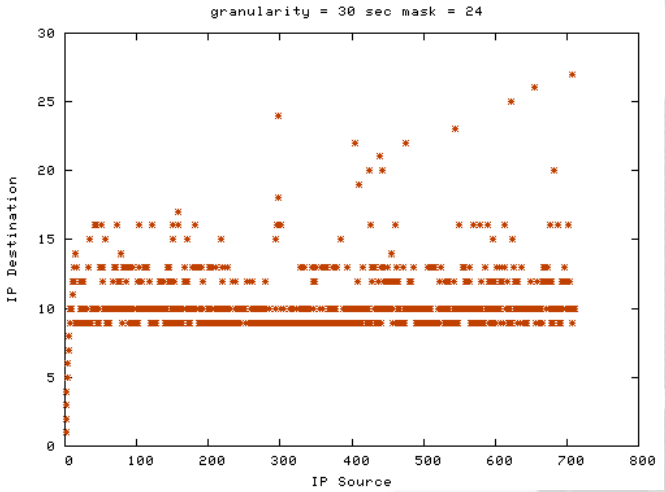


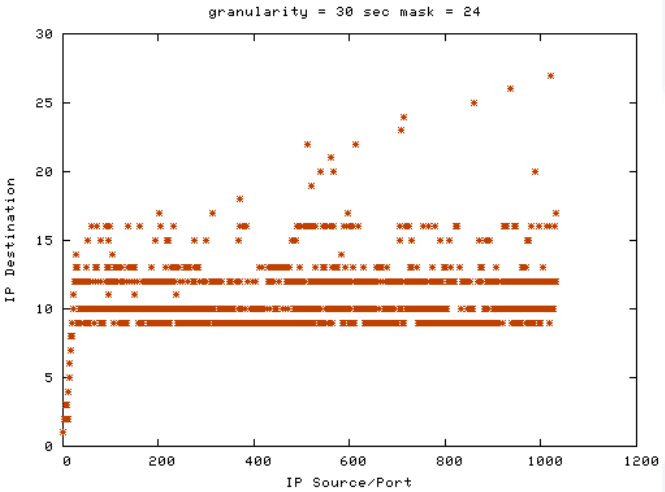


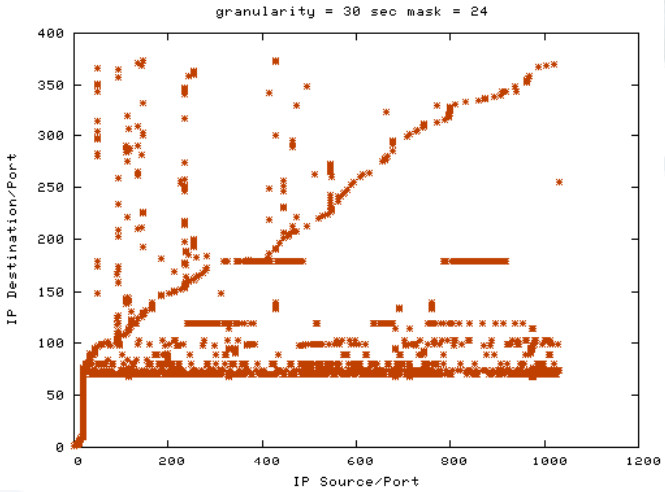


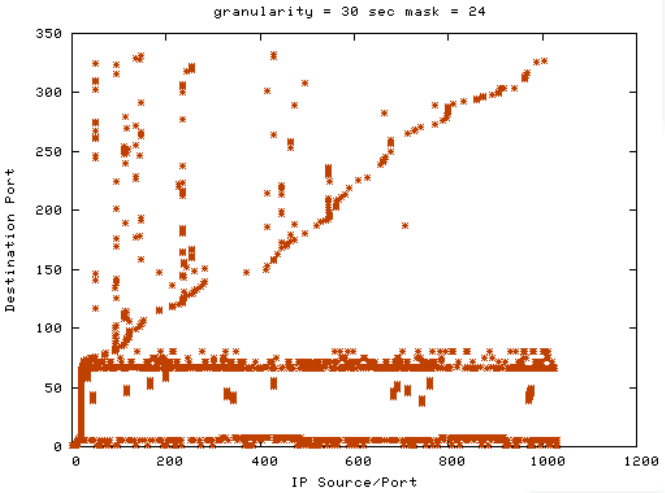


Flash crowd example

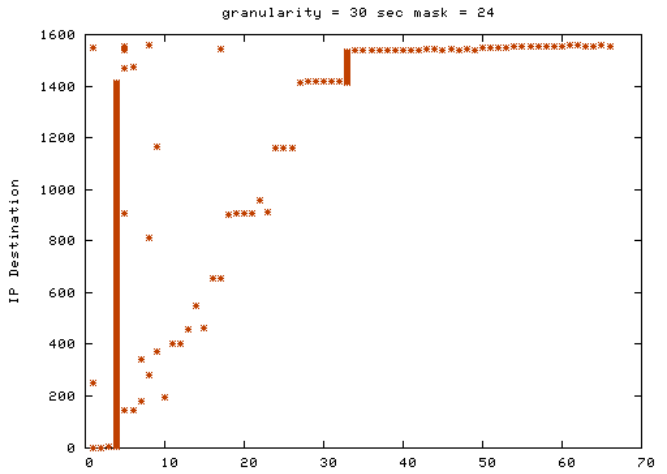


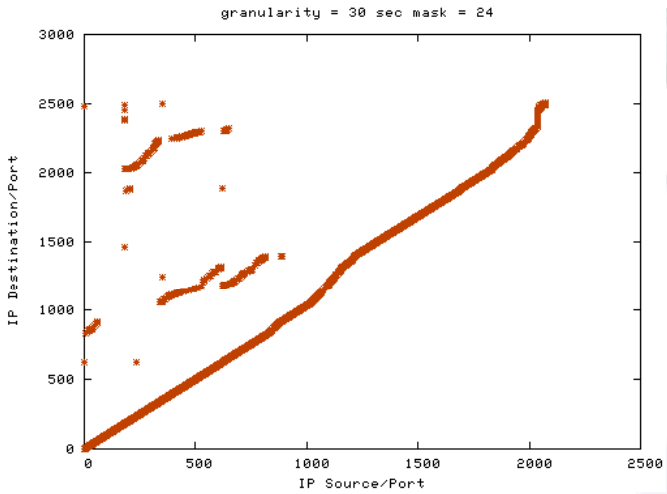


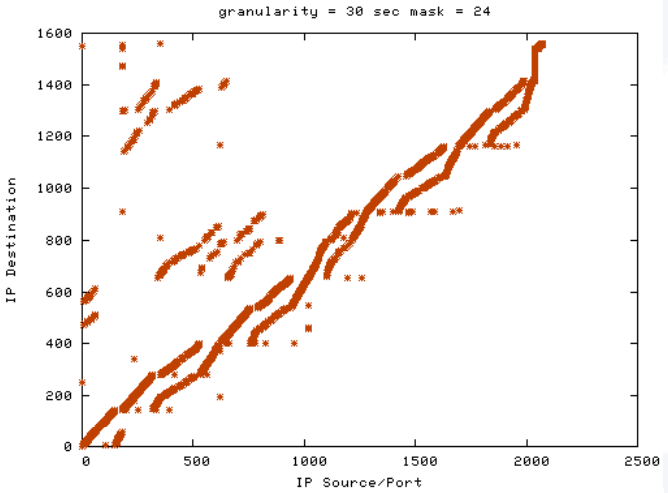


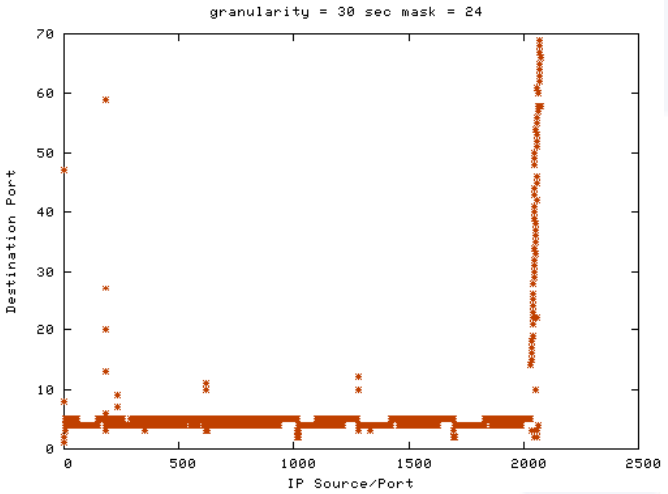


Network scan example

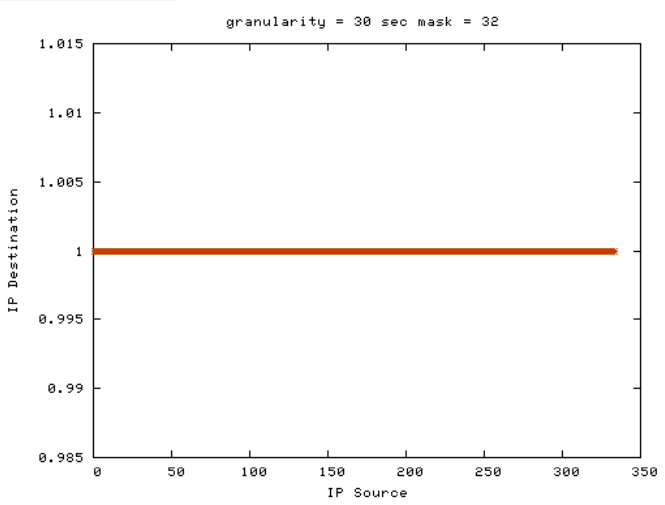


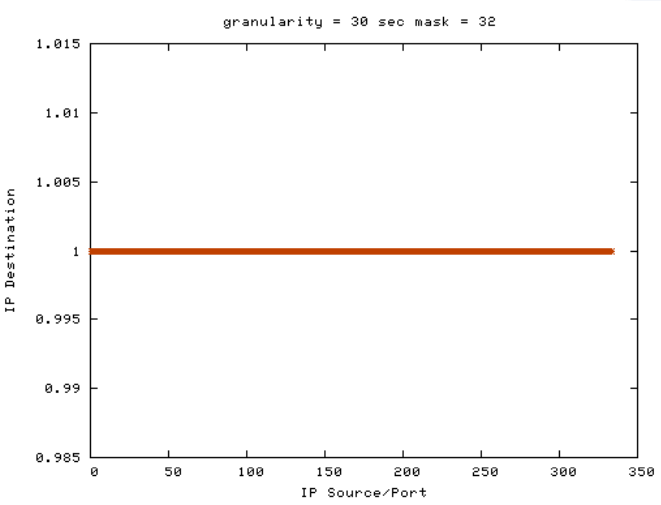


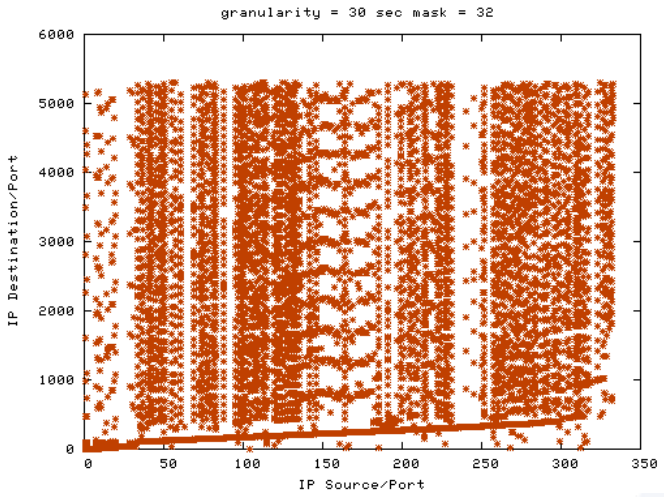


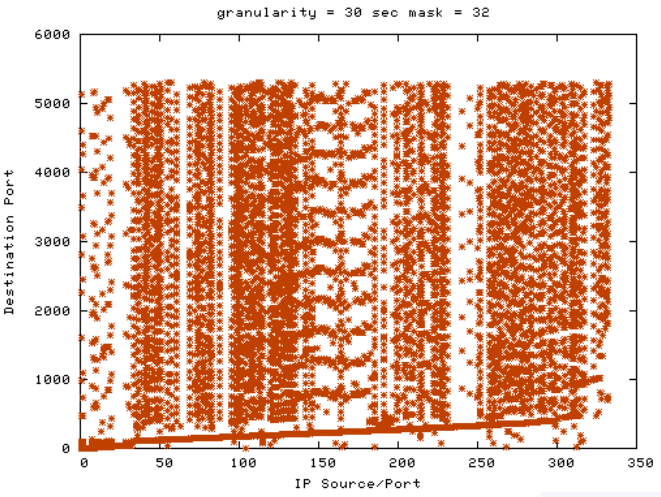


Brute force attack example

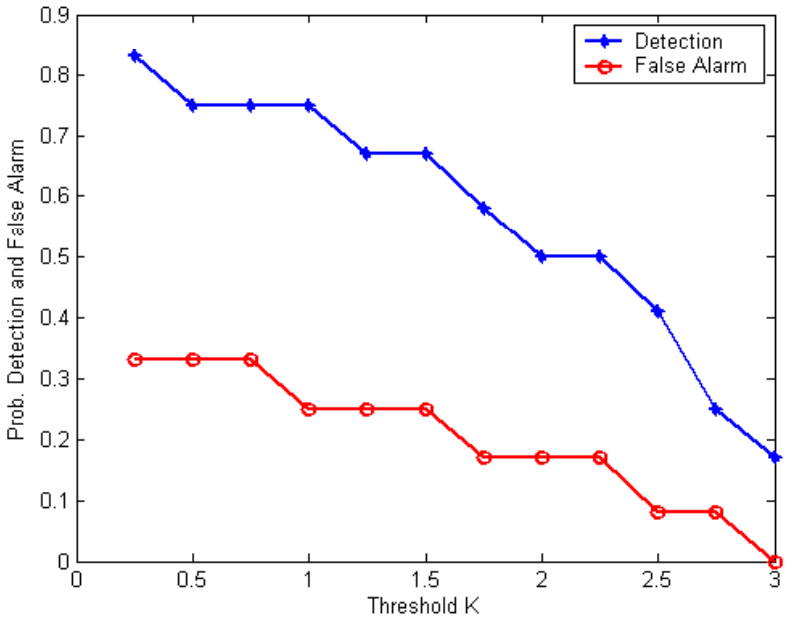


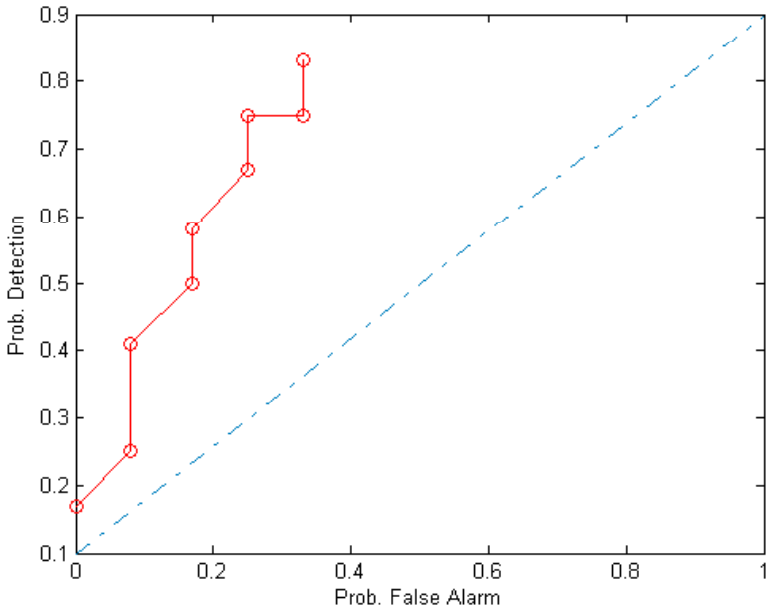




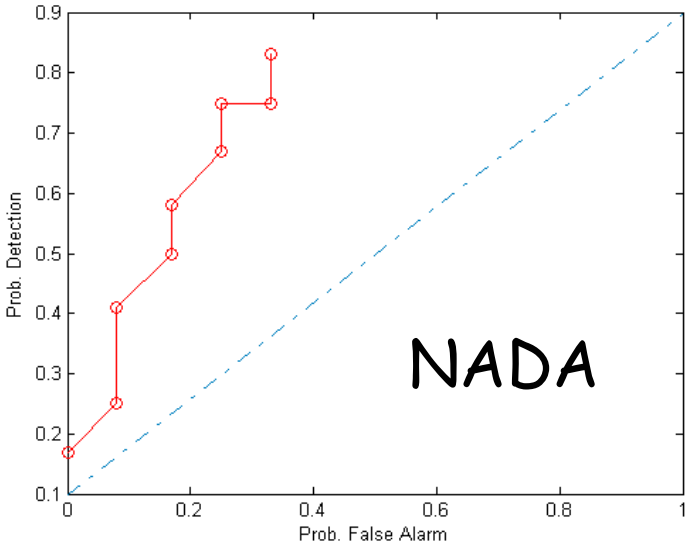


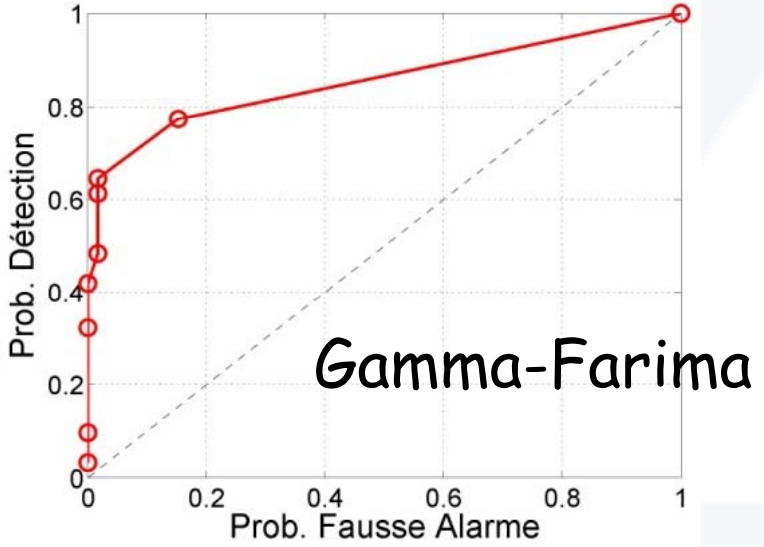
NAD tool assessment

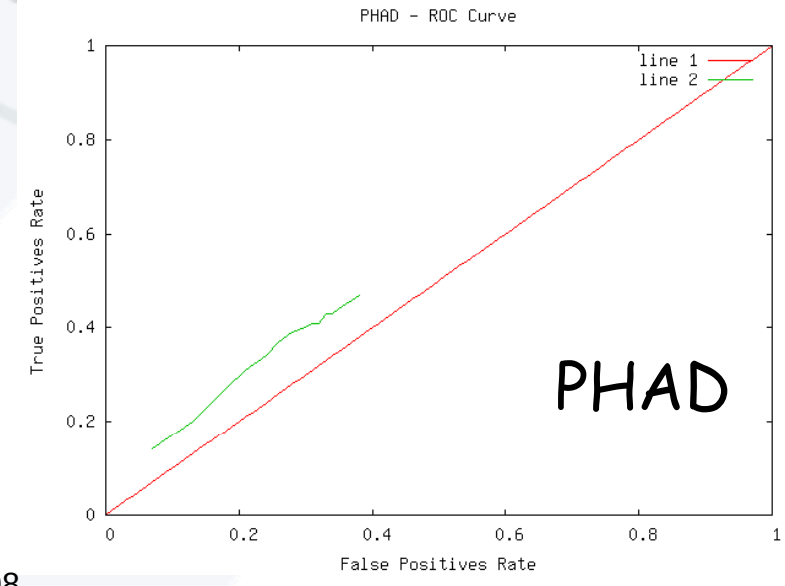




Comparison with other tools







Conclusion

- Experimental platform with monitoring and measurement capabilities
- IDS assessment methodology (KDD is dead : RIP)
- Its related database of traces with anomalies
  - Unfortunately not publicly available : cf. CNIL
- Original anomalies detection, classification and identification algorithms
  - Which proved to be efficient and accurate
  - Which raised many interests : FT, WIDE, …
- Traffic generator

More information

http://www.laas.fr/METROSEC