Summary Review Documentation for

“Quantifying Violations of Destination-based Forwarding on the Internet”

Authors: T. Flach, E. Katz-Bassett, R. Govindan

Reviewer #1

Summary: This paper presents a suite of probing techniques that can help identify situations where probes to the same destination from different vantage points may take different forward paths even after they converge, a phenomenon the authors refer to as violations of destination based forwarding. They present a measurement study of the extent and causes of the violations both at the node/link level and the AS level. The measurement results have implications for topology mapping efforts.

Strengths: Understand the extent and causes of these violations is important.

The techniques are intuitive and explained well.

Weaknesses: Results are not surprising.

Techniques have limitations, whose broader implications are unknown.

Comments to authors: While it is useful to quantify the extent of violations, the fact that they happen and that the underlying causes are techniques like MPLS and load balancing are well known. Thus, the results based on the limited set of paths probed are not surprising at all. Some results such as "AS level forks are not caused by load balancing" are entirely obvious.

Perhaps deeper analysis of what portions of the network topology are most afflicted by these problems, what types of links/routers are missed (e.g., core vs edge), extent to which different metrics are impacted by violations (links properties such as latency vs topological structure) and some more concrete, non-trivial thoughts on how to overcome them would have been much more desirable.

The technique you use is new but not too novel as it derives from tricks in prior papers such as [11, 18].

More importantly, the technique you present has key limitations, as it relies on ICMP RR option which can only record a limited number of forward/reverse hops. These limitations cast doubt on the true extent of path violations, and indeed on whether topology mapping efforts are impacted to the extent you claim. You show how many links your mapping approaches miss relative to the set of paths you probed, but this may not be representative of the impact of broader Internet probing. I was a bit disappointed as I wished the paper had an answer for this broader question.

In summary, the question the paper sets out to answer is important, but the analysis needs to be a lot deeper to be interesting and useful.

Reviewer #2

Summary: This paper provides a measurement methodology and accompanying study for assessing how often points in the Internet topology demonstrably forward on more information than just the destination address; i.e., two packets with the same destination might take different next hops. Along with prevalence, the analysis includes assessing how far such deviations continue until the different paths merge.

While I find the topic of only marginal interest given prior work (e.g., Paris traceroute) in this space, I appreciated the solid development here of methodology and results.

Strengths: The technical development in the paper appears carefully executed. The authors pay attention to a lot of considerations that potentially complicate the measurement process.

Weaknesses: I found a fair amount of the technical discussion is quite hard to follow.

Presumably much of this can be remedied with editing, though I worry I might be missing some methodological problems.

The topic is not all that fresh anymore, given prior work that has already identified the issues as well as the main technique/trick used for the measurement itself.

Comments to authors: At the end of the introduction, it would be good to clarify what is meant by a "pathological" violation. Similarly, at the beginning of Section 2, it is worth discussing that "measure a path" is already not necessarily well-defined; the result depends on the measurement procedure and potentially even on its timing.

It is confusing whether RR probing *always* involves spoofing (the top right of page 2 implies this) or only sometimes (as implied by the discussion of the Set R/PL+S dataset).

In the section on "Establishing Fork Causality", I was confused regarding the detection of load balancers. It sounds like nodes get marked as such if they *ever* have divergent next hops, but can such divergence instead reflect policy routing and not load balancing?

Tell us how many PL nodes you selected and how many you then removed due to spoof filters. Did the later mean there were some ASes you could not measure from?

I had trouble following this comment in section 4: "As discussed earlier, it also differs from our results in Table 3, likely because of our use of RR." Why is that the likely explanation?

I was not quite clear on "enabling a consistency check” at the end
Weaknesses: It is not clear whether there are any implications of what is learned from the study. The discussion on the impact of the results on probing tools is useful but fairly obvious.

Comments to authors: Overall, this is a nicely written paper that covers both a measurement technique and a study.

Some presentation comments:

- Is there any reason to believe that nodes may consider traffic type (e.g., next protocol) as part of forwarding decision? This gets to the broader question of what policy-based routing is deployed, which is an issue that is mentioned but not really discussed.

- The description of the technique in Section 2 is a bit hard to follow. It may be possible to improve the figures to clarify the packet exchanges.

- With respect to Figure 4, can you identify any possible reason for the big differences, based on general knowledge about the ISPs?

Section 4 is a bit hard to follow. It might be better to discuss possible solutions right after you have explained the problem.

Reviewer #4

Summary: The authors develop a measurement technique to determine when IP forwarding paths are not entirely destination based. They then employ this technique (along with several other, known techniques) to measure the prevalence of non-destination-based forwarding, as well as categorizing the cause between load balancing, MPLS, and others. The authors use PlanetLab to conduct a world-wide measurement of a variety of ASes.

Strengths: The measurement trick described by the authors is carefully crafted, and appears to work (although with significant noted limitations), and the authors have clearly thought hard about the various idiosyncrasies involved. The measurement study is reasonably large scale, which gives some confidents that the results are representative.

Weaknesses: This area is very well explored. While this particular measurement has not previously been conducted to my knowledge, the results are not particularly surprising, and it is not clear (from this paper, at least) what the implications are for real applications (although the authors do comment on its impact on two other measurement tools).

Comments to authors: The paper is well written, and clearly describes what appears to be a well-crafted study. My overall takeaway, though, is that there is nothing really exciting in what you have discovered, and it is not clear to me what the impact would or should be on either how operators manage their network or applications use it.

Regarding the study, I wonder a bit about its representativeness. There is, of course, the usual concern regarding PL bias, but there are several other factors at play here as well. How many and which routers employ spoofing filters? Does the limited number of hops your tool can expose have any statistical implications on your results? Clearly, for example, it seems that Table 4 is biased since the converged paths are necessarily truncated by your measurement length. You also comment on operators that disable MPLS router exposure: how many do this, and how will it impact your results?

Your results regarding ASes talk about the top few; just how many ASes did you discover that do this? How many did your study traverse?

Reviewer #5

Summary: Some recent measurement tools such as reverse traceroute and Doubletree assume that routers use the same next hop to forward packets destined to the same address. This paper argues that this assumption no longer holds given the use of MPLS and load balancing on the Internet. The authors developed a measurement methodology to quantify violations of destination-based forwarding. The results show a significant fraction of measured paths (10.2%) violate destination based forwarding, and these violations impact the accuracy of path measurement tools.

Strengths: This work uncovers a key weakness of previous measurement tools, and can help improve those tools. The paper is well written, and the measurement work is solid.

Weaknesses: The measurement methodology is not completely novel, and bears much similarity with previous work reverse traceroute.

Comments to authors: I enjoyed reading your paper. Very nice work. Your measurement technique uses IP record route option, IP spoofing, and ICMP echo request/reply. Those are the core techniques used by reverse traceroute. Although your technique has a different goal, it would be nice to acknowledge reverse traceroute for the measurement methodology.

Paths may change during the course of your measurement. How do you rule out the possibility that a routing change caused a path change? Can routing changes explain the fraction of unknown IP/AS forks in your measurements? It would strengthen the paper if you dive deeper into the causes of path forks, especially for AS forks. I am not sure inter-AS MPLS is commonly used in practice. It is puzzling to observe so many AS fork incidents in your data.

Response from the Authors

We thank all reviewers for their constructive feedback, which helped clarifying the important concepts and enhancing the paper with extra content.

A major drawback in our paper was the missing discussion of unclassified forks. To provide more insight, we added a discussion about a couple of interesting violations to our paper.

We acknowledge the concerns, that our measurements might be biased and limited in scope since we rely on RR pings. Our cited
references verified that RR pings are capable of recording a large number of reachable nodes in a ping as long as enough and well distributed vantage points for the measurements are available. Our experiment do not achieve the same coverage since we only consider the first 7 (instead of 8) hops for analysis but we think that this is still enough to analyze a significant number of nodes. In addition to that, we clarified that using traceroutes improved the spread of routes we analyzed.

We clarified the aspect that in this study we only modified the point of injection for a packet (which also affects the source address). As a result, our methodology remained simple, yet powerful enough to reach our goal of showing that violations exist and that a non-trivial number of nodes in the Internet is responsible for them. Consequently, we do not explore violations which could be caused by routers making forwarding decisions based on the port number, protocol type, etc.

Finally, we made smaller modifications and added extra references to other parts which raised specific questions by the reviewers.