Scamper update

Matthew Luckie
University of Waikato
mjl@wand.net.nz

Recent work on scamper

- Enhanced control socket
- Numerous enhancements to regular traceroute
- Load-balancer traceroute
- IP Alias resolution techniques
- Firewall support (limited)
- Sting

- http://www.wand.net.nz/scamper/

Traceroute probe method and forward IP path inference

Matthew Luckie

Young Hyun

Brad Huffaker

Traceroute methods surveyed

- UDP
  - probe id: dport (unused); ephemeral sport;
- **UDP-Paris**
  - probe id: UDP checksum field; ephemeral sport; unused dport;
- ICMP
  - probe id: icmp sequence field;
- **ICMP-Paris**
  - probe id: icmp sequence field;
- **TCP (port 80)**
  - probe id: IP ID; dport 80, ephemeral sport
- **UDP-Paris DNS**
  - probe id: UDP checksum field; 5-tuple constant; sport 53; unused dport; valid DNS payload

Goals

- Determine which traceroute technique is the most effective
  - most reachable destinations
  - most complete paths
  - most IP links discovered
  - most AS links discovered
  - fewest gap limits (5 consecutive unresponsive hops)
  - fewest loops
  - fewest obviously spoofed responses
- … depending on the destination type
  - 261,530 routable IP addresses selected at random
  - top 500 webservers as ranked by alexa (422 IPs)
  - 2000 routers selected at random
- will focus mostly on random routable IP addresses

Random routable IP addresses

- 257,504 prefixes observed at routeviews for week of 19-25 March 2005 (median snapshot per day)
- 255,981 prefixes observed in at least 3 snapshots
  - one random address per prefix if prefix is more specific than /16
  - one per /16 otherwise
  - never select more than 1 address per /24, addresses in team cymru bogon list, do-not-probe (1.14 /8s)
- 261,530 addresses selected
- use unique list per vantage point

Methodology

- conduct six traceroutes for each destination in random order
  - UDP *
  - UDP-Paris
  - UDP-Paris DNS *
  - ICMP *
  - ICMP-Paris
  - TCP
- 5 second cool-down between methods finishing
- conduct traceroutes at 100pps from *.ark.caida.org
  - 11 vantage points
  - 2 attempts per hop
  - 5 hop gaplimit
  - halt on first loop *

261,530 routable IP addresses: cbg-uk

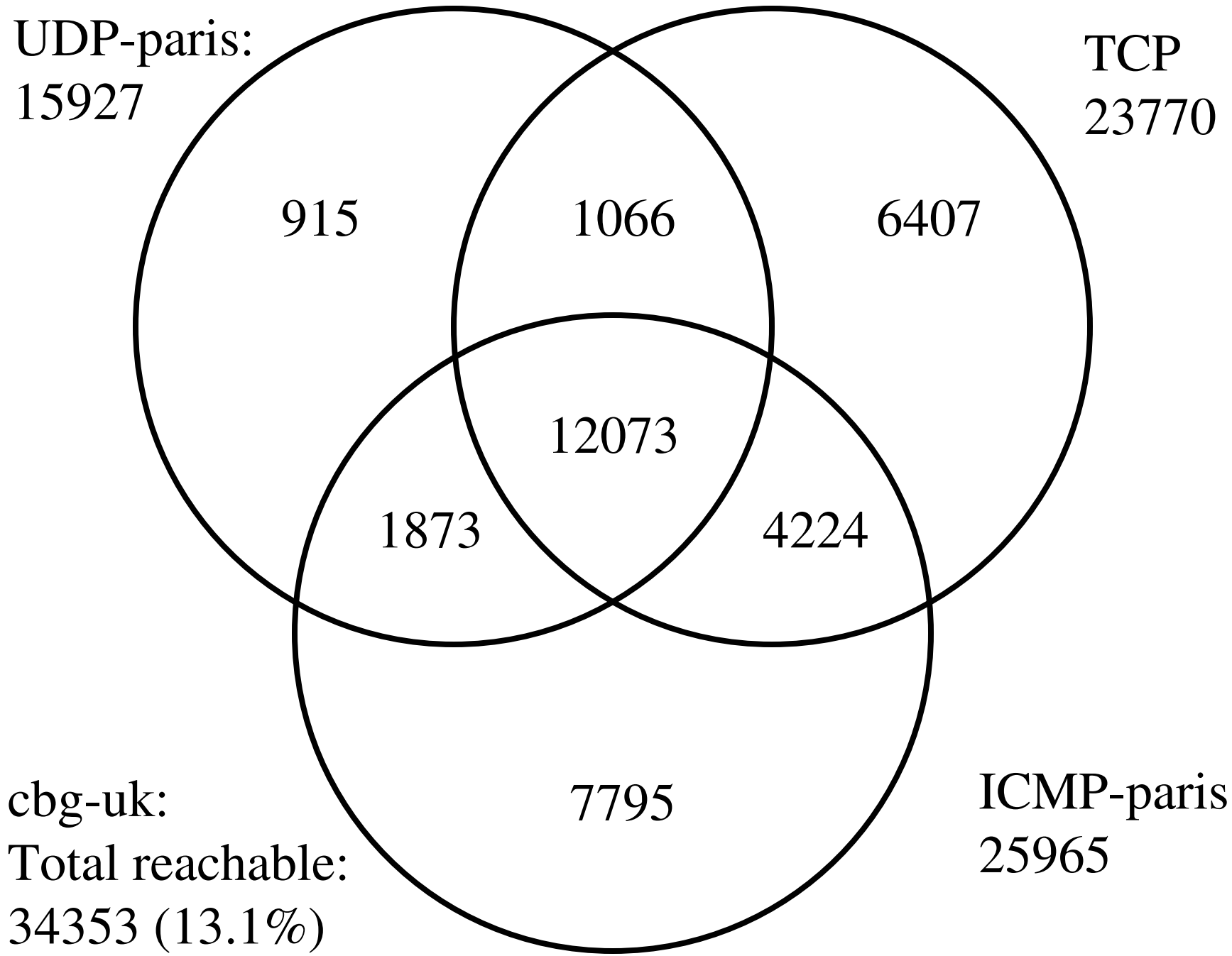
	reached	icmp unreach	loop	gaplimit
udp	5.9%	10.8%	10.0%	73.3%
udp-paris	6.1%	11.0%	7.9%	75.1%
udp-paris dns	6.0%	11.1%	7.9%	75.0%
icmp	9.8%	12.2%	9.2%	68.8%
icmp-paris	9.9%	12.4%	8.0%	69.7%
tcp (p 80)	9.1%	11.4%	7.8%	71.8%

Comments

- ICMP-Paris reaches most destinations
  - also obtains most ICMP unreachables, which is better than having your probe silently discarded
- UDP reaches the least
  - But it and the ICMP technique are known to produce invalid IP paths more frequently than their Paris counterpart
- UDP-Paris DNS performs slightly worse than UDP-Paris

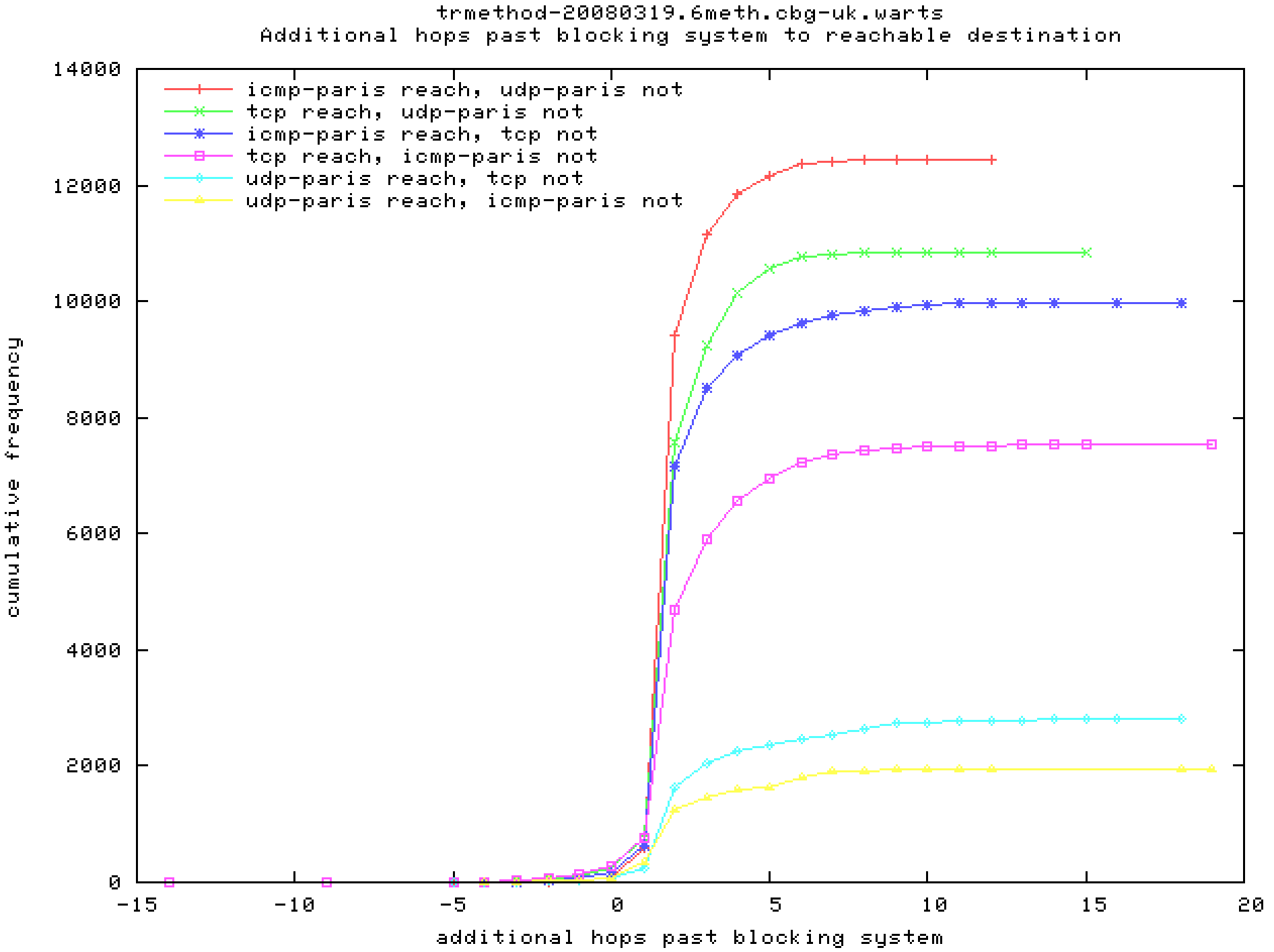
Comments

- Reachability results very similar across other ten vantage points
  - despite different IP lists
- Some variation in ICMP-Unreach, Loops, Gaplimit
  - vantage point a factor


UDP-paris:
15927
TCP
23770
915
1066
6407
12073
1873
4224
7795
cbg-uk:
Total reachable:
34353 (13.1%)
ICMP-paris
25965

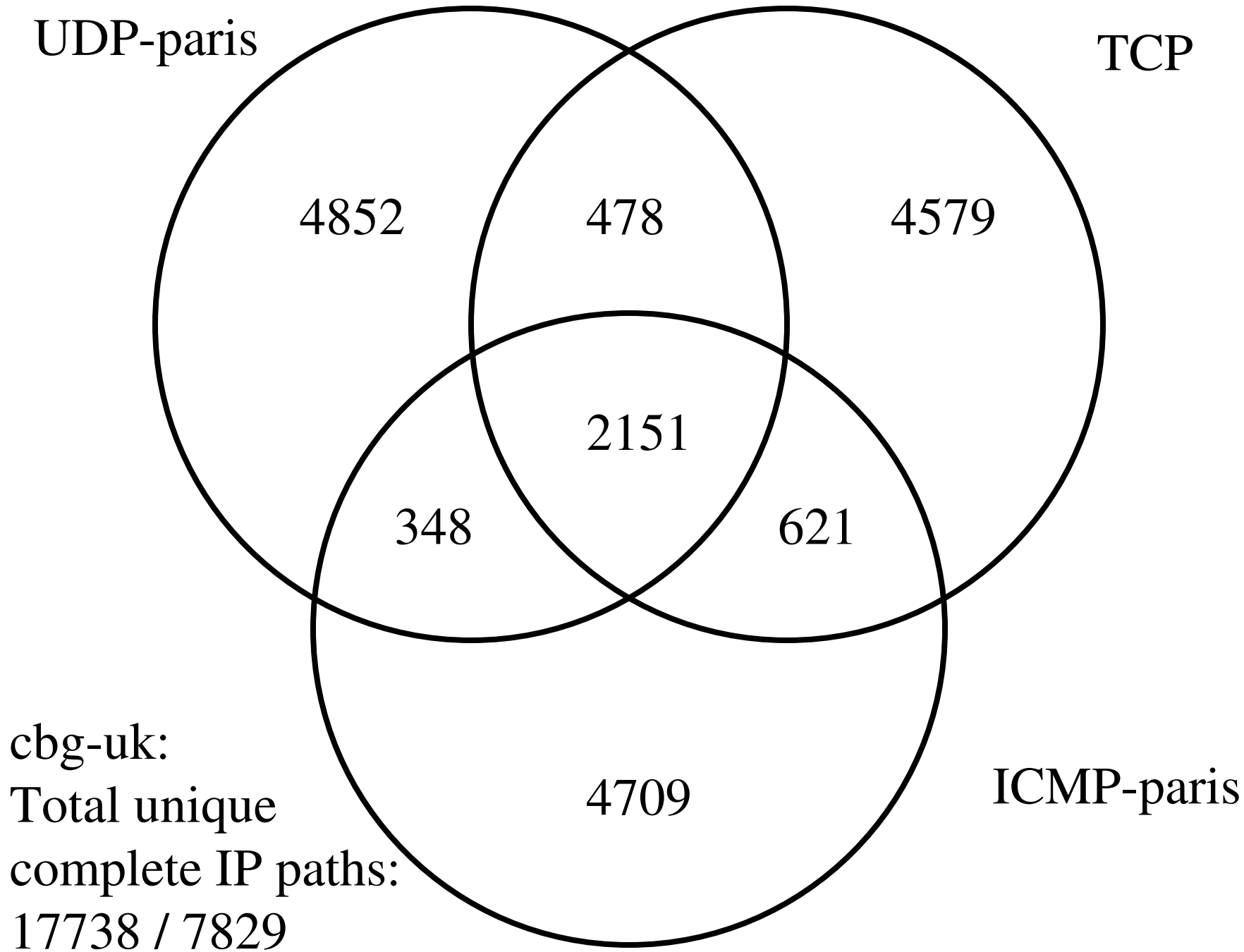
Reachable destinations

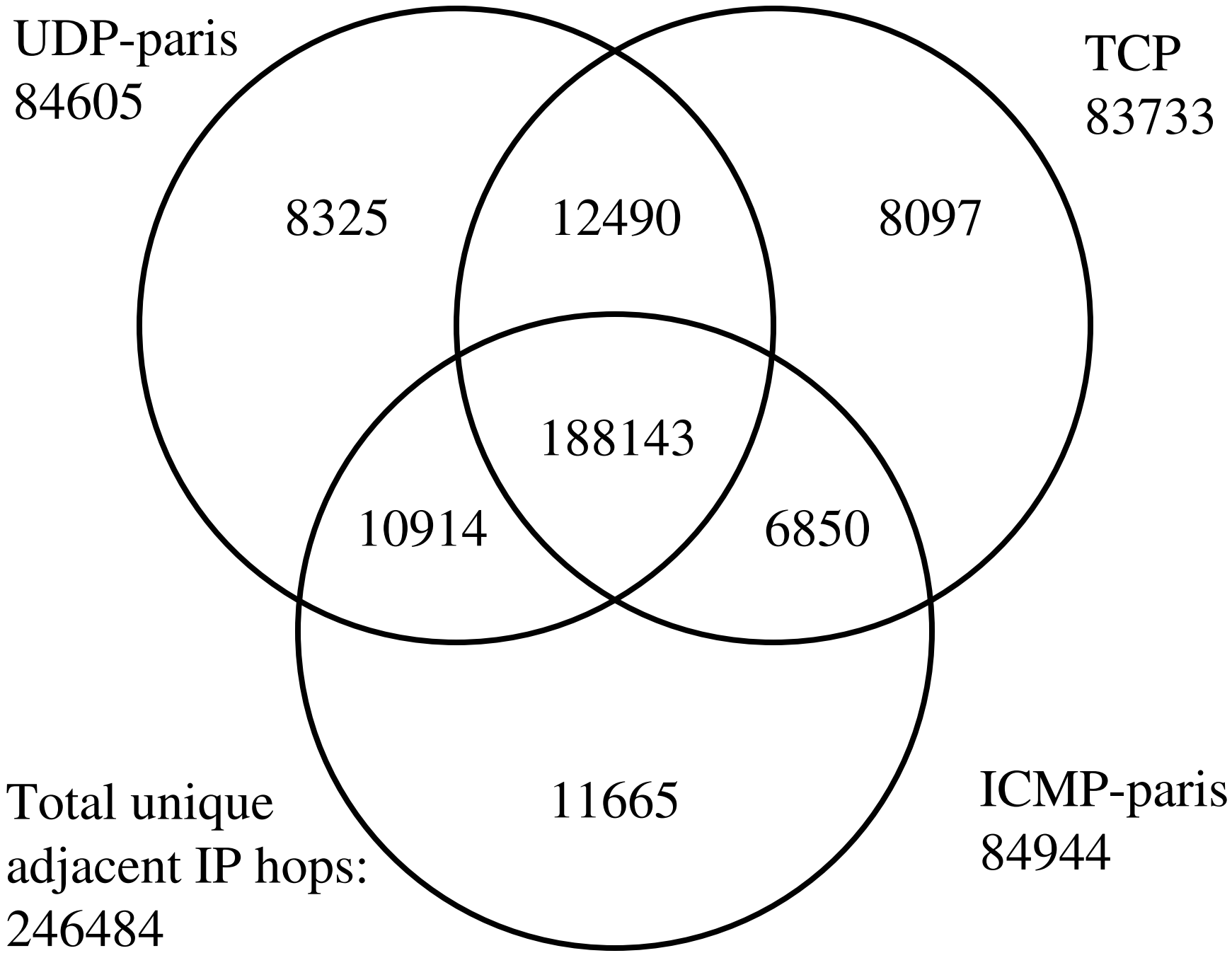
- Total reachable: 34353 (13.1%)
- ICMP-paris by itself yields the most:
  - 25965 (9.9%)
- ICMP-paris and TCP to get:
  - 33438 (12.8%)
- Not using UDP misses 2.7% of destinations reachable with three methods


trmethod-20080319.6meth.cbg-uk.warts
Additional hops past blocking system to reachable destination
icmp-paris reach, udp-paris not
tcp reach, udp-paris not
icmp-paris reach, tcp not
tcp reach, icmp-paris not
udp-paris reach, tcp not
udp-paris reach, icmp-paris not
cumulative frequency
additional hops past blocking system
0
2000
4000
6000
8000
10000
12000
14000
-15
-10
-5
0
5
10
15
20

Complete Paths

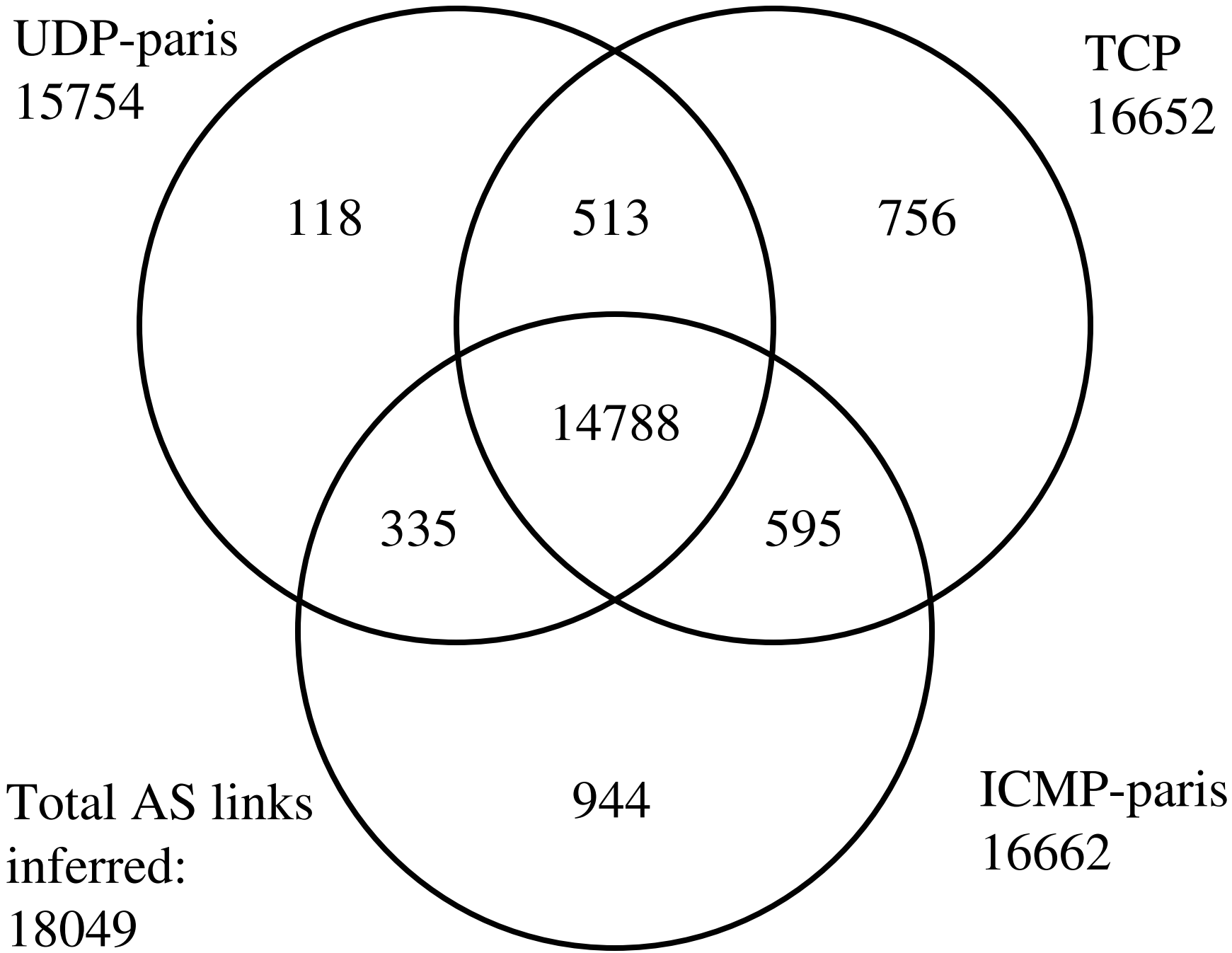
- Defined as reaching destination and every hop returning an ICMP message
  - UDP-Paris: 10842
  - ICMP-Paris: 17703
  - TCP: 15244
  - Intersection: 7829


UDP-paris
TCP
4852
478
4579
2151
348
621
4709
ICMP-paris
cbg-uk:
Total unique
complete IP paths:
17738 / 7829


UDP-paris
84605
TCP
83733
8325
12490
8097
188143
10914
6850
11665
Total unique
adjacent IP hops:
246484
ICMP-paris
84944

Unique adjacent IP hops

- Total 246484
  - UDP-Paris 89.2%
  - ICMP-Paris 88.3%
  - TCP 87.4%
- ICMP-paris and UDP-paris to get 96.7%


UDP-paris
15754
TCP
16652
118
513
756
14788
335
595
944
Total AS links
inferred:
18049
ICMP-paris
16662

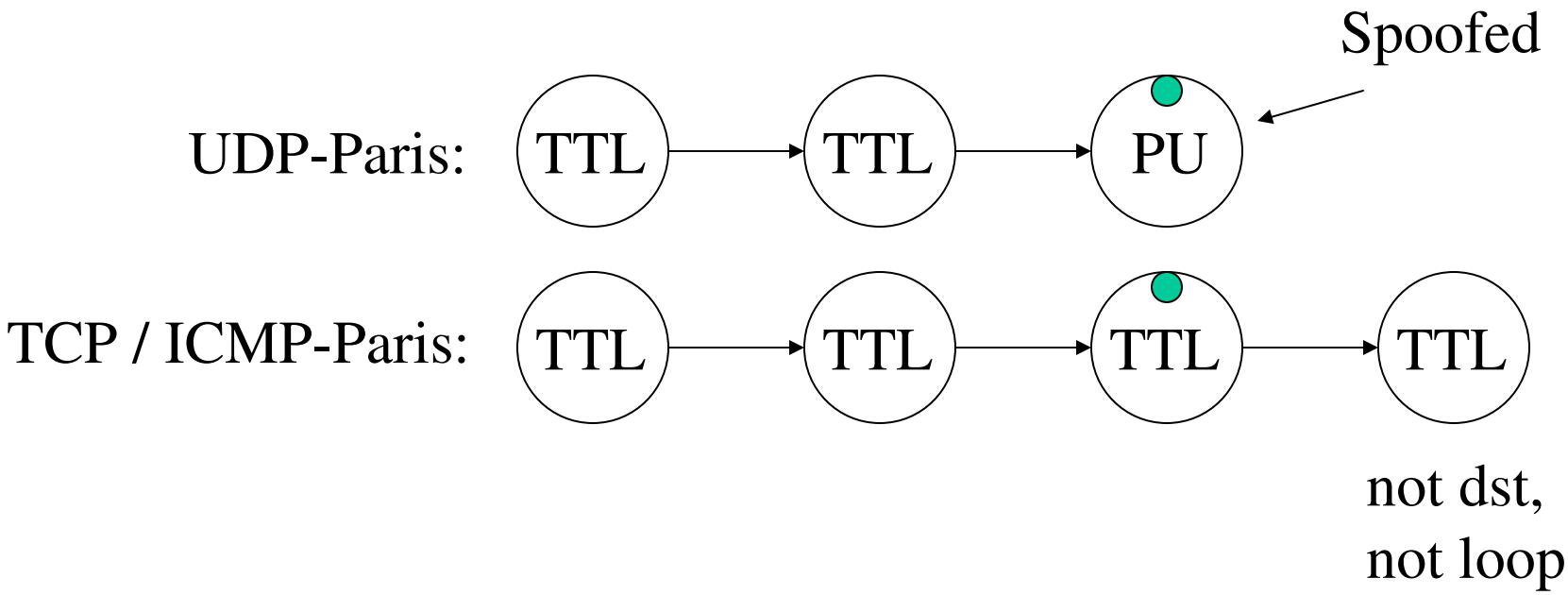
Summary so far

- ICMP-paris reaches most destinations, infers most AS links
  - TCP not far behind
- UDP-paris infers most IP links
  - TCP least
- TCP and ICMP IP paths appear to be the most similar
  - vantage point has an effect, but trend is there
- Firewalls are most commonly two TTLs from the target.

Inferring Spoofed Destinations #1

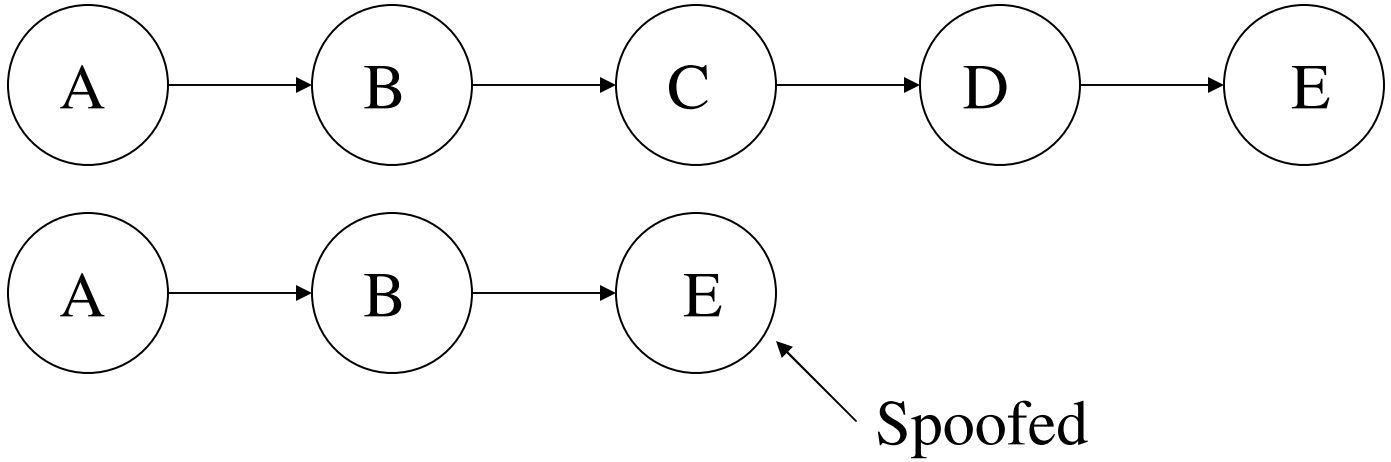
- ICMP destination unreachable: port unreachable
  - RFC 792: Indicated port is not running an active process
  - Source address may vary, but supposed to be from destination
  - Used in alias resolution

Inferring Spoofed Destinations #1



Of 13335 port unreachables for UDP-Paris, 44 were spoofed

Inferring Spoofed Destinations #2



Of 23770 destinations reached with TCP, 212 were spoofed.

162 SYN/ACK
43 RST/ACK

Packet counts

- ICMP-Paris: 6,183,075
- TCP: 6,266,375
- UDP-Paris: 6,362,914 (3% more than ICMP)

Router list

- 2000 IP addresses selected at random
- Previously observed in traceroute path:
  - to send time exceeded message
  - at least one additional ICMP time exceeded past the address, from a different IP

2000 random routers

	reached	icmp unreach	loop	gaplimit
udp	69.2%	5.8%	1.7%	23.3%
udp-paris	70.0%	5.8%	0.8%	23.4%
udp-paris DNS	68.2%	6.0%	0.8%	25.1%
icmp	84.5%	5.9%	1.4%	8.2%
icmp-paris	85.1%	5.8%	0.8%	8.3%
tcp (p 80)	67.1%	6.7%	0.7%	25.6%

Webserver list

- Screen scrape of alexa.com top 500
- Resolved from san-us.ark.caida.org
- 422 IP addresses selected
  - 58 Google ccTLD instances => 4
  - Ebay ccTLD instances
  - Akamai

422 webservers

	reached	icmp unreach	loop	gaplimit
udp	43.0%	4.3%	3.3%	49.4%
udp-paris	43.0%	3.5%	2.4%	51.1%
udp-paris DNS	46.3%	2.6%	2.4%	48.7%
icmp	76.4%	2.4%	2.6%	18.7%
icmp-paris	76.6%	1.9%	2.1%	19.4%
tcp (p 80)	95.5%	nil	2.1%	2.4%

Conclusion

- ICMP-Paris is superior in destinations reached, AS links
- UDP-Paris finds more intra-AS IP links
- Using multiple probe methods improves coverage
  - Also allows integrity of IP paths to be tested
- UDP-Paris DNS bit of a flop