Validity of Router Responses for IP Aliases Resolution

Santiago Garcia-Jimenez, Eduardo Magaña, Mikel Izal, Daniel Morató

Validity of router responses for IP aliases resolution

Santiago Garcia-Jimenez, Eduardo Magaña, Mikel Izal and Daniel Morató

Public University of Navarre, Campus Arrosadia, 31006 Pamplona, Spain
santiago.garcia@unavarra.es

Abstract. In order to obtain close-to-reality Internet maps, IP aliases resolution allows identifying IP addresses belonging to the same router. Mainly, active probing is used for IP aliases resolution following direct and indirect schemes. Also, different types of probe packets are used (ICMP, UDP, etc.) focusing on different header fields and characteristics of IP and higher layers. Responsiveness of routers is different not only in the number of response packets received, but also in the validity of those packets to be used in IP aliases identification. Therefore, specific behavior of routers generating those response packets can decide the success or failure of specific IP aliases resolution methods. In this paper, an in-depth analysis of router behaviors is provided considering not only router responsiveness, but also the validity of those responses to be used in IP aliases resolution. Our results show that although responsiveness is better for indirect probing, direct probing with ICMP Echo probe packets and IPID-based behavior provide the best identification ratio for IP aliases resolution.

Keywords: IP aliases resolution, router responsiveness, active probing, direct and indirect probing

1 Introduction

Several attempts have been put forward over the last decade to obtain an Internet map, like ARK [1], iPlane [2], Skitter [3] and DIMES [4]. They are mostly based on the traceroute tool, launched periodically between a high number of vantage points (controllable nodes that generate probe packets). This generates a graph composed by nodes (IP addresses) and links between nodes (adjacencies obtained from traceroute paths).

A special case of Internet map is the one in which the nodes in the graph are routers instead of IP addresses. This is a router-level Internet map where the graph links represent the connectivity between interfaces of different routers. Those router-level Internet maps are useful in network simulation, P2P protocol optimization, improvement of routing protocols, geolocation of IP addresses and many other applications.

This topology information is not provided by almost any Internet carrier or Autonomous System. The reasons are related to security and reluctance to share

network information with competing ISPs. This means that router-level Internet maps have to be inferred from passive or active monitoring schemes. In passive monitoring, traffic at specific network points is captured and analyzed looking for some specific information. In active monitoring, probe packets are sent to the network infrastructure, and the responses are analyzed to discover network characteristics. In topology discovery, mainly active monitoring is used because it allows discovering remote networks from a limited number of vantage points.

The traceroute tool discovers the IP addresses of the routers in the path to the target IP address. When probing a high number of target IP addresses from different vantage points, an approximation of an Internet map can be provided. To construct a router-level Internet map, IP addresses of the same router have to be aggregated. Those IP addresses are called *IP aliases* and the process of aggregation is called *IP aliases resolution* [5]. Therefore, two phases have to be performed: IP addresses discovery and IP aliases resolution. Some projects like Rocketfuel [5] and, more recently, MIDAR [6] perform IP aliases resolution at large scale.

IP aliases resolution techniques are also based mainly on active probing and, therefore, it is important to select the right type of probe packet and measurement procedure to obtain the highest number of responses possible. The percentage of response packets over the number of probe packets is called *responsiveness* [7]. However, the responses, depending on their characteristics, could be useless to perform IP aliases resolution and, therefore, the responsiveness indicator is not enough to determine the final results from the IP aliases resolution procedure. Router responsiveness to active probing was analyzed in [7] and an evaluation of performance for several IP aliases resolution schemes is available in [8]. However, there are not studies about the *validity* of this responsiveness: this means the ratio of responses that really are useful to apply IP aliases resolution techniques. Validity of responses will depend on the great variety of router implementations and configurations in Internet. This paper focuses on this router behavior and it will identify those active monitoring schemes that provide the best ratios of valid responses in IP aliases resolution. In fact, it will be shown that strategies with more responsiveness will not always provide the best identification ratios in IP aliases resolution.

The rest of the paper is organized as follows. Section 2 presents different schemes of IP aliases resolution techniques in the state of the art that will be evaluated in the paper. In section 3, the network scenario used in the evaluation is presented. Router behaviors related to IP aliases resolution are presented in section 4. Section 5 presents the evaluation of IP aliases resolution based on the types of routers behaviors. Finally, conclusions are presented.

2 Related work

There are different possibilities of probing schemes that can be used by IP aliases resolution techniques. These schemes can be classified depending on multiple

aspects: the need of probe traffic, the directiveness of the measurement, the type of probe packets and the type of router behavior.

First, depending on the necessity of sending probe packets, IP aliases resolutions schemes can be classified in active and inference-based. Active probing techniques are based on sending probing packets to the routers and analyzing the responses. They provide the best performance in IP aliases resolution [9], but they are intrusive and they need to be controlled in order not to get confused with network scanning or attacks. Inference techniques are the other possibility. They try to deduce aliases information by analyzing data extracted from traceroute paths or from out-of-band measurements such as checking similarities of DNS names in router interfaces. We will focus in active probing techniques.

Second, looking at the measurement directiveness, indirect methods send the probe packet to different IP addresses than the target IP addresses of the aliases resolution technique. Traceroute tool is an example of indirect method for network discovery. In direct methods, the probe packet is addressed at the target IP interface of the aliases resolution technique. Sending ICMP Echo Request packets is an example of direct method. As stated in [7], router responsiveness is greater in indirect methods than in direct ones. However, the validity of those responses to be used in IP aliases techniques was not evaluated in that work. We will perform an analysis of validity of probe responses in section 4.

Third, several types of probe packets are used in IP aliases resolution techniques: UDP, TCP, ICMP Echo Request and ICMP Timestamp Request. As stated in [7], ICMP Echo Request provides the best responsiveness results. The validity of those responses is analyzed in section 4.

Finally, IP aliases resolution techniques are based on different peculiarities of router behaviors. Routers fill up some fields of response packets following specific patterns that can be used to identify aliases. The main behaviors used in IP aliases resolution techniques are IPID-based, Timestamp-based and Source IP-based.

The IPID is the identifier field in the IP header. This IPID is originally used in the procedures of fragmentation and reassembly of IP packets. Typical TCP/IP implementations use a counter which is incremented by one for each packet generated (not forwarded) by the router, independently of destination, protocol or service. Therefore, several packets received from the same router and near in time will have close IPID values, following an incremental pattern. Probing different IP addresses of the same router simultaneously, an incremental sequence of IPIDs is obtained. This behavior was used first by the Ally technique [5], with 3 UDP probe packets being sent and allowing an IPID offset of 200 IPIDs between the first and the third response in order to consider both IP addresses to belong to the same router.

Timestamp-based behavior uses the prespecified timestamp option in the IP header that allows selecting up to four IP addresses and receiving the timestamps from those IP addresses. Typical implementations provide milliseconds timestamps that allow checking if two IP addresses are aliases (they will have

the same timestamp). It was used for the first time in the Prespecified Timestamp technique with direct ICMP probe packets [10].

Source IP-based behavior uses special probe packets to generate ICMP Error response packets from the target routers. Probe packets are usually UDP packets sent to a random port at the target IP address. The corresponding router answers with an ICMP Error Port Unreachable packet whose IP address can be different from the destination IP address of the probe packet. In fact, the source IP address of the response is usually chosen from the interface with shortest path to the destination. Therefore, probing different IP addresses from the same vantage point, they will be aliases if the response packets have the same source IP address. This behavior was used for the first time in the Mercator technique [11], using UDP probe packets.

Some of the most commonly used techniques for IP aliases resolution, besides those previously described, are presented below. TraceNet [12] uses direct/indirect probing, source-IP based behavior and ICMP/UDP probe packets. It infers the subnetworks, and it tries to obtain aliases at the same time that the traceroute is performed. It is based on distance to provoke ICMP Error TTL exceeded responses.

Palmtree [13] uses direct probing, source-IP based behavior and ICMP/UDP probe packets sent to inferred /30 and /31 subnetworks. Those probe packets have bounded TTL in order to obtain ICMP Error TTL exceeded responses with the desired source IP addresses.

In [14], Ally-based techniques are proposed extending the types of probe packets (ICMP, TCP) and the number of probe packets compared with the standard Ally. The rate at which probe packets are generated is also controlled with 0.3 secs inter-packet delay.

Radargun [15] uses direct probing, IPID-based behavior and UDP/TCP probe packets to apply a velocity modeling to characterize IPID evolution per router. It allows to check for IPID evolution in thousands of IP addresses simultaneously. Also, Midar [6] proposal argues to identify aliases with an improved variation of IPID-based behavior, but the current version (September 2011) is limited to 200 IP addresses and its identification results are not as good as expected.

Focusing in active probing, the following sections analyze the validity of the responses obtained as a funtion of the directiveness of the measurement, the type of probe packets and the type of router behavior. Finally, a performance comparison for previous IP aliases resolution techniques will be presented.

3 Network scenario

In order to compare the IP aliases resolution techniques over the same network scenario, specific requirements are needed for this scenario. Some techniques, like TraceNet, need a large set of vantage points to perform indirect probing between them. We have used vantage points belonging to the Planetlab measurement infrastructure [16]: 25 Planetlab nodes have been used as vantage points to

perform IP aliases resolution for IP addresses of the routers in between. Those IP addresses have been discovered using paris-traceroutes [17] between each pair of vantage points, resulting in 2037 different IP addresses discovered, some of them belonging to the same router (aliases).

As the underlying topology is unknown, the quality of IP aliases resolution techniques can not be checked for the existence of false positives and false negatives. There are some NRENs (National Research and Educational Networks) that provide public information about their network topologies, but they are small and they are composed by similar router behaviors (same manufacturer and even router models in many cases). Some examples of those networks are Geant [18], Canet4 [19] and GlobalNOC [20], but they do not provide more than 500 IP addresses at most. Besides, we do not have enough nodes in the border of those networks to be used as vantage points (needed for indirect methods).

Planetlab provides a bigger topology with a great variability of router behaviors as different Internet service providers are traversed. Networks are not only academic because several Planetlab nodes are connected to commercial Internet trunks or these commercial Internet trunks are traversed in the interconnection. However, the main reason to use Planetlab has been the necessity of having distributed vantage points around the network topology that would enable to perform indirect probing. We did not have access to similar vantage points for the above-mentioned NRENs.

IP addresses of the Planetlab topology between vantage points have been obtained by indirect probing (paris-traceroute) and there is no knowledge of real IP addresses. Therefore, direct probing will be performed over those IP addresses, and responsiveness in that case will correspond to the subset of IP addresses that are the intersection between direct probing responsiveness and indirect probing responsiveness. As our analysis focuses on the validity of the responses, the set of IP addresses will not imply any limitation.

4 Analysis of router behaviors

Unresponsiveness, as stated in [7], can be due to several reasons. The main one is the configuration of routers to ignore or filter certain types of probe packets, mainly for security reasons but also in order to avoid extra processing load. Rate limiting of ICMP responses at the target router is another reason for not receiving response packets. This rate limiting can depend on the internal router congestion and be applied in order to reduce the impact of this low priority traffic on the router. Finally, the routers can have private or duplicated public IP addresses and, therefore, not be reachable from the public Internet.

Besides router responsiveness, finding the expected header fields with the right content in returned packets is imperative to apply specific IP aliases resolution techniques. The different alternatives that can be found in router behavior are explained in the following subsections depending on the IP aliases resolution technique: IPID-based, Timestamp-based and SourceIP-based. Not all responses

to packet probes will be useful for IP aliases resolution. Those useful will be called valid responses.

4.1 IPID-based router behaviors

In IPID-based techniques, the routers are expected to increase their internal IPID counter for each IP packet they generated. The probe packets sent to some routers will originate response packets with IPID fields following an incremental sequence, useful for IPID-based techniques. This behavior is called *Incremental*, but several others have been detected in Internet routers. In *Zero* behavior, the IPID field is always filled up with zero value. In *Random* behavior, the IPID field is filled up with a random value for each packet. Finally, in *Copy* behavior, the IPID field is a copy of the IPID field in the probe packet received by the router.

All these four behaviors are present in direct probing, but only Incremental, Zero and Random behaviors have been found in indirect probing. Only the Incremental behavior can provide positive aliases in IPID-based techniques. The other behaviors can be used only to identify negative aliases because different behaviors can not be present simultaneously in the same router depending on the network interface or the network path followed by the probe request/response packets.

Experimental measurements have been performed over the 2037 IP addresses in the Planetlab scenario. Series of 20 probe packets of different types (ICMP Echo/Tstamp, UDP, TCP) have been sent to each IP address (direct probing) or to IP addresses in the border nodes (indirect probing), and responses have been analyzed looking for the IPID behavior. In indirect probing, TTL-limited probes are used to scan intermediate IP addresses in the path to each target IP address. In tables 1 and 2, percentages for each type of IPID behavior are presented in indirect and direct probing cases respectively. They show the percentage of each IPID behavior obtained in responses for different types of probe packets. As IP addresses have been obtained from indirect probing (paris-traceroutes), responsiveness is total for indirect probing and partial for direct probing as expected. However, validity of the responses is quite different as only Incremental behavior is useful to proceed with positive IP aliases resolution. In general, Incremental behavior appears in a bigger percentage in direct probing. Specifically, for ICMP Echo probes, the responses following Incremental behavior in the experiments are 35.87 % in indirect probing and 48.40% in direct probing. With UDP probes, indirect probing provides better results, but with TCP probes it is direct probing that gives the best results (33.08% compared to 26.53% for the indirect alternative). The column called valid responsiveness in tables 1 and 2 represents the percentage of responses by pair of IP addresses that contributes with positive or negative aliases identification results. It includes responses in which both IP addresses are incremental (positive or negative aliases) and responses in which each IP address has different behavior (negative aliases). In indirect probing with ICMP Echo, with 100% responsiveness, only 61.65% is useful responsiveness. The valid responsiveness increases to 70.51% in direct probing keeping the same type of probe packet (ICMP Echo).

UDP probes provide almost a negligible percentage of responses in direct probing. This makes unusable that kind of probe packets for direct probing. This happens because routers are usually configured to not respond with ICMP Error port unreachable packets. On the other hand, IPID-based aliases resolution methods will obtain better identification results using ICMP Echo as probe packets, for both direct and indirect probing.

Table 1. IPID-based behaviors in indirect probing

Type of probe packet	*Zero* (%)	*Incremental* (%)	*Random* (%)	*Copy* (%)	*Unresponsive* (%)	*Valid responsiveness(%)*
ICMP Echo	37.94	35.87	26.17	0	0	61.65
UDP	41.23	20.77	37.98	0	0	53.09
TCP	41.21	26.53	32.24	0	0	57.17

Table 2. IPID-based behaviors in direct probing

Type of probe packet	*Zero* (%)	*Incremental* (%)	*Random* (%)	*Copy* (%)	*Unresponsive* (%)	*Valid responsiveness(%)*
ICMP Echo	0	48.40	13.59	35.00	2.99	70.51
ICMP Tstamp	0	25.92	6.67	16.54	50.85	18.74
UDP	0.78	0.04	0.29	6.23	92.63	0
TCP	3.04	33.08	63.81	0.04	0	55.26

Another interesting finding is that router responsiveness is different depending on whether the router is in an access or core network (close or not to the network border). In figure 1, response ratio of routers located at different hop distances from the vantage points is plotted. In the left-one figure, responsiveness for ICMP Echo probes depends clearly on the distance from the vantage point, being more responsiveness access routers compared to core routers. However, the important parameter to IP aliases resolution is the valid responsiveness, that is related to the incremental behavior plotted in the right-one figure. In ICMP Echo responses, incremental behavior (related with valid responsiveness) is reduced for access routers and greater for core routers. The differentiation in valid responsiveness for access and core routers will need a specific future work.

4.2 Timestamp-based router behaviors

In timestamp-based techniques, IP prespecified timestamp option is used in probe packets. Those timestamps can be accounted in milliseconds since midnight UTC (standard) but if the time is not available in milliseconds or cannot be provided with respect to midnight UTC, then any time may be inserted as timestamp (non-standard).

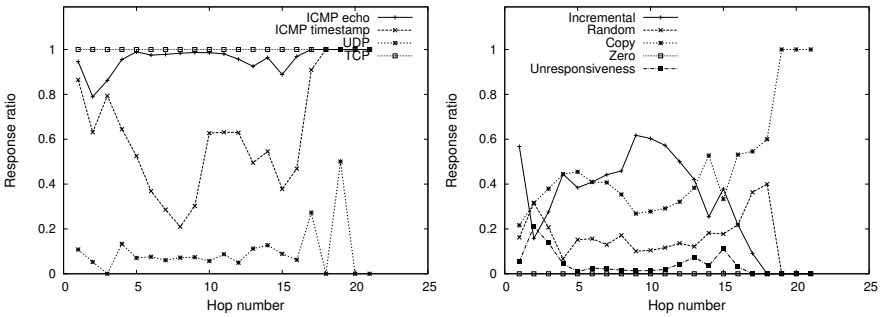

Fig. 1. Per-hop response ratio for each type of probe packet (left) and ICMP Echo behaviors (right) in direct probing

Timestamp-based techniques need routers that fill up the timestamp for their interfaces if they are requested. However, several behaviors are obtained in response to those probe packets:

- *N-tstamp*: the router is able to fill up N timestamps in the IP option, with $4 \geq N \geq 1$
- *Always*: the router always fills up the timestamps even for IP addresses not belonging to it. This behavior is undesirable.
- *None*: the router does not answer with the IP prespecified timestamp option enabled.

Timestamp-based techniques can be applied only if at least 2 timestamps belonging to the target router are filled up (valid responsiveness). Therefore, only N-tstamp behaviors with $4 \geq N \geq 2$ can be used for Timestamp-based techniques.

The 2037 IP addresses in the Planetlab scenario have been checked for valid responsiveness with timestamp-based router behaviors. Table 3 presents the results obtained in responses to probes with IP prespecified timestamp option in direct and indirect probing. Percentages of responsive and unresponsive routers are shown. Again, for this technique, direct probing provides better values of valid responsiveness: 42.87% compared to 21.10% for indirect probing.

Table 3. Timestamp-based behaviors in direct and indirect probing

Type of probe packet	*1-tstamp* (%)	*2-tstamp* (%)	*3-tstamp* (%)	*4-tstamp* (%)	*Always* (%)	*None* (%)	*Unresp.* (%)	*Valid resp.(%)*
ICMP Echo (direct)	9.51	6.08	0.09	36.70	1.47	0.09	45.94	42.87
ICMP Echo (indirect)	8.00	0.19	0.0	20.91	0.00	0.09	71.13	21.10

4.3 SourceIP-based router behaviors

Source IP address in response packets is the base of IP aliases resolution techniques such as Mercator. In this case, there are two expected behaviors:

- *Same-interface*: source IP address of response packet matches always target IP address of probe packet.
- *Different-interface*: source IP address of response packet does not always match target IP address of probe packet.

In this case, only UDP probes make sense because they produce ICMP Error responses. Those ICMP Error response packets can be generated from a different interface (and therefore IP address) than the incoming probe packet. In ICMP or TCP, the response packets are always generated from the same IP address that was the target IP address of the probe packet. Also, direct probing is the only way to perform this type of IP aliases resolution.

In the case of UDP probe packets, the behavior needed to apply IP aliases resolution is Different-interface behavior and, therefore, it will be considered to identify the valid responsiveness. If a response packet is received from a different source IP address than the original target IP address of the probe packet, both IP addresses are considered aliases.

Experimental results have been performed over the Planetlab scenario, with series of 20 packets sent to each one of the 2037 IP addresses in direct probing. In table 4, percentages of occurrences for each SourceIP-based behavior are presented. As stated in [14], very low values of responsiveness are present in this method with direct UDP probing. Besides, valid responsiveness has also very low values: 7.26% of routers answer with Different-interface behavior usable to apply this technique for IP aliases resolution.

Table 4. SourceIP-based behavior in direct probing

Type of probe packet	*Same-interface* (%)	*Different-interface* (%)	*Unresponsive* (%)	*Valid responsiveness(%)*
UDP	0.09	7.26	92.63	7.26

5 Behaviors applied to IP aliases resolution

The identification ratio for each type of IP aliases resolution scheme depends on the responsiveness and valid responsiveness ratios presented in previous sections. Table 5 shows the identification ratios obtained using the most frequent IP aliases resolution techniques for the Planetlab scenario described in section 3. The experiments were run using the original software provided by the creators of each technique (Palmtree, Tracenet, Radargun, Ally-based) or with custom

software where the original software was not available (Mercator, Ally, Prespecified timestamps). All software and data files used in this paper are available online at [21].

Table 5 shows the percentage of positives, negatives, error and unknown identifications over the total number of pairs of IP addresses presented. "Positives" indicate the pairs of IP addresses identified as aliases by each technique. "Negatives" identify those not aliases. "Errors" are those pairs of IP addresses with some error in the technique like not responding with the desired header field (they did not provide any information at all). "Unknown" are those pairs of IP addresses that have not provided enough information to identify the aliasing (they provided some but not enough information). Take note that the percentage of false positives and false negatives can not be provided because the real network topology is unknown (those ratios can be found in studies like [14]).

The column called Identified is the sum of positives and negatives, indicating the total pairs of IP addresses identified as being aliases or not. This is the main column in order to compare the different techniques. Also, a column with the number of resulting nodes in the network graph after applying the technique is shown. The column called "X-based" indicates the type of technique: IPID-based, Timestamp-based and SourceIP-based. It will indicate whether a technique will be affected by some router behavior or another. Finally, there is a column indicating if the specific technique uses direct or indirect probing.

As expected, IPID-based techniques provide better identification results, mainly Radargun and Ally-based techniques. Both use ICMP Echo with direct probing that provided the best valid responsiveness in previous sections. In fact, valid responsiveness reviewed in previous sections is the most important factor in determining results of IP aliases resolution techniques. However, results are not as good as expected by the valid responsiveness in Prespecified Timestamps technique. The reason is that the number of negatives is very low. To check for negative aliases both routers whose IP addresses are being checked must be in the same path from the vantage point. This is not feasible with a reduced number of vantage points compared with the number of IP addresses to check for aliases that would be the most common case.

The technique called "All" is a merge of the results coming from all the techniques, representing the expected results if all methods could be used simultaneously to verify IP aliases in a certain network topology. It is very expensive in terms of time and amount of probing traffic, but it provides the best results in the identification.

6 Conclusions

This paper has analyzed the impact of different router behaviors in answering to probing schemes for IP aliases resolution techniques. Schemes that provide a high percentage of response are not enough. It has been discussed how important is the quality of the responses. Only part of the responses can be used in an IP aliases process, and this subset comprises the so-called valid responsiveness.

Table 5. IP aliases resolution results for more important methods

Technique	*Positives* (%)	*Negatives* (%)	*Identified* (%)	*Error* (%)	*Unknown* (%)	*Resulting* nodes	*X-based*	*Direct/* Indirect
Mercator	0.00	0.00	0.00	0.00	99.99	2029	SourceIP	Direct
Palmtree	0.03	-	0.03	99.97	-	1343	SourceIP	Direct
Tracenet	0.10	-	0.10	99.9	-	857	SourceIP	Indirect
Ally	0.00	0.04	0.04	99.96	0.00	2025	IPID	Direct
Radargun	0.11	20.27	20.39	79.49	0.11	1625	IPID	Direct
Ally-based (6 packets)	0.07	19.72	19.80	7.65	72.55	1212	IPID	Direct
Ally-based (20 packets)	0.12	62.66	62.79	0.33	36.85	1129	IPID	Direct
Prespecified timestamps	0.06	0.24	0.31	99.68	-	1523	Timestamp	Indirect
All	0.34	73.85	74.19	0.03	25.77	492	All	Both

Although routers are more responsive to indirect probing, valid responsiveness is greater in direct probing. Therefore, direct probing provides better results in IP aliases resolution. Besides, the type of probe packet is very important. If possible, ICMP Echo probe packets should be used as they provide the best results in valid responsiveness, reaching ratios of almost 70% of valid responses. Indirect probing makes sense to be used in network topology discovery. Direct probing will be the best alternative in IP aliases resolution.

The percentage of identification in IP aliases resolution follows the same criteria as with valid responsiveness. In this case, techniques with direct probing and ICMP Echo probe packets provide the best identification results. For example, Ally-based techniques reach almost 62% of identification with respect to the total number of pairs of IP addresses in the network scenario.

In order to propose new IP aliases resolution techniques, as a rule of design, it is recommended to consider a direct probing scheme combined with ICMP Echo probe packets in order to get the best ratios of valid responsiveness in IPID-behavior schemes that provide the best identification ratios.

References

1. CAIDA. ARK, Archipelago Measurement Infrastructure. http://www.caida.org/projects/ark/, 2002.
2. Harsha V. Madhyastha, Tomas Isdal, Michael Piatek, Colin Dixon, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. iPlane: An information Plane for Distributed Services. In *7th USENIX Symposium on Operating Systems Desing and Implementation*, pages 367–380, Seattle, WA, November 2006.
3. D. McRobb, K. Claffy, and T. Monk. Skitter: CAIDA's macroscopic Internet topology discovery and tracking tool. Available from http://www.caida.org/tools/measurement/skitter/, 1999.
4. Y. Shavitt and E. Shir. DIMES: Let the Internet Measure Itself. *ACM SIGCOMM Computer Communication Review*, 35(5):71–74, October 2005.

5. N. Spring, R. Mahajan, and D. Wetherall. Measuring ISP topologies with Rocketfuel. In *In Proc. ACM SIGCOMM*, pages 133–145, Pittsburgh, August 2002.
6. K. Keys, Y. Hyun, M. Luckie, and k. claffy. Internet-Scale IPv4 Alias Resolution with MIDAR: System Architecture. Technical report, Cooperative Association for Internet Data Analysis (CAIDA), May 2011.
7. Mehmet H. Gunes and Kamil Sarac. Analyzing router responsiveness to active measurement probes. In *Proceedings of the 10th International Conference on Passive and Active Network Measurement*, PAM '09, pages 23–32, Berlin, Heidelberg, April 2009. Springer-Verlag.
8. K. Keys. Internet-Scale IP Alias Resolution Techniques. *ACM SIGCOMM Computer Communication Review (CCR)*, 40(1):50–55, Jan 2010.
9. Mehmet H. Gunes and Kamil Sarac. Resolving IP aliases in building traceroute-based Internet maps. *IEEE/ACM Transactions on Networking*, 17:1738–1751, December 2009.
10. Justine Sherry, Ethan Katz-Bassett, Mary Pimenova, Harsha V. Madhyastha, Thomas Anderson, and Arvind 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, November 2010. ACM.
11. R. Govindan and H. Tangmunarunkit. Heuristics for internet map discovery. In *Proc. IEEE INFOCOM*, March 2000.
12. Kamil Sarac M. Engin Tozal. Tracenet: An internet topology data collector. *Internet Measurement Conference IMC*, pages 356–368, November 2010.
13. Kamil Sarac M. Engin Tozal. Palmtree: An ip alias resolution algorithm with linear probing complexity. *Computer Communications*, 34(5):658–669, April 2011.
14. Santiago Garcia-Jimenez, Eduardo Magaña, Daniel Morató, and Mikel Izal. On the performance and improvement of alias resolution methods for Internet core networks. *Annals of Telecommunications, Springer*, 66:31–43, feb 2011.
15. Adam Bender, Rod Sherwood, and Neil Spring. Fixing Ally's Growing Pains with Velocity Modeling. In *(IMC 08) 8th ACM SIGCOMM conference on Internet measurement*, pages 337–342, New York, NY, USA, October 2008. ACM.
16. B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman. Planetlab: An overlay testbed for broad-coverage services. *ACM SIGCOMM Computer Communications Review*, 33:3–12, July 2003.
17. Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viget, Matthieu Latapy Timur Friedman, Clemence Magnien, and Renata Teixeira. Avoiding traceroute anomalies with paris traceroute. In *6th ACM SIGCOMM*, pages 153–158, Rio de Janeiro, Brazil, October 2006.
18. Geant official site. http://www.geant.net/pages/home.aspx.
19. Canet4 looking glass web tool. http://dooka.canet4.net/lg/lg.php.
20. Globalnoc looking glass tool. http://routerproxy.grnoc.iu.edu/.
21. Santiago Garcia-Jimenez et al. Tools and data sets used in this paper. http://www.tlm.unavarra.es/∼santi/research/paper11.html.