Don’t Trust Traceroute (Completely)

Pietro Marchetta†  Valerio Persico‡  Ethan Katz-Bassett‡  Antonio Pescapé§
†University of Napoli “Federico II”, Italy  ‡University of Southern California, CA, USA
§University of California, CA, USA
{pietro.marchetta, valerio.persico, pescape}@unina.it  ethan.kb@usc.edu

Traceroute and its Applications

How Traceroute works

- TTL = 1
- TTL = 2
- TTL = 3
- TTL = 4
- TTL = 5

ICMP Time Exceeded
ICMP Port Unreachable

UDP Packet Probe

Uses of Traceroute

- Network Troubleshooting
- Anomaly Detection
- Performance Analysis
- Geolocation
- Censorship Detection
- Internet Topology Discovery

Our Contributions

Analysis and preliminary quantification of the following observed phenomena:
- Traceroute
- may suggest false path changes
- may overestimate the presence of load-balancers

Don’t trust Traceroute that much!

False path changes

Different IPs appearing at the same hop of consecutive Traceroute measurements do not necessarily imply the path has changed.

Hops

At time t₁: S - A - B - C - D
At time t₂: S - A - B - C - D

Differing IP, Different Routers?

Did the path from S to D really change?

Overestimation of load-balanced paths

Multiple IPs appearing at the same hop of a multipath Traceroute measurement are not always related to multiple paths at router level.

Hops

Flow1
Flow2
Flow3

Differing IP, Different Routers?

How many different paths exist from S to D?

Preliminary Experimental Analysis

- 720k paths collected by 4 PlanetLab nodes in two consecutive days
- Extracted 38k distinct paths containing at least one different hop but unchanged in terms of number of hops

Alias Resolution

to check whether a path has really changed

- 32.1% of the paths changed at the IP level proved to be unchanged at the router-level

- 8.4k IP load-balanced paths collected by 14 PlanetLab nodes

Alias Resolution

to check if there are really multiple paths toward the destination

- Load balanced paths appear to be overestimated!
- 14% of routes with multiple IP level paths turned out to be a unique router-level path

Conclusion and Future Work

- Traceroute reports interfaces, not routers
- Traceroute can suggest that two measurements represent distinct paths even though they traverse the same routers
- Alias Resolution is essential to improve state-of-the-art implementations of Traceroute
- In the light of our findings, previous results on route stability and path diversity could be reassessed

How is it possible?

Traceroute is commonly believed to report the incoming interface of the routers. However, Traceroute may actually report also outgoing interfaces.

RFC1812: The source address of an ICMP error packet must correspond to the outgoing interface of the ICMP reply, rather than the interface on which the packet triggering the error was received.

RFC-compliant routers exist \[\text{[Mao2003]}\]