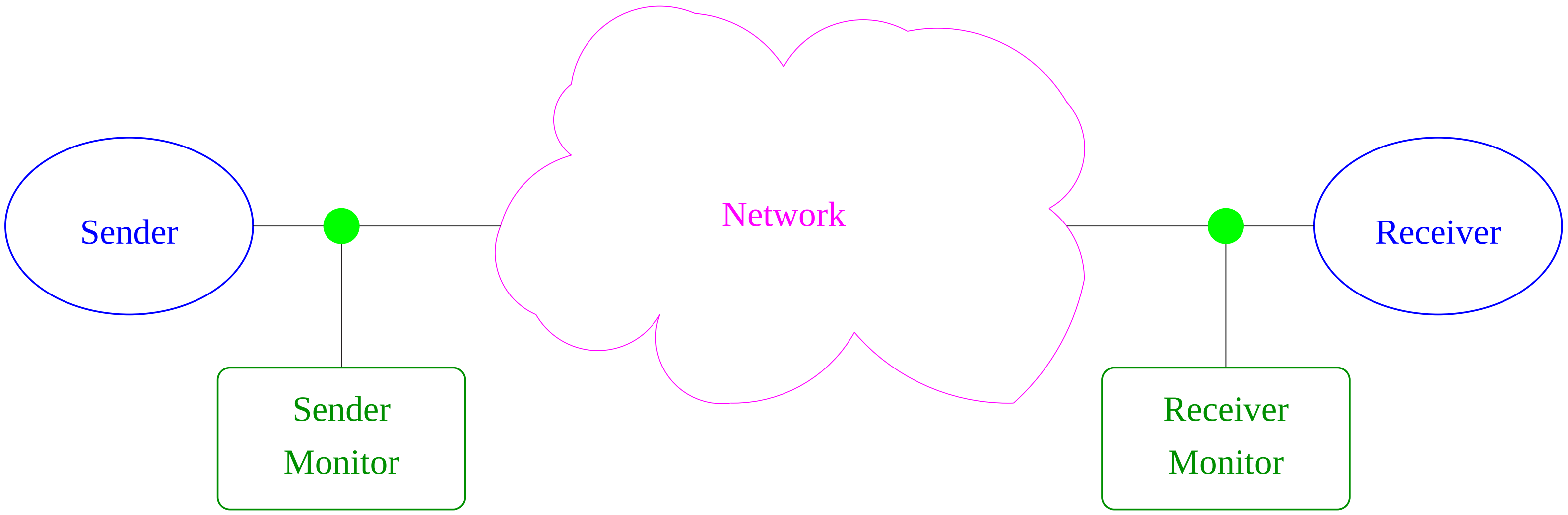
Active Probing with ICMP Packets

Fabien Viger
fabien.viger@normalesup.org

Internship in the Department of Electrical and Electronic Engineering,
University of Melbourne

Supervisor : Darryl Veitch

Active Probing: A Brief Overview



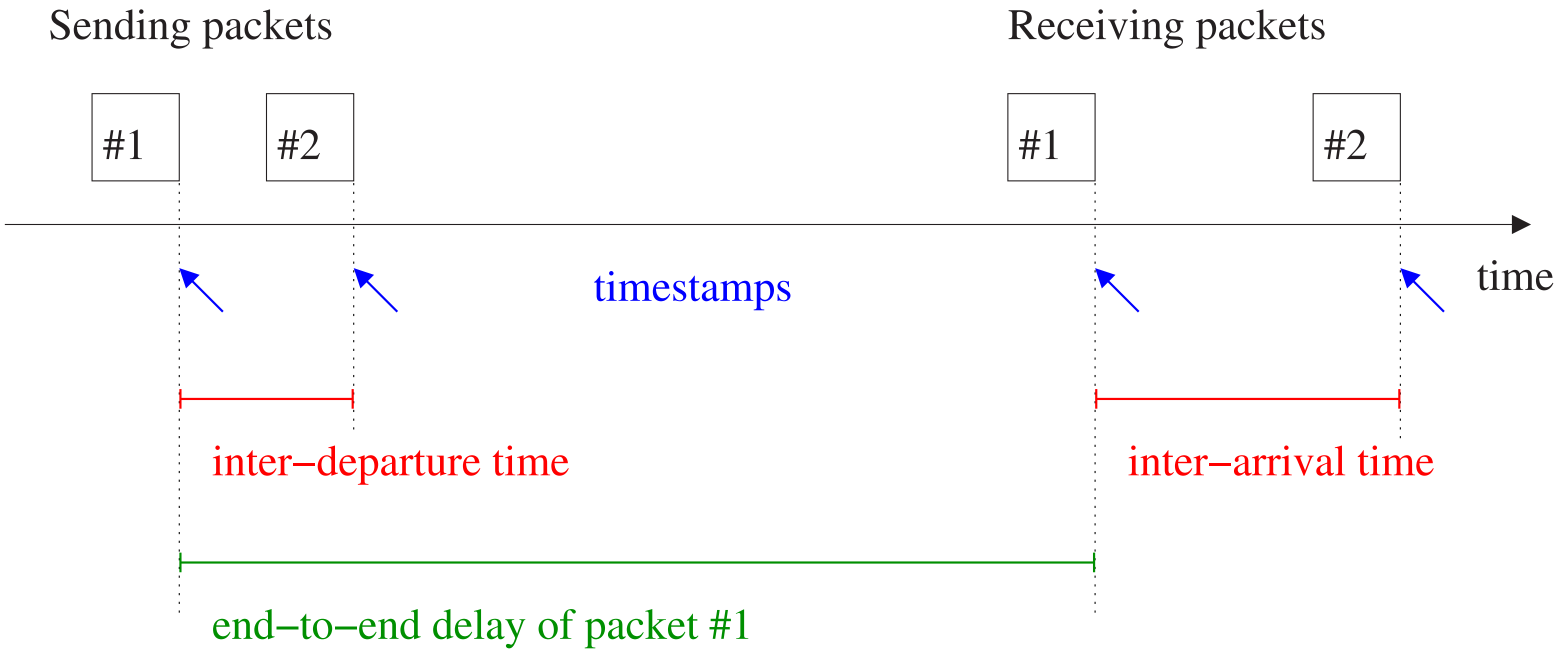
Experimental Data :

- departure and arrival times
- other : order, loss

Constraints :

- non-invasive (rate)
- not too many probes

Timestamps in Active Probing : What for ?



Key Probe Parameters

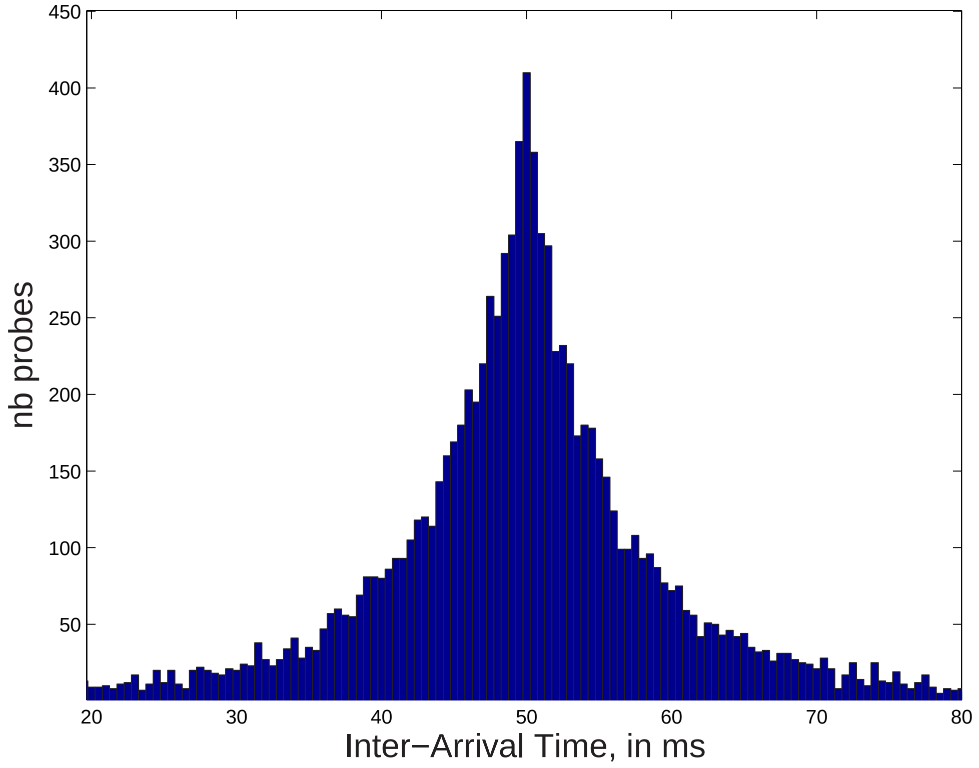
Key Probe Parameters

- Packet size

Key Probe Parameters

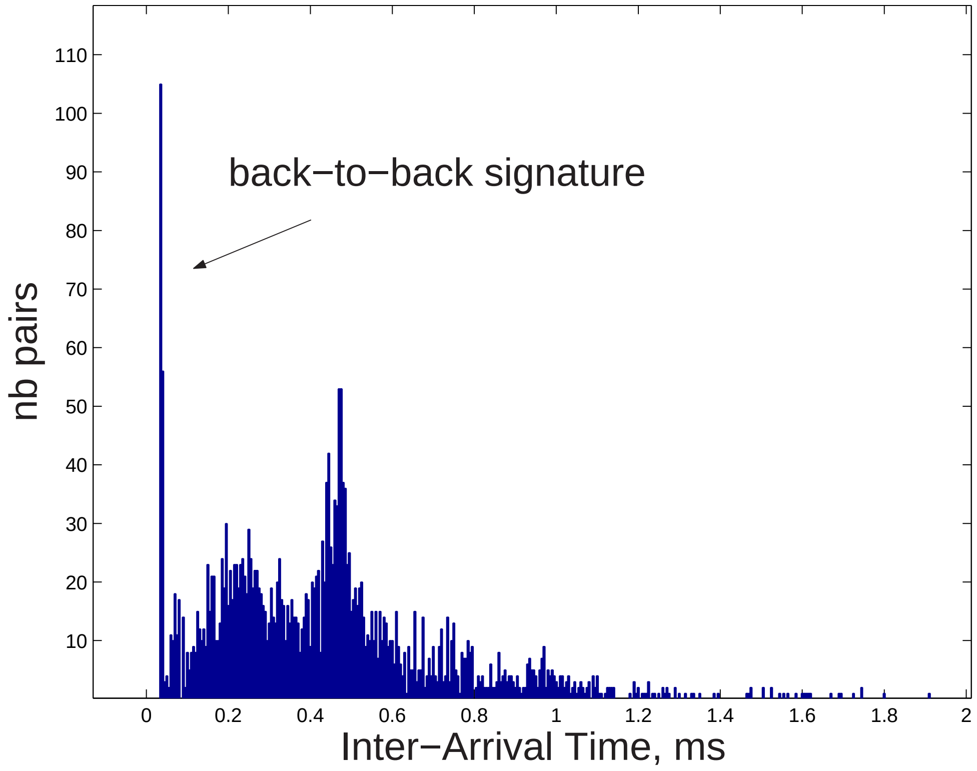
- Packet size
- Inter-Departure Time :
  - ⇒ Independant probes
  - ⇒ Back-to-back probes

Inter-Arrivals of Independant Probes



Inter-Departure Time : 50ms
probes : 56 byte UDP packets

Inter-Arrivals of Back-to-Back Probes



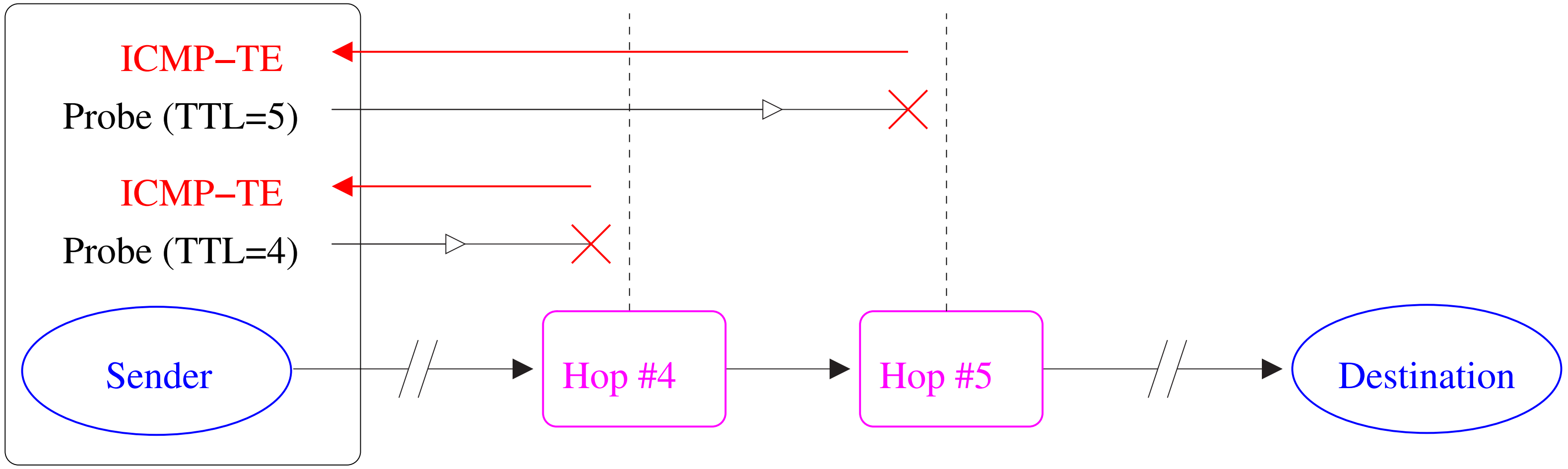
Probes sent in pairs, back-to-back within pairs
probes : 56 byte UDP packets

Key Probe Parameters

- Packet size
- Inter-Departure Time
- Packet type : UDP, TCP, ICMP

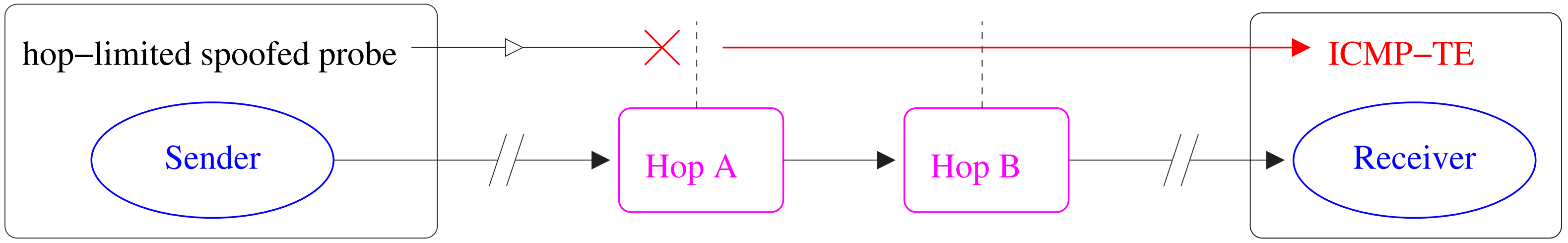
Key Probe Parameters

- Packet size
- Inter-Departure Time
- Packet type : UDP, TCP, ICMP
- TTL : *hop-limited* probes (ex : traceroute)



Key Probe Parameters

- Packet size
- Inter-Departure Time
- Packet type : UDP, TCP, ICMP
- TTL
- Source IP address : *Spoofing*



Why is ICMP interesting in Active Probing ?

An Alternative to UDP probes

- ICMP *Echo Reply*

  ⇒ No interaction with routers

  ⇒ Can generate ICMP *Time Exceeded*

- ICMP *Time Exceeded*

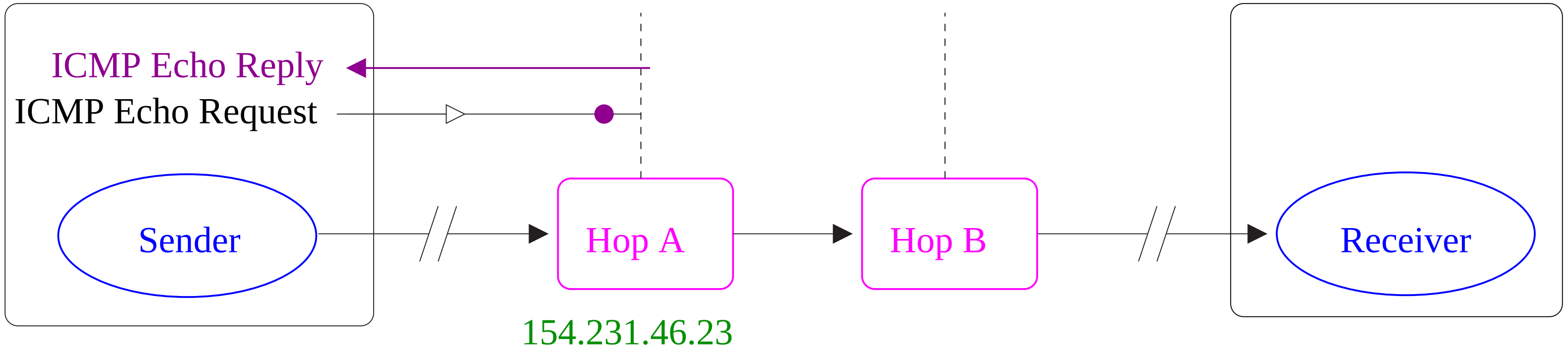
  ⇒ No interaction with routers

  ⇒ Never generate ICMP *Time Exceeded*

Why is ICMP Interesting in Active Probing ?

Allows Interaction with *Specific* Router

- Router chosen by direct addressing
  - ⇒ Routers reply to ICMP packets
  - ⇒ Example : *ping*

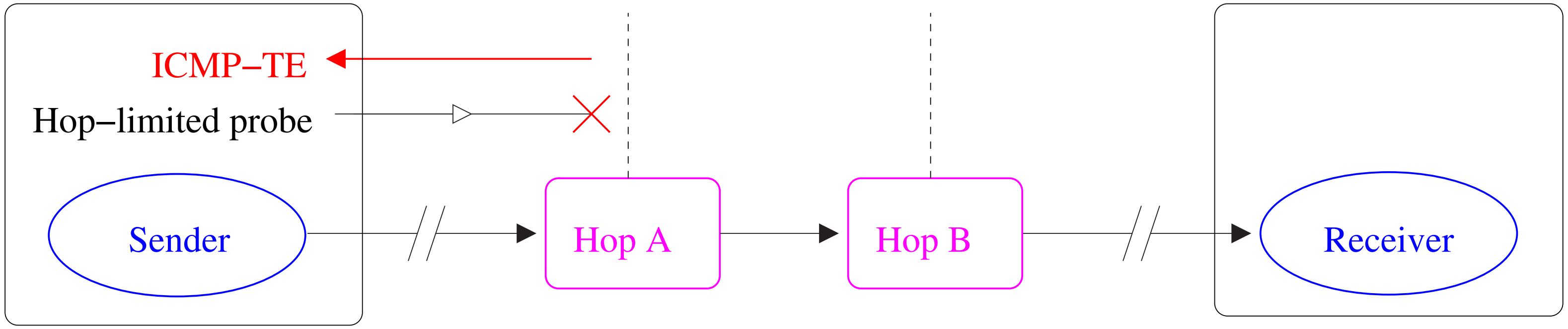


Why is ICMP Interesting in Active Probing ?

Allows Interaction with *Specific* Router

- Router chosen by direct addressing
- Router chosen by TTL

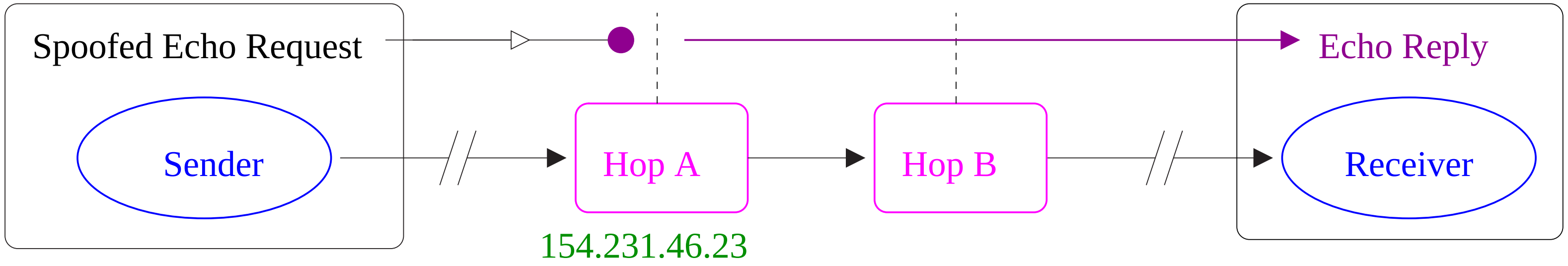
⇒ Answer is an ICMP *Time Exceeded*



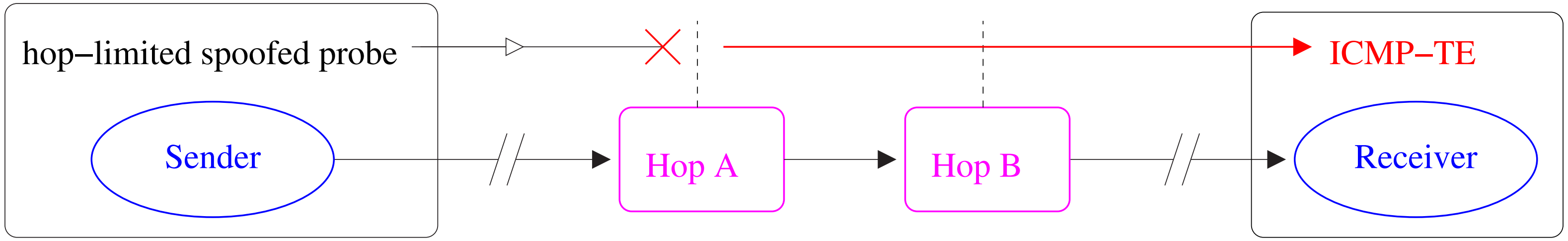
Why is ICMP Interesting in Active Probing ?

Add Spoofing

- *Spoofed* ping

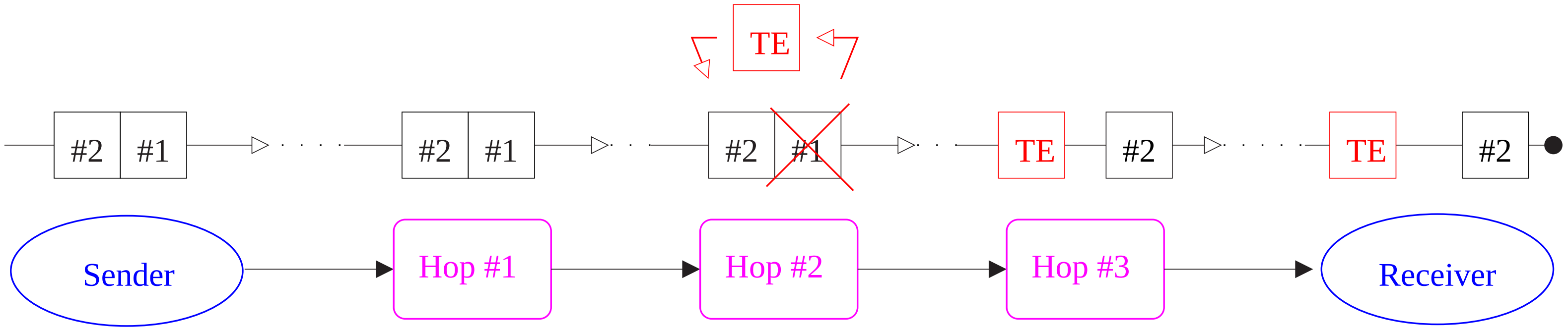


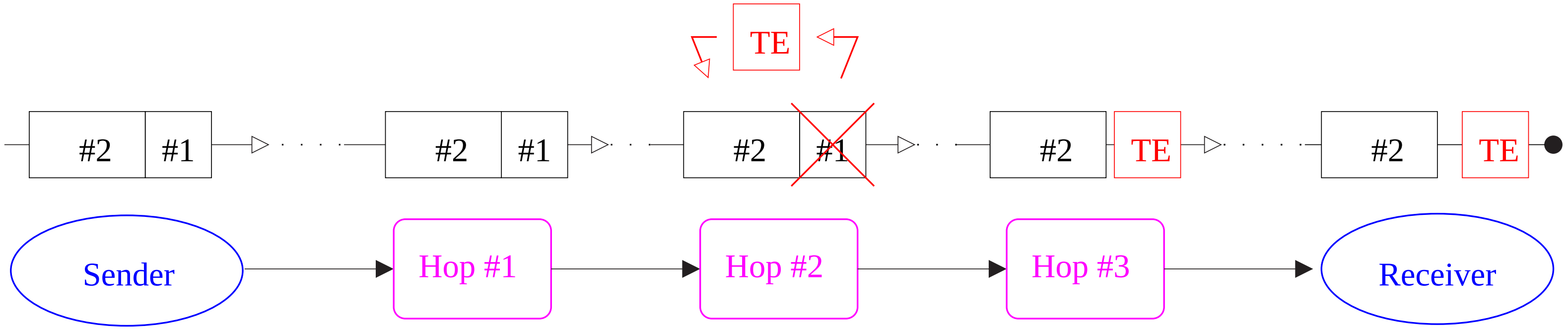
- *Spoofed* hop-limited probes



Something New with ICMP : Reordering

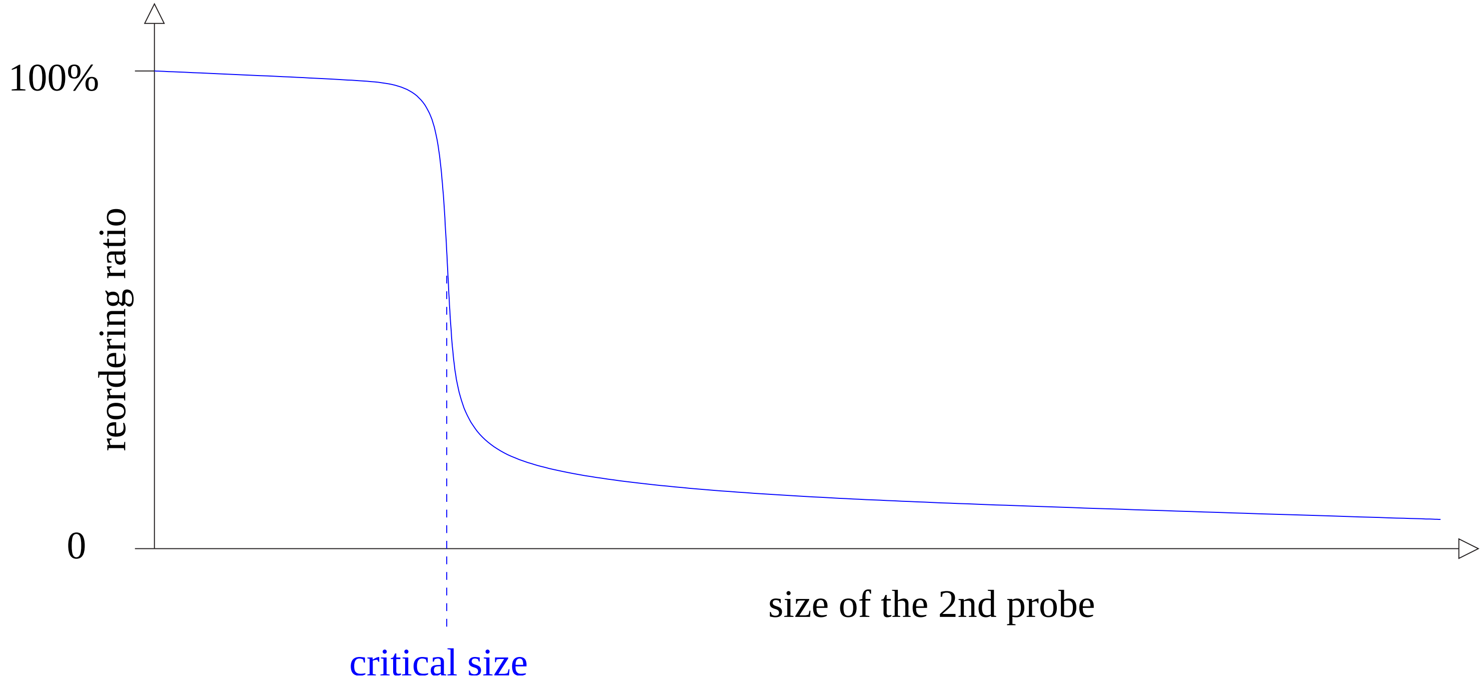
Experimental Methodology





Something New with ICMP : Reordering

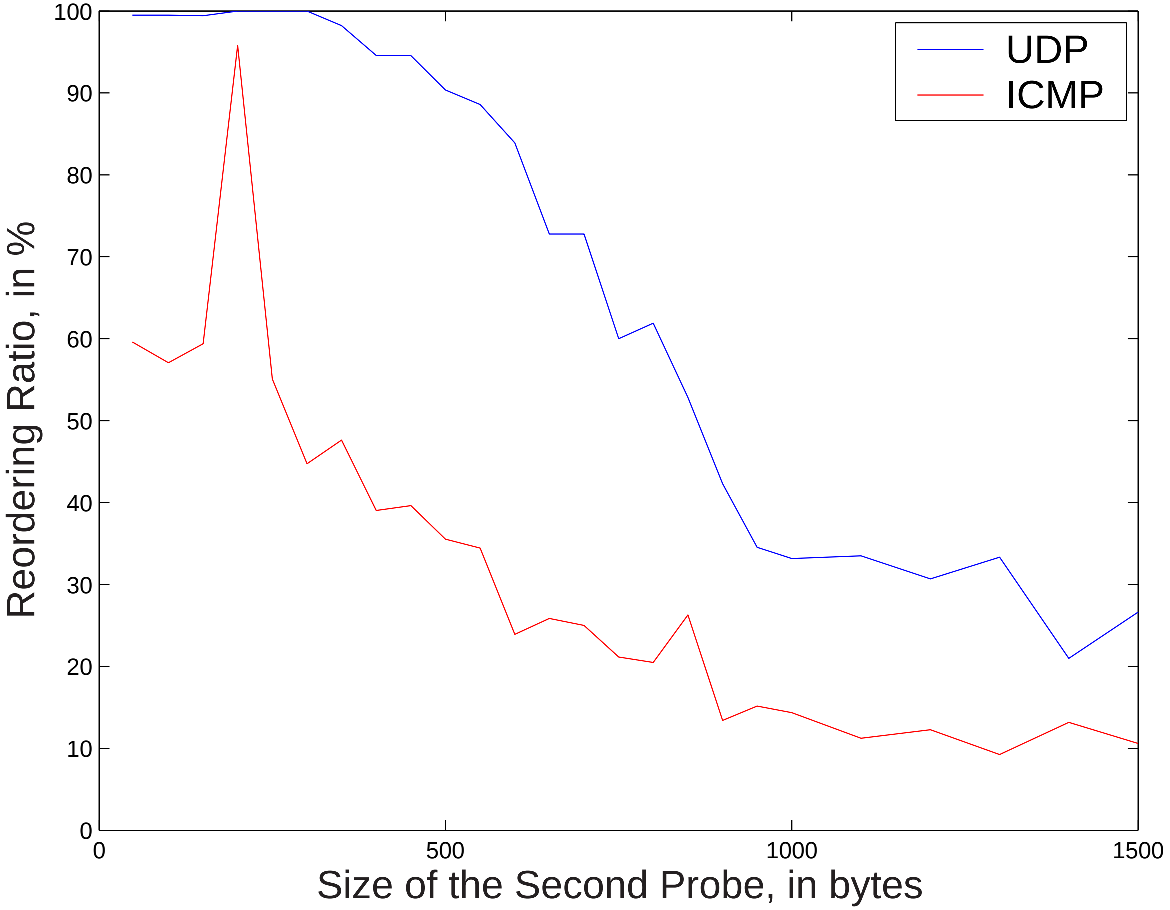
Theoritical Results



$$bandwidth = \frac{critical\ size}{ICMP\ generation\ time}$$

Something New with ICMP : Reordering

Experimental Results

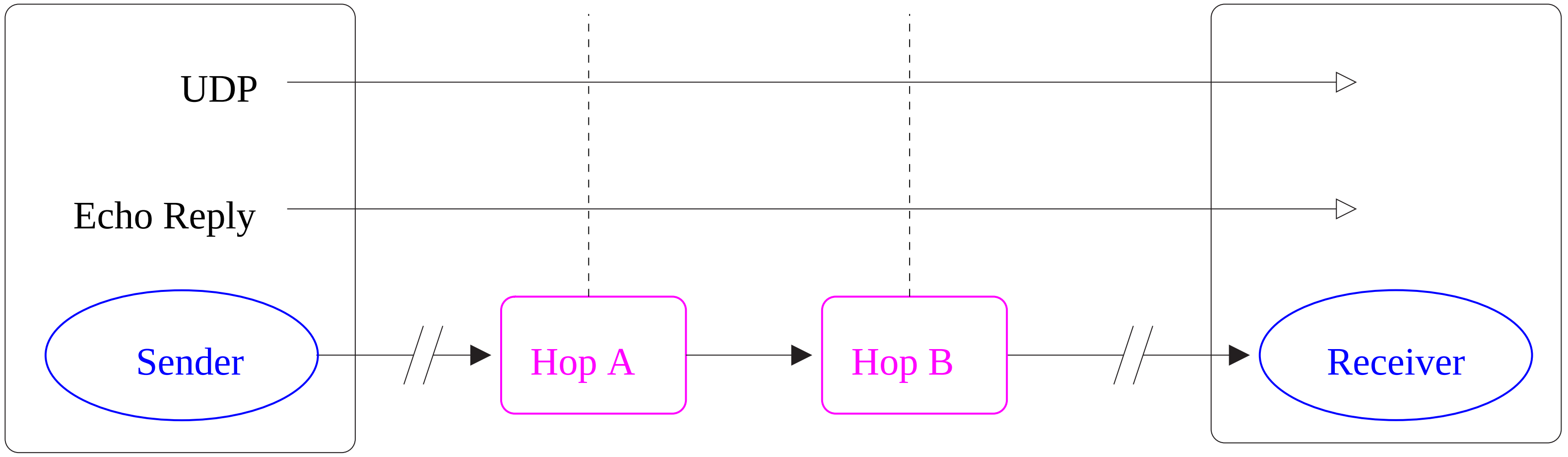


We need to know more about ICMP processing !

- What is going on ?
- To use all the possibilities that ICMP offers
- To discover, perhaps, some new tricks for Active Probing

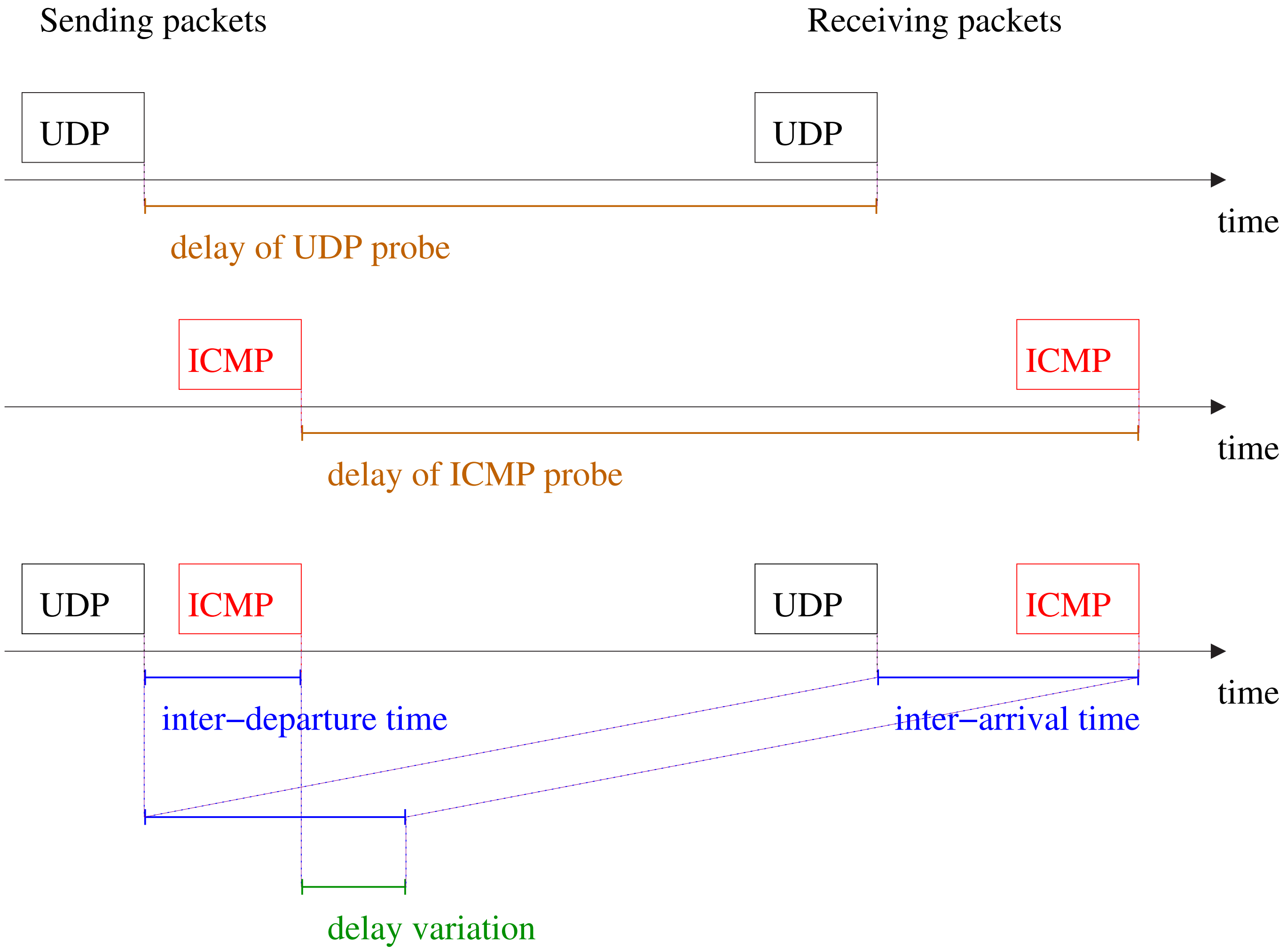
End-to-End Delay : Comparison between ICMP and UDP

Methodology



End-to-End Delay : Comparison between ICMP and UDP

Methodology



End-to-End Delay : Comparison between ICMP and UDP

Data processing

- Get N samples
- Get average delay variation : choose the apropriate filter

$\Rightarrow$ Average : too sensitive to noise

$\Rightarrow$ Robust Average : better, but still disturbed by outliers assymetry

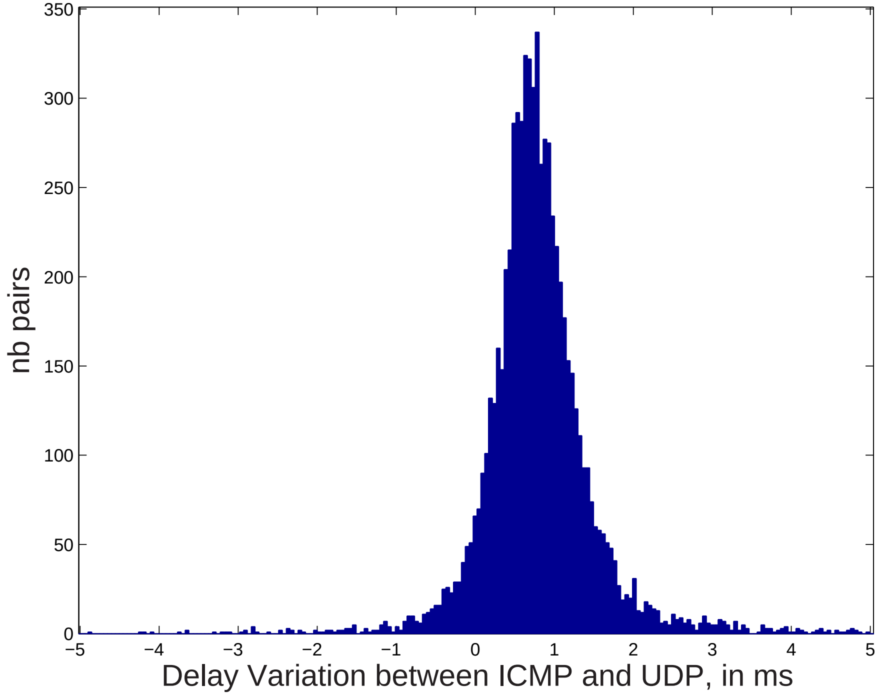
$\Rightarrow$ Difference of the Medians : quite good

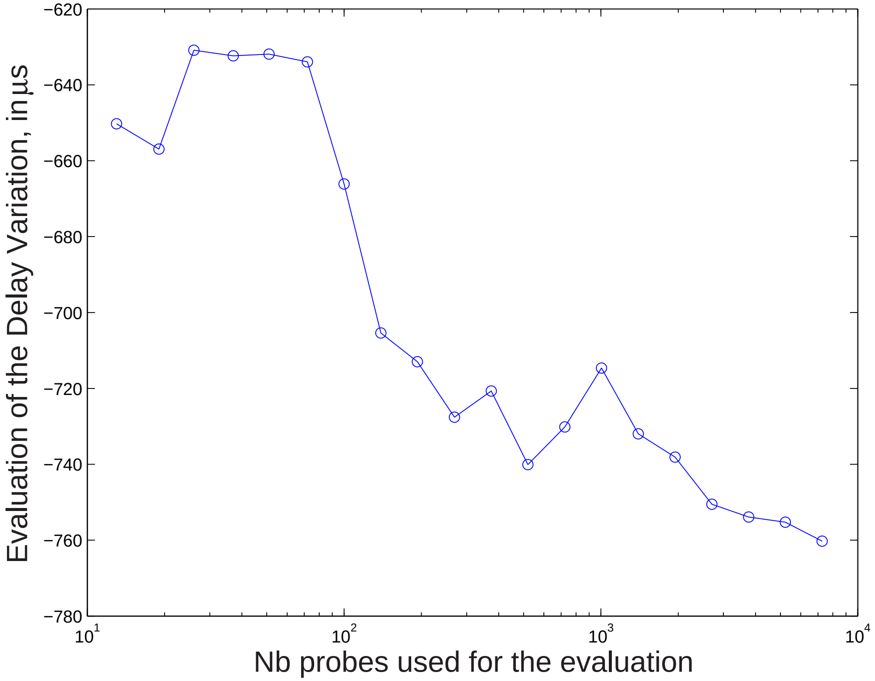
$\Rightarrow$ Median of the Differences : better

End-to-End Delay : Comparison between ICMP and UDP

Experiment on single Router

Route from France to Australia

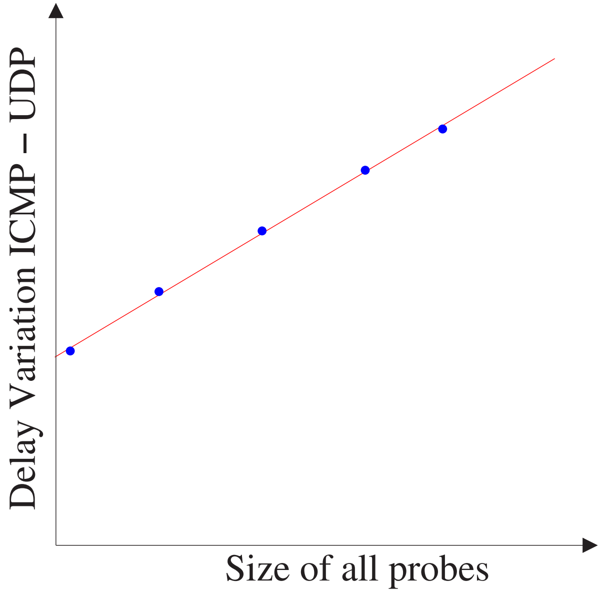




End-to-End Delay : Comparison between ICMP and UDP

Packet Size Dependance

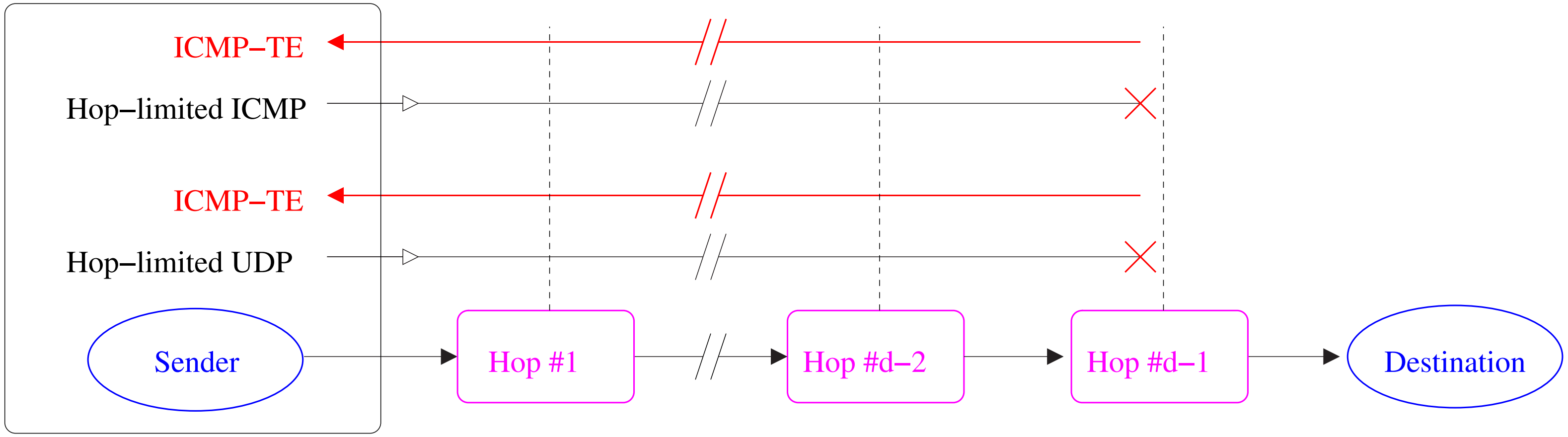
Size (bytes)	Delay variation (μs)
56	760
400	990
800	1225
1200	1460
1500	1620



End-to-End Delay : Comparison between ICMP and UDP

Larger Experiment : Methodology

- Pick a random destination host
- Run traceroute to get distance between us and host
- Run experiment with hop-limited probes, $TTL = distance - 1$



$$delay\ variation = RTT_{ICMP} - RTT_{UDP}$$

End-to-End Delay : Comparison between ICMP and UDP

Larger Experiment : Results

15 hosts around the world

- 6/15 : no ICMP-TE generation for *Echo Reply* probes
- 11/15 : Delay variation $< 30\mu s$
  $\Rightarrow$ Non-existent or insignificant ICMP difference
- 4/15 : ICMP slower than UDP
  $\Rightarrow$ Delay variation $\sim 250\mu s$ on 2 of them
  $\Rightarrow$ Delay variation $\sim 1ms$ on the 2 others

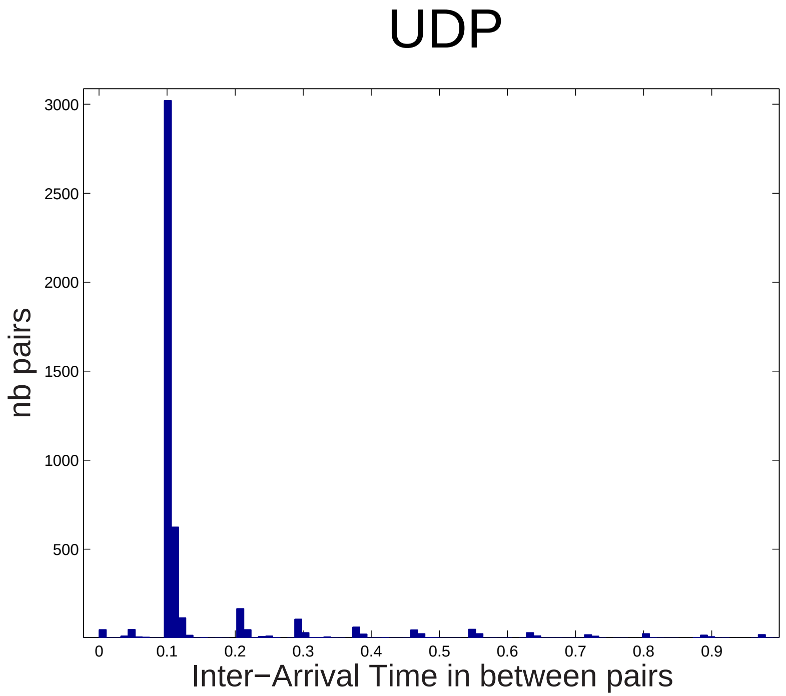
End-to-End Delay : Comparison between ICMP and UDP

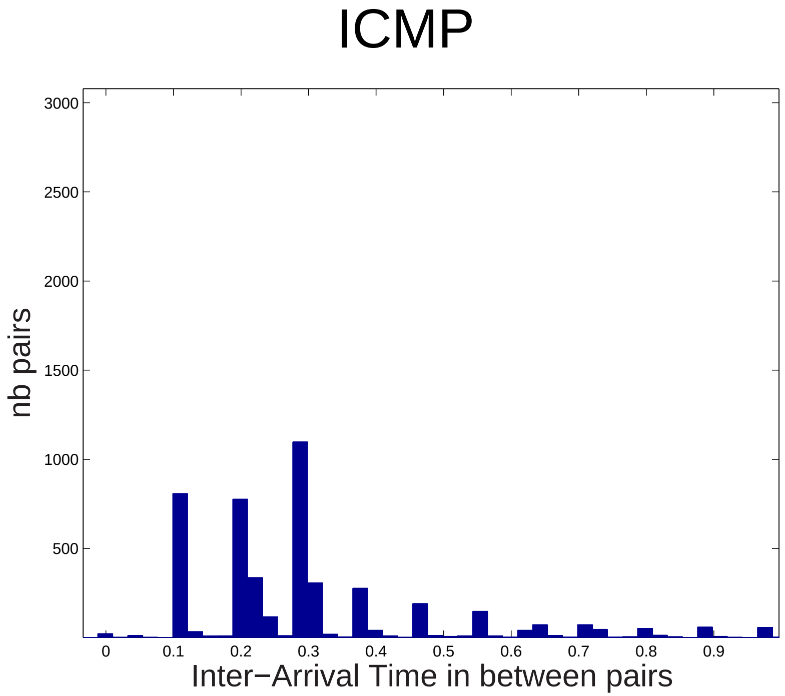
Others Types of ICMP

- Experiment was done only on a few routes
- UDP and ICMP *Time Exceeded*
- ICMP *Echo Reply* and ICMP *Time Exceeded*
- ICMP *Echo Reply* and ICMP *Echo Request*

⇒ Same delay

End-to-End Delay : Comparison between ICMP and UDP
Back-to-Back Probes





Inter-Arrival Time of probes sent back-to-back

⇒ Back-to-back ICMP pairs have Inter-Arrival Time bigger than UDP ones

⇒ ICMP queueing may be different in some routers

CUBIN

End-to-End Delay : Comparison between ICMP and UDP

Conclusions

- Some routers forward ICMP slower than UDP

  $\Rightarrow$ Delay variation $=$ Cst $+\lambda*$Size

  $\Rightarrow$ Practically, 80% have delay variation $< 2ms$

- But most treat them the same

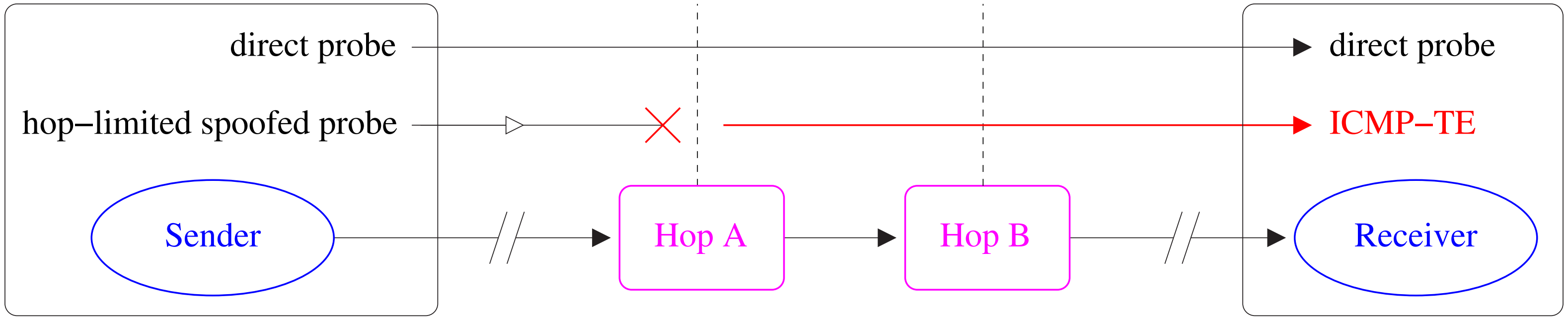
- However, ICMP-specific routers could become the norm

ICMP Generation Time

- Is it significant ?
- Is it always the same, for a given router ?
- If not, how does it vary ? (Noise, Size dependance . . .)

ICMP-TE Generation Time

State of the Art : Govindan & Paxson 1997



$$\text{ICMP-TE generation time} = D_{hop\ limited} - D_{direct}$$

- ICMP *Echo Reply* probes
- They used *Spoofing*
- Estimation were made over 200 Internet routers

ICMP-TE Generation Time

State of the Art : Govindan & Paxson 1997

The Results

$\Rightarrow$ For most routers (80%), ICMP-TE generation time $< 1ms$

$\Rightarrow$ 50% are even $< 300\mu s$

$\Rightarrow$ Sending back-to-back probes, they had 81% reordering

ICMP-TE Generation Time

Experimental Results

- The Results :

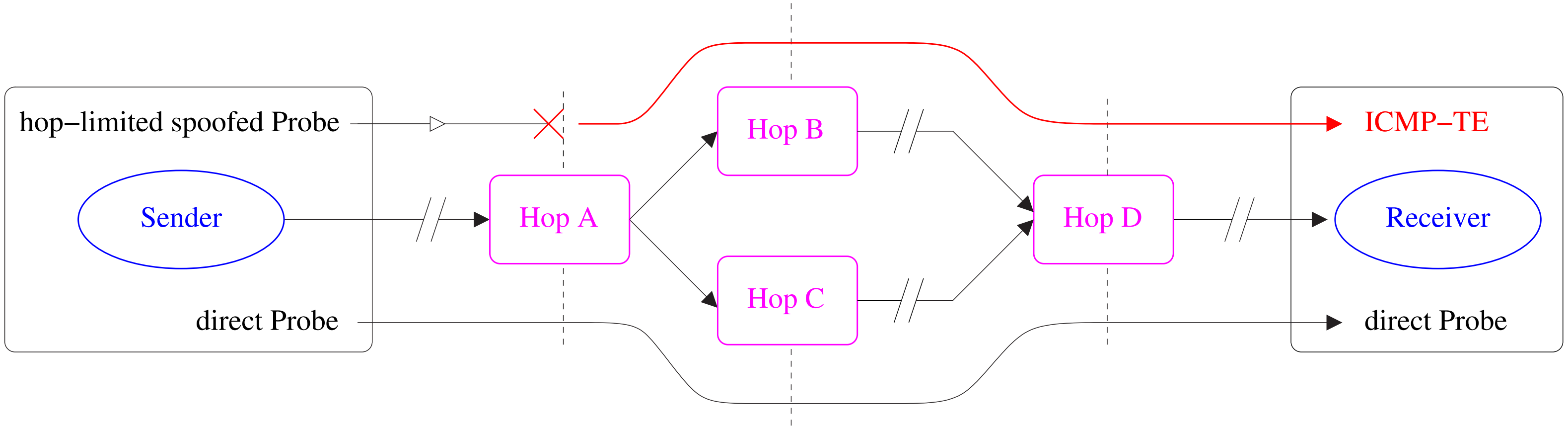
Route	Router	Gen. Time (μs)
CUBIN → CUBIN	CUBINlab Firewall	< 5
Paris → CUBIN	ENS Gateway	1250
Paris → CUBIN	Router #3	~ 100
Paris → CUBIN	Router #4	-9200

Spoofing protection reduces drastically the testbed

- Consistent with Govindan and Paxson's results
- The router #4 singularity

ICMP-TE Generation Time
Experimental Results

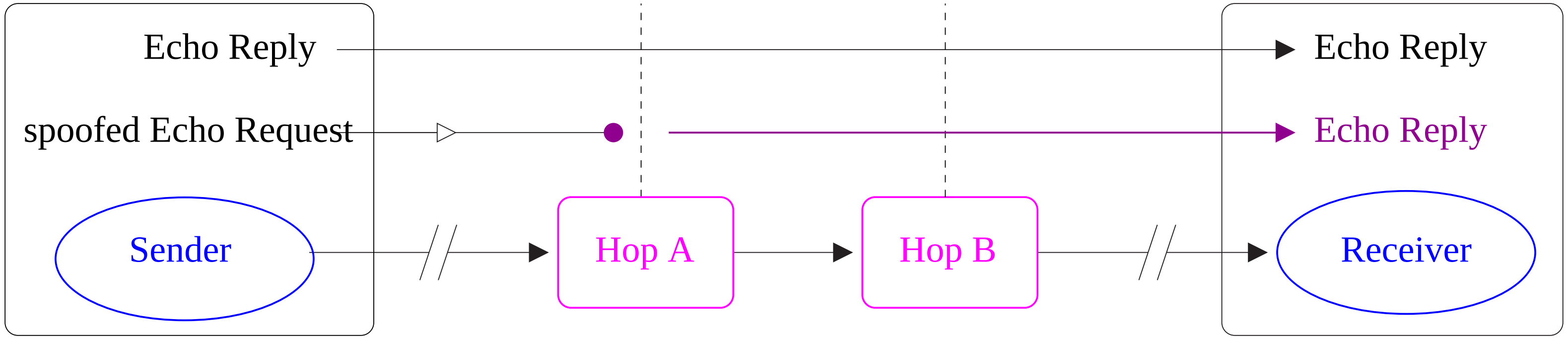
The router #4 singularity : a route change ?



⇒ Spoofing doesn’t always work properly

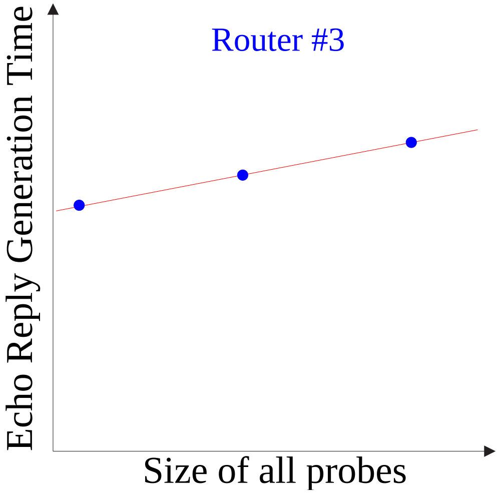
⇒ But no such result in Govindan and Paxson’s paper

ICMP *Echo Reply* Generation Time



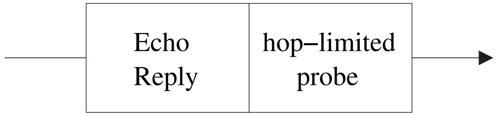
- The Results :

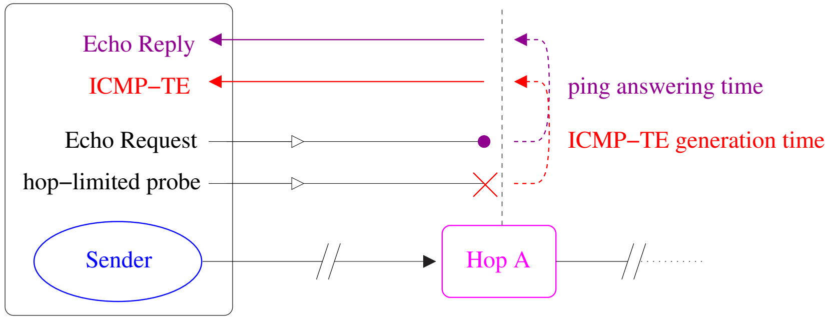
Router	Gen. Time (μs)
ENS Gateway	< 20
Router #3	~ 116
Router #4	~ 20



ICMP can be Powerful without Spoofing

Experimental Methodology

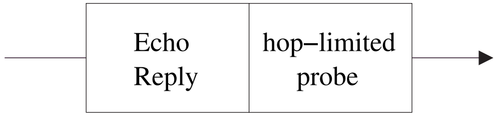


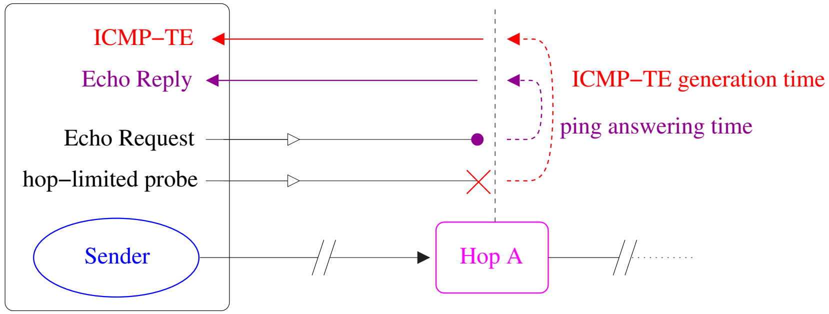


ICMP-TE generation time $=$ *ping* answer time

ICMP can be Powerful without Spoofing

Experimental Methodology





ICMP-TE generation time $>$ *ping* answer time

ICMP can be Powerful without Spoofing

Advantages

- doesn't need Spoofing
- Sender = Receiver
- Many adjustable Parameters :
  - ⇒ Size of the hop-limited probe
  - ⇒ Size of the *ping* probe
  - ⇒ Initial Order

ICMP can be Powerful without Spoofing

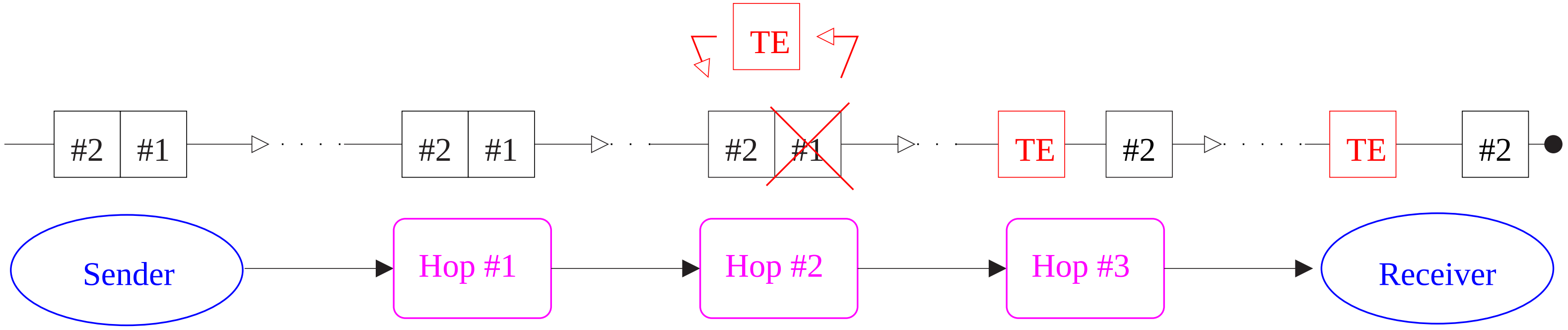
Some Results

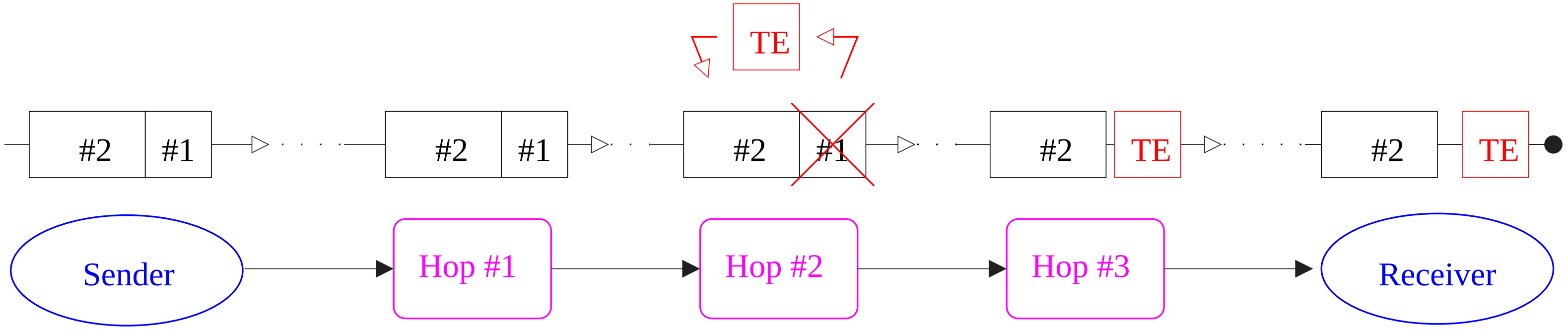
- Tests on 3 routes
  - ⇒ Route #1 : No reordering
  - ⇒ Route #2 : 100% reordering, i.e. ping is much too faster
  - ⇒ Route #3 : Some reordering, but ratio decreases with size
- A promising avant-goût : that could work!

ICMP is More Resistant to Natural Reordering

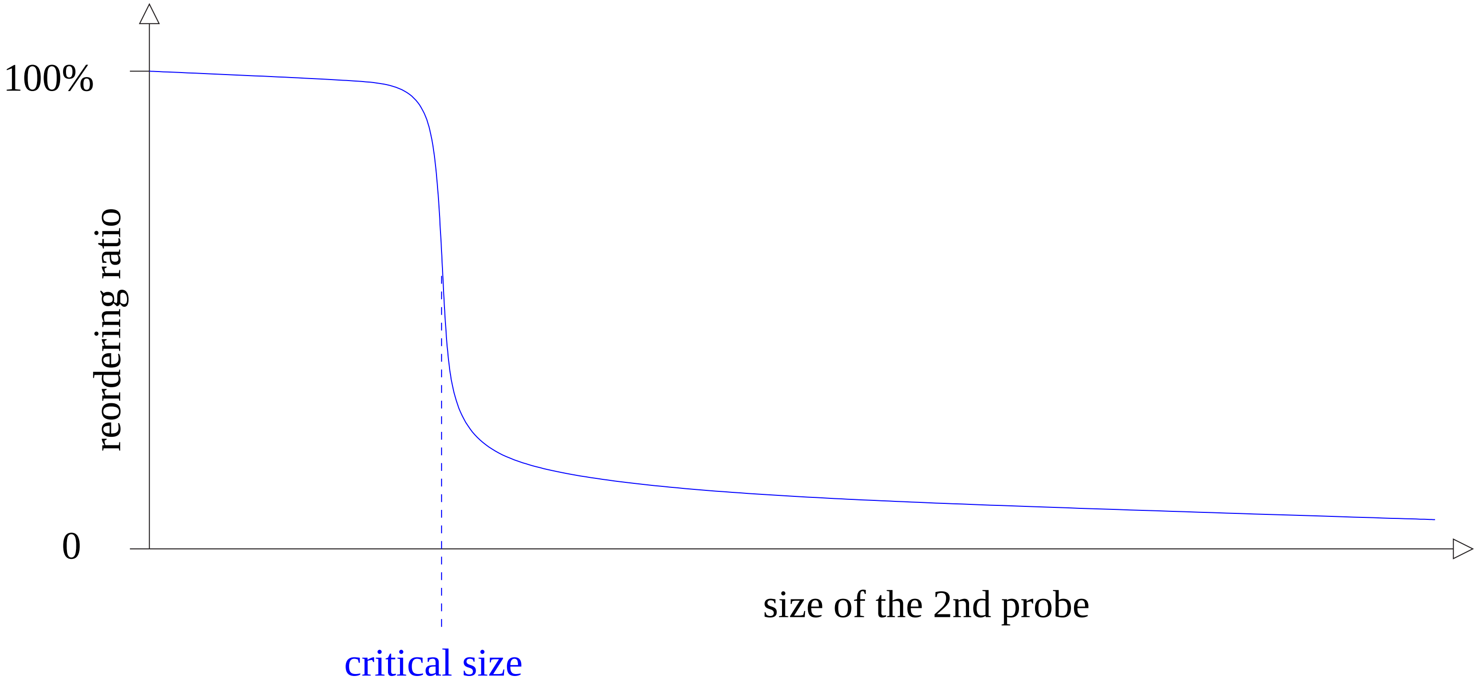
- Natural Reordering exists : tests with UDP packets
  - ⇒ Small passing one bigger
  - ⇒ Many smalls passing one bigger
  - ⇒ Never passing more than one
- No (or a very little) natural reordering with ICMP packets
- Using ICMP reduces the reordering noise

Application : Failed Experiment



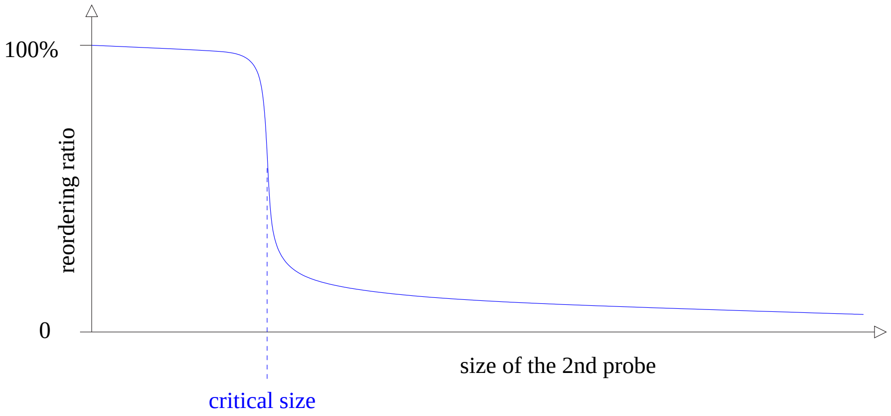


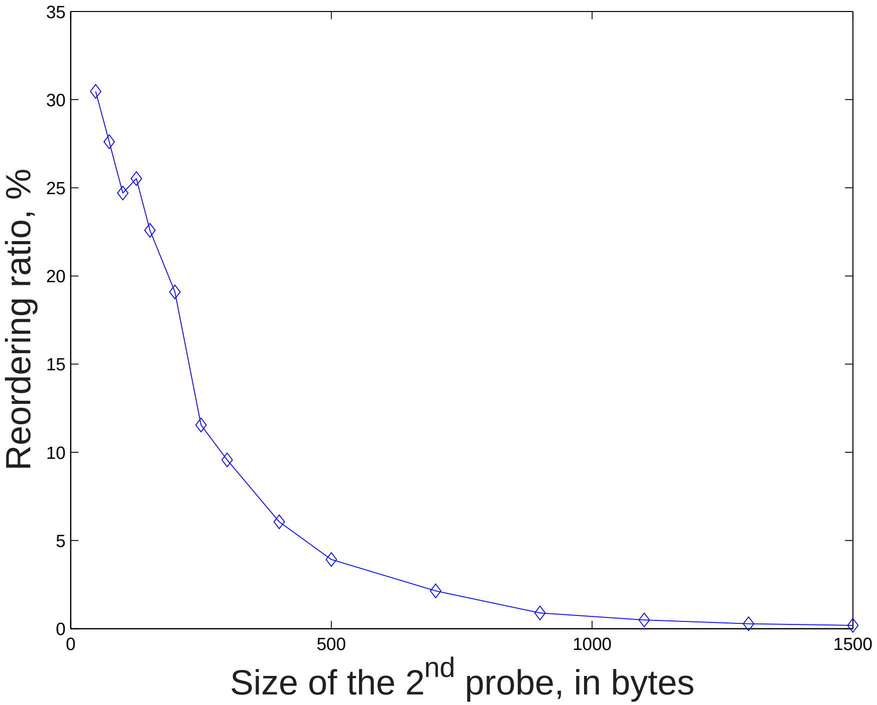
Application : Failed Experiment



$$bandwidth = \frac{critical\ size}{ICMP\ generation\ time}$$

Application : Failed Experiment . . . Finally Works!





Application : Failed Experiment . . . Finally Works!

What changed ?

- ICMP probes instead of UDP

  ⇒ removed ICMP delay difference

  ⇒ removed Natural Reordering

- Direct 2nd probe is now Spoofed Echo Request

Conclusion

ICMP offers many possibilities :

- Alternative to classical probes

  ⇒ Add degrees of freedom

- Router-interaction probe

  ⇒ Add new concepts

⇒ Enlarges the possibilities of Active Probing