How and How Much Traceroute Confuses Our Understanding of Network Paths

Pietro Marchetta[1], Antonio Montieri[2], Valerio Persico[1], and Antonio Pescapé[1,2]
[1]Universitá di Napoli "Federico II" and
[2] NM2 s.r.l.
(Italy)
{pietro.marchetta, valerio.persico, pescape}@unina.it
montieri@nm-2.com

Ítalo Cunha
Universidade Federal de Minas Gerais
(Brazil)
cunha@dcc.ufmg.br

Ethan Katz-Bassett
University of Southern California
(CA, USA)
ethan.kb@usc.edu

***Abstract*—Traceroute is largely considered as the number-one tool when troubleshooting the network, with innumerable applications, such as pinpointing the routing deficiencies or detecting and locating network outages. Previous works have extensively investigated pitfalls and flaws causing the measurements performed with this tool to be inaccurate or incomplete. In this paper, we show how, even in the absence of all these well-investigated pitfalls and flaws, our ability to properly troubleshoot the network with Traceroute is strongly limited. Indeed, by using state-of-the-art alias resolution techniques, we investigate how and how much the IP-level description provided by Traceroute can distort our understanding of the characteristics of Internet paths. We experimentally evaluate the impact on path properties like equal-cost multipaths, loops, routing cycles, load balancing, route prevalence and persistence. Our results confirm that researchers and network operators relying on Traceroute may poorly estimate (i) the number of multiple equal-cost routes to the destination; (ii) the presence of suboptimal routing in the network; (iii) the routing stability.**

I. Introduction

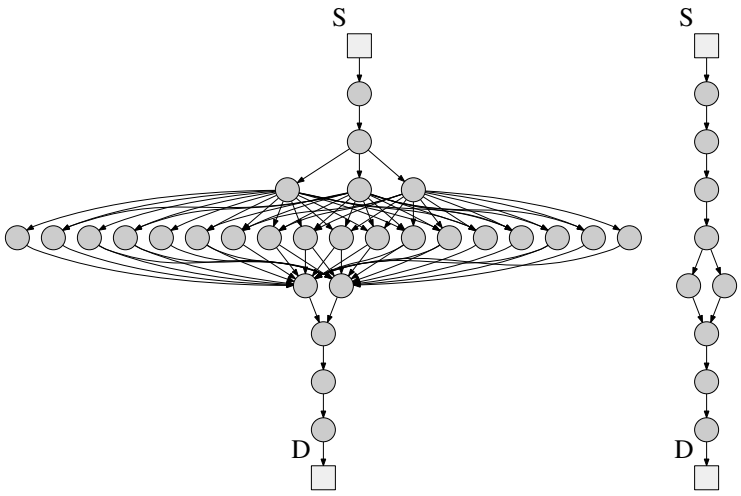
Researchers and operators heavily rely on Traceroute to gather information about the Internet, the *de facto* standard when tracing network paths. Typical aims are locating network failures, troubleshooting performance or routing problems, and reverse engineering the network topology. Unfortunately, Traceroute is also well known to be affected by several pitfalls and flaws challenging researchers and network operators willing to investigate the status of the network. A large body of existing literature has been devoted to investigate and partially solve these issues including anonymous and hidden routers, hidden MPLS tunnels, third-party addresses and middle-boxes [1], [5], [7], [9], [17], [29].

In this paper, we want to increase the awareness related to another very basic Traceroute limitation: even in the absence of all the issues mentioned above, the outcome of Traceroute-based analyses can be still severely biased by the naive IP-level description of the path provided by the tool. Although domain experts well know how Traceroute can only identify interfaces belonging to the traversed routers on the path, to the best of our knowledge, no other study has systematically investigated how and how much this tool can provide a biased or misleading information of the path in terms of traversed devices.

A correct interpretation of Traceroute measurements is complicated by three main factors: (i) routers have—by definition—multiple interfaces, (ii) some routers perform load balancing, and (iii) each router may answer Traceroute by using either the IP address of the probe's incoming interface or of the reply's outgoing interface. In this paper we combine rich IP aliasing information [12], [14], [18] with Paris Traceroute's Multipath Detection Algorithm [1], [29] to show how the interface-level view is not representative of the router-level view from a source to a destination and assess the consequences. An example is reported in Fig. 1: the figure shows the outcome of a real measurement and exposes to what extent the interface-level view of a path traversing routers that perform load-balancing (Fig. 1(a)) is dramatically different than the real router-level view of the same path (Fig. 1(b)). Our experimental results highlight a number of implications opposite to common assumptions: (i) two different interface-level route segments may be identical at the router-level, so a path change observed at the interface level does not imply a change at the router-level; (ii) branched interface-level route segments may overestimate or underestimate the number of branches at the router-level; (iii) a route without loops or cycles at the interface level may expose loops or cycles at the router-level. These results imply that network operators and researchers relying on Traceroute may poorly estimate important characteristics of the measured paths such as the presence of suboptimal routing in the network, the number of routes to the destination, as well as the routing stability.

The remainder of the paper is organized as follows: Sec. II describes the adopted terminology. Sec. III quantifies the discrepancy between interface- and router-level views of a large number of Internet paths. Sec. IV shows how results

978-1-4673-9882-4/16/$31.00



(a) Interface-level. (b) Router-level.

Fig. 1. A real path measured at interface- and router-level. Interface- and router-level may dramatically differ, generating a number of implications opposite to common assumptions.

change when assessing route persistence and prevalence at the interface- and router-level. Finally, Sec. V describes the related works while Sec. VI ends the paper with concluding remarks.

II. Definitions

As proposed in previous works [3], [22], we adopt the term *virtual path* to refer to the connectivity between a monitor and a destination. At any point in time, a virtual path is realized by a *route*. A virtual path changes over time from one route to another as the result of intra- and inter-domain routing changes. Traceroute obtains a sequence of IP addresses belonging to routers that packets traverse on the way to the destination. Normally, each IP address reported by Traceroute can be mapped to a router in the network.[1] We denote *IP-level routes*, the Traceroute measurements, and *router-level routes*, the sequence of routers that IP-level addresses map to. Furthermore, by borrowing the concepts introduced by Augustin et al. [1], a route may contain (i) *loops* if the same IP address or router appears at two *consecutive* hops in the path; or (ii) *cycles* when the same IP address or router appears multiple times in non-consecutive hops.

Finally, load balancing is common practice today (e.g., ECMP [10], [27]), and tools such as Paris Traceroute's Multipath Detection Algorithm (MDA) [29] can identify load balancers and multiple routes to the destination. When routers perform load balancing, we may identify *branched* sequences of IP addresses and routers in a path that we denote, respectively, as *IP-level multiroutes* and *router-level multiroutes*.

[1]Exceptions exist, such as routers exposing private or unroutable IP addresses.

III. Distorted Router-level paths

In this section, we study the gap between the IP-level route provided by Traceroute and the router-level route followed by the packets. By using also examples observed from real measurements (but simplified for ease of exposition), we show that IP-level routes can distort our understanding of characteristics of the router-level routes.

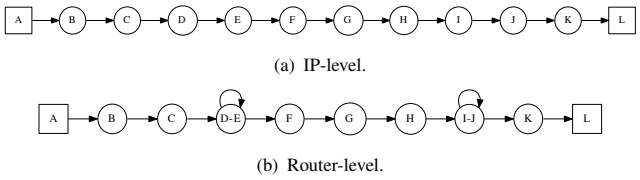
A. Methodology and datasets

We deployed Paris Traceroute with its Multipath Detection Algorithm (MDA) [29] enabled in 90 PlanetLab nodes. We configured each node to trace IP-level routes toward 10 thousand destinations selected at random from a list of 102,404 reachable destinations in different $/16$ prefixes we obtained from the PREDICT project [11]. Our dataset contains more than 900 thousand IP-level (multi)routes and 324,313 IP addresses. The IP addresses span 32,014 different ASes and 98% of the ASes with more than 50 customers [16].

We combine state-of-the-art alias-resolution techniques [13] (techniques glueing addresses belonging to the same router) to build an IP aliasing database and map the IP-level (multi)routes observed with Traceroute into router-level (multi)routes. We build IP aliasing database D_1 running IGMP probing [18] and iffinder [12] on all IPs we observed in our Traceroutes. IGMP probing and iffinder have high accuracy but limited coverage (i.e., the fraction of IPs in the Traceroutes mapped to routers is limited). We also build IP aliasing database D_2 running IGMP probing, iffinder, and MIDAR [14]. Database D_2 trades off accuracy for coverage, including also information collected with MIDAR (note that MIDAR is known to guarantee a low false positive rate, however [14]). We show the number of routers, the number of aliased IPs (i.e., that belong to the routers), and the fraction of IPs in the Traceroutes we can map to a router (coverage) in

TABLE I
IP ALIASING RESOLUTION DATABASES

	Goal	Routers	Aliased IPs	Traceroute Coverage
D_1	Accuracy	41,558	192,790	20.15%
D_2	Coverage	47,260	212,098	26.10%



(a) IP-level.

(b) Router-level.

Fig. 2. Zero-TTL-forwarding devices (invisible to Traceroute) can generate loops visible only at the router-level.

Table I. Note that all quantitative results computed with our datasets are lower-bounds on the real number of occurrences in the Internet due to the limited coverage of the alias-resolution techniques [13].

B. Router-level loops

Router-level routes may have loops that are invisible at the IP-level: we found 40,421 IP-level routes with loops and 43,717 (44,370) router-level routes with loops when using D_1 (D_2), respectively. We detected between 7% and 9% more loops at the router-level. A concrete example of router-level loops that are not visible at IP-level is reported in Fig. 2: while the IP-level shows no repeated addresses, two consecutive IP addresses discovered by Traceroute belong to the same router. In our analysis we found a practical explanation to this phenomenon in routers that forward packets with a time-to-live (TTL) of zero, causing the following router to answer Traceroute twice. Although these devices have been already identified in the past [1] our analysis demonstrates that their frequency in traces has been potentially underestimated. By looking at the IP-level routes indeed, one may uncover routers that forward zero-TTL packets only if the following device answers both probes with the same IP address (so the Traceroute has the same IP address repeated in consecutive hops). However, if the router answers by using different source addresses, Traceroute is not able to give evidence of the presence of these devices.

C. Router-level cycles

Mapping an IP-level route to a router-level route may uncover cycles that are invisible at the IP-level. Overall, we found 12,230 IP-level routes with cycles and 13,284 (13,722) router-level routes with cycles when using D_1 (D_2), respectively: an increase of 8% (11%) compard to the IP-level routes.

An experimentally observed route exposing a cycle only at the router-level is reported in Fig. 3. The IP-level route toward the destination exposes two MPLS tunnels (red-dotted and blue-solid thick lines), does not experience load balancing, and contains no cycles (Fig. 3(a)). However, the router-level route shows a cycle (Fig. 3(b)). Even if packets reach the destination, they waste bandwidth and are delayed traversing hops that do not take them closer to the destination. We note that router D-I, traversed twice, routes the same packet differently each time because the packet reaches the node D-I on different MPLS tunnels (i.e., with different MPLS labels). Manual validation shows that a number of cycles exists where MPLS tunnels cause the same router to be traversed twice. Note that Traceroute cannot identify these cases as router D-I is replying with different addresses. In addition, the positive circumstance in which the traversed MPLS tunnels are explicit (i.e., visible in the Traceroute) does not guarantee identification of these router-level cycles. This shows that Traceroute, a widely-used network diagnostic and troubleshooting tool [6], [26], may fail to identify cases of suboptimal routing.

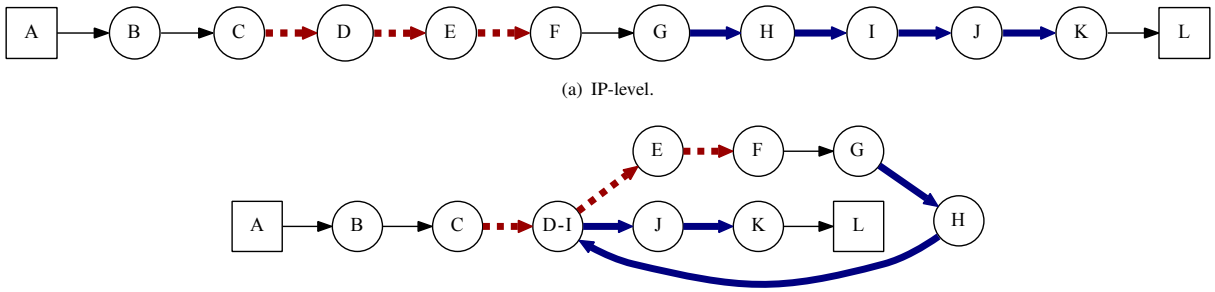
D. Misinterpretation of multiroutes

We discovered an IP-level multiroute can overestimate or underestimate the number of branches in the underlying router-level multiroute. In some cases, an IP-level multiroute may not have any branches at the router level (i.e., be a simple route). Fig. 4 shows an example of an IP-level multiroutes consisting of two routes diverging at the interface C (Fig. 4(a)). These IP-level routes map to two different underlying router-level routes shown in Figs. 4(b) and 4(c).

Load balancing can help improve resource utilization and robustness to outages. When there are multiple branches in a multiroute between a source and a destination, failures in one branch does not prevent communication. If IP alias resolution reveals that the router-level route is as shown in Fig. 4(b), an outage in *any* router prevents end-to-end communication while the IP-level route suggests a much more robust scenario. Conversely, if IP alias resolution reveals that the router-level path is as shown in Fig. 4(c), then communication can proceed when routers D and I experience an outage (assuming routing through E and H) while the IP-level suggests communication would be impossible.

To quantify this effect, we compute the number of branches in IP-level and router-level (multi)routes. About 25% of the 900 thousand monitored virtual paths expose multiroutes at the IP-level (i.e., having more than one branch). Figure 5 shows the distribution of the number of alternative routes in the extracted multiroutes. These results confirm, over a larger dataset, a phenomenon we observed in a very preliminary measurement campaign documented in a previous work [20]: IP-level multiroutes may overestimate the number of alternative routes existing at the router-level between a source and a destination. Indeed, when using the D_1 (D_2) alias-resolution dataset, we observed that about 12% (19%) of IP-level multiroutes turned out to be single not branched routes at the router level; on average, we noticed a reduction of the alternative routes at the router-level by 20% (38%).

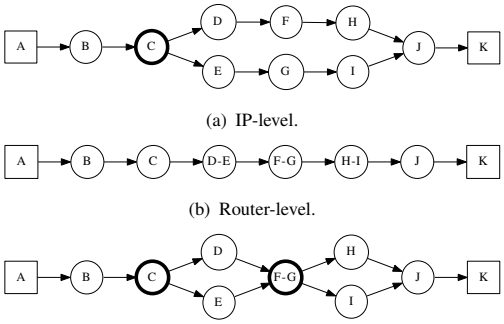
An alternate metric to assess the robustness of IP-level and router-level multiroutes is the *max-width*, defined as the maximum number of different IP addresses (routers) appearing



(a) IP-level.

(b) Router-level.

Fig. 3. A number of experimental evidences show how the IP-level view of the route may not expose suboptimal routing in the network when different MPLS tunnels may traverse the same router and inflate route length. The figure reports one significant example (red-dotted and blue-solid thick lines represent MPLS tunnels identified).



(a) IP-level.

(b) Router-level.

(c) Alternative Router-level.

Fig. 4. The IP-level view of the route may be very different at router-level.

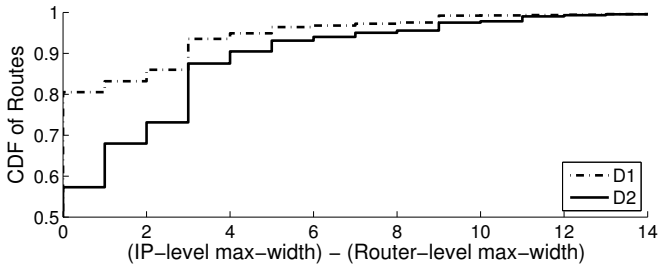


Fig. 6. Max-width reduction.

at the same hop in an IP-level (router-level) route. Figure 6 shows the difference between the max-width of a route when observed at the IP-level and at the router-level. When using D_1 (D_2), we observed that about 17% (33%) of the multiroutes show a smaller max-width at the router-level; the absolute max-width reduction at the router level is on average 0.78 $\pm$ 2.14 (1.54 $\pm$ 2.66).

Another metric we consider is the number of IPs and routers that perform load balancing (or *load balancers*), i.e., that branch out to multiple IPs or routers on the next hop. In particular, we note that IP addresses that balance load across different branches on the IP-level route may not balance load on the underlying router-level route, and vice-versa. For example, IP address C in the IP-level multiroute in Fig. 4(a) is a load balancer; but router C shown in the router-level route in Fig. 4(b) is not. Conversely, router F-G in the router-level multiroute in Fig. 4(c) is a load balancer; but IP addresses F and G in the IP-level multiroute in Fig. 4(a) are not. The number of load balancers decreases by 12% and 22% when we map IP-level multiroutes to the route level using D_1 and D_2, respectively, while the relative fraction of per-packet and per-flow load balancers remains unchanged.

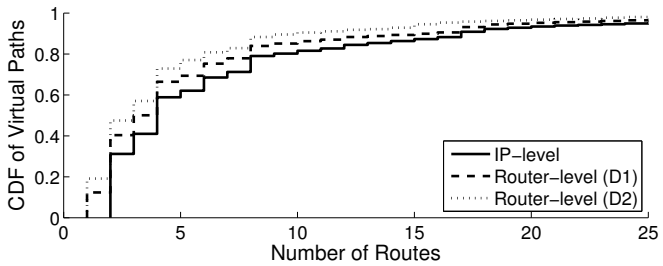


Fig. 5. Multiroutes number.

Tab. II shows the fraction of IPs and routers we identify as load balancers using D_1 and D_2 for different load balancer types. Our analysis shows that, a small but significant (1% in D_1 and 3% in D_2) part of routers that perform load balancing appears to be undetectable at the IP-level. Conversely, around 4% and 6% of IP-level load balancers are not load balancers at the router level.

IV. IP- and Router-level Stability

An important property of Internet paths is *route stability*, i.e., how often routes change and if they are stable over time. Routing stability is typically assessed by (i) relying on Traceroute to repeatedly measure the virtual path over time and (ii) comparing the collected IP-level multiroutes to identify routing changes [3], [22].

In a seminal work on Internet route dynamics, Paxson introduced two distinct views of stability [22]: *route persistence* indicates how long a route is likely to endure before changing; *route prevalence* refers to the overall fraction of time a virtual path is realized by its prevalent route, i.e. the route that most frequently realizes the virtual path.

From the previous section, one would expect router-level stability to be higher than IP-level stability; as the IP-level route may change even if the router-level route remains stable. In this section we quantify this effect.

A. Methodology and datasets

For this analysis, we used DTRACK [4], an active monitoring tool implementing a path sampling method that guarantees a good trade-off between two conflicting needs: (i) monitoring of a large number of virtual paths and (ii) the need for frequent measurements to track path changes. Initially, DTRACK measures all the multiroutes in each monitored virtual path. After this initial mapping phase, DTRACK sends few, targeted detection probes to detect path changes. When a change is detected (by observing an IP address that does not match the last measured multiroute), DTRACK uses Paris Traceroute's MDA [29] to remap the multiroute.[2]

We deployed DTRACK on 73 PlanetLab nodes and configured each node to probe paths toward 1,000 destinations from our hitlist (Sec. III). We configured DTRACK to send 16 probes per second to detect changes and observed a total of 1,289,747 routes in 3 days.

To convert the collected IP-level multiroutes to the router-level, we extended our D_1 IP aliasing dataset to cover IP addresses observed on DTRACK measurements.

As in the previous section, the adopted alias resolution dataset is accurate but also limited in terms of coverage. This conservative approach may underestimate path stability of router-level routes.[3]

B. Route persistence

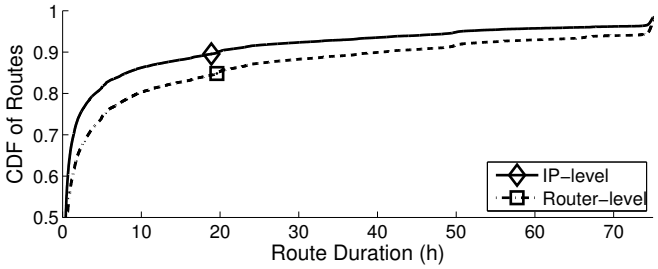
Our goal is to understand if the assessed route persistence differs at IP- and router-level. In order to mitigate the limitations affecting all the studies on route stability we measured each path with a high rate thanks to DTRACK.

[2]We configure DTRACK to probe all paths at the same rate to avoid biasing our measurements toward unstable routes, but still make use of the optimized change detection mechanism.

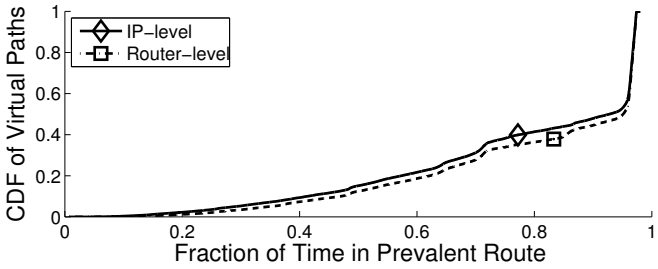
[3]Note we can also overestimate path stability if we miss path changes (e.g., when a path changes from route A to B, then back to A before we detect and remap B).

TABLE II
IP- AND ROUTER-LEVEL LOAD-BALANCERS.

BREAKDOWN	D_1		D_2	
IP-level load balancers	**13,771**	**100%**	**13,771**	**100%**
confirmed at router-level	**13,229**	**96%**	**12,958**	**94%**
per-flow	5,452	41%	4,626	36%
per-packet	7,777	59%	8,332	64%
not conf. at router-level	**542**	**4%**	**813**	**6%**
per-flow	215	40%	286	35%
per-packet	327	60%	527	65%
Router-level balancers	**12,053**	**100%**	**10,751**	**100%**
confirmed at IP-level	**11,907**	**99%**	**10,428**	**97%**
per-flow	4,932	41%	3,654	35%
per-packet	6,975	59%	6,774	65%
not confirmed at IP-level	**146**	**1%**	**323**	**3%**
per-flow	12	8%	99	31%
per-packet	134	92%	224	69%



(a) Route persistence



(b) Route prevalence over 3 days

Fig. 7. Route stability differs at IP- and router-level.

Results are reported in Fig. 7(a) showing the distribution of the route persistence for the monitored paths as observed at the IP- and router-level. In both cases, short-lived routes are predominant: respectively, 74% and 65% of the IP and router-level routes persist for less than 2 hours. On average (median), a route at the IP-level persists for 6.6 (0.4) hours whereas at router-level a route persists for 9.7 (0.6) hours: when a route is observed at router-level instead of simply relying on the IP-level view provided by the state-of-the-art implementations of Traceroute, the persistence of the route is 50% higher on average. This result confirms that even if the sequence of routers traversed to the destination is perfectly the same, the IP-level route provided by Traceroute may erroneously suggest routing instability.

C. Route prevalence

The significant gap between IP- and router-level in terms of route persistence may suggest a similar impact on route prevalence. However, this is not the case as we explain in the following.

Fig. 7(b) reports the distribution of the route prevalence for the monitored virtual paths as perceived at the IP- and router-level. Differently from what observed for the route persistence, the gap between IP- and router-level route prevalence is limited: on average (median), a virtual path stays in its prevalent route for about 78% (92%) of the time at IP-level while about 80% (95%) of the time at router-level. The route prevalence only slightly grows on average by 2.8%.

To understand the reason behind this result, i.e., a great impact on route persistence but only a limited impact on route prevalence, let us consider the simple yet realistic scenario

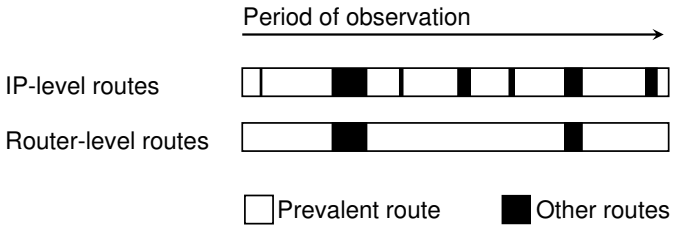


Fig. 8. Route stability for a virtual path.

reported in Fig. 8: the figure depicts the evolution over time of the routes of a virtual path at both IP- and router-level. Over the observation period, the prevalent route at IP-level appears continuously interrupted by other short-lived routes. Most of these short-lived routes, however, disappear at the router-level. In this scenario, the persistence at the router-level of each route significantly grows, i.e. each route endures for a longer period of time. At the same time, the overall fraction of time the virtual path stays in its prevalent route does not significantly grow as well since only very short period of instability disappeared.

V. Related work

Traceroute accuracy. Well known sources of inaccuracy and incompleteness for Traceroute are mainly unresponsive [9] or hidden [5] routers, ICMP rate-limiting and filtering policies, third-party addresses [17] and per-packet or uneven load balancing [29]. In this work, we focus on the existing gap between the Traceroute's outcome and the actual router-level route.

We use Paris Traceroute's Multipath Detection Algorithm (MDA) to measure IP-level multiroutes [1], [29]. MDA systematically varies IP flow-IDs to induce load balancers to forward probes over different branches. It dynamically computes the number of probes and flow-IDs to bound the probability of missing a branch, assuming load balancers split flow-IDs evenly among its available branches. We use MDA with its default configuration, which has been shown to high coverage of the branches [29].

IP alias resolution. To convert the collected IP-level multiroutes to the router-level, we applied alias resolution. Several active alias resolution techniques have been proposed to identify addresses owned by the same router [13]. Basically, they work (i) by inducing the router to reply with an address different than the probed one (Pansiot *et al.* [21], iffinder [12], Palmtree [28]); (ii) by monitoring over time the evolution of the IPID value in the replies collected from different addresses (ally [25], radargun [2] MIDAR [14]); (iii) by wisely crafting IP option-equipped probe packets (Sherry *et al.* [24], Pythia [19]). Alias resolution is primarily used for the reverse engineering of the router-level network topology and is applied only after a large amount of paths have been measured with Traceroute. In this work, we use alias resolution on individual Traceroute measurements.

To the best of our knowledge, only few works have applied alias resolution on single paths measured with Traceroute. Authors in [25] proposed a technique that leverages a pair-wise IPID-based alias resolution procedure, that is applied to the Traceroute measurements, in order to accurately reconstruct ISP router-level topologies. Authors in [15] applied alias resolution on single IP-level routes to enumerate the false links inferred by the classic implementation of Traceroute that does not identify multiroutes. Authors in [8], instead, merged an IPID-based alias resolution technique with the Traceroute mechanism in a new tool called Pamplona Traceroute. Indeed, in all these cases the final goal is an accurate reconstructed router-level topology of the network. Our goal is different; we used alias resolution to evaluate the gap between the IP-level *multi*route provided by Traceroute and the actual router-level *multi*route demonstrating how properties (like route stability or robustness) of the path may change at the two levels.

Route stability. Route stability was first investigated in a seminal work by Vern Paxson in 1997 [22]. Successively, Schwartz *et al.* [23] reappraised route stability at different levels (IP, prefix, city, AS, country), however, not taking into account load-balancing. More recently, Cunha *et al.* [3] proposed FastMapping, a tool including a load balancing aware probing scheme able to monitor a large amount of virtual paths and reassess Paxson's results. None of the works cited above considered the possibility that the route stability may differ at the IP- and router-level: in this paper, instead, we demonstrated that Traceroute may suggest routing instability even if at the router-level the route is perfectly stable over time. This paper extends a previous work providing very preliminary results [20].

VI. Conclusion

Tracing Internet paths is an essential operation to gather knowledge about the network and its status. To this end, researchers and network operators heavily rely on Traceroute. This standard de facto tool is also known to be affected by several issues such as anonymous or hidden routers causing the collected information to be inaccurate and incomplete. In this paper, we experimentally observed how Traceroute—even in the absence of all the issues already investigated in literature—may provide a blurred image of the traversed routers confusing our understanding of key characteristics of the path such as the number of alternative equal-cost routes, the number and location of load balancers or the presence of suboptimal routing. We also experimentally demonstrated how Traceroute may expose unreal short-lived routing instability that disappears when looking the path at the router level. Together with the existing literature, our results suggest even more caution to researchers and network operators relying on this tool for their analysis.

Acknowledgment

This work is partially funded by art. 11 DM 593/2000 for NM2 srl (Italy).

REFERENCES

[1] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. Avoiding traceroute anomalies with paris traceroute. In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, IMC '06, pages 153–158, New York, NY, USA, 2006. ACM.

[2] A. Bender, R. Sherwood, and N. Spring. Fixing Ally's growing pains with velocity modeling. In *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement*, IMC '08, pages 337–342, New York, NY, USA, 2008. ACM.

[3] I. Cunha, R. Teixeira, and C. Diot. Measuring and characterizing end-to-end route dynamics in the presence of load balancing. In *Passive and Active Measurement*, PAM'11, pages 235–244, Berlin, Heidelberg, 2011. Springer-Verlag.

[4] I. Cunha, R. Teixeira, D. Veitch, and C. Diot. Predicting and tracking internet path changes. In *Proceedings of the ACM SIGCOMM 2011 Conference*, SIGCOMM '11, pages 122–133, New York, NY, USA, 2011. ACM.

[5] G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet. Revealing middlebox interference with tracebox. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 1–8, New York, NY, USA, 2013. ACM.

[6] B. Donnet and T. Friedman. Internet topology discovery: a survey. *IEEE Communications Surveys and Tutorials*, 9(4):56–69, 2007.

[7] B. Donnet, M. Luckie, P. Mérindol, and J.-J. Pansiot. Revealing mpls tunnels obscured from traceroute. *SIGCOMM Comput. Commun. Rev.*, 42(2):87–93, Mar. 2012.

[8] S. Garcia-Jimenez, E. Magana, D. Morato, and M. Izal. Pamplona-traceroute: Topology discovery and alias resolution to build router level internet maps. In *Global Information Infrastructure Symposium, 2013*, pages 1–8, Oct 2013.

[9] M. H. Gunes and K. Saraç. Resolving anonymous routers in Internet topology measurement studies. In *INFOCOM*, pages 1076–1084, 2008.

[10] C. Hopps. Rfc 2992: Analysis of an equal-cost multi-path algorithm, 2000.

[11] IP Address Hitlist. PREDICT ID USC-LANDER internet-address-hitlist-it56w-20130917. 2011-05-20 to 2013-10-20. http://www.isi.edu/ant/lander.

[12] K. Keys. iffinder tool. http://www.caida.org/tools/measurement/iffinder/, 2000.

[13] K. Keys. Internet-scale IP alias resolution techniques. *SIGCOMM Comput. Commun. Rev.*, 40(1):50–55, Jan. 2010.

[14] K. Keys, Y. Hyun, M. Luckie, and K. Claffy. Internet-scale IPv4 alias resolution with MIDAR. *IEEE/ACM Transactions on Networking*, 21(2):383–399, Apr. 2013.

[15] M. Luckie, A. Dhamdhere, k. claffy, and D. Murrell. Measured impact of crooked traceroute. *SIGCOMM Comput. Commun. Rev.*, 41(1):14–21, Jan. 2011.

[16] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy. As relationships, customer cones, and validation. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 243–256, New York, NY, USA, 2013. ACM.

[17] P. Marchetta, W. de Donato, and A. Pescapé. Detecting third-party addresses in traceroute traces with IP timestamp option. In *Proceedings of the 14th International Conference on Passive and Active Measurement*, PAM'13, pages 21–30, Berlin, Heidelberg, 2013. Springer-Verlag.

[18] P. Marchetta, P. Mérindol, B. Donnet, A. Pescapé, and J. Pansiot. Topology discovery at the router level: a new hybrid tool targeting ISP networks. *JSAC*, 29(9):1776–1787, 2011.

[19] P. Marchetta, V. Persico, and A. Pescapè. Pythia: Yet another active probing technique for alias resolution. In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, CoNEXT '13, pages 229–234, New York, NY, USA, 2013. ACM.

[20] P. Marchetta, V. Persico, A. Pescapè, and E. Katz-Bassett. Don't trust traceroute (completely). In *Proceedings of the 2013 Workshop on Student Workhop*, CoNEXT Student Workhop '13, pages 5–8, New York, NY, USA, 2013. ACM.

[21] J.-J. Pansiot and D. Grad. On routes and multicast trees in the internet. *SIGCOMM Comput. Commun. Rev.*, 28(1):41–50, Jan. 1998.

[22] V. Paxson. End-to-end routing behavior in the internet. *SIGCOMM Comput. Commun. Rev.*, 36(5):41–56, Oct. 2006.

[23] Y. Schwartz, Y. Shavitt, and U. Weinsberg. On the diversity, stability and symmetry of end-to-end internet routes. In *INFOCOM IEEE Conference on Computer Communications Workshops , 2010*, pages 1–6, March 2010.

[24] J. Sherry, E. K. Bassett, M. Pimenova, H. V. Madhyastha, T. Anderson, and A. Krishnamurthy. Resolving IP aliases with prespecified timestamps. In *Proceedings of the 10th annual conference on Internet measurement*, IMC '10, pages 172–178, New York, NY, USA, 2010. ACM.

[25] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson. Measuring ISP topologies with rocketfuel. *IEEE/ACM Transactions on Networking*, 12(1):2–16, Feb. 2004.

[26] R. Steenbergen. A practical guide to (correctly) troubleshooting with traceroute. *North American Network Operators Group*, pages 1–49, 2009.

[27] D. Thaler and C. Hopps. Rfc 2991, 2000.

[28] M. E. Tozal and K. Sarac. Palmtree: An IP alias resolution algorithm with linear probing complexity. *Computer Communications*, 34(5):658 – 669, 2011. Special Issue: Complex Networks.

[29] D. Veitch, B. Augustin, T. Friedman, and R. Teixeira. Failure Control in Multipath Route Tracing. In *IEEE INFOCOM*, 2009.