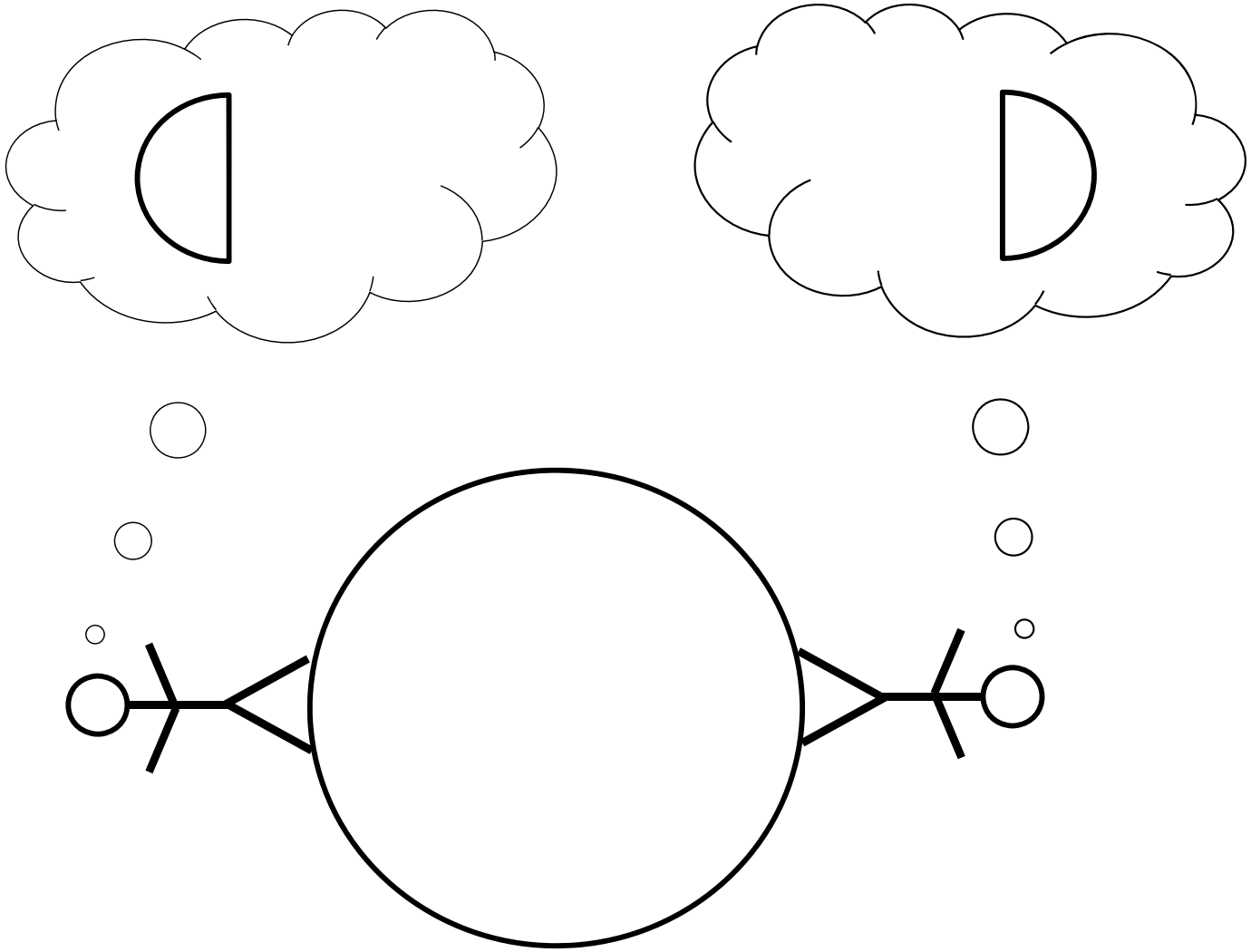
Comparable Metrics for IP Darkspace Analysis

Tanja Zseby
(with tools from Alistair King and Nevil Brownlee)

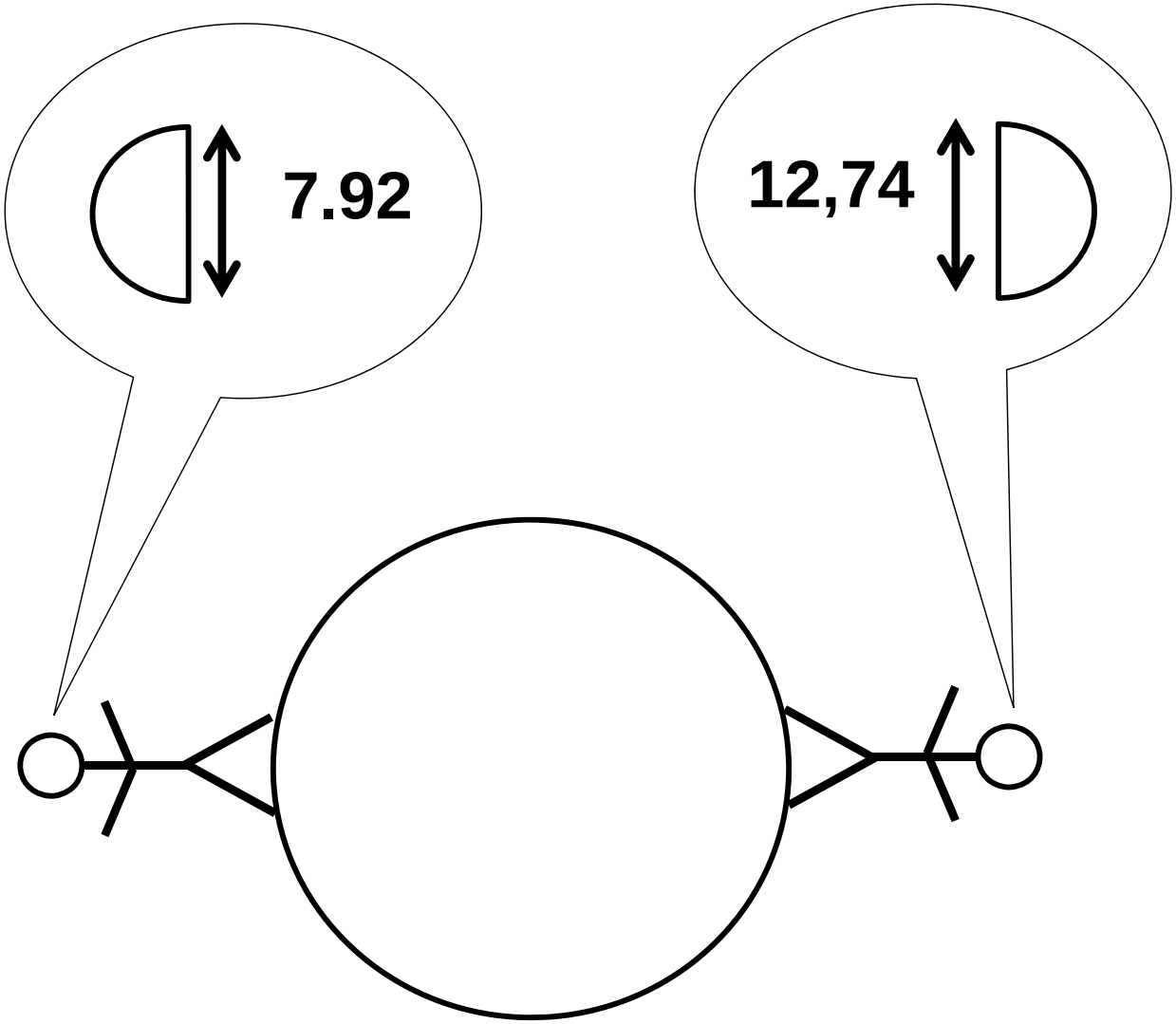
CAIDA and Fraunhofer FOKUS

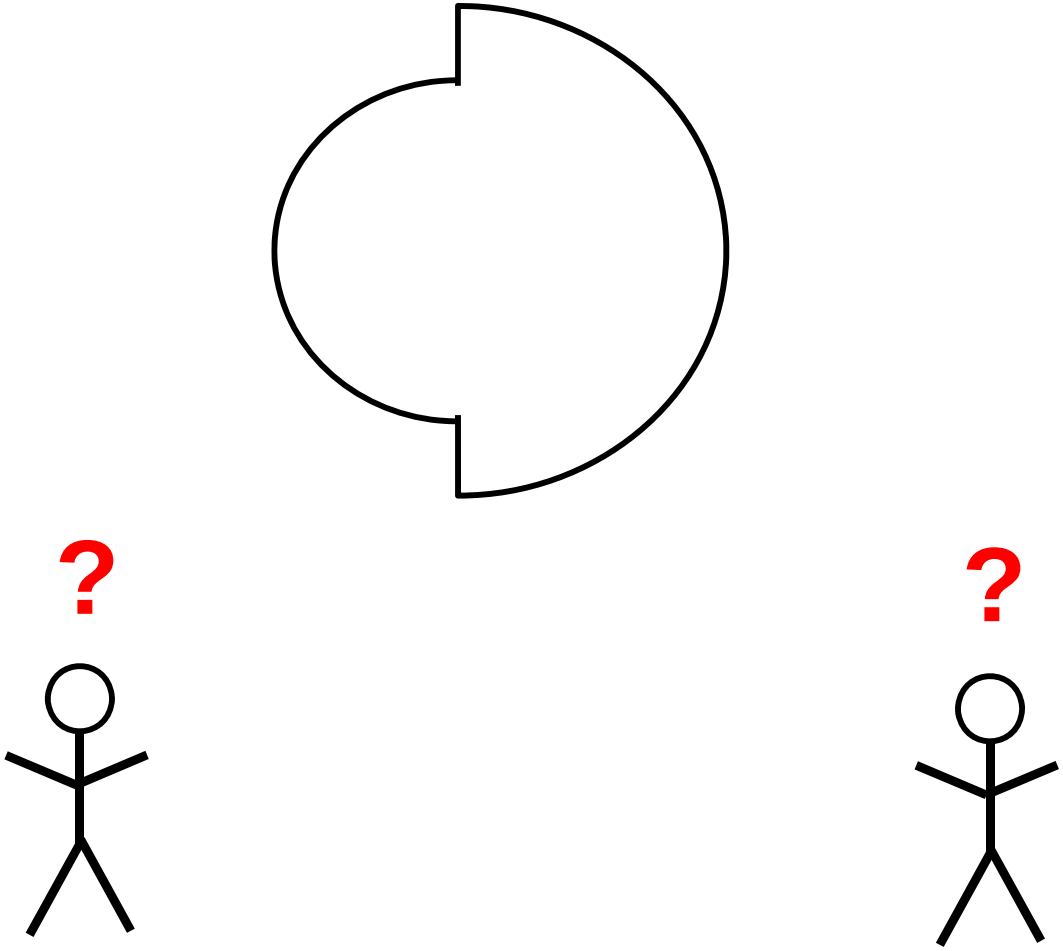
DUST 2012
May 15, 2012

Information Sharing



Information Sharing



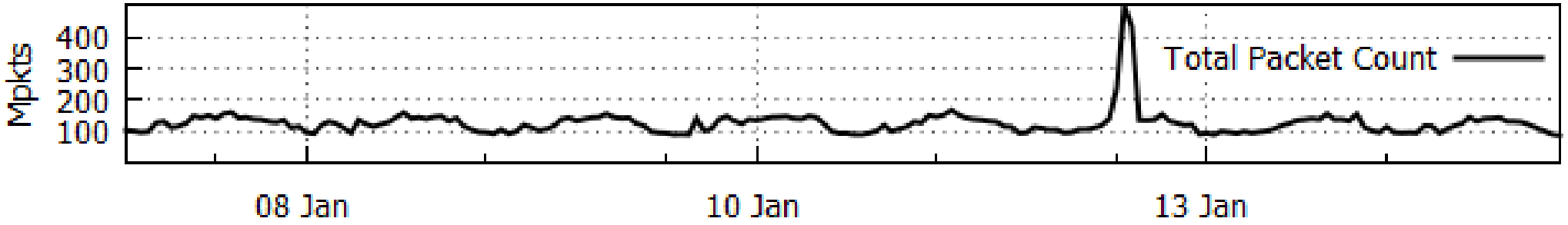


pcap?

- But:
  - A lot of data
  - Privacy/data protection

- At least agree on
  - Capturing method
  - Snapsize, filtering
  - Clock sync

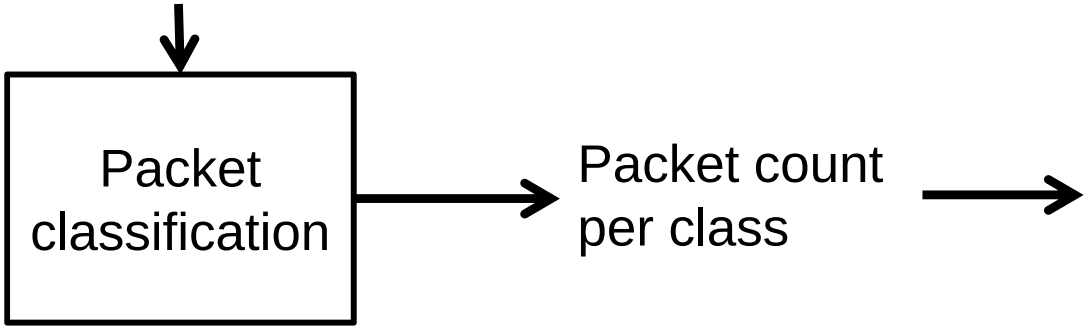
Aggregation



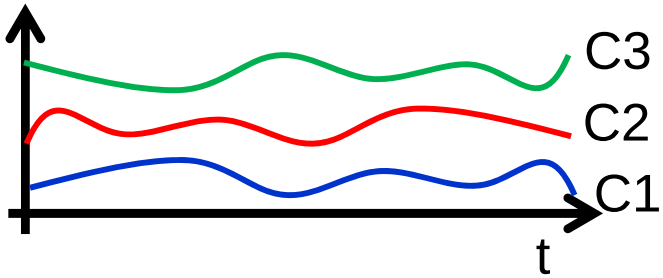
- Much less data ☺
- No privacy issues ☺
- Not much information ☹

Aggregation Examples

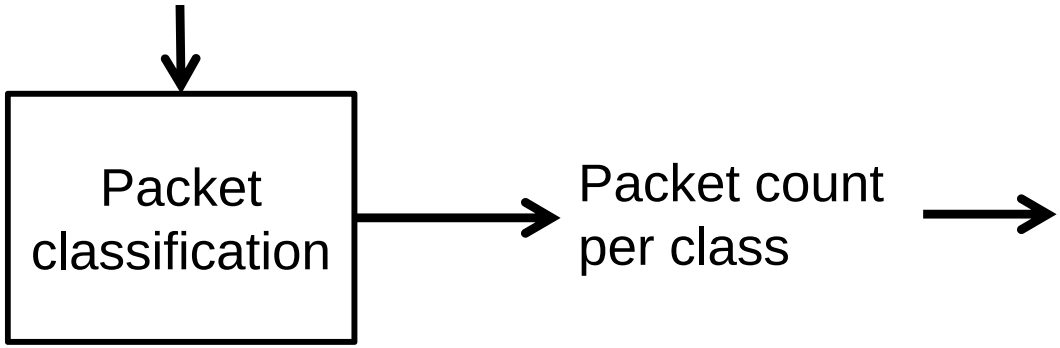
Classification rules
(feature combinations)



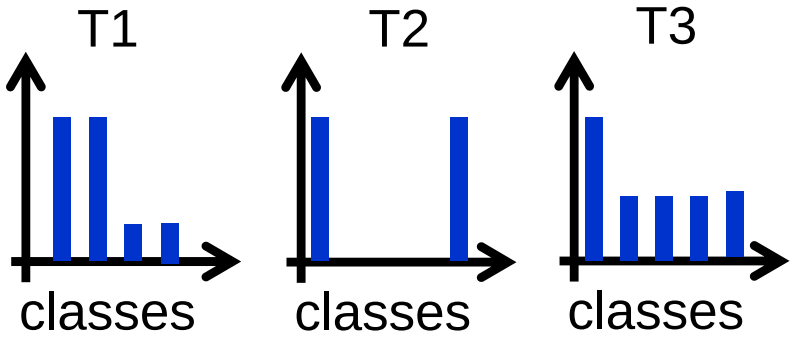
Time series of packet counts
for selected feature combinations



Classification rules
(selected features)



Distributions for selected
features

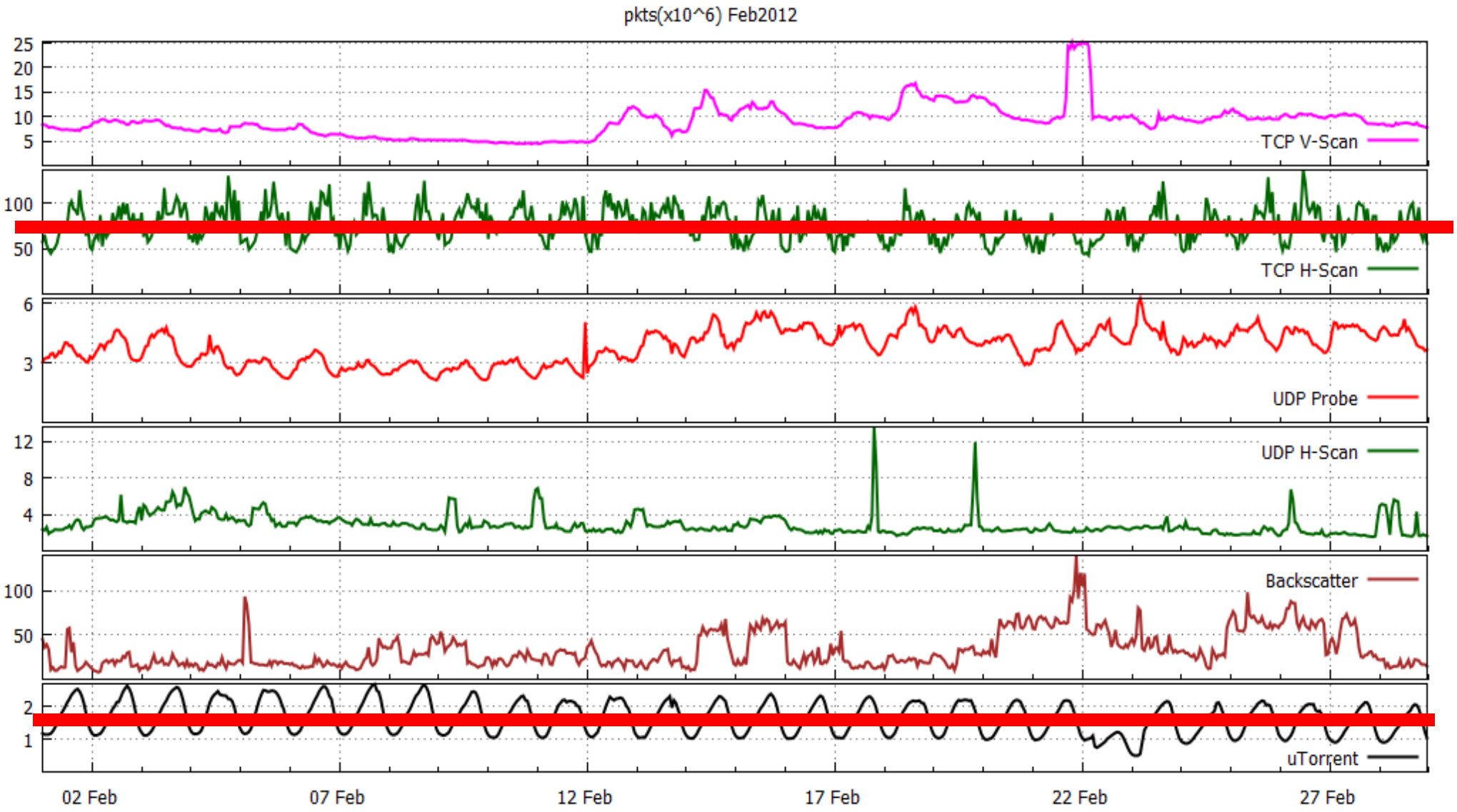


“I see 20% Backscatter”

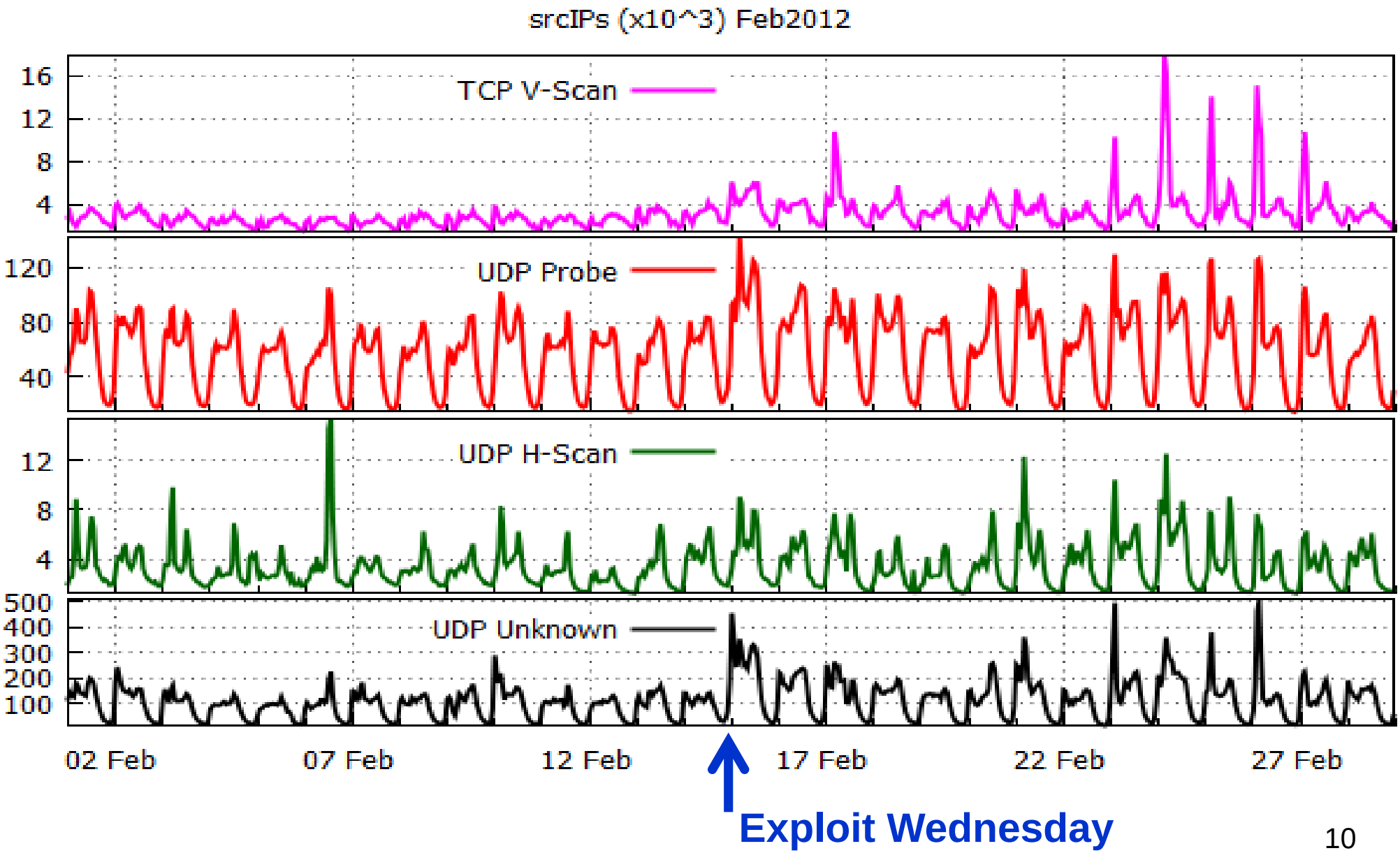
- Based on which packet attributes?
- Which rules?
- How many classes?
- Which classes?
- Time intervals?

- ➔ Agree on Classification Rules

Sampling (Spatial)

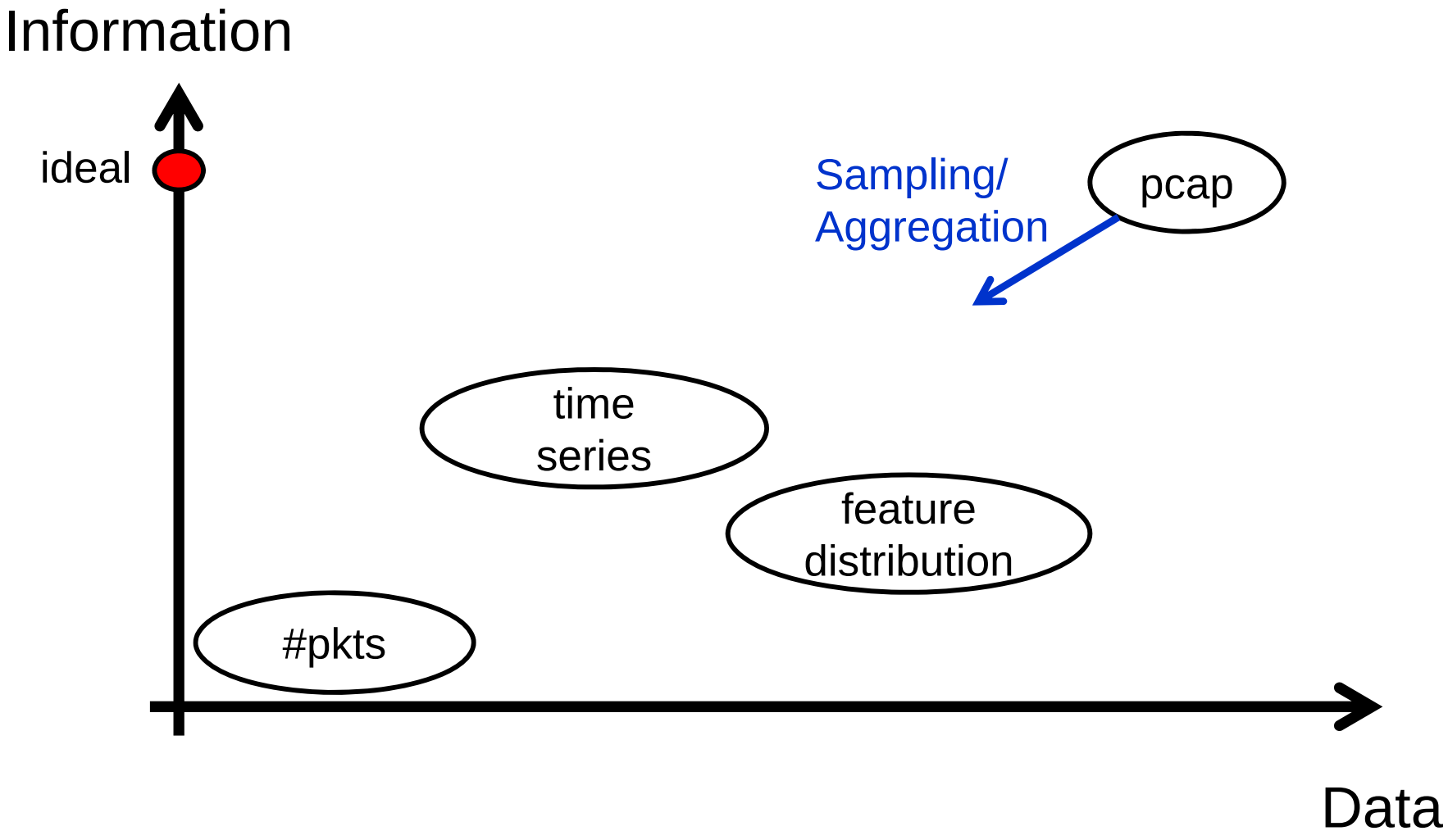


Sampling (temporal)



Exploit Wednesday

Reduce Data, Keep Information



Entropy

- Darkspace traffic
  - Random addresses or ports
  - Specific addresses or ports
  - In different combinations (➔ see J. Treurniet talk)
  - ➔ dispersion/concentration in feature distributions
- Dispersion and concentration ➔ entropy
- Q: can we recognize different traffic types in darkspace by just looking at entropy?
  - IP addresses
  - Port numbers

Related Work

Anomaly detection in light (non-dark) traffic:

- Lee/Xiang 2001
  - Information Theoretic Measures for Anomaly Detection
- Feinstein/Schnackenberg 2003
  - Detection of DDoS attacks based on source IP entropy
- Lakhina et al.2005
  - Detection of scanning, DDoS, outages based on combinations of entropy from addresses and ports
- Brauckhoff et al. 2009
  - Kullback Leibler divergence
- Ziviani et al. 2007
  - Generalized entropy

ML Entropy Estimation

<u>Definition from [LaCD05]:</u>

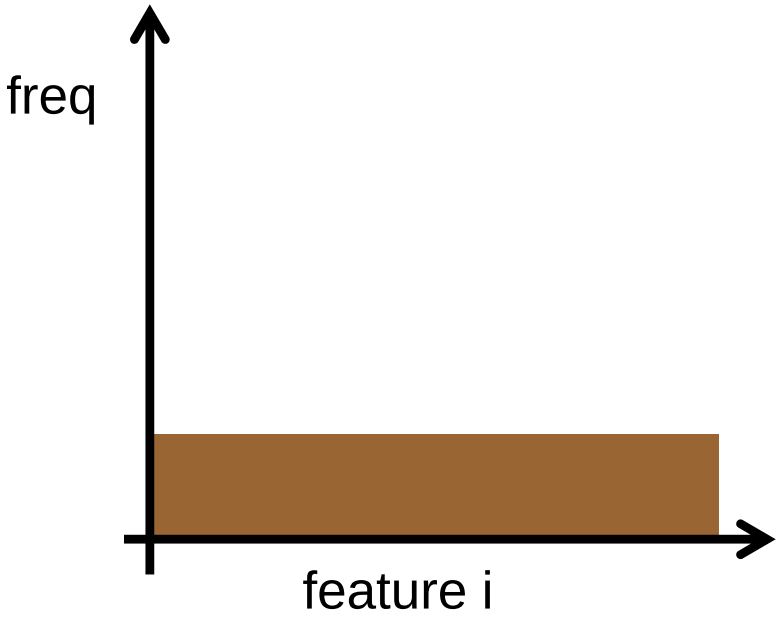
Histogram $X = \{n_i, i = 1, ..., N\}$

Total number of observations $S = \sum_{i=1}^{N} n_i$

$$\boxed{H(X) = -\sum_{i=1}^{N} \left(\frac{n_i}{S}\right) \log_2 \left(\frac{n_i}{S}\right)}$$

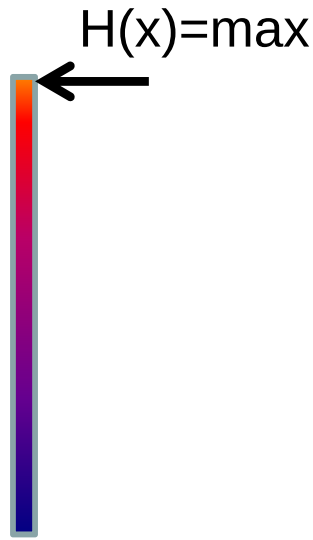
[LaCD05] Lakhina, Crovella, Diot: Mining Anomalies Using Traffic Feature Distributions. *SIGCOMM*2005

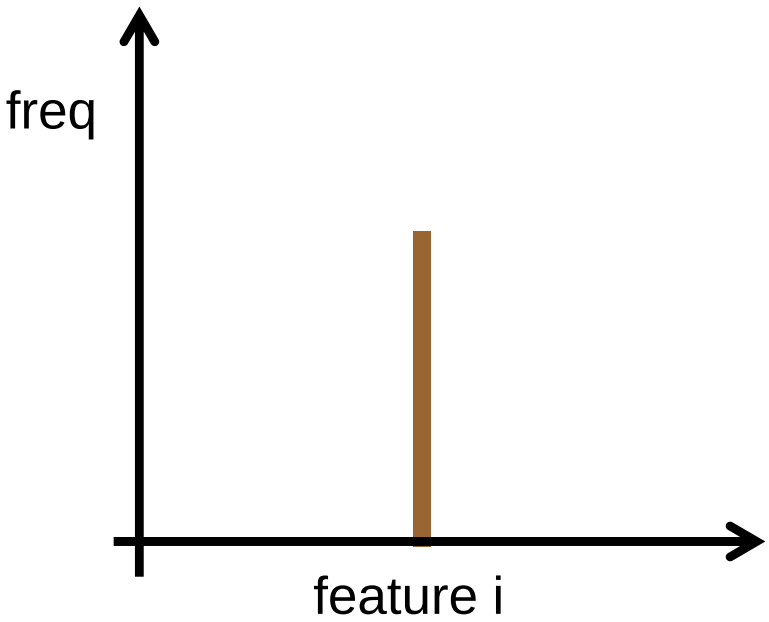
Entropy Example



Each packet different
➔ distribution disperses

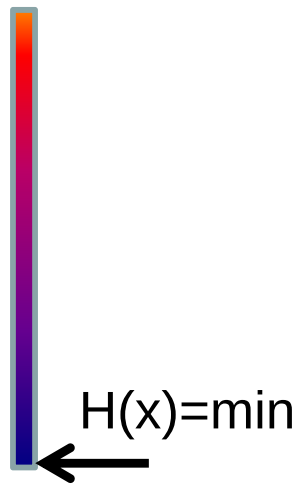
➔ Entropy= max
$H(X) = \log_2 N$





All packets equal
➔ distribution concentrates

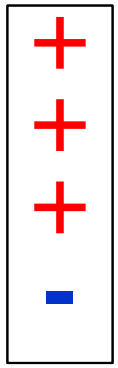
➔ Entropy = min
$H(X) = 0$

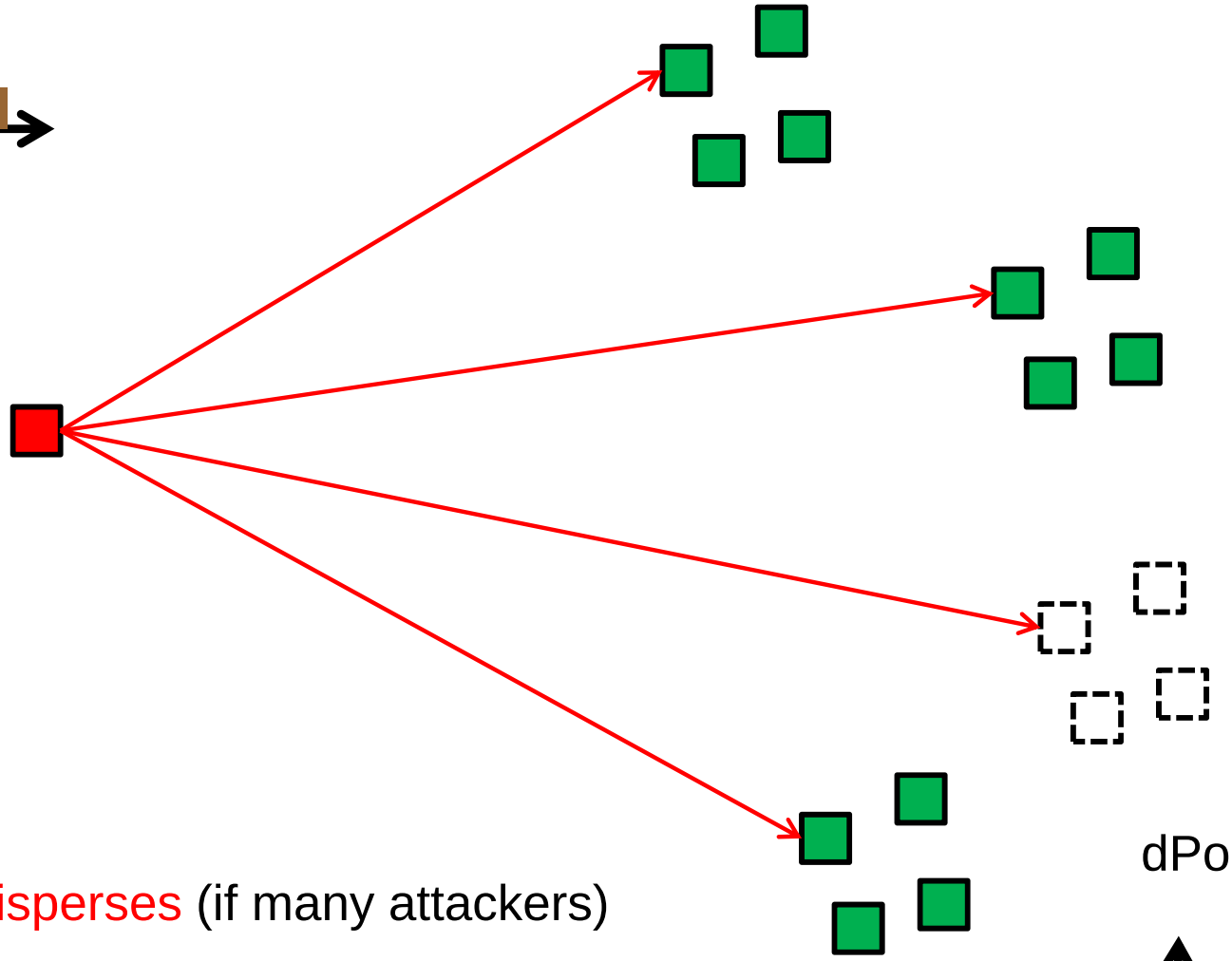


Horizontal Scanning

sIP ➔ disperses (if many attackers)

dIP ➔ disperses





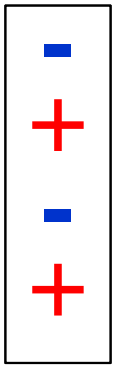
sPort ➔ disperses (if many attackers)

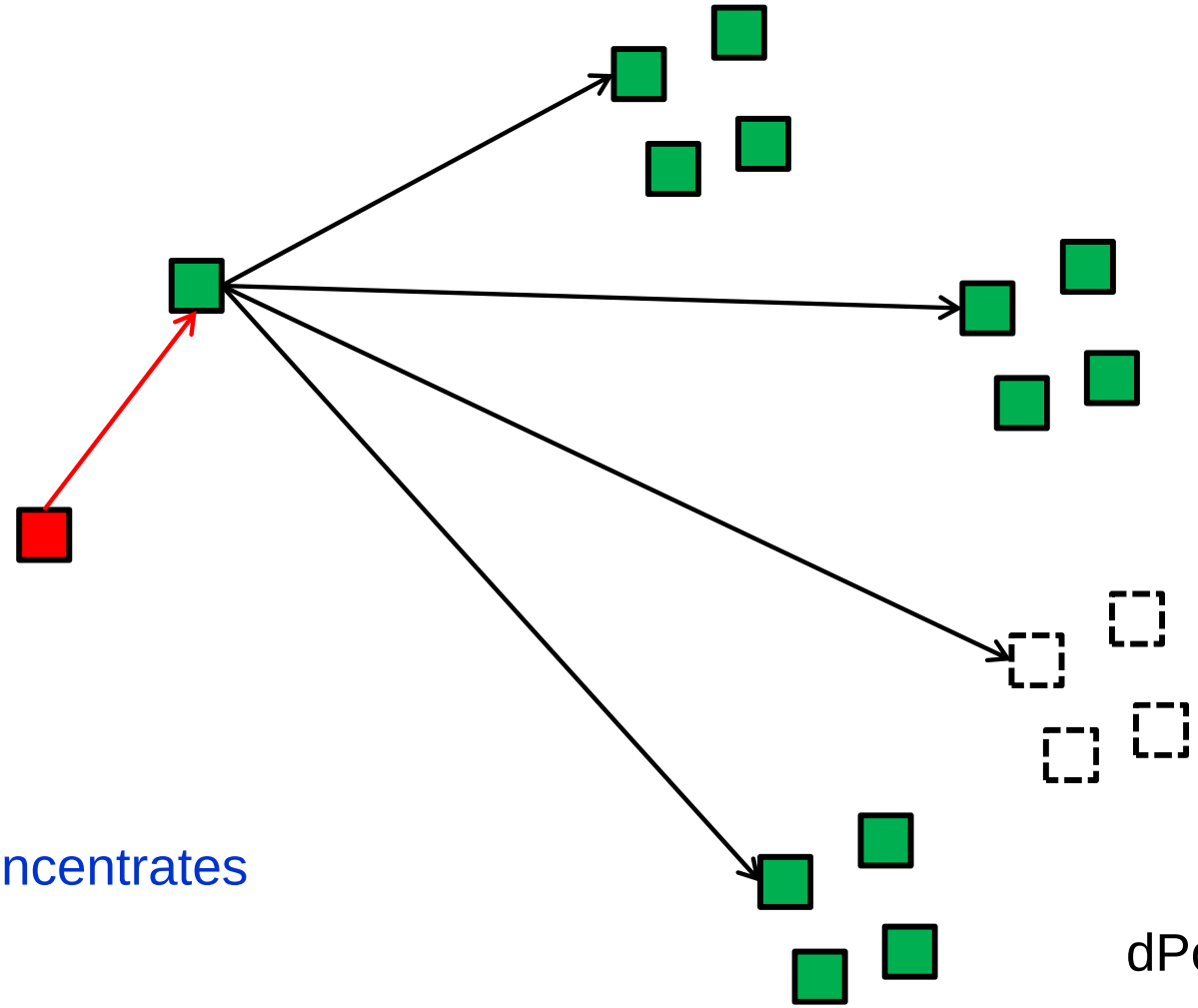
dPort ➔ concentrates

Backscatter

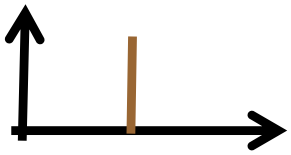
sIP ➔ concentrates (victims)

dIP ➔ disperses



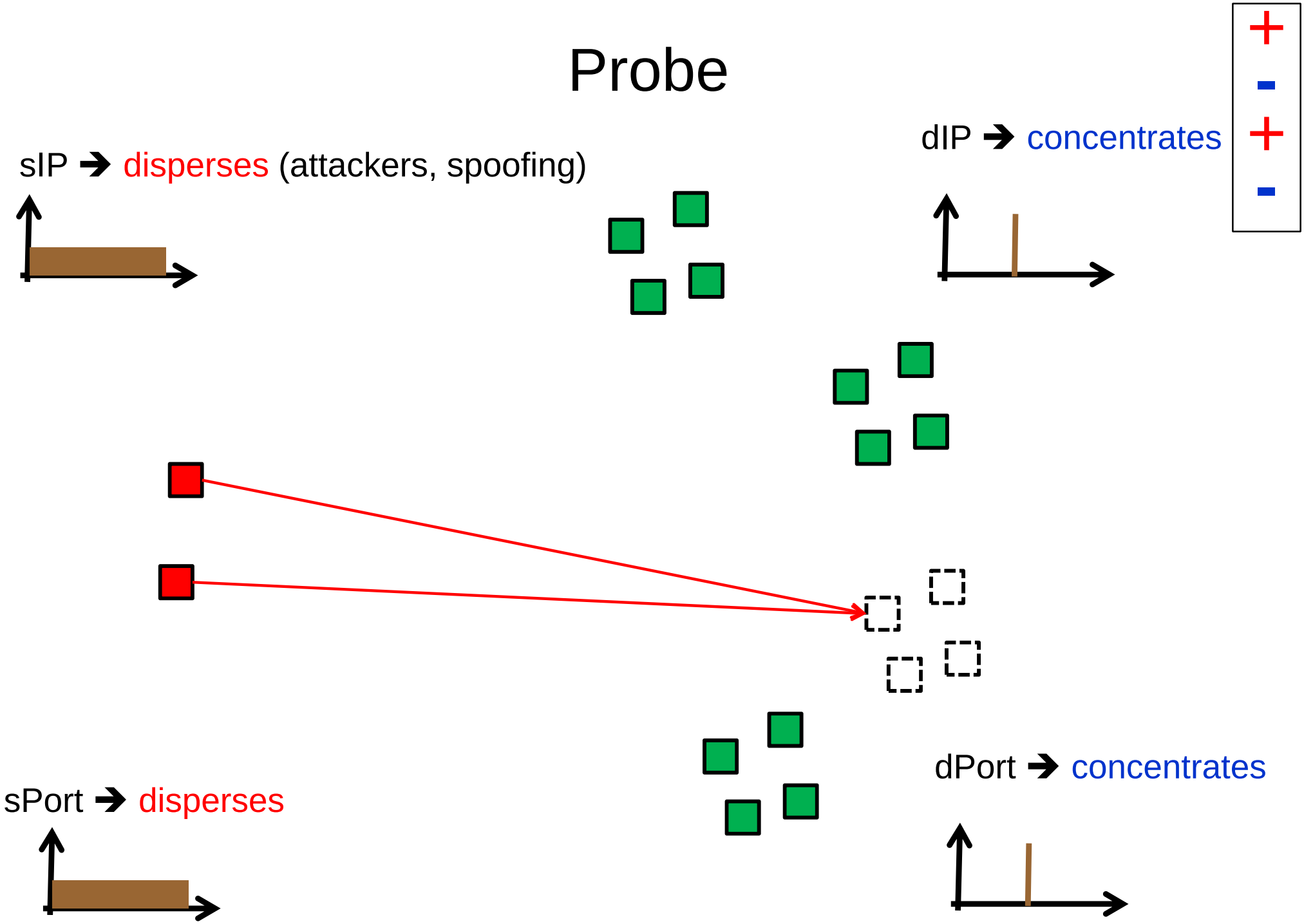


sPort ➔ concentrates



dPort ➔ disperses

Probe


sIP ➔ disperses (attackers, spoofing)
dIP ➔ concentrates
+
-
+
-
sPort ➔ disperses
dPort ➔ concentrates

Expected Entropy Patterns

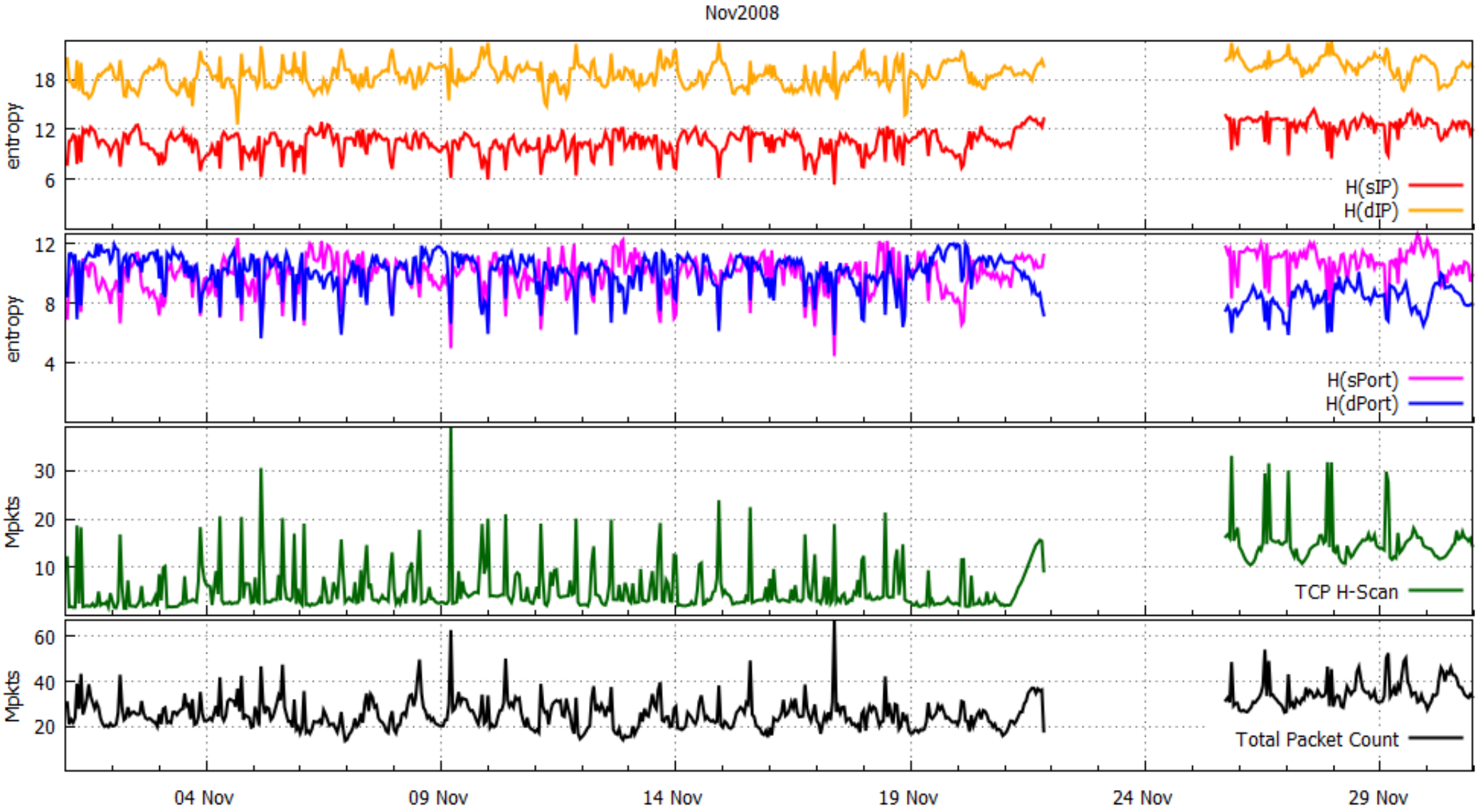
	Multisource H-Scan	**Backscatter**	**Multisource Probe**	**V-Scan**
sIP	disperses ↑	concentrates ↓	disperses ↑	concentrates ↓
dIP	(disperses) ⇡	(disperses) ⇡	concentrates ↓	concentrates ↓
sPort	disperses ↑	concentrates ↓	disperses ↑	disperses ↑
dPort	concentrates ↓	disperses ↑	concentrates ↓	disperses ↑

Analysis

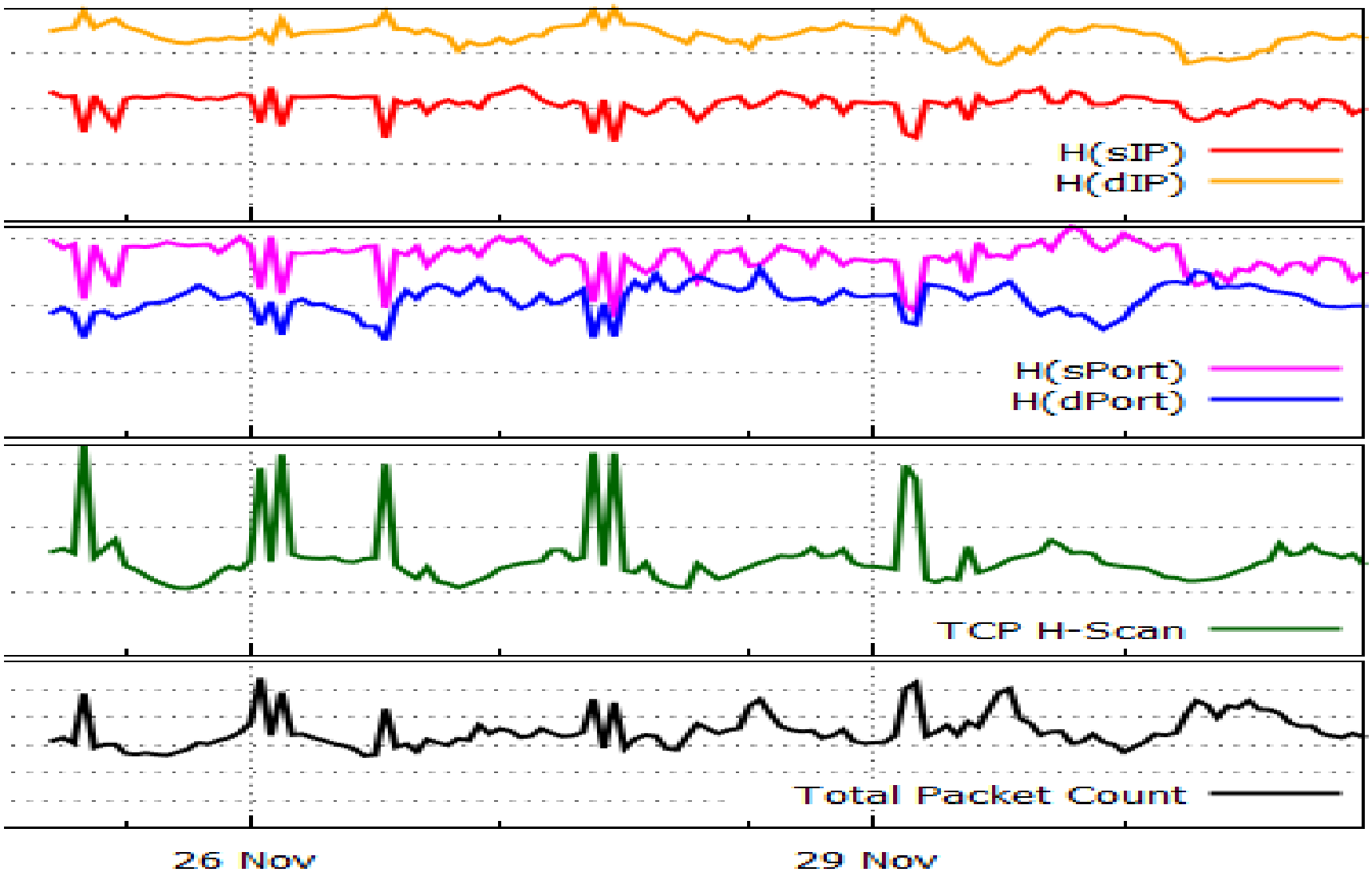
- Time Intervals: per hour

- 5 month
  - Nov 2008, Jan/Feb 2011, Jan/Feb 2012
- 4 features
  - srcIP, destIP, srcPort, destPort
- 3.5 tools
  - iatmon, Corsaro, R, (SiLK)

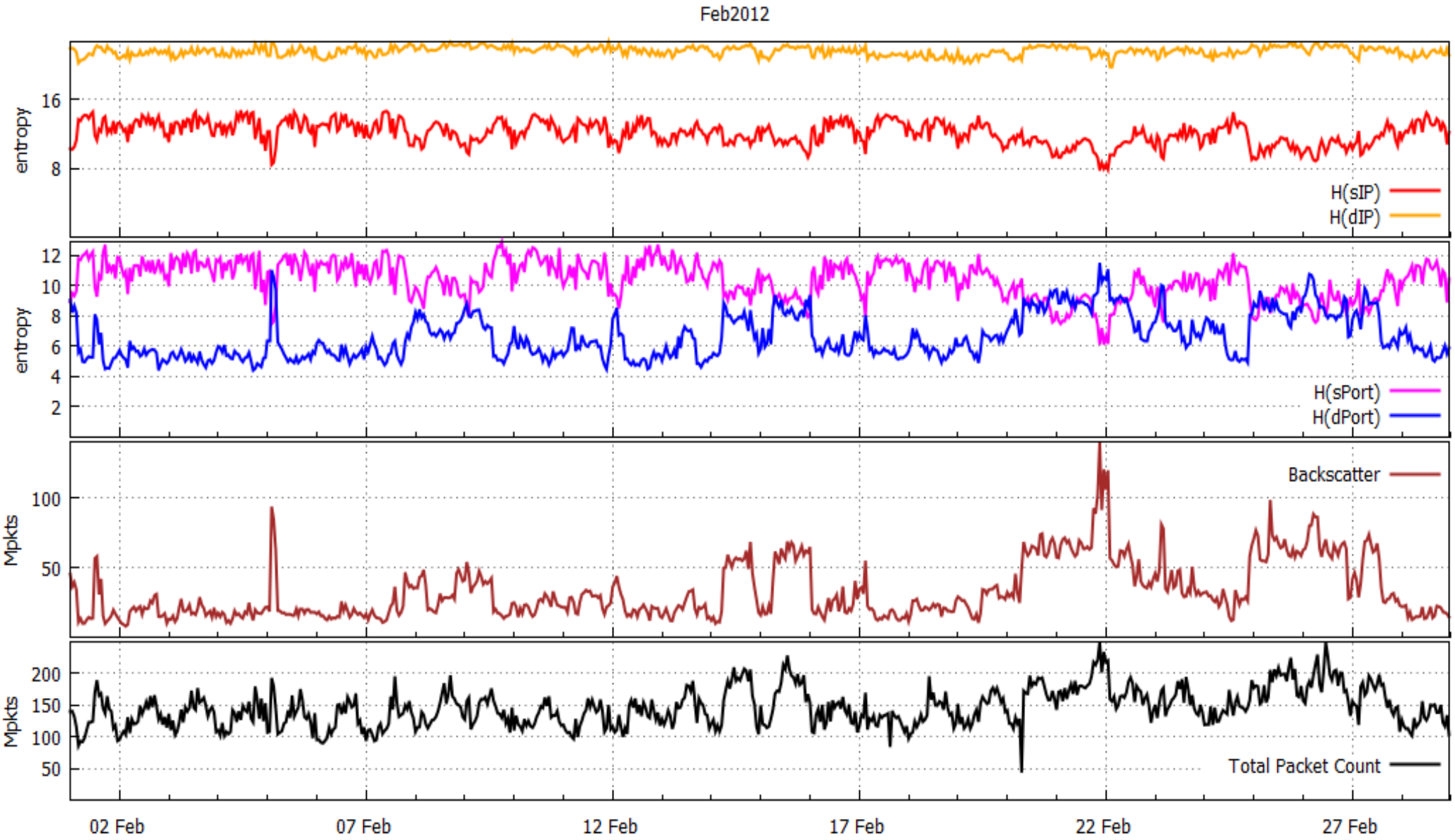
Nov 2008


Nov2008
entropy
18
12
6
H(sIP)
H(dIP)
entropy
12
8
4
H(sPort)
H(dPort)
Mpkts
30
20
10
TCP H-Scan
Mpkts
60
40
20
Total Packet Count
04 Nov
09 Nov
14 Nov
19 Nov
24 Nov
29 Nov

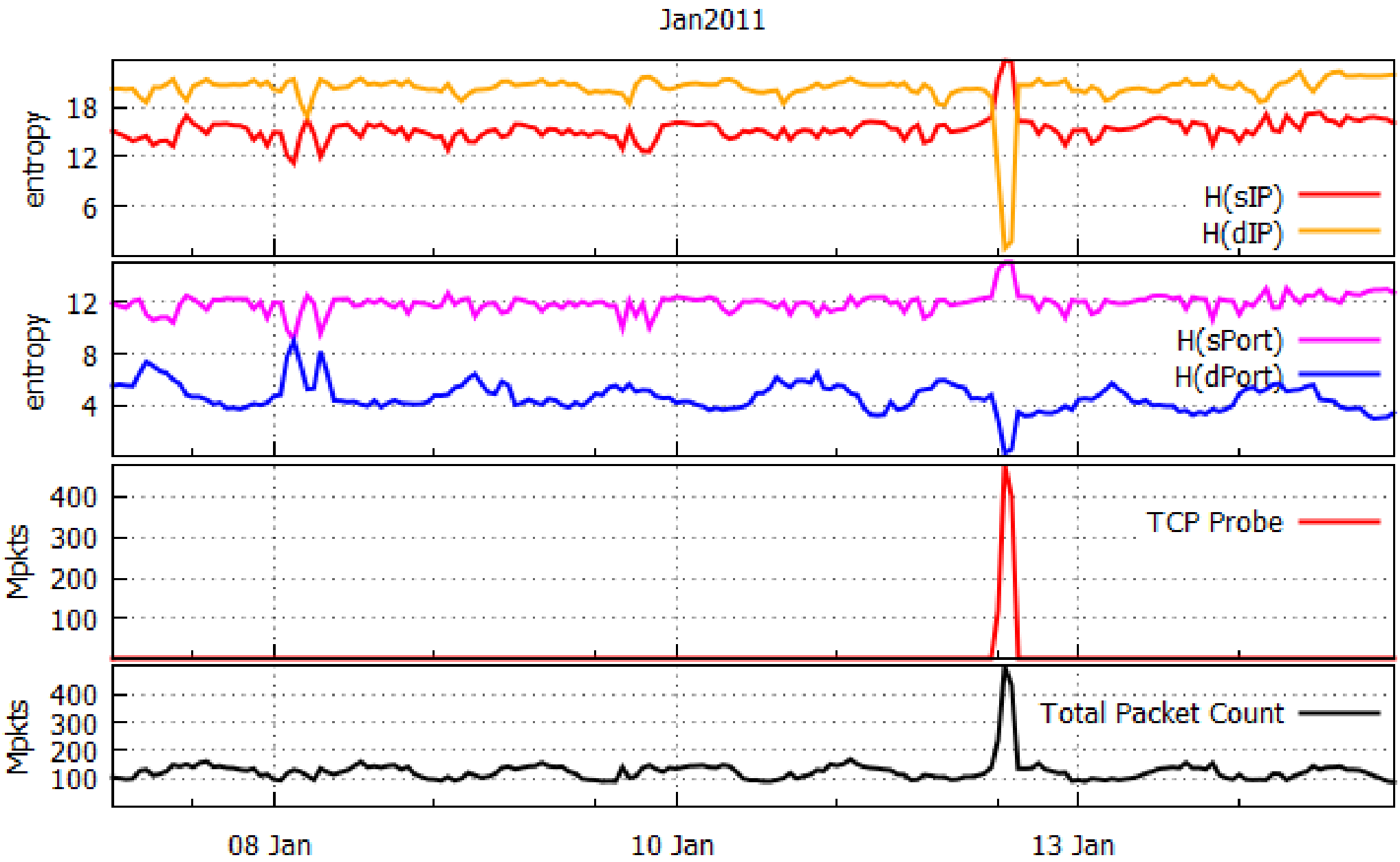
Details


H(sIP)
H(dIP)
H(sPort)
H(dPort)
TCP H-Scan
Total Packet Count
26 Nov
29 Nov

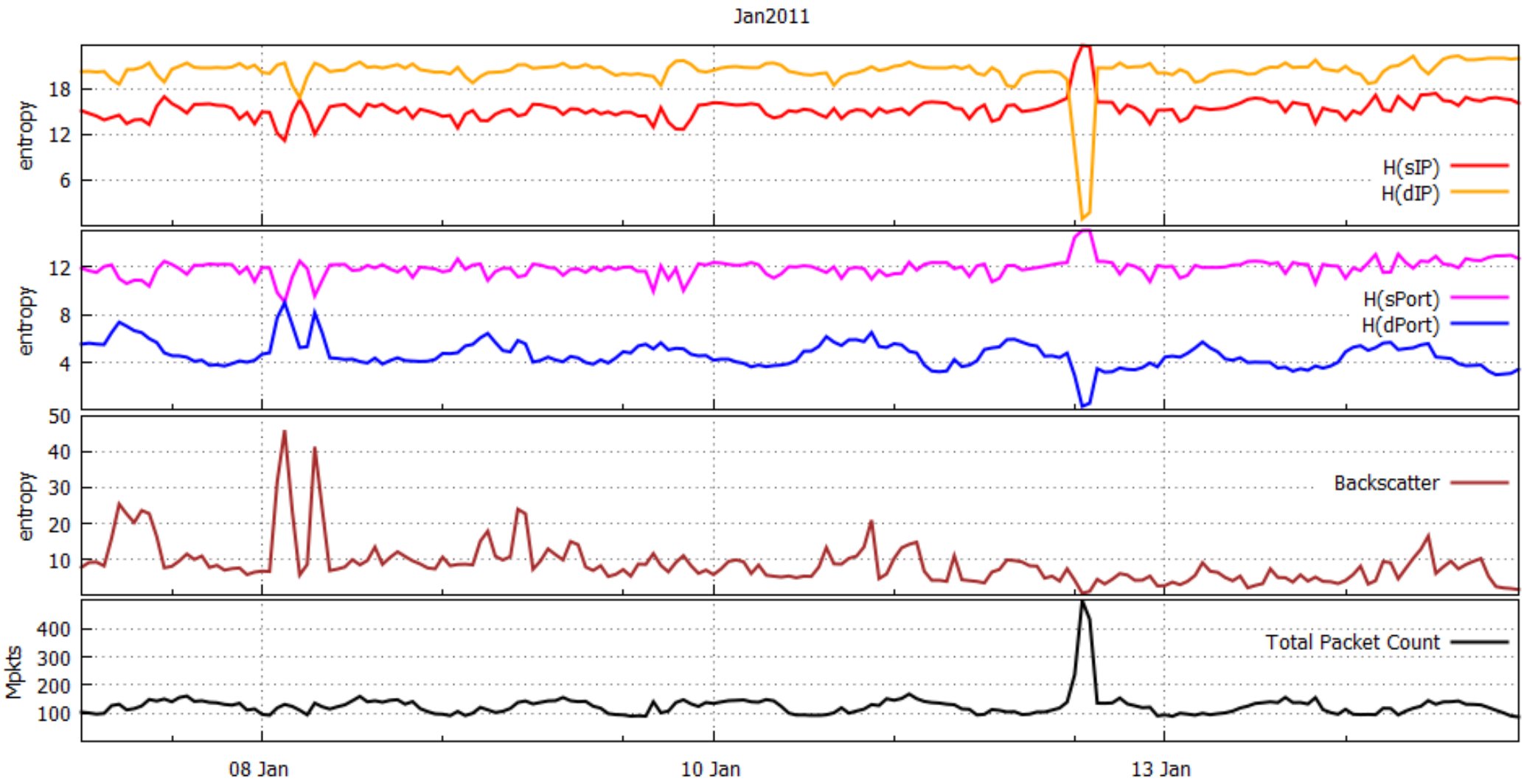
Feb 2012


Feb2012
entropy
16
8
H(sIP)
H(dIP)
entropy
12
10
8
6
4
2
H(sPort)
H(dPort)
Mpkts
100
50
Backscatter
Mpkts
200
150
100
50
Total Packet Count
02 Feb
07 Feb
12 Feb
17 Feb
22 Feb
27 Feb

Jan 2011


Jan2011
entropy
18
12
6
H(sIP)
H(dIP)
entropy
12
8
4
H(sPort)
H(dPort)
Mpkts
400
300
200
100
TCP Probe
Mpkts
400
300
200
100
Total Packet Count
08 Jan
10 Jan
13 Jan

Jan2011


Jan2011
entropy
18
12
6
H(sIP)
H(dIP)
entropy
12
8
4
H(sPort)
H(dPort)
entropy
50
40
30
20
10
Backscatter
Mpkts
400
300
200
100
Total Packet Count
08 Jan
10 Jan
13 Jan

Discussion

- Entropy
  - Based on IP addresses, ports
  - Comparable
  - Better than packet count, not as good as iatmon
- Challenges
  - Small events ➔ generalized entropy
  - Nested Events ➔ smaller time intervals, sliding window

A Call for Cooperation

- Cooperation on entropy
  - Share data? distributions/hour
    - frequencies sufficient, no IP addresses required
  - Run tools on your data?
- Joint investigation of Patch Tuesday effects
  - Do you see similar effects?
- DUST 2013?
  - same time period from different darkspaces?

Thank you!

contact: tanja@caida.org