TTL-based Fingerprinting and MPLS

Yves Vanaubel[1], Jean-Jacques Pansiot[2], Pascal Merindol[2] and Benoit Donnet[1]

[1]ULg (Belgium), [2]UDS (France),

April 11, 2013

Summary

- Introduction to the TTL-based signatures
- Motivations
- Measurement campaign
- MPLS use case
- Ongoing work and conclusions

Time To Live (TTL)

- Field in the IP header (avoid routing loops)
- Maximum number of hops for an IP packet
- Initial value of the TTL field may vary, depending on:
  - the hardware (CISCO, Juniper, ...)
  - the Operating System
  - the protocol used (TCP/UDP/ICMP)

ICMP messages

- We consider two types of ICMP messages:
  1. Time-exceeded messages, obtained with Traceroute
  2. Echo-reply messages, obtained with Ping
- We also tried UDP probes: marginal gain
- Initial values of TTLs used by nodes: 32, 64, 128, 255
- TTL initialized differently by a node when it sends:
  - an error packet (Time-exceeded)
  - an information packet (Echo-reply)

TTL-based signatures

- Pair of initial TTLs:

<Time-exceeded, Echo-reply>

- Diversity in the signatures (in theory : 5^n, n : # probes)
- Examples : <255-255>, <255-*>, <255-128>, ...

Motivations

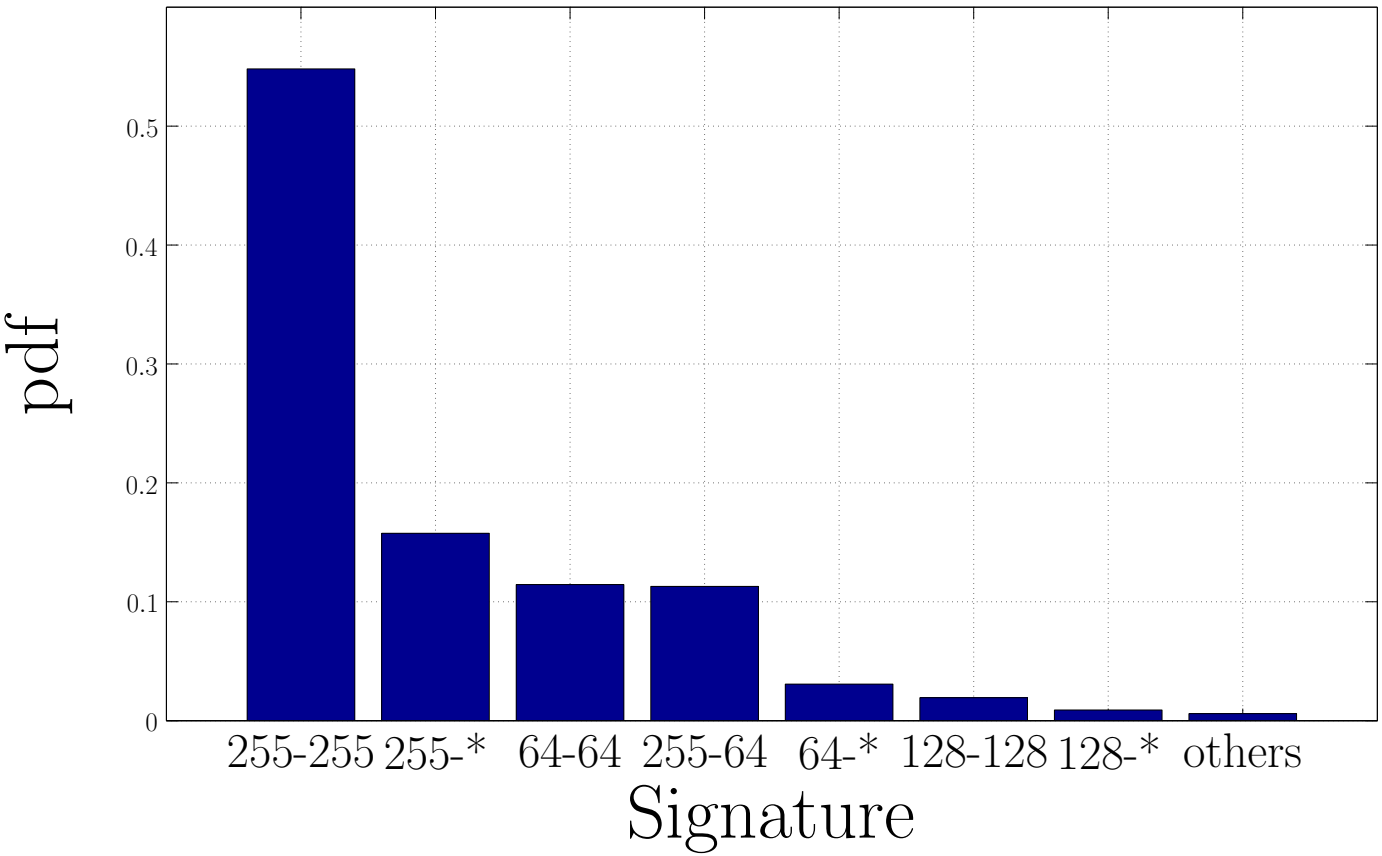
- Understanding the characteristics of the Internet:
  - hardware distribution (CISCO, Juniper, etc...)
  - operating systems deployed
  - ...
- Alias resolution : clustering approach
- Understanding MPLS tunnels
- ...

Measurement campaign

- Measurement campaign on the PlanetLab network
- 1M of destinations from CAIDA data
- 200 vantage points (VP), i.e. 5000 destinations/VP
- Each IP on a trace pinged 6 times
- Scamper with paris-traceroute
- About 8h of probing per VP
- About 3 days of campaign due to the PlanetLab instabilities

Signatures

- Signatures seen in the campaign:



- CISCO $\Rightarrow$ <255-255>
- Juniper $\Rightarrow$ <255-64>

Signatures consistency

- Assumption : *the signature of a router is unique*
- For a given IP address, a signature may be:
  - **Consistent**: signature always the same
  - **Incomplete**: signature most of the time complete, but sometimes incomplete (e.g. <255-255> and <255-*>)
  - **Inconsistent** : several complete signatures, but different from each other

Signatures consistency - intra VP

- For 21% of the VP, all signatures are consistent
- For all VP, no incomplete signatures
- In the remaining 79% VPs:
  some (rare) inconsistent signatures (less than 0.02% on average)

Signatures consistency - inter VP

- About 97.6% of the signatures are consistent
- Some incomplete signatures (2.2%)
- A bit more inconsistent signatures, but still rare (0.08%)

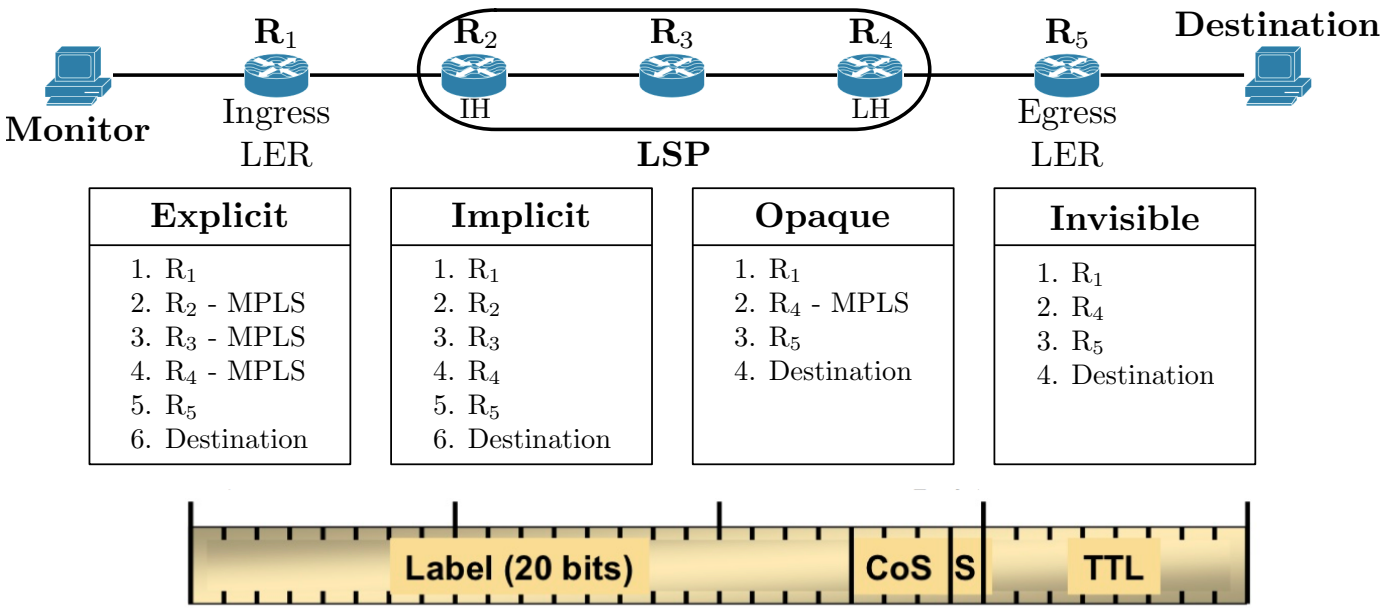
Signatures consistency - Conclusions

- In the vast majority, consistent signatures
  - Inconsistency due to our initial TTL determination technique?
- Incomplete signatures not encountered inside a VP
  - Filtering at some VP
  - Possibility to complete the signatures
    (e.g. <255-*> ⇒ <255-255>)
- ⇒ Assumption correct:

  Each IP address is associated to a unique signature
- Our technique can be used to help alias resolution

MPLS use case

- Measurement-based classification of MPLS tunnels (traceroute)
  - TTL-propagate × RFC4950:

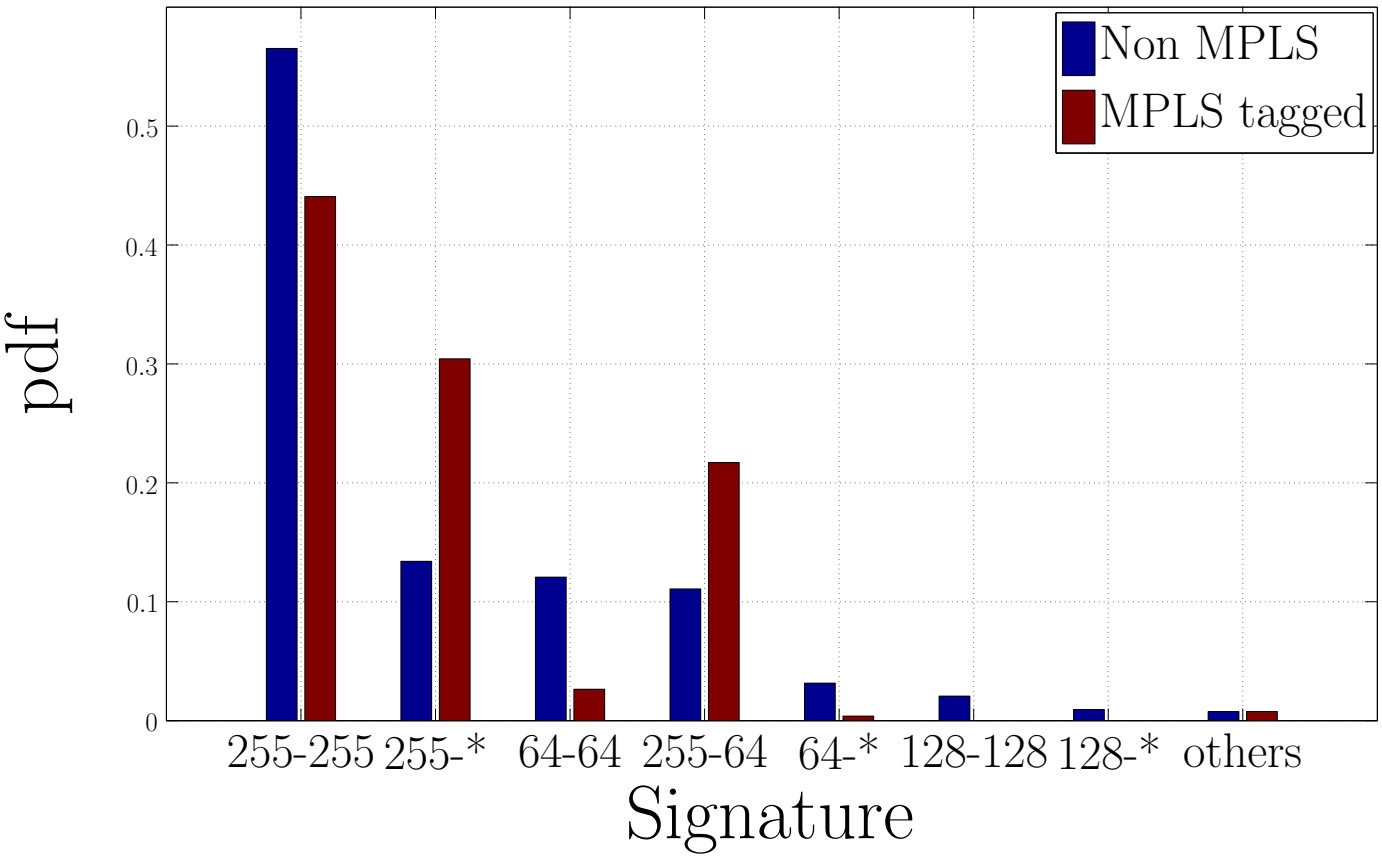


MPLS use case

- Proportion of IP addresses in
  - explicit tunnels: 14.23%
  - implicit tunnels: 25.51%
  - opaque tunnels: 0.33%
  - all MPLS tunnels: 30.37%
- Some addresses belongs to different types of tunnels
- MPLS seems well deployed in the Internet today

Global view

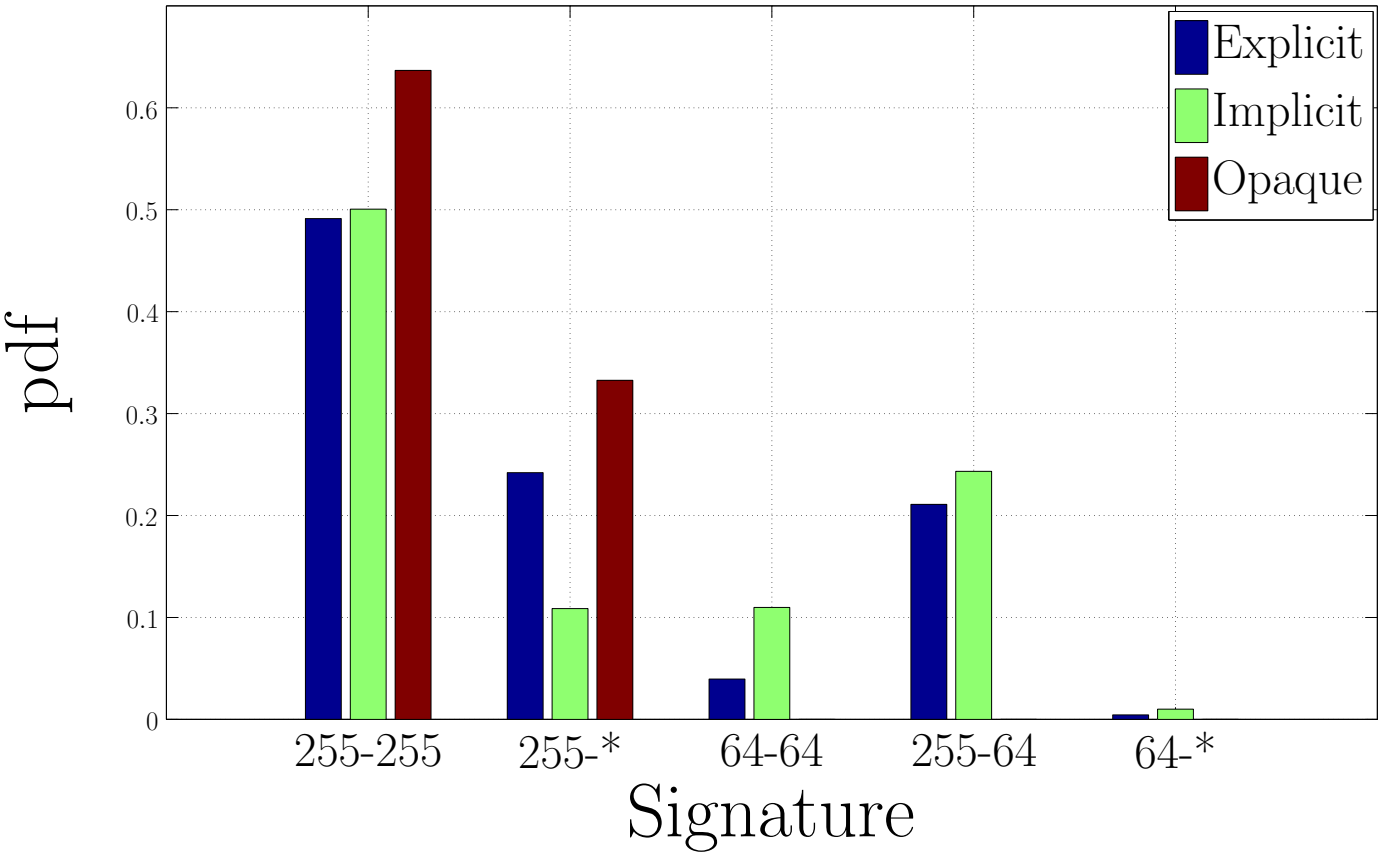
- Signatures distribution in the MPLS case:



- Why such a difference?

Refined view

- Signatures distribution in the different observed MPLS tunnels:



- Opaque tunnels : only one signature : <255-255> (and <255-*> but may be completed)
  - Invisible tunnels underestimated.

Ongoing work

- Aim : obtaining a better distribution in the signatures to limit the complexity of alias resolution:
  - MPLS TTL : 1 and 255
  - ICMP time exceeded packet sizes
  - Other probes (TCP, UDP, ...)
  - Several characteristics (internal nodes, ingress, egress, etc.)

Conclusion

- Each IP/router has a unique TTL-based fingerprint
- Can help alias resolution
- Help to understand MPLS tunnels (especially the opaque ones)
- Work still in progress (MPLS TTL, ICMP packets size, other probes, etc.)