Improving the Discovery of IXP Peering Links through Passive BGP Measurements

Vasileios Giotsas, Shi Zhou
Department of Computer Science
University College London
Email: v.giotsas, s.zhou@cs.ucl.ac.uk

***Abstract*—The Internet Autonomous System (AS) topology has important implications on end-to-end routing, network economics and security. Despite the significance of the AS topology research, it has not been possible to collect a complete map of the AS interconnections due to the difficulties involved in discovering peering links. The problem of topology incompleteness is amplified by the increasing popularity of Internet eXchange Points (IXPs) and the "flattening" AS hierarchy. A recent study discovered that the number of missing peering links at a single IXP is larger than the total number of the observable peering links. As a result a large body of research focuses on measurement techniques that can alleviate the incompleteness problem. Most of these proposals require the deployment of additional BGP vantage points and traceroute monitors. In this paper we propose a new measurement methodology for improving the discovery of hidden peering links through the publicly available BGP data. Our approach utilizes the traffic engineering BGP Communities used by IXPs' Route Servers to implement multi-lateral peering agreements. We are able to discover 36K additional p2p links from 11 large IXPs. The discovered links are not only invisible to public BGP data, but also 97% of those links are invisible to traceroute data from CAIDA's Ark and DIMES projects for June 2012. The advantages of the proposed technique are threefold. First, it provides a new source of previously hidden p2p links. Second, it does not require changes in the existing measurement infrastructure. Finally, it offers a new source of policy data regarding multilateral peering links at IXPs.**

***Index Terms*—BGP, Internet, Autonomous Systems, BGP, measurement, inter-domain, routing, IXP, topology, missing links.**

I. Introduction

The Internet inter-domain routing infrastructure is composed by self-organized networks of routers called Autonomous System (AS). The de-facto protocol for inter-domain routing is the Border Gateway Protocol (BGP), and it is probably the most critical piece of the Internet infrastructure that glues the whole Internet together. The AS topology has important implications on the performance, security and quality-of-service of overlay protocols and applications, and has therefore attracted significant research interest from a variety of disciplines. In the last two decades there has been a great effort in collecting and studying the Internet topology at the AS level. A number of topology datasets were collected, various topological properties were discovered and a number of network models were proposed [1], [2], [3].

Despite the extensive research, many of the findings have been characterized as controversial due to the widely documented incompleteness of the existing topology datasets [4], [5], [6], [7], [8], [9]. The most widely-used methodologies for compiling the AS graph utilize either public BGP feeds or traceroute monitors. The incompleteness problem emanates mainly from the inability of those data sources to capture a number of peer-to-peer AS links due to the restrictions imposed on their propagation. The incompleteness problem is amplified by the increasing popularity of the Internet eXchange Points (IXPs) as a paradigm for the establishment of peering interconnections. Two recent studies on IXP peerings provided evidence that the amount of missing links may lie in a range from 50% to more than 100% of the visible AS links based on public BGP and traceroute data [10], [11]. To address this problem a number measurements methodologies have been proposed or deployed. These proposals include new approaches for the placement of the BGP vantage points [12], [13], [14], aggressive deployment of traceroute monitors at the edge of the network through crowd-sourcing [8], [15], and the combination of different data sources including Internet Routing Registries (IRRs) and looking glass servers [16], [17], [18], [10].

In this paper we propose a new measurement methodology to improve the discovery of invisible AS peerings from publicly available BGP data. Our approach is based on inferring IXP peerings over Route Servers which are used to implement multilateral peerings. The default behavior of Route Servers is to advertise everything they learn to all the connected networks, but many IXPs allow to its members to control how their prefixes are advertised by using a set of special-purpose BGP Community values. We implement an algorithm to mine these Community values and extract the Route Server participants and their export policies for 11 IXPs. By combining these data we are able to infer more than 36K peer-to-peer links which are not visible in the BGP AS paths. We exhibit the correctness of the inferred links by evaluating them against connectivity information obtained through hundreds of traceroute and looking glass servers.

The proposed link discovery methodology has three main advantages: (i) It unveils a large number of hidden IXP peer-to-peer links that are not visible to other available topology datasets. IRR records do not register the peerings with the Route Server members but only with the Route Server. Moreover, only 1062 of the discovered links are included in the topology information obtained from CAIDA's Ark and DIMES. Therefore, our methodology is complementary

and not overlapping to the other sources of AS topology information. (ii) It works on the existing sources of BGP data (i.e. RouteViews, RIPE RIS, PCH) and it can be easily reproduced without requiring the deployment of additional equipment. Moreover, our approach can help to reduce the cost of active measurement methodologies dedicated in the discovery of IXP peering, or help in achieving better-targeted probing (iii) In addition to link discover, our approach provides a new data source in IXP peering policies, and how IXP members select their peering partners in Multilateral Peering Agreements (MLPA).

The rest of the paper is organized as follows: Section II provides the background information and related works. Section III introduces our measurement methodology. Section IV presents our results and validation efforts. Finally, Section V concludes.

II. Background

A. Inter-domain Routing

A network of routers under the same administrative entity is called an Autonomous System (AS) and comprises a routing domain. Each AS is identified by a unique 32-bit number (ASN) and has been assigned with one or more IP address blocks (IP prefixes). The ASs are autonomous in the sense that they can independently decide which Interior Gateway Protocol (IGP) will be used for routing inside their own domains. To achieve global reachability ASes should interconnect and exchange prefix reachability information among each other. The de-facto protocol for inter-domain routing today is the Border Gateway Protocol (BGP). In inter-domain routing connectivity does not imply reachability, which is fundamentally determined by the routing policies specified by the AS operators. These policies depend largely on the business relationships agreed by the ASes upon the establishment of their links. The AS business relationships define the economics of routing and have been coarsely divided into three categories. A customer-to-provider (c2p) relationship is established when an AS (customer) pays a better-connected AS (provider) to transit traffic to the rest of the Internet. A peer-to-peer (p2p) relationship is agreed when two ASes exchange traffic only between themselves and their customers to minimize the costs of sending traffic through their providers. Finally, a sibling relationship expresses the connection between ASes under the same organization, which can freely exchange traffic without cost or routing restrictions.

BGP routes are usually exported following the so-called *valley-free* rule [19], i.e. a customer route can be exported to any neighbor, but a route from a peer or a provider can only be exported to customers. Hence, a path (a series of adjacent AS links) is valley-free if it complies with one of the following patterns[1]: (1) $n\times$c2p + $m\times$p2c; or (2) $n\times$c2p + p2p + $m\times$p2c; where n and m ≥ 0. The valley-free rule describes a typical routing path that is valid for inter-domain routing. Most valid routing paths are valley-free because they comply with the business interest of ASes, i.e. to minimize operation cost and maximize revenue. It should be noted that the valley-free rule is not an enforcement rule. It is observed that a small number of routing paths do not follow this rule, either because of policy misconfigurations [20], or due to the complexity of some AS relationships which is not captured by the simple customer/peer/sibling model [21].

B. AS Topology Data Sources

The most widely used sources of AS topology data are the BGP Route Monitors, such as RouteViews, RIPE RIS, Packet Clearing House and the Abilene Observatory. These projects connect to a number of ASes and passively collect feeds of BGP table dumps and updates. Each table and update entry include an AS Path attribute that corresponds to the list of ASes that should be traversed to reach the an IP prefix. The AS path is the primary source of AS adjacencies and it is generally considered as a reliable source in terms of false positives. BGP misconfigurations or route hijacks may introduce artificial links that are usually filtered based on the lifetime of an AS path, assuming that such phenomena are short-lived [9]. Other sources of BGP data include looking glass servers that allow the remote execution of non-privileged BGP commands through a web interface or remote login. There are more than 1,000 available looking glass servers[2] but in the general case querying using automated tools is prohibited, and typically they are used in one-off studies and not for the periodical collection data.

A second popular source of topology information is the IP-level paths collected through globally distributed traceroute monitors that actively probe a list of IP addresses. AS links can be obtained by mapping the collected IP addresses to ASNs. However, such mapping is non-trivial and can produce considerable artifacts [22]. Finally, the Internet Routing Registry (IRR) is a publicly accessible database where AS administrators voluntarily and manually register routing information. IRR data are frequently inaccurate, incomplete or intentionally false, although certain databases - notably RIPE - are significantly more reliable. It has been shown that with the proper filtering techniques IRR can provide a useful source of topology data [23], [24]. More topology data sources exist (e.g. syslogs) but they are usually proprietary and not available to the research community.

C. The Topology Incompleteness Problem

The most significant limitation of the existing BGP collection projects is the large number of missing links. Missing links have been categorized to two types, *hidden* and *invisible* [25]. Hidden links are usually backup c2p links that can be observable by a set of BGP monitors if the preferred path towards a prefix changes. On the other hand, invisible links are impossible to be observed because of the number and placement of the BGP monitors. Invisible links are typically of

[1]The sibling links can be found in any position of the path without changing the valley-free property.

[2]Updated lists of looking glass servers can be founded in the traceroute.org and peeringdb.org websites.

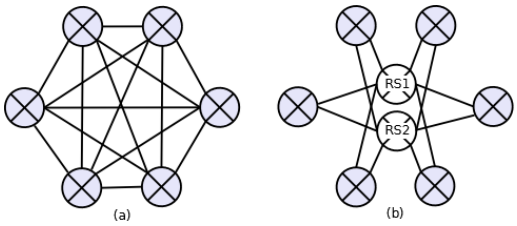

Fig. 1. Bi-lateral (a) vs Multi-lateral (b) peering for a full-mesh connection between 6 ASes. In bi-lateral peering $n \cdot (n-1)/2$ BGP sessions would be required. MLP would require only n sessions with the Route Server, or $2n$ when two Route Servers are used for redundancy.

p2p type and they cannot be observed due to the propagation restrictions of the valley-free rule. Invisible p2p links consist the majority of missing links, and are mostly located in the periphery of the AS graph [7], [9]. BGP feeds are mostly provided by high-tier ASes which often overlap, while some geographic areas are very poorly covered. Even worse, many BGP feeders treat their connection with the monitors as a p2p link and they advertise only prefixes learned from their customers. Therefore, a better placement of the BGP monitors can help towards mitigating the incompleteness problem [12], [13], [14]. However, BGP feeders participate voluntarily in these projects while some may not wish to share their BGP data. Hence, it is difficult to design an optimal BGP route collection infrastructure.

The traceroute paths have similar problems with BGP measurements in terms of missing links, but it is considerably easier to deploy traceroute monitors even to personal computers. Highly distributed traceroute monitoring infrastructures [15], [8] is a very promising approach to optimize the discovery of invisible AS links. While these efforts improve the accuracy of the collected AS topologies, it has not been possible yet to obtain a complete map.

A critical component of the AS ecosystem is the Inernet eXchange Points (IXPs) substrate, that provide a physical infrastructure to facilitate connectivity between ASes. IXPs provide an attractive and cost-effective peering platform, especially for small and medium-sized ASes that want to openly peer without having to establish multiple point-to-point links. There has been evidence that the discovery of p2p links in IXPs is the key towards obtaining complete AS connectivity maps [18]. This hypothesis has been confirmed by a 2009 Internet-wide traceroute study that specifically targeted the discovery of IXP peerings [10]. In total, about 58K IXP peering were discovered, of which almost 44K where not visible in any public dataset including traceroute data from CAIDA's Ark and DIMES. Ager et.al. presented the most recent in-depth study of a large IXP using sFlow traffic data collected at the IXP's infrastructure [11]. Their analysis revealed that the peering fabric is much richer than previously estimated. In that single IXP alone there were discovered 50K p2p links, about 10K more compared to the public BGP data of the same period.

Despite the importance of the techniques presented in [10], [18] for the discovery of IXP links, they have not been regularly repeated to provide periodical data. The main reason is the cost involved in conducting large-scale targeted traceroute measurements in terms of time and number of queries. Also, the use of looking glass servers is highly constrained and not appropriate for being used as a regular measurement platform [26], while sFlow data used in [11] are private and normally not available to the broader research community.

TABLE I
PATTERNS OF BGP COMMUNITIES FOR THE CONTROL OF ROUTE ANNOUNCEMENT TO THE MEMBERS OF A ROUTE SERVER

Community	Action
rs-asn:rs-asn	Announcement of route to all peers (Open)
rs-asn:peer-asn	Announcement of route to peer-asn (Exclude)
0:rs-asn	Block announcement of route to all peers (Restrictive)
0:peer-asn	Block route announcement to peer-asn (Include)

III. FRAMEWORK FOR DISCOVERING MISSING IXP LINKS

From the analysis in section II-C it can be understood that unearthing IXP links can be decisive towards obtaining complete AS topologies. At the same time, the cost of a measurement methodology should be kept low in order to allow the periodical execution of the measurements. Towards this direction we present in this section a framework for discovering invisible IXP peering links through public BGP data. This is achieved by mining the connectivity and reachability data used to establish Multilateral Peering (MLP) agreements.

A. Multilateral Peering Agreements

An increasing number IXPs offer two interconnection paradigms, bi-lateral and multi-lateral peering. In bi-lateral agreements, for every peering a new BGP session should be established. This approach has scalability problems in the case of large IXPs where most of the participants have an open peering policy and wish to maximize their peering connections. Indeed, in [11] it was reported that more than 50K peerings were established in a single IXP due to the dense connectivity among tier-2 and leaf ASes. Managing a separate BGP session for each peer router can involve considerable overhead. MLP offers a scalable way to support dense peering interconnections. Instead of establishing direct BGP sessions among them, MLP participants connect with one or more Route Servers (figure 1). A Route Server reflects the BGP routes learned from one participant to all the other participants, without changing the BGP attributes and without forwarding any traffic. Peerings over a Route Server can happen even if the traffic requirements are not met. For example, Google (AS15169) requires at least 100Mbps peak traffic to establish a bi-lateral peering, but networks with less than 100Mbps traffic are invited to peer in any European IXP Route Server[3]. Although connection to Route Servers is not mandatory, usually a large percentage of IXPs' participants

[3]https://peering.google.com/about/peering_policy.html

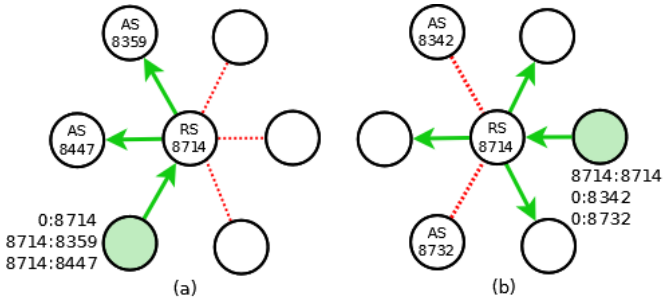

Fig. 2. Control of route advertisements in a Route Server using BGP Communities

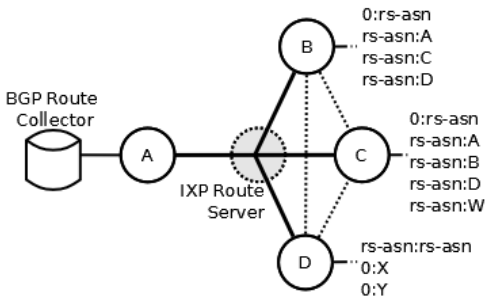

Fig. 3. Discovery of missing Route Server peerings through the use of BGP Communities.

opt in. AMS-IX reports that about 77% of its participants also connect to its Route Servers [4].

BGP routes sent to a Route Server are by default advertised to all the connected networks. However, Route Server participants can apply inbound and outbound filtering to control which networks receive their routes. Such filtering mechanisms are essential for IXP participants because even ASes with very open routing policy may not wish to peer with everybody. The are several techniques to implement policy filters, but the most popular practice is through the use of Communities, an optional 32-bit BGP attribute used to encode additional information on a BGP route [27]. The values of BGP Communities are not standardized, but the majority of IXPs follow a common format presented in Table I.

To better understand how these Communities are used to control the announcement of routes consider the example presented in figure 2 for a Route Server with rs-asn 8714. When a path is advertised with the Communities `0:8714 8714:8359 8714:8447`, the Route Server will advertise this route only to AS8359 and AS8447. If the Communities `8714:8714 0:8342 0:8732` are applied on a BGP path, the Route Server will advertise it to all the connected networks except AS8342 and AS8732. Note that the applied Communities are either *Open + Exclude*, or *Restrictive + Include*.

Therefore, two ASes can have a peering over a Route Server if two requirements are satisfied. First, *connectivity* which is enabled by establishing a session with the Route Server. Second, *reachability* which is enabled by configuring the appropriate outbound filters using BGP Communities (when Communities are used for advertisement control) and inbound AS-PATH filters.

B. Discovering MLP Links

The key towards discovering MLP peerings is to find the BGP Communities used for advertisement control in Route Servers (*RS Communities*). The BGP Communities is a transitive attribute that can be propagated along an AS path. If at least one Route Server participant (or one of its customers) provides a BGP feed to a route collector it is possible to obtain the RS Communities for a number of IXP participants and infer a large number of missing links.

[4]https://www.ams-ix.net/connected_parties

Before we explain in detail the algorithm consider the example illustrated in Figure 3; assume that A, B, C and D are four ASes connected to the same IXP Route Server (among other ASes). Also, assume that these four ASes have a mesh connectivity over the Route Server. If A peers with a BGP route collector it will advertise the paths learned from B, C and D which are the visible p2p links. The links that do not involve A will be invisible. Although we know that B, C and D connect to the same Route Server, we do not know if they peer or not. However, these paths will be accompanied by the RS Communities that B, C and D have applied and provide the reachability information. By processing these RS Communities we can infer that B asks the Route Server to advertise its routes to A, C and D, while D allows its routes to be advertised to any peer connected to the Route Server except X and Y. By combining these data we can infer the existence of a p2p link between B and D, since both the connectivity and reachability requirements are met. Even if we have only one BGP feeder from an IXP, if this feeder is densely connected we can obtain the RS Communities for a large number of a Route Server's participants.

To implement the above measurement methodology we need a list of the participants in IXPs' Route Servers. We obtain this list either directly through the websites of the IXPs or from PeeringDB, a popular database for the sharing of peering information [28]. These sources have been found to be reliable and up-to-date [18].

Based on the above intuition, we discover the missing links according to the following steps:

1) For every BGP record we parse the Communities attribute to extract the values that indicate Route Server policies. We determine the IXP based on the first 16 bits of those Community values that encode the ASN of the Route Server.
2) When a set of RS Communities has been identified, we parse the AS path to pin-point the AS that applied these Communities (Setter). We check every AS in the path against the list of the IXP's participants. We distinguish the following cases:
   a) If the AS path contains less than two IXP participants we cannot pin-point the Setter.
   b) If the AS path contains two IXP participants, we

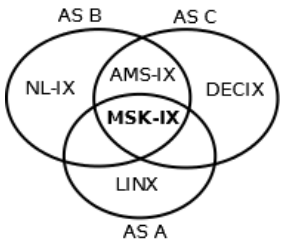

Fig. 4. Cross examination of the excluded ASes can help us determine the IXP to which the exclusion RS Communities pertain.

identify as the Setter the AS closer to the IP prefix.

c) If the AS path contains more than two IXP participants, we need to determine which two have a p2p relationship (normally only one p2p relationship should be observed in an AS path, as explained in II-A). For this purpose we use the AS relationships from [29] which have been shown to be the most accurate. After we find the IXP participants with the p2p relationship, we identify as Setter the AS whose position in the path is closer to the prefix.

3) For the Setter AS we construct a list A containing the Route Server participants to which its routes are advertised. We have two cases depending on the type of the RS Communities:
   a) *Open + Exclude*: $A = P - E$, where P is the list of all the IXP participants and C is the list of the IXP participants excluded by the RS Communities, with $C \subset P$.
   b) *Restrictive + Include*: $A = I$, where I is the list of IXP participants included by the RS Communities, with $I \subset P$.
4) For a pair of Setter ASes (s, s') we infer a peering link if $s \in A(s')$ and $s' \in A(s)$.

For many Route Servers the "advertise to all" BGP Community has essentially no effect since this is the default operation. When implementing an Open peering policy the `rs-asn:rs-asn` Community may be omitted. Instead, the RS Communities may contain only the array of *Exclude* values of type `0:peer-asn` which makes it difficult to determine the IXP as described in step 1. We can still determine the IXP by examining the IXPs to which the excluded ASes participate. Each AS can participate in many IXPs, but cross-examination of all the excluded IXPs can help us nail-down the candidate IXPs to only one. Figure 4 illustrates this approach for an array of Exclude Community values `0:A 0:B 0:C`.

IV. Results and Validation

We accumulate daily BGP table dumps and update messages from the RouteViews and RIPE RIS Repositories from 1 - 30 June 2012. We filter out (1) the reserved and private AS numbers (i.e. 23456 and 56320 – 65535) that should not appear in normal BGP advertisements and (2) path cycles that result from misconfiguration. Misconfigurations can also happen in setting the Community values. Typically such errors are transient and to avoid them we use only paths that appear for 7 consecutive days or more. We also collect BGP Communities data for 11 large IXP Route Servers from their websites or their IRR records.

TABLE II
Results for the discovery of invisible MLP links per IXP.

IXP Name	IXP Feeders	RS Comm. Setters	# Links
EQUINIX(all)	46	155	10870
DE-CIX	50	132	7127
LINX	47	120	5856
AMS-IX	47	110	4912
France-IX	11	101	4544
MSK-IX	11	43	722
ECIX	5	38	572
LONAP	4	33	419
STHIX	3	26	290
SFINX	7	21	188
TOP-IX	7	21	175

Table II presents the results of our algorithm. The IXP Feeders column corresponds to the ASs A of Figure 3. If a link exists in more than one IXPs it is reported only once for the larger IXP. In total we discover 35,675 invisible p2p links among 512 IXP participants. To put this number in context, for the same period there were 49,600 visible peering links to all the RouteViews and RIPE collectors while the number of total AS links was 128,368. Hence, our methodology revealed 73% additional peering links and 28% additional links in total. Interestingly, almost all the discovered p2p links are also invisible to the existing public sources of traceroute topology data, CAIDA's Ark and DIMES. Only 3% of the discovered links can be also obtained from these datasets. As explained in [10] these projects are not designed to discover peering links, thus they can miss a large number of IXP peerings.

A. Validation

To validate our link discovery framework we test the agreement of our dataset with connectivity information extracted from public Looking Glass (LG) servers. By querying the PeeringDB database we collected the address of 477 LG servers of which 203 are relevant to the discovered links. Relevant means that a LG offers an interface to the collectors of an AS that appears in our RS Communities Setters, or one of its customers. For every discovered link relevant to a particular LG server we examine its existence by querying the LG with the command `show ip bgp [prefix]` that outputs the contents of the BGP table for the specified IP prefix. We use four to six different prefixes to ensure that path diversity due to traffic engineering techniques will not cause our validation to miss existing links. In total we tested about 3K links, and for 94% of those we were able to validate their existence. We did not attempt to validate more links due to the restrictions in the usage of LG servers with automated tools. The links that were not validated does not mean that do not exist. Some LG servers have sessions with route collectors that are geographically distant from the IXP link we want to validate. Even if the IXP link exists it may serve local traffic

and for this reason be hidden from a distant route collector.

B. Limitations

Although we discover a large number of missing links our methodology is not a complete solution to the incompleteness problem. From the results in Table II we can see that for DE-CIX we discovered about 7K links while it is known that more than 50K links exists [11][5]. However there is no single source of topological data that can provide a complete topology. Hence, the effort for improving the accuracy of AS connectivity should rely on a combination of measurement methodologies and our study contributes towards this direction.

V. Conclusion

In this paper we present a new methodology for the discovery of invisible IXP p2p links. We focus on multilateral peering agreements established over IXP Route Servers, because the nature of these interconnections make possible their discovery through public BGP data. The proposed methodology is easily implemented and can be executed as often as required. In total we are able to discover 36K peering links which correspond to 73% additional peering links to those currently visible in the AS Paths of the public BGP data. More importantly, the majority of these links is not visible to IRR and the public traceroute datasets. Thus there is little overlap between our measurement methodology and the other existing sources of data. We validated our methodology using 203 BGP looking glass servers by comparing the connectivity information for 3K of the discovered links. About 94% of those links were cross-referenced exhibiting the correctness of the proposed methodology.

References

[1] B. Donnet and T. Friedman, "Internet topology discovery: A survey," *IEEE Communications Surveys and Tutorials*, vol. 9, no. 1-4, pp. 56–69, 2007.

[2] A. Dhamdhere and C. Dovrolis, "Twelve years in the evolution of the internet ecosystem," *Networking, IEEE/ACM Transactions on*, vol. PP, no. 99, p. 1, 2011.

[3] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, k. c. claffy, and A. Vahdat, "The internet AS-level topology: three data sources and one definitive metric," *SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 1, pp. 17–26, 2006.

[4] Q. Chen, H. Chang, R. Govindan, and S. Jamin, "The origin of power laws in internet topologies revisited," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, 2002, pp. 608 – 617 vol.2.

[5] A. Lakhina, J. Byers, M. Crovella, and P. Xie, "Sampling biases in IP topology measurements," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1, 30 2003, pp. 332 – 341 vol.1.

[6] R. Cohen and D. Raz, "The internet dark matter - on the missing links in the AS connectivity map," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April 2006, pp. 1 –12.

[7] M. Roughan, S. J. Tuke, and O. Maennel, "Bigfoot, sasquatch, the yeti and other missing links: what we don't know about the AS graph," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, ser. IMC '08. New York, NY, USA: ACM, 2008, pp. 325–330.

[5]The authors of [11] do not explicitly mention DE-CIX as the IXP they studied but it is understood according to the description provided.

[8] 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 *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, ser. CoNEXT '09. New York, NY, USA: ACM, 2009, pp. 217–228.

[9] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, "The (in)completeness of the observed internet AS-level structure," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 109–122, February 2010.

[10] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: mapped?" in *IMC '09: Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. New York, NY, USA: ACM, 2009, pp. 336–349.

[11] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a large European IXP," in *Proceedings of the ACM SIGCOMM 2012 conference*. New York, NY, USA: ACM, 2012, pp. 163–174.

[12] Y. Zhang, Z. Zhang, Z. M. Mao, C. Hu, and B. MacDowell Maggs, "On the impact of route monitor selection," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ser. IMC '07. New York, NY, USA: ACM, 2007, pp. 215–220.

[13] Y. Shavitt and U. Weinsberg, "Quantifying the importance of vantage points distribution in internet topology measurements," in *INFOCOM 2009, IEEE*, april 2009, pp. 792 –800.

[14] 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 *IMC '12: Proceedings of the 2012 ACM conference on Internet measurement conference*. New York, NY, USA: ACM, 2012, pp. 253–264.

[15] Y. Shavitt and E. Shir, "DIMES: let the internet measure itself," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 5, pp. 71–74, 2005.

[16] H. Chang, R. Govindan, S. Jamin, S. J. Shenker, and W. Willinger, "Towards capturing representative AS-level internet topologies," *Comput. Netw.*, vol. 44, no. 6, pp. 737–755, 2004.

[17] B. Zhang, R. Liu, D. Massey, and L. Zhang, "Collecting the internet AS-level topology," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 1, pp. 53–61, Jan. 2005.

[18] 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 Trans. Netw.*, vol. 17, no. 2, pp. 391–404, 2009.

[19] L. Gao and J. Rexford, "Stable internet routing without global coordination," *IEEE/ACM Trans. Netw.*, vol. 9, pp. 681–692, December 2001.

[20] S. Qiu, P. McDaniel, and F. Monrose, "Toward valley-free inter-domain routing," in *Communications, 2007. ICC '07. IEEE International Conference on*, 2007, pp. 2009 –2016.

[21] V. Giotsas and S. Zhou, "Valley-free violation in Internet routing: Analysis based on BGP Community data," in *Communications (ICC), 2012 IEEE International Conference on*, june 2012, pp. 1193 –1197.

[22] 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," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 9, pp. 1822 –1836, october 2011.

[23] G. Siganos and M. Faloutsos, "Analyzing bgp policies: methodology and tool," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 3, march 2004, pp. 1640 –1651 vol.3.

[24] G. D. Battista, T. Refice, and M. Rimondini, "How to extract BGP peering information from the internet routing registry," in *MineNet '06: Proceedings of the 2006 SIGCOMM workshop on Mining network data*. New York, NY, USA: ACM, 2006, pp. 317–322.

[25] R. V. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, "In search of the elusive ground truth: the internet's as-level connectivity structure," in *Proceedings of the 2008 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*. New York, NY, USA: ACM, 2008, pp. 217–228.

[26] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, "10 lessons from 10 years of measuring and modeling the internets autonomous systems," *Selected Areas in Communications, IEEE Journal on*, October 2011.

[27] B. Donnet and O. Bonaventure, "On BGP communities," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 55–59, 2008.

[28] "Peeringdb," http://www.peeringdb.com.

[29] "CAIDA AS Relationships," http://www.caida.org/data/active/as-relationships/.