Internet Topology Data Comparison

Bradley Huffaker, Marina Fomenkov, kc claffy
{bradley,marina,kc}@caida.org
CAIDA, University of California, San Diego*

ABSTRACT

Internet topology maps are an important tool for those who seek to describe, analyze, or model various aspects of the Internet's structure, behavior, and evolution. While different methods of measuring topology yield substantially different views of the Internet, many studies rely on only a single data source, sometimes outdated or incomplete, or mix fundamentally different data sources into a single topology. These compromises may undermine the fidelity of derived models and integrity of analysis results. We report on the results of our systematic comparison of Internet topologies derived from different data sources and characterizing the Internet at three granularities relevant to research as well as operations of network infrastructure: IP address (interface), router, and Autonomous System (AS).

1. INTRODUCTION

Topology maps of the Internet are indispensable for characterizing this critical infrastructure and understanding its properties, dynamics, and evolution. They are also vital for developing the theory of large-scale complex networks. These maps can be constructed for different layers (or granularities), e.g., fiber, IP address, router, Points-of-Presence (PoPs), autonomous system (AS), ISP/organization. Router-level and PoP-level topology maps can powerfully inform and calibrate vulnerability assessments. ISP-level topologies, sometimes called AS-level or interdomain routing topologies (although an ISP may own multiple ASes so an AS-level graph is a slightly finer granularity) provide insights into technical, economic, policy, and security needs of the largely unregulated peering ecosystem.

Over the last decade, many studies have focused on the structure of observable Internet topologies [19, 40, 16, 24, 20, 42] including considerable controversy over the quality of data and associated inferences [17, 28, 41]. Substantially different views of the Internet result from different methods of measuring topology. Relating particulars of measurements to artifacts and specifics of collected data is necessary for objective evaluation of the scope and the validity of the resulting Internet maps. In our 2006 study [32], we compared AS topology graphs generated from three different data sources: traceroute (using skitter, CAIDA's previous active measurement infrastructure), BGP (Routeviews), and IRR data (RIPE's WHOIS registry). Here we extend the scope of this comparative analysis to include two additional types of graphs (IP-interface and router level graphs) and five additional data sources (RIPE-RIS, Ark-IPv4-traceroute, iPlane, DIMES, and IRL). We provide what we believe is the most comprehensive systemic study thus far comparing and interpreting structural characteristics of topologies inferred from the best available data sources.

Section 2 describes our **data sources**. Section 3 defines the **metrics** we use for graph comparison. Section 4 discusses background and methodology for how we process the data to derive corresponding **Internet topology graphs** at three granularities: IP, router, and AS. Section 5 presents our comparative analaysis framed around the metrics described in Section 3. Section 6 summarizes key results.

2. DATA SOURCES

2.1 Traceroute data

Underpinning many Internet topology studies are data sets collected by traceroute-based measurements. Traceroute probing methodologies [7] infer the IP-level forward path through the network by sending a series of packets to the same destination, each with incrementing TTL values, and recording the IP addresses of the intermediate routers that return ICMP *time-exceeded* messages.[1] The most prevalent probing technique uses ICMP packets, although UDP- or TCP-based probing is also used [29]. Traceroute probing from multiple vantage points to many destinations reveals a multitude of IP interfaces and links between them. An *IP-interface* or *IP-level* graph results from merging the results of traceroute measurements across many vantage points (Section 4.1).

In order to construct a more realistic map of actual physical devices (routers) from this raw traceroute data, we must estimate which pairs (sets) of IP addresses in the traceroute

* Support for this work is provided by DHS N66001-08-C-2029 and NSF CNS-0958547.

[1] Sometimes the source IP address in these ICMP response packets is that of the outgoing interface for the return path rather than the interface on the forward path, but it is always an IP address on the router where the TTL expired.

	date	interval	type	graph level			vantage points		
				IP	Rtr	AS	points	ASes	ctries
DIMES	2011.04.04 - 2011.04.17	14 days	traceroute	X		X	947		
iPlane	2011.04.06 - 2011.04.20	15 days	traceroute	X	X	X	517	190	40
Ark IPv4 All Prefix /24	2011.04.01 - 2011.04.15	15 days	traceroute	X	X	X	54	54	29
RouteViews2	2011.01.16 - 2011.01.20	4 days	BGP			X	1	33	11
BGP Full	2011.01.16 - 2011.01.20	4 days	BGP			X	19	336	21
IRL	2011.04.01 - 2011.04.15	15 days	BGP			X	N/A[1]		
RIPE WHOIS	2009.04.20 - 2011.04.20	2 years	IRR			X	1	20,905	183

[1] The IRL documentation does not specify how many sources were in the dataset we used.

Table 1: Datasets listed by type, date, and derivable graphs.

paths belong to the same router, a process known as *IP address alias resolution*. A router by definition has at least two interfaces, with Internet core routers having possibly hundreds of interfaces. The process of alias resolution yields **router-level topology** (Section 4.2).

One can also create AS-level graphs from traceroute-derived IP-level data. The first step in this process is mapping IP addresses to ASes as follows. Each IP address belongs to an *address prefix* that is originally announced by an independent routing entity in the global routing system, called an *Autonomous System (AS)*. Converting IP-level data to an AS-level graph requires determining the origin AS for each prefix from BGP data, annotating each IP address with its origin AS, and inferring AS links corresponding to each traceroute-observed IP link. Alternatively, one can start with a router-level topology derived through alias resolution, annotate each router with the AS that owns it, and infer AS links corresponding to each link in the router-level topology. We describe AS graph construction in Section 4.4.

For this study we used traceroute data from three sources (see Table 1): **DIMES**, **iPlane**, and **Ark IPv4 All Prefix /24**. **DIMES** is a distributed scientific research project run by Tel Aviv University. Traceroute measurements are executed in parallel by volunteers who have deployed the netDIMES measurement software on their personal computers (1065 vantage points shown in Table 1, although we could not find out how many vantage points were active in the sub-interval we compared). **iPlane** is a topology collection research project run by the University of Washington on PlanetLab [3], a global network of academic research servers. During the interval we studied, there were 251 vantage points with 517 monitors, most vantage points having multiple monitors. **iPlane** constructs an annotated map of Internet topology focusing on "core" Internet backbones that contain most used paths. **Ark IPv4 All Prefix /24** is traceroute data collected by CAIDA's Ark [1] measurement infrastructure which, during the period used in this report, consisted of 54 dedicated PCs acting as vantage points and controlled by a central server at CAIDA. The Ark monitors attempt to probe a single random address in each globally routed IPv4 /24 prefix, with a complete cycle through the routed IPv4 address space taking approximately 48 hours.

2.2 BGP data for AS-level topologies

ASes use the **Border Gateway Protocol (BGP)** [34] to exchange routing information on the Internet. Each BGP-speaking router maintains a table of IP-prefix-to-AS mappings that designate reachability to ASes by describing a ”chain” or path vector of ASes. One can derive an AS-level graph of the Internet directly from this BGP data.

Two repository projects collect and archive BGP routing tables for research: Route Views [8] run by the University of Oregon and the Routing Information Service (RIS) collection provided by RIPE NCC [5]. Each peer contributes a BGP table that stores a set of routed IP prefixes and the computed best path from that peer to each prefix.

Our first source of BGP data for this study is the single Route Views server with the largest number of peers, **RouteViews2** (with 33 vantage points). The second source, **BGP Full**, is a combination of routing tables from 5 Route Views servers and 14 RIPE-NCC RIS servers, that is, all servers available on 1-14 January 2011 (19 vantage points). Creating a BGP-based AS-level graph using the maximum available number of collectors for a given time interval is the same method we use to produce the AS-level graphs underlying our AS-ranking project [2]. Our third source of BGP data is UCLA's Internet Research Lab (**IRL**) [10] compilation, which includes BGP data from Route Views, RIPE-NCC RIS, Packet Clearing House, traceroute.org, and the Looking Glass Wiki (http://www.bgp4.net/rs). The IRL documentation does not specify how many sources contributed to the dataset we used.

2.3 IRR Data for AS-level topologies

The Regional Internet Registries (RIR) support query access to their databases of Internet address assignment information via the WHOIS [18] query and response protocol. At least one RIR database (RIPE) stores voluntarily contributed and (sometimes) maintained routing policy information such as the set of announcements an AS accepts from its neighboring ASes. This information is useful for ISPs in the detection of AS invalid paths (i.e., paths that do not follow the advertised policies of the ASes in the path.) One can also build an AS-level graph of Internet connectivity from these

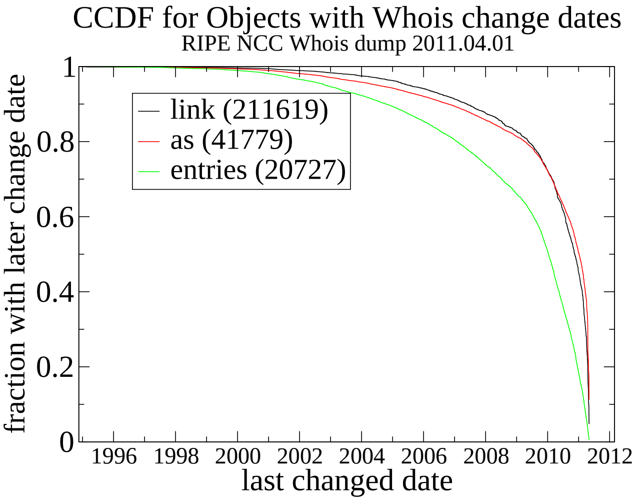


Figure 1: ***Statistics of entries in the RIPE NCC WHOIS database. The green line shows the fraction of records that have their changed field set to a value equal or more recent than the corresponding x value. The red line is the fraction of ASes and the black line is the fraction of AS links found in those ”changed after the given date” entries.***

AS links.

In 2004, Siganos and Faloutsos [38] analyzed the RIR databases and found that the RIPE NCC maintains the largest database with the most accurate topological information. They also found that only 28% of the ASes, almost all of them registered with the RIPE registry, had registered polices that were both internally consistent and consistent with observable Route Views BGP routing tables at the time of their analysis. We thus chose the RIPE NCC WHOIS database as the source of IRR data for an AS-level graph [11]. A major problem with this data source is that the WHOIS databases are manually and voluntarily maintained, with no requirement to update registered information. Thus many records are likely obsolete, and we must decide how to filter out stale or unreliable information.

We obtained the RIPE-NCC WHOIS database dump on 20 August 2011 and used the following approach to retain sufficiently fresh entries. A WHOIS record *changed* field typically shows the date a change was made, although it does not specify whether routing policy information was updated. But a recent date in the *changed* field at least means that somebody reviewed the entry then, increasing the likelihood that the routing policy information is still current. The green line in Figure 1 shows the fraction of records in RIPE-NCC's WHOIS database that have their *changed* date field set to a value equal to or greater than the date given on the x-axis. The red line shows the fraction of ASes and the black line shows the fraction of AS links (i.e., listed as peers of the recorded AS) found in those ”changed after the given date” entries.

The older the change date, the larger the fraction of ASes and AS links in these ASes' records that changed after this date. The inflection point is at about June 2009, with only 25% of ASes and AS links having change dates in the preceding 13 years vs. 75% in the following two years. Considering this tradeoff reasonable, we retained all entries with changed dates less than two years old as the data source for our analysis, which includes IRR connectivity data for 20,905 ASes (out of more than 39 thousand ASes total). Since database records only show links from each AS to its immediate neighbors, each AS acts as a vantage point (hence, 20,905 vantage points in Table 1) providing a local view of the network 1-hop away.

3. TOPOLOGICAL METRICS

We selected the following four basic statistical characteristics for comparison between available Internet topology graphs. Mahadevan *et al.* [31] showed that reproducing these metrics is sufficient to capture all essential topological characteristics of Internet AS- and router-level topologies.

Average Node Degree. The two most basic graph properties are the **number of nodes** n (also referred as **graph size**) and the **number of links** m. The ratio of links to nodes defines the **average node degree** $k = 2m/n$. Average node degree is the coarsest connectivity characteristic of a given topology. Networks with higher k are better connected on average and consequently, all other things equal, likely to be more efficient and robust, as well as potentially vulnerable, since diffusion of malware is also more efficient.

Degree Distribution. Let $n(k)$ be the number of nodes of degree k (k-degree nodes). The **node degree distribution** is the probability that a randomly selected node is k-degree: $P(k) = n(k)/n$. In this report we analyze and compare the complementary cumulative distribution function (CCDF) of node degree, which shows the fraction of nodes that have a a degree equal to or greater then the argument value. Most network researchers agree that the degree distribution $P(k)$ for the AS level graphs of the Internet follows a power law function $P(k) = k^{-\gamma}$ with exponent γ near 2 [19, 16, 24, 32]. We check whether this power-law approximation fits our data and report the values of the exponent γ.

Average Neighbor Degree. Let $a(i, k)$ be the average degree of the immediate neighbors of the i-th node of degree k. Then the **average neighbor degree** for degree k is the average for all nodes $i = 1...I_k$ with degree k: $a_{nn}(k) = \sum_{i=1}^{k} a(i, k)/n(k)$. The average neighbor degree is a summary statistic of the joint degree distribution. It shows whether ASes of a given degree preferentially connect to high- or low-degree ASes. In a full mesh graph, $a_{nn}(k)$ reaches its maximal possible value $n - 1$. Therefore, for uniform graph comparison we plot normalized values $a_{nn}(k)/(n - 1)$.

Clustering. Let $m_{nn}(k)$ be the average number of links between the neighbors of k-degree nodes. **Local clustering** is the ratio of this number to the maximum possible number of such links: $C(k) = 2m_{nn}(k)/(k - 1)$. If two neighbors of a node connect, then these three nodes together form a triangle (3-cycle). Therefore, by definition, local clustering is the average number of 3-cycles involving k-degree nodes. **Mean local clustering** is the average of $C(k)$ over all values of node degrees k : $\bar{C} = \sum C(k)P(k)$. Clustering expresses local robustness in the graph: the higher the local clustering of a node, the more interconnected are its neighbors, thus increasing path diversity locally around the node.

4. CONSTRUCTING INTERNET TOPOLOGY GRAPHS FROM THE AVAILABLE DATA

In this section we describe our procedures for construction topology graphs at the three analyzed granularities: IP, router, and AS. The data processing techniques are extensive and due to space constraints we refer the reader to the extended technical report version of this paper [14] for details, so that we can focus on analysis of the resulting graphs in this paper.

4.1 IP-level graphs

An Internet Protocol (IP) interface-level graph is constructed by extracting IP links directly from the traceroute output: two IP addresses are inferred to form a link if they were observed adjacent to each other in a traceroute output. The **DIMES** project does not publish the complete traceroute paths measured by the netDIMES clients, but rather extracts from these measurements a set of such inferred IP links, yielding an IP-level graph we will refer to as **DIMES IP**. In contrast, **iPlane** and **Ark IPv4 All Prefix /24** data include a complete set of observed IP forward paths. In order to obtain an IP-level graph from these data, a researcher has to parse the raw paths into IP links. Although it is conceptually straightforward to enumerate every pair of adjacent IP addresses in a collected path, the simplicity evaporates in the face of millions of real-world traceroutes. Raw paths may contain nonresponsive hops, loops, private [35] or bogon [6] addresses, and other irregularities. Different methods of handling these anomalies will induce different effects on the resulting topology. For example, a nonresponsive hop appears in a traceroute path when a router forwards packets, but does not generate a *time exceeded* message when it drops a packet. In this case, the resulting trace will have a gap between two known IP addresses on either side of the non-responding router. In traceroute output these hops are typically represented by an asterisk (“*”).

We used a simplified trace processing procedure to create the **Ark IPv4Pref IP** and **iPlane IP** graphs from the **Ark All Prefix /24** and **iPlane** data sets. For consistent comparision with the router-level graph and ground truth (Section 4.3), we ignore all responses from destinations and build a topology from transit addresses. If a repeated address appears in a path, we assume a loop and truncate the path just before the repeated address. We treat private addresses as nonresponsive (see Section 4.2.4), since they can not be uniquely mapped, and we discard IPs with no adjacent hops, since they add nothing to the resulting topology. After we process each trace, we generate IP links between the remaining adjacent hops with IP addresses, but create no links to or over nonresponsive hops.

4.2 Router-level graphs

4.2.1 *Related work on alias resolution techniques*

The process of mapping IP addresses to routers is known as alias resolution. A variety of techniques have been developed and implemented for this task. Here we briefly review the techniques relevant to processing the data sets in this study. A survey of other existing alias resolution techniques and implementations is available in [25].

The earliest alias resolution techniques, Mercator and Mercator-like ones [33, 21, 9, 36], attempt to identify aliases by sending a probe packet to an unused port on an interface and collecting the resulting error messages. Probing one interface and getting this error from a different interface is a strong suggestion that the two interfaces belong to the same router. However, when applied to Internet-scale topologies, this method generates a high rate of false positive alias pairs, for example due to middleboxes in the path responding [26].

Other techniques employ different properties of existing Internet protocols to resolve interfaces into routers. Ally [39] infers that two addresses are aliases if probe packets sent to them produce responses with increasing but appropriately proximate IP ID values, since the IP ID field increments with each packet sent from the router. RadarGun [15] further refined this technique by looking for similarities in IP ID time series collected from many addresses. Sherry [37] describes iPlane’s recent use of the IP prespecified timestamp option to infer aliases. *MIDAR*, CAIDA’s Monotonic ID-Based Alias Resolution tool [26], expanded on the IP velocity techniques of RadarGun by implementing an extremely precise ID comparison test based on monotonicity rather than proximity, integrating multiple probing methods from multiple vantage points, and employing a novel sliding-window probe scheduling algorithm that increased scalability to the Internet scale of millions of IP addresses.

APAR [22] and kapar [25] use sophisticated graph analysis techniques to infer subnets linking routers, and from that, aliases.

4.2.2 *Alias Resolution techniques applied to our compared data sets*

According to their 2005 paper [36], **DIMES** uses a Mercator-like technique [21] for alias resolution. Due to the high rate of false positives of this older method, we did not use the DIMES-provided alias resolution data in our comparisons.

iPlane implements a two-phased approach to alias resolution, first generating a list of alias candidate pairs and then testing them. It generates candidate pairs using a combination of Mercator-like [21] and APAR-like [22] techniques. It tests the resulting list of candidate pairs using additional probing and inferences based on similar IP-ID values (the Ally method [39]) and timestamp values [37]. Further details of the alias resolution methodology used by iPlane are available in [30] and [37].[2]

The resulting **iPlane** alias resolution data show which interfaces are inferred to be on the same router, but links between routers are not included. To create the router links for the **iPlane router** graph, we started with the **iPlane IP** graph and used **iPlane**'s router aliases to merge aliased IP nodes and corresponding links into router nodes and links.

To collapse IP addresses in **Ark IPv4 All Prefix /24** data into routers, we employed CAIDA's alias resolution tools *iffinder* [9], *kapar* [25], and *MIDAR* [26]. Router-level topologies produced from **Ark IPv4 All Prefix /24** traceroutes using combinations of the three tools are the core of the Internet Topology Data Kit (ITDK) datasets regularly released by CAIDA [12]. The process of constructing these ITDK topologies involves the following steps. First, *kapar* breaks the observed IP paths into IP links (Section 4.2.3), which become the input for further alias resolution measurements and analysis by *MIDAR* and *iffinder*. The result is a MIDAR-iffinder topology **Ark ITDK $\mathbf{R_{mi}}$**. *kapar* can also heuristically infer the set of IP addresses that belong to the same router, and the set of two or more routers on the same "IP link" (either a point-to-point link, or LAN, or shared medium with multiple attached IP addresses) producing a more-aggressively-inferred MIDAR-iffinder-kapar topology **Ark ITDK $\mathbf{R_{mik}}$**. We elucidate the differences between these topologies in Section 4.3.

4.2.3 kapar *processing of IP paths into IP links*

We refined the basic approach of extracting IP links from paths described for IP graphs (Section 4.1) to the two-phase procedure implemented in *kapar* for constructing router-level graphs, so that we more fairly compare the IP-level and router-level graphs.[3] The first phase involves cleaning and splitting IP paths into segments. Similar to the trace processing for IP-level graph construction, we ignore responses from the target destination, and treat private addresses as nonresponsive. We make more conservative choices with respect to removing potential loops and dealing with multiple responses at a given hop, to avoid false positives in alias resolution. To minimize the presence (and problem) of nonresponsive hops in traces, we discard 3-hop segments containing nonresponsive hops in the middle if we have a 2-hop segment with the same two edge IP addresses of the 3-hop segment.

In the second phase *kapar* infers IP links from the segments as follows. For each path segment (A, B), it postulates a link between the router (node) $R1$ containing interface A and the router $R2$ containing interface B, and assumes that unless $node\ R2$ is already linked to $node\ R1$, this link connects the interface B on $node\ R2$ and an *implied unknown interface ?* on $node\ R1$ $[A\ ?] \leftrightarrow [B]$. We use a construct called a *hyperlink* (or "link cloud") to represent connectivity between more then two nodes in the case of multiple non-aliased predecessors to an address (see Figure 3).

4.2.4 *Dealing with nonresponsive hops*

If there is no path that would resolve a triplet with a non-responsive hop in the middle, then we include the triplet into the final graph assuming a provisional placeholder node between the two known nodes. This approach allows us to maintain information about the connectivity without knowledge of the intermediate hop. Note that if a known node has more than one placeholder node as its immediate neighbor, then we cannot distinguish whether it is in reality a single nonresponsive node or a different nonresponsive node for each next hop observed in the traces. 7.8% of nodes (inferred routers) in our ITDK data set have only non-responding hops as neighbor(s). Some of these inferred routers could possibly further collapse into higher-degree routers with additional data that we do not have.

We considered three scenarios for dealing with inferred routers that have nonresponsive hops as neighbors, essentially assuming their adjacent missing connectivity as zero, one, or more than one unknown neighbors. Each scenario trades off accuracy and completeness of the resulting graph. Discussion and analysis of the effects of these three assumptions on the degree distribution of the inferred graphs are available in the technical report [14]. We concluded that the most consevative approach was to remove the links to missing neighbors altogether. Since 7.8% of nodes in the router-level graph had only nonresponsive neighbors, removing their links meant also removing these nodes from the graph.

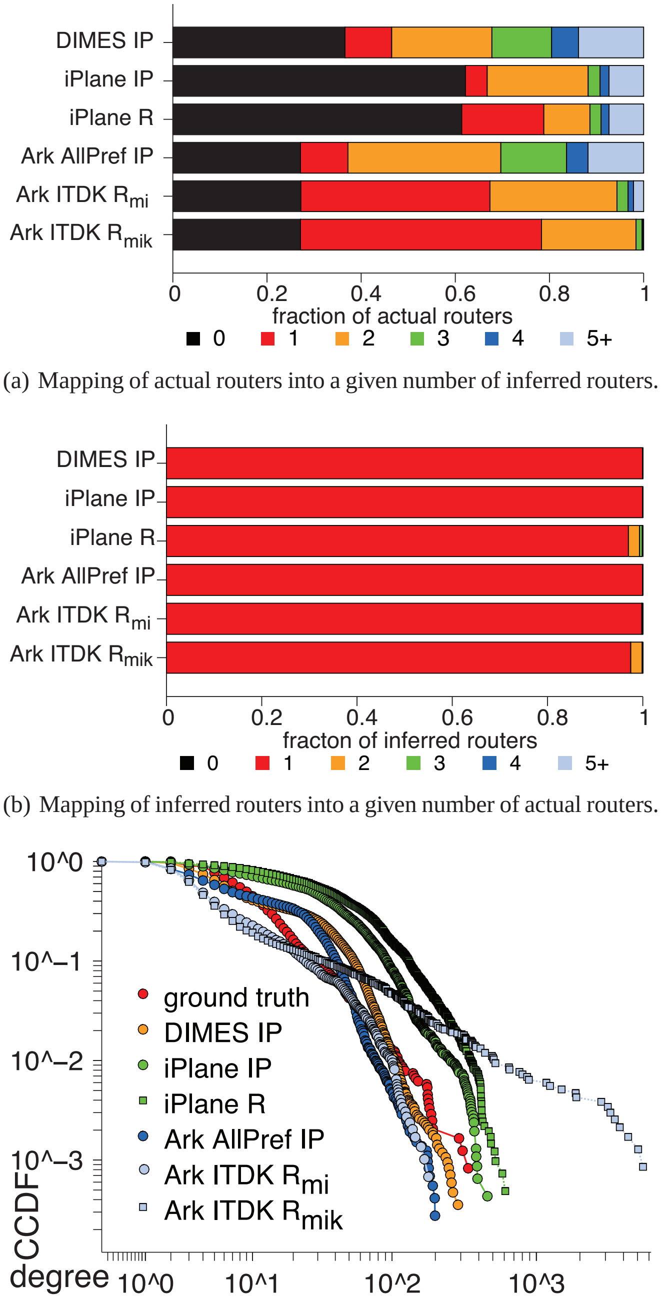
4.3 Comparison of IP- and router- level graphs with the ground truth

Since IP addresses in an IP-level graph represent interfaces on the actual routers, IP-level graphs are an approximation of what we ideally would like—a map of how each router is connected, identifying (the IP addresses of) as many IP interfaces on each router as possible. We compared all IP- and router-level graphs available for this study to a ground truth dataset provided by a Tier 1 ISP for their backbone AS (2420 routers). That ISP gave us a complete listing of the domain names of their core routers and the heuristic they use to map router interfaces into domain names. Unfortunately, this ground truth dataset does not indicate actual links between the routers, only the presence of interfaces on routers, making it impossible to assess the accuracy of clustering or average neighbor degree of the inferred topologies.

Figure 2(a) illustrates the coverage of each methodology, showing the fraction of real routers that: (i) could not be mapped to any router in the inferred topology (the black segments); (ii) is mapped to a single router (the red segments) - these are the correct answers that we seek to maximize; and (iii) is mapped to 2 or more routers (all other color segments) - the routers that are undercollapsed in the inferred topologies. The black segments are the shortest for

[2] The technical report [14] also expands on this process.

[3] We provide greater detail on the algorithm in the extended technical report [14]; a complete description of *kapar* is in [25].



(a) Mapping of actual routers into a given number of inferred routers.

(b) Mapping of inferred routers into a given number of actual routers.

(c) The CCDF of node degrees for each processing method and data source.

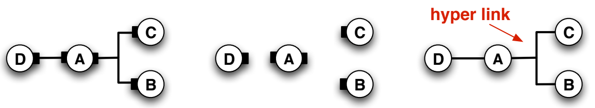
Figure 2: Comparison between a Tier 1 ISPs set of (2420) core routers and the corresponding inferred topologies derived from three traceroute datasets.

the topologies derived from the **Ark IPv4 All Prefix /24** dataset, which fails to capture 27% of this ISP's routers. The **DIMES** dataset misses 37% of the true routers for this ISP, and **iPlane** is the least complete at 62%. That Ark detected a larger fraction of the real topology's routers is somewhat suprising given that **Ark** has the fewest vantage points. We surmise that because each Ark monitor sends significantly more probes than the other platforms, it captures a larger number of IP addresses and, in turn, this larger view of the overall topology enables detection of a greater fraction of the ground truth routers.

The red segment of each bar shows the fraction of real routers that correctly had their interfaces mapped to a single router. It does not mean that the dataset captured every interface on a given router, only that all the interfaces captured did map to the same router. IP-level graphs treat every observed IP address as a separate router, which means a real router will be mapped to as many routers as it has IP interfaces. This inference is clearly wrong, as reflected by the short red segments in bars for all of the IP-level graphs in Figure 2(a): **DIMES IP**, **iPlane IP**, and **Ark IPv4Pref IP**. The process of resolving IP aliases (i.e., merging interface addresses) into common routers increases the fraction of correct one-to-one mappings. For the **iPlane** data, the fraction of real routers that map to a single inferred router increases from 4.6% in their IP-level graph to 17.4% in their router-level graph. For the router-level topologies in the Ark-derived ITDK, this fraction rises from 10% to 40% for the MIDAR-iffinder topology and to 51% in the MIDAR-iffinder-kapar topology.

At the same time, alias resolution can overcollapse routers by assigning interfaces from multiple distinct real routers to the same inferred router (i.e., a false positive). Figure 2(b) illustrates the prevalence of such false inferences for a single backbone ISP (with 2420 routers). Here the red segment of each bar shows the fraction of inferred routers that correctly contain only IP addresses from a single real router. Since IP level graphs always interpret a single IP address as a separate inferred router, for these graphs the red segments are trivially 100% by definition. **iPlane**'s alias resolution process creates falsely inferred routers for 3% of the real routers in this ISP's ground truth data. Alias resolution using MIDAR-iffinder results in a tiny fraction of false inferences (0.2% of the actual routers for this ISP), while MIDAR-iffinder-kapar processing overcollapses 2.6% of the ISP's actual routers. The fractions of false inferences in all router-level topologies seem small, but Figure 2(c) shows that they may have a dramatic effect on the resulting node degree distributions.

Canonically, a node degree is the number of neighbors connected to each node (see Figure 3, left column), but our ground truth data provides only the number of active interfaces on each router (Figure 3, center column). The presence of hyperlinks (described above) in a router-level graph can cause these two numbers to differ. The right column of Figure 3 shows the number of links attached to each node in our



	real graph (# of neighbors)	ground truth (# of interfaces)	router graph (# of links)
A	3	2	2
B	2	1	1
C	2	1	1
D	1	1	1

Figure 3: ***Degree inferred from different sources of data: the actual graph, the ground truth data (in the format) we were provided, and our inferred router-level graph. Our ground truth data does not provide the actual number of neighbors, but only the number of interfaces per router.***

inferred router-level graph, which more closely matches the number of interfaces in the ground truth data than it matches the number of neighbors in the actual graph. Therefore, to compare the inferred graphs with the ground truth data available to us (Figure 2(c)), we use the number of links rather then the number of neighbors. If we correctly infer the hyperlinks, the number of links and the number of interfaces should match, whereas counting the number of neighbors in the hyperlink (cloud) construct will overestimate the number of neighbors.

We first extract the set of routers from the inferred topology with at least one interface matching an interface in the ground truth data and compare (Figure 2(c)) the CCDFs of the number of links connecting to each such extracted router against the number of interfaces on a router in the ground truth data (the red symbols) as proxies for the CCDFs of node degree distributions. Both **iPlane-derived** graphs (the green symbols) significantly overestimate the number of routers (in this ISP) with degrees > 10: 40% in the ground truth data set vs. 70% and 74% in the **iPlane** topologies. The **DIMES IP** (the yellow circles) and the **Ark IPv4Pref IP** (the blue circles) topologies yield reasonable approximations of the degree distribution for the 60% of the ground truth routers that have degrees < 10, but begin to diverge for degrees between 10 and 60, which represents about 37% of routers in the ground truth data. The **DIMES IP** graph is the closest to the ground truth in the large degrees (> 100) range, but this range represents only 1% of the ground truth routers. DIMES' much larger number of edge vantage points will naturally capture a larger number of interfaces entering core routers from the periphery. Both ITDK-derived router-level topologies (the light blue diamonds and squares) underestimate the degrees of small degree (< 20) nodes, which is 84% of ground truth routers, yet the **Ark ITDK Router**$_{\textbf{mi}}$ topology that uses only MIDAR-iffinder processing (the light blue squares) matches the ground truth perfectly in the range of node degrees between 20 and 100, or 15% of our ground truth routers. In contrast, the MIDAR-iffinder-kapar topology (**Ark ITDK Router**$_{\textbf{mik}}$, the light blue diamonds) contains unrealistically super-high degree nodes that appear when two (or more) routers are merged into a single super-router: 4.6% of Ark **ITDK Router**$_{\textbf{mik}}$ routers have degrees > 100 vs. only 1.2% of the corresponding ground truth routers. Adding *kapar* inferences to the MIDAR-iffinder results increases the completeness of alias resolution (cf. Figure 2(a)), but this additional processing also overcollapses the routers (cf. 2(b)) skewing the node degree distribution toward unrealistically large degrees. To avoid the false positives and associated distorted statistics, we use the more conservatively-inferred **Ark ITDK Router**$_{\textbf{mi}}$ topology (publicly released as part of each ITDK package) in the rest of this report.

4.4 AS-level graphs

AS-level graphs represent the topology of the Internet at the level of Autonomous Systems (ASes), which are approximately network(s) under a single administrative control. ASes peer with each other to exchange traffic, and these peering relationships define the high-level global Internet topology. For the purposes of analysis, these peering relationships are represented with an AS graph, where nodes represent ASes and links represent peering relationships. This section focuses on the construction of AS-level graphs from three available data sources: raw traceroute data, BGP (Border Gateway Protocol) inter-AS routing table dumps, and RIPE's WHOIS routing registry database entries voluntarily contributed by some ISPs to RIPE's Internet Routing Registry (IRR).

4.4.1 Traceroute-based AS-level graphs

A typical starting point for constructing AS-level Internet topologies from traceroute data uses BGP table dumps from the Route Views Project [8] and RIPE-NCC RIS [5] to map IP addresses found in the collected traces to the origin ASes of their corresponding prefixes routable in the global routing system. A small percentage of IP prefixes maps to an *AS set*, i.e., a set of ASes any of which could be announcing the prefix. We leave the origin of those IP prefixes unresolved and discard such AS sets.[4] Some prefixes originate from multiple ASes, in which case we select the AS most frequently seen in the BGP tables as the origin AS. Out of 366,294 prefixes found in Routeviews BGP tables in the first half of April 2011 (the period of Ark data collection used in this report), 2,299 prefixes (0.6%) originated from AS sets, and 18 prefixes (0.005%) had multiple origin ASes.

Once we have a mapping between the IP address space and the AS space, the simplest method of constructing an AS-level graph entails mapping each IP address in the traces to its origin AS, and inferring AS links corresponding to observed IP links. We used this technique to generate the **iPlane AS** and the **Ark IPv4Pref AS** AS links files. We also used this method in our previous paper [32] comparing AS-level Internet topologies. Note that DIMES provides their own set of AS links **DIMES AS**, which we used directly.

For the **Ark ITDK Router**$_{\textbf{mi}}$ topology, we examined two

[4] IETF is in the process of deprecating AS sets [27].

methods to create AS-level Internet graphs: ***router-observed***, and ***router-inferred***. In both cases, the first step is to assign router ownership to ASes. Knowing the origin AS for each interface IP address on a given router, we assign the router to the AS that originates the most interface IP addresses. In the case of a tie between two ASes, we assign the router to the AS with the smallest degree. Further details of router-to-AS assignment algorithms are in [23].

Router-observed AS links. This method starts with the observed IP interfaces in the path, uses the alias resolution data to map these interfaces to routers, and then uses router-AS assignment data to map these routers to ASes [23]. This mapping results in an AS path, which we then split into AS links. We call the AS graph derived by this method **Ark ITDK AS$_{\mathbf{ro}}$**.

Router-inferred AS links. This method starts with the ITDK graph, uses the same router-AS assignment data as above to map these routers to ASes, resulting in an AS graph, which we then split into AS links. The conceptual distinction between the two methods is that an AS-graph constructed using the ***router-observed*** method contains only AS-links that correspond to IP links that were directly observed via measurement, while a graph constructed by the **router-inferred** method also includes links that were not actually output of the measurement process, but can be inferred from the router-level graph. We name this graph **Ark ITDK AS$_{\mathbf{ri}}$**.

Although we excluded the destination addresses when constructing IP- and router-level graphs (since these graphs focus on routers, not edge hosts), we retained these addresses when building AS-level graphs, for the following reason. Although the router just before the destination may be managed by the same AS as the destination, we often see only its provider-facing address in the collected traceroute output. In this case, retaining the destination address provides a way to capture additional AS connectivity; dropping the destination addresses would decrease the size of the resulting AS-level graph by 29%.

4.4.2 BGP-based AS-level graphs

In order to generate an AS-level graph from BGP data, we start with the AS paths found for each prefix and break these AS paths into individual AS links. We discard links that contain private ASes. For the **RouteViews2** and **BGP Full** data sets we collect a RIB on five consecutive days, and extract AS links only from the persistent paths (paths seen in the majority of RIB tables) during this interval.

The **IRL** data set used BGP data from active Route Views, Internet2 [13], RIPE RIS servers, and some looking glass servers (at bgp4.net), although the IRL documentation was not sufficient to explain exactly which parts of which data resources they were using.

4.4.3 WHOIS AS-level graph

To derive an AS-level graph from the **RIPE WHOIS IRR** data, we use the import and export fields that list ASes registered as BGP neighbors of a given AS (represented by its autonomous system number, or *aut-num* in the IRR record). We create links between the *aut-num*'s AS and the ASes listed in these import and export fields, excluding ASes that only appear as neighbors but do not have their own *aut-num* lines. Such ASes are external to the database and we cannot correctly estimate their topological properties (e.g., node degree). We also filter out private ASes.

5. STATISTICAL COMPARISON OF RESULTING INTERNET TOPOLOGY GRAPHS

5.1 IP- and Router- Level Graphs

Table 2 compares the basic statistics of three IP-level graphs and two router-level graphs. The number of links observed in the IP-level graphs **DIMES IP** and Ark IPv4Pref IP data are similar, with only 4% more links in **DIMES IP**, despite having 27% fewer nodes. The **iPlane IP** graph has only a fraction (11-15%) as many nodes and 40% as many links as the other two graphs. The smaller size of the **iPlane IP** graph is consistent with its focus on capturing only the Internet core topology, which also explains its larger average degree. The **iPlane IP** graph does have a smaller maximum node degree, perhaps because it has so many fewer nodes. The **iPlane IP** graph has an order of magnitude higher mean local clustering than the **Ark IPv4Pref IP graph**, but this disparity disappears after alias resolution: the **Ark IPv4Pref Router$_{\mathbf{mi}}$** graph has 13% higher mean local clustering than the **iPlane Router** graph. The **Ark ITDK Router$_{\mathbf{mi}}$** graph created by our alias resolution process has 23% less nodes and 31% less links than the corresponding IP level graph **Ark IPv4Pref IP**. In comparison, the iPlane alias resolution reduces the number of nodes in the **iPlane IP** graph by 7% and and the number of links by 8%. It appears that the alias resolution methods used by the **iPlane** project are less aggressive and/or efficient than CAIDA's *MIDAR/iffinder/kapar*.

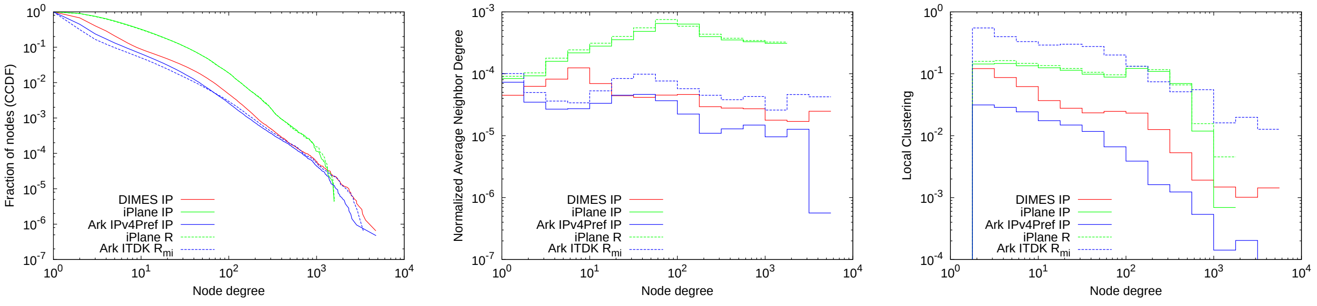
Figure 4(a) reveals that the node degree distribution in both **iPlane** graphs is skewed toward high-degree nodes: 30% of nodes have a degree larger than 10, compared to 10% or fewer for both Ark-derived (the blue lines) and the **DIMES IP** (the red line) graphs. We have already noted this effect in the ground truth comparison (cf. Figure 2(c)).

Figure 4(b) plots normalized average neighbor degrees. Unlike the degree distributions, which describe nodes in isolation, average neighbor degree captures how nodes of different degrees interconnect. We see two types of behavior. For both **iPlane** graphs, the average neighbor degree is initially increasing as the node degree increases, but high degree nodes $k > 100$ tend to connect to smaller degree nodes and the average neighbor degree decreases. The **DIMES IP** graph has similar behavior, but the average neighbor degree starts decreasing for $k > 10$. In contrast, the average neighbor degree remains nearly constant (within a factor of 3) for both **Ark**-derived graphs across all node degrees.

Considering local clustering as a function of node degree

	number of		degree		normalized avg avg	mean local
	nodes	edges	avg	max	neighbor degree	clustering
Ark IPv4Pref IP	2,111,019	4,073,080	3.860	4,772	5.53e-05	0.012
DIMES IP	1,543,320	4,230,578	5.480	4,742	6.31e-05	0.065
iPlane IP	233,996	1,661,041	14.200	1,586	2.16e-04	0.120
Ark ITDK Router$_{mi}$	1,633,126	2,729,618	3.340	3,439	8.48e-05	0.150
iPlane Router	218,399	1,531,736	14.030	1,600	2.38e-04	0.130

Table 2: Basic statistics of IP and router topology graphs.



(a) CCDF of Node Degree (b) Average Neighbor Degree (c) Local Clustering

Figure 4: ***Statistical characteristics of the IP- and router-level graphs.***

(Figure 4(c)), we notice the ITDK Router graph generally has the largest clustering, followed, in turn, by both **iPlane** data sets, **DIMES**, and **Ark IPv4Pref IP**. Alias resolution, i.e., aggregating IP addresses into a router-level graph, increases clustering since it decreases the number of nodes but makes them densely connected.

5.2 Characteristics of AS-Level Graphs

Due to the large number of data sources used for AS-level graph comparison, we first analyze AS-graphs within each subgroup: Ark, traceroute, BGP – and then select a representative from each subgroup for our overall comparison which also includes an AS graph derived from WHOIS data.

5.2.1 *Differences between Ark-based AS graphs*

First, we compare AS-graphs constructed directly from Ark data (**Ark IPv4Pref AS**) and from the router-level graph in ITDK (**Ark ITDK AS$_{\text{ro}}$** and **Ark ITDK AS$_{\text{ri}}$**).

Figure 5 illustrates the similarity of our three topological metrics for the three Ark/ITDK-derived AS graphs, although the **Ark ITDK AS$_{\text{ri}}$** graph (the black lines) exhibits higher degrees and higher local clustering than the other two graphs due to the inclusion of the additional links inferred in the process of IP-to-router and router-to-AS mappings.

Degree distributions of the **Ark IPv4Pref AS** (the purple line) and **Ark ITDK AS$_{\text{ro}}$** (the blue line) graphs are noticeably different for the largest nodes with $k > 1000$ (Figure 5(a)). We select the **Ark ITDK AS$_{\text{ro}}$** graph as the representative of our Ark/ITDK-derived group of AS-level Internet graphs for comparison with other traceroute-derived AS-level graphs. This graph is likely more accurate than the **Ark IPv4Pref AS** graph because the former is derived from the router-level graph of the Internet which is a more faithful representation of the real connectivity of the Internet than the IP-level graph. Among the two router-based AS-level graphs, the ***router-observed*** one more closely reflects observed paths, and thus captures some policy restrictions not conveyed in the ***router-inferred*** graph.

5.2.2 *Differences between Traceroute-based AS graphs*

Figure 6 compares the **Ark ITDK AS$_{\text{ro}}$** AS-level topology (the blue line) with the two other traceroute-based AS graphs, **DIMES AS** (the red line) and **iPlane AS** (the green line). The CCDFs of node degree (Figure 6(a)) and local clustering (Figure 6(c)) are similar for all three graphs. For each value of node degree, the average neighbor degree is the highest for the **iPlane AS** graph and the lowest for the **Ark ITDK AS$_{\text{ro}}$** graph (Figure 6(b)).

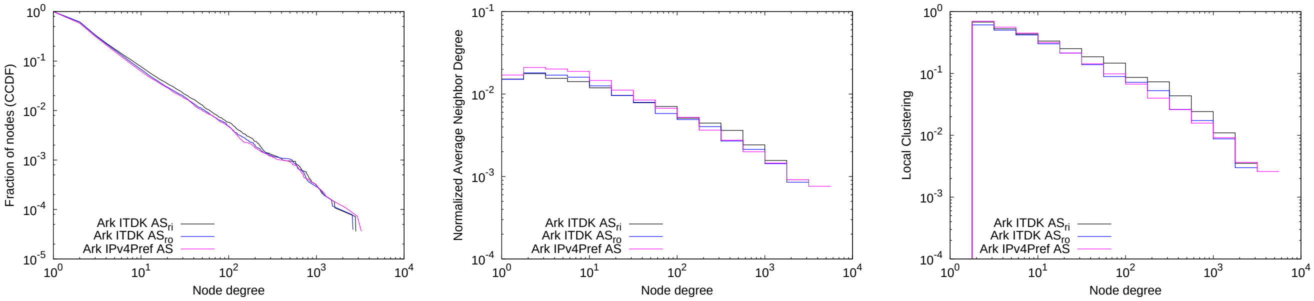
5.2.3 *Differences between BGP-based AS graphs*

Next, we consider the three BGP-based graphs: **RouteViews2** generated from a single largest BGP collector, RouteViews2 server, **BGP Full** derived from all available BGP servers (5 in Routeviews and 14 in RIPE NCC RIS), and **IRL** compiled by IRL from multiple sources. Table 3 shows that the more contributors to a given data set, the more edges and the higher average degree and mean clustering of the resulting topology. This result is intuitive: the more vantage points, the more edges they can observe, in particular tangential links between low- and medium- degree nodes [32] (cf. also Figure 7(a) below).

Figure 7(a), the CCDF of node degree, confirms that **IRL AS** graph (the cyan line), compiled from the largest number of diverse contributors (Route Views, RIPE-NCC RIS,

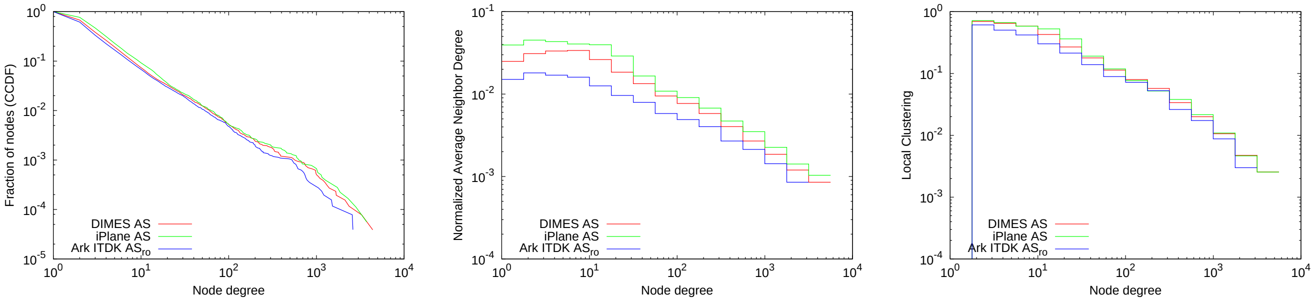
						normalized	mean	γ	
		number of		degree		avg avg	local	lst-sqr	max.-like.
	data type	nodes	edges	avg	max	neig. deg.	clust.	CCDF	deg. seq.
Ark IPv4Pref AS	traceroute	27,399	68,685	5.010	3,245	0.019	0.350		
Ark ITDK AS$_{r}o$	traceroute	25,578	66,401	5.190	2,607	0.016	0.330	2.190	2.180
Ark ITDK AS$_{r}i$	traceroute	27,797	77,965	5.610	2,815	0.018	0.360	2.110	2.200
DIMES AS	traceroute	25,774	78,373	6.080	4,386	0.029	0.430	2.120	2.18
iPlane AS	traceroute	17,937	61,218	6.830	3,753	0.042	0.500	2.110	2.22
RouteViews2 AS	BGP	37,606	80,051	4.260	3,100	0.016	0.210	2.150	2.12
BGP full AS	BGP	36,876	103,481	5.610	2,972	0.014	0.240	2.120	1.97
IRL AS	BGP	38,524	125,105	6.490	3,211	0.015	0.300	2.130	1.900
WHOIS RIPE AS	WHOIS	22,898	134,448	11.740	3,727	0.027	0.370		

Table 3: Basic statistics of AS graphs. All of the data sources other than WHOIS RIPE AS match a model of the AS degree distribution as a power law function with exponent γ between 2.1 and 2.2. The closer the value of the power law exponent to 2, the relatively more hubs (high-degree nodes) in the network.



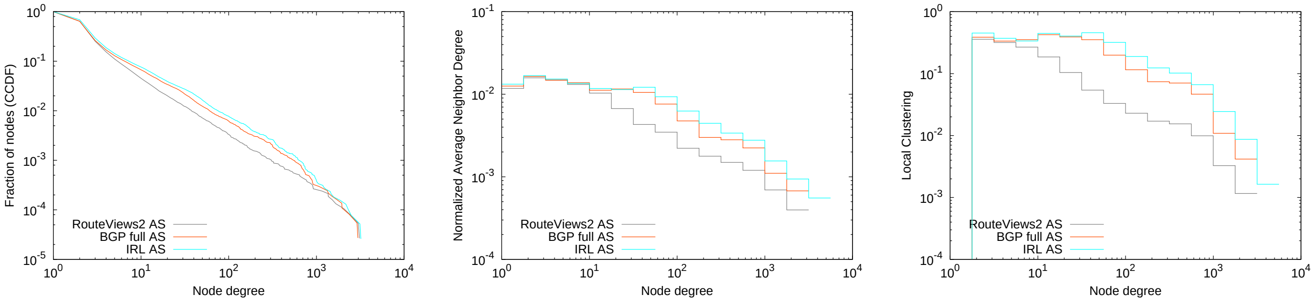
(a) CCDF of Node Degree (b) Average Neighbor Degree (c) Local Clustering

Figure 5: ***Statistical characteristics of the AS-level graphs derived from the Ark/ITDK data using three different methods.***



(a) CCDF of Node Degree (b) Average Neighbor Degree (c) Local Clustering

Figure 6: ***Statistical characteristics of the traceroute-based AS-level graphs.***



(a) CCDF of Node Degree (b) Average Neighbor Degree (c) Local Clustering

Figure 7: ***Statistical characteristics of the AS-level graphs derived from BGP data sources.***

Packet Clearing House, traceroute.org, bgp4.net), has a slightly larger percentage of high-degree nodes than the other two graphs: 0.77% of **IRL AS** nodes have degree greater than 100, compared to 0.62% for **BGP Full AS** and 0.33% for **RouteViews2 AS** data. Although these high-degree nodes make up only a tiny fraction of the total graphs, they represent the top of the Internet routing hierarchy, serving a critical routing function. Notably, AS 3356 (Level3) and AS 174 (Cogent) COGENT are consistently ranked first and second, and ASes 7018 (ATT) and 3549 (Global Crossing) are ranked third and fourth in all data sets except for WHOIS. However, the fractions of nodes with an order of magnitude larger degrees (> 1000) are similar in all three graphs: 0.04%, 0.03%, and 0.02%, for **IRL AS**, **BGP Full AS**, and **RouteViews2 AS**, respectively. Increasing the number and diversity of BGP-data contributors seems to reveal additional connectivity mostly for nodes with medium degrees.

Figure 7(b) shows that for small degrees ($k < 10$ for the **RouteViews2 AS** graph, $k < 70$ for the **IRL AS** and **BGP Full AS** graphs) the average neighbor degree is nearly constant, and it becomes a decreasing function of node degree at larger degrees. AS-level graphs are known [32] to be disassortative: small ASes connect to larger ASes. The flat areas for **BGP full AS** and **IRL AS** for ASes with degrees between 10 and 50 indicate again that the larger number of vantage points used to collect the raw data, the denser connectivity between middle-tier ASes they can capture.

Figure 7(c) shows that as the node degree increases, the local clustering drops much faster for **RouteViews2** (the black line) than for the other two graphs. In contrast, for the **BGP Full AS** and **IRL AS** topologies, the local clustering is approximately constant or even increasing slightly for small node degrees, and starts decreasing only for degrees above 50. Again, a larger number of vantage points captures more tangential links between small nodes. The **BGP Full AS** graph, derived from a combination of multiple BGP tables, is noticeably more complete than the **RouteViews2 AS** graph derived from just a single BGP table, but using a combination of seven diverse contributors in the case of the **IRL AS** graph does not add much to the connectivity already captured from BGP tables.

All the characteristics of the **BGP Full AS** (the red line) and the **IRL AS** (the cyan line) graphs presented in Figure 7 are similar for all node degrees, suggesting that the combination of BGP tables used in the **BGP Full AS** data set is capturing a representative sample of the underlying AS topology even with fewer contributors than the **IRL AS** data set. Therefore, we select the **BGP Full AS** graph as a representative of BGP-derived AS-level graphs for the overall comparison in the next subsection.

5.2.4 All AS-level graphs

The final comparison includes a single representative AS topology graph from each of the previous three AS-level comparisons, and the **RIPE WHOIS AS** graph, which exists as a class of its own.

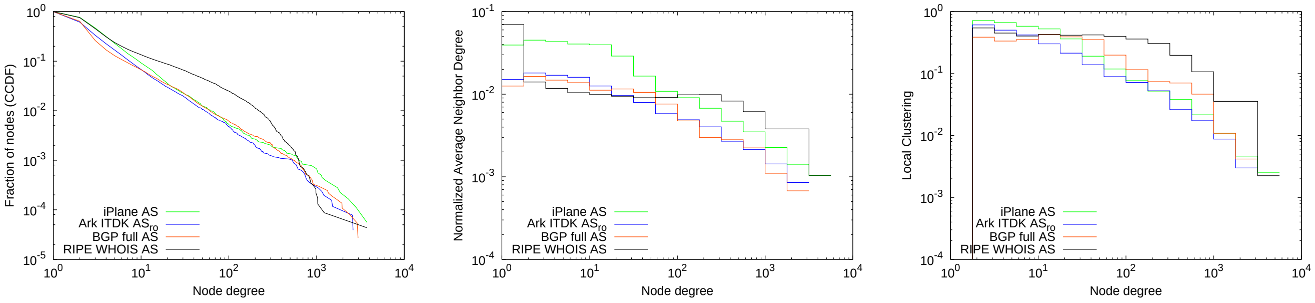
Note that the RIPE NCC service region consists of countries in Europe, the Middle East and parts of Central Asia [4], so the AS graph derived from their WHOIS database represents primarily European connectivity. In [32] when we compared statistical properties of AS-level graphs derived from BGP tables, traceroute measurements, and WHOIS data, we investigated whether the substantial difference in topological properties between the WHOIS-based graph and the other two graphs could be explained by the geographical biases in the data. We confirmed that geographic bias could not fully explain the disparity, since when we took the subset of topology including only nodes common in both the BGP and WHOIS graphs, the resulting reduced graphs preserved the normalized topological properties of the original graphs.

Figure 8(a), the CCDF of node degrees, shows that the **BGP full AS** (the red line) and the **Ark ITDK AS$_{\mathbf{ro}}$** (the blue line) graphs have relatively higher fractions of edge ASes with degrees 1 and 2: 36% and 39% vs. 25% in the **RIPE WHOIS AS** graph (the black line) and 23% in the **iPlane AS** graph (the green line). In comparison with the other three graphs, the **RIPE WHOIS AS** graph has so many nodes with medium degrees, between 5 and 500, that it does not fit a power law function. **iPlane AS** has the largest fraction of ASes with degree > 1000: 0.07% compared to 0.03% or fewer for the **Ark ITDK AS$_{\mathbf{ro}}$**, **BGP full AS**, and **WHOIS RIPE AS** graphs.

Considering the average neighbor degree (Figure 8(b)), we notice that the **RIPE WHOIS AS** graph (the black line) has the largest average neighbor degree for ASes with a degree of 1. In all four graphs, the average AS neighbor degree decreases as the AS degree increases (i.e., the AS-graphs are disassortative), although for the **RIPE WHOIS AS** graph it remains nearly constant for degrees between 2 and 200 and only starts decreasing at larger degrees. This behavior reflects a relative excess of medium-degree nodes in this graph. Among the other three graphs, **iPlane AS** (the green line) has the highest average neighbor degree across all degree ranges while the values of this metric for the **BGP Full AS** and the **Ark ITDK AS$_{\mathbf{ro}}$** graphs are lower and distributed similarly.

The **RIPE WHOIS AS** graph (the black line) also stands apart from the other graphs in Figure 8(c), which depicts local clustering as the function of node degree. For this graph, local clustering remains nearly constant (and mostly higher than for the other three graphs) for node degrees < 200. Comparing the black **RIPE WHOIS AS** lines in Figures 8(b) and 8(c), we see that the inflection points in both plots occur at around node degree of 200. This coincidence could mean that as the average neighbor degree decreases, these neighbors do not have a high enough degree to form clusters by connecting to other (too numerous) neighbors of a given high-degree node.

For the other three graphs in Figure 8(c), we notice that the local clustering in the **iPlane AS** graph (the green line)



(a) CCDF of Node Degree

(b) Average Neighbor Degree

(c) Local Clustering

hs derived from different types of data sources.

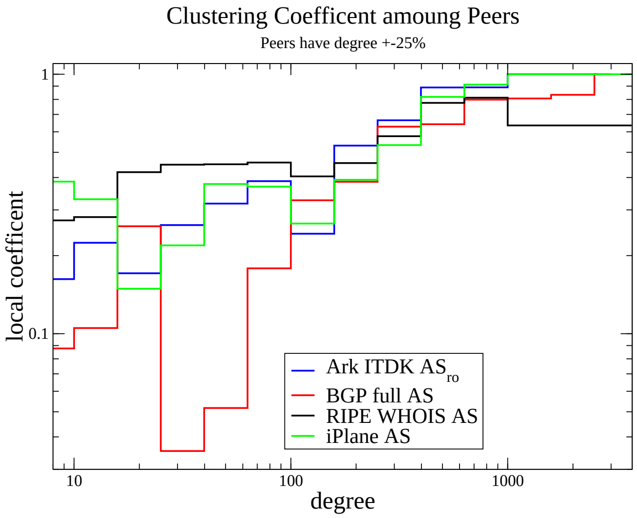


Figure 9: ***Local clustering calculated for subgraphs formed by nodes with degrees within 25% of each other. As the degree increases so does the local clustering coefficient, indicating that nodes of a similar size tend to be interconnected.***

is slightly higher or the same as in the **Ark ITDK AS_{ro}** graph (the blue line) at each degree value. The local clustering of the BGP-based **BGP Full AS** graph (the red line) is lower than that of the traceroute-based **iPlane AS** and **Ark ITDK AS_{ro}** graphs for small degrees < 10, but is higher in the medium degree range of $10 < k < 800$. Consistent with how BGP vs traceroute data is collected, BGP graphs shed more light on higher-degree ASes than on the periphery; conversely, traceroute infrastructures with vantage points scattered at the periphery capture relatively more low-degree nodes.

When studying AS relationships in the real world, we often assume that ASes that are at similar levels in the AS hierarchy enter into peering relationships to decrease transit costs. The manifestation of this assumption in the AS-level graphs is a tendency to form cliques between ASes of a similar size. Figure 9 examines the behavior of local clustering if we include only nodes of roughly the same size into the clustering calculations, specifically, neighbors that have degrees within ±25% of each other. In contrast to Figure 8(c) where local clustering is a decreasing function of node degree, local clustering becomes an increasing function of node degree in Figure 9. This simulation supports the clique-forming hypothesis between ASes of similar sizes. Notably, in this plot, the **RIPE WHOIS AS** clustering is similar to that of the other graphs. So **RIPE WHOIS AS**'s higher clustering values seen for nodes with degrees between 100 and 600 in 8(c) is the result of **RIPE WHOIS AS** having fewer small nodes over all, thus fewer links to lower degree nodes and so do not have their overall clustering lowered.

6. CONCLUSIONS

Researchers need topology maps to describe, analyze, or model Internet structure. Unfortunately, many studies use single, inconsistent, incomplete, or undocumented data sources, which can undermine integrity of research and analysis results. Our objective with this study is to enable more informed selection of topology datasets, by taking a rigorous approach to systematically comparing the topologies inferred from the best available data sources and typically used inference techniques. Following up on our 2006 study [32], we compared topology graphs at three granularities (IP interface, router, and AS) derived from seven different topology data sources: CAIDA's traceroute data, BGP (Routeviews and RIPE NCC RIS), IRR data, RIPE's WHOIS registry, iPlane, DIMES, and IRL. As far as we know, this the most comprehensive study thus far of this type, based on with published sources of data and processing methodologies.

Like many Internet data analysis projects, what seemed like a conceptually straightforward proposition at the beginning turned into an extended struggle with incongruent, incomplete, and underdocumented data sets. For example, before we could even begin to use WHOIS data, which is inconsistently volunteered and maintained by ISPs, we had to heuristically estimate the maximum age of data we would still trust to accurately reflect peering topology. Other challenges included determination of specific processing applied to the traceroute data for each topology granularity, simulating and evaluating different techniques for handling nonresponsive hops, applying our best understanding of alias resolution techniques to the processing and interpretation of the data sources, and comparing the results to a moderately sized and limited ground truth data set – a Tier1 backbone

ISP (with 2420 routers).

We used three definitive statistical metrics to compare topology data sets: CCDF of node degree distribution, and average neighbor degree and local clustering as functions of node degree. When compared to ground truth, none of the topologies perfectly reflect reality, nor do they claim to. Since **iPlane** focuses on capturing the backbone topology not the edge, it has an order of mangitude less nodes than the **DIMES** and **Ark** data sets, but of higher degree. **Iplane**'s alias resolution methods appear to be less aggressive (more conservative) than those we implement to derive our router-level graphs (ITDKs). Even a small fraction of false inferences can substantially affect statistical properties of the graph. To avoid false positives and associated distorted statistics, we use the more conservatively-inferred Ark router-level topology (of the two in each ITDK) in our comparisons.

We also learned that a "full" BGP table derived from a combination of multiple BGP tables is noticeably more complete than just using one BGP table, but the seven diverse contributors in the case of the IRL AS graph did not change the connectivity characteristics significantly from the "full" BGP graph.

All of the data sources other than WHOIS RIPE AS match a model of the AS degree distribution as a power law function with exponent between 2.1 and 2.2, reflecting an abundance of high-degree (hub) nodes in the network. We also confirmed that ASes of similar size tend to interconnect, while the graph is also disassortative, i.e., low-degree ASes tend to connect with high-degree ASes.

The same four ASes (of Level 3, Cogent, ATT, and Global Crossing) are consistently ranked in the top four in our data sets, and the fractions of ASes with peering degree over 1000 is less than 0.04% in all three BGP-based graphs. Consistent with how BGP vs traceroute data is collected, BGP graphs shed more light on higher-degree ASes than on the periphery; and conversely, traceroute infrastructures with vantage points scattered at the periphery capture relatively more low-degree nodes. Increasing the number and diversity of BGP data contributors seems to reveal additional connectivity mostly for nodes with medium degrees.

7. REFERENCES

[1] Archipelago Measurement Infrastructure. `http://www.caida.org/projects/ark/`.

[2] CAIDA AS Rank. `http://as-rank.caida.org/`.

[3] PlanetLab. `http://www.planet-lab.org/`.

[4] RIPE NCC - From Wikipedia, the free encyclopedia. `http://en.wikipedia.org/wiki/RIPE_NCC`.

[5] RIPE NCC Routing Information Service. `http://www.ripe.net/data-tools/stats/ris/routing-information-service/`.

[6] Team Cymru's Bogon list. `http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt`.

[7] Traceroute and Looking Glass applications and code. `http://www.traceroute.org/#source%20code`.

[8] University of Oregon RouteViews Project. `http://www.routeviews.org`.

[9] iffinder Alias Resolution Tool, 2012. `http://www.caida.org/tools/measurement/iffinder/`.

[10] Internet Research Lab, 2012. `http://irl.cs.ucla.edu/`.

[11] Internet Routing Registry, 2012. `http://www.irr.net/`.

[12] Internet Topology Data Kit (ITDK), 2012. `http://www.caida.org/data/active/internet-topology-data-kit/`.

[13] Internet2's BG collections, 2012. `http://www.internet2.edu/observatory/archive/data-collections.html`.

[14] B. Huffaker, M. Fomenkov, and k claffy. Internet Topology Data Comparison. Tech. rep., CAIDA, 2012. `http://www.caida.org/research/topology/topo_comparison`.

[15] Bender, A., Sherwood, R., and Spring, N. Fixing Ally's Growing Pains with Velocity Modeling. In *Proc. of the ACM Internet Measurement Conf.* (2008), pp. 337–342.

[16] Bu, T., and Towsley, D. On Distinguishing between Internet Power Law Topology Generators. In *Proc. of IEEE INFOCOM* (2002), vol. 2, pp. 638–647.

[17] Chen, Q., Chang, H., Govindan, R., Jamin, S., Shenker, S. J., and Willinger, W. The Origin of Power Laws in Internet Topologies Revisited. In *Proc. of IEEE INFOCOM* (2002), pp. 608–617.

[18] Daigle, L. WHOIS Protocol Specification. RFC 3912 (Draft Standard), 2004. `http://www.ietf.org/rfc/rfc3912.txt`.

[19] Faloutsos, M., Faloutsos, P., and Faloutsos, C. On Power-law Relationships of the Internet Topology. In *Proc. of ACM SIGCOMM* (1999), pp. 251–262.

[20] Gaertler, M., and Patrignani, M. Dynamic Analysis of the Autonomous System Graph. In *International Workshop on Inter-domain Performance and Simulation* (2004), pp. 13–24.

[21] Govindan, R., and Tangmunarunkit, H. Heuristics for Internet Map Discovery. In *Proc. of IEEE INFOCOM* (2000), vol. 3, pp. 1371–1380.

[22] Gunes, M., and Sarac, K. Analytical IP Alias Resolution. In *IEEE International Conf. on Communications* (2006), pp. 459–464.

[23] Huffaker, B., Dhamdhere, A., Fomenkov, M., and k. claffy. Toward Topology Dualism: Improving the Accuracy of AS Annotations for Routers. In *Proc. of the Passive and Active Measurement Workshop* (2010), vol. 6032, pp. 101–110.

[24] Jaiswal, S., Rosenberg, A. L., and Towsley, D. Comparing the structure of power-law graphs and the Internet AS graph. In *Proc. of the IEEE International Conf. on Network Protocols* (2004), pp. 294–303.

[25] Keys, K. Internet-Scale IP Alias Resolution Techniques. *ACM SIGCOMM Computer Communications Review 40*, 1 (2010), 50–55.

[26] Keys, K., Hyun, Y., Luckie, M., and k. claffy. Internet-Scale IPv4 Alias Resolution with MIDAR. *Transactions on Networking* (2012). Accepted. `http://www.caida.org/publications/papers/2012/alias_resolution_midar/`.

[27] Kumari, W., and Sriram, K. Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP. RFC 6472 (Best Current Practice), 2011. `http://www.ietf.org/rfc/rfc6472.txt`.

[28] Li, L., Alderson, D., Willinger, W., and Doyle, J. A First-Principles Approach to Understanding the Internet Router-Level Topology. In *Proc. of ACM SIGCOMM* (2004), vol. 34, pp. 3–14.

[29] LUCKIE, M., HYUN, Y., AND HUFFAKER, B. Traceroute Probe Method and Forward IP Path Inference. In *Proc. of the ACM Internet Measurement Conf.* (2008), pp. 311–324.

[30] MADHYASTHA, H. V., ISDAL, T., PIATEK, M., DIXON, C., ANDERSON, T., KRISHNAMURTHY, A., AND VENKATARAMANI, A. iPlane: An Information Plane for Distributed Services. In *7th USENIX Symposium OSDI* (2006), pp. 367–380.

[31] MAHADEVAN, P., KRIOUKOV, D., FALL, K., AND VAHDAT, A. Systematic Topology Analysis and Generation Using Degree Correlations. In *Proc. of ACM SIGCOMM* (2006), no. 4, pp. 135–146.

[32] MAHADEVAN, P., KRIOUKOV, D., FOMENKOV, M., HUFFAKER, B., DIMITROPOULOS, X., K. CLAFFY, AND VAHDAT, A. The Internet AS-Level Topology: Three Data Sources and One Definitive Metric. *ACM SIGCOMM Computer Communications Review 36*, 1 (2006), 17–26.

[33] PANSOIT, J.-J., AND GRAD, D. On Routes and Multicast Trees in the Internet. In *Proc. of ACM SIGCOMM* (1998), vol. 28, pp. 41–50.

[34] REKHTER, Y., AND LI, T. A Border Gateway Protocol (BGP-4). RFC 1771 (Draft Standard), 1995. `http://www.ietf.org/rfc/rfc1771.txt`.

[35] REKHTER, Y., MOSKOWITZ, R. G., KARRENBERG, D., DE GROOT, G. J., AND LEAR, E. Address Allocation for Private Internets. RFC 1918 (Best Current Practice), 1996. `http://www.ietf.org/rfc/rfc1918.txt`.

[36] SHAVITT, Y., AND SHIR, E. DIMES: Let the Internet Measure Itself. *ACM SIGCOMM Computer Communications Review 35*, 5 (2005), 71–74.

[37] SHERRY, J., KATZ-BASSETT, E., PIMENOVA, M., MADHYASTHA, H. V., ANDERSON, T., AND KRISHNAMURTHY, A. Resolving IP Aliases with Prespecified Timestamps. In *Proc. of the ACM Internet Measurement Conf.* (2010), pp. 172–178.

[38] SIGANOS, G., AND FALOUTSOS, M. Analyzing BGP Policies: Methodology and Tool. In *Proc. of IEEE INFOCOM* (2004), pp. 1640–1651.

[39] SPRING, N., MAHAJAN, R., WETHERALL, D., AND ANDERSON, T. Measuring ISP Topologies with Rocketfuel. *IEEE/ACM Transactions on Networking 12*, 1 (2004), 2–16.

[40] TANGMUNARUNKIT, H., GOVINDAN, R., JAMIN, S., SHENKER, S., AND WILLINGER, W. Network Topology Generators: Degree-Based vs. Structural. In *Proc. of ACM SIGCOMM* (2002), vol. 32, pp. 147–159.

[41] ZHOU, S., AND MONDRAGON, R. J. Accurately Modeling the Internet Topology. *Physical Review E 70*, 066108 (2004).

[42] ZHOU, S., AND MONDRAGON, R. J. Redundancy and robustness of AS-level Internet topology and its models. *Electronic Letters 40*, 2 (2004), 151–152.