ACM SRC - GRAND FINAL REPORT

Candidate: Pietro Marchetta,
Institute: University of Napoli "Federico II".
Email: pietro.marchetta@unina.it
Website: http://wpage.unina.it/pietro.marchetta
Advisor: prof. Antonio Pescapè

(1) Problem and Motivation

A deep and exhaustive understanding of Internet is essential to study and guide a positive evolution of such incredibly complex and ever-changing ecosystem. In this context, Internet measurements have played and play an essential role. One of most used Internet measurement technique is Traceroute [1]. Traceroute injects into the network packets crafted with an increasing value of the Time-to-Live (TTL) field in order to solicit ICMP Time Exceed error messages from the network-layer devices located along the path toward the destination. By simply extracting the source addresses of the collected ICMP error messages, the Traceroute originator is able to reconstruct the network path toward the destination as a sequence of IP addresses, one for each router traversed toward the targeted destination. Traceroute is widely adopted in both industry and research: on the one hand, Traceroute is used by network operators to troubleshoot network performance problems like persistent or transient routing anomalies [2]. On the other hand, researchers make an extensive use of this tool to infer network topological properties [3-19], and, more in general, in active monitoring approaches for anomaly detection [20-22], performance analysis [23-24], geolocation [25-26], and analysis of Internet censorship [27, 28].

Unfortunately, despite all these applications and improvements, it has been profusely demonstrated how Traceroute suffers from several limitations [29–32] and, accordingly, measurements based on Traceroute may result inaccurate, misleading or incomplete: (a.) load balancing routers split the traffic issued toward the same destination over multiple equal cost paths and cause Traceroute to infer false links and bogus network loops; (b.) middleboxes (NAT, Firewall, etc.) applying filtering policies may prevent Traceroute to reach the destination; (c.) anonymous routers do not reply to Traceroute causing the collected traces to be incomplete; (d.) ICMP rate limiting policies may prevent Traceroute to collect all the required replies from the network.

All these limitations have been profusely investigated and partially solved [29–32]. However, other strong and often largely ignored limitations still exist. The so-called **third-party addresses** [34-35], i.e. addresses associated to interfaces which are not actually traversed by the packets sent toward the Traceroute destination, may induce the inference of false Autonomous System (AS) level links when Traceroute is used to overcome the incompleteness [36] of BGP-derived AS-level topologies [5, 37-38]. While an anonymous router reveals at least its presence as non responsive hop, an even worse limitation is represented by **hidden routers**. A hidden router does not manage the TTL and, as consequence, it results totally invisible to Traceroute [39]. Middleboxes and certain implementations of multi-protocol label switching may act as hidden routers. Hidden routers cause missing nodes and incorrect link inferences. Both hidden routers and third-party addresses may have a great impact on the Internet topological properties assessed today. In this scenario, several open questions remain: how many hidden routers are currently deployed in Internet? What is the magnitude of the third-party address phenomenon? What is the actual accuracy of a Traceroute-derived Internet topology? Are all the efforts to model the Internet topology (for advanced studies such as simulations of the Internet) based on empirical observations biased or compromised or the Traceroute applications impacted?

Our contribution consists of a set of innovative active probing techniques able to investigate the magnitude of the third-party address and hidden router phenomena: our techniques and large-scale experimental campaigns demonstrate how these Traceroute limitations are not uncommon in Internet.

(2) Background and Related Work

In this section, we deepen third-party addresses and hidden routers and provide a background on the scientific papers that have considered such Traceroute limitations.

Third-party addresses. The RFC1812 states that the source address of an ICMP error packet should correspond to the outgoing interface of the ICMP reply, rather than the interface on which the packet triggering the error was received [34]. This behavior can cause a Traceroute IP path to include addresses associated to interfaces not included in the path actually traversed.

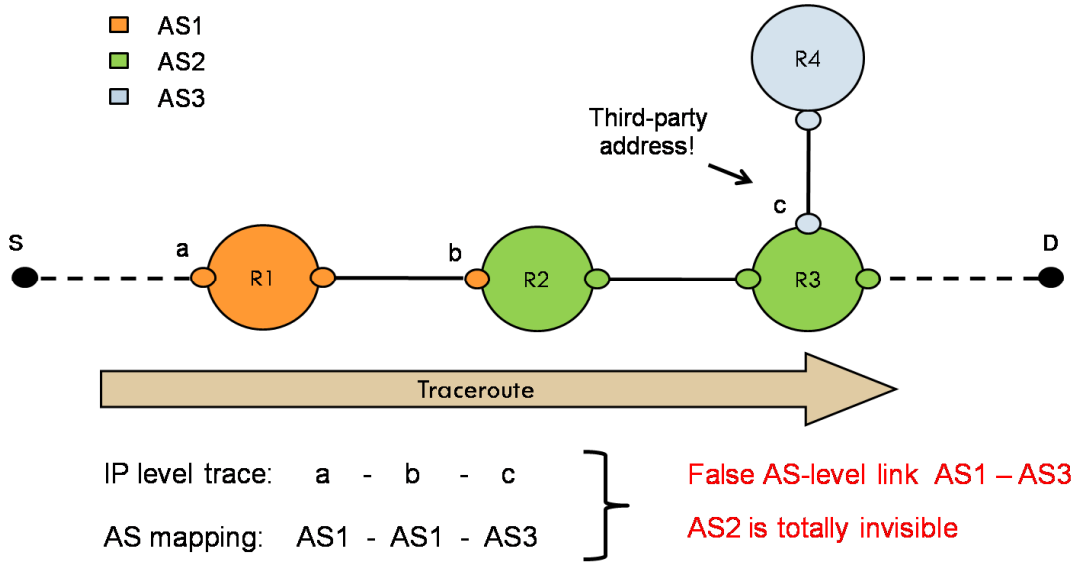
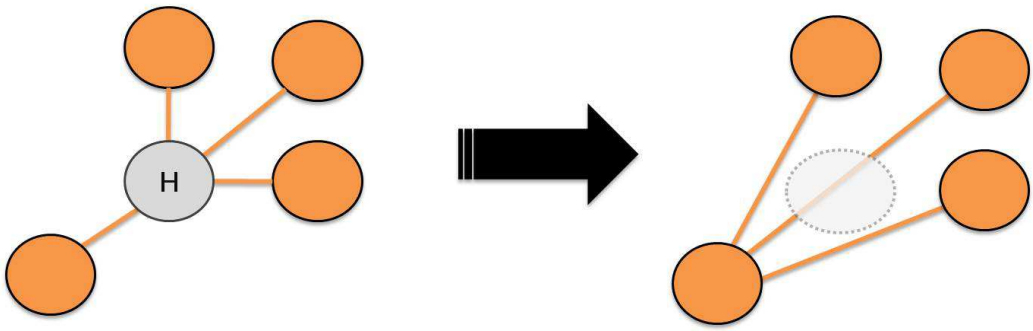


Fig. 1: TP addresses may induce the inference of false AS links

For instance, the trace from S to D in Fig. 1 contains the sequence (a; b; c) of IP addresses (hereafter IPs), where a and b are associated to the incoming interfaces of routers A and B respectively, and c is the interface used by router C to send ICMP replies to the Traceroute originator. The IP c is a third-party address since it is associated in this specific trace to an interface not effectively traversed by the packets sent from S to D. The occurrence of third-party addresses can have a significant impact on some Traceroute applications. The major impact is related to the inference of AS-level links from Traceroute traces: as shown in previous works [34-35], third-party addresses may cause the inference of false AS links. Consider again Fig. 1: if the IP address b Fig. 1: third-party addresses inducing the inference of false AS links belongs to ASx, and c belongs to the ASz addressing space, then the IP-to-AS mapping of the trace will induce the inference of a false AS link, i.e. ASx-ASz. Note also how the third-party address hides the ASy which, tough traversed, does not appear in the mapped AS-level trace. While several other causes may impact the accuracy of AS links derived from Traceroute such as unmapped hops, Internet exchange points (IXPs), multi-origin AS prefixes, and siblings AS, third-party addresses (when shared between peering AS neighbors) were recently defined by Zhang et al. [35] as “the last and the most difficult cause to be inferred” and as “a huge obstruction towards the accuracy of Traceroute measurements”. Several works, by using heuristic methods,

tried to deal with such issues with different objectives: to explain the mismatches between BGP- and Traceroute derived AS paths [5, 35], or to complement the AS-level topology inferred from BGP repositories [5, 37, 38]. However, to the best of our knowledge, only two works tried to isolate and study the phenomenon of third-party addresses in order to quantify their impact, achieving different conclusions. By adopting a heuristic method based on IP-to-AS mapped Traceroute traces, Hyun et al. [34] conclude that third-party addresses mostly appear at the border of multi-homed ASes and cannot be a significant source of AS map distortion. On the other hand, by using precomputed AS-level graphs and pre-acquired knowledge about routers interfaces, Zhang et al. [35] conclude that third-party addresses cause 60% of mismatches between BGP- and Traceroute-derived AS paths, where mismatches affect from 12% to 37% of the paths depending on the vantage point.
To shed light on this controversial topic, we have developed an active probing technique able to classify the addresses reported by Traceroute as third-party addresses or not. The proposed approach allowed to demonstrate how third-party addresses are very common supporting the conclusions drawn by Zhang et al. [35].

Hidden routers. Fig. 2 shows the hidden router impact on the topology as inferred with Traceroute. The inferred topology is both incomplete and inaccurate: nodes and links of the actual topology are not revealed while the inferred links are false. Despite such a huge potential impact, hidden routers have been often ignored. To the best of our knowledge, only two papers (proposed by the same research team) have partially tackled the problem: Sherwood *et al.* [39-40] proposed a solution based on a novel Traceroute enhanced by the Record Route (RR) option to identify load balancers, anonymous routers, and possibly, hidden routers. The injected probes collect along the path additional IP addresses in the RR option. They used the disjunctive logic programming to merge the addresses stored in the RR option and the Traceroute data uncovering 329 hidden routers (0.3% of all the discovered devices). Unfortunately, aligning RR paths and Traceroute paths is an extremely computationally expensive process [12] and the proposed technique can be applied on Internet paths no longer than 9 hops, being thus strongly limited.



(a) Actual Topology (b) Inferred Topology

Fig. 2: Hidden router impact on inferred topology.

To tackle this problem, we have developed a Traceroute enhanced by the Timestamp option in order to detect hidden routers in Traceroute trace. Compared to the proposals in literature, our technique is very light and can be profitably applied on paths up to 24 hops. Such higher applicability allows us to demonstrate how hidden routers are not so uncommon as previously supposed and cannot be ignored any more.

(3) Approach and Uniqueness

The active probing techniques developed to investigate hidden routers and third-party addresses are based on different variants of the IP Timestamp option as reported in the following.

Third-party addresses [42-43]. The proposed technique is based on the IP prespecified timestamp option that allows to *prespecify* in a single packet up to four IP addresses from which a timestamp is requested. Thanks to a large-scale measurement campaign [41], we observed that most routers (including Cisco devices), when processing such option, insert one timestamp only if the packet probe passes through the interface associated to the prespecified address. Accordingly, to state if an IP address X discovered by Traceroute toward a destination D is a third-party address or not, the technique sends a packet probe toward D prespecifying X: if the router owning X provides its own timestamp, we conclude that X is on the true IP path, otherwise X is a third-party address. The adopted technique is much more complex to deal with the heterogeneity of the Internet routers. Interested readers may refer to [42-43]. Differently from most previous works, our technique does not rely on the information provided by BGP or pre-collected information about the topology. To the best of our knowledge, this is the first active probing technique in literature able to identify third-party addresses in Traceroute trace.

Hidden routers [44]. In order to detect hidden routers in Traceroute trace, we developed an enhanced version of Traceroute: the packet probes injected into the network are equipped with the basic variant of the Timestamp IP option. In this way, each traversed router along the path is requested to manage the Timestamp option. The key idea used to detect hidden routers is based on the comparison between the number of routers managing the Timestamp option and those decrementing the TTL: there is an evidence of hidden routers on the path every time the hops managing the TS option are more than those decrementing the TTL. This basic principle can be profitably applied to any portion of the Trace: this allows not only to detect hidden routers but also to locate them along the path. While this simple idea represents the starting point for the development of a more sophisticated multi-step approach (interested readers may refer to [44]), the resulting active probing technique represents the first technique in literature specifically designed to investigate hidden routers in Internet.

Part of the novelty of the presented techniques comes from the use of IP options. The IP optional headers represent today a controversial topic for the community. Most researchers have simply ignored such a powerful mechanism for long time, mainly due to anecdotal evidences about the filtering of packet probes carrying IP options somehow confirmed by small-scale experimental analysis. Our works aims at also encouraging a wider discussion about the IP options and their practical utility.

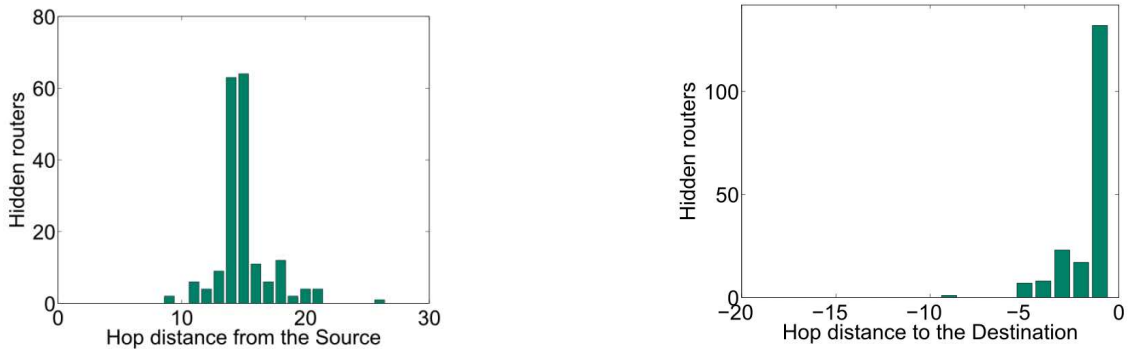
(4) Results and Contributions

In this section, we briefly describe the main findings achieved thanks to the basic mechanisms described in the previous section.

Third-party addresses [42-43]. Thanks to a large scale measurements campaign targeting more than 19K distinct AS collecting more than 12M of Traceroute traces, we observed a general trend: most Traceroute traces contain many more third-party addresses than addresses on the true path. In other words, most of the intermediate routers encountered along a path reply to Traceroute by using an interface different from the ones actually traversed by the packets sent to the targeted destination. In particular, we observed how the same IP address may be a third-party address or not depending on the (i) originating node and (ii) the targeted destination, essentially due to both inter- and intra-domain routing. From the dataset, we extracted about 34K AS-level links: 17% of AS-level links are affected by third-party addresses. Such surprisingly high value confirmed the conclusion drawn by Zhang et al. [35] on the severity of this phenomenon. Our technique allowed also to explain why such conclusion conflicts with the one achieved by Hyun et al [34]: on our dataset, their heuristic method was able to discover only 1.5% of the third-party addresses recognized by our technique essentially due the intrinsic limited information provided by the public BGP repositories. Such findings raise doubts about the real possibility of using Traceroute to study the AS-level topology. For example, the high number of peer-to-peer AS-level relations discovered thanks to Traceroute-based

experimental campaigns specifically designed to travel across Internet Exchange Points [37-38] raised great interest from the community but it could be largely affected by third-party addresses.

Hidden routers [44]. The evaluation of the proposed methods consisted in a large-scale measurement campaign targeting representative addresses in 25K distinct ASes. Applying the mechanism described in the previous section allowed to detect hidden routers in 6% of the considered Traceroute trace. Taking into account how the phenomenon has been largely ignored, such a value appears surprisingly high and demonstrates that hidden routers exists and are not uncommon: Internet topologies inferred through classic topology discovery approaches based on Traceroute may be heavily affect by hidden routers. For those hidden routers that have been exactly located, we computed the hop distance from the Traceroute originator (Fig. 3(a)) and destination (Fig. 3(b)): 70% of these devices are just one hop far from the destination. Such result seems confirming how a portion of the detected hidden routers could be middleboxes located in the proximity of the targeted destination: indeed, some middleboxes such as the Cisco firewall Adaptive Security Appliance [45] do not decrement the TTL by default. Interested readers may find many more details and results in [44].



(a) Relative to the source (b) Relative to the destination

Fig. 3: Positions of hidden routers exactly located.

The proposed innovative techniques exploit IP options to investigate often ignored limitations of Traceroute. Our results demonstrate how such limitations represent a strong source of inaccuracy for Traceroute-based Internet measurements and cannot be neglected any more. Our contribution represents the starting point for the investigation of the impact of these limitations on all those results achieved through Traceroute-based measurements such as the Internet topological properties.

Bibliography

[1] V. Jacobson, "traceroute," Feb. 1989, ftp://ftp.ee.lbl.gov/traceroute.tar.gz..
[2] R. A. Steenbergen, "A practical guide to (correctly) troubleshooting with traceroute" North American Network Operators Group 2009.
[3] Y. Shavitt and E. Shir, "DIMES: Let the Internet measure itself," ACM SIGCOMM CCR, 2005.
[4] KC Claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov, "Internet mapping: from art to science," CATCH 2009.
[5] K. Chen, D. R. Choffnes, R. Potharaju, Y. Chen, F. E. Bustamante, D. Pei, Y. Zhao, "Where the sidewalk ends: Extending the internet AS graph using traceroutes from P2P users," ACM CoNEXT, Dec. 2009.
[6] B. Donnet, T. Friedman, "Internet topology discovery: A survey," Communications Surveys & Tutorials, IEEE, 9(4):56-69, 2007.
[7] M. Luckie, "Scamper: a scalable and extensible packet probet for active measurement of the Internet," ACM SIGCOMM IMC 2010.
[8] H. Burch, B. Cheswick, "Internet Mapping Project," http://cm.bell-labs.com/who/ches/map.
[9] k. cla_y, T. Monk, D. Mc Robb, "Internet Tomography," Nature Magazine, Web Matters.
[10] Hal Burch, Bill Cheswick, "Mapping the Internet," IEEE Computer, Apr. 1999, vol. 32.
[11] R. Govindan, H. Tangmunarunkit, "Heuristics for Internet Map Discovery," IEEE INFOCOM 2000, Tel Aviv, Israel, 2000.
[12] K. Keys, "Internet-Scale IP Alias Resolution Techniques," ACM SIGCOMM CCR, vol. 40, no. 1, Jan 2010.

[13] N. Spring, R. Mahajan, D. Wetherall, "Measuring ISP Topologies with Rocketfuel," ACM SIGCOMM 2002, Pittsburg, 2002.
[14] R. Bush, J. Hiebert, O. Maennel, M. Roughan, S. Uhlig, "Testing the reachability of (new) address space," INM SIGCOMM Workshop, 2007.
[15] R. Beverly, A. Berger, G. G. Xie, "Primitives for active internet topology mapping: toward high-frequency characterization," ACM SIGCOMM IMC 2010.
[16] B. Augustin, T. Friedman, R. Teixeira, "Measuring load-balanced paths in the Internet," pp. 149-160, ACM SIGCOMM IMC 2007.
[17] Z. M. Mao, D. Johnson, J. Rexford, J. Wang, and R. H. Katz, "Scalable and accurate identification of AS-level forwarding paths," IEEE INFOCOM 2004.
[18] P. Marchetta, P. Mérindol, B. Donnet, A. Pescapè, J-J Pansiot, "Topology Discovery at the Router Level: A New Hybrid Tool Targeting ISP Networks," JSAC 2011.
[19] P. Marchetta, P. Mèrindol, B. Donnet, A. Pescapè, and J. Pansiot, "Quantifying and Mitigating IGMP Filtering in Topology Discovery," in IEEE GLOBECOM, 2012.
[20] E. Katz-Bassett, H. V. Madhyastha, J. P. John, A. Krishnamurthy, "Studying black holes in the Internet with Hubble," NSDI, 2008.
[21] M. Zhang, C. Zhang, V. Pai, L. Peterson, and R. Wang, "PlanetSeer: Internet path failure monitoring and characterization in wide-area services," OSDI, 2004.
[22] Y.Zhang, Z.M.Mao, M.Zhang, "Effective diagnosis of routing disruptions from end systems," NSDI, 2008.
[23] R. Mahajan, M. Zhang, L. Poole, V. Pai, "Uncovering performance differences among backbone ISPs with Netdiff," NSDI, 2008.
[24] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani, "iPlane: An information plane for distributed services," OSDI, 2006.
[25] B. Gueye, A. Ziviani, M. Crovella, S. Fdida. "Constraint-based geolocation of Internet hosts," IEEE/ACM Transactions on Networking, 2006.
[26] B. Wong, I. Stoyanov, E. G. Sirer, "Octant: A comprehensive framework for the geolocalization of Internet hosts," NSDI, 2007.
[27] J. Karlin, S. Forrest, and J. Rexford. Nation-state routing: Censorship, wiretapping, and BGP. arXiv 2009
[28] X. Xu, Z. M. Mao, and J. A. Halderman. Internet censorship in china: where does the filtering occur? PAM 2011
[29] M. Gunes and K. Sarac. Resolving anonymous routers in internet topology measurement studies. IEEE INFOCOM 2008
[30] X. Jin, W. Yiu, S. Chan, and Y. Wang, "Network topology inference based on end-to-end measurements," JSAC, vol. 24, no. 12, 2006.
[31] B. Yao, R. Viswanathan, F. Chang, and D. Waddington, "Topology inference in the presence of anonymous routers" IEEE INFOCOM 2003.
[32] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, R. Teixeira, "Avoiding traceroute anomalies with Paris traceroute," ACM SIGCOMM IMC 2006.
[33] M. Luckie, A. Dhamdhere, K.C. Claffy, D. Murrell, "Measured impact of crooked traceroute," ACM SIGCOMM CCR 41, 1 14-21.
[34] Y. Hyun, A. Broido, and K.C. Claffy. On third-party addresses in traceroute paths. PAM, 2003.
[35] Y. Zhang, R. Oliveira, Y. Wang, S. Su, B. Zhang, J. Bi, H. Zhang, and L. Zhang. A framework to quantify the pitfalls of using traceroute in as-level topology measurement. IEEE JSAC, 2011.
[36] E. Gregori, A. Improta, L. Lenzini, L. Rossi, and L. Sani. On the incompleteness of the AS-level graph: a novel methodology for BGP route collector placement. ACM SIGCOMM IMC, 2012.
[37] B. Augustin, B. Krishnamurthy, and W. Willinger. IXPs: mapped? In ACM SIGCOMM IMC, 2009.
[38] Y. He, G. Siganos, M. Faloutsos, and S. Krishnamurthy. Lord of the links: a framework for discovering missing links in the Internet topology. IEEE/ACM Transactions on Networking, 2009.
[39] R. Sherwood, A. Bender, and N. Spring, "Discarte: a disjunctive internet cartographer," ACM SIGCOMM CCR, 2008.
[40] R. Sherwood and N. Spring, "Touring the internet in a tcp sidecar," ACM SIGCOMM IMC 2006.
[41] W. de Donato, P. Marchetta, and A. Pescapé. A hands-on look at active probing using the ip prespecified timestamp option. PAM 2012.
[42] P. Marchetta, W. de Donato, and A. Pescapé. Detecting third-party addresses in Traceroute ip paths. In Proc. ACM SIGCOMM, 2012. BEST POSTER.
[43] P. Marchetta, W. de Donato, and A. Pescapé. Detecting Third-party Addresses in Traceroute Traces with IP Timestamp Option. PAM 2013.
[44] P. Marchetta and A. Pescapè. DRAGO: Detecting, Quantifying and Locating Hidden Routers in Traceroute IP Paths. Global Internet Symposium 2013.
[45] Cisco Systems, "Asa/pix/fwsm: Handling ICMP pings and traceroute." http://www.cisco.com/image/gif/paws/15246/31.pdf.