A Study on Traceroute Potentiality in Revealing the Internet AS-level Topology

Adriano Faggiani*†, Enrico Gregori†, Alessandro Improta†, Luciano Lenzini*, Valerio Luconi*, Luca Sani†
*Information Engineering Department, University of Pisa, Pisa, Italy
firstname.lastname@iet.unipi.it
†IIT-CNR, Pisa, Italy
firstname.lastname@iit.cnr.it

***Abstract*—Several works over the past few years have shown that the Internet AS-level topology is partially hidden from the current Internet measurement infrastructures. Most have focused on the incompleteness of the connectivity extracted from BGP data. A few have analysed the connectivity collected by traceroute measurement infrastructures showing the amount of connections introduced by traceroute campaigns. None, however, have investigated in detail the underlying rationale, i.e. the economic nature of the Internet. In this paper we fill this gap by analysing five traceroute infrastructures, found to be active in October 2013, with the p2c-distance metric, which is specifically designed to capture the complex economic dynamics that rule the Internet. We found that the traceroute infrastructures that currently run topology discovery measurements (Ark, DIMES and Portolan), together with BGP route collectors, are able to reveal the full connectivity of 23.50% of the Internet core ASes. This is a considerable improvement given that the BGP infrastructure alone is able to cover only 15.90% of the Internet core. This percentage could be increased up to 48.48% if the remaining two infrastructures (Dasu/Ono and RIPE Atlas) performed topology discovery campaigns. We also found that the placement of traceroute probes is not optimal from a topology discovery perspective, as it causes several probes to provide only redundant connectivity information. We show that the same number of traceroute probes optimally deployed, would be able to completely reveal the full AS connectivity of the Internet core.**

Keywords*—Internet; Traceroute; BGP; AS-level topology; p2c-distance

I. Introduction

Over the last twenty years the Internet has evolved from a collection of a few academic networks to a tangled web of interconnected heterogeneous networks essentially driven by commercial interests. Privatization began in 1995, the year of the decommission of the NSFNET backbone and the birth of the first national-scale ISPs. This milestone also represented the end of being able to have complete knowledge of the structure of the Internet. Some years later the quest to reveal the complete Internet structure officially began [1], [2]. Since then, great research interest focused on finding ways to infer the Internet topological structure at different levels of abstraction. The Autonomous System (AS) level is one of the most investigated approaches since it captures the real economic nature of the inter-domain routing in the Internet. No tools (or protocols) have been designed to discover the Internet AS-level connectivity. However, it is still possible to infer such information by exploiting the collateral effects of the Border Gateway Protocol (BGP) and the traceroute tool. In the BGP case, the `AS_PATH` attribute of `UPDATE` messages can be used to extract inter-domain connectivity information, although the attribute was originally introduced to prevent routing loops. Similarly, the sequence of IP interfaces obtained via traceroute can be used to infer AS-level connectivity [3], [4], even though the tool was originally conceived for network diagnostics. Despite the above techniques being workarounds, they have been used by several infrastructures to perform topology discovery measurements. However, research has shown that the topology inferred by the current measurement infrastructures is highly incomplete. Most of these works have focused on analysing the incompleteness of data obtained through BGP route collectors [5], [6], [7] or showing that traceroute measurements could introduce additional AS-level topology information [8] and are particularly effective in revealing missing links on Internet Exchange Points (IXPs) [9], [10], [11]. To the best of our knowledge, only [5] has developed a methodology for quantifying the portion of the Internet that can be revealed via BGP route collectors.

In this paper we complete the analysis started in [5] by focusing on the traceroute measurement infrastructures, and showing how they can be used to integrate BGP data. We analyse five traceroute measurement infrastructures that were active in October 2013. Three (CAIDA Archipelago, DIMES and Portolan) are topology-discovery oriented, while the other two (Dasu/Ono and RIPE Atlas) are designed for other purposes. By applying the methodology described in [5], we quantify the amount of connectivity that the traceroute infrastructures, together with the BGP route collectors, can potentially reveal. We show that CAIDA Archipelago, DIMES and Portolan are able increase the coverage of the Internet core from the 15.90% achieved by BGP route collectors up to 23.50%. If we also consider Dasu/Ono and RIPE Atlas, this coverage could increase to 48.48%. We further deepen our analysis by quantifying the geographic pervasiveness of each traceroute infrastructure, and show that coverage achieved in six different geographic macro-areas changes considerably. Finally, we also show that traceroute probes are not optimally distributed in a topology discovery perspective, thus several probes provide

ISBN 978-3-901882-58-6

redundant information. If the same number of probes were deployed following an optimal strategy, full coverage of the Internet core could be achieved. To the best of our knowledge this is the first work that performs a quantitative analysis on the coverage achievable through traceroute infrastructures.

The paper is organized as follows. Section II overviews related studies. Section III details the five traceroute infrastructures considered in our study, in terms of the the properties and the geographic distribution of the ASes hosting at least one of their probes. Section IV explains the concept of p2c-distance and the related optimization problems used in our study. Section V the analyses the coverage achieved by traceroute infrastructures. Some conclusions are drawn in Section VI.

II. Related work

The problem of the incompleteness of the existing Internet AS-level topology measurement infrastructure has been addressed mostly for the BGP route collecting infrastructure. One of the first attempts to quantify this incompleteness is in [12], where the authors compared the amount of AS-level connectivity inferred by BGP data collected by RouteViews and from looking glass servers with the amount inferred by Internet Routing Registries (IRR) data, showing that several AS connections were missing in BGP data. A similar approach was followed in [6], where the AS-level topology inferred by BGP data was compared with a ground truth of real topology data provided by several organizations, i.e. Internet Service Providers (ISPs), research networks and Content Distribution Networks (CDNs). Results showed again that the inferred AS-level topology was missing a huge number of links.

While the above works focused on showing the number of links that the BGP measurement infrastructure was missing, [13] was a first attempt to study and quantify the portion of the Internet that the existing BGP measurement infrastructure is able to reveal. The authors introduced the concept of the *eyeshot* of a vantage point (i.e. a BGP route collector), which is the portion of the Internet that can be observed by that vantage point. With this information they showed that several vantage points provide redundant information and that the same results could be obtained with a fewer number of vantage points, thus reducing the cost of the measurement infrastructure. However, the authors did not quantify the exact number of required vantage points. The last step is provided by [5], where the *p2c-distance* metric was proposed. Using the p2c-distance metric the authors quantified the amount of transit ASes whose full connectivity can be revealed with the current BGP infrastructure and the number of BGP feeders that should be added to reach the complete coverage of the Internet core.

Few works focused on quantifying the incompleteness of the information provided by the traceroute measurement infrastructure, from an AS-level topology discovery perspective. Several works have analysed the amount of bias introduced by traceroute measurements when trying to discover the topology of several ad-hoc generated networks. In [14] the authors empirically demonstrate that when sampling such networks from a small set of sources, the inferred topology misses several links. An extension is provided in [15], where the analysis is broadened to all the classes of networks. Other works have demonstrated that traceroute-based infrastructures can be helpful in increasing the number of links revealed by BGP route collectors. For instance, in [16] the authors used a traceroute-capable P2P client to perform a large-scale measurement campaign, which was able to find a large number of links invisible to BGP route collectors. In [9] a framework is built for discovering missing AS links in BGP data with the help of IRRs and traceroutes. Again, the authors revealed a large number of new links, claiming that the vast majority are p2p links. The BGP and traceroute inferred topologies were also compared in [17], by the means of a new metric, the *weighted spectral distribution*. Results show that BGP and traceroute inferred topologies are complementary, as they discover different portions of the Internet. Finally, in [8], BGP and traceroute data are merged in order to obtain a more complete view of the AS-level topology of the Internet.

Only recently in [18] was the importance of a broad distribution of traceroute monitors proved in a topology discovery perspective, however the authors did not quantify the amount of AS-level connectivity that a better distribution could discover. Instead, they focused on analysing the properties of the inferred topology as new monitors were added.

To the best of our knowledge, the only work that manages to numerically quantify the incompleteness of any AS-level topology-oriented measurement infrastructure is [5], but they only focused on BGP route collectors.

III. Traceroute infrastructures

Traceroute is a network diagnostic tool that was initially developed by Van Jacobson in 1988. It exploits the Time To Live (TTL) field of IP packets to retrieve information on the path used to reach a certain destination. The output of traceroute is a sequence of IP interfaces representing the path from source to destination. The related AS-level path can be inferred by exploiting one of the available IP-to-AS mapping techniques (e.g. [3], [4]) not without any precaution (e.g. [19], [20], [21]). Over the last few years several infrastructures that perform traceroute measurements have been deployed, some of which were explicitly aimed at revealing the Internet topology. In this section we analyse the characteristics of the most popular infrastructures that perform traceroute measurements and we show how the distribution of their vantage points seems to be valuable from a topology discovery perspective.

A. Traceroute infrastructures

We found five infrastructures running in October 2013 that were able to perform traceroute measurements. For each one we managed to obtain a list of ASes where their monitors were placed, hereafter *probing ASes*.

Aqualab Dasu and Ono are two large-scale systems conceived at the Northwestern University. Dasu is targeted at broadband characterization and network experimentation [22], whereas Ono aims to improve BitTorrent downloads by choosing the most suitable peer using CDN redirections [23]. They both perform traceroute measurements by means of Vuze's BitTorrent extensions, which are freely available on

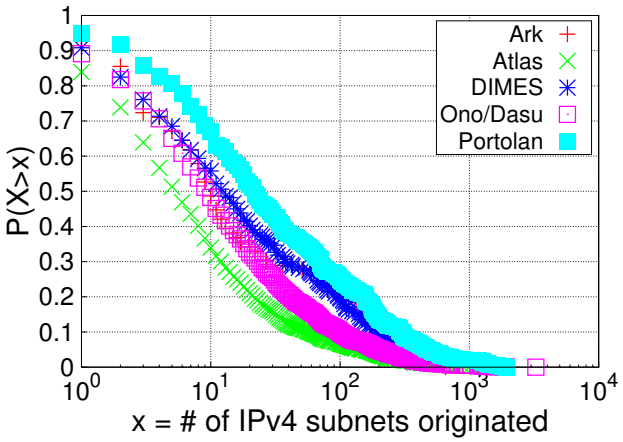


Figure 1: CCDF of the IPv4 space originated by probing ASes

Project	*Prob. ASes*	*Non stub ASes*	*Stub ASes*
Ark	76	60 (78.95%)	16 (21.05%)
Atlas	2,135	1,310 (61.36%)	825 (38.64%)
Dasu/Ono	2,442	1,398 (57.25%)	1,044 (42.75%)
DIMES	251	145 (57.77%)	106 (42.23%)
Portolan	360	246 (68.33%)	114 (31.67%)

Table I: Distribution of probing ASes

the web[1][2]. Both Dasu and Ono perform traceroutes randomly to a subset of connected BitTorrent peers. The number of traceroutes performed by each client varies depending on the number of peers they connect to and on the amount of time they remain connected. Periodically Ono also launches traceroutes to CDN servers in order to collect proximity information on other Ono peers. Both Dasu and Ono use the classic traceroute provided by the operating system and do not perform traceroute measurements aimed at revealing the Internet topology. The Dasu/Ono dataset of probing ASes was obtained by direct interaction with the Aqualab team.

CAIDA Archipelago (Ark) [24] was designed and implemented by the Cooperative Association for Internet Data Analysis (CAIDA). Traceroutes are performed from a set of ASes that host Ark monitors on a volunteer basis. Monitors are divided into three probing teams. Each team probes a portion of all routed /24 subnets in parallel and independently in order to terminate each traceroute campaign in a short time. Ark performs its measurements with *Scamper* [25] which implements the ICMP, UDP and TCP version of the Paris Traceroute [26]. Every month Ark performs extensive traceroute measurements using the ICMP-Paris Traceroute. In order to obtain the AS-level topology from IP traces, CAIDA uses RouteViews[3] routing tables to map IP addresses to ASes. The Ark dataset of probing ASes was downloaded from the project website[4].

Distributed Internet MEasurement System (DIMES) [27] consists in a distributed measurement infrastructure developed at Tel Aviv University, leveraging on the volunteer contribution of users. Each volunteer installs a software agent available on the DIMES website[5], which runs background traceroute and ping measurements according to the user's location. The traceroutes are then collected and combined together to periodically produce AS-level topologies. In order to associate the IP addresses with ASes, DIMES looks for the longest prefix match in their database, which is built using BGP routing tables obtained from RouteViews. We obtained the DIMES dataset of agent IPs directly from the project team. Then, we mapped each agent IP to the related AS using IP to AS data provided by Isolario[28].

Portolan [29], [30] was recently developed by the University of Pisa and IIT-CNR in order to reveal the Italian AS-level topology. To the best of our knowledge, Portolan is the first crowdsourcing platform based on mobile devices to perform topology discovery measurements. Volunteers can install an app for Android[6] which implements a UDP version of the Paris Traceroute [26], [31]. In October 2013, Portolan began traceroute campaigns aimed at revealing regional characteristics of the Internet. In order to map IP addresses to ASes, Portolan uses IP to AS data provided by Isolario [28]. The Portolan probing ASes were obtained by direct interaction with the project team.

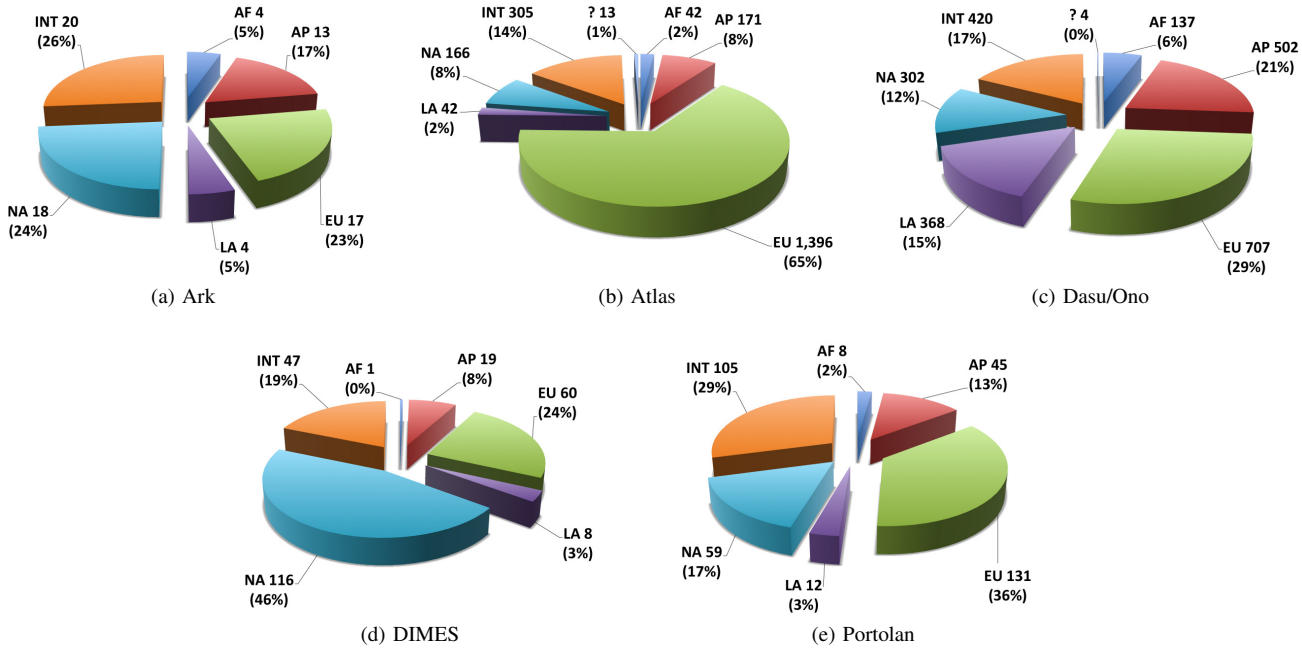
RIPE Atlas [32] is a Réseaux IP Européens (RIPE) project which distributes probing devices to interested users in order to sense the Internet. The user is required to physically host at least one Atlas probe in his/her own network in order to start a measurement campaign. Each campaign consumes user credits which are earned by keeping the probe(s) active. The user in turn can exploit the entire Atlas probing network to perform real time customized measurements. The Atlas probing ASes were extracted from the RIPE Atlas database using the REST API. To the best of our knowledge, currently the Atlas staff is not running any continuous traceroute measurements aimed at revealing the Internet AS-level topology.

B. Infrastructure characterization

In this section we detail the characteristics of the traceroute infrastructures introduced above, by analysing the properties and the geographical distribution of their probing ASes. Probing ASes are well distributed in small ASes located in the periphery of the Internet. Most probing ASes were indeed announcing a small number of subnets towards the Internet[7]

[1]http://plugins.vuze.com/plugin_details.php?plugin=dasu
[2]http://plugins.vuze.com/plugin_details.php?plugin=ono
[3]http://www.routeviews.org
[4]http://www.caida.org/projects/ark/
[5]http://www.netdimes.org

[6]https://play.google.com/store/apps/details?id=it.unipi.iet.portolan.traceroute
[7]This information was obtained by analysing the routing data provided by BGP route collectors during the analysed period.



(a) Ark (b) Atlas (c) Dasu/Ono

(d) DIMES (e) Portolan

Figure 2: Geographic distribution of probing ASes per project

(Fig. 1). Moreover, several probing ASes are stub ASes (Table I), i.e. ASes that do not transit any traffic for any other AS[8]. Stub ASes are at the bottom of the Internet hierarchy and usually are owned by very small organizations. The pervasiveness of probing ASes in the periphery of the Internet is particularly important. Indeed BGP route collectors are currently unable to discover much of the AS-level connectivity of the periphery of the Internet hierarchy [5].

Another characteristic that makes the traceroute infrastructures extremely appealing from a topology discovery perspective, is their large number of probing ASes (Table I), and the low overlap coefficient[9] among different infrastructures (Table II). In other words, each project introduces new points of view. The heterogeneous pervasiveness of the traceroute infrastructures is also maintained at a geographical scope. This is even more important because enables regional characteristics of the Internet to be revealed. To get a better insight into the geographical pervasiveness of each traceroute infrastructure, we computed the geographical scope of each of its probing ASes. To do this, we collected the subnets announced by each probing AS from the routing data gathered by BGP route collectors, and then we geolocated each of them using the Maxmind GeoIPLite database [33]. We thereby identified five macro-areas: Africa (AF), Asia-Pacific (Asia and Oceania – AP), Europe (EU), Latin America (LA), and North America (NA). Whenever an AS is found in more than one continent, we refer to it as an *intercontinental* AS (INT). More details on this geolocation technique and its correctness can be found in [34]. As can be seen from Fig. 2, most probing ASes are located in a single continent, and each traceroute infrastructure has a different geographical pervasiveness. For example, DIMES is mostly used in North America, while Atlas probes are hosted mostly on European ASes, as Atlas is a project managed by RIPE.

From this preliminary analysis, traceroute infrastructures seem to be extremely promising from a topology discovery perspective. They bring a huge number of probing ASes mostly located in the lower layers of the Internet hierarchy. In addition, each infrastructure introduces different well-geographically distributed point of views, thus increasing the diversity of the sources of measurements. However, *"All that glisters is not gold"...* [35].

IV. The Researcher's Guide to the Coverage

The analysis provided in Section III cannot quantify the real contribution of probing ASes, since it does not take

A \ B	*Ark*	*Atlas*	*Dasu/Ono*	*DIMES*	*Portolan*
Ark	–	0.577	0.310	0.239	0.155
Atlas	0.019	–	0.296	0.049	0.088
Dasu/Ono	0.009	0.259	–	0.045	0.100
DIMES	0.068	0.414	0.438	–	0.243
Portolan	0.031	0.522	0.675	0.169	–

Table II: Overlap coefficient $O(A, B)$ among probing ASes of different projects

[8]Stub/non stub ASes can be inferred from data collected from BGP route collectors analysing the position of each AS in AS paths [5].

[9]The overlap coefficient of the two sets A and B is defined as the fraction of elements that A shares with B, i.e. $O(A, B) = \frac{|A \cap B|}{|A|}$

into account the economic nature of the Internet inter-domain routing. ASes agree to exchange routing information on the basis of technical *and* economic factors. As a consequence, traffic flowing in the Internet – e.g. a traceroute probe – is constrained in AS paths that directly reflect the business agreements established among organizations owning the ASes. These business agreements lead to a plethora of possible scenarios in which ASes exchange different subsets of routes with their neighbours. In this paper we focus on the classical provider-to-customer (p2c) and peer-to-peer (p2p) subdivisions [36], which are considered to capture most cases [7].

In [5] we designed a new metric – the p2c-distance – which is based on these economic relationships and enables to quantify the amount of Internet core[10] that can be revealed via BGP route collectors. Non stub ASes are the ASes whose coverage is the most interesting to be revealed, since most of them are interested in developing peer-to-peer connectivity [5], which is known to be missing in public datasets [6], [5], [7].

In this work we exploit the same metric to quantify the possible coverage of the set of traceroutes probing ASes. This section overviews the concept of p2c-distance, how it can be used to carry out the coverge analysis of the traceroute measurement infrastructure, and how the p2c-distance is computed.

A. p2c-distance

The p2c-distance originates from the analysis of the economic relationships described in [36]. The key concept is that only a *customer* in a p2c relationship is able to reveal the full connectivity of its *provider*. This is because in p2c relationships, the provider announces to the customer the routes to reach all the Internet destinations, while the customer announces back only the routes to reach its own networks and the networks obtained from its own customers (if any). In order to prevent the provider traffic from transiting in the customer, the customer does not advertise networks obtained from its other providers and peers. Similarly, in p2p relationships the two peers only exchange routes required to reach their own networks and the networks obtained from their respective customers. The p2c-distance between a target AS T and a source AS S is thus defined as the minimum number of consecutive p2c links connecting T with S. For example, in Fig. 3, the p2c-distance of AS E from AS A is 1, the p2c-distance of AS E from AS C is 2, and the p2c-distance of AS B from AS F is undefined (as well as the p2c-distance of AS B from all other ASes). Whenever the value of the p2c-distance is undefined – i.e. there is no AS path consisting only of p2c connections from T to S – it is possible to state that a route collector placed in S will never discover a p2p link established by T. In other words, a necessary – but not sufficient – condition for a route collector to gather the full connectivity of a target AS X is that the p2c-distance of X from that route collector is defined [5]. For example, suppose that we want to discover the full connectivity of AS B in Fig. 3 and that we can deploy a route collector. The only way to fulfill this objective is to connect the route collector to AS B. Similarly, this metric can be applied to determine whether a traceroute probing AS can reveal the full connectivity of a target AS T. If T has a finite p2c-distance from the probing AS, then the full connectivity of T may be revealed by the probing AS.

[10]In this work we use the term *Internet core* to refer to the set of non stub ASes, since each one transits traffic for at least another AS.

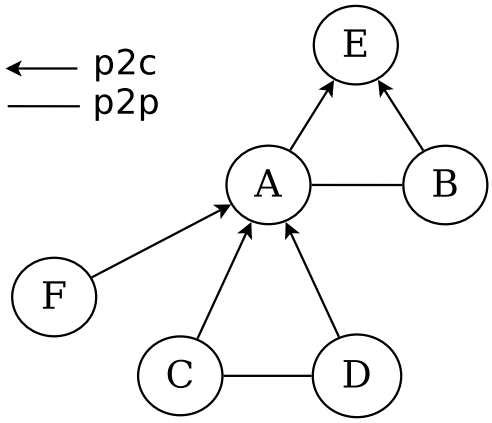


Figure 3: p2c-distance example

B. Coverage optimization problems

The definition of p2c-distance enables the coverage capability of any given AS-level measurement infrastructure to be revealed. It is possible to state that a given measurement infrastructure may reveal the full connectivity of every non stub AS only if each non stub has a defined p2c-distance from at least one of the monitors of the infrastructure. This statement can be cast into an optimization problem known as the *Minimum Set Cover* (MSC) problem [37] aimed – in our context – at finding the minimum number of ASes hosting a monitor such that each non stub AS has a finite and bounded p2c-distance from the measurement infrastructure [5]. The original problem was applied to reveal the number of missing feeders in the BGP collecting infrastructure. The same problem can be also applied to the traceroute measurement infrastructures in order to find the minimum number of probing ASes to reveal the full connectivity of all non stub ASes.

The p2c-distance metric can also be exploited as a basis for another optimization problem known as Maximum Coverage (MC) [37]. The aim of this problem – in our context – is *to find the maximum number of non stub ASes whose p2c-distance is finite and bounded from a fixed number of ASes hosting monitors* [5]. The solution to this problem allows us, for example, to quantify how many non stub ASes would be fully covered if the current number of probing ASes were distributed according to an optimal strategy based on the p2c-distance metric.

C. Economic relationship inference

Computation of the p2c-distances between non stub ASes and probing ASes requires knowledge of which links between ASes are actually p2c. To get this knowledge, in this paper

we use the algorithm described in [38], whose accuracy in inferring p2c relationships was found to be around 90% [39]. This algorithm requires a set of routes together with their evolution during the observation period. After a spurious route filtering phase, the algorithm infers economic relationships by analyzing the AS paths contained in the remaining routes. We applied the algorithm to the set of routes collected by RouteViews, RIS[11], PCH[12] and BGPmon[13] projects and we found that 100,882 out of 192,467 AS links were p2c.

In theory, even the set of IP-level paths gathered by traceroutes could be translated into a set of AS paths, and then given as input to an economic tagging algorithm. However, mapping an IP-level path and an AS-level path is prone to errors (e.g. [3], [4], [20], [21]). Moreover, AS paths inferred from IP-level paths lack a temporal characterization, which is fundamental in order to prevent errors during economic tagging due to ephemeral and spurious routes [38]. Finally, as pointed out in Section III, only Ark makes traceroute IP-level paths publicly available. For these three reasons we exploited only AS paths gathered from BGP data.

Note that several studies have highlighted that the vast majority of missing links in the AS-level topology are of type p2p. This bias does not affect the accurate discovery of p2c links [6], [5], thus the inferred p2c-distance values can be considered as reliable.

V. A DEEPER ANALYSIS OF TRACEROUTE INFRASTRUCTURE COVERAGE

The concepts and methodologies introduced in Section IV lead to a deeper examination regarding the true coverage of non stub ASes[14] through the use of traceroute infrastructures. The distribution of non stub ASes covered by each infrastructure (Table III) shows that their contribution is not directly proportional to the number of probing ASes. This is proved by analysing the ratio between the number of non stubs covered and the number of probing ASes in each project (Table III). As can be seen, the infrastructures introducing the largest number of probing ASes are also those showing the lowest ratio value, meaning that several of their probing ASes cover the same set of non stubs. The main reason for this is the poor diversity of the providers of the ASes where the traceroute monitors are placed. In fact, several probing ASes share a common set of providers and thus provide redundant information, although the sets of probing ASes in each project do not overlap (Table II).

	d = 1		**d = 2**		**d = 3**	
	Val	Rat	Val	Rat	Val	Rat
Ark	361 (4.41%)	4.75	789 (9.64%)	10.38	1,117 (13.65%)	14.69
Atlas	2,367 (28.93%)	1.10	2,820 (34.47%)	1.32	2,949 (36.05%)	1.38
Dasu/Ono	2,465 (30.13%)	1.00	2,867 (35.04%)	1.17	2,981 (36.44%)	1.22
DIMES	517 (6.32%)	2.05	987 (12.06%)	3.93	1,332 (16.28%)	5.30
Portolan	700 (8.56%)	1.94	1,158 (14.16%)	3.21	1,458 (17.82%)	4.05

Table III: Non stubs covered by each project with p2c-distance less than/equal to d. Val = # of non stubs ASes covered (percentage), Rat = Ratio between non stubs covered and probing ASes

To prove this, we define the *p2c-overlap* coefficient of AS X as

$$\frac{|ns_d(X) \cap (\cup_{Y \neq X} ns_d(Y))|}{|ns_d(X)|} \quad (1)$$

where X and Y are ASes hosting a monitor, and $ns_d(X)$ is the set of non stub ASes with a p2c distance less than or equal to d from X. Fig. 4 shows the CCDFs of the p2c-overlap coefficient of the ASes involved in each infrastructure, computed with $d = 1, 2, 3$. As expected, the p2c-overlap coefficient tends to be high in each infrastructure, even in the scenario with $d = 1$, and gets larger as the p2c-distance increases, due to the small number of providers at the top of the Internet hierarchy. This means that the contribution of each probing AS is limited. Note however that even in the distribution related to $d = 3$ the amount of *completely* overlapping probing ASes – i.e. probing ASes whose p2c-overlap coefficient is equal to 1 – ranges between 23.51% (DIMES) and 34.12% (Atlas). Thus, most probing ASes actually do contribute to revealing different parts of the Internet core.

To study how traceroutes infrastructures can help in revealing AS-level connectivity, we start from the coverage achieved from the BGP full feeders[15] by considering the following three ideal covering scenarios: *Scenario I* is the

	# VPs	***d***	***Cov***	***Imp***	***Rat***
Scenario I	*166*	1	648 (7.92%)	-	3.90
		2	1,068 (13.05%)	-	6.43
		3	1,301 (15.90%)	-	7.83
Scenario II	*729*	1	1,288 (15.74%)	+98.76%	1.76
		2	1,728 (21.12%)	+61.80%	2.37
		3	1,923 (23.50%)	+47.81%	2.63
Scenario III	*4,222*	1	3,623 (44.22%)	+459.10%	0.85
		2	3,912 (47.82%)	+266.29%	0.92
		3	3,966 (48.48%)	+204.84%	0.93

Table IV: Non stubs covered per Scenario. *Cov* = # of non stubs covered (percentage), *Imp* = percentage of improvement with respect to Scenario I, *Rat* = ratio between non stubs covered and probing ASes

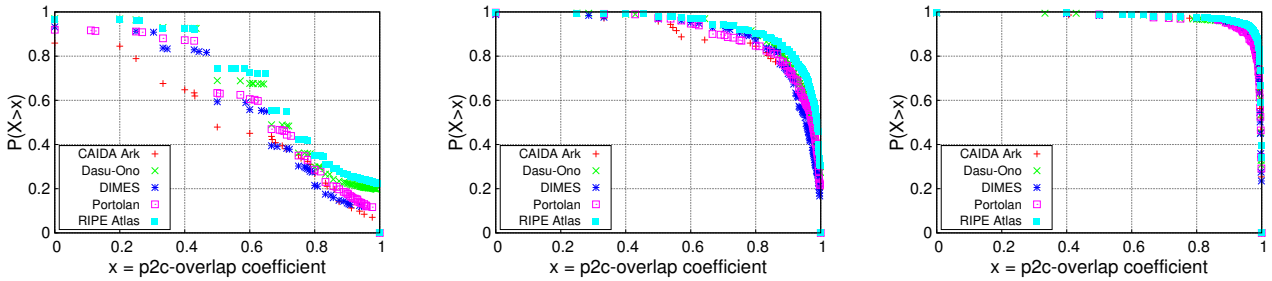
[11] http://www.ripe.net/data-tools/stats/ris/routing-information-service

[12] http://www.pch.net

[13] http://bgpmon.netsec.colostate.edu

[14] A non stub AS is identifiable from BGP route collector data as an AS appearing at least once in the middle of an AS path. In October 2013 we found 8,181 non stub ASes.

[15] A BGP *full feeder* is an AS which announces to a BGP route collector an IPv4 space close to its full routing table.



(a) d=1 (b) d=2 (c) d=3

Figure 4: p2c-overlap coefficient distributions

coverage achieved by BGP route collectors; *Scenario II* is the coverage achieved by BGP route collectors *plus* the probing ASes belonging to traceroute infrastructures that currently are performing extensive and continuous campaigns to discover the Internet AS-level topology (i.e. Ark, DIMES and Portolan); *Scenario III* is the coverage achieved by BGP route collectors *plus* all probing ASes belonging to a traceroute infrastructure. Hereafter Vantage Points (VPs) is used to refer both to BGP feeders and traceroute probing ASes.

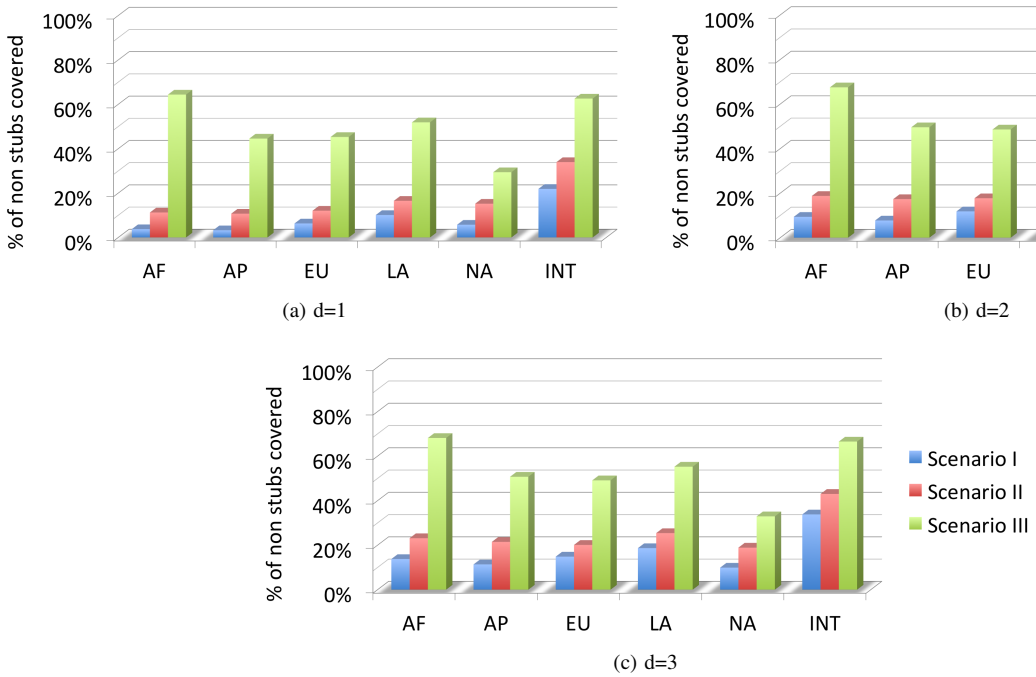
The coverage achieved by these scenarios is depicted in Table IV. The percentage of non stub ASes covered increases from values ranging between 7.92% and 15.90% (scenario I) to those between 15.74% and 23.50% (scenario II). Despite the improvements in these two scenarios ranging from +47.81% ($d = 3$) to +98.76% ($d = 1$), the coverage efficacy of each VP actually decreases, since on average each probing AS now only covers from 1.76 ($d = 1$) to 2.63 ($d = 3$) non stub ASes. In other words, quadrupling the number of probing ASes leads only to doubling the non stubs covered. This affects scenario III even more. In this scenario, the number of VPs is more than 25 times the number of BGP feeders, but the percentage of non stubs covered only ranges between 44.22% and 48.48%, representing improvements with respect to Scenario I ranging only from +204.84% ($d = 3$) to +459.10% ($d = 1$), i.e. about two to about five times the original coverage of BGP feeders.

The main reason for these relatively poor improvements is again the poor diversity of VP providers. This can be highlighted by analysing the results obtained by applying the MSC problem to each scenario (Table V). The full coverage is far from being achieved in every scenario despite the large number of VPs, and a large number of additional VPs are still required. The number of VPs that need to be added is *almost* the same in Scenario I and Scenario II (the difference is about 100 for all values of d). This problem is even worse in Scenario III, where the number of additional ASes required decreases by only about a thousand units, despite the number of VPs in this scenario being about three thousand units more than in Scenario II. The percentage of ASes providing only redundant AS-level connectivity information is extremely high in every scenario, i.e. the set of VPs deployed in each scenario tends to cover the same set of non stub ASes. Thus, the actual coverage achieved via traceroute infrastructure is even more limited than would have been expected by just analysing the p2c-overlap coefficients of each traceroute infrastructure separately. The poor diversity of VP providers can also be seen by analysing the geographical distribution of the non stub ASes covered. The class of ASes which is mostly populated by large ISPs (i.e. intercontinental ASes) is in fact the class usually most covered in each scenario (Fig. 5). On the other hand, only about 20% of the non stubs located in a single region are covered by infrastructures that actually run topology discovery measurements. The coverage of these ASes would improve greatly only if Atlas and Dasu/Ono were performing extensive measurement campaigns. It is worth also noting that scenario III reflects the drop in BitTorrent users recorded in North America in 2013 [40], which strongly affects the number of probing ASes introduced in that region by Dasu/Ono (Fig. 2).

These results become even more interesting when compared with the coverage achievable by ideally and arbitrarily introducing a number of VPs equal to the number of VPs of each scenario, i.e. by applying the MC problem on the AS-level topology collected by BGP route collectors as if no VPs were connected. By placing a monitor in 729 ASes as in Scenario II it would be possible to cover at least 3,017 non stub ASes (36.88%) at $d = 1$, 3,913 (47.83%) at $d = 2$, and 4,228 (51.68%) at $d = 3$. While by placing a monitor in 4,222 ASes as in Scenario III it would be possible to cover at least 7,612

	$d=1$		$d=2$		$d=3$	
	Add	*Red*	*Add*	*Red*	*Add*	*Red*
Scenario I	4,593	104 (63.65%)	4,136	130 (78.31%)	4,075	147 (82.12%)
Scenario II	4,444	518 (71.05%)	4,027	584 (80.11%)	3,978	603 (82.72%)
Scenario III	3,435	3,002 (71.10%)	3,199	3,249 (76.95%)	3,177	3,295 (78.04%)
Ideal scenario	4,655	–	4,172	–	4,104	–

Table V: MSC problem solutions - *Add* = # of VPs to add, *Red* = # of current VPs which provide only redundant coverage in the final optimal coverage



(a) d=1

(b) d=2

(c) d=3

Figure 5: Geographical distribution of non stubs covered

non stub ASes (93.05%) at $d = 1$, and each of the 8,181 non stub ASes at $d = 2$ and $d = 3$. Likewise, the current coverage achieved by Scenarios II and III (Table IV) could be obtained by placing monitors respectively in only 119 ASes for $d = 1$, 75 ASes for $d = 2$ and 49 ASes with $d = 3$ (Scenario II) instead of 729 ASes, and in only 1,042 ASes for $d = 1$, 729 ASes for $d = 2$ and 611 ASes with $d = 3$ (Scenario III) instead of 4,222.

VI. Conclusions

We have focused on the potential impact of traceroute infrastructures, which were active throughout October 2013, in improving the Internet AS-level connectivity discovery. We found that these infrastructures seem to be particularly useful in completing the Internet AS-level topology revealed via BGP route collectors. Their monitors are connected to a large number of ASes that do not currently feed a BGP route collector and are mostly located in the Internet periphery. By exploiting our p2c-distance metric and focusing on the economic nature of the Internet enabled us to discover that a large number of ASes hosting at least one traceroute monitor are covering the same set of non stub ASes and provide only a redundant contribution in terms of AS-level connectivity. The main reason behind this redundancy is the poor diversity in terms of providers, which is also highlighted when analysing the coverage of traceroute infrastructures at a geographic level. This redundancy strongly affects the actual coverage of traceroute infrastructures, thus limiting the usefulness of having a large additional number of probing ASes available. This is extremely clear if we consider that the same coverage achieved by traceroute infrastructures together with a BGP route collecting infrastructure could be obtained by using a seven times smaller number of vantage points.

Nevertheless, traceroute infrastructures increase the non stub coverage currently achieved by using the BGP route collecting infrastructure alone. We found that the coverage of non stub ASes could increase up to 23.50% if the set of probing ASes belonging to traceroute infrastructures that currently perform extensive Internet topology measurements (CAIDA Ark, DIMES, Portolan) is added to the set of BGP feeders commonly used in AS-level topology related studies. More interestingly, we found that RIPE Atlas and Dasu/Ono would be extremely useful in a topology discovery perspective only if they were performing an extensive traceroute campaign. The percentage of non stub ASes covered would indeed increase to 48.48%. We are aware that the infrastructures of Atlas and Dasu/Ono rely on dedicated software agents that are available only when the user turns on his/her device, and that it would be impossible to run traceroute campaigns 24/7 from every agent. Nevertheless, we strongly believe that it could be possible for these infrastructures to exploit the coverage redundancy shown in this paper to create ad-hoc traceroute campaigns for revealing the hidden part of the Internet core while maintaining a low workload on their agents.

ACKNOWLEDGEMENTS

This work has been partially supported by the European Commission within the framework of the CONGAS project FP7-ICT-2011-8-317672.

REFERENCES

[1] H. Burch and B. Cheswick, "Mapping the Internet," *IEEE Computer*, vol. 32, no. 4, pp. 97–98, 102, 1999.

[2] J.-J. Pansiot and D. Grad, "On Routes and Multicast Trees in the Internet," *ACM SIGCOMM CCR*, vol. 28, no. 1, pp. 41–50, 1998.

[3] H. Chang, S. Jamin, and W. Willinger, "Inferring AS-level Internet Topology from Router-Level Path Traces," in *Proc. of SPIE ITCom*, 2001, pp. 196–207.

[4] Z. Morley Mao, J. Rexford, J. Wang, and R. H. Katz, "Towards an Accurate AS-level Traceroute Tool," in *Proc. of ACM SIGCOMM*, 2003, pp. 365–378.

[5] 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," in *Proc. of ACM SIGCOMM IMC*, 2012, pp. 253–264.

[6] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, "The (in)completeness of the Observed Internet AS-level Structure," *IEEE ACM ToN*, vol. 18, no. 1, pp. 109–122, 2010.

[7] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, "10 Lessons from 10 Years of Measuring and Modeling the Internet's Autonomous Systems," *IEEE JSAC*, vol. 29, no. 9, pp. 1810–1821, 2011.

[8] E. Gregori, A. Improta, L. Lenzini, and C. Orsini, "The Impact of IXPs on the AS-level Topology Structure of the Internet," *Computer Communications*, vol. 34, no. 1, pp. 68–82, 2011.

[9] 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 ToN*, vol. 17, no. 2, pp. 391–404, 2009.

[10] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: mapped?" in *Proc. of ACM SIGCOMM IMC*, 2009, pp. 336–349.

[11] N. Chatzis, G. Smaragdakis, J. Böttger, T. Krenc, and A. Feldmann, "On the Benefits of Using a Large IXP As an Internet Vantage Point," in *Proc. of ACM SIGCOMM IMC*, 2013, pp. 333–346.

[12] H. Chang, R. Govindan, S. Jamin, S. Shenker, and W. Willinger, "Towards Capturing Representative AS-level Internet Topologies," *Computer Networks*, vol. 44, no. 6, pp. 737–755, 2004.

[13] K. Chen, C. Hu, W. Zhang, Y. Chen, and B. Liu, "On the Eyeshots of BGP Vantage Points," in *Proc. of IEEE GLOBECOM*, 2009, pp. 1–6.

[14] A. Lakhina, J. W. Byers, M. Crovella, and P. Xie, "Sampling Biases in IP Topology Measurements," in *Proc. of INFOCOM*, 2003, pp. 332–341.

[15] D. Achlioptas, A. Clauset, D. Kempe, and C. Moore, "On the Bias of Traceroute Sampling: or, Power-law Degree Distributions in Regular Graphs," in *Proc. of ACM STOC*, 2005, pp. 694–703.

[16] K. Chen, D. R. Choffnes, R. Potharaju, Y. Chen, F. E. Bustamante, D. Pei, and Y. Zhao, "Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes from P2P Users," in *Proc. of ACM SIGCOMM CoNEXT*, 2009, pp. 217–228.

[17] H. Haddadi, D. Fay, S. Uhlig, A. Moore, R. Mortier, and A. Jamakovic, *Mixing Biases: Structural Changes in the AS Topology Evolution*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, vol. 6003, pp. 32–45.

[18] Y. Shavitt and U. Weinsberg, "Quantifying the Importance of Vantage Points Distribution in Internet Topology Measurements," in *Proc. of IEEE INFOCOM*, 2009, pp. 792–800.

[19] R. Bush, O. Maennel, M. Roughan, and S. Uhlig, "Internet optometry: Assessing the broken glasses in internet reachability," in *Proc. of ACM SIGCOMM IMC*, 2009, pp. 242–253.

[20] P. Marchetta, W. de Donato, and A. Pescapé, "Detecting Third-Party Addresses in Traceroute Traces with IP Timestamp Option," in *Proc. of PAM*, 2013, pp. 21–30.

[21] Y. Zhang, R. Oliveira, H. Zhang, and L. Zhang, "Quantifying the pitfalls of traceroute in as connectivity inference," in *Proc. of PAM*, 2010, pp. 91–100.

[22] M. A. Sánchez, J. S. Otto, Z. S. Bischof, D. R. Choffnes, F. E. Bustamante, B. Krishnamurthy, and W. Willinger, "Dasu: Pushing Experiments to the Internet's Edge," in *Proc. of USENIX NSDI'13*, 2013, pp. 487–500.

[23] D. R. Choffnes and F. E. Bustamante, "Taming the Torrent: a Practical Approach to Reducing Cross-ISP Traffic in Peer-to-Peer Systems," in *Proc. of ACM SIGCOMM*, 2008, pp. 363–374.

[24] K. Claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov, "Internet Mapping: From Art to Science," in *Proc. of CATCH*, 2009, pp. 205–211.

[25] M. Luckie, "Scamper: A Scalable and Extensible Packet Prober for Active Measurement of the Internet," in *Proc. ACM SIGCOMM IMC*, 2010, pp. 239–245.

[26] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira, "Avoiding Traceroute Anomalies with Paris Traceroute," in *Proc. of ACM SIGCOMM IMC*, 2006, pp. 153–158.

[27] Y. Shavitt and E. Shir, "DIMES: Let the Internet Measure Itself," *SIGCOMM CCR*, vol. 35, no. 5, pp. 71–74, 2005.

[28] "Isolario," http://www.isolario.it.

[29] A. Faggiani, E. Gregori, L. Lenzini, S. Mainardi, and A. Vecchio, "On the Feasibility of Measuring the Internet through Smartphone-based Crowdsourcing," in *Proc. of WiOpt*, 2012, pp. 318–323.

[30] E. Gregori, L. Lenzini, V. Luconi, and A. Vecchio, "Sensing the Internet through Crowdsourcing," in *Proc. of IEEE PerMoby*, 2013, pp. 248–254.

[31] B. Augustin, T. Friedman, and R. Teixeira, "Measuring Load-balanced Paths in the Internet," in *Proc. ACM SIGCOMM IMC*, 2007, pp. 149–160.

[32] "RIPE Atlas," https://atlas.ripe.net/.

[33] "Maxmind GeoLite Database," http://dev.maxmind.com/geoip/geolite.

[34] E. Gregori, A. Improta, L. Lenzini, L. Rossi, and L. Sani, "Discovering the geographic properties of the Internet AS-level topology," *Networking Science*, vol. 3, no. 1-4, pp. 34–42, 2013.

[35] W. Shakespeare, "The Merchant of Venice," Act II - Scene VII - Prince of Morocco, 1596 (supposed).

[36] L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE ACM ToN*, vol. 9, no. 6, pp. 733–745, 2001.

[37] G. L. Nemhauser and L. A. Wolsey, *Integer and combinatorial optimization*. New York, NY, USA: Wiley-Interscience, 1988.

[38] E. Gregori, A. Improta, L. Lenzini, L. Rossi, and L. Sani, "Improving the Reliability of Inter-AS Economic Inferences Through a Hygiene Phase on BGP Data," *Computer Networks*, vol. 62, pp. 197–207, 2014.

[39] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. Claffy, "AS Relationships, Customer Cones, and Validation," in *Proc. of ACM SIGCOMM IMC*, 2013, pp. 243–256.

[40] "Global Internet Phenomena Report: 2H 2013," https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report-pdf.pdf.