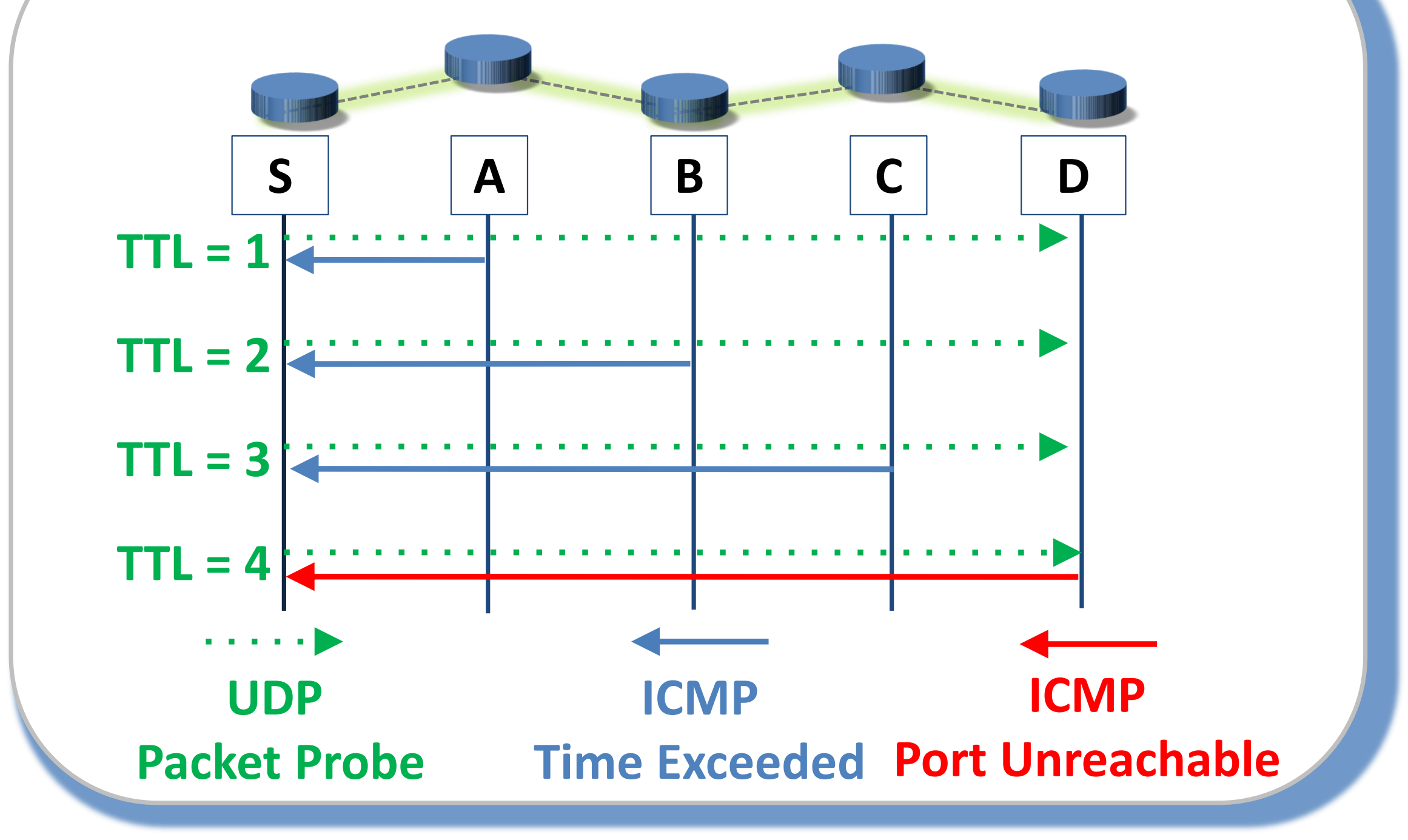
Don’t Trust Traceroute (Completely)

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

Traceroute and its Applications

How Traceroute works



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

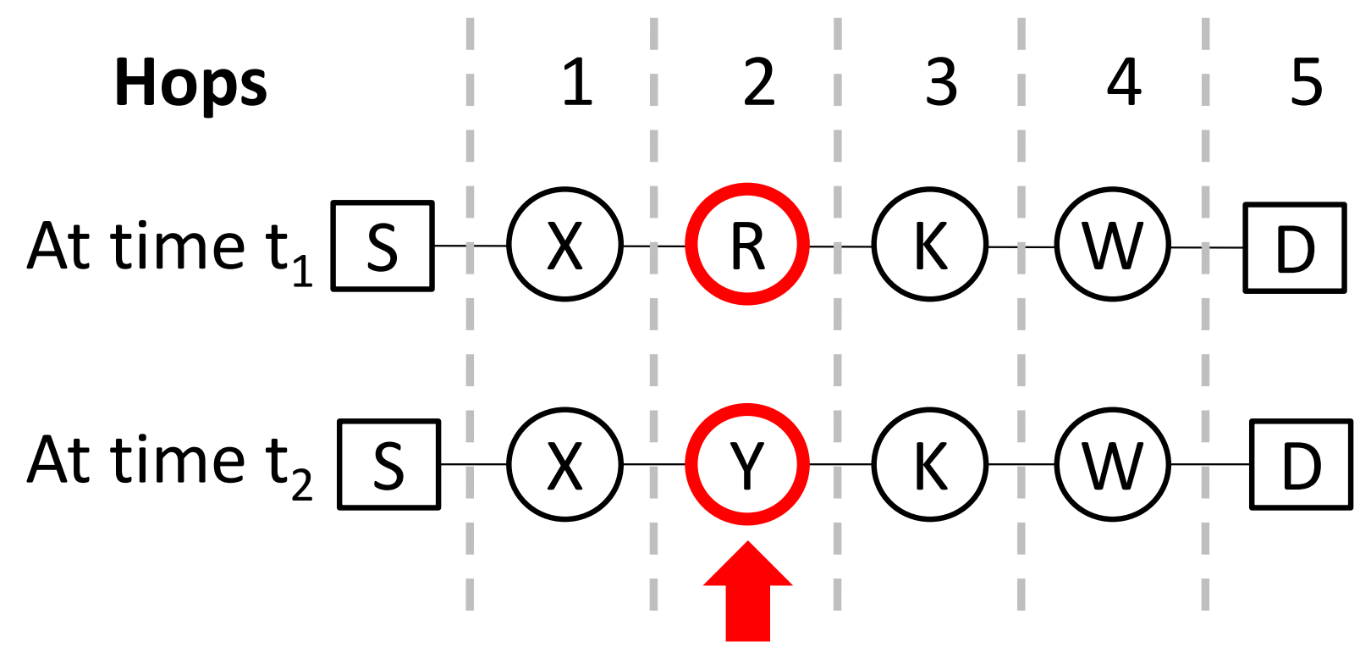
- ✓may **suggest false path changes**
- ✓may **overestimate the presence of load-balancers**

Don’t trust Traceroute that much!

Scenarios

False path changes

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

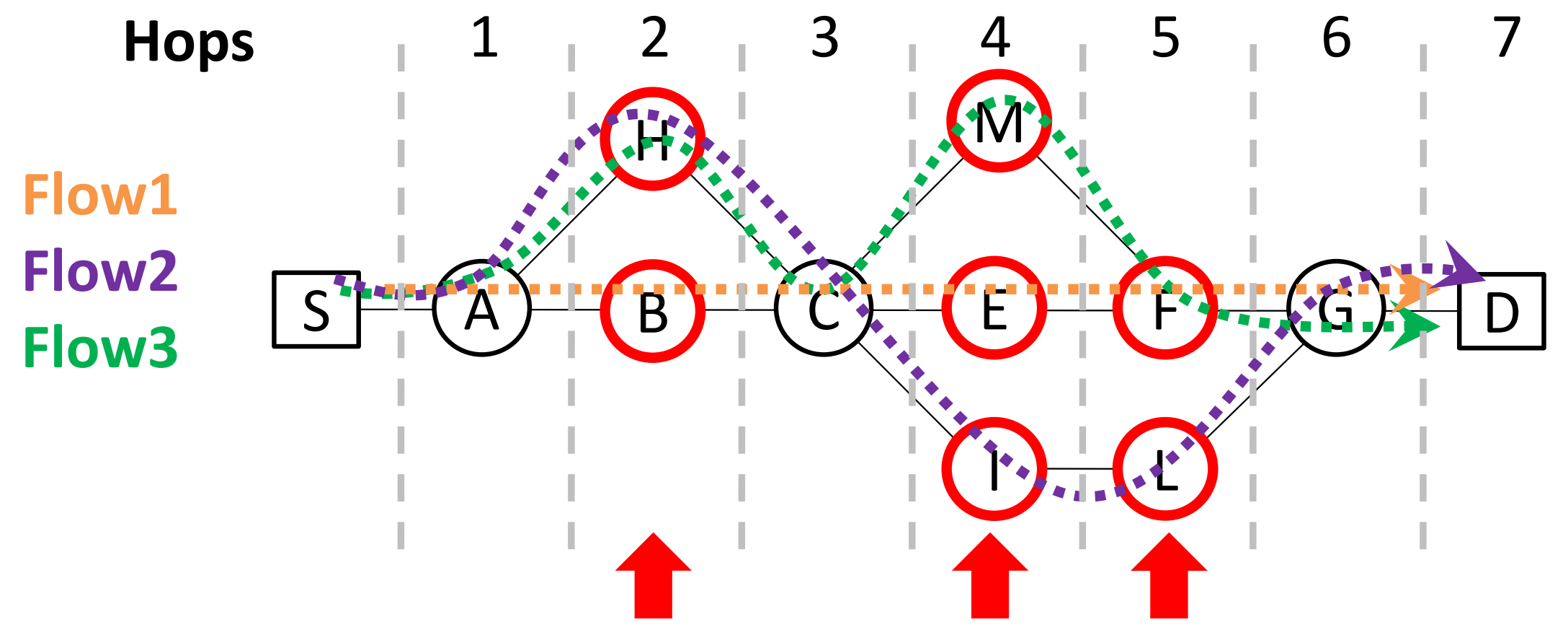


Differing IP, Different Routers?

Did the path from S to D *really* change?

Overestimation of load-balanced paths

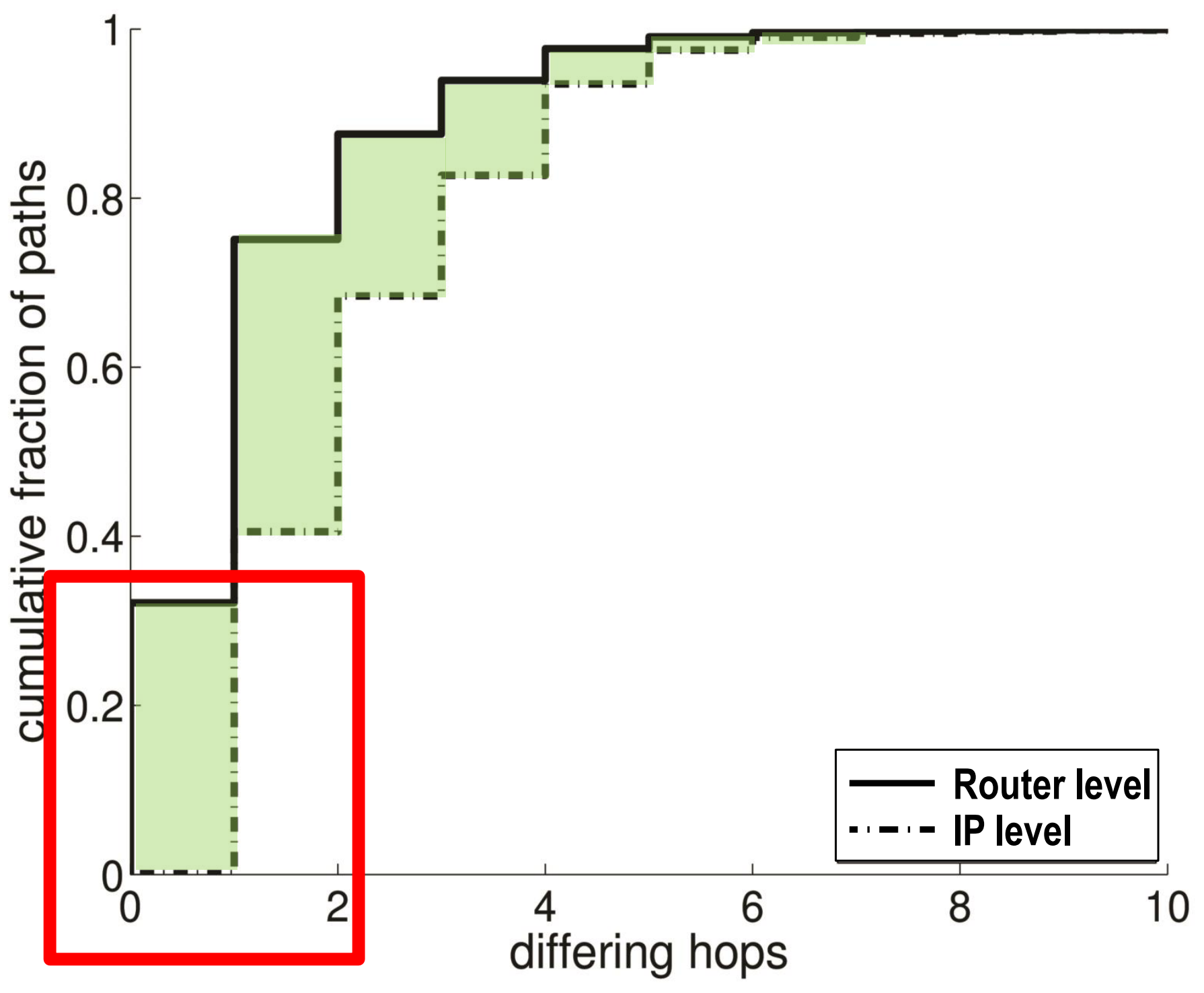
Multiple IPs appearing at the same hop of a multipath Traceroute measurement are not always related to multiple paths at router level



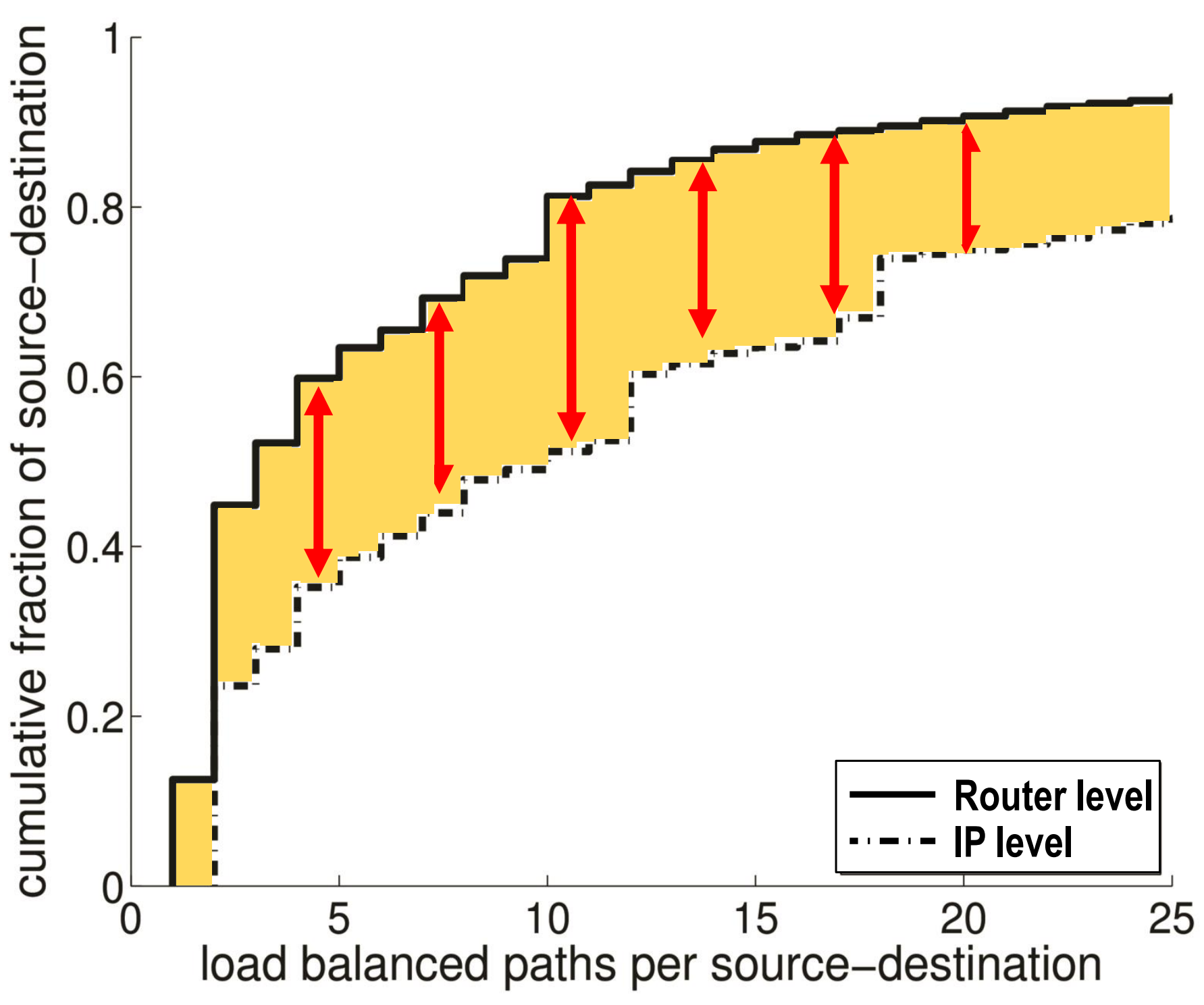
Differing IP, Different Routers?

How many *different* paths exist from S to D?

Preliminary Experimental Analysis



1. ✓ 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
2. ✓**Alias Resolution** to check whether a path has really changed
3. **• 32.1% of the paths changed at the IP level proved to be unchanged at the router-level**

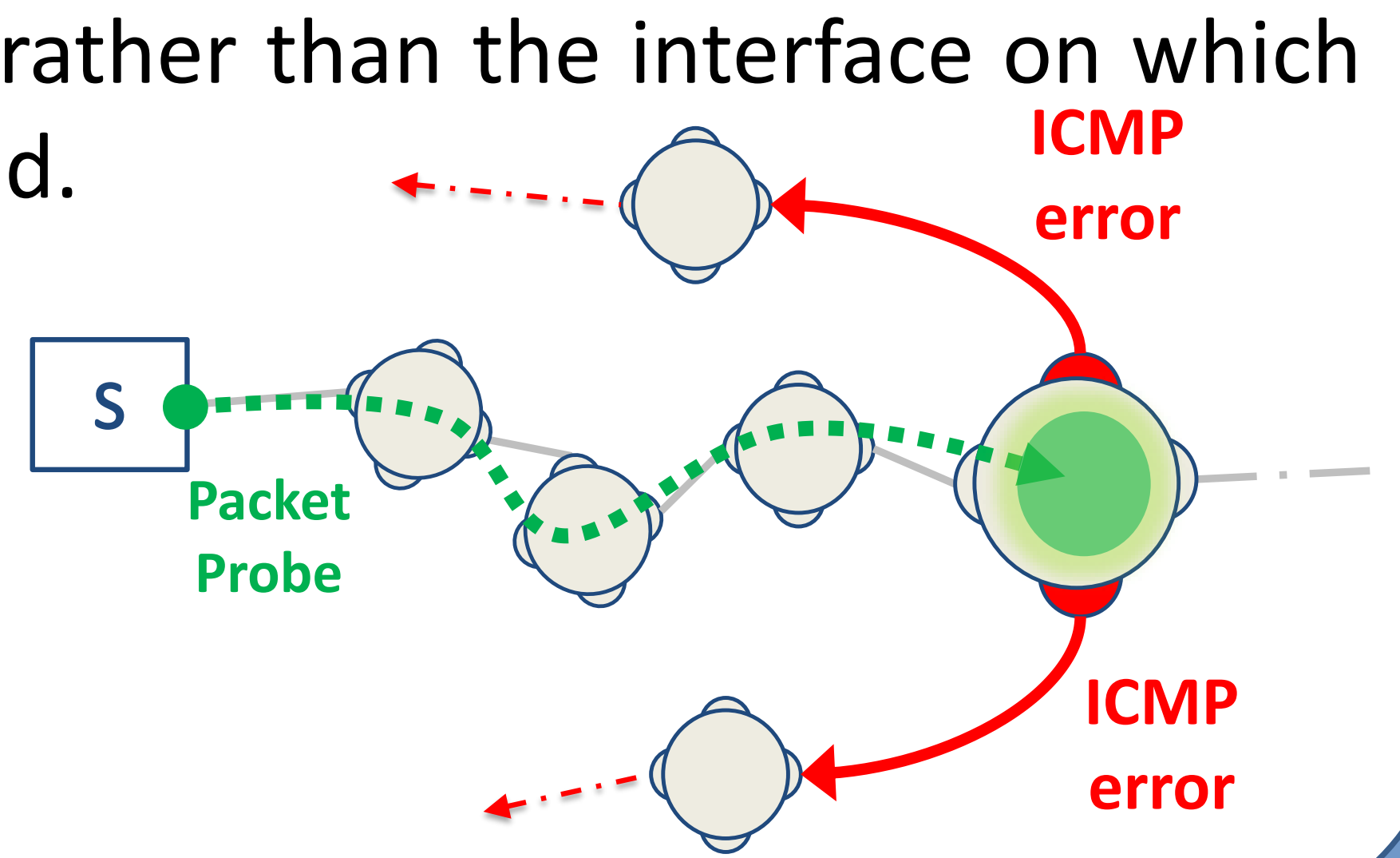


1. ✓8.4k IP load-balanced paths collected by 14 PlanetLab nodes
2. ✓**Alias Resolution** to check if there are really multiple paths toward the destination
3. **• Load balanced paths appear to be overestimated!**
   • 14% of routes with multiple IP level paths turned out to be a unique router-level path

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 [Mao2003]



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

[Mao2003] Z. Mao, J. Rexford, J. Wang, and R. Katz. Towards an accurate AS-level Traceroute tool. In Proc. ACM SIGCOMM, 2003.